

Administración de Oracle® Solaris 11.1: servicios de seguridad

Copyright © 2002, 2014, Oracle y/o sus filiales. Todos los derechos reservados.

Este software y la documentación relacionada están sujetos a un contrato de licencia que incluye restricciones de uso y revelación, y se encuentran protegidos por la legislación sobre la propiedad intelectual. A menos que figure explícitamente en el contrato de licencia o esté permitido por la ley, no se podrá utilizar, copiar, reproducir, traducir, emitir, modificar, conceder licencias, transmitir, distribuir, exhibir, representar, publicar ni mostrar ninguna parte, de ninguna forma, por ningún medio. Queda prohibida la ingeniería inversa, desensamblaje o descompilación de este software, excepto en la medida en que sean necesarios para conseguir interoperabilidad según lo especificado por la legislación aplicable.

La información contenida en este documento puede someterse a modificaciones sin previo aviso y no se garantiza que se encuentre exenta de errores. Si detecta algún error, le agradeceremos que nos lo comuniqué por escrito.

Si este software o la documentación relacionada se entrega al Gobierno de EE.UU. o a cualquier entidad que adquiera licencias en nombre del Gobierno de EE.UU. se aplicará la siguiente disposición:

U.S. GOVERNMENT END USERS:

Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

Este software o hardware se ha desarrollado para uso general en diversas aplicaciones de gestión de la información. No se ha diseñado ni está destinado para utilizarse en aplicaciones de riesgo inherente, incluidas las aplicaciones que pueden causar daños personales. Si utiliza este software o hardware en aplicaciones de riesgo, usted será responsable de tomar todas las medidas apropiadas de prevención de fallos, copia de seguridad, redundancia o de cualquier otro tipo para garantizar la seguridad en el uso de este software o hardware. Oracle Corporation y sus subsidiarias declinan toda responsabilidad derivada de los daños causados por el uso de este software o hardware en aplicaciones de riesgo.

Oracle y Java son marcas comerciales registradas de Oracle y/o sus subsidiarias. Todos los demás nombres pueden ser marcas comerciales de sus respectivos propietarios.

Intel e Intel Xeon son marcas comerciales o marcas comerciales registradas de Intel Corporation. Todas las marcas comerciales de SPARC se utilizan con licencia y son marcas comerciales o marcas comerciales registradas de SPARC International, Inc. AMD, Opteron, el logotipo de AMD y el logotipo de AMD Opteron son marcas comerciales o marcas comerciales registradas de Advanced Micro Devices. UNIX es una marca comercial registrada de The Open Group.

Este software o hardware y la documentación pueden ofrecer acceso a contenidos, productos o servicios de terceros o información sobre los mismos. Ni Oracle Corporation ni sus subsidiarias serán responsables de ofrecer cualquier tipo de garantía sobre el contenido, los productos o los servicios de terceros y renuncian explícitamente a ello. Oracle Corporation y sus subsidiarias no se harán responsables de las pérdidas, los costos o los daños en los que se incurra como consecuencia del acceso o el uso de contenidos, productos o servicios de terceros.

Contenido

Prefacio	23
 Parte I Descripción general de la seguridad	 25
1 Servicios de seguridad (descripción general)	27
Seguridad del sistema	28
Servicios criptográficos	29
Servicios de autenticación	30
Autenticación con cifrado	30
Auditoría	31
Política de seguridad	31
 Parte II Seguridad de sistemas, archivos y dispositivos	 33
2 Gestión de seguridad de equipos (descripción general)	35
Control de acceso a un sistema informático	35
Mantenimiento de la seguridad física	35
Mantenimiento del control de inicio de sesión	36
Control de acceso a dispositivos	41
Política de dispositivos (descripción general)	41
Asignación de dispositivos (descripción general)	42
Control de acceso a recursos del equipo	43
Ejecución aleatoria de la disposición del espacio de direcciones	43
Limitación y supervisión del acceso del superusuario	43
Configuración del control de acceso basado en roles para reemplazar al superusuario	44
Prevención del uso indebido involuntario de los recursos del sistema	44
Restricción de archivos ejecutables setuid	46

Uso de la configuración de seguridad predeterminada	46
Uso de funciones de gestión de recursos	46
Uso de zonas de Oracle Solaris	47
Supervisión del uso de los recursos del equipo	47
Supervisión de la integridad de archivos	47
Control de acceso a archivos	48
Protección de archivos con cifrado	48
Uso de listas de control de acceso	48
Uso compartido de archivos entre equipos	49
Restricción de acceso root a archivos compartidos	49
Control de acceso a la red	50
Mecanismos de seguridad de red	50
Autenticación y autorización para acceso remoto	51
Sistemas de cortafuegos	53
Cifrado y sistemas de cortafuegos	53
Comunicación de problemas de seguridad	54
3 Control de acceso a sistemas (tareas)	55
Protección de inicios de sesión y contraseñas (tareas)	55
Protección de inicios de sesión y contraseñas (mapa de tareas)	55
▼ Cómo cambiar la contraseña root	56
▼ Cómo mostrar el estado de inicio de sesión de un usuario	57
▼ Cómo visualizar usuarios sin contraseñas	58
▼ Cómo desactivar temporalmente inicios de sesión de usuarios	58
Acerca de las conexiones fallidas	59
Cambio de algoritmo predeterminado para cifrado de contraseña (tareas)	59
▼ Cómo especificar un algoritmo para cifrado de contraseña	59
▼ Cómo especificar un nuevo algoritmo de contraseña para un dominio NIS	61
▼ Cómo especificar un nuevo algoritmo de contraseña para un dominio LDAP	61
Supervisión y restricción del acceso root (tareas)	62
▼ Cómo supervisar quién está utilizando el comando su	62
▼ Cómo restringir y supervisar inicios de sesión de root	63
Control de acceso a hardware del sistema (tareas)	65
▼ Cómo requerir una contraseña para el acceso al hardware de SPARC	65
▼ Cómo desactivar una secuencia de interrupción del sistema	66

4 Servicio de análisis de virus (tareas)	67
Acerca del análisis de virus	67
Acerca del servicio Vscan	68
Uso del servicio Vscan (tareas)	69
▼ Cómo activar el análisis de virus en un sistema de archivos	69
▼ Cómo activar el servicio Vscan	70
▼ Cómo agregar un motor de análisis	70
▼ Cómo ver propiedades de Vscan	70
▼ Cómo cambiar propiedades de Vscan	71
▼ Cómo excluir archivos del análisis de virus	72
5 Control de acceso a dispositivos (tareas)	73
Configuración de política de dispositivos (tareas)	73
Configuración de política de dispositivos (mapa de tareas)	73
▼ Cómo ver una política de dispositivos	74
▼ Cómo auditar cambios en la política de dispositivos	74
▼ Cómo recuperar información MIB-II IP de un dispositivo /dev/*	75
Gestión de asignación de dispositivos (tareas)	75
Gestión de asignación de dispositivos (mapa de tareas)	75
▼ Cómo activar la asignación de dispositivos	76
▼ Cómo autorizar a usuarios para que asignen un dispositivo	77
▼ Cómo ver la información de asignación de un dispositivo	78
▼ Cómo asignar de manera forzada un dispositivo	78
▼ Cómo desasignar de manera forzada un dispositivo	79
▼ Cómo cambiar los dispositivos que se pueden asignar	79
▼ Cómo auditar la asignación de dispositivos	80
Asignación de dispositivos (tareas)	81
▼ Cómo asignar un dispositivo	81
▼ Cómo montar un dispositivo asignado	82
▼ Cómo desasignar un dispositivo	84
Protección de dispositivos (referencia)	84
Comandos de la política de dispositivos	85
Asignación de dispositivos	85

6 Verificación de la integridad de archivos mediante el uso de BART (tareas)	93
BART (descripción general)	93
Funciones de BART	93
Componentes de BART	94
Uso de BART (tareas)	96
Consideraciones de seguridad de BART	96
Uso de BART (mapa de tareas)	96
▼ Cómo crear un manifiesto de control	96
▼ Cómo personalizar un manifiesto	99
▼ Cómo comparar manifiestos para el mismo sistema a lo largo del tiempo	100
▼ Cómo comparar manifiestos de diferentes sistemas	102
▼ Cómo personalizar un informe de BART especificando atributos de archivos	104
▼ Cómo personalizar un informe de BART mediante un archivo de reglas	104
Manifiestos, archivos de reglas e informes de BART (referencia)	106
Formato de archivo de manifiesto de BART	106
Formato de archivo de reglas de BART	107
Creación de informes de BART	108
7 Control de acceso a archivos (tareas)	111
Uso de permisos UNIX para proteger archivos	111
Comandos para visualizar y proteger archivos	111
Propiedad de archivos y directorios	112
Permisos de archivo UNIX	113
Permisos de archivo especiales (setuid, setgid y bit de permanencia)	113
Valor umask predeterminado	115
Modos de permiso de archivo	116
Uso de listas de control de acceso para proteger archivos UFS	118
Cómo evitar que los archivos ejecutables pongan en riesgo la seguridad	118
Protección de archivos (tareas)	119
Protección de archivos con permisos UNIX (mapa de tareas)	119
▼ Cómo visualizar información de archivos	120
▼ Cómo cambiar el propietario de un archivo	121
▼ Cómo cambiar la propiedad de grupo de un archivo	122
▼ Cómo cambiar los permisos de archivo en modo simbólico	123
▼ Cómo cambiar permisos de archivo en modo absoluto	124

▼ Cómo cambiar permisos de archivo especiales en modo absoluto	125
Protección contra programas con riesgo de seguridad (mapa de tareas)	126
▼ Cómo buscar archivos con permisos de archivo especiales	126
▼ Cómo impedir que programas usen pilas ejecutables	127
Parte III Roles, perfiles de derechos y privilegios	129
8 Uso de roles y privilegios (descripción general)	131
Control de acceso basado en roles (descripción general)	131
RBAC: una alternativa al modelo de superusuario	131
Elementos y conceptos básicos de RBAC	135
Escalada de privilegios	137
Autorizaciones RBAC	138
Autorizaciones y privilegios	139
Aplicaciones con privilegios y RBAC	139
Perfiles de derechos de RBAC	141
Roles de RBAC	141
Shells de perfil y RBAC	142
Ámbito de servicio de nombres y RBAC	142
Consideraciones de seguridad al asignar directamente atributos de seguridad	143
Consideraciones de uso al asignar directamente atributos de seguridad	143
Privilegios (descripción general)	144
Privilegios con protección de procesos del núcleo	144
Descripciones de privilegios	145
Diferencias administrativas en un sistema con privilegios	146
Privilegios y recursos del sistema	147
Cómo se implementan los privilegios	148
Cómo obtienen privilegios los procesos	149
Asignación de privilegios	150
Privilegios y dispositivos	152
Privilegios y depuración	153
Sobre el RBAC en esta versión	153

9	Uso del control de acceso basado en roles (tareas)	155
	Uso de RBAC (tareas)	155
	Visualización y uso de valores predeterminados de RBAC (tareas)	156
	Visualización y uso de valores predeterminados de RBAC (mapa de tareas)	156
	▼ Cómo visualizar todos los atributos de seguridad definidos	157
	▼ Cómo visualizar los derechos asignados	158
	▼ Cómo asumir un rol	161
	▼ Cómo cambiar los atributos de seguridad de un usuario	162
	▼ Cómo usar los derechos administrativos que tiene asignados	164
	Personalización de RBAC para su sitio (tareas)	168
	Configuración inicial de RBAC (mapa de tareas)	168
	▼ Cómo planificar la implementación de RBAC	169
	▼ Cómo crear un rol	171
	▼ Cómo asignar un rol	173
	▼ Cómo auditar roles	174
	▼ Cómo crear un perfil de derechos	175
	▼ Cómo clonar y modificar un perfil de derechos del sistema	177
	▼ Cómo crear una autorización	180
	▼ Cómo agregar propiedades RBAC a las aplicaciones antiguas	181
	▼ Cómo solucionar problemas de asignación de privilegios y RBAC	182
	Gestión de RBAC (tareas)	186
	Gestión de RBAC (mapa de tareas)	186
	▼ Cómo cambiar la contraseña de un rol	187
	▼ Cómo cambiar los atributos de seguridad de un rol	188
	▼ Cómo volver a ordenar atributos de seguridad asignados	189
	▼ Cómo restringir a un administrador a derechos asignados explícitamente	190
	▼ Cómo permitir que un usuario use su propia contraseña para asumir un rol	191
	▼ Cómo cambiar el rol root a un usuario	192
	Uso de privilegios (tareas)	194
	▼ Cómo enumerar los privilegios en el sistema	195
	▼ Cómo determinar los privilegios que se le asignaron directamente	196
	▼ Cómo determinar los comandos con privilegios que puede ejecutar	198
	▼ Cómo determinar los privilegios de un proceso	199
	▼ Cómo determinar los privilegios que necesita un programa	201
	▼ Cómo aplicar una política de privilegio extendida a un puerto	202
	▼ Cómo ejecutar una secuencia de comandos de shell con comandos con privilegios	203

10	Atributos de seguridad en Oracle Solaris (referencia)	205
	Perfiles de derechos	205
	Visualización del contenido de los perfiles de derechos	207
	Orden de búsqueda para atributos de seguridad asignados	207
	Autorizaciones	208
	Convenciones de denominación de autorizaciones	208
	Autoridad de delegación en autorizaciones	209
	Bases de datos RBAC	209
	Bases de datos de RBAC y servicios de nombres	210
	Base de datos user_attr	210
	Base de datos auth_attr	211
	Base de datos prof_attr	211
	Base de datos exec_attr	212
	Archivo policy.conf	212
	Comandos de RBAC	213
	Comandos que gestionan RBAC	213
	Comandos seleccionados que requieren autorizaciones	214
	Con privilegios	215
	Comandos administrativos para la gestión de privilegios	215
	Archivos con información de privilegios	216
	Privilegios y auditoría	217
	Cómo evitar la escalada de privilegios	217
	Aplicaciones antiguas y el modelo de privilegios	218
Parte IV	Servicios criptográficos	219
11	Estructura criptográfica (descripción general)	221
	Introducción a la estructura criptográfica	221
	Terminología de la estructura criptográfica	223
	Ámbito de la estructura criptográfica	225
	Comandos administrativos de la estructura criptográfica	226
	Comandos de nivel de usuario de la estructura criptográfica	226
	Complementos de la estructura criptográfica	227
	Zonas y servicios criptográficos	227
	Estructura criptográfica y FIPS-140	228

Estructura criptográfica y servidores SPARC T-Series en esta versión	228
12 Estructura criptográfica (tareas)	229
Protección de los archivos con la estructura criptográfica (tareas)	229
Protección de archivos con la estructura criptográfica (mapa de tareas)	229
▼ Cómo generar una clave simétrica con el comando pktool	230
▼ Cómo calcular un resumen de un archivo	234
▼ Cómo calcular un MAC de un archivo	236
▼ Cómo cifrar y descifrar un archivo	238
Administración de la estructura criptográfica (tareas)	241
Administración de la estructura criptográfica (mapa de tareas)	241
▼ Cómo mostrar los proveedores disponibles	242
▼ Cómo agregar un proveedor de software	246
▼ Cómo utilizar la estructura criptográfica en modo FIPS-140	248
▼ Cómo evitar el uso de un mecanismo de nivel de usuario	249
▼ Cómo evitar el uso de un proveedor de software de núcleo	251
▼ Cómo mostrar proveedores de hardware	254
▼ Cómo desactivar funciones y mecanismos del proveedor de hardware	255
▼ Cómo actualizar o reiniciar todos los servicios criptográficos	256
13 Estructura de gestión de claves	259
Administración de tecnologías de clave pública (descripción general)	259
Utilidades de la estructura de gestión de claves	260
Gestión de políticas KMF	261
Gestión de complementos de KMF	261
Gestión de almacenes de claves KMF	261
Uso de la estructura de gestión de claves (tareas)	262
Uso de la estructura de gestión de claves (mapa de tareas)	262
▼ Cómo crear un certificado con el comando pktool gencert	263
▼ Cómo importar un certificado al almacén de claves	264
▼ Cómo exportar un certificado y una clave privada en formato PKCS #12	266
▼ Cómo generar una frase de contraseña mediante el comando pktool setpin	267
▼ Cómo generar un par de claves utilizando el comando pktool genkeypair	268
▼ Cómo firmar una solicitud de certificación utilizando el comando pktool signcsr	272
▼ Cómo gestionar complementos de terceros en KMF	273

Parte V	Servicios de autenticación y comunicación segura	275
14	Uso de módulos de autenticación conectables	277
	PAM (descripción general)	277
	Ventajas del uso de PAM	277
	Introducción a la estructura PAM	278
	Cambios en PAM para esta versión	279
	PAM (tareas)	279
	PAM (mapa de tareas)	280
	Planificación de la implementación de PAM	280
	▼ Cómo agregar un módulo PAM	281
	▼ Cómo evitar el acceso de tipo .rhost desde sistemas remotos con PAM	282
	▼ Cómo registrar los informes de errores de PAM	282
	▼ Cómo asignar una política PAM personalizada a un usuario	283
	▼ Cómo asignar una nueva política de derechos a todos los usuarios	284
	Configuración de PAM (referencia)	285
	Orden de búsqueda de configuración PAM	285
	Sintaxis de archivo de configuración de PAM	285
	Política de autenticación por usuario	287
	Cómo funciona el apilamiento PAM	287
	Ejemplo de apilamiento PAM	291
15	Uso de Secure Shell	293
	Secure Shell (descripción general)	293
	Autenticación de Secure Shell	294
	Secure Shell en la empresa	295
	Secure Shell y el proyecto OpenSSH	296
	Secure Shell y FIPS-140	297
	Configuración de Secure Shell (tareas)	298
	Configuración de Secure Shell (mapa de tareas)	298
	▼ Cómo configurar la autenticación basada en host para Secure Shell	298
	▼ Cómo configurar el reenvío del puerto en Secure Shell	301
	▼ Cómo crear excepciones de host y usuario para valores predeterminados de Secure Shell	302
	▼ Cómo crear un directorio aislado para archivos sftp	303

Uso de Secure Shell (tareas)	304
Uso de Secure Shell (mapa de tareas)	304
▼ Cómo generar un par de clave pública y clave privada para utilizar con Secure Shell	305
▼ Cómo cambiar la frase de contraseña de una clave privada de Secure Shell	307
▼ Cómo iniciar sesión en un host remoto con Secure Shell	307
▼ Cómo reducir indicadores de contraseñas en Secure Shell	309
▼ Cómo administrar ZFS con Secure Shell de forma remota	310
▼ Cómo utilizar el reenvío del puerto en Secure Shell	312
▼ Cómo copiar archivos con Secure Shell	313
▼ Cómo configurar conexiones Secure Shell predeterminadas a hosts fuera de un cortafuegos	314
16 Secure Shell (referencia)	317
Una sesión de Secure Shell típica	317
Características de la sesión en Secure Shell	318
Autenticación e intercambio de claves en Secure Shell	318
Ejecución de comandos y reenvío de datos en Secure Shell	319
Configuración de cliente y servidor en Secure Shell	320
Configuración de clientes en Secure Shell	320
Configuración de servidores en Secure Shell	320
Palabras clave en Secure Shell	320
Parámetros específicos de host Secure Shell	325
Secure Shell y variables de entorno de inicio de sesión	325
Mantenimiento de hosts conocidos en Secure Shell	326
Archivos de Secure Shell	326
Comandos de Secure Shell	329
17 Uso de autenticación simple y capa de seguridad	331
SASL (descripción general)	331
SASL (referencia)	332
Complementos de SASL	332
Variable de entorno de SASL	332
Opciones de SASL	333

18 Autenticación de servicios de red (tareas)	335
Descripción general de RPC segura	335
Servicios NFS y RPC segura	335
Autenticación Kerberos	336
Cifrado DES con NFS seguro	336
Autenticación Diffie-Hellman y RPC segura	336
Administración de autenticación con RPC segura (tareas)	340
Administración de RPC segura (mapa de tareas)	340
▼ Cómo reiniciar el servidor de claves RPC segura	340
▼ Cómo configurar una clave Diffie-Hellman para un host NIS	341
▼ Cómo configurar una clave Diffie-Hellman para un usuario NIS	342
▼ Cómo compartir archivos NFS con autenticación Diffie-Hellman	343
 Parte VI Servicio Kerberos	 345
 19 Introducción al servicio Kerberos	 347
¿Qué es el servicio Kerberos?	347
Cómo funciona el servicio Kerberos	348
Autenticación inicial: el ticket de otorgamiento de tickets	349
Autenticaciones Kerberos posteriores	351
Aplicaciones remotas de Kerberos	352
Principales de Kerberos	352
Dominios de Kerberos	353
Servidores Kerberos	354
Servicios de seguridad de Kerberos	355
Componentes de las distintas versiones de Kerberos	356
Componentes de Kerberos	356
Acerca de Kerberos en esta versión	358
 20 Planificación del servicio Kerberos	 361
¿Por qué planificar implementaciones Kerberos?	362
Planificación de dominios Kerberos	362
Nombres de dominio	362
Número de dominios	362

Jerarquía de dominios	363
Asignación de nombres de host en dominios	363
Nombres de principal de servicio y cliente	364
Puertos para KDC y servicios de administración	365
El número de KDC esclavos	365
Asignación de credenciales GSS a credenciales UNIX	366
Migración de usuario automática a dominio Kerberos	366
Qué sistema de propagación de base de datos se debe utilizar	367
Sincronización de reloj dentro de un dominio	367
Opciones de configuración de cliente	367
Mejora de seguridad de inicio de sesión de cliente	368
Opciones de configuración de KDC	368
Confianza de servicios para la delegación	369
Tipos de cifrado Kerberos	369
URL de ayuda en pantalla en la herramienta gráfica de administración de Kerberos	370
21 Configuración del servicio Kerberos (tareas)	371
Configuración del servicio Kerberos (mapa de tareas)	371
Configuración de servicios Kerberos adicionales (mapa de tareas)	372
Configuración de servidores KDC	373
▼ Cómo configurar automáticamente un KDC maestro	374
▼ Cómo configurar interactivamente un KDC maestro	375
▼ Cómo configurar manualmente un KDC maestro	376
▼ Cómo configurar un KDC para utilizar un servidor de datos LDAP	380
▼ Cómo configurar automáticamente un KDC esclavo	386
▼ Cómo configurar interactivamente un KDC esclavo	387
▼ Cómo configurar manualmente un KDC esclavo	388
▼ Cómo refrescar las claves del servicio de otorgamiento de tickets en un servidor maestro	392
Configuración de autenticación entre dominios	393
▼ Cómo establecer la autenticación entre dominios jerárquica	393
▼ Cómo establecer la autenticación entre dominios directa	394
Configuración de servidores de aplicaciones de red de Kerberos	395
▼ Cómo configurar un servidor de aplicaciones de red de Kerberos	396
▼ Cómo utilizar el servicio de seguridad genérico con Kerberos al ejecutar FTP	397

Configuración de servidores NFS con Kerberos	398
▼ Cómo configurar servidores NFS con Kerberos	399
▼ Cómo crear una tabla de credenciales	401
▼ Cómo agregar una única entrada a la tabla de credenciales	401
▼ Cómo proporcionar asignación de credenciales entre dominios	402
▼ Cómo configurar un entorno NFS seguro con varios modos de seguridad de Kerberos ..	403
Configuración de clientes Kerberos	405
Configuración de clientes Kerberos (mapa de tareas)	405
▼ Cómo crear un perfil de instalación de cliente Kerberos	406
▼ Cómo configurar automáticamente un cliente Kerberos	406
▼ Cómo configurar interactivamente un cliente Kerberos	408
▼ Cómo configurar un cliente Kerberos para un servidor de Active Directory	411
▼ Cómo configurar manualmente un cliente Kerberos	412
▼ Cómo desactivar la verificación del ticket de otorgamiento de tickets	418
▼ Cómo acceder a un sistema de archivos NFS protegido con Kerberos como el usuario root	419
▼ Cómo configurar la migración automática de usuarios en un dominio Kerberos	420
▼ Cómo configurar el bloqueo de cuenta	422
▼ Cómo renovar automáticamente todos los tickets de otorgamiento de tickets (TGT)	423
Sincronización de relojes entre clientes Kerberos y KDC	424
Intercambio de un KDC maestro y un KDC esclavo	425
▼ Cómo configurar un KDC esclavo intercambiable	425
▼ Cómo intercambiar un KDC maestro y un KDC esclavo	426
Administración de la base de datos de Kerberos	430
Copia de seguridad y propagación de la base de datos de Kerberos	430
▼ Cómo realizar copias de seguridad de la base de datos de Kerberos	432
▼ Cómo restaurar la base de datos de Kerberos	433
▼ Cómo convertir una base de datos de Kerberos después de una actualización de servidor	433
▼ Cómo reconfigurar un KDC maestro para utilizar la propagación incremental	434
▼ Cómo reconfigurar un KDC esclavo para utilizar la propagación incremental	436
▼ Cómo configurar un KDC esclavo para utilizar la propagación completa	437
▼ Cómo verificar que los servidores KDC estén sincronizados	440
▼ Cómo propagar manualmente la base de datos de Kerberos a los KDC esclavos	442
Configuración de propagación en paralelo	442
Pasos de configuración para la propagación en paralelo	443

Administración del archivo intermedio	444
▼ Cómo eliminar un archivo intermedio	444
▼ Cómo emplear una nueva clave maestra	445
Gestión de un KDC en un servidor de directorios LDAP	447
▼ Cómo mezclar atributos de principales de Kerberos en un tipo de clase de objeto que no es de Kerberos	447
▼ Cómo destruir un dominio en un servidor de directorios LDAP	448
Aumento de la seguridad en servidores Kerberos	448
▼ Cómo restringir el acceso a servidores KDC	449
▼ Cómo utilizar un archivo de diccionario para aumentar la seguridad de contraseñas	449
22 Mensajes de error y resolución de problemas de Kerberos	451
Mensajes de error de Kerberos	451
Mensajes de error de la herramienta SEAM	451
Mensajes de error comunes de Kerberos (A-M)	452
Mensajes de error comunes de Kerberos (N-Z)	462
Resolución de problemas de Kerberos	466
▼ Cómo identificar problemas con números de versión de clave	466
Problemas con el formato del archivo krb5.conf	467
Problemas al propagar la base de datos de Kerberos	467
Problemas al montar un sistema de archivos NFS Kerberizado	468
Problemas de autenticación como usuario root	468
Observación de asignación de credenciales GSS a credenciales UNIX	469
Uso de DTrace con el servicio Kerberos	469
23 Administración de las políticas y los principales de Kerberos (tareas)	471
Maneras de administrar las políticas y los principales de Kerberos	471
Herramienta SEAM	472
Equivalentes de línea de comandos de la herramienta SEAM	473
El único archivo modificado por la herramienta SEAM	474
Funciones de impresión y ayuda en pantalla de la herramienta SEAM	474
Trabajo con listas extensas en la herramienta SEAM	474
▼ Cómo iniciar la herramienta SEAM	475
Administración de los principales de Kerberos	476
Administración de los principales de Kerberos (mapa de tareas)	476

Automatización de la creación de nuevos principales de Kerberos	477
▼ Cómo ver la lista de los principales de Kerberos	478
▼ Cómo ver los atributos de un principal de Kerberos	480
▼ Cómo crear un nuevo principal de Kerberos	482
▼ Cómo duplicar un principal de Kerberos	485
▼ Cómo modificar un principal de Kerberos	485
▼ Cómo suprimir un principal de Kerberos	487
▼ Cómo configurar valores predeterminados para crear nuevos principales de Kerberos ..	487
▼ Cómo modificar los privilegios de administración de Kerberos	488
Administración de las políticas de Kerberos	490
Administración de las políticas de Kerberos (mapa de tareas)	490
▼ Cómo ver la lista de políticas de Kerberos	491
▼ Cómo ver los atributos de una política de Kerberos	493
▼ Cómo crear una nueva política de Kerberos	495
▼ Cómo duplicar una política de Kerberos	497
▼ Cómo modificar una política de Kerberos	497
▼ Cómo suprimir una política de Kerberos	498
Referencia de la herramienta SEAM	499
Descripción de los paneles de la herramienta SEAM	499
Uso de la herramienta SEAM con privilegios de administración de Kerberos limitados .	502
Administración de los archivos keytab	504
Administración de archivos keytab (mapa de tareas)	505
▼ Cómo agregar un principal de servicio de Kerberos a un archivo keytab	505
▼ Cómo eliminar un principal de servicio de un archivo keytab	506
▼ Cómo visualizar la lista de claves (principales) en un archivo keytab	507
▼ Cómo deshabilitar temporalmente la autenticación de un servicio en un host	508
24 Uso de aplicaciones Kerberos (tareas)	511
Gestión de tickets de Kerberos	511
¿Debe preocuparse por los tickets?	511
Creación de un ticket de Kerberos	512
Visualización de tickets de Kerberos	513
Destrucción de tickets de Kerberos	514
Gestión de contraseñas de Kerberos	515
Consejos para elegir una contraseña	515

	Cambio de la contraseña	516
	Otorgamiento de acceso a su cuenta	518
	Comandos de usuario de Kerberos	520
	Descripción general de comandos Kerberizados	520
	Reenvío de tickets de Kerberos	523
	Uso de comandos Kerberizados (ejemplos)	525
25	El servicio Kerberos (referencia)	527
	Archivos de Kerberos	527
	Comandos de Kerberos	529
	Daemons de Kerberos	530
	Terminología de Kerberos	531
	Terminología específica de Kerberos	531
	Terminología específica de la autenticación	531
	Tipos de tickets	532
	Cómo funciona el sistema de autenticación Kerberos	537
	Cómo interactúa el servicio Kerberos con DNS y el servicio nsswitch	537
	Obtención de acceso a un servicio con Kerberos	537
	Obtención de una credencial para el servicio de otorgamiento de tickets	537
	Obtención de una credencial para un servidor	539
	Obtención de acceso a un servicio específico	540
	Uso de los tipos de cifrado de Kerberos	541
	Tabla de uso de gsscred	543
	Diferencias importantes entre Oracle Solaris Kerberos y MIT Kerberos	543
Parte VII	Auditoría en Oracle Solaris	545
26	Auditoría (descripción general)	547
	¿Qué es la auditoría?	547
	Conceptos y terminología de auditoría	548
	Eventos de auditoría	551
	Clases de auditoría y preselección	552
	Registros de auditoría y tokens de auditoría	553
	Módulos de complemento de auditoría	554

Registros de auditoría	555
Almacenamiento y gestión de la pista de auditoría	557
Indicaciones de hora confiables	558
Gestión de un repositorio remoto	558
¿Cómo se relaciona la auditoría con la seguridad?	558
¿Cómo funciona la auditoría?	559
¿Cómo se configura la auditoría?	560
Auditoría en un sistema con zonas de Oracle Solaris	561
Acerca del servicio de auditoría en esta versión	562
27 Planificación de la auditoría	563
Planificación de la auditoría (tareas)	563
▼ Cómo planificar auditoría en zonas	564
▼ Cómo planificar a quién y qué auditar	565
▼ Cómo planificar espacio en el disco para los registros de auditoría	568
▼ Cómo prepararse para transmitir los registros de auditoría al almacenamiento remoto	569
Comprensión de la política de auditoría	571
Control de costos de auditoría	573
Costo de mayor tiempo de procesamiento de datos de auditoría	574
Costo de análisis de datos de auditoría	574
Costo de almacenamiento de datos de auditoría	574
Auditoría eficaz	575
28 Gestión de auditoría (tareas)	577
Configuración del servicio de auditoría (tareas)	577
Configuración del servicio de auditoría (mapa de tareas)	578
▼ Cómo visualizar los valores predeterminados del servicio de auditoría	578
▼ Cómo preseleccionar clases de auditoría	580
▼ Cómo configurar las características de auditoría de un usuario	581
▼ Cómo cambiar la política de auditoría	585
▼ Cómo cambiar controles de colas de auditoría	587
▼ Cómo configurar el alias de correo electrónico audit_warn	589
▼ Cómo agregar una clase de auditoría	590
▼ Cómo cambiar una pertenencia a clase de un evento de auditoría	591
Configuración de registros de auditoría (tareas)	592

Configuración de registros de auditoría (mapa de tareas)	593
▼ Cómo crear sistemas de archivos ZFS para archivos de auditoría	593
▼ Cómo asignar espacio de auditoría para la pista de auditoría	597
▼ Cómo enviar archivos de auditoría a un repositorio remoto	600
▼ Cómo configurar un repositorio remoto para los archivos de auditoría	601
▼ Cómo configurar registros de auditoría syslog	605
Configuración del servicio de auditoría en las zonas (tareas)	607
▼ Cómo configurar todas las zonas de forma idéntica para la auditoría	607
▼ Cómo configurar la auditoría por zona	610
Activación y desactivación del servicio de auditoría (tareas)	611
▼ Cómo refrescar el servicio de auditoría	611
▼ Cómo desactivar el servicio de auditoría	613
▼ Cómo activar el servicio de auditoría	613
Gestión de registros de auditoría en sistemas locales (tareas)	614
Gestión de registros de auditoría en sistemas locales (mapa de tareas)	614
▼ Cómo visualizar definiciones de registros de auditoría	615
▼ Cómo fusionar archivos de auditoría de la pista de auditoría	616
▼ Cómo seleccionar eventos de auditoría de la pista de auditoría	618
▼ Cómo visualizar el contenido de los archivos de auditoría binarios	620
▼ Cómo depurar un archivo de auditoría not_terminated	622
▼ Cómo evitar el desbordamiento de la pista de auditoría	623
Solución de problemas del servicio de auditoría (tareas)	625
Solución de problemas del servicio de auditoría (mapa de tareas)	625
▼ Cómo determinar que la auditoría se está ejecutando	626
▼ Cómo reducir el volumen de los registros de auditoría que se producen	628
▼ Cómo auditar todos los comandos por usuarios	630
▼ Cómo buscar registros de auditoría de los cambios realizados en archivos específicos	632
▼ Cómo actualizar la máscara de preselección de usuarios con sesión iniciada	634
▼ Cómo evitar la auditoría de eventos específicos	635
▼ Cómo limitar el tamaño de los archivos de auditoría binarios	636
▼ Cómo comprimir archivos de auditoría en un sistema de archivos dedicado	637
▼ Cómo auditar inicios de sesión de otros sistemas operativos	638
▼ Cómo auditar transferencias de archivos FTP y SFTP	639

29 Auditoría (referencia)	641
Servicio de auditoría	641
Páginas del comando man del servicio de auditoría	643
Perfiles de derechos para administración de auditoría	644
Auditoría y zonas de Oracle Solaris	645
Archivos de configuración de auditoría y empaquetado	645
Clases de auditoría	646
Sintaxis de la clase de auditoría	646
Complementos de auditoría	647
Servidor de auditoría remoto	648
Política de auditoría	648
Políticas de auditoría para eventos síncronos y asíncronos	649
Características del proceso de auditoría	650
Pista de auditoría	651
Convenciones de nombres de archivos de auditoría binarios	651
Estructura de registro de auditoría	651
Análisis de registro de auditoría	652
Formatos de token de auditoría	653
Token acl	654
Token argument	655
Token attribute	655
Token cmd	655
Token exec_args	656
Token exec_env	656
Token file	656
Token fmri	657
Token group	657
Token header	657
Token ip address	658
Token ip port	658
Token ipc	658
Token IPC_perm	659
Token path	659
Token path_attr	659
Token privilege	660
Token process	660

Token return	660
Token sequence	661
Token socket	661
Token subject	661
Token text	662
Token trailer	662
Token use of authorization	662
Token use of privilege	662
Token user	663
Token xclient	663
Token zonename	663
Glosario	665
Índice	677

Prefacio

Administración de Oracle Solaris 11.1: servicios de seguridad explica cómo administrar las funciones de seguridad en uno o varios sistemas Oracle Solaris.

Nota – Esta versión de Oracle Solaris es compatible con sistemas que usen arquitecturas de las familias de procesadores SPARC y x86. Los sistemas compatibles aparecen en las *Listas de compatibilidad del sistema operativo Oracle Solaris*. Este documento indica las diferencias de implementación entre los tipos de plataforma.

Quién debe utilizar este manual

Este manual está destinado a los administradores que son responsables de la seguridad en los sistemas Oracle Solaris. Para utilizar esta guía, se debe tener más de dos años de experiencia en la administración de sistemas UNIX. Puede resultar útil participar en cursos de formación sobre la administración de sistemas UNIX.

Acceso a Oracle Support

Los clientes de Oracle tienen acceso a soporte electrónico por medio de My Oracle Support. Para obtener más información, visite <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info> o, si tiene alguna discapacidad auditiva, visite <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs>.

Convenciones tipográficas

La siguiente tabla describe las convenciones tipográficas utilizadas en este manual.

TABLA P-1 Convenciones tipográficas

Tipos de letra	Descripción	Ejemplo
AaBbCc123	Los nombres de los comandos, los archivos, los directorios y los resultados que el equipo muestra en pantalla	Edite el archivo <code>.login</code> . Utilice el comando <code>ls -a</code> para mostrar todos los archivos. <code>nombre_sistema%</code> tiene correo.
AaBbCc123	Lo que se escribe, en contraposición con la salida del equipo en pantalla	<code>nombre_sistema% su</code> Contraseña:
<i>aabbcc123</i>	Marcador de posición: sustituir por un valor o nombre real	El comando para eliminar un archivo es <code>rm filename</code> .
<i>AaBbCc123</i>	Títulos de los manuales, términos nuevos y palabras destacables	Consulte el capítulo 6 de la <i>Guía del usuario</i> . Una <i>copia en caché</i> es aquella que se almacena localmente. <i>No</i> guarde el archivo. Nota: Algunos elementos destacados aparecen en negrita en línea.

Indicadores de los shells en los ejemplos de comandos

La tabla siguiente muestra los indicadores de sistema UNIX y los indicadores de superusuario para shells incluidos en el sistema operativo Oracle Solaris. En los ejemplos de comandos, el indicador de shell muestra si el comando debe ser ejecutado por un usuario normal o un usuario con privilegios.

TABLA P-2 Indicadores de shell

Shell	Indicador
Shell Bash, shell Korn y shell Bourne	\$
Shell Bash, shell Korn y shell Bourne para superusuario	#
Shell C	machine_name%
Shell C para superusuario	machine_name#

P A R T E I

Descripción general de la seguridad

Este manual se centra en las funciones que mejoran la seguridad en el SO Oracle Solaris. El manual está pensado para administradores del sistema y usuarios de estas funciones de seguridad. El [Capítulo 1, “Servicios de seguridad \(descripción general\)”](#), presenta los temas que se tratarán en la guía.

Servicios de seguridad (descripción general)

Para mantener la seguridad del SO Oracle Solaris, el software proporciona las siguientes funciones:

- “Seguridad del sistema” en la página 28: la capacidad para evitar la intrusión, proteger los recursos y dispositivos del equipo contra el uso inapropiado, y proteger los archivos contra la modificación maliciosa o involuntaria realizada por usuarios o intrusos.
- “Servicios criptográficos” en la página 29: la capacidad para codificar datos de manera que sólo el remitente y el receptor designado puedan leer el contenido, y para gestionar proveedores criptográficos y objetos de clave pública.
- “Servicios de autenticación” en la página 30: la capacidad para identificar a un usuario de manera segura, lo que requiere el nombre del usuario y alguna forma de prueba, normalmente, una contraseña.
- “Autenticación con cifrado” en la página 30: la capacidad para garantizar que las partes autenticadas se puedan comunicar sin interceptación, modificación ni falsificación.
- “Auditoría” en la página 31: la capacidad para identificar el origen de cambios de seguridad en el sistema, incluidos el acceso a archivos, las llamadas del sistema relacionadas con la seguridad y los errores de autenticación.
- “Política de seguridad” en la página 31: el diseño y la implementación de directrices de seguridad para un sistema o una red de sistemas.

Seguridad del sistema

La seguridad del sistema garantiza que los recursos del sistema sean utilizados correctamente. Los controles de acceso pueden restringir quién tiene permitido el acceso a los recursos en el sistema. Entre las funciones de Oracle Solaris para la seguridad del sistema y el control de acceso se incluyen las siguientes:

- **Herramientas de administración de inicios de sesión:** comandos para supervisar y controlar la capacidad de un usuario para iniciar sesión. Consulte [“Protección de inicios de sesión y contraseñas \(mapa de tareas\)” en la página 55.](#)
- **Acceso a hardware:** comandos para limitar el acceso a la PROM y para restringir las personas que pueden iniciar el sistema. Consulte [“Control de acceso a hardware del sistema \(tareas\)” en la página 65.](#)
- **Acceso a recursos:** herramientas y estrategias para maximizar el uso adecuado de los recursos del equipo y, a la vez, minimizar el uso indebido de dichos recursos. Consulte [“Control de acceso a recursos del equipo” en la página 43.](#)

Para la gestión de recursos en Oracle Solaris Zones, consulte la [Parte I, “Gestión de recursos de Oracle Solaris” de Administración de Oracle Solaris 11.1: zonas de Oracle Solaris, zonas de Oracle Solaris 10 y gestión de recursos.](#)

- **Control de acceso basado en roles (RBAC):** una arquitectura para crear cuentas de usuario restringidas especiales que tengan permitido realizar tareas administrativas específicas. Consulte [“Control de acceso basado en roles \(descripción general\)” en la página 131.](#)
- **Privilegios:** derechos discretos en procesos para realizar operaciones. Estos derechos de procesos se aplican en el núcleo. Consulte [“Privilegios \(descripción general\)” en la página 144.](#)
- **Gestión de dispositivos:** la *política* de dispositivos, además, protege los dispositivos que ya están protegidos con permisos UNIX. La *asignación* de dispositivos controla el acceso a dispositivos periféricos, como un micrófono o una unidad de CD-ROM. Al suprimir la asignación, las secuencias de comandos de limpieza de dispositivos pueden borrar datos del dispositivo. Consulte [“Control de acceso a dispositivos” en la página 41.](#)
- **Verificación de archivo BART:** una instantánea, denominada *manifiesto*, de los atributos de archivo de los archivos en un sistema. Mediante la comparación de los manifiestos entre sistemas o en un sistema a lo largo del tiempo, se pueden supervisar cambios en los archivos a fin de reducir los riesgos de seguridad. Consulte el [Capítulo 6, “Verificación de la integridad de archivos mediante el uso de BART \(tareas\)”.](#)
- **Permisos del archivo:** atributos de un archivo o directorio. Los permisos restringen los usuarios y grupos que tienen permiso para leer, escribir o ejecutar un archivo, o buscar en un directorio. Consulte el [Capítulo 7, “Control de acceso a archivos \(tareas\)”.](#)
- **Software antivirus:** un servicio vscan verifica archivos en busca de virus antes de que una aplicación utilice los archivos. Un sistema de archivos puede invocar este servicio para analizar los archivos en tiempo real para las definiciones de virus más recientes antes que los clientes del sistema de archivos accedan a los archivos.

El análisis en tiempo real se realiza mediante aplicaciones de terceros. Un archivo se puede analizar cuando se abre y después de que se cierra. Consulte el [Capítulo 4, “Servicio de análisis de virus \(tareass\)”](#).

Servicios criptográficos

La criptografía es la ciencia de cifrar y descifrar datos. La criptografía se utiliza para garantizar la integridad, la privacidad y la autenticidad. Integridad significa que los datos no han sido alterados. Privacidad significa que otros usuarios no pueden leer los datos. Autenticidad para datos significa que lo que se ha entregado es lo que se envió. Autenticación de usuario significa que el usuario ha suministrado una o más pruebas de identidad. Los mecanismos de autenticación verifican, matemáticamente, el origen de los datos o la prueba de la identidad. Los mecanismos de cifrado codifican datos, de manera que un observador casual no pueda leer los datos. Los servicios criptográficos proporcionan mecanismos de autenticación y cifrado para aplicaciones y usuarios.

- **Estructura criptográfica:** una estructura central de servicios criptográficos para consumidores en el nivel del núcleo y el nivel del usuario, que se basa en el siguiente estándar: Interfaz de token criptográfico RSA Security Inc. PKCS #11 (Cryptoki). Utiliza contraseñas, IPsec y aplicaciones de terceros. La estructura centraliza fuentes de hardware y software para el cifrado. La biblioteca PKCS #11 proporciona una API para que los desarrolladores de terceros conecten los requisitos criptográficos para sus aplicaciones. Consulte el [Capítulo 11, “Estructura criptográfica \(descripción general\)”](#).
- **Mecanismos de cifrado por aplicación:**
 - Para el uso de DES en RPC seguro, consulte [“Descripción general de RPC segura” en la página 335](#).
 - Para el uso de DES, 3DES, AES y ARCFOUR en el servicio Kerberos, consulte el [Capítulo 19, “Introducción al servicio Kerberos”](#).
 - Para el uso de RSA, DSA y cifrados, como AES en Secure Shell, consulte el [Capítulo 15, “Uso de Secure Shell”](#).
 - Para el uso de algoritmos criptográficos en contraseñas, consulte [“Cambio de algoritmo predeterminado para cifrado de contraseña \(tareass\)” en la página 59](#).
- La estructura de gestión de claves (KMF) proporciona una utilidad central para gestionar objetos de clave pública, incluidos los certificados, las políticas y las claves. KMF gestiona estos objetos para tecnologías de clave pública PKCS #11, NSS y OpenSSL. Consulte el [Capítulo 13, “Estructura de gestión de claves”](#).

Servicios de autenticación

La autenticación es un mecanismo que identifica a un usuario o un servicio según los criterios predefinidos. Los servicios de autenticación abarcan desde pares de nombre y contraseña simples hasta sistemas de desafío y respuesta más elaborados, por ejemplo, tarjetas de token y biometría. Los mecanismos de autenticación compleja dependen de que un usuario proporcione información que sólo él sepa y de que un dato personal se pueda verificar. Un nombre de usuario es un ejemplo de información que la persona sabe. Una tarjeta inteligente o una huella digital, por ejemplo, se pueden verificar. Entre las funciones de Oracle Solaris para autenticación, se incluyen:

- **RPC seguro:** un mecanismo de autenticación que utiliza el [protocolo de Diffie-Hellman](#) para proteger los montajes NFS y un servicio de nombres, como NIS. Consulte “[Descripción general de RPC segura](#)” en la [página 335](#).
- **Módulo de autenticación conectable (PAM):** una estructura que permite que distintas tecnologías de autenticación se conecten en un servicio de entrada del sistema sin recompilar el servicio. Algunos de los servicios de entrada del sistema incluyen login y ftp. Consulte el [Capítulo 14, “Uso de módulos de autenticación conectables”](#).
- **Autenticación sencilla y capa de seguridad (SASL):** una estructura que proporciona servicios de autenticación y seguridad para protocolos de red. Consulte el [Capítulo 17, “Uso de autenticación simple y capa de seguridad”](#).
- **Secure Shell:** un protocolo de inicio de sesión remoto seguro y transferencia que cifra comunicaciones en una red no segura. Consulte el [Capítulo 15, “Uso de Secure Shell”](#).
- **Servicio Kerberos:** una arquitectura de cliente-servidor que proporciona cifrado con autenticación a través de una red segura. Consulte la [Parte VI](#).

Autenticación con cifrado

La autenticación con cifrado es la base de una comunicación segura. La autenticación ayuda a garantizar que el origen y el destino sean las partes deseadas. El cifrado codifica la comunicación en el origen y decodifica la comunicación en el destino. El cifrado impide que los intrusos puedan leer cualquier transmisión que logren interceptar. Entre las funciones de Oracle Solaris para la comunicación segura, se incluyen:

- **Secure Shell:** un protocolo para proteger transferencias de datos y sesiones de red de usuarios interactivos contra intrusiones, usurpaciones de sesión y ataques de tipo “Man-in-the-middle”. La autenticación compleja se proporciona mediante criptografía de clave pública. Los servicios de ventanas X y otros servicios de red se pueden enviar por túnel de manera segura mediante conexiones de Secure Shell para obtener una protección adicional. Consulte el [Capítulo 15, “Uso de Secure Shell”](#).
- **Servicio Kerberos:** una arquitectura de cliente y servidor que proporciona autenticación con cifrado. Consulte la [Parte VI](#).

- **Arquitectura de seguridad de protocolo de Internet (IPsec):** una arquitectura que proporciona protección de datagramas de IP. Las protecciones incluyen la confidencialidad, la integridad sólida de los datos, la autenticación de datos y la integridad de secuencia parcial. Consulte [Protección de la red en Oracle Solaris 11.1](#).

Auditoría

La auditoría es un concepto fundamental del mantenimiento y la seguridad del sistema. La auditoría es el proceso de examinar el historial de las acciones y los eventos en un sistema para determinar lo que ha sucedido. El historial se mantiene en un registro, donde se indica qué se hizo, cuándo se hizo, quién lo hizo y qué se afectó. Consulte la [Parte VII](#).

Política de seguridad

La política de seguridad de frases o [política](#) se utiliza en este manual para referirse a las instrucciones de seguridad de una organización. La política de seguridad de su sitio es el conjunto de reglas que definen la confidencialidad de la información que se está procesando y las medidas que se utilizan para proteger la información contra el acceso no autorizado. Las tecnologías de seguridad, como Secure Shell, autenticación, RBAC, autorización, privilegios y control de recursos, proporcionan medidas para proteger la información.

Algunas tecnologías de seguridad también utilizan la política de palabras cuando se describen aspectos específicos de su implementación. Por ejemplo, Oracle Solaris utiliza opciones de políticas de auditoría para configurar algunos aspectos de la política de auditoría. En la siguiente tabla, se hace referencia al glosario, a las páginas del comando man y a información sobre las funciones que utilizan la palabra "política" para describir aspectos específicos de su implementación.

TABLA 1-1 Uso de la palabra "política" en Oracle Solaris

Término "política"	Páginas del comando man seleccionadas	Más información
política de auditoría	auditconfig(1M)	Capítulo 26, "Auditoría (descripción general)"
política en la estructura criptográfica	cryptoadm(1M)	Capítulo 11, "Estructura criptográfica (descripción general)"
política de dispositivos	getdevpolicy(1M)	"Control de acceso a dispositivos" en la página 41
política Kerberos	krb5.conf(4)	Capítulo 23, "Administración de las políticas y los principales de Kerberos (tareas)"

TABLA 1-1 Uso de la palabra “política” en Oracle Solaris (Continuación)		
Término "política"	Páginas del comando man seleccionadas	Más información
políticas de red	ipfilter(5), ipadm(1M), ike.config(4), ipsecconf(1M), routeadm(1M)	<i>Protección de la red en Oracle Solaris 11.1</i>
política de contraseñas	passwd(1), crypt.conf(4), pam.conf(4), policy.conf(4)	“Mantenimiento del control de inicio de sesión” en la página 36 “Cómo asignar una política PAM personalizada a un usuario” en la página 283
política para tecnologías de clave pública	kmfcfg(1)	Capítulo 13, “Estructura de gestión de claves”
política RBAC	rbac(5), policy.conf(4)	“Archivo policy.conf” en la página 212

P A R T E I I

Seguridad de sistemas, archivos y dispositivos

En esta sección, se trata la seguridad que se puede configurar en un sistema que no está conectado a la red. En los capítulos, se discute sobre la planificación, la supervisión y el control del acceso al disco, a los archivos y a los dispositivos periféricos.

- Capítulo 2, “Gestión de seguridad de equipos (descripción general)”
- Capítulo 3, “Control de acceso a sistemas (tareas)”
- Capítulo 4, “Servicio de análisis de virus (tareas)”
- Capítulo 5, “Control de acceso a dispositivos (tareas)”
- Capítulo 6, “Verificación de la integridad de archivos mediante el uso de BART (tareas)”
- Capítulo 7, “Control de acceso a archivos (tareas)”

Gestión de seguridad de equipos (descripción general)

Mantener la información de una máquina segura es una responsabilidad de administración del sistema importante. En este capítulo, se proporciona información general sobre la gestión de seguridad de equipos.

- “Control de acceso a un sistema informático” en la página 35
- “Control de acceso a dispositivos” en la página 41
- “Control de acceso a recursos del equipo” en la página 43
- “Control de acceso a archivos” en la página 48
- “Control de acceso a la red” en la página 50
- “Comunicación de problemas de seguridad” en la página 54

Control de acceso a un sistema informático

En el espacio de trabajo, todos los equipos conectados a un servidor pueden considerarse como un gran sistema multifacético. Usted es responsable de la seguridad de este sistema más grande. Debe proteger la red contra los desconocidos que intentan obtener acceso. También debe garantizar la integridad de los datos en los equipos de la red.

En el nivel de archivos, Oracle Solaris proporciona funciones de seguridad estándar que usted puede utilizar para proteger archivos, directorios y dispositivos. En los niveles de sistema y de red, los problemas de seguridad son generalmente los mismos. La primera línea de defensa de seguridad es controlar el acceso a su sistema, tal como se describe en las siguientes secciones.

Mantenimiento de la seguridad física

Para controlar el acceso al sistema, debe mantener la seguridad física del entorno informático. Por ejemplo, un sistema cuya sesión está iniciada pero desatendida es vulnerable al acceso no autorizado. Un intruso puede obtener acceso al sistema operativo y a la red. El entorno y el hardware del equipo deben estar físicamente protegidos contra el acceso no autorizado.

Puede proteger un sistema SPARC contra el acceso no autorizado a la configuración de hardware. Utilice el comando `eeprom` para solicitar una contraseña para acceder a la PROM. Para obtener más información, consulte [“Cómo requerir una contraseña para el acceso al hardware de SPARC” en la página 65](#). Para proteger el hardware x86, consulte la documentación del proveedor.

Mantenimiento del control de inicio de sesión

También debe prevenir los inicios de sesión no autorizados en un sistema o en la red. Puede realizar esto mediante la asignación de contraseñas o el control de inicios de sesión. Todas las cuentas de un sistema deben tener una contraseña. Una contraseña es un mecanismo de autenticación simple. Si una cuenta no tiene una contraseña, un intruso que adivina el nombre de un usuario puede acceder a toda la red. Un algoritmo de contraseña complejo protege contra ataques por fuerza bruta.

Cuando un usuario inicia sesión en un sistema, el comando `login` verifica que el servicio de nombres o la base de datos de servicio de directorios sean apropiados según la información en el servicio de cambio de nombres, `svc:/system/name-service/switch`. Las siguientes bases de datos pueden afectar el inicio de sesión:

- `files`: designa los archivos `/etc` en el sistema local
- `ldap`: designa el servicio de directorios LDAP en el servidor LDAP
- `nis`: designa la base de datos NIS en el servidor maestro NIS
- `dns`: designa el servicio de nombre de dominio en la red

Para obtener una descripción del servicio de nombres, consulte la página del comando `man nscd(1M)`. Para obtener información acerca de los servicios de nombres y los servicios de directorios, consulte *Oracle Solaris Administration: Naming and Directory Services*.

El comando `login` verifica el nombre de usuario y la contraseña proporcionados por el usuario. Si el nombre de usuario no está en la base de datos de contraseñas, el comando `login` niega el acceso al sistema. Si la contraseña no es correcta para el nombre de usuario especificado, el comando `login` niega el acceso al sistema. Cuando el usuario proporciona un nombre de usuario válido y la contraseña correspondiente, se le otorga acceso al sistema.

Los módulos PAM pueden optimizar el inicio de sesión a las aplicaciones después de iniciar sesión correctamente en el sistema. Para obtener más información, consulte el [Capítulo 14, “Uso de módulos de autenticación conectables”](#).

Los sistemas Oracle Solaris disponen de mecanismos de autorización y autenticación sofisticados. Para ver una explicación de los mecanismos de autorización y autenticación en el nivel de red, consulte [“Autenticación y autorización para acceso remoto” en la página 51](#).

Gestión de información de contraseñas

Cuando los usuarios inician sesión en un sistema, deben proporcionar un nombre de usuario y una contraseña. Aunque los nombres de usuario son de conocimiento público, las contraseñas deben mantenerse en secreto. Únicamente cada usuario individual debe conocer su contraseña. Los usuarios deben seleccionar sus contraseñas con cuidado y cambiarlas con frecuencia.

Las contraseñas se crean inicialmente al configurar una cuenta de usuario. Para mantener la seguridad de las cuentas de usuario, puede configurar la caducidad de las contraseñas para forzar a los usuarios a que cambien las contraseñas regularmente. También puede desactivar una cuenta de usuario mediante el bloqueo de la contraseña. Para obtener información detallada sobre la administración de contraseñas, consulte el [Capítulo 1, “Gestión de cuentas de usuario y entornos de usuario \(descripción general\)”](#) de *Gestión de las cuentas de usuario y los entornos de usuario en Oracle Solaris 11.1* y la página del comando `man passwd(1)`.

Contraseñas locales

Si la red utiliza archivos locales para autenticar usuarios, la información de contraseñas se conserva en los archivos `/etc/passwd` y `/etc/shadow` del sistema. El nombre de usuario y otra información se conservan en el archivo `/etc/passwd`. La contraseña cifrada se conserva en un archivo *shadow* separado, `/etc/shadow`. Esta medida de seguridad impide que un usuario obtenga acceso a las contraseñas cifradas. Mientras que el archivo `/etc/passwd` está disponible para cualquier persona que pueda iniciar sesión en un sistema, únicamente la cuenta `root` puede leer el archivo `/etc/shadow`. Puede utilizar el comando `passwd` para cambiar la contraseña de un usuario en un sistema local.

Contraseñas NIS

Si la red utiliza NIS para autenticar a los usuarios, la información de contraseñas se conserva en el mapa de contraseñas NIS. NIS no admite la caducidad de las contraseñas. Puede utilizar el comando `passwd -r nis` para cambiar la contraseña de un usuario que está almacenada en un mapa de contraseñas NIS.

Contraseñas LDAP

El servicio de nombres LDAP de Oracle Solaris almacena información de contraseñas e información *shadow* en el contenedor `ou=people` del árbol de directorios LDAP. En el cliente del servicio de nombres LDAP de Oracle Solaris, puede utilizar el comando `passwd -r ldap` para cambiar la contraseña de un usuario. El servicio de nombres LDAP almacena la contraseña en el repositorio LDAP.

La política de contraseñas se aplica en Oracle Directory Server Enterprise Edition. En concreto, el módulo `pam_ldap` del cliente sigue los controles de políticas de contraseñas que se aplican en Oracle Directory Server Enterprise Edition. Para obtener más información, consulte “[Modelo de seguridad de servicios de nombres LDAP](#)” de *Trabajo con servicios de nombres y directorios en Oracle Solaris 11.1*.

Cifrado de contraseña

El cifrado de contraseña seguro proporciona una barrera temprana contra un ataque. El software Oracle Solaris proporciona seis algoritmos de cifrado de contraseña. Los algoritmos [Blowfish](#), [MD5](#) y [SHA](#) proporcionan un cifrado sólido de contraseñas.

Identificadores de algoritmos de contraseña

Puede especificar la configuración de los algoritmos para su sitio en el archivo `/etc/security/policy.conf`. En el archivo `policy.conf`, los algoritmos se denominan según el identificador, como se muestra en la siguiente tabla. Para la asignación identificador-algoritmo, consulte el archivo `/etc/security/crypt.conf`.

TABLA 2-1 Algoritmos de cifrado de contraseña

Identificador	Descripción	Página del comando man de algoritmo
1	El algoritmo MD5 que es compatible con algoritmos MD5 en los sistemas BSD y Linux.	crypt_bsdmd5(5)
2a	El algoritmo Blowfish que es compatible con el algoritmo Blowfish en los sistemas BSD.	crypt_bsdbf(5)
md5	El algoritmo MD5 de Sun, que se considera más fuerte que la versión de MD5 de BSD y Linux.	crypt_sunmd5(5)
5	El algoritmo SHA256. SHA es la sigla en inglés correspondiente al algoritmo de hash seguro. Este algoritmo es un miembro de la familia SHA-2. SHA256 admite contraseñas de 255 caracteres.	crypt_sha256(5)
6	El algoritmo SHA512.	crypt_sha512(5)
__unix__	Descartado. El algoritmo de cifrado tradicional de UNIX. Este algoritmo puede ser útil cuando se conecte a sistemas antiguos.	crypt_unix(5)

Configuración de algoritmos en el archivo `policy.conf`

A continuación, se muestra la configuración predeterminada de los algoritmos en el archivo `policy.conf`:

```
#
...
# crypt(3c) Algorithms Configuration
#
# CRYPT_ALGORITHMS_ALLOW specifies the algorithms that are allowed
to
# be used for new passwords. This is enforced only in crypt_gensalt(3c).
#
CRYPT_ALGORITHMS_ALLOW=1,2a,md5,5,6

# To deprecate use of the traditional unix algorithm, uncomment below
```

```
# and change CRYPT_DEFAULT= to another algorithm. For example,
# CRYPT_DEFAULT=1 for BSD/Linux MD5.
#
#CRYPT_ALGORITHMS_DEPRECATE=__unix__

# The Oracle Solaris default is a SHA256 based algorithm. To revert to
# the policy present in Solaris releases set CRYPT_DEFAULT=__unix__,
# which is not listed in crypt.conf(4) since it is internal to libc.
#
CRYPT_DEFAULT=5
...
```

Al cambiar el valor para CRYPT_DEFAULT, las contraseñas de los usuarios nuevos se cifran con el algoritmo que está asociado al valor nuevo.

Cuando los usuarios existentes cambian sus contraseñas, la manera en que se cifró la contraseña anterior afecta el algoritmo que se utiliza para cifrar la contraseña nueva. Por ejemplo, supongamos lo siguiente: CRYPT_ALGORITHMS_ALLOW=1, 2a, md5, 5, 6 y CRYPT_DEFAULT=1. La siguiente tabla muestra qué algoritmo se utilizaría para generar la contraseña cifrada.

Identificador = algoritmo de contraseña		
Contraseña inicial	Contraseña cambiada	Explicación
1 = crypt_bsmd5	Utiliza el mismo algoritmo	El identificador 1 también es el valor de CRYPT_DEFAULT. La contraseña del usuario se seguirá cifrando con el algoritmo crypt_bsmd5.
2a = crypt_bsdbf	Utiliza el mismo algoritmo	El identificador 2a está en la lista CRYPT_ALGORITHMS_ALLOW. Por lo tanto, la contraseña nueva se cifra con el algoritmo crypt_bsdbf.
md5 = crypt_md5	Utiliza el mismo algoritmo	El identificador md5 está en la lista CRYPT_ALGORITHMS_ALLOW. Por lo tanto, la contraseña nueva se cifra con el algoritmo crypt_md5.
5 = crypt_sha256	Utiliza el mismo algoritmo	El identificador 5 está en la lista CRYPT_ALGORITHMS_ALLOW. Por lo tanto, la contraseña nueva se cifra con el algoritmo crypt_sha256.
6 = crypt_sha512	Utiliza el mismo algoritmo	El identificador 6 está en la lista CRYPT_ALGORITHMS_ALLOW. Por lo tanto, la contraseña nueva se cifra con el algoritmo crypt_sha512.
__unix__ = crypt_unix	Utiliza el algoritmo crypt_bsmd5	El identificador __unix__ no está en la lista CRYPT_ALGORITHMS_ALLOW. Por lo tanto, el algoritmo crypt_unix no se puede utilizar. La contraseña nueva se cifra con el algoritmo CRYPT_DEFAULT.

Para obtener más información sobre la configuración de opciones de algoritmos, consulte la página del comando `man policy.conf(4)`. Para especificar algoritmos de cifrado de contraseña, consulte “Cambio de algoritmo predeterminado para cifrado de contraseña (tareas)” en la página 59.

Cuentas especiales del sistema

La cuenta `root` es una de las diversas cuentas especiales del *sistema*. De estas cuentas, sólo a la cuenta `root` se le asigna una contraseña y se la puede utilizar para iniciar sesión. Con la cuenta `nuucp`, se puede iniciar sesión para realizar transferencias de archivos. Las otras cuentas del sistema sirven para proteger archivos o ejecutar procesos administrativos sin utilizar el poder total de `root`.



Precaución – Nunca cambie la configuración de contraseña de una cuenta del sistema. Las cuentas del sistema de Oracle Solaris se entregan en un estado seguro y protegido.

En la siguiente tabla, se muestran algunas cuentas del sistema junto con sus usos. Las cuentas del sistema realizan funciones especiales. Cada cuenta tiene un UID que es menor que 100.

TABLA 2-2 Cuentas del sistema seleccionado y sus usos

Cuenta del sistema	uid	Uso
root	0	Prácticamente no tiene restricciones. Puede sustituir otros permisos y protecciones. La cuenta <code>root</code> tiene acceso a todo el sistema. La contraseña para la cuenta <code>root</code> debe estar protegida muy cuidadosamente. La cuenta <code>root</code> posee la mayoría de los comandos de Oracle Solaris.
daemon	1	Controla el procesamiento en segundo plano.
bin	2	Posee algunos de los comandos Oracle Solaris.
sys	3	Posee muchos archivos del sistema.
adm	4	Posee algunos archivos administrativos.
lp	71	Posee los archivos de datos del objeto y los archivos de datos de cola de impresión para la impresora.
uucp	5	Posee los archivos de datos del objeto y los archivos de datos de cola de impresión para UUCP, el programa de copia de UNIX a UNIX.
nuucp	9	Utilizada por los sistemas remotos para iniciar sesión en el sistema e iniciar transferencias de archivos.

Inicios de sesión remotos

Los inicios de sesión remotos ofrecen una vía tentadora para los intrusos. Oracle Solaris proporciona varios comandos para supervisar, limitar y desactivar los inicios de sesión remotos. Para conocer los procedimientos, consulte [“Protección de inicios de sesión y contraseñas \(mapa de tareas\)” en la página 55](#).

De manera predeterminada, con los inicios de sesión remotos, no se pueden controlar ni leer determinados dispositivos del sistema, como el mouse, el teclado, el búfer de trama o el dispositivo de audio. Para obtener más información, consulte la página del comando `man logindevperm(4)`.

Control de acceso a dispositivos

Los dispositivos periféricos conectados a un sistema informático presentan un riesgo de seguridad. Los micrófonos pueden captar conversaciones y transmitirlas a sistemas remotos. Los CD-ROM pueden dejar evidencia de información que el siguiente usuario del dispositivo de CD-ROM podrá leer. Se puede acceder a las impresoras de forma remota. Los dispositivos que son una parte integral del sistema también pueden presentar problemas de seguridad. Por ejemplo, las interfaces de red, como bge0, se consideran dispositivos integrales.

El software Oracle Solaris proporciona varios métodos de control de acceso a los dispositivos.

- **Configurar política de dispositivos:** puede requerir que el proceso que accede a un dispositivo determinado se esté ejecutando con un conjunto de privilegios. Los procesos sin estos privilegios no pueden utilizar el dispositivo. En el momento del inicio, el software Oracle Solaris configura la política de dispositivos. Los controladores de terceros se pueden configurar con la política de dispositivos durante la instalación. Después de la instalación, usted, como administrador, puede agregar la política de dispositivos a un dispositivo.
- **Permitir la asignación de dispositivos:** puede requerir que un usuario deba asignar un dispositivo antes del uso. La asignación restringe el uso de un dispositivo a un usuario a la vez. Además, puede exigir que el usuario esté autorizado para utilizar el dispositivo.
- **Impedir que se utilicen los dispositivos:** puede impedir que cualquier usuario de un sistema informático utilice un dispositivo, como un micrófono. Un quiosco informático puede ser una buena opción para evitar que se utilicen determinados dispositivos.
- **Restringir un dispositivo a una zona determinada:** puede asignar el uso de un dispositivo a una zona no global. Para obtener más información, consulte “[Uso de dispositivos en zonas no globales](#)” de *Administración de Oracle Solaris 11.1: zonas de Oracle Solaris, zonas de Oracle Solaris 10 y gestión de recursos*. Para obtener una explicación general de dispositivos y zonas, consulte “[Sistema de archivos /dev en zonas no globales](#)” de *Administración de Oracle Solaris 11.1: zonas de Oracle Solaris, zonas de Oracle Solaris 10 y gestión de recursos*.

Política de dispositivos (descripción general)

El mecanismo de política de dispositivos permite especificar que los procesos que abran un dispositivo requieren determinados privilegios. Únicamente los procesos que se ejecutan con los privilegios especificados por la política de dispositivos pueden acceder a los dispositivos que están protegidos mediante la política de dispositivos. Oracle Solaris proporciona la política de dispositivos predeterminada. Por ejemplo, las interfaces de red, como bge0, requieren que los

procesos que acceden a la interfaz se ejecuten con el privilegio `net_rawaccess`. El requisito se aplica en el núcleo. Para obtener más información sobre los privilegios, consulte [“Privilegios \(descripción general\)” en la página 144](#).

En Oracle Solaris, los dispositivos están protegidos mediante permisos de archivo y la política de dispositivos. Por ejemplo, el archivo `/dev/ip` tiene permisos 666. Sin embargo, únicamente un proceso con los privilegios adecuados puede abrir el dispositivo.

La configuración de la política de dispositivos se puede auditar. El evento de auditoría `AUE_MODDEVPLCY` registra los cambios en la política de dispositivos.

Para obtener más información sobre la política de dispositivos, consulte lo siguiente:

- [“Configuración de política de dispositivos \(mapa de tareas\)” en la página 73](#)
- [“Comandos de la política de dispositivos” en la página 85](#)
- [“Privilegios y dispositivos” en la página 152](#)

Asignación de dispositivos (descripción general)

El mecanismo de asignación de dispositivos permite restringir el acceso a un dispositivo periférico, como un CD-ROM. Si la asignación de dispositivos no está activada, los dispositivos periféricos se protegen únicamente mediante permisos de archivo. Por ejemplo, de manera predeterminada, los dispositivos periféricos están disponibles para los siguientes usos:

- Cualquier usuario puede leer y escribir en un disquete o CD-ROM.
- Cualquier usuario puede conectar un micrófono.
- Cualquier usuario puede acceder a una impresora conectada.

La asignación de dispositivos puede restringir un dispositivo a usuarios autorizados. La asignación de dispositivos también puede impedir que se acceda a un dispositivo en todo momento. Un usuario que asigna un dispositivo tiene el uso exclusivo de ese dispositivo hasta que lo desasigne. Cuando se desasigna un dispositivo, las secuencias de comandos `device-clean` borran los datos restantes. Puede escribir una secuencia de comandos `device-clean` para depurar la información de los dispositivos que no tienen una secuencia de comandos. Para ver un ejemplo, consulte [“Redacción de secuencias nuevas de comandos device-clean” en la página 92](#).

Se pueden auditar los intentos de asignación de un dispositivo, desasignación de un dispositivo y enumeración de los dispositivos asignables. Los eventos de auditoría forman parte de la clase de auditoría `other`.

Para obtener más información sobre la asignación de dispositivos, consulte lo siguiente:

- [“Gestión de asignación de dispositivos \(mapa de tareas\)” en la página 75](#)
- [“Asignación de dispositivos” en la página 85](#)
- [“Comandos de asignación de dispositivos” en la página 87](#)

Control de acceso a recursos del equipo

Algunos recursos del sistema están protegidos de manera predeterminada. Además, como administrador del sistema, puede controlar y supervisar la actividad del sistema. Puede definir límites sobre quién puede utilizar determinados recursos. Puede registrar el uso de recursos y supervisar quién los está utilizando. También puede configurar los sistemas para minimizar el uso indebido de los recursos.

Ejecución aleatoria de la disposición del espacio de direcciones

Oracle Solaris etiqueta muchos de sus datos binarios de espacio de usuarios para activar la ejecución aleatoria de la disposición del espacio de direcciones (ASLR). ASLR ejecuta aleatoriamente la dirección de inicio de partes clave de un espacio de direcciones. Este mecanismo de defensa de seguridad puede hacer que los ataques de la programación orientada al retorno (ROP) fallen cuando traten de explotar las vulnerabilidades de software.

Las zonas heredan esta disposición de ejecución aleatoria para sus procesos. Como el uso de ASLR puede no ser óptimo para todos los datos binarios, el uso de ASLR se puede configurar en el nivel de zona y en el nivel binario.

Estas tres configuraciones de ASLR son posibles:

- **Desactivado:** ASLR está desactivado para todos los datos binarios.
- **Datos binarios etiquetados:** ASLR está controlado por la etiqueta codificada en los datos binarios.
El valor de Oracle Solaris predeterminado para ASLR es `tagged-binaries`. Muchos datos binarios en la versión de Oracle Solaris están etiquetados para usar ASLR.
- **Activado:** ASLR está activado para todos los datos binarios, excepto aquellos explícitamente etiquetados para desactivarlos.

El comando `sxadm` se utiliza para configurar ASLR. Para ejecutar este comando, debe asumir el rol `root`. Para obtener ejemplos e información, consulte la página del comando `man sxadm(1M)`. Para obtener ayuda del desarrollador, consulte *Developer's Guide to Oracle Solaris 11 Security*.

Limitación y supervisión del acceso del superusuario

El sistema requiere una contraseña `root` para el acceso del superusuario. En la configuración predeterminada, un usuario no puede iniciar sesión de manera remota en un sistema como `root`. Al iniciar sesión de manera remota, el usuario debe utilizar el nombre de usuario y, luego, el comando `su` para convertirse en `root`. Puede supervisar quién ha utilizado el comando `su`, en

especial, aquellos usuarios que están intentando obtener acceso de superusuario. Para conocer los procedimientos para supervisar al superusuario y limitar el acceso al superusuario, consulte [“Supervisión y restricción del acceso root \(tareas\)” en la página 62.](#)

Configuración del control de acceso basado en roles para reemplazar al superusuario

El control de accesos basado en roles (RBAC), una función de Oracle Solaris, está diseñado para distribuir las capacidades de superusuario a roles administrativos. El superusuario (usuario root) tiene acceso a todos los recursos del sistema. Con RBAC, puede reemplazar muchas de las responsabilidades de root con un conjunto de roles con funciones discretas. Por ejemplo, puede configurar un rol para manejar la creación de cuentas de usuario y otro rol para manejar la modificación de archivos del sistema. Aunque puede que no modifique la cuenta root, puede dejar la cuenta como un rol y, entonces, no asignar el rol. Esta estrategia de forma eficaz elimina el acceso a la root del sistema.

Cada rol requiere que un usuario conocido inicie sesión con su nombre de usuario y contraseña. Después de iniciar sesión, el usuario asume el rol con una contraseña de rol específica. Para obtener más información sobre RBAC, consulte [“Control de acceso basado en roles \(descripción general\)” en la página 131.](#)

Prevención del uso indebido involuntario de los recursos del sistema

Puede prevenir que los usuarios y que usted realicen errores involuntarios de las siguientes formas:

- Puede evitar ejecutar un caballo de Troya si configura correctamente la variable PATH.
- Puede asignar un shell restringido a los usuarios. Un shell restringido previene los errores del usuario al guiar a los usuarios a las partes del sistema que necesitan para su trabajo. De hecho, mediante una configuración cuidadosa, usted puede asegurarse de que los usuarios sólo accedan a las partes del sistema que los ayudan a trabajar de manera eficiente.
- Puede establecer permisos restrictivos para los archivos a los que los usuarios no necesitan acceder.

Configuración de la variable PATH

Debe asegurarse de configurar correctamente la variable PATH. De lo contrario, puede ejecutar accidentalmente un programa introducido por otra persona. El programa intruso puede dañar los datos o el sistema. Este tipo de programa, que crea un riesgo de seguridad, se conoce como *caballo de Troya*. Por ejemplo, es posible que se coloque un programa su sustituto en un

directorio público y que usted, como administrador del sistema, ejecute el programa sustituto. Esa secuencia de comandos sería igual que el comando su habitual. Debido a que la secuencia de comandos se elimina sola después de la ejecución, habría pocas pruebas para mostrar que, en realidad, se ejecutó un caballo de Troya.

La variable PATH se configura automáticamente en el momento del inicio de sesión. La ruta se define mediante los archivos de inicialización, como `.bashrc` y `/etc/profile`. Si configura la ruta de búsqueda del usuario para que el directorio actual (`.`) esté en último lugar, estará protegido contra la ejecución de este tipo de caballo de Troya. La variable PATH para la cuenta root no debe incluir el directorio actual.

Asignación de un shell restringido a los usuarios

El shell estándar permite que un usuario abra archivos, ejecute comandos, etc. El shell restringido limita la capacidad de un usuario para cambiar directorios y para ejecutar comandos. El shell restringido se invoca con el comando `/usr/lib/rsh`. Tenga en cuenta que el shell restringido no es el shell remoto, que es `/usr/sbin/rsh`.

El shell restringido se diferencia de un shell estándar de las siguientes formas:

- El usuario está limitado al directorio principal del usuario, de modo que no puede utilizar el comando `cd` para cambiar de directorios. Por lo tanto, el usuario no puede examinar los archivos del sistema.
- El usuario no puede cambiar la variable PATH, de manera que sólo puede utilizar comandos en la ruta definida por el administrador del sistema. El usuario tampoco puede ejecutar comandos o secuencias de comandos mediante un nombre completo de ruta.
- El usuario no puede redirigir la salida con `>` o `>>`.

El shell restringido permite limitar la capacidad de un usuario para desviarse hacia los archivos del sistema. El shell crea un entorno limitado para un usuario que necesita realizar tareas específicas. Sin embargo, el shell restringido no es completamente seguro y sólo tiene el propósito de impedir que los usuarios sin experiencia causen daños involuntariamente.

Para obtener información sobre el shell restringido, use el comando `man -s1m rsh` para ver la página del comando `man rsh(1M)`.

Restricción de acceso a datos de archivos

Dado que Oracle Solaris es un entorno multiusuario, la seguridad del sistema de archivos es el riesgo de seguridad más básico de un sistema. Puede utilizar las protecciones de archivos UNIX tradicionales para proteger los archivos. También puede utilizar las listas de control de acceso (ACL) más seguras.

Posiblemente desee permitir que algunos usuarios lean determinados archivos y conceder a otros usuarios permiso para cambiar o suprimir archivos. Es posible que existan datos que no desee que nadie más vea. En el [Capítulo 7, “Control de acceso a archivos \(tareas\)”](#), se describe cómo establecer permisos de archivo.

Restricción de archivos ejecutables `setuid`

Los archivos ejecutables pueden constituir riesgos para la seguridad. Algunos programas ejecutables todavía deben ejecutarse como `root` para que funcionen correctamente. Estos programas `setuid` se ejecutan con el ID de usuario establecido en `0`. Cualquier persona que ejecuta estos programas lo hace con el ID `root`. Un programa que se ejecuta con el ID `root` crea un posible problema de seguridad si el programa no se escribió pensando en la seguridad.

Excepto para los ejecutables que Oracle envía con el bit `setuid` establecido en `root`, debe prohibir el uso de programas `setuid`. Si no puede prohibir el uso de programas `setuid`, debe restringir su uso. Una administración segura requiere pocos programas `setuid`.

Para obtener más información, consulte [“Cómo evitar que los archivos ejecutables pongan en riesgo la seguridad” en la página 118](#). Para ver los procedimientos, consulte [“Protección contra programas con riesgo de seguridad \(mapa de tareas\)” en la página 126](#).

Uso de la configuración de seguridad predeterminada

De forma predeterminada, cuando Oracle Solaris está instalado, se desactiva un gran conjunto de servicios de red. Esta configuración se denomina "seguridad predeterminada" (SBD). Con SBD, el único servicio de red que acepta solicitudes de red es el daemon `sshd`. Todos los demás servicios de red están desactivados o solamente manejan solicitudes locales. Puede activar servicios de red individuales, como `ftp`, con la función de utilidad de gestión de servicios (SMF) de Oracle Solaris. Para obtener más información, consulte las páginas del comando `man netsservices(1M)` y `smf(5)`.

Uso de funciones de gestión de recursos

El software Oracle Solaris ofrece funciones de gestión de recursos. Con estas funciones, usted puede asignar, programar, supervisar y limitar el uso de recursos por parte de aplicaciones en un entorno de consolidación de servidores. La estructura de control de recursos permite establecer restricciones a los recursos del sistema consumidos por los procesos. Estas restricciones ayudan a prevenir ataques de denegación del servicio por parte de una secuencia de comandos que intenta colapsar los recursos del sistema.

Con estas funciones de gestión de recursos, puede designar recursos para proyectos determinados. También puede adaptar dinámicamente los recursos disponibles. Para obtener más información, consulte la [Parte I, “Gestión de recursos de Oracle Solaris” de Administración de Oracle Solaris 11.1: zonas de Oracle Solaris, zonas de Oracle Solaris 10 y gestión de recursos](#).

Uso de zonas de Oracle Solaris

Las zonas de Oracle Solaris proporcionan un entorno de ejecución de aplicaciones en el que los procesos están aislados del resto del sistema dentro de una única instancia del SO Oracle Solaris. Este aislamiento evita que los procesos que se están ejecutando en una zona sean controlados o se vean afectados por los procesos que se están ejecutando en otras zonas. Incluso un proceso que se está ejecutando con capacidades de superusuario no puede ver ni afectar la actividad de otras zonas.

Las zonas de Oracle Solaris son ideales para entornos que tienen varias aplicaciones en un único servidor. Para obtener más información, consulte la [Parte II, “Zonas de Oracle Solaris” de Administración de Oracle Solaris 11.1: zonas de Oracle Solaris, zonas de Oracle Solaris 10 y gestión de recursos](#).

Supervisión del uso de los recursos del equipo

Como administrador del sistema, debe supervisar la actividad del sistema. Debe conocer todos los aspectos de los equipos, incluidos los siguientes:

- ¿Cuál es la carga normal?
- ¿Quién tiene acceso al sistema?
- ¿Cuándo acceden los usuarios al sistema?
- ¿Qué programas se ejecutan generalmente en el sistema?

Con este tipo de conocimiento, puede utilizar las herramientas disponibles para auditar el uso del sistema y supervisar las actividades de usuarios individuales. La supervisión es muy útil cuando se sospecha que existe una infracción de seguridad. Para obtener más información sobre el servicio de auditoría, consulte el [Capítulo 26, “Auditoría \(descripción general\)”](#).

Supervisión de la integridad de archivos

Como administrador del sistema, debe garantizar que los archivos instalados en los sistemas que administra no hayan cambiado de manera inesperada. En las instalaciones de gran tamaño, una herramienta de comparación y elaboración de informes sobre la pila de software en cada uno de los sistemas permite realizar un seguimiento de los sistemas. La herramienta básica de creación de informes de auditoría (BART) permite validar exhaustivamente los sistemas mediante comprobaciones en el nivel de archivos de uno o varios sistemas a lo largo del tiempo. Los cambios en un *manifiesto* BART en varios sistemas, o en un sistema a lo largo del tiempo, pueden validar la integridad de los sistemas. BART permite crear y comparar manifiestos, y proporciona reglas para los informes de secuencias de comandos. Para obtener más información, consulte el [Capítulo 6, “Verificación de la integridad de archivos mediante el uso de BART \(tareas\)”](#).

Control de acceso a archivos

Oracle Solaris es un entorno multiusuario. En un entorno multiusuario, todos los usuarios que iniciaron sesión en un sistema pueden leer los archivos que pertenecen a otros usuarios. Con los permisos de archivo adecuados, los usuarios también pueden utilizar archivos que pertenecen a otros usuarios. Para obtener más información, consulte el [Capítulo 7, “Control de acceso a archivos \(tareas\)”](#). Para obtener instrucciones paso a paso sobre cómo configurar permisos adecuados en los archivos, consulte [“Protección de archivos \(tareas\)” en la página 119](#).

Protección de archivos con cifrado

Para mantener un archivo seguro, puede impedir que otros usuarios accedan a él. Por ejemplo, nadie puede leer un archivo con permisos de `600`, excepto el propietario y la cuenta `root`. De manera similar, un directorio con permisos de `700` es inaccesible. Sin embargo, alguien que adivine su contraseña o que descubra la contraseña `root` puede acceder a ese archivo. Además, el archivo inaccesible se conserva en una cinta de copia de seguridad cada vez que se realiza una copia de seguridad de los archivos del sistema en medios sin conexión.

Los sistemas de archivos ZFS se pueden crear con cifrado de discos. Para obtener más información, consulte [“Cifrado de sistemas de archivos ZFS” de Administración de Oracle Solaris 11.1: sistemas de archivos ZFS](#).

La estructura criptográfica proporciona los comandos `digest`, `mac` y `encrypt`. Los usuarios normales pueden utilizar estos comandos para proteger archivos y directorios. Para obtener más información, consulte el [Capítulo 11, “Estructura criptográfica \(descripción general\)”](#).

Uso de listas de control de acceso

Las ACL pueden proporcionar un mayor control de los permisos de archivo. Puede agregar ACL cuando las protecciones de archivos UNIX tradicionales no son suficientes. Las protecciones de archivos UNIX tradicionales proporcionan permisos de lectura, escritura y ejecución para las tres clases de usuarios: propietario, grupo y otros usuarios. Una ACL proporciona un nivel de seguridad de archivos más específico.

Las ACL permiten definir permisos de archivos detallados, incluidos los siguientes:

- Permisos de propietario de archivo
- Permisos de archivo para el grupo del propietario
- Permisos de archivo para otros usuarios que están fuera del grupo del propietario
- Permisos de archivo para usuarios específicos
- Permisos de archivo para grupos específicos
- Permisos predeterminados para cada una de las categorías anteriores

Para proteger archivos ZFS con listas de control de acceso (ACL), consulte el [Capítulo 7, “Uso de listas de control de acceso y atributos para proteger archivos Oracle Solaris ZFS” de *Administración de Oracle Solaris 11.1: sistemas de archivos ZFS*](#). Para obtener más información sobre el uso de las ACL en sistemas de archivos antiguos, consulte “Uso de listas de control de acceso para proteger archivos UFS” en la página 118.

Uso compartido de archivos entre equipos

Un servidor de archivos de red puede controlar qué archivos están disponibles para uso compartido. Un servidor de archivos de red también puede controlar qué clientes tienen acceso a los archivos y qué tipo de acceso está permitido para esos clientes. En general, el servidor de archivos puede otorgar acceso de lectura y escritura o acceso de sólo lectura a todos los clientes o a clientes específicos. El control de acceso se especifica cuando los recursos están disponibles con el comando `share`.

Al crear un recurso compartido NFS de un sistema de archivos ZFS, el sistema de archivos se comparte permanentemente hasta que se elimine el recurso compartido. SMF gestiona automáticamente el recurso compartido cuando el sistema se reinicia. Para obtener más información, consulte “Oracle Solaris ZFS y sistemas de archivos tradicionales” de [Administración de Oracle Solaris 11.1: sistemas de archivos ZFS](#).

Restricción de acceso root a archivos compartidos

En general, al superusuario no se le permite el acceso root a los sistemas de archivos que se comparten en la red. El sistema NFS impide el acceso root a los sistemas de archivos montados cambiando el usuario del solicitante al usuario `nobody` con el ID de usuario `60001`. Los derechos de acceso del usuario `nobody` son los mismos que se otorgan al público. El usuario `nobody` tiene los derechos de acceso de un usuario sin credenciales. Por ejemplo, si el público sólo tiene permiso de ejecución para un archivo, el usuario `nobody` sólo puede ejecutar ese archivo.

Un servidor NFS puede otorgar acceso root a un sistema de archivos compartidos por host. Para otorgar estos privilegios, utilice la opción `root=hostname` para el comando `share`. Debe utilizar esta opción con cuidado. Para obtener una explicación de opciones de seguridad con NFS, consulte el [Capítulo 3, “Acceso a los sistemas de archivos de red \(referencia\)” de *Gestión de sistemas de archivos de red en Oracle Solaris 11.1*](#).

Control de acceso a la red

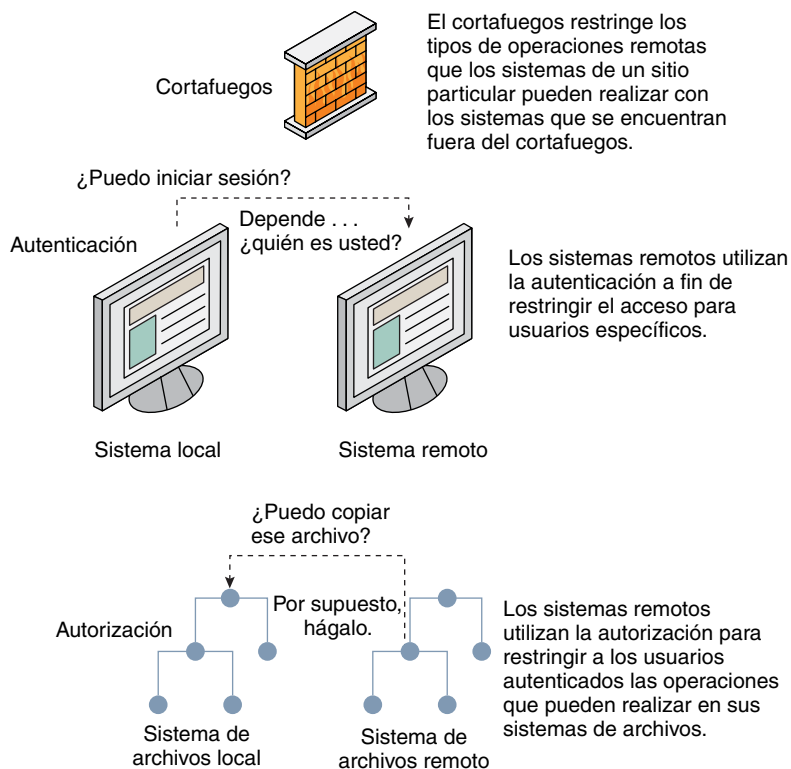
Los equipos suelen formar parte de una *red* de equipos. Una red permite que los equipos conectados intercambien información. Los equipos conectados a la red pueden acceder a datos y demás recursos de otros equipos de la red. Las redes de equipos crean un entorno informático potente y sofisticado. Sin embargo, las redes complican la seguridad de los equipos.

Por ejemplo, dentro de una red de equipos, los sistemas individuales permiten el uso compartido de información. El acceso no autorizado es un riesgo de seguridad. Debido a que muchas personas tienen acceso a una red, el acceso no autorizado es más probable, especialmente como consecuencia de errores del usuario. Un mal uso de contraseñas también puede originar el acceso no autorizado.

Mecanismos de seguridad de red

La seguridad de red, generalmente, se basa en la limitación o el bloqueo de operaciones de sistemas remotos. En la siguiente figura, se describen las restricciones de seguridad que se pueden imponer en las operaciones remotas.

FIGURA 2-1 Restricciones de seguridad para operaciones remotas



Autenticación y autorización para acceso remoto

La *autenticación* es una manera de restringir el acceso a usuarios específicos cuando acceden a un sistema remoto. La autenticación se puede configurar en el nivel del sistema y en el nivel de red. Después de que un usuario haya obtenido acceso a un sistema remoto, la *autorización* es una manera de limitar las operaciones que el usuario puede realizar. En la siguiente tabla, se muestran los servicios que proporcionan autenticación y autorización.

TABLA 2-3 Servicios de autenticación para el acceso remoto

Servicio	Descripción	Para obtener más información
IPsec	IPsec proporciona autenticación basada en host y en certificado, y cifrado de tráfico de red.	Capítulo 6, “Arquitectura de seguridad IP (descripción general)” de <i>Protección de la red en Oracle Solaris 11.1</i>
Kerberos	Kerberos utiliza el cifrado para autenticar y autorizar a un usuario que está iniciando sesión en el sistema.	Para ver un ejemplo, consulte “ Cómo funciona el servicio Kerberos ” en la página 348.

TABLA 2-3 Servicios de autenticación para el acceso remoto (Continuación)

Servicio	Descripción	Para obtener más información
LDAP	El servicio de directorios LDAP puede proporcionar autenticación y autorización a nivel de red.	Oracle Solaris Administration: Naming and Directory Services
Comandos de inicio de sesión remoto	Los comandos de inicio de sesión remoto permiten que los usuarios inicien sesión en un sistema remoto a través de la red y utilicen sus recursos. Algunos de los comandos de inicio de sesión remoto son rlogin, rcp y ftp. Si usted es un "host de confianza", la autenticación es automática. De lo contrario, se le pedirá que se autentique.	Capítulo 3, "Acceso a sistemas remotos (tareas)" de Gestión de sistemas remotos en Oracle Solaris 11.1
SASL	La autenticación sencilla y capa de seguridad (SASL) es una estructura que proporciona autenticación y servicios de seguridad opcionales a los protocolos de red. Los complementos permiten seleccionar el protocolo de autenticación adecuado.	"SASL (descripción general)" en la página 331
RPC segura	Las RPC seguras mejoran la seguridad de los entornos de red al autenticar a los usuarios que realizan solicitudes en equipos remotos. Puede utilizar un mecanismo de autenticación UNIX, DES o Kerberos para las RPC seguras.	"Descripción general de RPC segura" en la página 335
	Las RPC seguras también se pueden utilizar para proporcionar seguridad adicional en un entorno NFS. Un entorno NFS con RPC seguras se denomina NFS seguro.	"Servicios NFS y RPC segura" en la página 335
Secure Shell	Secure Shell cifra el tráfico de red a través de una red no segura. Secure Shell proporciona autenticación mediante el uso de contraseñas, claves públicas, o ambos.	"Secure Shell (descripción general)" en la página 293

Una posible alternativa a las RPC seguras es el mecanismo de *puerto con privilegios* de Oracle Solaris. A un puerto con privilegios se le asigna un número de puerto menor que 1024. Después de que un sistema cliente haya autenticado la credencial del cliente, el cliente crea una conexión al servidor mediante el puerto con privilegios. A continuación, el servidor verifica la credencial del cliente examinando el número de puerto de la conexión.

Es posible que los clientes que no están ejecutando el software Oracle Solaris no puedan comunicarse mediante el puerto con privilegios. Si los clientes no se pueden comunicar a través del puerto, se mostrará un mensaje de error similar al siguiente:

"Weak Authentication
NFS request from unprivileged port"

Sistemas de cortafuegos

Puede configurar un sistema de cortafuegos para proteger los recursos de la red contra el acceso exterior. Un *sistema de cortafuegos* es un host seguro que actúa como una barrera entre la red interna y las redes externas. La red interna trata las otras redes como si no fueran de confianza. Debe considerar esta configuración como obligatoria entre la red interna y cualquier red externa, como Internet, con la que se comunica.

Un cortafuegos actúa como una puerta de enlace y como una barrera. Como puerta de enlace, transfiere datos entre las redes. Como barrera, bloquea la transferencia libre de datos desde y hacia la red. Un usuario de la red interna debe iniciar sesión en el sistema de cortafuegos para acceder a hosts de redes remotas. De forma similar, un usuario de una red externa debe iniciar sesión en el sistema de cortafuegos antes de que se le otorgue acceso a un host de la red interna.

Un cortafuegos también puede ser útil entre algunas redes internas. Por ejemplo, puede configurar un cortafuegos o un equipo de puerta de enlace segura para restringir la transferencia de paquetes por dirección o por protocolo. Por ejemplo, puede permitir paquetes para transferir correo, pero no permitir paquetes para el comando ftp.

Además, todos los correos electrónicos que se envían desde la red interna primero se envían al sistema de cortafuegos. A continuación, el cortafuegos transfiere el correo a un host de una red externa. El sistema de cortafuegos también recibe todos los correos electrónicos entrantes y los distribuye a los hosts de la red interna.



Precaución – Un cortafuegos impide que usuarios no autorizados accedan a los hosts de la red. Debe mantener una seguridad estricta y rigurosa en el cortafuegos, pero la seguridad en otros hosts de la red puede ser más flexible. Sin embargo, si un intruso logra entrar al sistema de cortafuegos, puede acceder a todos los otros hosts de la red interna.

Un sistema de cortafuegos no debe tener hosts de confianza. Un *host de confianza* es un host desde el cual un usuario puede iniciar sesión sin tener que proporcionar una contraseña. Un sistema de cortafuegos no debe compartir ninguno de sus sistemas de archivos ni montar sistemas de archivos de otros servidores.

La función de filtro IP e IPsec de Oracle Solaris puede proporcionar protección de cortafuegos. Para obtener más información sobre la protección de tráfico de red, consulte [Protección de la red en Oracle Solaris 11.1](#).

Cifrado y sistemas de cortafuegos

La mayoría de las redes de área local transmiten datos entre equipos en bloques denominados *paquetes*. Mediante un procedimiento denominado *intercepción de paquetes*, los usuarios no autorizados que están afuera de la red pueden dañar o destruir los datos.

La interceptación de paquetes captura los paquetes antes de que lleguen a destino. A continuación, el intruso inserta datos arbitrarios en el contenido y envía los paquetes de vuelta en su curso original. En una red de área local, la interceptación de paquetes es imposible porque los paquetes llegan a todos los sistemas, incluido el servidor, al mismo tiempo. La interceptación de paquetes puede producirse en una puerta de enlace; por lo tanto, asegúrese de que todas las puertas de enlace de la red estén protegidas.

Los ataques más peligrosos afectan la integridad de los datos. Estos ataques implican cambiar el contenido de los paquetes o suplantar a un usuario. Los ataques que implican intrusiones no comprometen la integridad de los datos. Una intrusión registra conversaciones para reproducirlas más adelante. Una intrusión no implica suplantar a un usuario. Aunque los ataques de intrusión no afectan la integridad de los datos, afectan la privacidad. Puede proteger la privacidad de la información confidencial mediante el cifrado de los datos que se transmiten por la red.

- Para cifrar operaciones remotas a través de una red no segura, consulte el [Capítulo 15, “Uso de Secure Shell”](#).
- Para cifrar y autenticar datos a través de una red, consulte el [Capítulo 19, “Introducción al servicio Kerberos”](#).
- Para cifrar datagramas de IP, consulte el [Capítulo 6, “Arquitectura de seguridad IP \(descripción general\)”](#) de *Protección de la red en Oracle Solaris 11.1*.

Comunicación de problemas de seguridad

Si experimenta una presunta infracción de seguridad, puede ponerse en contacto con el Equipo de Respuesta ante Emergencias Informáticas/Centro de Coordinación (CERT/CC). El CERT/CC es una Agencia de Proyectos de Investigación Avanzada de Defensa (DARPA) que se encuentra en el Instituto de Ingeniería de Software de Universidad Carnegie Mellon. Esta agencia puede ayudarlo con los problemas de seguridad que pueda tener. También puede derivarlo a otros equipos de respuesta ante emergencias informáticas que puedan ser más adecuados para sus necesidades específicas. Para conocer la información de contacto actual, consulte el sitio web de CERT/CC (http://www.cert.org/contact_cert/).

Control de acceso a sistemas (tareas)

En este capítulo, se describen los procedimientos para controlar quién puede acceder a sistemas Oracle Solaris.

En este capítulo, se tratan los siguientes temas:

- “Protección de inicios de sesión y contraseñas (tareas)” en la página 55
- “Cambio de algoritmo predeterminado para cifrado de contraseña (tareas)” en la página 59
- “Supervisión y restricción del acceso root (tareas)” en la página 62
- “Control de acceso a hardware del sistema (tareas)” en la página 65

Para obtener una descripción general sobre la seguridad del sistema, consulte el [Capítulo 2](#), “Gestión de seguridad de equipos (descripción general)”.

Protección de inicios de sesión y contraseñas (tareas)

Puede limitar inicios de sesión remotos, solicitar que los usuarios tengan contraseñas y solicitar que la cuenta root tenga una contraseña compleja. También puede mostrar un mensaje de seguridad a los usuarios, supervisar los intentos de acceso incorrecto, y desactivar los inicios de sesión temporalmente.

Protección de inicios de sesión y contraseñas (mapa de tareas)

El siguiente mapa de tareas hace referencia a procedimientos que supervisan inicios de sesión de usuarios y que desactivan inicios de sesión de usuarios.

Tarea	Descripción	Para obtener instrucciones
Informar a los usuarios de la seguridad de un sitio en el inicio de sesión.	Muestra un mensaje de texto en la pantalla de inicio de sesión con la información de seguridad del sitio.	“Cómo insertar un mensaje de seguridad en archivos de banner” de Directrices de seguridad de Oracle Solaris 11 “Cómo insertar un mensaje de seguridad en la pantalla de inicio de sesión del escritorio” de Directrices de seguridad de Oracle Solaris 11
Cambiar la contraseña de usuario root.	Garantiza que la cuenta root cumpla con los requisitos de contraseñas.	“Cómo cambiar la contraseña root” en la página 56
Visualizar el estado de inicio de sesión de un usuario.	Muestra amplia información sobre la cuenta de inicio de sesión de un usuario, por ejemplo, el nombre completo y la caducidad de las contraseñas.	“Cómo mostrar el estado de inicio de sesión de un usuario” en la página 57
Buscar usuarios que no tienen contraseñas.	Busca sólo aquellos usuarios cuyas cuentas no necesitan una contraseña.	“Cómo visualizar usuarios sin contraseñas” en la página 58
Desactivar inicios de sesión temporalmente.	Deniega inicios de sesión de usuario a un equipo como parte del cierre o mantenimiento de rutina del sistema.	“Cómo desactivar temporalmente inicios de sesión de usuarios” en la página 58

▼ Cómo cambiar la contraseña root

Para cambiar la contraseña root, debe cumplir con los requisitos de contraseñas que se aplican a todos los usuarios del sistema.

Antes de empezar Debe asumir el rol root. Para obtener más información, consulte [“Cómo usar los derechos administrativos que tiene asignados” en la página 164](#).

● Cambie la contraseña.

```
# passwd root
New Password:
Re-enter new Password:
passwd: password successfully changed for root
```

Un mensaje aparecerá en la pantalla si su contraseña no cumple con los requisitos. Los mensajes son informativos. Después de tres intentos, debe volver a ejecutar el comando nuevamente para cambiar la contraseña.

```
passwd: Password too short - must be at least 6 characters.
passwd: The password must contain at least 2 alphabetic character(s).
passwd: The password must contain at least 1 numeric or special character(s).
```

▼ Cómo mostrar el estado de inicio de sesión de un usuario

Antes de empezar Debe asumir el rol root. Para obtener más información, consulte [“Cómo usar los derechos administrativos que tiene asignados” en la página 164](#).

- Visualice el estado de inicio de sesión de un usuario mediante el comando `logins`.

```
# logins -x -l username
```

`-x` Muestra un conjunto ampliado de información de estado de inicio de sesión.

`-l username` Muestra el estado de inicio de sesión para el usuario especificado. La variable `username` es el nombre de inicio de sesión de un usuario. Varios nombres de inicio de sesión se separan con comas.

El comando `logins` utiliza la base de datos de contraseñas adecuada para obtener el estado de inicio de sesión de un usuario. La base de datos puede ser el archivo `/etc/passwd` local o una base de datos de contraseñas para el servicio de nombres. Para obtener más información, consulte la página del comando `man logins(1M)`.

Ejemplo 3–1 Visualización del estado de inicio de sesión de un usuario

En el ejemplo siguiente, se muestra el estado de inicio de sesión del usuario `jdoe`.

```
# logins -x -l jdoe
jdoe      500      staff      10      Jaylee Jaye Doe
           /home/jdoe
           /bin/bash
PS 010103 10 7 -1
```

`jdoe` Identifica el nombre de inicio de sesión del usuario.

`500` Identifica el ID de usuario (UID).

`staff` Identifica el grupo principal del usuario.

`10` Identifica el ID de grupo (GID).

`Jaylee Jaye Doe` Identifica el comentario.

`/home/jdoe` Identifica el directorio principal del usuario.

`/bin/bash` Identifica el shell de inicio de sesión.

```
PS 010170 10 7 -1
```

Especifica la información de caducidad de las contraseñas:

- Última fecha en la que se cambió la contraseña
- Número de días que son necesarios entre los cambios

- Número de días antes de que un cambio sea necesario
- Período de advertencia

▼ Cómo visualizar usuarios sin contraseñas

Antes de empezar Debe asumir el rol root. Para obtener más información, consulte [“Cómo usar los derechos administrativos que tiene asignados” en la página 164.](#)

- Visualice todos los usuarios que no tienen contraseñas con el comando `logins`.

```
# logins -p
```

La opción `-p` muestra una lista de usuarios que no tienen contraseñas. El comando `logins` utiliza la base de datos `passwd` del sistema local a menos que se especifique un servicio de nombres distribuido en la propiedad `password` del servicio `system/name-service/switch`.

Ejemplo 3-2 Visualización de cuentas sin contraseñas

En el siguiente ejemplo, el usuario `pmorph` y el rol `roletop` no tienen contraseñas.

```
# logins -p
pmorph      501      other      1      Polly Morph
roletop     211      admin     1      Role Top
#
```

▼ Cómo desactivar temporalmente inicios de sesión de usuarios

Desactive temporalmente inicios de sesión de usuarios durante el cierre o el mantenimiento de rutina del sistema. Los inicios de sesión root no se ven afectados. Para obtener más información, consulte la página del comando `man nologin(4)`.

Antes de empezar Debe convertirse en un administrador con la autorización `solaris.admin.edit/etc/nologin` asignada. De manera predeterminada, el rol root tiene esta autorización. Para obtener más información, consulte [“Cómo usar los derechos administrativos que tiene asignados” en la página 164.](#)

- 1 Cree el archivo `/etc/nologin` en un editor de texto.

```
# pfedit /etc/nologin
```

Para ver un ejemplo del uso de la autorización `solaris.admin.edit/etc/nologin`, consulte [Ejemplo 3-3.](#)

- 2 Incluya un mensaje sobre la disponibilidad del sistema.
- 3 Cierre y guarde el archivo.

Ejemplo 3-3 Desactivación de inicios de sesión de usuarios

En este ejemplo, un usuario tiene autorización para escribir la notificación de que un sistema no está disponible.

```
% pfedit /etc/nologin
***No logins permitted.***

***The system will be unavailable until 12 noon.***
```

Acerca de las conexiones fallidas

Para supervisar todas las conexiones fallidas en el sistema, consulte la pista de auditoría que genera el servicio de auditoría. Para obtener más información, consulte [Parte VII](#).

Cambio de algoritmo predeterminado para cifrado de contraseña (tareas)

De manera predeterminada, las contraseñas de usuario se cifran con el algoritmo `crypt_sha256`. Si lo desea, puede cambiar el algoritmo predeterminado para interoperar en un entorno de red heterogéneo, por ejemplo, para iniciar sesión en sistemas antiguos que se utilizan frecuentemente en la red.

▼ Cómo especificar un algoritmo para cifrado de contraseña

En este procedimiento, la versión de BSD-Linux del algoritmo MD5 es el algoritmo de cifrado predeterminado que se utiliza cuando los usuarios cambian sus contraseñas. Este algoritmo es adecuado para una red mixta de sistemas que ejecutan las versiones de Oracle Solaris, BSD y Linux de UNIX. Para obtener una lista de algoritmos de cifrado de contraseña e identificadores de algoritmo, consulte la [Tabla 2-1](#).

Antes de empezar Debe asumir el rol `root`. Para obtener más información, consulte “[Cómo usar los derechos administrativos que tiene asignados](#)” en la página 164.

- **Especifique el identificador para el algoritmo de cifrado seleccionado.**

Escriba el identificador como el valor de la variable CRYPT_DEFAULT en el archivo `/etc/security/policy.conf`.

Puede que desee comentar el archivo para explicar su elección.

```
# cat /etc/security/policy.conf
...
CRYPT_ALGORITHMS_ALLOW=1,2a,md5,5,6
#
# Use the version of MD5 (5) that works with Linux and BSD systems.
# Passwords previously encrypted with SHA256 (1) will be encrypted
# with MD5 when users change their passwords.
#
#
#CRYPT_DEFAULT=5
CRYPT_DEFAULT=1
```

En este ejemplo, la configuración de algoritmos garantiza que el algoritmo sha256 no se utiliza para cifrar una contraseña. Los usuarios cuyas contraseñas se cifraron con el módulo sha256 obtienen una contraseña cifrada con `crypt_bsdmd5` cuando cambian sus contraseñas.

Para obtener más información sobre la configuración de opciones de algoritmos, consulte la página del comando `man policy.conf(4)`.

Ejemplo 3–4 Restricción de algoritmos de cifrado de contraseña en un entorno heterogéneo

En este ejemplo, el administrador en una red que incluye los sistemas BSD y Linux configura las contraseñas para que se puedan usar en todos los sistemas. Debido a que algunas aplicaciones de red no pueden manejar cifrado SHA512, el administrador no incluye su identificador en la lista de algoritmos permitidos. El administrador conserva el algoritmo SHA256, 5 como valor para la variable CRYPT_DEFAULT. La variable CRYPT_ALGORITHMS_ALLOW contiene el identificador MD5, que es compatible con sistemas BSD y Linux, y el identificador Blowfish, que es compatible con sistemas BSD. Debido a que 5 es el algoritmo CRYPT_DEFAULT, no es necesario incluirlo en la lista CRYPT_ALGORITHMS_ALLOW. Sin embargo, con fines de mantenimiento, el administrador coloca 5 en la lista CRYPT_ALGORITHMS_ALLOW y los identificadores no utilizados en la lista CRYPT_ALGORITHMS_DEPRECATED.

```
CRYPT_ALGORITHMS_ALLOW=1,2a,5
#CRYPT_ALGORITHMS_DEPRECATED=__unix__,md5,6
CRYPT_DEFAULT=5
```


▼ Cómo especificar un nuevo algoritmo de contraseña para un dominio NIS

Cuando los usuarios en un dominio NIS cambian sus contraseñas, el cliente NIS consulta su configuración local de algoritmos en el archivo `/etc/security/policy.conf`. El sistema cliente NIS cifra la contraseña.

Antes de empezar Debe asumir el rol root. Para obtener más información, consulte [“Cómo usar los derechos administrativos que tiene asignados” en la página 164](#).

- 1 Especifique el algoritmo de cifrado de contraseña en el archivo `/etc/security/policy.conf` del cliente NIS.
- 2 Copie el archivo `/etc/security/policy.conf` modificado en cada sistema cliente del dominio NIS.
- 3 Para evitar confusiones, copie el archivo `/etc/security/policy.conf` modificado en el servidor raíz NIS y en los servidores esclavos.

▼ Cómo especificar un nuevo algoritmo de contraseña para un dominio LDAP

Cuando el cliente LDAP se ha configurado correctamente, el cliente LDAP puede utilizar los nuevos algoritmos de contraseña. El cliente LDAP se comporta igual que el cliente NIS.

Antes de empezar Debe asumir el rol root. Para obtener más información, consulte [“Cómo usar los derechos administrativos que tiene asignados” en la página 164](#).

- 1 Especifique un algoritmo de cifrado de contraseña en el archivo `/etc/security/policy.conf` del cliente LDAP.
- 2 Copie el archivo `policy.conf` modificado en cada sistema cliente del dominio LDAP.
- 3 Asegúrese de que el archivo `/etc/pam.conf` no utilice un módulo `pam_ldap`. Asegúrese de que un signo de comentario (`#`) preceda las entradas que incluyen `pam_ldap.so.1`. Además, no utilice la opción `server_policy` con el módulo `pam_authtok_store.so.1`.

Las entradas PAM en el archivo `pam.conf` del cliente permiten que la contraseña se cifre según la configuración local de algoritmos. Las entradas PAM también permiten que la contraseña se autentique.

Cuando los usuarios en el dominio LDAP cambian sus contraseñas, el cliente LDAP consulta su configuración local de algoritmos en el archivo `/etc/security/policy.conf`. El sistema cliente LDAP cifra la contraseña. A continuación, el cliente envía la contraseña cifrada, con una etiqueta `{crypt}`, al servidor. La etiqueta indica al servidor que la contraseña ya se ha cifrado. La contraseña se almacena, tal como está, en el servidor. Para la autenticación, el cliente recupera la contraseña almacenada desde el servidor. A continuación, el cliente compara la contraseña almacenada con la versión cifrada que el cliente acaba de generar a partir de la contraseña introducida del usuario.

Nota – Para aprovechar los controles de política de contraseña en el servidor LDAP, utilice la opción `server_policy` con las entradas `pam_authtok_store` en el archivo `pam.conf`. Las contraseñas se cifran en el servidor LDAP. Para conocer el procedimiento, consulte [Capítulo 11, “Configuración de Oracle Directory Server Enterprise Edition con clientes LDAP \(tareas\)”](#) de *Trabajo con servicios de nombres y directorios en Oracle Solaris 11.1*.

Supervisión y restricción del acceso root (tareas)

De manera predeterminada, el rol `root` se asigna el usuario inicial, y no puede iniciar sesión directamente en el sistema local ni de manera remota en cualquier sistema Oracle Solaris.

▼ Cómo supervisar quién está utilizando el comando `su`

El archivo `su.log` lista cada uso del comando (`su`) del usuario de cambio, no sólo los intentos de `su` que se utilizan para cambiar de usuario a `root`.

Antes de empezar Debe asumir el rol `root`. Para obtener más información, consulte [“Cómo usar los derechos administrativos que tiene asignados”](#) en la página 164.

- Supervise el contenido del archivo `/var/adm/suLog` de manera regular.

```
# more /var/adm/suLog
SU 12/20 16:26 + pts/0 stacey-root
SU 12/21 10:59 + pts/0 stacey-root
SU 01/12 11:11 + pts/0 root-rimmer
SU 01/12 14:56 + pts/0 jdoe-root
SU 01/12 14:57 + pts/0 jdoe-root
```

Las entradas muestran la información siguiente:

- La fecha y la hora en las que el comando se introdujo.
- Si el intento se realizó correctamente. Un signo más (+) indica un intento con éxito. Un signo menos (-) indica un intento fallido.
- El puerto desde el que se ha ejecutado el comando.
- El nombre del usuario y el nombre de la identidad cambiada.

El registro de su en este archivo se activa de manera predeterminada mediante la siguiente entrada en el archivo `/etc/default/su`:

```
SULOG=/var/adm/sulog
```

Errores más frecuentes

Las entradas que incluyen ??? indican que el terminal de control para el comando su no se pueden identificar. Normalmente, las invocaciones del sistema del comando su antes de que el escritorio aparezca incluyen ???, como en `SU 10/10 08:08 + ??? root - root`. Después de que el usuario inicia una sesión de escritorio, el comando `ttynam` devuelve el valor del terminal de control a `sulog`: `SU 10/10 10:10 + pts/3 jdoe - root`.

Las entradas similares a las siguientes pueden indicar que el comando su no fue invocado en la línea de comandos: `SU 10/10 10:20 + ??? root - oracle`. Es posible que un usuario de Trusted Extensions haya cambiado al rol `oracle` utilizando una GUI.

▼ Cómo restringir y supervisar inicios de sesión de root

Este método permite detectar inmediatamente los intentos de acceso al sistema local por parte del usuario root.

Antes de empezar

Debe asumir el rol root. Para obtener más información, consulte [“Cómo usar los derechos administrativos que tiene asignados” en la página 164](#).

1 Consulte la entrada **CONSOLE** en el archivo `/etc/default/login`.

```
CONSOLE=/dev/console
```

De manera predeterminada, el dispositivo de consola se establece en `/dev/console`. Con este valor, root puede iniciar sesión en la consola. root no puede iniciar sesión de manera remota.

2 Verifique que root no pueda iniciar sesión de manera remota.

Desde un sistema remoto, intente iniciar sesión como root.

```
mach2 % ssh -l root mach1
Password: <Type root password of mach1>
Password:
```

Password:

Permission denied (gssapi-keyex,gssapi-with-mic,publickey,keyboard-interactive).

En la configuración predeterminada, root es un rol, y los roles no pueden iniciar sesión. Además, en la configuración predeterminada el protocolo ssh impide el inicio de sesión por parte del usuario root.

3 Supervise intentos de convertirse en usuario root.

De manera predeterminada, los intentos de convertirse en usuario root se imprimen en la consola mediante la utilidad SYSLOG.

a. Abra una consola del terminal en el escritorio.

b. En otra ventana, utilice el comando su para convertirse en root.

```
% su -
Password:      <Type root password>
#
```

Se imprime un mensaje en la consola del terminal.

```
Sep 7 13:22:57 mach1 su: 'su root' succeeded for jdoe on /dev/pts/6
```

Ejemplo 3–5 Registro de intentos de acceso root

En este ejemplo, los intentos de root no están siendo registrados por SYSLOG. Por lo tanto, el administrador está registrando esos intentos eliminando el comentario de la entrada `#CONSOLE=/dev/console` en el archivo `/etc/default/su`.

```
# CONSOLE determines whether attempts to su to root should be logged
# to the named device
#
CONSOLE=/dev/console
```

Cuando un usuario intenta convertirse en root, el intento se imprime en la consola del terminal.

```
SU 09/07 16:38 + pts/8 jdoe-root
```

Errores más frecuentes

Para convertir root desde un sistema remoto cuando el archivo `/etc/default/login` contiene la entrada `CONSOLE` predeterminada, los usuarios primero deben iniciar sesión con su nombre de usuario. Después de iniciar sesión con su nombre de usuario, los usuarios pueden utilizar el comando `su` para convertirse en root.

Si la consola muestra una entrada similar a `Last login: Wed Sep 7 15:13:11 2011 from mach2`, el sistema se configura para permitir inicios de sesión root remotos. Para evitar el acceso

remoto de root, cambie la entrada `#CONSOLE=/dev/console` a `CONSOLE=/dev/console` en el archivo `/etc/default/login`. Para devolver el protocolo ssh al predeterminado, consulte la página del comando `man sshd_config(4)`.

Control de acceso a hardware del sistema (tareas)

Puede proteger el sistema físico mediante la solicitud de una contraseña para obtener acceso a la configuración del hardware. También puede proteger el sistema impidiendo que un usuario use la secuencia de interrupción para salir del sistema de ventanas.

Para proteger el BIOS, consulte la documentación de ese proveedor.

▼ Cómo requerir una contraseña para el acceso al hardware de SPARC

Antes de empezar

Se debe convertir en administrador con perfiles de derechos asignados de seguridad de dispositivos, mantenimiento y reparación, o administrador del sistema. Para obtener más información, consulte [“Cómo usar los derechos administrativos que tiene asignados” en la página 164](#).

1 En una ventana de terminal, escriba el modo de seguridad de la PROM.

```
# eeprom security-mode=command
```

```
Changing PROM password:
New password:      <Type password>
Retype new password:  <Retype password>
```

Seleccione el valor `command` o `full`. Para obtener más información, consulte la página del comando `man eeprom(1M)`.

Si, cuando escribe el comando anterior, no se le solicita una contraseña para la PROM, el sistema ya tiene una.

2 (Opcional) Para cambiar la contraseña de la PROM, escriba el siguiente comando:

```
# eeprom security-password=      Press Return
Changing PROM password:
New password:      <Type password>
Retype new password:  <Retype password>
```

El modo de seguridad y la contraseña nuevos de la PROM entran en vigor inmediatamente. Sin embargo, es más probable que se puedan observar en el próximo inicio.



Precaución – No olvide la contraseña de la PROM. El hardware no se puede utilizar sin esta contraseña.

▼ Cómo desactivar una secuencia de interrupción del sistema

Nota – Algunos sistemas del servidor tienen un conmutador de claves. Cuando el conmutador de claves se establece en la posición segura, el conmutador sustituye la configuración de interrupción de teclado del software. Por lo tanto, los cambios que realice con el siguiente procedimiento podrían no ser implementados.

Antes de empezar

Debe convertirse en un administrador con la autorización `solaris.admin.edit/etc/default/kbd` asignada. De manera predeterminada, el rol `root` tiene esta autorización. Para obtener más información, consulte [“Cómo usar los derechos administrativos que tiene asignados” en la página 164](#).

1 Cambie el valor de `KEYBOARD_ABORT` a `disable`.

Elimine el comentario de la línea `enable` en el archivo `/etc/default/kbd`. Luego, agregue una línea `disable`:

```
# cat /etc/default/kbd
...
# KEYBOARD_ABORT affects the default behavior of the keyboard abort
# sequence, see kbd(1) for details. The default value is "enable".
# The optional value is "disable". Any other value is ignored.
...
#KEYBOARD_ABORT=enable
KEYBOARD_ABORT=disable
```

2 Actualice los valores predeterminados del teclado.

```
# kbd -i
```

Servicio de análisis de virus (tareas)

En este capítulo, se proporciona información sobre el uso del software antivirus y se tratan los siguientes temas:

- “Acerca del análisis de virus” en la página 67
- “Acerca del servicio Vscan” en la página 68
- “Uso del servicio Vscan (tareas)” en la página 69

Acerca del análisis de virus

Los datos están protegidos contra virus por un servicio de análisis, vscan, que utiliza varios *motores de análisis*. Un [motor de exploración](#) es una aplicación de terceros que reside en un host externo, que examina un archivo para ver si contiene virus conocidos. Un archivo es un candidato para el análisis de virus si el sistema de archivos admite el servicio vscan, el servicio se ha activado y el tipo de archivo no ha quedado exento. El análisis de virus se realiza en un archivo durante operaciones de apertura y cierre si el archivo no se ha analizado previamente con las definiciones de virus actuales o si el archivo se ha modificado desde el último análisis.

El servicio vscan se puede configurar para que utilice varios motores de análisis. Se recomienda que el servicio vscan utilice un mínimo de dos motores de análisis. Las solicitudes para análisis de virus se distribuyen entre todos los motores de análisis disponibles. La [Tabla 4-1](#) muestra los motores de análisis que son compatibles cuando están configurados con sus parches más recientes.

TABLA 4-1 Software de motor de análisis antivirus

Software antivirus	Compatibilidad ICAP
Symantec Antivirus Scan Engine 4.3	Es compatible
Symantec Antivirus Scan Engine 5.1	Es compatible

TABLA 4-1 Software de motor de análisis antivirus (Continuación)

Software antivirus	Compatibilidad ICAP
Computer Associates eTrust AntiVirus 7.1	No es compatible ¹
Computer Associates Integrated Threat Management 8.1	
Trend Micro Interscan Web Security Suite (IWSS) 2.5	Es compatible
McAfee Secure Internet Gateway 4.5	Es compatible

¹ Requiere la instalación de Sun StorageTek 5000 NAS ICAP Server para Computer Associates Antivirus Scan Engine. Obtenga el paquete de [Oracle Software Downloads](http://www.oracle.com/technetwork/indexes/downloads/index.html) (<http://www.oracle.com/technetwork/indexes/downloads/index.html>).

Acerca del servicio Vscan

La ventaja del método de análisis en tiempo real es que un archivo se escanea con las últimas definiciones de virus *antes* de que se utilice. Con este enfoque, los virus pueden ser detectados antes de que pongan en peligro los datos.

A continuación se describe el proceso de análisis de virus:

1. Cuando un usuario abre un archivo del cliente, el servicio vscan determina si el archivo debe ser analizado según si el archivo se ha analizado previamente con las definiciones de virus actuales y si el archivo se ha modificado desde el último análisis.
 - Si el archivo debe ser analizado, el archivo se transfiere al [motor de exploración](#). Si una conexión a un motor de análisis falla, el archivo se envía a otro motor de análisis. Si no hay ningún motor de análisis disponible, el análisis de virus falla y es posible que se deniegue el acceso al archivo.
 - Si el archivo no necesita ser analizado, al cliente se le permite acceder al archivo.
2. El motor de análisis analiza el archivo utilizando las definiciones de virus actuales.
 - Si se detecta un virus, el archivo se marca como en cuarentena. Un archivo en cuarentena no se puede leer, ejecutar ni cambiar de nombre pero se puede suprimir. El registro del sistema registra el nombre del archivo en cuarentena y el nombre del virus y, si la auditoría se ha activado, se crea el registro de auditoría con la misma información.
 - Si el archivo no está infectado, el archivo se etiqueta con un sello de análisis y se le permite al cliente acceder al archivo.

Uso del servicio Vscan (tareas)

El análisis de archivos en busca de virus está disponible cuando se cumplen los siguientes requisitos:

- Al menos un motor de análisis está instalado y configurado.
- Los archivos residen en un sistema de archivos que admite análisis de virus.
- El análisis de virus está activado en un sistema de archivos.
- El servicio vscan está activado.
- El servicio vscan está configurado para analizar archivos del tipo de archivo especificado.

En la siguiente tabla se señalan las tareas que puede realizar para configurar el servicio vscan.

Tarea	Descripción	Para obtener instrucciones
Instalar un motor de exploración .	Instala y configura uno o más productos de terceros enumerados en la Tabla 4–1 .	Consulte la documentación del producto.
Activar el sistema de archivos para permitir el análisis de virus.	Permite el análisis de virus en un sistema de archivos ZFS. De manera predeterminada, los análisis están desactivados.	“Cómo activar el análisis de virus en un sistema de archivos” en la página 69
Activar el servicio vscan.	Inicia el servicio de análisis.	“Cómo activar el servicio Vscan” en la página 70
Agregar un motor de análisis al servicio vscan.	Incluye motores de análisis específicos en el servicio vscan.	“Cómo agregar un motor de análisis” en la página 70
Configurar el servicio vscan.	Visualiza y cambia propiedades de vscan.	“Cómo ver propiedades de Vscan” en la página 70 “Cómo cambiar propiedades de Vscan” en la página 71
Configurar el servicio vscan para tipos de archivo específicos.	Especifica los tipos de archivo que se van a incluir y excluir en un análisis.	“Cómo excluir archivos del análisis de virus” en la página 72

▼ Cómo activar el análisis de virus en un sistema de archivos

Utilice el comando del sistema de archivos para permitir el análisis de virus de archivos. Por ejemplo, para incluir un sistema de archivos ZFS en un análisis de virus, utilice el comando `zfs(1M)`.

El sistema de archivos ZFS permite que algunas tareas administrativas se deleguen a usuarios específicos. Para obtener más información acerca de la administración delegada, consulte el [Capítulo 8, “Administración delegada de ZFS Oracle Solaris” de Administración de Oracle Solaris 11.1: sistemas de archivos ZFS](#).

Antes de empezar Debe convertirse en un administrador con el perfil de derechos de gestión del sistema de archivos ZFS o el perfil de derechos de gestión de almacenamiento ZFS asignado. Para obtener más información, consulte [“Cómo usar los derechos administrativos que tiene asignados” en la página 164](#).

- Active el análisis de virus en un sistema de archivos ZFS, por ejemplo, `pool/volumes/vol1`.

```
# zfs set vscan=on path/pool/volumes/vol1
```

▼ Cómo activar el servicio Vscan

Antes de empezar Debe convertirse en un administrador con el perfil de derechos de gestión VSCAN asignado. Para obtener más información, consulte [“Cómo usar los derechos administrativos que tiene asignados” en la página 164](#).

- Active el servicio de detección de virus.

```
# svcadm enable vscan
```

▼ Cómo agregar un motor de análisis

Antes de empezar Debe convertirse en un administrador con el perfil de derechos de gestión VSCAN asignado. Para obtener más información, consulte [“Cómo usar los derechos administrativos que tiene asignados” en la página 164](#).

- Para agregar un motor de análisis al servicio vscan con propiedades predeterminadas, escriba:

```
# vscanadm add-engine engine_ID
```


Para obtener más información, consulte la página del comando `man vscanadm(1M)`.

▼ Cómo ver propiedades de Vscan

Antes de empezar Debe convertirse en un administrador con el perfil de derechos de gestión VSCAN asignado. Para obtener más información, consulte [“Cómo usar los derechos administrativos que tiene asignados” en la página 164](#).

- Visualice las propiedades del servicio vscan, de todos los motores de análisis o de un motor de análisis específico.
 - Para ver las propiedades de un motor de análisis específico, escriba:


```
# vscanadm get-engine engineID
```
 - Para ver las propiedades de todos los motores de análisis, escriba:


```
# vscanadm get-engine
```
 - Para ver una de las propiedades del servicio vscan, escriba:


```
# vscanadm get -p property
```

Donde *property* es uno de los parámetros descritos en la página del comando man para el comando vscanadm(1M).

Por ejemplo, si desea ver el tamaño máximo de un archivo que se puede analizar, escriba:

```
# vscanadm get max-size
```

▼ Cómo cambiar propiedades de Vscan

Puede cambiar las propiedades de un determinado motor de análisis y las propiedades generales del servicio vscan. Muchos motores de análisis limitan el tamaño de los archivos que analizan, por lo que la propiedad *max-size* del servicio vscan se debe establecer en un valor menor o igual que el tamaño máximo permitido del motor de análisis. Luego se define si los archivos que son más grandes que el tamaño máximo, y que por lo tanto no se analizan, son accesibles.

Antes de empezar

Debe convertirse en un administrador con el perfil de derechos de gestión VSCAN asignado. Para obtener más información, consulte [“Cómo usar los derechos administrativos que tiene asignados” en la página 164](#).

- 1 Visualice las propiedades actuales mediante el comando `vscanadm show`.
- 2 Establezca el tamaño máximo de análisis de virus, por ejemplo, 128 megabytes.


```
# vscanadm set -p max-size=128M
```
- 3 Especifique que se deniega el acceso a cualquier archivo no analizado debido a su tamaño.


```
# vscanadm set -p max-size-action=deny
```

Para obtener más información, consulte la página del comando man `vscanadm(1M)`.

▼ Cómo excluir archivos del análisis de virus

Cuando activa la protección antivirus, puede especificar que todos los archivos de tipos específicos se excluyan del análisis de virus. Debido a que el servicio vscan afecta el rendimiento del sistema, puede conservar los recursos del sistema especificando tipos de archivo específicos para el análisis de virus.

Antes de empezar Debe convertirse en un administrador con el perfil de derechos de gestión VSCAN asignado. Para obtener más información, consulte [“Cómo usar los derechos administrativos que tiene asignados” en la página 164](#).

1 Visualice la lista de todos los tipos de archivos que se incluyen en el análisis de virus.

```
# vscanadm get -p types
```

2 Especifique los tipos de archivo que se van a analizar en busca de virus:

- Excluya un tipo de archivo específico, por ejemplo el tipo JPEG, del análisis de virus.

```
# vscanadm set -p types=-jpg, +*
```

- Incluya un tipo de archivo específico, como archivos ejecutables, en el análisis de virus.

```
# vscanadm set -p types=+exe, -*
```

Para obtener más información, consulte la página del comando `man vscanadm(1M)`.

Control de acceso a dispositivos (tareas)

Este capítulo proporciona instrucciones paso a paso para proteger dispositivos, además de una sección de referencia. En este capítulo, se tratan los siguientes temas:

- “Configuración de política de dispositivos (tareas)” en la página 73
- “Gestión de asignación de dispositivos (tareas)” en la página 75
- “Asignación de dispositivos (tareas)” en la página 81
- “Protección de dispositivos (referencia)” en la página 84

Para obtener información general sobre la protección de dispositivos, consulte “Control de acceso a dispositivos” en la página 41.

Configuración de política de dispositivos (tareas)

La política de dispositivos restringe o impide el acceso a los dispositivos que son una parte integral del sistema. La política se aplica en el núcleo.

Configuración de política de dispositivos (mapa de tareas)

El siguiente mapa de tareas hace referencia a los procedimientos de configuración de dispositivos relativos a la política de dispositivos.

Tarea	Descripción	Para obtener instrucciones
Ver la política de dispositivos para los dispositivos del sistema.	Muestra los dispositivos y su política de dispositivos.	“Cómo ver una política de dispositivos” en la página 74
Auditar cambios en la política de dispositivos.	Registra los cambios en la política de dispositivos en la pista de auditoría.	“Cómo auditar cambios en la política de dispositivos” en la página 74

Tarea	Descripción	Para obtener instrucciones
Acceder a /dev/arp.	Obtiene información MIB-II IP de Oracle Solaris.	“Cómo recuperar información MIB-II IP de un dispositivo /dev/*” en la página 75

▼ Cómo ver una política de dispositivos

- Visualice la política de dispositivos para todos los dispositivos del sistema.

```
% getdevpolicy | more
DEFAULT
read_priv_set=none
write_priv_set=none
ip:*
read_priv_set=net_rawaccess
write_priv_set=net_rawaccess
...
```

Ejemplo 5-1 Visualización de la política de dispositivos para un dispositivo específico

En este ejemplo, se muestra la política de dispositivos para tres dispositivos.

```
% getdevpolicy /dev/allkmem /dev/ipsecesp /dev/bge
/dev/allkmem
read_priv_set=all
write_priv_set=all
/dev/ipsecesp
read_priv_set=sys_net_config
write_priv_set=sys_net_config
/dev/bge
read_priv_set=net_rawaccess
write_priv_set=net_rawaccess
```

▼ Cómo auditar cambios en la política de dispositivos

De manera predeterminada, la clase de auditoría as incluye el evento de auditoría AUE_MODDEVPLCY.

Antes de empezar Debe convertirse en un administrador con el perfil de derechos de configuración de auditoría asignado. Para obtener más información, consulte [“Cómo usar los derechos administrativos que tiene asignados” en la página 164](#).

- Preseleccione la clase de auditoría que incluye el evento de auditoría AUE_MODDEVPLCY.

```
# auditconfig -getflags
current-flags
# auditconfig -setflags current-flags,as
```

Para obtener instrucciones detalladas, consulte [“Cómo preseleccionar clases de auditoría” en la página 580](#).

▼ Cómo recuperar información MIB-II IP de un dispositivo /dev/*

Las aplicaciones que recuperan información MIB-II IP de Oracle Solaris deben abrir /dev/arp, no /dev/ip.

1 Determine la política de dispositivos en /dev/ip y /dev/arp.

```
% getdevpolicy /dev/ip /dev/arp
/dev/ip
read_priv_set=net_rawaccess
write_priv_set=net_rawaccess
/dev/arp
read_priv_set=none
write_priv_set=none
```

Tenga en cuenta que se requiere el privilegio net_rawaccess para la lectura y escritura en /dev/ip. No se requieren privilegios para /dev/arp.

2 Abra /dev/arp y utilice los módulos tcp y udp.

No se requieren privilegios. Este método es equivalente a abrir /dev/ip y utilizar los módulos arp, tcp y udp. Como la apertura de /dev/ip requiere ahora un privilegio, es preferible usar el método /dev/arp.

Gestión de asignación de dispositivos (tareas)

La asignación de dispositivos se suele implementar en sitios que requieren un nivel adicional de seguridad de dispositivos. Generalmente, los usuarios deben tener autorización para acceder a dispositivos asignables.

Gestión de asignación de dispositivos (mapa de tareas)

El siguiente mapa de tareas hace referencia a los procedimientos para activar y configurar la asignación de dispositivos, y para la resolución de problemas de la asignación de dispositivos. La asignación de dispositivos está desactivada de manera predeterminada. Después de que la asignación de dispositivos esté activada, consulte [“Asignación de dispositivos \(tareas\)” en la página 81](#) para obtener instrucciones sobre la asignación de dispositivos.

Tarea	Descripción	Para obtener instrucciones
Permitir que un dispositivo pueda asignarse. Desactivar la asignación de dispositivos.	Permite que un dispositivo se asigne a un usuario a la vez. Elimina las restricciones de asignación de todos los dispositivos.	“Cómo activar la asignación de dispositivos” en la página 76
Autorizar a los usuarios a asignar un dispositivo.	Asigna autorizaciones de asignación de dispositivos a los usuarios.	“Cómo autorizar a usuarios para que asignen un dispositivo” en la página 77
Ver los dispositivos asignables del sistema.	Muestra los dispositivos que se pueden asignar y el estado del dispositivo.	“Cómo ver la información de asignación de un dispositivo” en la página 78
Asignar de manera forzada un dispositivo.	Asigna un dispositivo a un usuario que tiene una necesidad inmediata.	“Cómo asignar de manera forzada un dispositivo” en la página 78
Desasignar de manera forzada un dispositivo.	Desasigna un dispositivo que está asignado actualmente a un usuario.	“Cómo desasignar de manera forzada un dispositivo” en la página 79
Cambiar las propiedades de asignación de un dispositivo.	Cambia los requisitos para asignar un dispositivo.	“Cómo cambiar los dispositivos que se pueden asignar” en la página 79
Auditar asignación de dispositivos.	Registra la asignación de dispositivos en la pista de auditoría.	“Cómo auditar la asignación de dispositivos” en la página 80
Crear una secuencia de comandos device-clean.	Depura datos de un dispositivo físico.	“Redacción de secuencias nuevas de comandos device-clean” en la página 92

▼ Cómo activar la asignación de dispositivos

Antes de empezar Debe convertirse en un administrador con el perfil de derechos de seguridad de dispositivo asignado. Para obtener más información, consulte [“Cómo usar los derechos administrativos que tiene asignados” en la página 164](#).

1 Active el servicio de asignación de dispositivos y verifique que el servicio esté activado.

```
# svcadm enable svc:/system/device/allocate
# svcs -x allocate
svc:/system/device/allocate:default (device allocation)
State: online since September 10, 2011 01:10:11 PM PDT
See: allocate(1)
See: deallocate(1)
See: list_devices(1)
See: device_allocate(1M)
See: mkdevalloc(1M)
See: mkdevmaps(1M)
See: dminfo(1M)
See: device_maps(4)
See: /var/svc/log/system-device-allocate:default.log
Impact: None.
```


- 2 Para desactivar el servicio de asignación de dispositivos, utilice el subcomando `disable`.

```
# svcadm disable device/allocate
```

▼ Cómo autorizar a usuarios para que asignen un dispositivo

Antes de empezar

Debe convertirse en un administrador con el perfil de derechos de seguridad de usuarios asignado. Los perfiles de derechos deben incluir la autorización `solaris.auth.delegate`. Para obtener más información, consulte [“Cómo usar los derechos administrativos que tiene asignados” en la página 164](#).

- 1 Cree un perfil de derechos que incluya la autorización y los comandos adecuados.

Generalmente, debe crear un perfil de derechos que incluya la autorización `solaris.device.allocate`. Siga las instrucciones de [“Cómo crear un perfil de derechos” en la página 175](#). Otorgue al perfil de derechos las propiedades adecuadas, como las siguientes:

- Nombre del perfil de derechos: Device Allocation
- Autorizaciones otorgadas: `solaris.device.allocate`
- Comandos con privilegios: `mount` con privilegio `sys_mount` y `umount` con privilegio `sys_mount`

- 2 (Opcional) Cree un rol para el perfil de derechos.

Siga las instrucciones de [“Cómo crear un rol” en la página 171](#). Utilice las siguientes propiedades del rol como guía:

- Nombre del rol: `devicealloc`
- Nombre completo del rol: Device Allocator
- Descripción del rol: Allocates and mounts allocated devices
- Perfil de derechos: Device Allocation

Este perfil de derechos debe ser el primero de la lista de perfiles incluidos en el rol.

- 3 Asigne el perfil de derechos a usuarios autorizados o roles autorizados.

- 4 Enseñe a los usuarios cómo utilizar la asignación de dispositivos.

Para ver ejemplos de cómo asignar medios extraíbles, consulte [“Cómo asignar un dispositivo” en la página 81](#).

▼ Cómo ver la información de asignación de un dispositivo

Antes de empezar

Ha completado “[Cómo activar la asignación de dispositivos](#)” en la página 76.

Debe convertirse en un administrador con el perfil de derechos de seguridad de dispositivo asignado. Para obtener más información, consulte “[Cómo usar los derechos administrativos que tiene asignados](#)” en la página 164.

● Visualice información sobre los dispositivos asignables en el sistema.

```
# list_devices device-name
```

Donde *device-name* es uno de los siguientes:

- `audio[n]`: micrófono y altavoz.
- `fd[n]`: unidad de disquete.
- `rmdisk[n]`: es un dispositivo de medios extraíbles, como un USB.
- `sr[n]`: unidad de CD-ROM.
- `st[n]`: unidad de cinta.

Errores más frecuentes

Si el comando `list_devices` devuelve un mensaje de error similar al siguiente, es posible que la asignación de dispositivos no esté activada o que usted no cuente con permisos suficientes para recuperar la información.

```
list_devices: No device maps file entry for specified device.
```

Para que el comando se ejecute correctamente, active la asignación de dispositivos y asuma un rol con la autorización `solaris.device.revoke`.

▼ Cómo asignar de manera forzada un dispositivo

La asignación forzada se utiliza cuando alguien ha olvidado desasignar un dispositivo. La asignación forzada también se puede utilizar cuando un usuario tiene una necesidad inmediata de un dispositivo.

Antes de empezar

Debe convertirse en un administrador con la autorización `solaris.device.revoke` asignada. Para obtener más información, consulte “[Cómo usar los derechos administrativos que tiene asignados](#)” en la página 164.

1 Determine si tiene las autorizaciones adecuadas en el rol.

```
$ auths
solaris.device.allocate solaris.device.revoke
```

2 Asigne de manera forzada el dispositivo al usuario que lo necesita.

En este ejemplo, la unidad USB se asigna de manera forzada al usuario jdoe.

```
$ allocate -U jdoe
```

▼ Cómo desasignar de manera forzada un dispositivo

Los dispositivos que un usuario ha asignado no se desasignan automáticamente cuando finaliza el proceso o cuando el usuario cierra la sesión. La desasignación forzada se utiliza cuando un usuario ha olvidado desasignar un dispositivo.

Antes de empezar

Debe convertirse en un administrador con la autorización `solaris.device.revoke` asignada. Para obtener más información, consulte [“Cómo usar los derechos administrativos que tiene asignados” en la página 164](#).

1 Determine si tiene las autorizaciones adecuadas en el rol.

```
$ auths
solaris.device.allocate solaris.device.revoke
```

2 Desasigne el dispositivo de manera forzada.

En este ejemplo, la impresora se desasigna de manera forzada. La impresora ahora está disponible para que otro usuario la asigne.

```
$ deallocate -f /dev/lp/printer-1
```

▼ Cómo cambiar los dispositivos que se pueden asignar

Antes de empezar

La asignación de dispositivos debe estar activada para que este procedimiento se realice correctamente. Para activar la asignación de dispositivos, consulte [“Cómo activar la asignación de dispositivos” en la página 76](#). Debe asumir el rol root.

● Especifique si se requiere autorización o especifique la autorización `solaris.device.allocate`.

Cambie el quinto campo en la entrada del dispositivo del archivo `device_allocate`.

```
audio;audio;reserved;reserved;solaris.device.allocate;/etc/security/lib/audio_clean
fd0;fd;reserved;reserved;solaris.device.allocate;/etc/security/lib/fd_clean
sr0;sr;reserved;reserved;solaris.device.allocate;/etc/security/lib/sr_clean
```

Donde `solaris.device.allocate` indica que un usuario debe tener la autorización `solaris.device.allocate` para utilizar el dispositivo.

Ejemplo 5-2 Permiso para que cualquier usuario asigne un dispositivo

En el ejemplo siguiente, cualquier usuario del sistema puede asignar cualquier dispositivo. El quinto campo en cada entrada de dispositivo del archivo `device_allocate` se cambió al símbolo arroba (@).

```
# pfedit /etc/security/device_allocate
audio;audio;reserved;reserved;@;/etc/security/lib/audio_clean
fd0;fd;reserved;reserved;@;/etc/security/lib/fd_clean
sr0;sr;reserved;reserved;@;/etc/security/lib/sr_clean
...
```

Ejemplo 5-3 Prevención de uso de algunos dispositivos periféricos

En el ejemplo siguiente, el dispositivo de audio no se puede utilizar. El quinto campo en la entrada del dispositivo de audio del archivo `device_allocate` se cambió a un asterisco (*).

```
# pfedit /etc/security/device_allocate
audio;audio;reserved;reserved;*/etc/security/lib/audio_clean
fd0;fd;reserved;reserved;solaris device.allocate;/etc/security/lib/fd_clean
sr0;sr;reserved;reserved;solaris device.allocate;/etc/security/lib/sr_clean
...
```

Ejemplo 5-4 Prevención de uso de todos los dispositivos periféricos

En el ejemplo siguiente, no se puede utilizar ningún dispositivo periférico. El quinto campo en cada entrada de dispositivo del archivo `device_allocate` se cambió a un asterisco (*).

```
# pfedit /etc/security/device_allocate
audio;audio;reserved;reserved;*/etc/security/lib/audio_clean
fd0;fd;reserved;reserved;*/etc/security/lib/fd_clean
sr0;sr;reserved;reserved;*/etc/security/lib/sr_clean
...
```

▼ Cómo auditar la asignación de dispositivos

De manera predeterminada, los comandos de asignación de dispositivos se encuentran en la clase de auditoría `other`.

Antes de empezar Debe convertirse en un administrador con el perfil de derechos de configuración de auditoría asignado. Para obtener más información, consulte [“Cómo usar los derechos administrativos que tiene asignados” en la página 164](#).

- **Preseleccione la clase de auditoría `ot`.**

```
$ auditconfig -getflags
current-flags
$ auditconfig -setflags current-flags,ot
```

Para obtener instrucciones detalladas, consulte [“Cómo preseleccionar clases de auditoría” en la página 580](#).

Asignación de dispositivos (tareas)

La asignación de dispositivos reserva el uso de un dispositivo a un usuario a la vez. Los dispositivos que requieren un punto de montaje deben montarse. Los siguientes procedimientos muestran a los usuarios la manera de asignar dispositivos.

▼ Cómo asignar un dispositivo

Antes de empezar

La asignación de dispositivos debe estar activada, como se describe en [“Cómo activar la asignación de dispositivos” en la página 76](#). Si se requiere autorización, el usuario debe contar con la autorización.

- 1 **Asigne el dispositivo.**
Especifique el nombre del dispositivo.
`% allocate device-name`
- 2 **Verifique que el dispositivo esté asignado.**
Ejecute el comando idéntico.
`% allocate device-name`
`allocate. Device already allocated.`

Ejemplo 5-5 Asignación de un micrófono

En este ejemplo, el usuario `jdoe` asigna un micrófono: `audio0`.

```
% whoami
jdoe
% allocate audio0
```

Ejemplo 5-6 Asignación de una impresora

En este ejemplo, un usuario asigna una impresora. Nadie más puede imprimir en `printer-1` hasta que el usuario la haya desasignado o hasta que la impresora se asigne de manera forzada a otro usuario.

```
% allocate /dev/lp/printer-1
```

Para ver un ejemplo de una desasignación forzada, consulte [“Cómo desasignar de manera forzada un dispositivo” en la página 79](#).

Ejemplo 5-7 Asignación de una unidad USB

En este ejemplo, un usuario asigna una unidad USB, `rmdisk1`.

```
% allocate rmdisk1
```

Errores más frecuentes

Si el comando `allocate` no puede asignar el dispositivo, se muestra un mensaje de error en la ventana de consola. Para obtener una lista de los mensajes de error de asignación, consulte la página del comando `man allocate(1)`.

▼ Cómo montar un dispositivo asignado

Los dispositivos se montan automáticamente si se le otorgan los privilegios adecuados. Siga este procedimiento si el dispositivo no logra montarse.

Antes de empezar

Ha asignado el dispositivo. Se le asignaron los privilegios requeridos para montar el dispositivo, como se describe en “[Cómo autorizar a usuarios para que asignen un dispositivo](#)” en la página 77.

1 Asuma un rol que permita asignar y montar un dispositivo.

```
% su - role-name
Password: <Type role-name password>
$
```

2 Cree y proteja un punto de montaje en el directorio principal del rol.

Únicamente debe realizar este paso la primera vez que necesita un punto de montaje.

```
$ mkdir mount-point ; chmod 700 mount-point
```

3 Enumere los dispositivos asignables.

```
$ list devices -l
List of allocatable devices
```

4 Asigne el dispositivo.

Especifique el nombre del dispositivo.

```
$ allocate device-name
```

5 Monte el dispositivo.

```
$ mount -o ro -F filesystem-type device-path mount-point
```

Donde

-o ro Indica que el dispositivo se montará en el modo de sólo lectura. Utilice
-o rw para que el dispositivo pueda escribirse.

<code>-F filesystem-type</code>	Indica el formato del sistema de archivos del dispositivo. Generalmente, un CD-ROM se formatea con un sistema de archivos HSFS. Un disquete suele formatearse con un sistema de archivos PCFS.
<code>device-path</code>	Indica la ruta del dispositivo. La salida del comando <code>list_devices -l</code> incluye <i>ruta_dispositivo</i> .
<code>mount-point</code>	Indica el punto de montaje creado en el Paso 2 .

Ejemplo 5-8 Asignación de una unidad de CD-ROM

En este ejemplo, un usuario asume un rol que permite asignar y montar una unidad de CD-ROM: `sr0`. La unidad está formateada como un sistema de archivos HSFS.

```
% roles
devicealloc
% su - devicealloc
Password: <Type devicealloc password>
$ mkdir /home/devicealloc/mymnt
$ chmod 700 /home/devicealloc/mymnt
$ list_devices -l
...
device: sr0 type: sr files: /dev/sr0 /dev/rsr0 /dev/dsk/c0t2d0s0 ...
...
$ allocate sr0
$ mount -o ro -F hsfs /dev/sr0 /home/devicealloc/mymnt
$ cd /home/devicealloc/mymnt ; ls
List of the contents of CD-ROM
```

Errores más frecuentes

Si el comando `mount` no puede montar el dispositivo, se muestra un mensaje de error: `mount: insufficient privileges`. Compruebe lo siguiente:

- Verifique que está ejecutando el comando `mount` en un shell de perfil. Si asumió un rol, el rol tiene un shell de perfil. Si es un usuario y se le asignó un perfil con el comando `mount`, debe crear un shell de perfil. Para obtener una lista de shells de perfil disponibles, consulte [pfexec\(1\)](#).
- Verifique que es el propietario del punto de montaje especificado. Debe tener acceso de lectura, escritura y ejecución al punto de montaje.

Póngase en contacto con el administrador si todavía no puede montar el dispositivo asignado. “[Cómo solucionar problemas de asignación de privilegios y RBAC](#)” en la [página 182](#) es un punto de partida.

▼ Cómo desasignar un dispositivo

La desasignación permite que otros usuarios asignen y utilicen el dispositivo cuando usted haya terminado.

Antes de empezar Debe haber asignado el dispositivo.

1 Si el dispositivo está montado, desmóntelo.

```
$ cd $HOME
$ umount mount-point
```

2 Desasigne el dispositivo.

```
$ deallocate device-name
```

Ejemplo 5–9 Desasignación de un micrófono

En este ejemplo, el usuario jdoe desasigna el micrófono: audio.

```
% whoami
jdoe
% deallocate audio0
```

Ejemplo 5–10 Desasignación de una unidad de CD-ROM

En este ejemplo, el rol de asignador de dispositivos desasigna una unidad de CD-ROM. Después de que se imprime el mensaje, se expulsa el CD-ROM.

```
$ whoami
devicealloc
$ cd /home/devicealloc
$ umount /home/devicealloc/mymnt
$ ls /home/devicealloc/mymnt
$
$ deallocate sr0
/dev/sr0:      326o
/dev/rsr0:     326o
...
sr_clean: Media in sr0 is ready. Please, label and store safely.
```

Protección de dispositivos (referencia)

Los dispositivos en Oracle Solaris están protegidos por una política de dispositivos en núcleo. Los dispositivos periféricos se pueden proteger mediante la asignación de dispositivos. La asignación de dispositivos se activa de manera opcional y se aplica en el nivel de usuario.

Comandos de la política de dispositivos

Los comandos de gestión de dispositivos administran la política de dispositivos en archivos locales. La política de dispositivos puede incluir requisitos de privilegios. Los usuarios asignados a los perfiles de derechos de seguridad de dispositivos y de gestión de dispositivos pueden gestionar dispositivos.

En la siguiente tabla, se muestran los comandos de gestión de dispositivos.

TABLA 5-1 Comandos de gestión de dispositivos

Página del comando man	Finalidad
devfsadm(1M)	Administra los dispositivos y los controladores de dispositivos en un sistema en ejecución. También carga la política de dispositivos. El comando <code>devfsadm</code> permite la limpieza de enlaces <code>/dev</code> sin referencia a dispositivos de disco, cinta, puerto, audio y pseudodispositivos. Los dispositivos para un controlador con nombre también se pueden volver a configurar.
getdevpolicy(1M)	Muestra la política asociada con uno o varios dispositivos. Cualquier usuario puede ejecutar este comando.
add_drv(1M)	Agrega un nuevo controlador de dispositivos a un sistema en ejecución. Contiene opciones para agregar la política de dispositivos al nuevo dispositivo. Generalmente, este comando se invoca en una secuencia de comandos cuando se está instalando un controlador de dispositivos.
update_drv(1M)	Actualiza los atributos de un controlador de dispositivos existente. Contiene opciones para actualizar la política de dispositivos para el dispositivo. Generalmente, este comando se invoca en una secuencia de comandos cuando se está instalando un controlador de dispositivos.
rem_drv(1M)	Elimina un dispositivo o un controlador de dispositivos.

Asignación de dispositivos

La asignación de dispositivos puede proteger su sitio contra pérdida de datos, virus informáticos y otras infracciones de seguridad. A diferencia de la política de dispositivos, la asignación de dispositivos es opcional. La asignación de dispositivos utiliza autorizaciones para limitar el acceso a los dispositivos asignables.

Componentes de la asignación de dispositivos

Los componentes del mecanismo de asignación de dispositivos son los siguientes:

- El servicio `svc:/system/device/allocate`. Para obtener más información, consulte la página del comando `man smf(5)` y las páginas del comando `man` para los comandos de asignación de dispositivos.
- Los comandos `allocate`, `deallocate`, `dminfo` y `list_devices`. Para obtener más información, consulte [“Comandos de asignación de dispositivos” en la página 87](#).
- Los perfiles de derechos de seguridad de dispositivos y de gestión de dispositivos. Para obtener más información, consulte [“Perfiles de derechos de asignación de dispositivos” en la página 86](#).
- Secuencias de comandos `device-clean` para cada dispositivo asignable.

Estos comandos y las secuencias de comandos utilizan los siguientes archivos locales para implementar la asignación de dispositivos:

- El archivo `/etc/security/device_allocate`. Para obtener más información, consulte la página del comando `man device_allocate(4)`.
- El archivo `/etc/security/device_maps`. Para obtener más información, consulte la página del comando `man device_maps(4)`.
- Un archivo de bloqueo, en el directorio `/etc/security/dev`, para cada dispositivo asignable.
- Los atributos modificados de los archivos de bloqueo que están asociados con cada dispositivo asignable.

Nota – Es posible que versiones futuras de Oracle Solaris no admitan el directorio `/etc/security/dev`.

Servicio de asignación de dispositivos

El servicio `svc:/system/device/allocate` controla la asignación de dispositivos. Este servicio se encuentra desactivado de manera predeterminada.

Perfiles de derechos de asignación de dispositivos

Los perfiles de derechos de seguridad de dispositivos y de gestión de dispositivos son necesarios para la gestión de dispositivos y la asignación de dispositivos.

Estos perfiles de derechos incluyen las siguientes autorizaciones:

- `solaris.device.allocate`: necesaria para asignar un dispositivo
- `solaris.device.cdrw`: necesaria para leer y escribir un CD-ROM
- `solaris.device.config`: necesaria para configurar los atributos de un dispositivo

- `solaris.device.mount.alloptions.fixed`: necesaria para especificar opciones de montaje cuando se monta un dispositivo fijo
- `solaris.device.mount.alloptions.removable`: necesaria para especificar opciones de montaje cuando se monta un dispositivo extraíble
- `solaris.device.mount.fixed`: necesaria para montar un dispositivo fijo
- `solaris.device.mount.removable`: necesaria para montar un dispositivo extraíble
- `solaris.device.revoke`: necesaria para revocar o recuperar un dispositivo

Comandos de asignación de dispositivos

Con opciones de mayúsculas, los comandos `allocate`, `deallocate` y `list_devices` son comandos administrativos. De lo contrario, estos comandos son comandos de usuario. En la siguiente tabla, se muestran los comandos de asignación de dispositivos.

TABLA 5-2 Comandos de asignación de dispositivos

Página del comando man	Finalidad
dminfo(1M)	Busca un dispositivo asignable por tipo de dispositivo, nombre del dispositivo y nombre de ruta completa.
list_devices(1)	Muestra el estado de los dispositivos asignables. Muestra todos los archivos especiales del dispositivo que están asociados con los dispositivos enumerados en el archivo <code>device_maps</code> . Con la opción <code>-U</code> , se muestran los dispositivos que se pueden asignar o que están asignados al ID de usuario especificado. Esta opción permite comprobar cuáles dispositivos son asignables y cuáles están asignados a otro usuario. Debe tener la autorización <code>solaris.device.revoke</code> .
allocate(1)	Reserva un dispositivo asignable para que lo utilice un usuario. De manera predeterminada, un usuario debe tener la autorización <code>solaris.device.allocate</code> para poder asignar un dispositivo. Puede modificar el archivo <code>device_allocate</code> para que no requiera autorización del usuario. De esa manera, cualquier usuario del sistema puede solicitar la asignación del dispositivo para su uso.
deallocate(1)	Elimina la reserva de asignación de un dispositivo.

Autorizaciones para los comandos de asignación

De manera predeterminada, los usuarios deben tener la autorización `solaris.device.allocate` para reservar un dispositivo asignable. Para crear un perfil de derechos a fin de incluir la autorización `solaris.device.allocate`, consulte [“Cómo autorizar a usuarios para que asignen un dispositivo” en la página 77](#).

Los administradores deben tener la autorización `solaris.device.revoke` para cambiar el estado de asignación de cualquier dispositivo. Por ejemplo, la opción `-U` para los comandos `allocate` y `list_devices`, y la opción `-F` para el comando `deallocate` requieren la autorización `solaris.device.revoke`.

Para obtener más información, consulte [“Comandos seleccionados que requieren autorizaciones” en la página 214](#).

Estado de error de asignación

Un dispositivo está en un *estado de error de asignación* cuando el comando `deallocate` no puede realizar la desasignación o cuando el comando `allocate` no puede realizar la asignación. Cuando un dispositivo asignable se encuentra en un estado de error de asignación, se debe desasignar de manera forzada. Sólo un usuario o un rol con el perfil de derechos de gestión de dispositivos o de seguridad de dispositivos puede manejar un estado de error de asignación.

El comando `deallocate` con la opción `-F` fuerza la desasignación. O bien, puede usar `allocate -U` para asignar el dispositivo a un usuario. Una vez que el dispositivo está asignado, puede investigar los mensajes de error que aparecen. Después de corregir los problemas con el dispositivo, puede desasignarlo de manera forzada.

Archivo `device_maps`

Los mapas de dispositivos se crean al configurar la asignación de dispositivos. El archivo `/etc/security/device_maps` incluye los nombres de los dispositivos, los tipos de dispositivos y los archivos especiales de los dispositivos que están asociados con cada dispositivo asignable.

El archivo `device_maps` define las asignaciones de archivos especiales para cada dispositivo, que en muchos casos no son intuitivas. Este archivo permite que los programas descubran qué archivos especiales de dispositivos se deben asignar a determinados dispositivos. Puede utilizar el comando `dminfo`, por ejemplo, para recuperar el nombre del dispositivo, el tipo de dispositivo y los archivos especiales del dispositivo que se deben especificar al configurar un dispositivo asignable. El comando `dminfo` utiliza el archivo `device_maps` para comunicar esta información.

Cada dispositivo se representa con una entrada de una línea con el formato:

device-name:device-type:device-list

EJEMPLO 5-11 Ejemplo de entrada `device_maps`

El siguiente es un ejemplo de una entrada en un archivo `device_maps` para una unidad de disquete, `fd0`:

```
fd0:\
fd:\
/dev/diskette /dev/rdiskette /dev/fd0a /dev/rfd0a \
```

EJEMPLO 5-11 Ejemplo de entrada `device_maps` (Continuación)

```
/dev/fd0b /dev/rfd0b /dev/fd0c /dev/fd0 /dev/rfd0c /dev/rfd0:\
```

Las líneas en el archivo `device_maps` pueden finalizar con una barra diagonal inversa (\) para continuar una entrada en la línea siguiente. También se pueden incluir comentarios. Un signo de almohadilla (#) indica que hay comentarios en todo el texto subsiguiente hasta la siguiente línea nueva que no está inmediatamente precedida por una barra diagonal inversa. En todos los campos, se permiten espacios iniciales y finales. Los campos se definen del modo siguiente:

- device-name* Especifica el nombre del dispositivo. Para obtener una lista de los nombres actuales de dispositivos, consulte [“Cómo ver la información de asignación de un dispositivo” en la página 78](#).
- device-type* Especifica el tipo de dispositivo genérico. El nombre genérico es el nombre para la clase de dispositivos, como `st`, `fd`, `rm disk` o `audio`. El campo *device-type* agrupa lógicamente dispositivos relacionados.
- device-list* Muestra los archivos especiales del dispositivo que están asociados con el dispositivo físico. *device-list* debe contener todos los archivos especiales que permiten el acceso a un dispositivo determinado. Si la lista está incompleta, un usuario malintencionado podrá obtener o modificar información privada. Las entradas válidas para el campo *device-list* reflejan los archivos del dispositivo que están ubicados en el directorio `/dev`.

Archivo `device_allocate`

Puede modificar el archivo `/etc/security/device_allocate` para cambiar dispositivos de asignables a no asignables, o para agregar nuevos dispositivos. A continuación, se presenta un ejemplo del archivo `device_allocate`.

```
st0;st;;;/etc/security/lib/st_clean
fd0;fd;;;/etc/security/lib/fd_clean
sr0;sr;;;/etc/security/lib/sr_clean
audio;audio;;;*/etc/security/lib/audio_clean
```

Una entrada en el archivo `device_allocate` no significa que el dispositivo es asignable, a menos que la entrada indique específicamente que el dispositivo es asignable. En el archivo `device_allocate` de ejemplo, observe el asterisco (*) en el quinto campo de la entrada del dispositivo de audio. Un asterisco en el quinto campo indica al sistema que el dispositivo no es asignable. Por lo tanto, el dispositivo no se puede utilizar. Si hay otros valores o si no hay ningún valor en este campo, el dispositivo se puede utilizar.

En el archivo `device_allocate`, cada dispositivo se representa con una entrada de una línea con el formato:

```
device-name;device-type;reserved;reserved;auths;device-exec
```

Las líneas en el archivo `device_allocate` pueden finalizar con una barra diagonal inversa (`\`) para continuar una entrada en la línea siguiente. También se pueden incluir comentarios. Un signo de almohadilla (`#`) indica que hay comentarios en todo el texto subsiguiente hasta la siguiente línea nueva que no está inmediatamente precedida por una barra diagonal inversa. En todos los campos, se permiten espacios iniciales y finales. Los campos se definen del modo siguiente:

<i>device-name</i>	Especifica el nombre del dispositivo. Para obtener una lista de los nombres actuales de dispositivos, consulte “Cómo ver la información de asignación de un dispositivo” en la página 78 .
<i>device-type</i>	Especifica el tipo de dispositivo genérico. El nombre genérico es el nombre para la clase de dispositivos, como <code>st</code> , <code>fd</code> y <code>sr</code> . El campo <i>device-type</i> agrupa lógicamente dispositivos relacionados. Cuando permita que un dispositivo pueda asignarse, recupere el nombre del dispositivo del campo <i>device-type</i> en el archivo <code>device_maps</code> .
<i>reserved</i>	Oracle reserva para uso futuro los dos campos marcados como <code>reserved</code> .
<i>auths</i>	Especifica si el dispositivo es asignable. Un asterisco (*) en este campo indica que el dispositivo no es asignable. Una cadena de autorización, o un campo vacío, indica que el dispositivo es asignable. Por ejemplo, la cadena <code>solaris.device.allocate</code> en el campo <i>auths</i> indica que se necesita la autorización <code>solaris.device.allocate</code> para poder asignar el dispositivo. Un símbolo arroba (@) en este archivo indica que cualquier usuario puede asignar el dispositivo.
<i>device-exec</i>	Proporciona el nombre de ruta de una secuencia de comandos que se debe invocar para tratamiento especial, como limpieza y protección contra la reutilización del objeto durante el proceso de asignación. La secuencia de comandos <i>device-exec</i> se ejecuta cuando el comando <code>deallocate</code> se ejecuta en el dispositivo.

Por ejemplo, la entrada siguiente para el dispositivo `sr0` indica que un usuario que cuente con la autorización `solaris.device.allocate` puede asignar la unidad de CD-ROM:

```
sr0;sr;reserved;reserved;solaris.device.allocate;/etc/security/lib/sr_clean
```

Puede decidir aceptar los servicios predeterminados y sus características definidas. Después de instalar un dispositivo nuevo, puede modificar las entradas. Los dispositivos que requieren asignación antes de su uso deben definirse en los archivos `device_allocate` y `device_maps` del sistema de ese dispositivo. En la actualidad, las unidades de cinta de cartucho, las unidades de disquete, las unidades de CD-ROM, los dispositivos de medios extraíbles y los chips de audio se consideran asignables. Estos tipos de dispositivos tienen secuencias de comandos `device-clean`.

Nota – Las unidades de cinta Xylogics o Archive también utilizan la secuencia de comandos `st_clean` proporcionada para los dispositivos SCSI. Debe crear sus propias secuencias de comandos `device-clean` para otros dispositivos, como terminales, tabletas gráficas y otros dispositivos asignables. La secuencia de comandos debe cumplir con los requisitos de reutilización de objetos para ese tipo de dispositivo.

Secuencias de comandos `device-clean`

La asignación de dispositivos cumple parte de lo que se conoce como requisito de *reutilización de objetos*. Las secuencias de comandos `device-clean` abordan el requisito de seguridad que establece que todos los datos utilizables deben depurarse de un dispositivo físico antes de volver a utilizarlo. Los datos se limpian antes de que otro usuario asigne el dispositivo. De manera predeterminada, las unidades de cinta de cartucho, las unidades de disquete, las unidades de CD-ROM y los dispositivos de audio requieren secuencias de comandos `device-clean`. Oracle Solaris proporciona las secuencias de comandos. Esta sección describe qué acciones realizan las secuencias de comandos `device-clean`.

Secuencia de comandos `device-clean` para cintas

La secuencia de comandos `st_clean` admite tres dispositivos de cinta:

- Cinta SCSI de ¼ de pulgada
- Cinta Archive de ¼ de pulgada
- Cinta de carrete abierto de ½ pulgada

La secuencia de comandos `st_clean` usa la opción `rewoffl` para el comando `mt` para limpiar el dispositivo. Para obtener más información, consulte la página del comando `man mt(1)`. Si la secuencia de comandos se ejecuta durante el inicio del sistema, la secuencia consulta al dispositivo para determinar si está en línea. Si el dispositivo está en línea, la secuencia de comandos determina si el dispositivo tiene medios. Los dispositivos de cinta de ¼ de pulgada que tienen medios se colocan en el estado de error de asignación. El estado de error de asignación fuerza al administrador a limpiar manualmente el dispositivo.

Durante el funcionamiento normal del sistema, cuando el comando `deallocate` se ejecuta en modo interactivo, se le indica al usuario que extraiga los medios. La desasignación se retrasa hasta que los medios se hayan extraído del dispositivo.

Secuencias de comandos device-clean para disquetes y unidades de CD-ROM

Las siguientes secuencias de comandos device-clean se proporcionan para disquetes y unidades de CD-ROM:

- **Secuencia de comandos fd_clean:** secuencia de comandos device-clean para disquetes.
- **Secuencia de comandos sr_clean:** secuencia de comandos device-clean para unidades de CD-ROM.

Las secuencias de comandos utilizan el comando `eject` para extraer los medios de la unidad. Si el comando `eject` falla, el dispositivo se coloca en el estado de error de asignación. Para obtener más información, consulte la página del comando `man eject(1)`.

Secuencia de comandos device-clean para audio

Los dispositivos de audio se limpian con una secuencia de comandos `audio_clean`. La secuencia de comandos realiza una llamada del sistema `ioctl AUDIO_GETINFO` para leer el dispositivo. A continuación, la secuencia de comandos realiza una llamada del sistema `ioctl AUDIO_SETINFO` para restablecer la configuración del dispositivo a los valores predeterminados.

Redacción de secuencias nuevas de comandos device-clean

Si agrega más dispositivos asignables al sistema, posiblemente deba crear sus propias secuencias de comandos device-clean. El comando `deallocate` pasa un parámetro a las secuencias de comandos device-clean. El parámetro, que se muestra aquí, es una cadena que contiene el nombre del dispositivo. Para obtener más información, consulte la página del comando `man device_allocate(4)`.

```
clean-script -[I|i|f|S] device-name
```

Si las secuencias de comandos device-clean devuelven “0”, son correctas; si devuelven valores mayores que “0”, fallaron. Las opciones `-I`, `-f` y `-S` determinan el modo de ejecución de la secuencia de comandos:

- I Se necesita durante el inicio del sistema únicamente. Todas las salidas deben ir a la consola del sistema. Si no se pueden expulsar de manera forzada los medios o si la expulsión falla, el dispositivo debe pasar al estado de error de asignación.
- i Similar a la opción `-I`, excepto que se suprime la salida.
- f Se utiliza para la limpieza forzada. La opción es interactiva y asume que el usuario está disponible para responder a las peticiones de datos. Una secuencia de comandos con esta opción debe intentar completar la limpieza si se produce un error en una parte de ésta.
- S Se utiliza para la limpieza estándar. La opción es interactiva y asume que el usuario está disponible para responder a las peticiones de datos.

Verificación de la integridad de archivos mediante el uso de BART (tareas)

En este capítulo, se describe la herramienta de comprobación de la integridad de archivos BART. BART es una herramienta de línea de comandos que le permite comprobar la integridad de los archivos de un sistema a lo largo del tiempo. En este capítulo, se tratan los siguientes temas:

- “BART (descripción general)” en la página 93
- “Uso de BART (tareas)” en la página 96
- “Manifiestos, archivos de reglas e informes de BART (referencia)” en la página 106

BART (descripción general)

BART es una herramienta de análisis de la integridad de los archivos y generación de informes que utiliza sumas de comprobación con potencia de cifrado y metadatos de sistema de archivos para determinar cambios. BART puede ayudarlo a detectar infracciones de seguridad o solucionar problemas de rendimiento en un sistema mediante la identificación de archivos dañados o inusuales. Mediante el uso de BART, puede reducir los costos de la administración de una red de sistemas de manera fácil y fiable, e informar las discrepancias en los archivos que se instalan en sistemas implementados.

BART le permite determinar los cambios que se produjeron en el nivel de archivo de un sistema, en relación con un punto de partida conocido. Puede utilizar BART para crear un manifiesto de *control* o punto de partida a partir de un sistema instalado y configurado totalmente. De esta manera, puede comparar este punto de partida con una instantánea del sistema en un momento posterior y generar un informe que enumera los cambios en el nivel de archivo que se produjeron en el sistema desde su instalación.

Funciones de BART

BART utiliza una sintaxis sencilla que es potente y flexible. La herramienta le permite realizar un seguimiento de los cambios en un sistema determinado a lo largo del tiempo. También

puede realizar un seguimiento de las diferencias de archivos entre sistemas similares. Dichas comparaciones lo pueden ayudar a ubicar archivos dañados o inusuales, o sistemas cuyo software esté desactualizado.

Entre los usos y los beneficios adicionales de BART, se incluyen los siguientes:

- Puede especificar los archivos que se van a supervisar. Por ejemplo, puede controlar las personalizaciones locales, que lo ayudarán a volver a configurar software de una forma sencilla y eficiente.
- Puede solucionar los problemas de rendimiento del sistema.

Componentes de BART

BART crea dos archivos principales, un *manifiesto* y un archivo de comparación, o *report*. Un *archivo de reglas* opcional le permite personalizar el manifiesto y el informe.

Manifiesto de BART

Un *manifiesto* es una instantánea de nivel de archivo de un sistema en un momento determinado. El manifiesto contiene información sobre los atributos de los archivos, que puede incluir información de identificación exclusiva, como una suma de comprobación. Las opciones del comando `bart create` pueden tener como objetivo directorios y archivos específicos. Cada archivo de reglas puede proporcionar un filtrado más detallado, como se describe en [“Archivo de reglas de BART” en la página 95](#).

Nota – De manera predeterminada, BART cataloga todos los sistemas de archivos ZFS en el directorio raíz (/). Otros tipos de sistemas de archivos, por ejemplo, los sistemas de archivos NFS o TMPFS, los CD-ROM montados se catalogan.

Puede crear un manifiesto de un sistema inmediatamente después de la instalación inicial de Oracle Solaris También puede crear un manifiesto después de configurar un sistema para cumplir con las políticas de seguridad de su sitio. Este tipo de manifiesto de control le proporciona una referencia para comparaciones posteriores.

Un manifiesto de línea base se puede utilizar para realizar un seguimiento de la integridad de los archivos en el mismo sistema a lo largo del tiempo. También se puede utilizar como base para la comparación con otros sistemas. Por ejemplo, se puede tomar una instantánea de otros sistemas en su red y, a continuación, comparar los manifiestos con el manifiesto de línea base. Las discrepancias de archivos informadas indican lo que se debe hacer para sincronizar los demás sistemas con el sistema de línea de base.

Para ver el formato de un manifiesto, consulte [“Formato de archivo de manifiesto de BART” en la página 106](#). Para crear un manifiesto, use el comando `bart create`, como se describe en [“Cómo crear un manifiesto de control” en la página 96](#).

Informe de BART

Un informe de BART muestra discrepancias por archivos entre dos manifiestos. Una *discrepancia* es un cambio en cualquier atributo para un archivo determinado que se cataloga para ambos manifiestos. Las agregaciones o supresiones de entradas de archivo también se consideran discrepancias.

Para una comparación útil, los dos manifiestos deben tener como destino los mismos sistemas de archivos. También debe crear y comparar los manifiestos con las mismas opciones y archivo de reglas.

Para ver el formato de un informe, consulte [“Creación de informes de BART” en la página 108](#). Para crear un informe, utilice el comando `bart compare`, tal y como se describe en [“Cómo comparar manifiestos para el mismo sistema a lo largo del tiempo” en la página 100](#).

Archivo de reglas de BART

Un archivo de reglas BART es un archivo que crea para filtrar o dirigir archivos particulares y atributos de archivos que deben incluirse o excluirse. Ahora utiliza este archivo al crear manifiestos e informes de BART. Cuando se comparan manifiestos, el archivo de reglas ayuda a marcar las discrepancias entre los manifiestos.

Nota – Al crear un manifiesto mediante un archivo de reglas, debe usar el mismo archivo de reglas para crear el manifiesto de comparación. Debe utilizar también el archivo de reglas al comparar los manifiestos. Por otra parte, el informe incluiría varias discrepancias no válidas.

El uso de un archivo de reglas para supervisar atributos de archivos y archivos específicos de un sistema requiere planificación. Antes de crear un archivo de reglas, decida qué archivos y atributos de archivos del sistema desea supervisar.

Debido a un error del usuario, un archivo de reglas también puede contener errores de sintaxis y otra información ambigua. Si un archivo de reglas tiene errores, estos errores también se registran.

Para el formato de un archivo de reglas, consulte la página del comando `man` [“Formato de archivo de reglas de BART” en la página 107](#) and the `bart_rules(4)`. Para crear un archivo de reglas, consulte [“Cómo personalizar un informe de BART mediante un archivo de reglas” en la página 104](#).

Uso de BART (tareas)

El comando `bart` se usa para crear y comparar manifiestos. Cualquier usuario puede ejecutar este comando. Sin embargo, los usuarios sólo pueden catalogar y controlar archivos que tiene permiso de acceso. De esta forma, los usuarios y la mayoría de los roles pueden catalogar útilmente los archivos en su directorio raíz, pero la cuenta `root` puede catalogar todos los archivos, incluidos los archivos del sistema.

Consideraciones de seguridad de BART

Cualquiera puede leer los informes y manifiestos de BART. Si la salida de BART puede contener información confidencial, tome las medidas adecuadas para protegerla. Por ejemplo, se pueden utilizar las opciones que generan archivos de salida con permisos restrictivos o colocar los archivos de salida en un directorio protegido.

Uso de BART (mapa de tareas)

Tarea	Descripción	Para obtener instrucciones
Crear un manifiesto de BART	Genera una lista de información sobre cada archivo instalado en un sistema.	“Cómo crear un manifiesto de control” en la página 96
Crear un manifiesto de BART personalizado	Genera una lista de información sobre archivos específicos instalados en un sistema.	“Cómo personalizar un manifiesto” en la página 99
Comparar manifiestos de BART	Genera un informe que compara los cambios en un sistema a lo largo del tiempo. O bien, genera un informe que compara uno o varios sistemas con un sistema de control.	“Cómo comparar manifiestos para el mismo sistema a lo largo del tiempo” en la página 100 “Cómo comparar manifiestos de diferentes sistemas” en la página 102
(Opcional) Personalizar un informe de BART	Genera un informe de BART personalizado de una de las siguientes formas: ■ Especificando atributos ■ Mediante un archivo de reglas	“Cómo personalizar un informe de BART especificando atributos de archivos” en la página 104 “Cómo personalizar un informe de BART mediante un archivo de reglas” en la página 104

▼ Cómo crear un manifiesto de control

En este procedimiento, se explica cómo crear un manifiesto de línea de base para su sistema. Utilice este tipo de manifiesto al instalar muchos sistemas desde una imagen central. O bien,

utilice este tipo de manifiesto para realizar comparaciones cuando desee comprobar que las instalaciones sean idénticas. Para obtener más información sobre los manifiestos de línea de base, consulte “[Manifiesto de BART](#)” en la [página 94](#). Para comprender las convenciones de formato, consulte el [Ejemplo 6–1](#).

Nota – No intente catalogar sistemas de archivos conectados en red. Al usar BART para supervisar los sistemas de archivos conectados a la red, se consume una gran cantidad de recursos para generar manifiestos de poco valor.

Antes de empezar

Para crear un manifiesto de control de su sistema, debe asumir el rol root .

1 Después de personalizar el sistema Oracle Solaris según los requisitos de seguridad de su sitio, cree un manifiesto de control y redirija la salida a un archivo.

```
# bart create options > control-manifest
```

- R Especifica el directorio raíz para el manifiesto. Todas las rutas especificadas por las reglas se interpretan en relación con este directorio. Todas las rutas informadas en el manifiesto están relacionadas con este directorio.
- I Acepta una lista de archivos individuales para catalogarlos, ya sea en la línea de comandos o leídos de la entrada estándar.
- r Nombre del archivo de reglas para este manifiesto. Un argumento - lee el archivo de reglas desde la entrada estándar.
- n Desactiva firmas de contenido para todos los archivos regulares en la lista de archivos. Esta opción se puede utilizar mejorar el rendimiento. De manera alternativa, puede utilizar esta opción si se espera que cambie el contenido de la lista de archivos, como en el caso de los archivos de registro del sistema.

2 Examine el contenido del manifiesto.

Para obtener una explicación del formato, consulte el [Ejemplo 6–1](#).

3 (Opcional) Proteja el manifiesto.

Una forma de proteger los manifiestos del sistema es colocarlos en un directorio al que sólo puede tener acceso la cuenta root.

```
# mkdir /var/adm/log/bartlogs
# chmod 700 /var/adm/log/bartlogs
# mv control-manifest /var/adm/log/bartlogs
```

Elija un nombre significativo para el manifiesto. Por ejemplo, utilice el nombre del sistema y la fecha en que se creó el manifiesto, como en mach1-120312.

Ejemplo 6-1 Explicación del formato de manifiesto BART

En este ejemplo, una explicación del formato del manifiesto sigue la salida de ejemplo.

```
# bart create
! Version 1.1
! HASH SHA256
! Friday, September 07, 2012 (22:22:27)
# Format:
#fname D size mode acl dirmtime uid gid
#fname P size mode acl mtime uid gid
#fname S size mode acl mtime uid gid
#fname F size mode acl mtime uid gid contents
#fname L size mode acl lnmtime uid gid dest
#fname B size mode acl mtime uid gid devnode
#fname C size mode acl mtime uid gid devnode
/ D 1024 40755 user::rwx,group::r-x,mask:r-x,other:r-x
3ebc418eb5be3729ffe7e54053be2d33ee884205502c81ae9689cd8cca5b0090 0 0
.
.
.
/zone D 512 40755 user::rwx group::r-x,mask:r-x,other:r-x 3f81e892
154de3e7bdfd0d57a074c9fae0896a9e2e04bebf5e872d273b063319e57f334 0 0
.
.
.
```

Cada manifiesto consta de un encabezado y entradas de archivos. Cada entrada de archivo consiste en una sola línea, según el tipo de archivo. Por ejemplo, para cada entrada de archivo en la salida anterior, el tipo F especifica un archivo y el tipo D especifica un directorio. También se muestra información sobre el tamaño, el contenido, el ID de usuario, el ID de grupo y los permisos. Las entradas de archivos en la salida se ordenan por versiones codificadas de los nombres de archivos, a fin de manejar correctamente los caracteres especiales. Todas las entradas se ordenan de manera ascendente por nombre de archivo. En todos los nombres de archivos no estándar, como los que contienen caracteres de tabulación o de línea nueva incrustados, escriba los caracteres no estándar entre comillas antes de ordenar las entradas.

Las líneas que empiezan por ! proporcionan metadatos sobre el manifiesto. La línea de versión del manifiesto indica la versión de especificación del manifiesto. La línea hash indica el mecanismo hash que se utilizó. Para obtener más información sobre el hash SHA256 usado como una suma de comprobación, consulte la página del comando [man sha2\(3EXT\)](#).

La línea de fecha muestra la fecha en la que se creó el manifiesto, en formato de fecha. Consulte la página del comando [man date\(1\)](#). La herramienta de comparación de manifiestos ignora algunas líneas. Las líneas ignoradas incluyen metadatos, líneas en blanco, líneas que contienen sólo espacios en blanco y comentarios que empiezan por #.

▼ Cómo personalizar un manifiesto

Puede personalizar un manifiesto de una de las siguientes formas:

- Especificando un subárbol
Especificar un subárbol individual es una forma eficaz de controlar cambios en archivos importantes seleccionados, como todos los archivos en el directorio /etc.
- Especificando un nombre de archivo
Especificar un nombre de archivo es una forma eficaz de controlar especialmente archivos confidenciales, como los archivos que configuran y ejecutan una aplicación de base de datos.
- Mediante un archivo de reglas
Al usar un archivo de reglas para crear y comparar manifiestos, obtiene flexibilidad para especificar varios atributos para más de un archivo o subárbol. Desde la línea de comandos, puede especificar una definición de atributo global que se aplica a todos los archivos de un manifiesto o informe. Desde un archivo de reglas, puede especificar los atributos que no se aplican de forma global.

Antes de empezar

Debe asumir el rol root. Para obtener más información, consulte [“Cómo usar los derechos administrativos que tiene asignados” en la página 164](#).

- 1 **Determine los archivos que desea catalogar y supervisar.**
- 2 **Cree un manifiesto personalizado mediante una de las siguientes opciones:**
 - Especificando un subárbol:

```
# bart create -R subtree
```
 - Especificando un nombre de archivo o nombres de archivos:

```
# bart create -I filename...
```


Por ejemplo:

```
# bart create -I /etc/system /etc/passwd /etc/shadow
```
 - Mediante un archivo de reglas:

```
# bart create -r rules-file
```
- 3 **Examine el contenido del manifiesto.**
- 4 **(Opcional) Guarde el manifiesto en un directorio protegido para su uso futuro.**
Para ver un ejemplo, consulte el [Paso 3](#) in [“Cómo crear un manifiesto de control” en la página 96](#).

Consejo – Si ha utilizado un archivo de reglas, guarde el archivo de reglas con el manifiesto. Para obtener una comparación útil, debe ejecutar la comparación con el archivo de reglas.

▼ Cómo comparar manifiestos para el mismo sistema a lo largo del tiempo

Mediante la comparación de los manifiestos durante el transcurso del tiempo, puede ubicar archivos dañados o inusuales, detectar infracciones de seguridad y solucionar problemas de rendimiento en un sistema.

Antes de empezar

Para crear y comparar manifiestos que incluyen archivos de sistema, debe asumir el rol root.

1 Cree un manifiesto de control de los archivos que se van a supervisar en el sistema.

```
# bart create -R /etc > control-manifest
```

2 (Opcional) Guarde el manifiesto en un directorio protegido para su uso futuro.

Para ver un ejemplo, consulte el [Paso 3](#) in “Cómo crear un manifiesto de control” en la [página 96](#).

3 Posteriormente, prepare un manifiesto idéntico al manifiesto de control.

```
# bart create -R /etc > test-manifest
```

4 Proteja el segundo manifiesto.

```
# mv test-manifest /var/adm/log/bartlogs
```

5 Compare los dos manifiestos.

Utilice las mismas opciones de la línea de comandos y el mismo archivo de reglas para comparar los manifiestos que usó para crearlos.

```
# bart compare options control-manifest test-manifest > bart-report
```

6 Examine el informe de BART para encontrar rarezas.

Ejemplo 6–2 Seguimiento de cambios de archivo para el mismo sistema a lo largo del tiempo

En este ejemplo, se muestra cómo realizar un seguimiento de los cambios en el directorio /etc a lo largo del tiempo. Este tipo de comparación le permite ubicar archivos importantes del sistema que se vieron comprometidos.

- Cree un manifiesto de control.


```
# cd /var/adm/logs/manifests
# bart create -R /etc > system1.control.090712
! Version 1.1
! HASH SHA256
! Friday, September 07, 2012 (11:11:17)
# Format:
#fname D size mode acl dirmtime uid gid
#fname P size mode acl mtime uid gid
#fname S size mode acl mtime uid gid
#fname F size mode acl mtime uid gid contents
#fname L size mode acl lnmtime uid gid dest
#fname B size mode acl mtime uid gid devnode
#fname C size mode acl mtime uid gid devnode
/.cpr_config F 2236 100644 owner@:read_data/write_data/append_data/read_xattr/write_xattr/read_attributes/write_attributes/read_acl/write_acl/write_owner/synchronize:allow,group@:read_data/read_xattr/read_attributes/read_acl/synchronize:allow,everyone@:read_data/read_xattr/read_attributes/read_acl/synchronize:allow
4e271c59 0 0 3ebc418eb5be3729ffe7e54053be2d33ee884205502c81ae9689cd8cca5b0090
/.login F 1429 100644 owner@:read_data/write_data/append_data/read_xattr/write_xattr/read_attributes/write_attributes/read_acl/write_acl/write_owner/synchronize:allow,group@:read_data/read_xattr/read_attributes/read_acl/synchronize:allow,everyone@:read_data/read_xattr/read_attributes/read_acl/synchronize:allow
4bf9d6d7 0 3 ff6251a473a53de68ce8b4036d0f569838cff107caf1dd9fd04701c48f09242e
.
.
.
```

- Más adelante, cree un manifiesto de prueba con las mismas opciones de la línea de comandos.

```
# bart create -R /etc > system1.test.101012
Version 1.1
! HASH SHA256
! Wednesday, October 10, 2012 (10:10:17)
# Format:
#fname D size mode acl dirmtime uid gid
#fname P size mode acl mtime uid gid
#fname S size mode acl mtime uid gid
#fname F size mode acl mtime uid gid contents
#fname L size mode acl lnmtime uid gid dest
#fname B size mode acl mtime uid gid devnode
#fname C size mode acl mtime uid gid devnode
/.cpr_config F 2236 100644 owner@:read_data/write_data/append_data/read_xattr/write_xattr/read_attributes/write_attributes/read_acl/write_acl/write_owner/synchronize:allow,group@:read_data/read_xattr/read_attributes/read_acl/synchronize:allow,everyone@:read_data/read_xattr/read_attributes/read_acl/synchronize:allow
4e271c59 0 0 3ebc418eb5be3729ffe7e54053be2d33ee884205502c81ae9689cd8cca5b0090
.
.
.
```

- Compare los manifiestos.

```
# bart compare system1.control.090712 system1.test.101012
/security/audit_class
mtime 4f272f59
```

La salida indica que la hora de modificación del archivo `audit_class` ha cambiado desde la creación del manifiesto de control. Si el cambio es inesperado, puede seguir investigando.

▼ Cómo comparar manifiestos de diferentes sistemas

Mediante la comparación de los manifiestos de distintos sistemas, puede determinar si los sistemas se instalaron de forma idéntica o se actualizaron en sincronización. Por ejemplo, si ha personalizado los sistemas para un determinado objetivo de seguridad, esta comparación busca cualquier discrepancia entre el manifiesto que representa su objetivo de seguridad y los manifiestos de los otros sistemas.

Antes de empezar Para comparar manifiestos del sistema, debe asumir el rol `root`.

1 Cree un manifiesto de control.

```
# bart create options > control-manifest
```

Para conocer las opciones, consulte la página del comando `man bart(1M)`.

2 (Opcional) Guarde el manifiesto en un directorio protegido para su uso futuro.

Para ver un ejemplo, consulte el [Paso 3](#) in “Cómo crear un manifiesto de control” en la [página 96](#).

3 En el sistema de prueba, utilice las mismas opciones `bart` para crear un manifiesto.

```
# bart create options > test1-manifest
```

4 (Opcional) Guarde el manifiesto en un directorio protegido para su uso futuro.

5 Para realizar la comparación, copie los manifiestos en una ubicación central.

Por ejemplo:

```
# cp control-manifest /net/ test-server/var/adm/logs/bartlogs
```

Si el sistema de prueba no es un sistema de montaje NFS, utilice `sftp` u otro medio fiable para copiar los manifiestos en una ubicación central.

6 Compare los manifiestos y redirija la salida a un archivo.

```
# bart compare control-manifest test1-manifest > test1.report
```

7 Examine el informe de BART para encontrar rarezas.

Ejemplo 6-3 Identificación de un archivo sospechoso en el directorio /usr/bin

En este ejemplo, se compara el contenido del directorio /usr/bin en dos sistemas.

- Cree un manifiesto de control.

```
# bart create -R /usr/bin > control-manifest.090711
! Version 1.1
! HASH SHA256
! Wednesday, September 07, 2011 (11:11:17)
# Format:
#fname D size mode acl dirmtime uid gid
#fname P size mode acl mtime uid gid
#fname S size mode acl mtime uid gid
#fname F size mode acl mtime uid gid contents
#fname L size mode acl lnmtime uid gid dest
#fname B size mode acl mtime uid gid devnode
#fname C size mode acl mtime uid gid devnode
/2to3 F 105 100555 owner@:read_data/read_xattr/write_xattr/execute/read_attributes/write_attributes/read_acl/write_acl/write_owner/synchronize:allow,group@:read_data/read_xattr/execute/read_attributes/read_acl/synchronize:allow,everyone@:read_data/read_xattr/execute/read_attributes/read_acl/synchronize:allow 4bf9d261 0
2 154de3e7bdfd0d57a074c9fae0896a9e2e04bebf5e872d273b063319e57f334
/7z F 509220 100555 owner@:read_data/read_xattr/write_xattr/execute/read_attributes/write_attributes/read_acl/write_acl/write_owner/synchronize:allow,group@:read_data/read_xattr/execute/read_attributes/read_acl/synchronize:allow,everyone@:read_data/read_xattr/execute/read_attributes/read_acl/synchronize:allow 4dad48a 0
2 3ecd418eb5be3729ffe7e54053be2d33ee884205502c81ae9689cd8cca5b0090
...
```

- Cree un manifiesto idéntico para cada sistema que desee comparar con el sistema de control.

```
# bart create -R /usr/bin > system2-manifest.101011
! Version 1.1
! HASH SHA256
! Monday, October 10, 2011 (10:10:22)
# Format:
#fname D size mode acl dirmtime uid gid
#fname P size mode acl mtime uid gid
#fname S size mode acl mtime uid gid
#fname F size mode acl mtime uid gid contents
#fname L size mode acl lnmtime uid gid dest
#fname B size mode acl mtime uid gid devnode
#fname C size mode acl mtime uid gid devnode
/2to3 F 105 100555 owner@:read_data/read_xattr/write_xattr/execute/read_attributes/write_attributes/read_acl/write_acl/write_owner/synchronize:allow,group@:read_data/read_xattr/execute/read_attributes/read_acl/synchronize:allow,everyone@:read_data/read_xattr/execute/read_attributes/read_acl/synchronize:allow 4bf9d261 0
2 154de3e7bdfd0d57a074c9fae0896a9e2e04bebf5e872d273b063319e57f334
...
```

- Copie los manifiestos en la misma ubicación.

```
# cp control-manifest.090711 /net/system2.central/bart/manifests
```

- Compare los manifiestos.

```
# bart compare control-manifest.090711 system2.test.101011 > system2.report
/su:
```

```
gid control:3 test:1
/ypcat:
mtime control:3fd72511 test:3fd9eb23
```

La salida indica que el ID de grupo del archivo su en el directorio `/usr/bin` no es el mismo que el del sistema de control. Esta información podría indicar que una versión distinta del software se ha instalado en el sistema de prueba. Como se ha cambiado el GID, el motivo más probable es que alguien haya alterado el archivo.

▼ Cómo personalizar un informe de BART especificando atributos de archivos

Este procedimiento resulta útil para filtrar las salidas de manifiestos ya existentes para determinados atributos de archivos.

Antes de empezar Debe asumir el rol root. Para obtener más información, consulte [“Cómo usar los derechos administrativos que tiene asignados” en la página 164](#).

- 1 Determine qué atributos de archivo se van a comprobar.
- 2 Compare dos manifiestos que contienen los atributos de archivos que se van a comprobar.

Por ejemplo:

```
# bart compare -i lnmtime,mtime control-manifest.121511 \
test-manifest.010512 > bart.report.010512
```

Use una coma en la sintaxis de la línea de comandos para separar cada atributo de archivo.

- 3 Examine el informe de BART para encontrar rarezas.

▼ Cómo personalizar un informe de BART mediante un archivo de reglas

Mediante el uso de un archivo de reglas, puede personalizar un manifiesto BART para determinados archivos y atributos de archivos de interés. Mediante el uso de distintos archivos de reglas en manifiestos BART predeterminados, puede ejecutar diferentes comparaciones para los mismos manifiestos.

Antes de empezar Debe asumir el rol root. Para obtener más información, consulte [“Cómo usar los derechos administrativos que tiene asignados” en la página 164](#).

- 1 Determine qué archivos y atributos de archivos desea supervisar.

- 2 Cree un archivo de reglas con las directivas adecuadas.
- 3 Cree un manifiesto de control con el archivo de reglas que ha creado.

```
# bart create -r myrules1-file > control-manifest
```
- 4 (Opcional) Guarde el manifiesto en un directorio protegido para su uso futuro.
 Para ver un ejemplo, consulte el [Paso 3](#) in “Cómo crear un manifiesto de control” en la página 96.
- 5 Cree un manifiesto idéntico en un sistema diferente, más tarde o al mismo tiempo.

```
# bart create -r myrules1-file > test-manifest
```
- 6 Compare los manifiestos utilizando el mismo archivo de reglas.

```
# bart compare -r myrules1-file control-manifest test-manifest > bart.report
```
- 7 Examine el informe de BART para encontrar rarezas.

Ejemplo 6–4 Uso del archivo de reglas para personalizar manifiestos BART y el informe de comparación

El siguiente archivo de reglas indica que el comando `bart create` muestre todos los atributos de los archivos en el directorio `/usr/bin`. Además, el archivo de reglas le indica al comando `bart compare` que sólo informe sobre los cambios de tamaño y contenido en el mismo directorio.

```
# Check size and content changes in the /usr/bin directory.
# This rules file only checks size and content changes.
# See rules file example.
```

```
IGNORE all
CHECK size contents
/usr/bin
```

- Cree un manifiesto de control con el archivo de reglas que ha creado.

```
# bart create -r usrbinrules.txt > usr_bin.control-manifest.121011
```
- Prepare un manifiesto idéntico cada vez que desee supervisar cambios realizados en el directorio `/usr/bin`.

```
# bart create -r usrbinrules.txt > usr_bin.test-manifest.121111
```
- Compare los manifiestos utilizando el mismo archivo de reglas.

```
# bart compare -r usrbinrules.txt usr_bin.control-manifest.121011 \
usr_bin.test-manifest.121111
```
- Examine la salida del comando `bart compare`.

```
/usr/bin/gunzip:  add
/usr/bin/ypcat:
delete
```

Esta salida de procedimiento indica que se suprimió el archivo `/usr/bin/ypcat` y se agregó el archivo `/usr/bin/gunzip`.

Manifiestos, archivos de reglas e informes de BART (referencia)

En esta sección, se describe el formato de archivos que BART utiliza y crea.

Formato de archivo de manifiesto de BART

Cada entrada de archivo de manifiesto consiste en una sola línea, según el tipo de archivo. Cada entrada comienza con *fname*, que es el nombre del archivo. Para evitar problemas de análisis causados por caracteres especiales incrustados en los nombres de archivos, estos últimos se codifican. Para obtener más información, consulte [“Formato de archivo de reglas de BART” en la página 107](#).

Los campos que se enumeran a continuación representan los siguientes atributos de archivos:

<i>type</i>	Tipo de archivo con los siguientes valores posibles: ▪ B para un nodo de dispositivo de bloques ▪ C para un nodo de dispositivo de caracteres ▪ D para un directorio ▪ F para un archivo ▪ L para un enlace simbólico ▪ P para una conducción ▪ S para un socket
<i>size</i>	Tamaño del archivo en bytes.
<i>mode</i>	Número octal que representa los permisos del archivo.
<i>acl</i>	Atributos de ACL del archivo. Para un archivo con atributos de ACL, contiene la salida de <code>acltotext()</code> .
<i>uid</i>	ID de usuario numérico del propietario de esta entrada.
<i>gid</i>	ID de grupo numérico del propietario de esta entrada.
<i>dirmtime</i>	Hora de la última modificación, en segundos, desde las 00:00:00 UTC del 1 de enero de 1970, para los directorios.

<i>lnmtime</i>	Hora de la última modificación, en segundos, desde las 00:00:00 UTC del 1 de enero de 1970, para los enlaces.
<i>mtime</i>	Hora de la última modificación, en segundos, desde las 00:00:00 UTC del 1 de enero de 1970, para los archivos.
<i>contents</i>	Valor de suma de comprobación del archivo. Este atributo sólo se especifica para los archivos regulares. Si desactiva la comprobación del contexto, o si las sumas de comprobación no se pueden calcular, el valor de este campo es -.
<i>dest</i>	Destino de un enlace simbólico.
<i>devnode</i>	Valor del nodo de dispositivo. Este atributo es sólo para archivos del dispositivo de caracteres y archivos del dispositivo de bloques.

Para obtener más información, consulte la página del comando `man bart_manifest(4)`.

Formato de archivo de reglas de BART

Los archivos de reglas son archivos de texto que constan de líneas que especifican qué archivos se van a incluir en el manifiesto y qué atributos de archivos se van a incluir en el manifiesto o el informe. La herramienta ignora las líneas que empiezan por #, las líneas en blanco y las líneas que contienen espacios en blanco.

Los archivos de entrada tienen tres tipos de directivas:

- Directiva de subárbol, con modificadores de coincidencia de modelos opcionales
- Directiva CHECK
- Directiva IGNORE

EJEMPLO 6-5 Formato de archivo de reglas

```
<Global CHECK/IGNORE Directives>
<subtree1> [pattern1..]
<IGNORE/CHECK Directives for subtree1>

<subtree2> [pattern2..]
<subtree3> [pattern3..]
<subtree4> [pattern4..]
<IGNORE/CHECK Directives for subtree2, subtree3, subtree4>
```

Nota – Todas las directivas se leen en orden. Las directivas posteriores pueden sustituir las directivas anteriores.

Una directiva de subárbol *debe* comenzar por un nombre de ruta absoluto, seguido de cero o más sentencias de coincidencia de modelos.

Atributos de archivo de reglas

Las sentencias CHECK y IGNORE definen qué atributos de archivos se deben seguir o ignorar. Los metadatos que inician cada manifiesto muestra las *palabras clave* de atributo por tipo de archivo. Si desea ver un ejemplo, consulte el [Ejemplo 6–1](#).

La palabra clave `all` se refiere a todos los atributos del archivo.

Sintaxis de comillas

El idioma de especificación del archivo de reglas que BART utiliza es la sintaxis de comillas estándar de UNIX para representar nombres de archivos no estándar. Los caracteres incrustados de tabulación, espacio, línea nueva o caracteres especiales se codifican en sus formas octales para permitir que la herramienta lea nombres de archivos. Esta sintaxis de comillas no uniforme evita que determinados nombres de archivos, como los que contienen un retorno de carro incrustado, se procesen correctamente en una canalización de comando. El idioma de especificación de reglas permite la expresión de criterios de filtrado de nombres de archivos complejos, que sería difícil de describir, y poco eficaz, al utilizar la sintaxis de shell sola.

Para obtener más información, consulte la página del comando `man bart_rules(4)`.

Creación de informes de BART

En el modo predeterminado, un informe de BART comprueba todos los archivos instalados en el sistema, con la excepción de las marcas de tiempo de directorio modificadas (`dirmtime`):

```
CHECK all
IGNORE dirmtime
```

Si proporciona un archivo de reglas, las directivas globales CHECK `all` e IGNORE `dirmtime`, en ese orden, se anteponen automáticamente al archivo de reglas.

Salida de BART

Se devolvieron los siguientes valores de salida:

0	Éxito
1	Error no fatal durante el procesamiento de archivos, como problemas de permisos
>1	Error fatal, como una opción de línea de comandos no válida

El mecanismo de creación de informes ofrece dos tipos de salidas, detallada y programática:

- La salida detallada es la salida predeterminada, y se localiza y se presenta en varias líneas. La salida detallada está internacionalizada y en lenguaje natural. Cuando el comando `bart compare` compara dos manifiestos el sistema, se genera una lista de diferencias de archivos.

La estructura de la salida es la siguiente:

```
filename attribute control:control-val test:test-val
```

filename Nombre del archivo que difiere entre el manifiesto de control y el manifiesto de prueba.

attribute Nombre del atributo de archivo que difiere entre los manifiestos que se comparan. El *control-val* precede al *test-val*. Cuando las discrepancias de varios atributos se producen en un mismo archivo, cada diferencia se indica en una línea separada.

A continuación, se muestra un ejemplo de las diferencias de atributos para el archivo `/etc/passwd`. La salida indica que los atributos `size`, `mtime` y `contents` han cambiado.

```
/etc/passwd:
size      control:74      test:81
mtime control:3c165879   test:3c165979
contents  control:daca28ae0de97afd7a6b91fde8d57afa
test:84b2b32c4165887355317207b48a6ec7
```

- La salida programática se genera con la opción `-p` al ejecutar el comando `bart compare`. Esta salida es adecuada para la manipulación programática.

La estructura de la salida es la siguiente:

```
filename attribute control-val test-val [attribute control-val test-val]*
```

filename Igual que el atributo *filename* en el formato predeterminado

atributo control-val test-val Una descripción de los atributos de archivos que difieren entre los manifiestos de control y de prueba para cada archivo

Para ver una lista de atributos admitidos por el comando `bart`, consulte [“Atributos de archivo de reglas” en la página 108](#).

Para obtener más información, consulte la página del comando `man bart(1M)`.

Control de acceso a archivos (tareas)

En este capítulo, se describe cómo proteger archivos en Oracle Solaris. Asimismo, se describe cómo proteger el sistema contra archivos cuyos permisos podrían ponerlo en peligro.

Nota – Para proteger archivos ZFS con listas de control de acceso (ACL), consulte el [Capítulo 7](#), “Uso de listas de control de acceso y atributos para proteger archivos Oracle Solaris ZFS” de *Administración de Oracle Solaris 11.1: sistemas de archivos ZFS*.

En este capítulo, se tratan los siguientes temas:

- “Uso de permisos UNIX para proteger archivos” en la página 111
- “Cómo evitar que los archivos ejecutables pongan en riesgo la seguridad” en la página 118
- “Protección de archivos con permisos UNIX (mapa de tareas)” en la página 119
- “Protección contra programas con riesgo de seguridad (mapa de tareas)” en la página 126

Uso de permisos UNIX para proteger archivos

Los archivos se pueden proteger mediante permisos de archivo UNIX y mediante ACL. Los archivos con bits de permanencia y los archivos que son ejecutables requieren medidas de seguridad especiales.

Comandos para visualizar y proteger archivos

En esta tabla, se describen los comandos para supervisar y proteger archivos y directorios.

TABLA 7-1 Comandos para proteger archivos y directorios

Comando	Descripción	Página de comando man
ls	Muestra los archivos en un directorio e información sobre los archivos.	ls(1)
chown	Cambia la propiedad de un archivo.	chown(1)
chgrp	Cambia la propiedad de grupo de un archivo.	chgrp(1)
chmod	Cambia permisos en un archivo. Puede utilizar el modo simbólico, que utiliza letras y símbolos, o el modo absoluto, que utiliza números octales, para cambiar los permisos en un archivo.	chmod(1)

Propiedad de archivos y directorios

Los permisos de archivo UNIX tradicionales pueden asignar propiedad a tres clases de usuarios:

- **usuario:** el propietario del archivo o directorio, que, normalmente, es el usuario que creó el archivo. El propietario de un archivo puede decidir quién tiene derecho a leer el archivo, escribir en el archivo (realizar cambios en él) o, si el archivo es un comando, ejecutar el archivo.
- **grupo:** los miembros de un grupo de usuarios.
- **otros:** todos los demás usuarios que no son los propietarios del archivo y no son miembros del grupo.

El propietario del archivo, normalmente, puede asignar o modificar permisos de archivo. Además, la cuenta root puede cambiar la propiedad de un archivo. Para sustituir la política del sistema, consulte el [Ejemplo 7-2](#).

Un archivo puede ser uno de siete tipos. Cada tipo se muestra con un símbolo:

- (símbolo menos)	Texto o programa
b	Archivo especial de bloques
c	Archivo especial de caracteres
d	Directorio
l	Enlace simbólico
s	Socket
D	Puerta
P	Conducción con nombre (FIFO)

Permisos de archivo UNIX

En la siguiente tabla, se muestran y se describen los permisos que puede otorgar a cada clase de usuario para un archivo o directorio.

TABLA 7-2 Permisos de archivos y directorios

Símbolo	Permiso	Objeto	Descripción
r	Lectura	Archivo	Los usuarios designados pueden abrir y leer el contenido de un archivo.
		Directorio	Los usuarios designados pueden enumerar archivos en el directorio.
w	Escritura	Archivo	Los usuarios designados pueden modificar el contenido del archivo o suprimir el archivo.
		Directorio	Los usuarios designados pueden agregar archivos o enlaces en el directorio. También pueden eliminar archivos o enlaces en el directorio.
x	Ejecución	Archivo	Los usuarios designados pueden ejecutar el archivo si es un programa o una secuencia de comandos de shell. También pueden ejecutar el programa con una de las llamadas del sistema <code>exec(2)</code> .
		Directorio	Los usuarios designados pueden abrir o ejecutar archivos en el directorio. También pueden hacer que el directorio y los directorios debajo de él sean los actuales.
-	Denegado	Archivo y directorio	Los usuarios designados no pueden leer, escribir ni ejecutar el archivo.

Estos permisos de archivo se aplican a archivos regulares y a archivos especiales, como dispositivos, sockets y conducciones con nombre (FIFO).

Para un enlace simbólico, los permisos que se aplican son los permisos del archivo al que el enlace hace referencia.

Puede proteger los archivos de un directorio y sus subdirectorios estableciendo permisos de archivo restrictivos en ese directorio. Tenga en cuenta que, sin embargo, el rol `root` tiene acceso a todos los archivos y directorios en el sistema.

Permisos de archivo especiales (setuid, setgid y bit de permanencia)

Tres tipos de permisos especiales están disponibles para archivos ejecutables y directorios públicos: `setuid`, `setgid` y bit de permanencia. Cuando estos permisos se establecen, cualquier usuario que ejecuta ese archivo ejecutable asume el ID del propietario (o grupo) del archivo ejecutable.

Debe ser extremadamente cuidadoso cuando define permisos especiales, porque los permisos especiales constituyen un riesgo de seguridad. Por ejemplo, un usuario puede obtener capacidades de root mediante la ejecución de un programa que establece el ID de usuario (UID) en 0, que es el UID de root. Además, todos los usuarios pueden establecer permisos especiales para archivos que poseen, lo cual constituye otro problema de seguridad.

Debe supervisar el sistema para detectar cualquier uso no autorizado de los permisos `setuid` y `setgid` con intención de obtener capacidades de root. Un permiso sospechoso concede la propiedad de un programa administrativo a un usuario, en lugar de a root o bin. Para buscar y mostrar todos los archivos que utilizan este permiso especial, consulte [“Cómo buscar archivos con permisos de archivo especiales” en la página 126](#).

Permiso `setuid`

Cuando el permiso `setuid` se establece en un archivo ejecutable, se otorga acceso a un proceso que ejecuta este archivo según el propietario del archivo. El acceso *no* se basa en el usuario que está ejecutando el archivo ejecutable. Este permiso especial permite a un usuario acceder a los archivos y directorios que, normalmente, están disponibles sólo para el propietario.

Por ejemplo, el permiso `setuid` del comando `passwd` hace posible que los usuarios cambien contraseñas. Un comando `passwd` con permiso `setuid` sería de la siguiente manera:

```
-r-sr-sr-x  3 root    sys      28144 Jun 17 12:02 /usr/bin/passwd
```

Este permiso especial presenta un riesgo de seguridad. Algunos usuarios determinados pueden buscar una manera de mantener los permisos que se les otorgan mediante el proceso `setuid`, incluso después de que el proceso ha terminado de ejecutarse.

Nota – El uso de permisos `setuid` con los UID reservados (de 0 a 100) de un programa podría no establecer el UID efectivo correctamente. Utilice una secuencia de comandos de shell o evite el uso de los UID reservados con permisos `setuid`.

Permiso `setgid`

El permiso `setgid` es similar al permiso `setuid`. Se cambia el ID de grupo (GID) efectivo del proceso al grupo que posee el archivo y se le concede acceso a un usuario según los permisos que se otorgan a ese grupo. El comando `/usr/bin/mail` tiene permisos `setgid`:

```
-r-x--s--x  1 root    mail     67504 Jun 17 12:01 /usr/bin/mail
```

Cuando el permiso `setgid` se aplica a un directorio, los archivos que se crearon en ese directorio pertenecen al grupo al que pertenece el directorio. Los archivos no pertenecen al grupo al que pertenece el proceso de creación. Cualquier usuario que tiene permisos de escritura y ejecución en el directorio puede crear un archivo allí. Sin embargo, el archivo pertenece al grupo que posee el directorio, no al grupo al que pertenece el usuario.

Debe supervisar el sistema para detectar cualquier uso no autorizado del permiso `setgid` con intención de obtener capacidades de `root`. Un permiso sospechoso otorga acceso de grupo a tal programa a un grupo poco común en lugar de a `root` o `bin`. Para buscar y mostrar todos los archivos que utilizan este permiso, consulte [“Cómo buscar archivos con permisos de archivo especiales” en la página 126](#).

Bit de permanencia

El *bit de permanencia* es un bit de permiso que protege los archivos dentro de un directorio. Si el directorio tiene el bit de permanencia establecido, un archivo sólo puede ser suprimido por el propietario del archivo, el propietario del directorio o un usuario con privilegios. El usuario `root` es un ejemplo de un usuario con privilegios. El bit de permanencia impide que un usuario suprima los archivos de otros usuarios de directorios públicos, como `/tmp`:

```
drwxrwxrwt 7 root sys 400 Sep 3 13:37 tmp
```

Asegúrese de definir el bit de permanencia manualmente al configurar un directorio público en un sistema de archivos TMPFS. Para obtener instrucciones, consulte el [Ejemplo 7-5](#).

Valor umask predeterminado

Al crear un archivo o directorio, se crea con un conjunto predeterminado de permisos. Los valores predeterminados del sistema son abiertos. Un archivo de texto tiene permisos `666`, que conceden permisos de lectura y escritura a todos los usuarios. Un directorio y un archivo ejecutable tienen permisos `777`, que conceden permisos de lectura, escritura y ejecución a todos los usuarios. Normalmente, los usuarios sustituyen los valores predeterminados del sistema en sus archivos de inicialización de shell, como `.bashrc` y `.kshrc.user`. Un administrador también puede establecer valores predeterminados en el archivo `/etc/profile`.

El valor asignado por el comando `umask` se obtiene del valor predeterminado. Este proceso tiene el efecto de denegar permisos de la misma forma que el comando `chmod` los otorga. Por ejemplo, el comando `chmod 022` otorga permiso de escritura para grupo y otros. El comando `umask 022` deniega permiso de escritura para grupo y otros.

En la siguiente tabla, se muestran algunos valores `umask` típicos y el efecto que tienen en un archivo ejecutable.

TABLA 7-3 Valores `umask` para niveles de seguridad diferentes

Nivel de seguridad	Valor <code>umask</code>	Permisos no permitidos
Permisivo (744)	022	w para grupo y otros
Moderado (741)	026	w para grupo, rw para otros
Estricto (740)	027	w para grupo, rwx para otros

TABLA 7-3 Valores umask para niveles de seguridad diferentes *(Continuación)*

Nivel de seguridad	Valor umask	Permisos no permitidos
Grave (700)	077	rwX para grupo y otros

Para obtener más información sobre la configuración del valor umask, consulte la página del comando `man umask(1)`.

Modos de permiso de archivo

El comando `chmod` permite cambiar los permisos en un archivo. Debe ser `root` o el propietario de un archivo o directorio para cambiar los permisos.

Puede utilizar el comando `chmod` para definir permisos en uno de los dos modos siguientes:

- **Modo absoluto:** use números para representar permisos de archivo. Al cambiar los permisos mediante el modo absoluto, representa los permisos para cada triplo con un número de modo octal. El modo absoluto es el método que se utiliza con más frecuencia para establecer permisos.
- **Modo simbólico:** utilice combinaciones de letras y símbolos para agregar o eliminar permisos.

En la siguiente tabla, se muestran los valores octales para configurar permisos de archivo en modo absoluto. Use estos números en conjuntos de tres para definir permisos para propietario, grupo y otros, en ese orden. Por ejemplo, el valor 644 establece permisos de lectura y escritura para propietario, y permisos de sólo lectura para grupo y otros.

TABLA 7-4 Establecimiento de permisos de archivo en modo absoluto

Valor octal	Permisos de archivo establecidos	Descripción de permisos
0	- - -	Sin permisos
1	- - X	Sólo permiso de ejecución
2	- W -	Sólo permiso de escritura
3	- W X	Permisos de escritura y ejecución
4	r - -	Sólo permiso de lectura
5	r - X	Permisos de lectura y ejecución
6	r W -	Permisos de lectura y escritura
7	r W X	Permisos de lectura, escritura y ejecución

En la siguiente tabla, se muestran los símbolos para establecer permisos de archivo en modo simbólico. Los símbolos pueden especificar los permisos de qué usuarios se van a definir o cambiar, la operación que se va a realizar y los permisos que se están asignando o cambiando.

TABLA 7-5 Establecimiento de permisos de archivo en modo simbólico

Símbolo	Función	Descripción
u	<i>who</i>	Usuario (propietario)
g	<i>who</i>	Grupo
o	<i>who</i>	Otros
a	<i>who</i>	All (Todo)
=	<i>operator</i>	Asignación
+	<i>operator</i>	Agregar
-	<i>operator</i>	Eliminar
r	<i>permissions</i>	Lectura
w	<i>permissions</i>	Escritura
x	<i>permissions</i>	Ejecución
l	<i>permissions</i>	Bloqueo obligatorio, bit <code>setgid</code> está activado, bit de ejecución de grupo está desactivado
s	<i>permissions</i>	Bit <code>setuid</code> o <code>setgid</code> está activado
t	<i>permissions</i>	Bit de permanencia está activado, bit de ejecución para otros está activado

Las designaciones *quién operador permisos* en la columna de función especifican los símbolos que cambian los permisos en el archivo o directorio.

who Especifica los permisos de qué usuarios se van a cambiar.

operator Especifica la operación que se va a realizar.

permissions Especifica qué permisos se van a cambiar.

Puede definir permisos especiales en un archivo en modo absoluto o modo simbólico. No obstante, debe utilizar el modo simbólico para definir o eliminar permisos `setuid` en un directorio. En el modo absoluto, los permisos especiales se establecen agregando un nuevo valor octal a la izquierda del tripo de permiso. En la siguiente tabla, se muestran los valores octales para definir permisos especiales en un archivo.

TABLA 7-6 Establecimiento de permisos de archivo especiales en modo absoluto

Valor octal	Permisos de archivo especiales
1	Bit de permanencia
2	setgid
4	setuid

Uso de listas de control de acceso para proteger archivos UFS

La protección de archivos UNIX tradicionales proporciona permisos de lectura, escritura y ejecución para las tres clases de usuario: propietario de archivo, grupo de archivos y otros. En un sistema de archivos UFS, una lista de control de acceso (ACL) proporciona una mayor seguridad para los archivos, ya que le permite hacer lo siguiente:

- Definir permisos de archivo para el propietario del archivo, el grupo, otros y usuarios y grupos específicos.
- Definir permisos predeterminados para cada una de las categorías anteriores.

Nota – Para las ACL en el sistema de archivos ZFS y las ACL en archivos NFSv4, consulte el [Capítulo 7, “Uso de listas de control de acceso y atributos para proteger archivos Oracle Solaris ZFS”](#) de *Administración de Oracle Solaris 11.1: sistemas de archivos ZFS*.

Por ejemplo, si desea que todos los usuarios de un grupo puedan leer un archivo, puede, simplemente, conceder permisos de lectura de grupo en ese archivo. Sin embargo, si desea que sólo una persona del grupo pueda escribir en ese archivo, puede utilizar una ACL.

Para obtener más información sobre las ACL en sistemas de archivos UFS, consulte la *Guía de administración del sistema: servicios de seguridad* para la versión Oracle Solaris 10.

Cómo evitar que los archivos ejecutables pongan en riesgo la seguridad

Los programas leen y escriben datos en la pila. Normalmente, se ejecutan de partes de memoria de sólo lectura que se designan específicamente por código. Algunos ataques que provocan que memorias intermedias de la pila se desborden intentan insertar nuevo código en la pila y provocar que el programa lo ejecute. Al eliminar el permiso de ejecución de la memoria de la pila se impide que estos ataques tengan éxito. Es decir, la mayoría de los programas pueden funcionar correctamente sin utilizar pilas ejecutables.

Los procesos de 64 bits siempre tienen pilas no ejecutables. De manera predeterminada, los procesos de SPARC de 32 bits tienen pilas ejecutables. La variable `noexec_user_stack` permite especificar si las pilas de los procesos de 32 bits son ejecutables.

Una vez que esta variable se define, se envía una señal `SIGSEGV` a los programas que intentan ejecutar el código en sus pilas. Esta señal, normalmente, tiene como resultado la terminación del programa con un volcado del núcleo central. Esos programas también generan un mensaje de advertencia que incluye el nombre del programa ofensivo, el ID de proceso y el UID real del usuario que ejecutó el programa. Por ejemplo:

```
a.out[347] attempt to execute code on stack by uid 555
```

El mensaje es registrado por el daemon `syslog` cuando la utilidad `syslog kern` está establecida en el nivel `notice`. Este registro está establecido de manera predeterminada en el archivo `syslog.conf`, lo que significa que el mensaje se envía a la consola y al archivo `/var/adm/messages`. Para obtener más información, consulte las páginas del comando `man syslogd(1M)` y `man syslog.conf(4)`.

El mensaje `syslog` es útil para observar posibles problemas de seguridad. El mensaje también identifica programas válidos que dependen de pilas ejecutables cuyo funcionamiento correcto ha sido impedido al establecer la variable `noexec_user_stack`. Si no desea que se registre ningún mensaje, establezca la variable de registro `noexec_user_stack_log` en cero, en el archivo `/etc/system`. Aunque los mensajes no se registran, la señal `SIGSEGV` puede continuar para hacer que el programa en ejecución finalice con un volcado del núcleo central.

Los programas pueden marcar o evitar de forma explícita la ejecución de las pilas. La función `mprotect()` en los programas marca explícitamente la pila como ejecutable. Para obtener más información, consulte la página del comando `man mprotect(2)`. Un programa compilado con `-M/usr/lib/ld/map.noexstk` hace que la pila no sea ejecutable independientemente de la configuración del sistema.

Protección de archivos (tareas)

Los siguientes procedimientos protegen archivos con permisos UNIX, identifican archivos con riesgos de seguridad y evitan que el sistema se ponga en riesgo por estos archivos.

Protección de archivos con permisos UNIX (mapa de tareas)

El siguiente mapa de tareas indica procedimientos que enumeran permisos de archivo, cambian permisos de archivo y protegen archivos con permisos de archivo especiales.

Tarea	Para obtener instrucciones
Visualizar información de archivos.	“Cómo visualizar información de archivos” en la página 120
Cambiar la propiedad de archivo local.	“Cómo cambiar el propietario de un archivo” en la página 121 “Cómo cambiar la propiedad de grupo de un archivo” en la página 122
Cambiar permisos de archivo local.	“Cómo cambiar los permisos de archivo en modo simbólico” en la página 123 “Cómo cambiar permisos de archivo en modo absoluto” en la página 124 “Cómo cambiar permisos de archivo especiales en modo absoluto” en la página 125

▼ Cómo visualizar información de archivos

Visualice información sobre todos los archivos en un directorio mediante el comando `ls`.

- **Escriba el siguiente comando para mostrar un listado largo de todos los archivos en el directorio actual.**

`% ls -la`

- l Muestra el formato largo que incluye la propiedad de usuario, la propiedad de grupo y los permisos de archivo.
- a Muestra todos los archivos, incluidos los archivos ocultos que empiezan con un punto (.).

Para todas las opciones del comando `ls`, consulte la página del comando `man ls(1)`.

Ejemplo 7-1 Visualización de información de archivos

En el siguiente ejemplo, se muestra una lista parcial de los archivos en el directorio `/sbin`.

```
% cd /sbin
% ls -la
total 4960
drwxr-xr-x  2 root    sys          64 Dec  8 11:57 ./
drwxr-xr-x 39 root    root         41 Dec  8 15:20 ../
-r-xr-xr-x  1 root    bin        21492 Dec  1 20:55 autopush*
-r-xr-xr-x  1 root    bin        33680 Oct  1 11:36 beadm*
-r-xr-xr-x  1 root    bin       184360 Dec  1 20:55 bootadm*
lrwxrwxrwx  1 root    root         21 Jun  7  2010 bpgetfile -> ...
-r-xr-xr-x  1 root    bin        86048 Dec  1 20:55 cryptoadm*
-r-xr-xr-x  1 root    bin        12828 Dec  1 20:55 devprop*
-r-xr-xr-x  1 root    bin       130132 Dec  1 20:55 dhcpagent*
-r-xr-xr-x  1 root    bin        13076 Dec  1 20:55 dhcpinfo*

.
.
.
```

Cada una de las líneas muestra información sobre un archivo en el siguiente orden:

- Tipo de archivo, por ejemplo, d. Para obtener una lista de tipos de archivo, consulte [“Propiedad de archivos y directorios” en la página 112](#).
- Permisos, por ejemplo, r-xr-xr-x. Para obtener una descripción, consulte [“Propiedad de archivos y directorios” en la página 112](#).
- Número de enlaces físicos, por ejemplo, 2.
- Propietario del archivo, por ejemplo, root.
- Grupo del archivo, por ejemplo, bin.
- Tamaño del archivo, en bytes, por ejemplo, 13076.
- Fecha de creación del archivo o la última fecha en la que el archivo se modificó, por ejemplo, Diciembre 1 20:55.
- Nombre del archivo, por ejemplo, dhcinfo.

▼ Cómo cambiar el propietario de un archivo

Antes de empezar

Si no es el propietario del archivo o directorio, debe tener asignado el perfil de derechos de gestión de acceso a objetos. Para cambiar un archivo que es un [objeto público](#), se debe asumir el rol root.

Para obtener más información, consulte [“Cómo usar los derechos administrativos que tiene asignados” en la página 164](#).

1 Visualice los permisos en un archivo local.

```
% ls -l example-file
-rw-r--r-- 1 janedoe staff 112640 May 24 10:49 example-file
```

2 Cambie el propietario del archivo.

```
# chown stacey example-file
```

3 Verifique que el propietario del archivo haya cambiado.

```
# ls -l example-file
-rw-r--r-- 1 stacey staff 112640 May 26 08:50 example-file
```

Para cambiar los permisos de acceso a archivos montados en NFS, consulte el [Capítulo 3, “Acceso a los sistemas de archivos de red \(referencia\)” de Gestión de sistemas de archivos de red en Oracle Solaris 11.1](#).

Ejemplo 7-2 Cómo permitir que los usuarios cambien la propiedad de sus propios archivos

Consideración de seguridad: necesita una buena razón para cambiar el valor de la variable `rstchown` a cero. El valor predeterminado evita que los usuarios enumeren sus archivos como pertenecientes a otros para omitir las cuotas de espacio.

En este ejemplo, el valor de la variable `rstchown` se define en cero, en el archivo `/etc/system`. Este valor permite al propietario de un archivo utilizar el comando `chown` para cambiar la propiedad del archivo a otro usuario. Este valor también permite al propietario utilizar el comando `chgrp` para establecer la propiedad de grupo de un archivo en un grupo al que el propietario no pertenece. El cambio entra en vigor cuando se reinicia el sistema.

```
set rstchown = 0
```

Para obtener más información, consulte las páginas del comando `man chown(1)` y `chgrp(1)`.

▼ **Cómo cambiar la propiedad de grupo de un archivo****Antes de empezar**

Si no es el propietario del archivo o directorio, debe tener asignado el perfil de derechos de gestión de acceso a objetos. Para cambiar un archivo que es un [objeto público](#), se debe asumir el rol `root`.

Para obtener más información, consulte “[Cómo usar los derechos administrativos que tiene asignados](#)” en la [página 164](#).

1 Cambie la propiedad de grupo de un archivo.

```
$ chgrp scifi example-file
```

Para obtener más información sobre la configuración de grupos, consulte el [Capítulo 1](#), “[Gestión de cuentas de usuario y entornos de usuario \(descripción general\)](#)” de *Gestión de las cuentas de usuario y los entornos de usuario en Oracle Solaris 11.1*.

2 Verifique que la propiedad de grupo del archivo haya cambiado.

```
$ ls -l example-file
-rw-r--r-- 1 stacey  scifi  112640 June 20 08:55 example-file
```

Consulte también el [Ejemplo 7-2](#).

▼ Cómo cambiar los permisos de archivo en modo simbólico

En el siguiente procedimiento, un usuario cambia permisos en un archivo que el usuario posee.

1 Cambie permisos en modo simbólico.

```
% chmod who operator permissions filename
```

who Especifica los permisos de qué usuarios se van a cambiar.

operator Especifica la operación que se va a realizar.

permissions Especifica qué permisos se van a cambiar. Para obtener la lista de símbolos válidos, consulte la [Tabla 7-5](#).

filename Especifica el archivo o directorio.

2 Verifique que los permisos del archivo hayan cambiado.

```
% ls -l filename
```

Nota – Si no es el propietario del archivo o directorio, debe tener asignado el perfil de derechos de gestión de acceso a objetos. Para cambiar un archivo que es un **objeto público**, se debe asumir el rol root.

Ejemplo 7-3 Cambio de permisos en modo simbólico

En el siguiente ejemplo, el permiso de lectura se quita de otros.

```
% chmod o-r example-file1
```

En el siguiente ejemplo, los permisos de lectura y ejecución se agregan a un archivo local para usuario, grupo y otros.

```
$ chmod a+rx example-file2
```

En el siguiente ejemplo, los permisos de lectura, escritura y ejecución para un grupo se asignan a un archivo local.

```
$ chmod g=rwx example-file3
```

▼ Cómo cambiar permisos de archivo en modo absoluto

En el siguiente procedimiento, un usuario cambia permisos en un archivo que el usuario posee.

1 Cambie permisos en modo absoluto.

```
% chmod nnn filename
```

nnn Especifica los valores octales que representan los permisos para el propietario de archivo, el grupo de archivos y otros, en ese orden. Para obtener la lista de valores octales válidos, consulte la [Tabla 7-4](#).

filename Especifica el archivo o directorio.

Nota – Si utiliza el comando `chmod` para cambiar permisos de archivos o directorios en objetos que ya tienen entradas de ACL, las entradas de la ACL cambiarán también. Los cambios exactos dependen de los cambios de operaciones de permisos `chmod` y de los valores de propiedad `aclmode` y `aclinherit` del sistema de archivos.

Para obtener más información, consulte el [Capítulo 7, “Uso de listas de control de acceso y atributos para proteger archivos Oracle Solaris ZFS”](#) de *Administración de Oracle Solaris 11.1: sistemas de archivos ZFS*.

2 Verifique que los permisos del archivo hayan cambiado.

```
% ls -l filename
```

Nota – Si no es el propietario del archivo o directorio, debe tener asignado el perfil de derechos de gestión de acceso a objetos. Para cambiar un archivo que es un [objeto público](#), se debe asumir el rol `root`.

Ejemplo 7-4 Cambio de permisos en modo absoluto

En el siguiente ejemplo, los permisos de un directorio público se cambian de 744 (lectura, escritura, ejecución; sólo lectura; y sólo lectura) a 755 (lectura, escritura, ejecución; lectura y ejecución; y lectura y ejecución).

```
# ls -ld public_dir
drwxr--r-- 1 jdoe  staff   6023 Aug  5 12:06 public_dir
# chmod 755 public_dir
# ls -ld public_dir
drwxr-xr-x 1 jdoe  staff   6023 Aug  5 12:06 public_dir
```

En el siguiente ejemplo, los permisos de una secuencia de comandos de shell ejecutable se cambian de lectura y escritura a lectura, escritura y ejecución.


```
% ls -l my_script
-rw----- 1 jdoe  staff  6023 Aug  5 12:06 my_script
% chmod 700 my_script
% ls -l my_script
-rwx----- 1 jdoe  staff  6023 Aug  5 12:06 my_script
```

▼ Cómo cambiar permisos de archivo especiales en modo absoluto

Antes de empezar

Si no es el propietario del archivo o directorio, debe tener asignado el perfil de derechos de gestión de acceso a objetos. Para cambiar un archivo que es un [objeto público](#), se debe asumir el rol root.

Para obtener más información, consulte “[Cómo usar los derechos administrativos que tiene asignados](#)” en la [página 164](#).

1 Cambie permisos especiales en modo absoluto.

```
% chmod nnnn filename
```

nnnn Especifica los valores octales que cambian los permisos en el archivo o directorio. El valor octal que se encuentra más a la izquierda establece los permisos especiales en el archivo. Para obtener la lista de valores octales válidos para permisos especiales, consulte la [Tabla 7-6](#).

filename Especifica el archivo o directorio.

Nota – Al utilizar el comando `chmod` para cambiar los permisos de grupo de archivos en un archivo con entradas de ACL, tanto los permisos de grupo de archivos como la máscara de la ACL se cambian a los nuevos permisos. Tenga en cuenta que los nuevos permisos de la máscara de ACL pueden cambiar los permisos para otros usuarios y grupos que tienen entradas de ACL en el archivo. Utilice el comando `getfacl` para asegurarse de que los permisos adecuados se establezcan para todas las entradas de la ACL. Para obtener más información, consulte la [página del comando `man getfacl\(1\)`](#).

2 Verifique que los permisos del archivo hayan cambiado.

```
% ls -l filename
```

Ejemplo 7-5 Establecimiento de permisos de archivo especiales en modo absoluto

En el ejemplo siguiente, el permiso `setuid` está establecido en el archivo `dbprog`.

```
# chmod 4555 dbprog
# ls -l dbprog
-r-sr-xr-x 1 db  staff  12095 May  6 09:29 dbprog
```

En el ejemplo siguiente, el permiso `setgid` está establecido en el archivo `dbprog2`.

```
# chmod 2551 dbprog2
# ls -l dbprog2
-r-xr-s--x  1 db      staff      24576 May  6 09:30 dbprog2
```

En el siguiente ejemplo, el permiso de bit de permanencia está establecido en el directorio `public_dir`.

```
# chmod 1777 public_dir
# ls -ld public_dir
drwxrwxrwt  2 jdoe    staff      512 May 15 15:27 public_dir
```

Protección contra programas con riesgo de seguridad (mapa de tareas)

El siguiente mapa de tareas indica procedimientos que buscan ejecutables riesgosos en el sistema y que impiden que los programas se aprovechen de una pila ejecutable.

Tarea	Descripción	Para obtener instrucciones
Buscar archivos con permisos especiales.	Localiza archivos con el bit <code>setuid</code> establecido, pero que no son propiedad del usuario <code>root</code> .	“Cómo buscar archivos con permisos de archivo especiales” en la página 126
Evitar que pilas ejecutables se desborden.	Impide que los programas se aprovechen de una pila ejecutable.	“Cómo impedir que programas usen pilas ejecutables” en la página 127
Evitar el registro de mensajes de pilas ejecutables.	Desactiva el registro de mensajes de pilas ejecutables.	Ejemplo 7–7

▼ Cómo buscar archivos con permisos de archivo especiales

Este procedimiento ubica el uso potencialmente no autorizado de permisos `setuid` y `setgid` en programas. Un archivo ejecutable sospechoso concede propiedad a un usuario en lugar de a `root` o `bin`.

Antes de empezar Debe asumir el rol `root`. Para obtener más información, consulte [“Cómo usar los derechos administrativos que tiene asignados” en la página 164](#).

- 1
- Busque archivos con permisos `setuid` mediante el comando `find`.

```
# find directory -user root -perm -4000 -exec ls -ldb {} \; >/tmp/filename
```

<code>find directorio</code>	Comprueba todas las rutas montadas a partir del <i>directorio</i> especificado, que puede ser <code>root (/)</code> , <code>sys</code> , <code>bin</code> o <code>mail</code> .
<code>-user root</code>	Muestra archivos que sólo son propiedad de <code>root</code> .
<code>-perm -4000</code>	Muestra archivos sólo con permisos establecidos en <code>4000</code> .
<code>-exec ls -ldb</code>	Muestra el resultado del comando <code>find</code> en formato <code>ls -ldb</code> .
<code>/tmp/filename</code>	Es el archivo que contiene los resultados del comando <code>find</code> .

2 Muestra los resultados en `/tmp/filename`.

```
# more /tmp/filename
```

Para obtener más información sobre los permisos `setuid`, consulte [“Permiso `setuid`” en la página 114](#).

Ejemplo 7-6 Búsqueda de archivos con permisos `setuid`

El resultado del siguiente ejemplo muestra que un usuario en un grupo denominado `rar` ha realizado una copia personal de `/usr/bin/sh` y ha establecido los permisos como `setuid` en `root`. Como resultado, el programa `/usr/rar/bin/sh` se ejecuta con permisos `root`.

Este resultado se ha guardado para referencia futura moviendo el archivo `/var/tmp/ckprm` a un archivo.

```
# find / -user root -perm -4000 -exec ls -ldb {} \; > /var/tmp/ckprm
# cat /var/tmp/ckprm
-r-sr-xr-x 1 root bin 38836 Aug 10 16:16 /usr/bin/at
-r-sr-xr-x 1 root bin 19812 Aug 10 16:16 /usr/bin/crontab
---s--x--x 1 root sys 46040 Aug 10 15:18 /usr/bin/ct
-r-sr-xr-x 1 root sys 12092 Aug 11 01:29 /usr/lib/mv_dir
-r-sr-sr-x 1 root bin 33208 Aug 10 15:55 /usr/lib/lpadmin
-r-sr-sr-x 1 root bin 38696 Aug 10 15:55 /usr/lib/lpsched
---s--x--- 1 root rar 45376 Aug 18 15:11 /usr/rar/bin/sh
-r-sr-xr-x 1 root bin 12524 Aug 11 01:27 /usr/bin/df
-rwsr-xr-x 1 root sys 21780 Aug 11 01:27 /usr/bin/newgrp
-r-sr-sr-x 1 root sys 23000 Aug 11 01:27 /usr/bin/passwd
-r-sr-xr-x 1 root sys 23824 Aug 11 01:27 /usr/bin/su
# mv /var/tmp/ckprm /export/sysreports/ckprm
```

▼ Cómo impedir que programas usen pilas ejecutables

Para obtener una descripción de los riesgos de seguridad de las pilas ejecutables de 32 bits, consulte [“Cómo evitar que los archivos ejecutables pongan en riesgo la seguridad” en la página 118](#).

Antes de empezar Debe asumir el rol root. Para obtener más información, consulte [“Cómo usar los derechos administrativos que tiene asignados” en la página 164.](#)

1 Edite el archivo `/etc/` y agregue la siguiente línea:

```
set noexec_user_stack=1
```

2 Reinicie el sistema.

```
# reboot
```

Ejemplo 7-7 Desactivación del registro de mensajes de pilas ejecutables

En este ejemplo, el registro de mensajes de pilas ejecutables se desactiva y el sistema se reinicia.

```
# cat /etc/system
set noexec_user_stack=1
set noexec_user_stack_log=0
# reboot
```

Véase también Para obtener más información, lea lo siguiente:

- http://blogs.oracle.com/gbrunett/entry/solaris_non_executable_stack_overview
- http://blogs.oracle.com/gbrunett/entry/solaris_non_executable_stack_continued
- http://blogs.oracle.com/gbrunett/entry/solaris_non_executable_stack_concluded

P A R T E I I I

Roles, perfiles de derechos y privilegios

En esta sección, se tratan el control de acceso basado en roles (RBAC, Role-Based Access Control) y la gestión de derechos de procesos. Los componentes de RBAC incluyen roles, perfiles de derechos y autorizaciones. La gestión de derechos de procesos se implementa a través de privilegios. Los privilegios se utilizan junto con RBAC para proporcionar una alternativa de administración más segura que la administración de un sistema con un superusuario.

- [Capítulo 8, “Uso de roles y privilegios \(descripción general\)”](#)
- [Capítulo 9, “Uso del control de acceso basado en roles \(tareas\)”](#)
- [Capítulo 10, “Atributos de seguridad en Oracle Solaris \(referencia\)”](#)

Uso de roles y privilegios (descripción general)

La función de control de acceso basado en roles (RBAC) de Oracle Solaris y la función de privilegios de Oracle Solaris proporcionan una alternativa administrativa más segura para el superusuario. En este capítulo, se proporciona información general sobre RBAC y los privilegios.

- “Control de acceso basado en roles (descripción general)” en la página 131
- “Privilegios (descripción general)” en la página 144
- “Sobre el RBAC en esta versión” en la página 153

Control de acceso basado en roles (descripción general)

El control de acceso basado en roles (RBAC) es una función de seguridad para controlar el acceso de usuarios a tareas que normalmente están restringidas al rol root. Mediante la aplicación de atributos de seguridad a procesos y usuarios, RBAC puede dividir las capacidades de superusuario entre varios administradores. La gestión de derechos de procesos se implementa a través de *privilegios*. La gestión de derechos de usuarios se implementa a través de RBAC.

- Para ver una explicación de la gestión de derechos de procesos, consulte “[Privilegios \(descripción general\)](#)” en la página 144.
- Para obtener información sobre las tareas de RBAC, consulte el [Capítulo 9, “Uso del control de acceso basado en roles \(tareas\)”](#).
- Para obtener información de referencia, consulte el [Capítulo 10, “Atributos de seguridad en Oracle Solaris \(referencia\)”](#).

RBAC: una alternativa al modelo de superusuario

En los sistemas UNIX convencionales, el usuario root, también conocido como superusuario, es omnipotente. Los programas que se ejecutan como root, o los programas setuid, son omnipotentes. El usuario root puede leer y escribir en cualquier archivo, ejecutar todos los

programas y enviar señales de terminación a cualquier proceso. De hecho, cualquier persona que puede convertirse en superusuario puede modificar el cortafuegos de un sitio, modificar la pista de auditoría, leer registros confidenciales y apagar toda la red. Un programa `setuid` usurpado puede realizar cualquier tarea en el sistema.

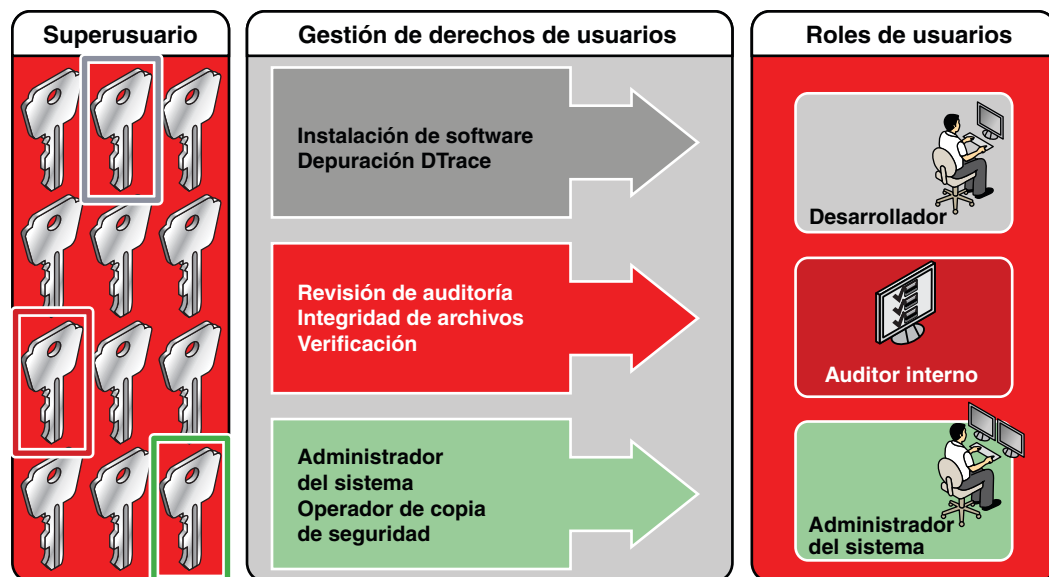
El control de acceso basado en roles (RBAC) ofrece una alternativa más segura al modelo de superusuario del tipo "todo o nada". Con RBAC, puede aplicar una política de seguridad en un nivel más específico. RBAC utiliza el principio de seguridad del *privilegio mínimo*. Privilegio mínimo significa que un usuario dispone exactamente de la cantidad de privilegios necesaria para realizar un trabajo. Los usuarios comunes tienen privilegios suficientes para utilizar sus aplicaciones, comprobar el estado de sus trabajos, imprimir archivos, crear archivos nuevos, etc. Las capacidades que van más allá de las capacidades de los usuarios comunes se agrupan en perfiles de derechos. Los usuarios que realizarán trabajos que requieren algunas de las capacidades de superusuario asumen un rol que incluye el perfil de derechos adecuado.

RBAC recopila las capacidades de superusuario en *perfiles de derechos*. Estos perfiles de derechos se asignan a cuentas de usuario especiales denominadas *roles*. Luego, un usuario puede asumir un rol para realizar un trabajo que requiere algunas de las capacidades de superusuario. Se incluyen perfiles de derechos predefinidos con el software Oracle Solaris. Usted crea los roles y asigna los perfiles.

Los perfiles de derechos pueden proporcionar capacidades amplias. Por ejemplo, el perfil de derechos de administrador del sistema permite a una cuenta realizar tareas que no están relacionadas con la seguridad, como la gestión de impresoras y trabajos cron. Los perfiles de derechos también se pueden definir de manera limitada. Por ejemplo, el perfil de derechos de gestión de cron se encarga de los trabajos `at` y `cron`. Al crear roles, se pueden asignar a los roles capacidades amplias, capacidades restringidas o ambas.

La siguiente figura ilustra cómo RBAC puede distribuir derechos a partes de confianza.

FIGURA 8-1 Distribución de derechos de RBAC



En el modelo RBAC, el superusuario crea uno o más roles. Los roles se basan en perfiles de derechos. El superusuario luego asigna los roles a los usuarios en los que confía para realizar las tareas del rol. Los usuarios inician sesión con su nombre de usuario. Después del inicio de sesión, los usuarios asumen roles que pueden ejecutar comandos administrativos restringidos y herramientas de la interfaz gráfica de usuario (GUI).

La flexibilidad en la configuración de los roles posibilita una variedad de políticas de seguridad. Aunque se incluyen pocos roles con Oracle Solaris, es posible configurar fácilmente diferentes roles. Puede basar la mayoría de los roles en perfiles de derechos del mismo nombre:

- **Root:** un rol potente equivalente al usuario root. Sin embargo, este usuario root no puede iniciar sesión. Un usuario común debe iniciar sesión y, a continuación, asumir el rol root asignado. Este rol está configurado de manera predeterminada.
- **Administrador del sistema:** un rol menos poderoso para la administración que no está relacionado con la seguridad. Este rol puede gestionar sistemas de archivos, correo e instalación de software. Sin embargo, este rol no puede definir contraseñas.
- **Operador:** rol de administrador junior para operaciones, como copias de seguridad y gestión de impresoras.

Nota – El perfil de derechos de copia de seguridad de medios proporciona acceso a todo el sistema de archivos raíz. Por lo tanto, si bien los perfiles de derechos de copia de seguridad de medios y operador están diseñados para un administrador junior, debe asegurarse de que el usuario es de confianza.

Es posible que también desee configurar uno o más roles de seguridad. Tres perfiles de derechos y sus perfiles suplementarios gestionan la seguridad: seguridad de información, seguridad de usuarios y seguridad de zonas. La seguridad de red es un perfil suplementario en el perfil de derechos de seguridad de información.

No es necesario implementar estos roles. Los roles representan una función de las necesidades de seguridad de una organización. Una posible estrategia consiste en configurar roles para administradores con fines especiales en áreas como seguridad, redes o administración de cortafuegos. Otra estrategia es crear un rol de administrador poderoso único junto con un rol de usuario avanzado. El rol de usuario avanzado sería para los usuarios que tienen permiso para corregir partes de sus propios sistemas.

El modelo de superusuario y el modelo RBAC pueden coexistir. La siguiente tabla resume las gradaciones de superusuario a usuario común restringido que son posibles en el modelo RBAC. La tabla incluye las acciones administrativas que se pueden supervisar en ambos modelos. Para obtener un resumen del efecto de los privilegios solamente en un sistema, consulte la [Tabla 8-2](#).

TABLA 8-1 Modelo de superusuario en contraste con el modelo RBAC con privilegios

Capacidades de usuario en un sistema	Modelo de superusuario	Modelo RBAC
Puede convertirse en superusuario con capacidades completas de superusuario	Puede	Puede
Puede iniciar sesión como usuario con capacidades completas de usuario	Puede	Puede
Puede convertirse en superusuario con capacidades limitadas	No puede	Puede
Puede iniciar sesión como usuario y tener capacidades de superusuario, esporádicamente	Puede, sólo con los programas setuid	Puede, con los programas setuid y con RBAC
Puede iniciar sesión como usuario con capacidades administrativas, pero sin capacidades completas de superusuario	No puede	Puede, con RBAC y con los privilegios y autorizaciones asignados directamente
Puede iniciar sesión como un usuario con menos capacidades que un usuario común	No puede	Puede, con RBAC y con los privilegios eliminados

TABLA 8-1 Modelo de superusuario en contraste con el modelo RBAC con privilegios (Continuación)

Capacidades de usuario en un sistema	Modelo de superusuario	Modelo RBAC
Puede supervisar las acciones de superusuario	Puede, mediante la auditoría del comando su	Puede, mediante la auditoría de llamadas a pfexec () Además, el nombre del usuario que asumió el rol root está en la pista de auditoría

Elementos y conceptos básicos de RBAC

El modelo RBAC en Oracle Solaris introduce los siguientes elementos:

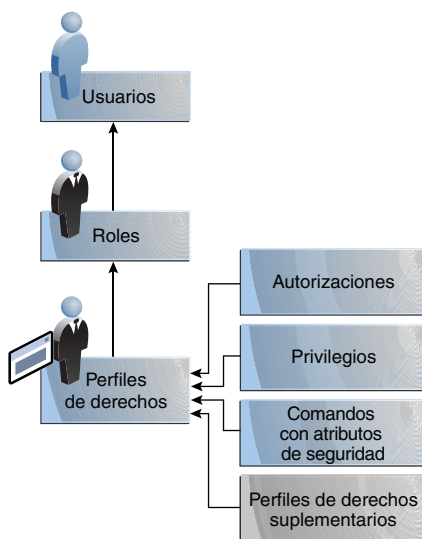
- **Autorización:** un permiso para que un usuario o un rol realice una clase de acciones que requieren derechos adicionales. Por ejemplo, la política de seguridad en la instalación otorga a los usuarios comunes la autorización `solaris.device.cdrw`. Esta autorización permite a los usuarios leer y escribir en un dispositivo de CD-ROM. Para obtener una lista de autorizaciones, consulte el archivo `/etc/security/auth_attr`.
- **Privilegio:** un derecho perfectamente definido que se puede otorgar a un comando, un usuario, un rol o un sistema. Los privilegios permiten que un proceso se realice correctamente. Por ejemplo, el privilegio `proc_exec` permite a un proceso llamar `execve()`. Los usuarios comunes tienen privilegios básicos. Para ver sus privilegios básicos, ejecute el comando `ppriv -vl basic`. Para obtener más opciones de comandos, consulte [“Comandos administrativos para la gestión de privilegios” en la página 215](#).
- **Atributos de seguridad:** un atributo que permite a un proceso efectuar una operación. En un entorno UNIX típico, un atributo de seguridad permite a un proceso efectuar una operación que, de lo contrario, está prohibida para los usuarios comunes. Por ejemplo, los programas `setuid` y `setgid` tienen atributos de seguridad. En el modelo RBAC, las autorizaciones y privilegios son atributos de seguridad además de los programas `setuid` y `setgid`. Estos atributos se pueden asignar a un usuario. Por ejemplo, un usuario con la autorización `solaris.device.allocate` puede asignar un dispositivo para uso exclusivo. Los privilegios se pueden colocar en un proceso. Por ejemplo, un proceso con el privilegio `file_flag_set` puede establecer atributos de archivos: inmutables, sin desvinculación o sólo anexo.
- **Aplicación con privilegios:** una aplicación o un comando que puede anular los controles del sistema mediante la comprobación de *atributos de seguridad*. En un entorno UNIX típico y en el modelo RBAC, los programas que usan `setuid` y `setgid` son aplicaciones con privilegios. En el modelo RBAC, los programas que necesitan privilegios o autorizaciones para ejecutarse correctamente también son aplicaciones con privilegios. Para obtener más información, consulte [“Aplicaciones con privilegios y RBAC” en la página 139](#).
- **Perfil de derechos:** una recopilación de atributos de seguridad que se pueden asignar a un rol o a un usuario. Un perfil de derechos puede incluir autorizaciones, privilegios asignados directamente, comandos con atributos de seguridad y otros perfiles de derechos. Los perfiles

que están dentro de otros perfiles se denominan perfiles de derechos suplementarios. Los perfiles de derechos ofrecen una forma práctica de agrupar los atributos de seguridad.

- **Rol:** una identidad especial para ejecutar aplicaciones con privilegios. Sólo los usuarios asignados pueden asumir la identidad especial. En un sistema ejecutado por roles, incluido el rol root, el superusuario es innecesario. Las capacidades de superusuario se distribuyen en roles diferentes. Por ejemplo, en un sistema de dos roles, las tareas de seguridad serían gestionadas por un rol de seguridad. El segundo rol se ocuparía de las tareas de administración del sistema que no están relacionadas con la seguridad. Los roles pueden ser más específicos. Por ejemplo, un sistema podría incluir roles administrativos independientes para gestionar la estructura criptográfica, las impresoras, la hora del sistema, los sistemas de archivos y la auditoría.

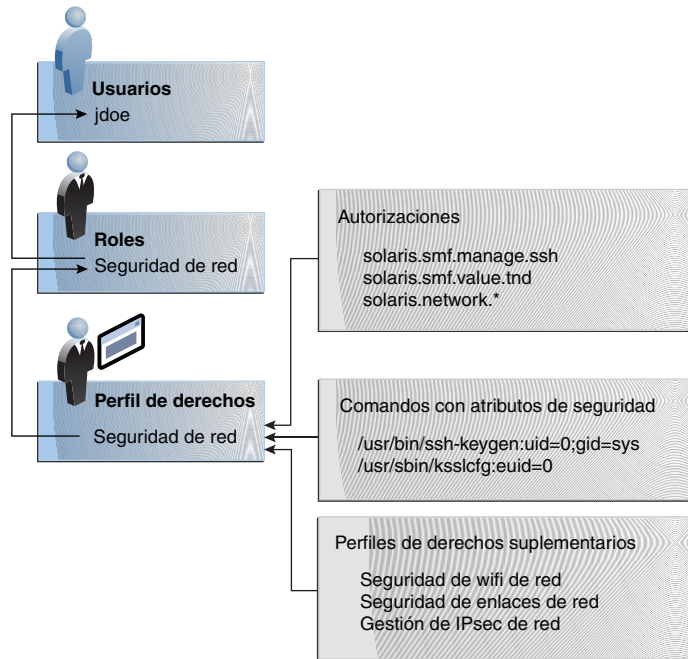
La siguiente figura muestra cómo trabajan juntos los elementos de RBAC.

FIGURA 8-2 Relaciones entre elementos de RBAC



La siguiente figura utiliza el rol de seguridad de la red y el perfil de derechos de seguridad de la red para demostrar las relaciones de RBAC.

FIGURA 8-3 Ejemplo de relaciones entre elementos de RBAC



El rol de seguridad de red se utiliza para gestionar IPsec, Wi-Fi y enlaces de red. El rol se asigna al usuario `jdoe`. `jdoe` puede asumir el rol si cambia a dicho rol y, a continuación, suministra la contraseña del rol. El administrador puede personalizar el rol para aceptar la contraseña de usuario en lugar de la contraseña del rol.

En la [Figura 8-3](#), el perfil de derechos de seguridad de la red se asigna al rol de seguridad de red. El perfil de derechos de seguridad de la red contiene perfiles complementarios que se evalúan en orden: seguridad de wifi de red, seguridad de enlaces de red y gestión de IPsec de red. Estos perfiles complementarios desempeñan las principales tareas del rol.

El perfil de derechos de seguridad de la red tiene tres autorizaciones asignadas directamente, ningún privilegio asignado directamente y dos comandos con atributos de seguridad. Los perfiles de derechos complementarios tienen autorizaciones asignadas directamente y dos de ellas tienen comandos con atributos de seguridad. En el rol de seguridad de la red, `jdoe` tiene todas las autorizaciones asignadas en estos perfiles y puede ejecutar todos los comandos con atributos de seguridad en estos perfiles. `jdoe` puede administrar la seguridad de la red.

Escalada de privilegios

Oracle Solaris proporciona a los administradores mucha flexibilidad al configurar la seguridad. Tal como está instalado, el software no permite la [escalada de privilegios](#). La escalada de

privilegios se produce cuando un usuario o un proceso obtienen más derechos administrativos de los que inicialmente se les iban a otorgar. En este sentido, un privilegio comprende cualquier atributo de seguridad, no sólo privilegios.

El software Oracle Solaris incluye atributos de seguridad que están asignados al rol `root` únicamente. Con otras protecciones de seguridad implementadas, es posible que un administrador asigne atributos que están diseñados para el rol `root` a otras cuentas, pero dicha asignación se debe realizar con cuidado.

El siguiente perfil de derechos y conjunto de autorizaciones pueden ampliar los privilegios de una cuenta no raíz.

- **Perfil de derechos de restauración de medios:** este perfil existe pero no es parte de ningún otro perfil de derechos. Debido a que la restauración de medios proporciona acceso a todo el sistema de archivos raíz, su uso constituye una posible escalada de privilegios. Se podrían restaurar medios alternativos o archivos modificados deliberadamente. De manera predeterminada, el rol `root` incluye este perfil de derechos.
- **Autorizaciones `solaris.*.assign`:** estas autorizaciones existen pero no están asignadas a ninguna cuenta o perfil de derechos. Una cuenta con una autorización `solaris.*.assign` puede asignar atributos de seguridad a otros que la cuenta en sí misma no tiene asignados. Por ejemplo, un rol con la autorización `solaris.profile.assign` puede asignar perfiles de derechos a otras cuentas que el rol en sí mismo no tiene asignados. De manera predeterminada, sólo el rol `root` tiene autorizaciones `solaris.*.assign`.

Es recomendable asignar autorizaciones `solaris.*.delegate`, no autorizaciones `solaris.*.assign`. Una autorización `solaris.*.delegate` permite al delegador asignar a otras cuentas sólo los atributos de seguridad que el delegador posee. Por ejemplo, un rol al que se le asigna la autorización `solaris.profile.delegate` puede asignar perfiles de derechos que el rol en sí mismo tiene asignado para otros usuarios y roles.

Para conocer las escaladas que afectan el atributo de seguridad del privilegio, consulte [“Cómo evitar la escalada de privilegios” en la página 217](#).

Autorizaciones RBAC

Una *autorización* es un derecho perfectamente definido que se puede otorgar a un rol o a un usuario. Las autorizaciones aplican políticas en el nivel de aplicación del usuario.

Aunque las autorizaciones pueden asignarse directamente a un rol o a un usuario, se recomienda incluirlas en un perfil de derechos. El perfil de derechos luego se agrega a un rol, y el rol se asigna a un usuario. Para ver un ejemplo, consulte la [Figura 8-3](#).

Las autorizaciones que incluyen las palabras `delegate` o `assign` permiten al usuario o rol asignar atributos de seguridad a otros.

Para evitar la escalada de privilegios, no asigne a una cuenta una autorización `assign`.

- Una autorización `delegate` permite al delegador asignar a otros sólo los atributos de seguridad que el delegador posee. Por ejemplo, un rol al que se le asigna la autorización `solaris.profile.delegate` puede asignar a otros perfiles de derechos que el rol en sí mismo tiene asignado.
- Una autorización `assign` permite al asignador otorgar a otros atributos de seguridad que la cuenta no posee. Por ejemplo, un rol con la autorización `solaris.profile.assign` pueden asignar a otros cualquier perfil de derechos.

Las autorizaciones `solaris.*.assign` se entregan, pero no se incluyen en ningún perfil. De manera predeterminada, sólo el rol `root` tiene autorizaciones `solaris.*.assign`.

Las aplicaciones compatibles con RBAC pueden comprobar las autorizaciones de un usuario antes de otorgar acceso a la aplicación o a operaciones específicas dentro de la aplicación. Esta comprobación reemplaza la verificación en las aplicaciones UNIX convencionales para `UID=0`. Para obtener más información sobre las autorizaciones, consulte las siguientes secciones:

- “Autorizaciones” en la página 208
- “Base de datos `auth_attr`” en la página 211
- “Comandos seleccionados que requieren autorizaciones” en la página 214

Autorizaciones y privilegios

Los privilegios aplican la política de seguridad en el núcleo. La diferencia entre las autorizaciones y los privilegios reside en el nivel en el que se aplica la política de seguridad. Sin el privilegio adecuado, el núcleo puede evitar que un proceso realice operaciones con privilegios. Sin las autorizaciones adecuadas, es posible que se le impida a un usuario utilizar una aplicación con privilegios o realizar operaciones que conllevan riesgos de seguridad dentro de una aplicación con privilegios. Para ver una explicación más detallada de los privilegios, consulte “Privilegios (descripción general)” en la página 144.

Aplicaciones con privilegios y RBAC

Las aplicaciones y los comandos que pueden anular los controles del sistema se consideran aplicaciones con privilegios. Los atributos de seguridad, como `UID=0`, los privilegios y las autorizaciones hacen que una aplicación sea una aplicación con privilegios.

Aplicaciones que comprueban UID y GID

Las aplicaciones con privilegios que comprueban la existencia de `root` (`UID=0`) o algún otro UID o GID especial han estado presentes en el entorno UNIX desde hace tiempo. El mecanismo de perfiles de derechos permite aislar comandos que requieren un ID específico. En lugar de cambiar el ID de un comando al que cualquiera puede acceder, puede colocar el comando con

atributos de seguridad asignados a un perfil de derechos. Un usuario o un rol con ese perfil de derechos luego pueden ejecutar el programa sin tener que convertirse en superusuario.

Los ID se pueden especificar como reales o efectivos. Se prefiere la asignación de ID efectivos en lugar de la asignación de ID reales. Los ID efectivos son equivalentes a la función `setuid` en los bits de permisos de archivo. Los ID efectivos también identifican el UID para auditoría. Sin embargo, dado que algunos programas y secuencias de comandos de shell requieren un UID real de root, también es posible definir UID reales. Por ejemplo, el comando `reboot` requiere un UID real en lugar de uno efectivo. Si un ID efectivo no es suficiente para ejecutar un comando, debe asignar el ID real al comando.

Aplicaciones que comprueban privilegios

Las aplicaciones con privilegios pueden comprobar el uso de privilegios. El mecanismo de perfiles de derechos de RBAC permite especificar los privilegios para comandos específicos que requieren atributos de seguridad. A continuación, puede aislar el comando con los atributos de seguridad asignados a un perfil de derechos. Un usuario o un rol con ese perfil de derechos luego pueden ejecutar el comando sólo con los privilegios que el comando necesita para una ejecución correcta.

Entre los comandos que comprueban la existencia de privilegios, se incluyen los siguientes:

- Comandos de Kerberos, como `kadmin`, `kprop` y `kdb5_util`.
- Comandos de redes, como `ipadm`, `routeadm` y `snoop`.
- Comandos de archivos y sistemas de archivos, como `chmod`, `chgrp` y `mount`.
- Comandos que controlan procesos, como `kill`, `pcrd` y `rcapadm`.

Para agregar comandos con privilegios a un perfil de derechos, consulte [“Cómo crear un perfil de derechos” en la página 175](#) y la página del comando `man profiles(1)`. Para determinar los comandos que comprueban privilegios en un perfil específico, consulte [“Cómo visualizar todos los atributos de seguridad definidos” en la página 157](#).

Aplicaciones que comprueban autorizaciones

Oracle Solaris proporciona además comandos que comprueban autorizaciones. Por definición, el usuario `root` tiene todas las autorizaciones. Por lo tanto, el usuario `root` puede ejecutar cualquier aplicación. Entre las aplicaciones que comprueban la existencia de autorizaciones, se incluyen las siguientes:

- Comandos de administración de auditoría, como `auditconfig` y `auditreduce`.
- Comandos de administración de impresoras, como `lpadmin` y `lpfilter`.
- Comandos relacionados con trabajos por lotes, como `at`, `atq`, `batch` y `crontab`.
- Comandos orientados a dispositivos, como `allocate`, `deallocate`, `list_devices` y `cdrw`.

Para probar las autorizaciones de una secuencia de comandos o un programa, consulte el [Ejemplo 9–23](#). Para escribir un programa que requiere autorizaciones, consulte [“About Authorizations” de Developer’s Guide to Oracle Solaris 11 Security](#).

Perfiles de derechos de RBAC

Un *perfil de derechos* es una recopilación de atributos de seguridad que se pueden asignar a un rol o a un usuario para realizar tareas que requieren derechos administrativos. Un perfil de derechos puede incluir autorizaciones, privilegios, comandos con atributos de seguridad asignados y otros perfiles de derechos. Los privilegios que se asignan en un perfil de derechos están vigentes para todos los comandos. Los perfiles de derechos también contienen entradas para reducir o extender el conjunto heredable inicial, y para reducir el conjunto de privilegios límite.

Para obtener más información sobre los perfiles de derechos, consulte las siguientes secciones:

- [“Perfiles de derechos” en la página 205](#)
- [“Base de datos prof_attr” en la página 211](#)
- [“Base de datos exec_attr” en la página 212](#)

Roles de RBAC

Un *rol* es un tipo especial de cuenta de usuario desde la que puede ejecutar aplicaciones con privilegios. Los roles se crean del mismo modo general que las cuentas de usuario. Los roles tienen un directorio principal, una asignación de grupo, una contraseña, etc. Los perfiles de derechos y las autorizaciones otorgan al rol capacidades administrativas. Los roles no pueden heredar capacidades de otros roles u otros usuarios. Los roles discretos dividen las capacidades de superusuario y, por lo tanto, permiten prácticas administrativas más seguras.

Cuando un usuario asume un rol, los atributos del rol reemplazan todos los atributos de usuario. La información del rol se almacena en las bases de datos `passwd`, `shadow` y `user_attr`. Las acciones de los roles se pueden auditar. Para obtener información detallada acerca de cómo configurar roles, consulte las siguientes secciones:

- [“Cómo planificar la implementación de RBAC” en la página 169](#)
- [“Cómo crear un rol” en la página 171](#)
- [“Cómo cambiar los atributos de seguridad de un rol” en la página 188](#)

Un rol se puede asignar a más de un usuario. Todos los usuarios que pueden asumir el mismo rol tienen el mismo directorio principal, trabajan en el mismo entorno y tienen acceso a los mismos archivos. Los usuarios pueden asumir roles de la línea de comandos. Para ello, deben ejecutar el comando `su` y proporcionar el nombre del rol y una contraseña. De manera predeterminada, los usuarios autentican un rol proporcionando la contraseña del *rol*. El administrador puede configurar el sistema para activar a un usuario para que realice la autenticación proporcionando la contraseña del *usuario*. Para conocer el procedimiento, consulte [“Cómo permitir que un usuario use su propia contraseña para asumir un rol” en la página 191](#).

Un rol no puede iniciar sesión directamente. Un usuario inicia sesión y, a continuación, asume un rol. Tras asumir un rol, el usuario no puede asumir otro rol sin salir primero de su rol actual. Tras salir del rol, el usuario puede asumir otro rol.

El hecho de que root es un rol en Oracle Solaris evita inicios de sesión root anónimos. Si se audita el comando de shell de perfil, `pfexec`, la pista de auditoría contiene el UID real del usuario que inició sesión, los roles que el usuario asumió y las acciones que el rol realizó. Para auditar operaciones de roles en el sistema o un usuario concreto, consulte [“Cómo auditar roles” en la página 174](#).

Los perfiles de derechos que se envían con el software están diseñados para asignarlos a roles. Por ejemplo, el perfil de derechos de administrador del sistema se puede utilizar para crear el rol de administrador del sistema. Para configurar un rol, consulte [“Cómo crear un rol” en la página 171](#).

Shells de perfil y RBAC

Los usuarios y roles pueden ejecutar aplicaciones con privilegios de un [shell de perfil](#). Un *shell de perfil* es un shell especial que reconoce los atributos de seguridad que se incluyen en un perfil de derechos. Los administradores pueden asignar un shell de perfil a un usuario específico como un shell de inicio, o el shell de perfil se inicia cuando ese usuario ejecuta el comando `su` para asumir un rol. En Oracle Solaris cada shell tiene un equivalente de shell de perfil. Por ejemplo, los equivalentes de shell de perfil para el shell Bourne (`sh`), el shell Bash (`bash`) y el shell Kornl (`ksh`) son los shells `pfsh`, `pfbash` y `pfksh` respectivamente. Para obtener una lista de shells de perfil, consulte la página del comando `man pfexec(1)`.

Los usuarios a los que se les ha asignado directamente un perfil de derechos y cuyo shell de inicio de sesión no es un shell de perfil deben invocar un shell de perfil para ejecutar los comandos con atributos de seguridad. Para conocer las consideraciones de seguridad y facilidad de uso, consulte [“Consideraciones de seguridad al asignar directamente atributos de seguridad” en la página 143](#).

Todos los comandos que se ejecutan en un shell de perfil pueden auditarse. Para obtener más información, consulte [“Cómo auditar roles” en la página 174](#).

Ámbito de servicio de nombres y RBAC

El ámbito de servicio de nombres es un concepto importante para comprender RBAC. El ámbito de un rol puede estar limitado a un host individual. El ámbito también puede incluir todos los hosts gestionados por un servicio de nombres, como LDAP. El ámbito de servicio de nombres para un sistema se especifica en el servicio de cambio de nombres, `svc:/system/name-service/switch`. Las consultas se detienen en la primera coincidencia. Por ejemplo, si un perfil de derechos existe en dos ámbitos de servicio de nombres, sólo se utilizan las entradas del primer ámbito de servicio de nombres. Si `files` es la primera coincidencia, el ámbito del rol se limita al host local.

Consideraciones de seguridad al asignar directamente atributos de seguridad

Por lo general, un usuario obtiene capacidades administrativas a través de un rol. Las autorizaciones, privilegios y los comandos con privilegios se agrupan en un perfil de derechos. El perfil de derechos se incluye en un rol, y el rol se asigna a un usuario.

La asignación directa de perfiles de derechos y atributos de seguridad también es posible:

- Se pueden asignar directamente perfiles de derechos, privilegios y autorizaciones a usuarios.
- Se pueden asignar directamente privilegios y autorizaciones a usuarios y roles.

Sin embargo, la asignación directa de privilegios no es una práctica segura. Los usuarios y los roles con un privilegio asignado directamente pueden anular la política de seguridad cada vez que el núcleo necesite este privilegio. Una práctica más segura es asignar el privilegio como atributo de seguridad de un comando en un perfil de derechos. Luego, ese privilegio sólo estará disponible para ese comando y un usuario que tenga ese perfil de derechos.

Dado que las autorizaciones funcionan en el nivel de usuario, la asignación directa de autorizaciones puede resultar menos riesgosa que la asignación directa de privilegios. Sin embargo, las autorizaciones pueden permitir a un usuario realizar tareas de seguridad elevada, por ejemplo, asignar indicadores de auditoría.

Consideraciones de uso al asignar directamente atributos de seguridad

La asignación directa de perfiles de derechos y atributos de seguridad puede afectar el uso:

- Los privilegios y las autorizaciones asignados directamente, y los comandos y las autorizaciones en un perfil de derechos asignados directamente deben ser interpretados por un shell de perfil para ser efectivos. De manera predeterminada, no se asigna a los usuarios un shell de perfil.

El usuario no se debe olvidar de abrir un shell de perfil y de ejecutar los comandos de ese shell.

- La asignación individual de autorizaciones no es ampliable. Y las autorizaciones asignadas directamente podrían no ser suficientes para realizar una tarea. Es posible que la tarea pueda requerir comandos con privilegios.

Los perfiles de derechos están diseñados para agrupar autorizaciones y comandos con privilegios. También son ampliables.

Privilegios (descripción general)

La gestión de derechos de procesos permite restringir procesos en el nivel de comando, usuario, rol o sistema. Oracle Solaris implementa la gestión de derechos de procesos a través de *privilegios*. Los privilegios disminuyen el riesgo de seguridad asociado a un usuario o un proceso que tiene capacidades completas de superusuario en un sistema. Los privilegios y RBAC ofrecen un modelo alternativo eficaz al modelo de superusuario tradicional.

- Para obtener más información sobre RBAC, consulte [“Control de acceso basado en roles \(descripción general\)” en la página 131](#).
- Para obtener información sobre cómo administrar privilegios, consulte [“Uso de privilegios \(tareas\)” en la página 194](#).
- Para obtener información de referencia sobre los privilegios, consulte [“Con privilegios” en la página 215](#).

Privilegios con protección de procesos del núcleo

Un privilegio es un derecho perfectamente definido que un proceso requiere para realizar una operación. El derecho se aplica en el núcleo. Un programa que funciona dentro de los límites del *conjunto básico* de privilegios funciona dentro de los límites de la política de seguridad del sistema. Los programas *setuid* son ejemplos de programas que funcionan fuera de los límites de la política de seguridad del sistema. Mediante el uso de privilegios, los programas eliminan la necesidad de realizar llamadas a *setuid*.

Los privilegios enumeran de forma discreta los tipos de operaciones que son posibles en un sistema. Los programas se pueden ejecutar con los privilegios exactos que permiten que el programa funcione correctamente. Por ejemplo, un programa que manipula los archivos puede necesitar los privilegios `file_dac_write` y `file_flag_set`. Estos privilegios en el proceso eliminan la necesidad de ejecutar el programa como `root`.

Históricamente, los sistemas no adoptaron el modelo de privilegios. En su lugar, los sistemas utilizaron el modelo de superusuario. En el modelo de superusuario, los procesos se ejecutan como `root` o como usuario. Los procesos de usuario se limitaban a trabajar en los directorios y los archivos del usuario. Los procesos `root` podían crear directorios y archivos en cualquier parte del sistema. Un proceso que requería la creación de un directorio fuera del directorio del usuario se ejecutaba con un `UID=0`, es decir, como `root`. La política de seguridad dependía del control de acceso discrecional (DAC, Discretionary Access Control) para proteger los archivos del sistema. Los nodos del dispositivo estaban protegidos por DAC. Por ejemplo, sólo los miembros del grupo `sys` podían abrir los dispositivos que pertenecían al grupo `sys`.

Sin embargo, los programas *setuid*, los permisos de archivo y las cuentas administrativas son vulnerables al uso indebido. Las acciones que un proceso *setuid* puede realizar son más numerosas que las acciones que requiere para completar su operación. Un programa *setuid*

puede verse comprometido por un intruso que luego se ejecuta como usuario `root` omnipotente. De modo similar, cualquier usuario con acceso a la contraseña `root` puede poner en peligro todo el sistema.

En cambio, un sistema que aplica la política con privilegios permite una gradación entre las capacidades de usuario y las capacidades de `root`. Es posible otorgar a un usuario privilegios para realizar actividades que van más allá de las capacidades de los usuarios comunes, y `root` puede limitarse a menos privilegios que los que `root` posee actualmente. Con RBAC, un comando que se ejecuta con privilegios se puede aislar en un perfil de derechos y asignar a un usuario o rol. La [Tabla 8–1](#) resume la gradación entre las capacidades de usuario y las capacidades de `root` que proporciona el modelo RBAC con privilegios.

El modelo de privilegios proporciona mayor seguridad que el modelo de superusuario. Los privilegios que se eliminaron de un proceso no se pueden utilizar. Los privilegios de proceso impiden que un programa o una cuenta administrativa obtengan acceso a todas las capacidades. Los privilegios de proceso pueden proporcionar una protección adicional para los archivos confidenciales, en donde las protecciones de DAC solamente pueden utilizarse para obtener acceso.

Los privilegios pueden restringir programas y procesos a las capacidades que el programa necesita únicamente. Esta capacidad se denomina *principio de privilegio mínimo*. En un sistema que implementa este principio, un intruso que captura un proceso puede acceder sólo a aquellos privilegios que tiene el proceso. El resto del sistema no corre peligro.

Descripciones de privilegios

Los privilegios se agrupan de manera lógica de acuerdo con el área del privilegio.

- **Privilegios FILE:** los privilegios que comienzan con la cadena `file` funcionan en los objetos del sistema de archivos. Por ejemplo, el privilegio `file_dac_write` anula el control de acceso discrecional al escribir en los archivos.
- **Privilegios IPC:** los privilegios que comienzan con la cadena `ipc` anulan los controles de acceso a objetos IPC. Por ejemplo, el privilegio `ipc_dac_read` permite a un proceso leer memoria compartida remota que está protegida por DAC.
- **Privilegios NET:** los privilegios que comienzan con la cadena `net` otorgan acceso a funcionalidades de red específicas. Por ejemplo, el privilegio `net_rawaccess` permite a un dispositivo conectarse con la red.
- **Privilegios PROC:** los privilegios que comienzan con la cadena `proc` permiten a los procesos modificar propiedades restringidas del propio proceso. Los privilegios PROC incluyen privilegios que tienen un efecto muy limitado. Por ejemplo, el privilegio `proc_clock_highres` permite a un proceso usar temporizadores de alta resolución.
- **Privilegios SYS:** los privilegios que comienzan con la cadena `sys` otorgan a los procesos acceso sin restricciones a distintas propiedades del sistema. Por ejemplo, el privilegio `sys_linkdir` permite a un proceso establecer y anular enlaces físicos a directorios.

Otros grupos lógicos incluyen CONTRACT, CPC, DTRACE, GRAPHICS, VIRT y WIN.

Algunos privilegios tienen un efecto limitado en el sistema y otros tienen un efecto amplio. La definición del privilegio `proc_taskid` indica su efecto limitado:

```
proc_taskid
    Allows a process to assign a new task ID to the calling process.
```

La definición del privilegio `net_rawaccess` indica su efecto amplio:

```
net_rawaccess
    Allow a process to have direct access to the network layer.
```

La página del comando `man privileges(5)` proporciona descripciones de cada privilegio. El comando `ppriv -lv` imprime una descripción de cada privilegio con formato estándar.

Diferencias administrativas en un sistema con privilegios

Un sistema tiene privilegios posee varias diferencias visibles con un sistema que no tiene privilegios. La siguiente tabla muestra algunas de las diferencias.

TABLA 8-2 Diferencias visibles entre un sistema con privilegios y un sistema sin privilegios

Función	Sin privilegios	Con privilegios
Daemons	Los daemons se ejecutan como root.	Los daemons se ejecutan como el daemon de usuario. Por ejemplo, estos daemons tienen asignados los privilegios adecuados y se ejecutan como daemon: <code>lockd</code> y <code>rpcbind</code> .
Propiedad de archivos de registro	Los archivos de registro son propiedad de root.	Los archivos de registro ahora son propiedad de daemon, que creó el archivo de registro. El usuario root no es propietario del archivo.
Mensajes de error	Los mensajes de error hacen referencia al superusuario. Por ejemplo, <code>chroot: not superuser</code> .	Los mensajes de error reflejan el uso de privilegios. Por ejemplo, el mensaje de error equivalente para el error <code>chroot</code> es <code>chroot: exec failed</code> .
Programas <code>setuid</code>	Los programas usan <code>setuid</code> para completar las tareas que los usuarios comunes no tienen permiso para realizar.	Muchos programas <code>setuid</code> se modificaron para ejecutarse con privilegios. Por ejemplo, los siguientes comandos usan privilegios: <code>audit</code> , <code>ikeadm</code> , <code>ipadm</code> , <code>ipseconf</code> , <code>ping</code> , <code>traceroute</code> y <code>newtask</code> .

TABLA 8-2 Diferencias visibles entre un sistema con privilegios y un sistema sin privilegios (Continuación)

Función	Sin privilegios	Con privilegios
Permisos de archivo	Los permisos de dispositivo están controlados por DAC. Por ejemplo, los miembros del grupo sys pueden abrir /dev/ip.	Los permisos de archivo (DAC) no predicen quién puede abrir un dispositivo. Los dispositivos están protegidos con DAC y la política de dispositivos. Por ejemplo, el archivo /dev/ip tiene 666 permisos, pero únicamente un proceso con los privilegios adecuados puede abrir el dispositivo. Los sockets sin formato siguen protegidos por DAC.
Eventos de auditoría	La auditoría del uso del comando su comprende varias funciones administrativas.	La auditoría del uso de privilegios comprende la mayoría de las funciones administrativas. Las clases de auditoría pm, ps, ex, ua y as incluyen eventos de auditoría que supervisan la política de dispositivos y el uso de privilegios.
Procesos	Los procesos están protegidos por el propietario del proceso.	Los procesos están protegidos por privilegios. Los privilegios de proceso y los indicadores de proceso están visibles como una nueva entrada en el directorio /proc/<pid>, priv.
Depuración	Ninguna referencia a privilegios en los volcados del núcleo central.	La sección de notas ELF de los volcados del núcleo central incluye información sobre los indicadores y privilegios de proceso en las notas NT_PRPRIV y NT_PRPRIVINFO. El comando ppriv y otros comandos muestran el número adecuado de conjuntos con tamaño apropiado. Los comandos asignan correctamente los bits de los conjuntos de bits a los nombres de privilegio.

Privilegios y recursos del sistema

En Oracle Solaris, los controles de recursos `project.max-locked-memory` y `zone.max-locked-memory` se pueden utilizar para limitar el consumo de memoria de los procesos que tienen asignado el privilegio `PRIV_PROC_LOCK_MEMORY`. Este privilegio permite a un proceso bloquear páginas en la memoria física.

Si asigna el privilegio `PRIV_PROC_LOCK_MEMORY` a un perfil de derechos, puede otorgar a los procesos que tienen este privilegio la posibilidad de bloquear toda la memoria. Como protección, defina un control de recursos para evitar que el usuario del privilegio bloquee toda la memoria. Para los procesos con privilegios que se ejecutan en una zona no global, defina el control de recursos `zone.max-locked-memory`. Para los procesos con privilegios que se ejecutan en un sistema, cree un proyecto y defina el control de recursos `project.max-locked-memory`. Para obtener información sobre estos controles de recursos, consulte el [Capítulo 6, “Controles de recursos \(descripción general\)” de Administración de Oracle Solaris 11.1: zonas de Oracle Solaris, zonas de Oracle Solaris 10 y gestión de recursos](#) y el [Capítulo 16, “Configuración de zonas no globales \(descripción general\)” de Administración de Oracle Solaris 11.1: zonas de Oracle Solaris, zonas de Oracle Solaris 10 y gestión de recursos](#).

Cómo se implementan los privilegios

Cada proceso tiene cuatro conjuntos de privilegios que determinan si un proceso puede usar un determinado privilegio. El núcleo calcula automáticamente el *conjunto vigente* de privilegios. Puede modificar el *conjunto heredable* inicial de privilegios. Un programa que está codificado para utilizar privilegios puede reducir el *conjunto permitido* de privilegios del programa. Puede reducir el *conjunto límite* de privilegios.

- **Conjunto vigente de privilegios o E (effective):** es el conjunto de privilegios que actualmente está en vigor. Un proceso puede agregar los privilegios que están en el conjunto permitido al conjunto vigente. Un proceso también puede eliminar privilegios de E.
- **Conjunto permitido de privilegios o P (permitted):** es el conjunto de privilegios que está disponible para su uso. Los privilegios pueden estar disponibles para un programa a través de herencia o mediante asignación. Un perfil de ejecución es una forma de asignar privilegios a un programa. El comando `setuid` asigna todos los privilegios que tiene `root` a un programa. Se pueden eliminar privilegios del conjunto permitido, pero no se pueden agregar privilegios al conjunto. Los privilegios que se quitan de P se eliminan automáticamente de E.

Un programa *para privilegios* elimina los privilegios que un programa nunca utiliza de su conjunto permitido. De esta forma, el programa ni ningún proceso malicioso pueden utilizar privilegios innecesarios. Para obtener más información sobre los programas para privilegios, consulte el [Capítulo 2, “Developing Privileged Applications” de *Developer’s Guide to Oracle Solaris 11 Security*](#).

- **Conjunto heredable de privilegios o I (inheritable):** es el conjunto de privilegios que un proceso puede heredar a través de una llamada a `exec`. Después de la llamada a `exec`, los privilegios heredados se colocan en los conjuntos permitido y vigente, por los que estos conjuntos son iguales, excepto en el caso especial de un programa `setuid`.

En un programa `setuid`, después de la llamada a `exec`, el conjunto heredable se ve restringido primero por el conjunto límite. Luego, el conjunto de privilegios que se heredaron (I), menos los privilegios que estaban en el conjunto límite (L), se asignan a P y E para ese proceso.

- **Conjunto límite de privilegios o L (limit):** es el límite externo de los privilegios que están disponibles para un proceso y sus procesos secundarios. De manera predeterminada, el conjunto límite incluye todos los privilegios. Los procesos pueden reducir el conjunto límite, pero nunca pueden ampliarlo. L se utiliza para restringir I. Por lo tanto, L restringe P y E al tiempo de `exec`.

Si se asignó a un usuario un perfil que incluye un programa con privilegios asignados, el usuario normalmente puede ejecutar ese programa. En un sistema sin modificaciones, los privilegios asignados del programa están dentro del conjunto límite del usuario. Los privilegios que se asignaron al programa pasan a formar parte del conjunto permitido del usuario. Para ejecutar el programa con privilegios asignados, el usuario debe ejecutar el programa desde un shell de perfil.

El núcleo reconoce un *conjunto básico de privilegios*. En un sistema sin modificaciones, cada conjunto heredable inicial del usuario es equivalente al conjunto básico en el inicio de sesión. Aunque no puede modificar el conjunto básico, puede modificar los privilegios que un usuario hereda del conjunto básico.

En un sistema sin modificaciones, los conjuntos de privilegios de un usuario en el inicio de sesión tendrían un aspecto similar al siguiente:

```
E (Effective): basic
I (Inheritable): basic
P (Permitted): basic
L (Limit): all
```

Por lo tanto, en el inicio de sesión, todos los usuarios tienen el conjunto básico en su conjunto heredable, su conjunto permitido y su conjunto vigente. El conjunto límite del usuario es equivalente al conjunto límite predeterminado para la zona global o no global. Para poner más privilegios en el conjunto vigente del usuario, debe asignar un perfil de derechos al usuario. El perfil de derechos incluiría los comandos en los que agregó privilegios. También puede asignar privilegios directamente al usuario o el rol, aunque dicha asignación de privilegios puede ser riesgosa. Para ver una explicación de los riesgos, consulte [“Consideraciones de seguridad al asignar directamente atributos de seguridad” en la página 143](#).

Cómo obtienen privilegios los procesos

Los procesos pueden heredar privilegios. O bien se pueden asignar privilegios a los procesos. Un proceso hereda privilegios de su proceso principal. En el inicio de sesión, el conjunto heredable inicial de privilegios del usuario determina los privilegios que están disponibles para los procesos del usuario. Todos los procesos secundarios del inicio de sesión inicial del usuario heredan ese conjunto.

También puede asignar directamente privilegios a programas, usuarios y roles. Cuando un programa requiere privilegios, puede asignar los privilegios al archivo ejecutable del programa en un perfil de derechos. A los usuarios o roles que tienen permiso para ejecutar el programa se les asigna el perfil que incluye el programa. En el inicio de sesión o cuando se indica un shell de perfil, el programa se ejecuta con privilegios al escribir el archivo ejecutable del programa en el shell de perfil. Por ejemplo, un rol que incluye el perfil de gestión del acceso a objetos puede ejecutar el comando `chmod` con el privilegio `file_chown`.

Cuando un rol o un usuario ejecutan un programa al que se asignó directamente un privilegio adicional, el privilegio asignado se agrega al conjunto heredable del rol o el usuario. Los procesos secundarios del programa al que se asignaron privilegios heredan los privilegios del proceso principal. Si el proceso secundario requiere más privilegios que el proceso principal, esos privilegios se deben asignar directamente al proceso secundario.

Los programas que están codificados para utilizar privilegios se denominan programas de [reconocimiento de privilegios](#). Un programa *para privilegios* activa el uso de privilegios y

desactiva el uso de privilegios durante la ejecución del programa. Para lograr un funcionamiento correcto en un entorno de producción, se deben asignar al programa los privilegios que el programa activa y desactiva.

Para ver ejemplos de código para privilegios, consulte el [Capítulo 2, “Developing Privileged Applications”](#) de *Developer’s Guide to Oracle Solaris 11 Security*. Para asignar privilegios a un programa que los requiera, consulte el [Ejemplo 9–18](#).

Asignación de privilegios

Como administrador de la seguridad, usted es responsable de asignar privilegios. Se recomienda asignar el privilegio a un comando en un perfil de derechos. El perfil de derechos luego se asigna a un rol o un usuario.

Los privilegios se pueden asignar directamente a un usuario, a un rol o a un perfil de derechos. Si confía en que un subconjunto de usuarios puede utilizar un privilegio de forma responsable a lo largo de sus sesiones, puede asignar el privilegio directamente. Los privilegios que tienen un efecto limitado, como `proc_clock_highres`, son buenos candidatos para la asignación directa. Los privilegios que tienen efectos de largo alcance, como `file_dac_write`, son malos candidatos para la asignación directa.

También es posible denegar privilegios a un usuario o un sistema. Se debe tener cuidado al eliminar privilegios del conjunto heredable inicial o el conjunto límite de un usuario o un sistema.

Ampliación de los privilegios de un usuario o rol

Los usuarios y roles tienen un conjunto heredable de privilegios. El conjunto límite no se puede ampliar, ya que incluye inicialmente todos los privilegios. El conjunto heredable inicial se puede ampliar para usuarios, roles y sistemas. Un privilegio que no está en el conjunto heredable también se puede asignar a un proceso.

Puede expandir los privilegios disponibles de tres formas.

- El conjunto heredable inicial se puede ampliar para usuarios, roles y sistemas.
- Un privilegio que no está en el conjunto heredable se puede asignar explícitamente a un proceso.
- Un privilegio que no se encuentra en el conjunto heredable se puede asignar explícitamente a un puerto de la red, UID u objeto de archivo. Este uso de privilegio se denomina *política extendida*.

La asignación de privilegios por proceso es la manera más precisa de agregar privilegios. Para ampliar la cantidad de operaciones con privilegios que puede realizar un usuario, debe asignar un rol al usuario. Se asignarán perfiles de derechos al rol que incluyen comandos con privilegios

agregados. Cuando el usuario asume el rol, obtiene el shell de perfil del rol. Cuando los comandos del perfil de derechos se escriben en el shell del rol, los comandos se ejecutan con los privilegios agregados.

También puede asignar un perfil de derechos al usuario en lugar de un rol que el usuario asumirá. Cuando el usuario abre un shell de perfil, como `pfksh`, el usuario puede ejecutar los comandos del perfil de derechos con privilegios del usuario. En un shell común, los comandos no se ejecutan con privilegios. El proceso con privilegios sólo se puede ejecutar en un shell con privilegios.

Ampliar el conjunto heredable inicial de privilegios para usuarios, roles o sistemas es una manera más riesgosa de asignar privilegios. Todos los privilegios del conjunto heredable están en el conjunto permitido y vigente. Todos los comandos que el usuario o el rol escriben en un shell puede utilizar los privilegios asignados directamente. Los privilegios asignados directamente permiten a un usuario o rol realizar fácilmente operaciones que pueden estar fuera de los límites de sus responsabilidades administrativas.

Para reducir ese riesgo, puede asignar privilegios a usuarios o roles para que puedan trabajar en un objeto a la vez. Los objetos posibles son los puertos de red, los UID y los objetos de archivo. Por ejemplo, puede asignarle a un usuario el privilegio `file_dac_read` para archivos en el directorio `/var/core`. El privilegio `file_dac_read` debe estar en el conjunto vigente del proceso del usuario cuando se aplique esta política extendida. Si es así, el usuario puede leer todos los archivos en el directorio `/var/core` cuando se asigna la política extendida a este usuario para este objeto de directorio.

Al aumentar el conjunto heredable inicial de privilegios en un sistema, todos los usuarios que inician sesión en el sistema tienen un conjunto más grande de privilegios básicos. Esa asignación directa permite a todos los usuarios del sistema realizar fácilmente operaciones que probablemente están fuera de los límites de los usuarios comunes.

Nota – El conjunto límite no se puede ampliar, ya que incluye inicialmente todos los privilegios.

Restricción de los privilegios de un usuario o rol

Al eliminar privilegios, puede impedir que los usuarios y los roles realicen determinadas tareas. Puede eliminar privilegios del conjunto heredable inicial y del conjunto límite. Debe probar con cuidado la eliminación de privilegios antes de distribuir un conjunto heredable inicial o un conjunto límite que es menor que el conjunto predeterminado. Al eliminar privilegios del conjunto heredable inicial, puede impedir que los usuarios inicien sesión. Cuando se eliminan privilegios del conjunto límite, es posible que se produzca un error en un programa `setuid` antiguo porque el programa necesita un privilegio que se eliminó.

Asignación de privilegios a una secuencia de comandos

Las secuencias de comandos son ejecutables, como los comandos. Por lo tanto, en un perfil de derechos, puede agregar privilegios a una secuencia de comandos del mismo modo que puede agregar privilegios a un comando. La secuencia de comandos se ejecuta con los privilegios agregados cuando un usuario o rol al que se asignó el perfil de derechos ejecuta la secuencia de comandos en un shell de perfil. Si la secuencia de comandos contiene comandos que requieren privilegios, los comandos con privilegios agregados también deben estar en un perfil de derechos asignado.

Los programas para privilegios pueden restringir los privilegios por proceso. Su función con un programa para privilegios consiste en asignar al archivo ejecutable sólo los privilegios que necesita el programa. Luego, prueba el programa para ver si el programa realiza sus tareas correctamente. También comprueba que el programa no abuse de su uso de privilegios.

Privilegios y dispositivos

El modelo de privilegios utiliza privilegios para proteger las interfaces del sistema que, en el modelo de superusuario, están protegidas sólo por los permisos de archivos. En un sistema con privilegios, los permisos de archivo son demasiado débiles para proteger las interfaces. Un privilegio como `proc_owner` puede anular los permisos de archivo y, a continuación, proporcionar acceso completo a todo el sistema.

Por lo tanto, en Oracle Solaris, la propiedad del directorio de dispositivos no es suficiente para abrir un dispositivo. Por ejemplo, a los miembros del grupo `sys` ya no se les permite abrir automáticamente el dispositivo `/dev/ip`. Los permisos de archivo en `/dev/ip` son `0666`, pero se requiere el privilegio `net_rawaccess` para abrir el dispositivo.

La política de dispositivos se controla mediante privilegios. El comando `getdevpolicy` muestra la política para cada dispositivo. El comando de configuración de dispositivos, `devfsadm`, instala la política de dispositivos. El comando `devfsadm` vincula los conjuntos de privilegios con `open` para la lectura o escritura de dispositivos. Para obtener más información, consulte las páginas del comando `man getdevpolicy(1M)` y `devfsadm(1M)`.

La política de dispositivos ofrece más flexibilidad en el momento de otorgar permiso para abrir dispositivos. Puede requerir privilegios distintos o más privilegios que la política de dispositivos predeterminada. Los requisitos de privilegios se pueden modificar para la política de dispositivos y para el propio controlador. Puede modificar los privilegios al instalar, agregar o actualizar un controlador de dispositivos.

Los comandos `add_drv` y `update_drv` se utilizan para modificar entradas de la política de dispositivos y privilegios específicos del controlador. Para cambiar la política de dispositivos, debe ejecutar el proceso que tenga el conjunto completo de privilegios. Para obtener más información, consulte las páginas de comando `man add_drv(1M)` y `update_drv(1M)`.

Privilegios y depuración

Oracle Solaris proporciona herramientas para depurar errores en privilegios. El comando `ppriv` y el comando `truss` proporcionan los resultados de la depuración. Para ver ejemplos, consulte la página del comando `man ppriv(1)`. Para conocer el procedimiento, consulte [“Cómo determinar los privilegios que necesita un programa” en la página 201](#). También puede utilizar el comando `dttrace`. Para obtener más información, consulte la página del comando `man dttrace(1M)`.

Sobre el RBAC en esta versión

Entre las funciones de RBAC, se incluyen las siguientes:

- El comando `pfedit` permite que un usuario o rol no root edite archivos de sistema especificados. El usuario o el rol deben tener asignada la autorización `solaris.admin.edit/path-to-system-file`. Este comando puede ser utilizado por el rol root para garantizar que las acciones root se coloquen en el registro de auditoría. Para obtener más información, consulte la página del comando `man pfedit(1M)`.
- La política de privilegio extendido permite que privilegios específicos se apliquen a nombres de archivos, números de puertos e ID de usuarios específicos. Para obtener más información, consulte las páginas del comando `man ppriv(1)` y `privileges(5)`. Para obtener un ejemplo de la aplicación de la política de privilegio extendido en un número de puerto, consulte [“Cómo aplicar una política de privilegio extendida a un puerto” en la página 202](#).
- El atributo de seguridad `pam_policy` permite que un administrador configure la política PAM en los niveles de sistema, perfil de derechos, usuario y módulo. Para obtener más información, consulte [“Cambios en PAM para esta versión” en la página 279](#) y [“Cómo asignar una política PAM personalizada a un usuario” en la página 283](#).
- El comando `auths` se extiende de manera similar que el comando `profiles`. Las autorizaciones se pueden gestionar desde la línea de comandos para los archivos y los repositorios de LDAP. Para obtener más información, consulte [“Cómo crear una autorización” en la página 180](#) y la página del comando `man auths(1)`.
- Hay interfaz gráfica de usuario de User Manager disponible para gestionar los usuarios y roles. Para obtener más información, consulte el [Capítulo 3, “Gestión de cuentas de usuarios mediante el uso de la interfaz gráfica de usuario de User Manager \(tareas\)” de *Gestión de las cuentas de usuario y los entornos de usuario en Oracle Solaris 11.1*](#).

Uso del control de acceso basado en roles (tareas)

En este capítulo, se describen las tareas para distribuir las capacidades de superusuario mediante roles discretos. Los mecanismos que los roles pueden utilizar incluyen perfiles de derechos, autorizaciones y privilegios. En este capítulo, se tratan los siguientes temas:

- “Uso de RBAC (tareas)” en la página 155
- “Uso de privilegios (tareas)” en la página 194

Para obtener una descripción general de RBAC, consulte “Control de acceso basado en roles (descripción general)” en la página 131. Para obtener información de referencia, consulte el Capítulo 10, “Atributos de seguridad en Oracle Solaris (referencia)”. Para utilizar privilegios, consulte “Uso de privilegios (tareas)” en la página 194.

Uso de RBAC (tareas)

Para utilizar RBAC, es necesario planificar, configurar RBAC y conocer cómo asumir un rol. Una vez que se haya familiarizado con los roles, puede personalizar aún más RBAC para utilizar nuevas operaciones. El siguiente mapa de tareas hace referencia a dichas tareas principales, incluido el uso de privilegios.

Tarea	Descripción	Para obtener instrucciones
Utilizar la configuración predeterminada de RBAC.	Muestra y usa RBAC sin modificar la instalación inicial.	“Visualización y uso de valores predeterminados de RBAC (mapa de tareas)” en la página 156
Planificar, configurar y utilizar RBAC.	Personaliza RBAC para su sitio.	“Configuración inicial de RBAC (mapa de tareas)” en la página 168
Administrar RBAC.	Actualiza la configuración de RBAC de su sitio.	“Gestión de RBAC (mapa de tareas)” en la página 186

Tarea	Descripción	Para obtener instrucciones
Gestionar y utilizar privilegios.	Agrega y elimina privilegios de usuarios, roles, sistemas y procesos. Usa privilegios. Muestra y depura el uso de privilegios.	“Uso de privilegios (tareas)” en la página 194

Visualización y uso de valores predeterminados de RBAC (tareas)

De manera predeterminada, se asignan derechos a los usuarios. Los derechos para todos los usuarios de un sistema se asignan en el archivo `/etc/security/policy.conf`.

Visualización y uso de valores predeterminados de RBAC (mapa de tareas)

En la instalación de Oracle Solaris, su sistema está configurado con derechos de usuario y derechos de proceso. Sin ninguna configuración adicional, utilice el siguiente mapa de tareas para visualizar y utilizar RBAC.

Tarea	Descripción	Para obtener instrucciones
Ver el contenido de las bases de datos de los atributos de seguridad.	Enumera autorizaciones, perfiles de derechos y comandos con atributos de seguridad en el sistema.	“Cómo visualizar todos los atributos de seguridad definidos” en la página 157
Ver los derechos.	Enumera perfiles de derechos, autorizaciones, privilegios y roles asignados.	“Cómo visualizar los derechos asignados” en la página 158
Asumir el rol de usuario root.	El usuario inicial obtiene derechos administrativos.	“Cómo asumir un rol” en la página 161
Modificar los derechos de un usuario.	Agrega los atributos de seguridad a un usuario normal o los elimina.	“Cómo cambiar los atributos de seguridad de un usuario” en la página 162
Convertirse en administrador.	Existen varios métodos disponibles para los usuarios que tienen asignados derechos administrativos para utilizar esos derechos.	“Cómo usar los derechos administrativos que tiene asignados” en la página 164

▼ Cómo visualizar todos los atributos de seguridad definidos

Utilice los siguientes comandos para enumerar las autorizaciones, los perfiles, los derechos y los comandos con atributos de seguridad en el sistema. Para ver una lista de todos los privilegios definidos, consulte [“Cómo enumerar los privilegios en el sistema” en la página 195](#).

1 Enumere todas las autorizaciones.

- Enumere los nombres de todas las autorizaciones en el servicio de nombres.

```
% auths info
solaris.account.activate
solaris.account.setpolicy
solaris.admin.edit
...
solaris.zone.login
solaris.zone.manage
```

- Enumere los nombres de autorización por perfil de derechos.

```
% getent auth_attr | more
solaris:::All Solaris Authorizations::help=AllSolAuthsHeader.html
solaris.account:::Account Management::help=AccountHeader.html
...
solaris.zone.login:::Zone Login::help=ZoneLogin.html
solaris.zone.manage:::Zone Deployment::help=ZoneManage.html
```

2 Enumere todos los perfiles de derechos.

- Enumere los nombres de todos los perfiles de derechos en el servicio de nombres.

```
% profiles -a
Console User
CUPS Administration
Desktop Removable Media User
...
VSCAN Management
WUSB Management
```

- Enumere las definiciones completas de todos los perfiles de derechos.

```
% getent prof_attr | more
All:::Execute any command as the user or role:help=RtAll.html
Audit Configuration:::Configure Solaris Audit:auths=solaris.smf.value.audit;
help=RtAuditCfg.html
...
Zone Management:::Zones Virtual Application Environment Administration:
help=RtZoneMngmnt.html
Zone Security:::Zones Virtual Application Environment Security:auths=solaris.zone.*,
solaris.auth.delegate;help=RtZoneSecurity.html ...
```

3 Enumere todos los comandos con atributos de seguridad.

```
% getent exec_attr | more
All:solaris:cmd::*:
Audit Configuration:solaris:cmd:::/usr/sbin/auditconfig:privs=sys_audit
...
Zone Security:solaris:cmd:::/usr/sbin/txzonemgr:uid=0
Zone Security:solaris:cmd:::/usr/sbin/zonecfg:uid=0 ...
```

▼ Cómo visualizar los derechos asignados

Utilice los siguientes comandos para ver las asignaciones de RBAC. Para ver todos los derechos que se pueden asignar, consulte [“Cómo visualizar todos los atributos de seguridad definidos” en la página 157.](#)

1 Enumere los perfiles de derechos.

```
% profiles
Basic Solaris User
All
```

Estos perfiles de derechos anteriores se asignan a todos los usuarios de manera predeterminada. Si es el usuario inicial, tiene una lista más grande.

```
% profiles Initial user
System Administrator
Audit Review
...
CPU Power Management
Basic Solaris User
All
```

2 Enumere las autorizaciones.

```
% auths
solaris.device.cdrw,solaris.device.mount.removable,solaris.mail.mailq
solaris.network.autoconf.read,solaris.admin.wusb.read
solaris.smf.manage.vbiosd,solaris.smf.value.vbiosd
```

Estas autorizaciones se incluyen en los perfiles de derechos que se asignan a todos los usuarios de manera predeterminada.

3 Enumere los roles asignados.

```
% roles
root
```

Este rol se asigna al usuario inicial de manera predeterminada. No `roles` indica que no se le ha asignado un rol.

4 Enumere los privilegios en el shell predeterminado.

```
% ppriv $$
1234: /bin/csh
flags = <none>
E: basic
I: basic
P: basic
L: all
```

A cada usuario se le asigna el conjunto de privilegios básico de manera predeterminada. El conjunto límite predeterminado incluye todos los privilegios.

```
% ppriv -vl basic
file_link any
    Allows a process to create hardlinks to files owned by a uid
    different from the process' effective uid.
file_read
    Allows a process to read objects in the filesystem.
file_write
    Allows a process to modify objects in the filesystem.
net_access
    Allows a process to open a TCP, UDP, SDP or SCTP network endpoint.
proc_exec
    Allows a process to call execve().
proc_fork
    Allows a process to call fork1()/forkall()/vfork()
proc_info
    Allows a process to examine the status of processes other
    than those it can send signals to. Processes which cannot
    be examined cannot be seen in /proc and appear not to exist.
proc_session
    Allows a process to send signals or trace processes outside its session.
```

5 Enumere los privilegios sobre comandos en sus perfiles de derechos.

```
% profiles -l
Basic Solaris User
...
/usr/bin/cdrecord.bin privs=file_dac_read,sys_devices,
    proc_lock_memory,proc_priocntl,net_privaddr
/usr/bin/readcd.bin privs=file_dac_read,sys_devices,net_privaddr
/usr/bin/cdda2wav.bin privs=file_dac_read,sys_devices,
    proc_priocntl,net_privaddr
All
*
```

Los perfiles de derechos de un usuario pueden incluir comandos que se ejecutan con privilegios particulares. El perfil de usuario básico de Solaris incluye los comandos que permiten a los usuarios leer y escribir en CD-ROM.

Ejemplo 9-1 Enumeración de autorizaciones de un usuario

```
% auths username
solaris.device.cdrw,solaris.device.mount.removable,solaris.mail.mailq
```

Ejemplo 9-2 Enumeración de los perfiles de derechos de un rol o un usuario

El siguiente comando muestra los perfiles de derechos de un usuario concreto.

```
% profiles jdoe
jdoe:
    Basic Solaris User
    All
```

El siguiente comando muestra los perfiles de derechos del rol cryptomgt.

```
% profiles cryptomgt
cryptomgt:
    Crypto Management
    Basic Solaris User
    All
```

El siguiente comando muestra los perfiles de derechos del rol root:

```
% profiles root
root:
    All
    Console User
    Network Wifi Info
    Desktop Removable Media User
    Suspend To RAM
    Suspend To Disk
    Brightness
    CPU Power Management
    Network Autoconf User
    Basic Solaris User
```

Ejemplo 9-3 Enumeración de los roles asignados de un usuario

El siguiente comando muestra los roles asignados de un usuario concreto.

```
% roles jdoe
root
```

Ejemplo 9-4 Enumeración de los privilegios de un usuario sobre comandos específicos

El siguiente comando muestra los comandos con privilegios en los perfiles de derechos de un usuario normal.

```
% profiles -l jdoe
jdoe:
    Basic Solaris User
    ...
    /usr/bin/cdda2wav.bin  privs=file_dac_read,sys_devices,
                          proc_priocntl,net_privaddr
    /usr/bin/cdrecord.bin  privs=file_dac_read,sys_devices,
                          proc_lock_memory,proc_priocntl,net_privaddr
    /usr/bin/readcd.bin    privs=file_dac_read,sys_devices,net_privaddr
    ...
```

▼ Cómo asumir un rol

Antes de empezar

Ya se debe tener asignado el rol. De manera predeterminada, solo existe el rol root.

1 En una ventana de terminal, determine los roles que puede asumir.

```
% roles
Comma-separated list of role names is displayed
```

2 Utilice el comando su para asumir un rol.

```
% su - rolename
Password: <Type rolename password>
$
```

El comando `su - rolename` cambia el shell a un shell de perfil para el rol. Un shell de perfil reconoce los atributos de seguridad, como autorizaciones, privilegios y bits de ID de conjunto.

3 (Opcional) Verifique si está ahora en un rol.

```
$ /usr/bin/whoami
rolename
```

Ahora puede realizar tareas del rol en esta ventana de terminal.

4 (Opcional) Vea las capacidades de su rol.

Para ver una salida de ejemplo, consulte [“Cómo visualizar los derechos asignados” en la página 158](#).

```
$ profiles -l
verbose rights profiles output
$ auths
authorizations output
```

Ejemplo 9-5 Asunción del rol root

En el ejemplo siguiente, el usuario inicial asume el rol root y enumera los privilegios en el shell del rol.

```
% roles
root
% su - root
Password: <Type root password>
# Prompt changes to root prompt
# ppriv $$
1200: pfksh
flags = <none>
E: all
I: basic
P: all
L: all
```

Para obtener información sobre los privilegios, consulte [“Privilegios \(descripción general\)” en la página 144.](#)

▼ Cómo cambiar los atributos de seguridad de un usuario

Las propiedades de usuario incluyen shell de inicio, perfiles de derechos y roles. El método más seguro para otorgar capacidades administrativas a un usuario es asignar un rol al usuario. Para ver una explicación, consulte [“Consideraciones de seguridad al asignar directamente atributos de seguridad” en la página 143.](#)

Antes de empezar

En la configuración predeterminada, debe asumir el rol root para modificar los atributos de seguridad del usuario.

Después de configurar RBAC para su sitio, tiene otras opciones. Para cambiar la mayoría de los atributos de seguridad de un usuario, incluso la contraseña, debe convertirse en un administrador con el perfil de derechos de seguridad de usuario asignado. Para asignar indicadores de auditoría o cambiar la contraseña de un rol, debe asumir el rol root. Para cambiar otros atributos de usuario, debe convertirse en un administrador con el perfil de derechos de gestión de usuarios asignado. Para obtener más información, consulte [“Cómo usar los derechos administrativos que tiene asignados” en la página 164.](#)

● Use el comando `usermod`.

Este comando modifica los atributos de un usuario que está definido en el servicio de nombres local o el servicio de nombres LDAP. Los argumentos RBAC para este comando son similares a los argumentos para los comandos `useradd` y `rolemod`, como se describe en la página del comando `man user_attr(4)` y se muestra en el [Paso 1 en “Cómo cambiar los atributos de seguridad de un usuario” en la página 162.](#)

Los argumentos de RBAC para el comando son los siguientes:

```
# usermod [-e expire] [-f inactive] [-s shell] [-m] [-A authorization-list] \
[-P profile] [-R role] [-K key=value] [-S repository] login
```

- e *expire* Fecha en la que caduca un inicio de sesión de usuario. Utilice esta opción para crear usuarios temporales.
- f *inactive* Número máximo de días que se permite entre inicios de sesión de usuario. Cuando el valor *inactive* se supera, el usuario no puede iniciar sesión. El valor predeterminado es 0, es decir, no hay ninguna fecha de caducidad.
- m Crea un directorio principal para *rolename* en la ubicación predeterminada.

-s <i>shell</i>	Shell de inicio de sesión para <i>rolename</i> . Este shell debe ser un shell de perfil, como <i>pfbash</i> . Para obtener una lista de shells de perfiles, consulte la página del comando <i>man pfexec(1)</i> .
Consejo – También puede ver la lista de shells de perfiles del directorio <i>/usr/bin</i> en su sistema, como en <i>ls /usr/bin/pf*sh</i> .	
-A <i>authorizations-list</i>	Una o más autorizaciones separadas por comas. Para ver la lista de autorizaciones disponibles, consulte “ Cómo visualizar todos los atributos de seguridad definidos ” en la página 157.
-P <i>profiles-list</i>	Uno o más perfiles de derechos separados por comas. Para ver la lista de perfiles de derechos, consulte “ Cómo visualizar todos los atributos de seguridad definidos ” en la página 157.
-R <i>roles-list</i>	Uno o más roles separados por comas. Para crear roles, consulte “ Cómo crear un rol ” en la página 171.
-K <i>key=value</i>	Un par <i>key=value</i> . Esta opción se puede repetir. Las siguientes claves están disponibles: <i>audit_flags</i> , <i>auths</i> , <i>profiles</i> , <i>project</i> , <i>defaultpriv</i> , <i>limitpriv</i> , <i>lock_after_retries</i> , <i>pam_policy</i> y <i>roleauth</i> . Para obtener información sobre las claves, sus valores y las autorizaciones que son necesarias para definir los valores, consulte la página del comando <i>man user_attr(4)</i> .
-S <i>repository</i>	Uno de <i>files</i> o <i>ldap</i> . Los archivos locales son el valor predeterminado.
<i>login</i>	Nombre de usuario.
Para asignar autorizaciones a un usuario, consulte el Ejemplo 9-7 .	
Para asignar un perfil de derechos a un usuario, consulte el Ejemplo 9-6 .	
Para asignar un rol existente a un usuario, consulte “ Cómo asignar un rol ” en la página 173. En la configuración predeterminada, puede asignar el rol <i>root</i> a un usuario existente.	
Para modificar los privilegios de un usuario, consulte el Ejemplo 9-13 y el Ejemplo 9-9 .	

Ejemplo 9-6 Creación de un usuario que puede gestionar DHCP

En este ejemplo, el administrador de seguridad crea un usuario en LDAP. Al iniciar sesión, el usuario *jdoe-dhcp* puede gestionar DHCP.

```
# useradd -P "DHCP Management" -s /usr/bin/pfbash -S ldap jdoe-dhcp
```

Debido a que el usuario tiene asignado `pfbash` como el shell de inicio de sesión, los atributos de seguridad en el perfil de derechos de gestión de DHCP están disponibles para el usuario en el shell predeterminado del usuario.

Ejemplo 9-7 Asignación de autorizaciones directamente a un usuario

En este ejemplo, el administrador de seguridad crea un usuario local que puede controlar el brillo de la pantalla.

```
# useradd -c "Screened JDoe, local" -s /usr/bin/pfbash \
-A solaris.system.power.brightness jdoe-scr
```

Esta autorización se agrega a las asignaciones existentes del usuario.

Ejemplo 9-8 Eliminación de privilegios del conjunto límite de un usuario

En el siguiente ejemplo, a todas las sesiones que se originan a partir del inicio de sesión inicial de `jdoe` se les impide utilizar el privilegio `sys_linkdir`. Es decir, el usuario no puede establecer enlaces físicos a directorios ni anular el enlace a directorios, incluso después de ejecutar el comando `su`.

```
$ usermod -K 'limitpriv=all,!sys_linkdir' jdoe
$ userattr limitpriv jdoe
all,!sys_linkdir
```

Ejemplo 9-9 Asignación de privilegios directamente a un usuario

En este ejemplo, el administrador de seguridad confía al usuario `jdoe` un privilegio muy específico que afecta la hora del sistema.

```
$ usermod -K defaultpriv='basic,proc_clock_highres' jdoe
```

Los valores de la palabra clave `defaultpriv` reemplazan los valores existentes. Por lo tanto, para que el usuario conserve los privilegios `basic`, se especifica el valor `basic`. En la configuración predeterminada, todos los usuarios tienen privilegios básicos. Para ver la lista de privilegios básicos, consulte el [Paso 4](#).

▼ Cómo usar los derechos administrativos que tiene asignados

En el rol `root`, el usuario inicial tiene todos los derechos administrativos.

El [Paso 1](#) muestra cómo administrar el sistema si tiene derechos administrativos asignados. El [Paso 2](#) muestra cómo cuentas que no son `root` pueden editar un archivo del sistema.

Antes de empezar

Se le han asignado derechos que no se asignan a usuarios comunes. Si no es el usuario root, se le debe asignar un rol, un perfil de derechos administrativos o privilegios específicos o autorizaciones.

1 Seleccione uno de los siguientes métodos para ejecutar los comandos administrativos.

Abra una ventana de terminal.

■ Conviértase en usuario root.

```
% su -
Password:      Type the root password
#
```

Nota – Este método funciona si root es un usuario o un rol. El signo de almohadilla (#) indica que ahora es un usuario root.

■ Asuma un rol que se le ha asignado.

En el siguiente ejemplo, asume un rol de configuración de auditoría. Este rol incluye el perfil de derechos de configuración de auditoría.

```
% su - audadmin
Password:      Type the audadmin password
$
```

El shell en el que escribió este comando se encuentra en un shell de perfil. En este shell, puede ejecutar el comando `auditconfig`. Para obtener más información sobre shells de perfiles, consulte [“Shells de perfil y RBAC” en la página 142](#).

Consejo – Utilice los pasos en [“Cómo visualizar los derechos asignados” en la página 158](#) para ver las capacidades de su rol.

■ Como usuario, use el comando `pfbash` para crear un shell que se ejecute con derechos administrativos.

Por ejemplo, el siguiente conjunto de comandos permite ver los valores de preselección de auditoría y la política de auditoría en el shell `pfbash`:

```
% pfbash
$ auditconfig -getflags
active user default audit flags = ua,ap,lo(0x45000,0x45000)
configured user default audit flags = ua,ap,lo(0x45000,0x45000)
$ auditconfig -getpolicy
configured audit policies = cnt
active audit policies = cnt
```

- **Como usuario, use el comando `pfexec` para crear un proceso que se ejecute con derechos administrativos.**

Ejecute el comando `pfexec` con el nombre de un comando con privilegios desde su perfil de derechos. Por ejemplo, el siguiente comando permite ver los indicadores de auditoría preseleccionados del usuario:

```
% pfexec auditconfig -getflags
active user default audit flags = ua,ap,lo(0x45000,0x45000)
configured user default audit flags = ua,ap,lo(0x45000,0x45000)
```

Las mismas limitaciones de privilegios se aplican a `pfexec` y `pfbash`. Sin embargo, para ejecutar otro comando con privilegios, debe escribir `pfexec` de nuevo antes de escribir el comando con privilegios.

```
% pfexec auditconfig -getpolicy
configured audit policies = cnt
active audit policies = cnt
```

- **Como usuario, use el comando `sudo` para crear un proceso que se ejecute con derechos administrativos.**

Ejecute el comando `sudo` con el nombre de un comando administrativo que se le asigna en el archivo `sudoers`. Para obtener más información, consulte las páginas del comando `man sudo(1M)` y `sudoers(4)`.

2 Para editar un archivo del sistema, use el comando `pfedit`.

Si no es un usuario `root` con UID de 0, no puede editar archivos del sistema de manera predeterminada. Sin embargo, si se le asigna la autorización `solaris.admin.edit/path-to-system-file`, puede editar *system-file*. Por ejemplo, si se le asigna la autorización `solaris.admin.edit/etc/security/audit_warn`, puede editar el archivo `audit_warn`.

```
$ pfedit /etc/security/audit_warn
```

El comando usa el valor de `$EDITOR` para determinar el editor de texto. Para obtener más información, consulte la página de comando `man pfedit(1M)`. El comando `pfedit` es ejecutado de manera útil por el rol `root`, si la auditoría está configurada para auditar eventos `AUE_PFEEXEC`.

Ejemplo 9–10 Almacenamiento en la caché de la autenticación para facilitar el uso del rol

En este ejemplo, el administrador configura un rol para gestionar la red, pero proporciona facilidad de uso mediante el almacenamiento en la caché de la autenticación del usuario. En primer lugar, el administrador crea y asigna el rol.

```
# roleadd -K roleauth=user -P "Audit Configuration" audadmin
# usermod -R +audadmin jdoe
```

Cuando `jdoe` utiliza la opción `-c` al cambiar al rol, se necesita una contraseña antes de que la salida de `auditconfig` se muestre:

```
% su - audadmin -c auditconfig option
Password:
    auditconfig output
```

Si la autenticación no se almacena en la caché y `jdoe` ejecuta el comando de nuevo inmediatamente, una solicitud de contraseña aparece.

El administrador crea un archivo en el directorio `pam.d` para que contenga una pila `su` que permite la autenticación, de manera que una contraseña se solicite de manera inicial, pero que no se vuelva a solicitar hasta después de un tiempo.

```
# pfedit /etc/pam.d/su
## Cache authentication for switched user
#
auth required      pam_unix_cred.so.1
auth sufficient    pam_tty_tickets.so.1
auth requisite     pam_authtok_get.so.1
auth required      pam_dhkeys.so.1
auth required      pam_unix_auth.so.1
```

Después de crear el archivo, el administrador comprueba que las entradas no tengan errores ortográficos, omisiones ni repeticiones.

El administrador debe proporcionar la pila `su` anterior completa. El módulo `pam_tty_tickets.so.1` implementa la caché. Para obtener más información sobre PAM, consulte la página del comando `man pam.conf(4)` y el [Capítulo 14, “Uso de módulos de autenticación conectables”](#).

Después de que el administrador agrega el archivo PAM `su` y reinicia el sistema, a todos los roles, incluido el rol `audadmin`, se les solicitará una vez una contraseña al ejecutar un grupo de comandos.

```
% su - audadmin -c auditconfig option
Password:
    auditconfig output
% su - audadmin -c auditconfig option
    auditconfig output
...
```

Personalización de RBAC para su sitio (tareas)

La configuración inicial de RBAC incluye la creación de usuarios que pueden asumir roles específicos, la creación de roles y la asignación de dichos roles a los usuarios correspondientes.

Configuración inicial de RBAC (mapa de tareas)

Utilice el siguiente mapa de tareas para planificar e implementar inicialmente RBAC en su sitio. Algunas tareas están ordenadas.

Tarea	Descripción	Para obtener instrucciones
Planificar la implementación de RBAC.	Implica examinar las necesidades de seguridad de su sitio y decidir cómo utilizará RBAC en su sitio.	“Cómo planificar la implementación de RBAC” en la página 169
Configurar los usuarios que pueden asumir un rol.	Crea las cuentas de inicio de sesión para usuarios de confianza que pueden asumir un rol administrativo.	“Configuración y administración de cuentas de usuario (mapa de tareas)” de Administración de Oracle Solaris: tareas comunes
Crear roles.	Crea roles y asigna los roles a los usuarios.	“Cómo crear un rol” en la página 171 “Cómo asignar un rol” en la página 173
(Recomendada) Auditar acciones de roles.	Preselecciona una clase de auditoría que incluye el evento de auditoría que registra las acciones de roles.	“Cómo auditar roles” en la página 174
Crear un perfil de derechos.	Crea un perfil de derechos.	“Cómo crear un perfil de derechos” en la página 175
Modificar un perfil de derechos.	Modifica asignaciones de privilegios en un perfil de derechos. Agrega privilegios a un comando en un perfil de derechos.	Ejemplo 9–16 Ejemplo 9–17
Clonar perfiles de derechos existentes.	Crea un perfil de derechos de un perfil de derechos del sistema. Agrega la autorización <code>solaris.admin.edit/file</code> a un perfil de derechos. Elimina las autorizaciones de un perfil de derechos.	“Cómo clonar y modificar un perfil de derechos del sistema” en la página 177 Ejemplo 9–19 Ejemplo 9–20

Tarea	Descripción	Para obtener instrucciones
Crear una autorización.	Crea una autorización. Usa la nueva autorización en un perfil de derechos.	“Cómo crear una autorización” en la página 180 Ejemplo 9–21
Proteger las aplicaciones antiguas.	Activa los permisos de ID de conjunto para las aplicaciones antiguas. Las secuencias de comandos pueden contener comandos con ID de conjuntos. Las aplicaciones antiguas pueden comprobar si existen autorizaciones, si corresponde.	“Cómo agregar propiedades RBAC a las aplicaciones antiguas” en la página 181 Ejemplo 9–23
Solucionar problemas de asignación de atributos de seguridad.	Depura el motivo por el cual los atributos de seguridad asignados podrían no estar disponibles para usuarios, roles o procesos.	“Cómo solucionar problemas de asignación de privilegios y RBAC” en la página 182

▼ Cómo planificar la implementación de RBAC

RBAC puede ser una parte integral de la manera en que una organización gestiona sus recursos de información. La planificación requiere un conocimiento exhaustivo de las capacidades de RBAC, así como de los requisitos de seguridad de la organización.

Nota – Los derechos predeterminados se asignan en el archivo `/etc/security/policy.conf`.

1 Aprenda los conceptos básicos de RBAC.

Lea [“Control de acceso basado en roles \(descripción general\)” en la página 131](#). Usar RBAC para administrar un sistema es muy diferente a utilizar las prácticas administrativas UNIX convencionales. Para estar familiarizado con los conceptos de RBAC antes de iniciar la implementación, consulte el [Capítulo 10, “Atributos de seguridad en Oracle Solaris \(referencia\)”](#).

2 Examine la política de seguridad.

La política de seguridad de la organización detalla las amenazas potenciales para el sistema, mide el riesgo de cada amenaza y brinda estrategias para contrarrestar dichas amenazas. Aislar las tareas relacionadas con la seguridad por medio de RBAC puede ser parte de la estrategia. Aunque puede utilizar las configuraciones de RBAC instaladas tal como están, puede que sea necesario personalizarlas para adherirse a su política de seguridad.

3 Decida qué nivel de RBAC necesita la organización.

En función de las necesidades de seguridad, puede utilizar distintos grados de RBAC, como se muestra a continuación:

- **Root como un rol:** este método se proporciona de manera predeterminada. Evita que cualquier usuario inicie sesión como root. En su lugar, un usuario debe iniciar sesión utilizando su inicio de sesión asignado antes de asumir el rol root.
- **Roles discretos:** este método crea roles que se basan en perfiles de derechos proporcionados. Los roles se pueden asignar según el nivel de responsabilidad, el ámbito de la tarea y el tipo de tarea. Por ejemplo, el rol de administrador del sistema puede realizar muchas tareas que el superusuario puede realizar, mientras que el rol de gestión de IPsec de red puede gestionar IPsec.

También puede separar las responsabilidades de seguridad de otras responsabilidades. El rol de gestión de usuarios puede crear usuarios, mientras que el rol de seguridad de usuarios puede asignar atributos de seguridad, como contraseñas, roles y perfiles de derechos. Sin embargo, el rol de seguridad de usuarios no puede crear un usuario y el rol de gestión de usuarios no puede asignar un perfil de derechos a un usuario.

- **Sin rol root:** este método requiere que se cambie la configuración predeterminada del sistema. En esta configuración, cualquier usuario que conoce la contraseña de root puede iniciar sesión y modificar el sistema. No puede saber qué usuario era superusuario.

4 Decida qué roles son adecuados para la organización.

Revise las capacidades de los roles recomendados y los perfiles de derechos predeterminados. Los perfiles de derechos predeterminados permiten a los administradores configurar un rol recomendado por medio de un único perfil.

Para examinar de forma más detallada los perfiles de derechos, realice una de las siguientes acciones:

- Visualice los perfiles de derechos disponibles en el sistema mediante el comando `getent prof_attr`.
- En esta guía, consulte [“Perfiles de derechos” en la página 205](#) para obtener resúmenes de algunos perfiles de derechos típicos.

5 Decida si otros roles o perfiles de derechos son adecuados para la organización.

Busque otras aplicaciones o familias de aplicaciones en su sitio que puedan beneficiarse del acceso restringido. Las aplicaciones que afectan la seguridad, que pueden causar problemas de denegación del servicio o que requieren una formación especial del administrador son opciones apropiadas para RBAC. Puede personalizar roles y perfiles de derechos para gestionar los requisitos de seguridad de la organización.

a. Determine qué comandos son necesarios para la nueva tarea.

b. Decida qué perfil de derechos es adecuado para esta tarea.

Compruebe si un perfil de derechos existente puede gestionar esta tarea o si es necesario crear un perfil de derechos independiente.

Nota – Los perfiles de derechos de copia de seguridad de medios o de restauración de medios proporcionan acceso a todo el sistema de archivos raíz. Por lo tanto, estos perfiles de derechos se asignan de manera adecuada solamente a usuarios de confianza. También puede optar por no asignar estos perfiles de derechos. De manera predeterminada, sólo el rol root es de confianza para realizar copias de seguridad y restaurar.

c. Determine qué rol es adecuado para este perfil de derechos.

Decida si el perfil de derechos para esta tarea se debe asignar a un rol existente o si es necesario crear un nuevo rol. Si utiliza un rol existente, compruebe que los perfiles de derechos originales del rol sean adecuados para los usuarios que están asignados a este rol. Ordene el nuevo perfil de derechos para que los comandos se ejecuten con los privilegios requeridos. Para obtener información sobre cómo ordenar, consulte [“Orden de búsqueda para atributos de seguridad asignados” en la página 207](#).

6 Decida qué usuarios se deben asignar a qué roles.

Según el principio de [privilegio mínimo](#), se asignan usuarios a roles que son adecuados para el nivel de confianza del usuario. Al impedir que los usuarios realicen tareas que los usuarios no necesitan realizar, se reducen los problemas potenciales.

▼ Cómo crear un rol

Los roles se pueden crear localmente y en un repositorio LDAP.

Antes de empezar

Para crear un rol, debe convertirse en un administrador con el perfil de derechos de gestión de usuarios asignado. Para asignar atributos de seguridad al rol, incluso la contraseña inicial, debe convertirse en un administrador con el perfil de derechos de seguridad de usuario asignado. Para obtener más información, consulte [“Cómo usar los derechos administrativos que tiene asignados” en la página 164](#).

1 Para crear un rol, use el comando `roleadd`.

Para ver las restricciones en cadenas aceptables, consulte la página del comando `man roleadd(1M)`.

```
# roleadd [-e expire] [-f inactive] [-s shell] [-m] [-S repository] \
[-A authorization-list] [-P profile-list] [-K key=value] rolename
```

Consejo – Cuando el nombre del rol refleja el nombre de un perfil de derechos, puede comprender con facilidad el objetivo del rol. Por ejemplo, asigne el perfil de derechos de revisión de auditoría al rol `audit review` para permitir que el rol lea, filtre y archive registros de auditoría.

Los argumentos RBAC para este comando son similares a los argumentos para el comando `usermod`, como se describe en la página del comando `man user_attr(4)` y se muestra en el Paso 1 en “[Cómo cambiar los atributos de seguridad de un usuario](#)” en la página 162. Por ejemplo, el siguiente comando crea un rol de administrador de usuarios local y un directorio principal:

```
# roleadd -c "User Administrator role, local" -s /usr/bin/pfbash \
-m -K profiles="User Security,User Management" useradm
80 blocks
# ls /export/home/useradm
local.cshrc      local.login      local.profile
```

2 Cree la contraseña inicial para el rol.

```
# passwd -r files useradm
Password:      <Type useradm password>
Confirm Password:  <Retype useradm password>
#
```

Nota – Normalmente, una cuenta de rol se asigna a más de un usuario. Por lo tanto, un administrador, normalmente, crea una contraseña de rol y proporciona a los usuarios la contraseña de rol fuera de banda.

3 Para asignar el rol a un usuario, ejecute el comando `usermod`.

Para conocer el procedimiento, consulte “[Cómo asignar un rol](#)” en la página 173 y el [Ejemplo 9–14](#).

Ejemplo 9–11 Creación de un rol de administrador de usuarios en el repositorio LDAP

En este ejemplo, el sitio del administrador utiliza un repositorio LDAP. Mediante la ejecución del siguiente comando, el administrador crea un rol de administrador de usuarios en LDAP.

```
# roleadd -c "User Administrator role, LDAP" -s /usr/bin/pfbash \
-m -S ldap -K profiles="User Security,User Management" useradm
```

Ejemplo 9–12 Creación de roles para la separación de tareas

En este ejemplo, el sitio del administrador utiliza un repositorio LDAP. Mediante la ejecución de los siguientes comandos, el administrador crea dos roles. El rol `usermgt` puede crear usuarios, darles directorios principales y realizar otras tareas que no son de seguridad. El rol `usermgt` no

puede asignar contraseñas u otros atributos de seguridad. El rol `usersec` no puede crear usuarios, pero puede asignar contraseñas y cambiar otros atributos de seguridad.

```
# roleadd -c "User Management role, LDAP" -s /usr/bin/pfbash \
-m -S ldap -K profiles="User Management" usermgt
# roleadd -c "User Security role, LDAP" -s /usr/bin/pfbash \
-m -S ldap -K profiles="User Security" usersec
```

Ejemplo 9–13 Creación de un rol de seguridad de archivo y dispositivo

En este ejemplo, el administrador crea un rol de seguridad de archivo y dispositivo para este sistema:

```
# roleadd -c "Device and File System Security admin, local" -s /usr/bin/pfbash \
-m -K profiles="Device Security,File System Security" devflsec
```

▼ Cómo asignar un rol

Este procedimiento asigna un rol a un usuario, reinicia el daemon de caché de nombres y luego muestra cómo el usuario puede asumir el rol.

Antes de empezar Agregó un rol y le asignó una contraseña, como se describe en [“Cómo crear un rol” en la página 171](#).

Para modificar la mayoría de los atributos de seguridad de un usuario, incluso la contraseña, debe convertirse en un administrador con el perfil de derechos de seguridad de usuario asignado. Para modificar indicadores de auditoría de un usuario, debe asumir el rol `root`. Para modificar otros atributos, debe convertirse en un administrador con el perfil de derechos de gestión de usuarios asignado. El rol `root` puede modificar cada atributo de un usuario. Para obtener más información, consulte [“Cómo usar los derechos administrativos que tiene asignados” en la página 164](#).

- **Asigne el rol a un usuario.**

```
usermod [-S repository] [RBAC-arguments] login
```

Por ejemplo, asigne el rol a un usuario local:

```
# usermod -R +useradm jdoe-local
```

Los cambios entran en vigencia a partir del siguiente inicio de sesión del usuario.

Para conocer las opciones del comando `usermod`, consulte la página del comando `man usermod(1M)` o la descripción de las opciones para `rolemod` en el [Paso 1 en “Cómo cambiar los atributos de seguridad de un usuario” en la página 162](#).

Ejemplo 9–14 Creación y asignación de un rol para administrar la criptografía

En este ejemplo, el administrador en una red LDAP crea un rol para administrar la estructura criptográfica y asigna el rol al UID 1111.

```
# roleadd -c "Cryptographic Services manager" \
-g 14 -m -u 104 -s /usr/bin/pfksh \
-S ldap -K profiles="Crypto Management" cryptmgt
# passwd cryptmgt
New Password:      <Type cryptmgt password>
Confirm password:  <Retype cryptmgt password>
# usermod -u 1111 -R +cryptmgt
```

El usuario con el UID 1111 inicia sesión, luego asume el rol y muestra los atributos de seguridad asignados.

```
% su - cryptmgt
Password:      <Type cryptmgt password>
Confirm Password:  <Retype cryptmgt password>
$ profiles -l
    Crypto Management
        /usr/bin/kmfcfg          euid=0
        /usr/sbin/cryptoadm      euid=0
        /usr/sfw/bin/CA.pl       euid=0
        /usr/sfw/bin/openssl     euid=0
$
```

Para obtener información sobre la estructura criptográfica, consulte el [Capítulo 11, “Estructura criptográfica \(descripción general\)”](#). Para administrar la estructura, consulte [“Administración de la estructura criptográfica \(mapa de tareas\)”](#) en la página 241.

▼ Cómo auditar roles

Las acciones que realiza un rol se pueden auditar. En el registro de auditoría, se incluye el nombre de inicio de sesión del usuario que asumió el rol, el nombre del rol y la acción que realizó el rol. El evento de auditoría 116: AUE_PFEXEC:execve(2) with pfexec enabled: ps, ex, ua, as captura acciones de roles. Mediante la preselección de una de las clases as, ex, ps o ua, se auditan las acciones de roles.

Antes de empezar

Para configurar la auditoría, debe convertirse en un administrador con el perfil de derechos de configuración de auditoría asignado. Para activar o refrescar el servicio de auditoría, debe convertirse en un administrador con el perfil de derechos de control de auditoría asignado. El rol root puede realizar cada tarea de este procedimiento. Para obtener más información, consulte [“Cómo usar los derechos administrativos que tiene asignados”](#) en la página 164.

1 Incluya la auditoría de roles en su plan de auditoría.

Para obtener información sobre planificación, consulte el [Capítulo 27, “Planificación de la auditoría”](#).

2 Preseleccione una de las clases `as`, `ex`, `ps` o `ua`.

- Si el servicio de auditoría está activado, revise las clases preseleccionadas.

```
# auditconfig -getflags
```

Si una de las clases `as`, `ex`, `ps` o `ua` está preseleccionada, las acciones de roles se están auditando. Si no es así, agregue una de estas clases a las clases existentes.

```
# auditconfig -setflags existing preselections,as
```

- Si la auditoría aún no está activada, preseleccione una clase que audite acciones de roles.

```
# auditconfig -setflags as
```

En este ejemplo, el administrador elige la clase `as`. Esta clase incluye otros eventos de auditoría. Para ver los eventos de auditoría que se incluyen en una clase, utilice el comando `audit record`, como se muestra en el [Ejemplo 28–28](#).

3 Active o refresque el servicio de auditoría.

```
# audit -s
```

▼ Cómo crear un perfil de derechos

Puede crear o cambiar un perfil de derechos cuando los perfiles de derechos proporcionados no contienen los atributos de seguridad de recopilación que necesita. Para obtener más información sobre los perfiles de derechos, consulte [“Perfiles de derechos de RBAC” en la página 141](#).

Antes de empezar

Para crear un perfil de derechos, debe convertirse en un administrador con el perfil de derechos de seguridad de archivos asignado. Para obtener más información, consulte [“Cómo usar los derechos administrativos que tiene asignados” en la página 164](#).

1 Cree un perfil de derechos.

```
# profiles -p [-S repository] profile-name
```

Se le pedirá una descripción.

2 Agregue contenidos al perfil de derechos.

Use el subcomando `set` para las propiedades de perfil que tengan un único valor, como `set desc`. Use el subcomando `add` para las propiedades que tengan más de un valor, como `add cmd`.

Por ejemplo, el siguiente comando crea el perfil de derechos PAM en “[Cómo asignar una nueva política de derechos a todos los usuarios](#)” en la [página 284](#) interactivamente. El nombre se acorta con fines de visualización.

```
# profiles -p -S LDAP "Site PAM LDAP"
profiles:Site PAM LDAP> set desc="Profile which sets pam_policy=ldap"
...LDAP> set pam_policy=ldap
...LDAP> commit
...LDAP> end
...LDAP> exit
```

Ejemplo 9–15 Creación de un perfil de derechos de usuarios Sun Ray

En este ejemplo, el administrador crea un perfil de derechos para usuarios Sun Ray en el repositorio LDAP. El administrador ya ha creado una versión Sun Ray del perfil de derechos de usuario de Solaris básico y ha eliminado todos los derechos de perfiles del archivo `policy.conf` en el servidor Sun Ray.

```
# profiles -p -S LDAP "Sun Ray Users"
profiles:Sun Ray Users> set desc="For all users of Sun Rays"
... Ray Users> add profiles="Sun Ray Basic User"
... Ray Users> set defaultpriv="basic,!proc_info"
... Ray Users> set limitpriv="basic,!proc_info"
... Ray Users> end
... Ray Users> exit
```

El administrador verifica el contenido.

```
# profiles -p "Sun Ray Users"
Found profile in LDAP repository.
profiles:Sun Ray Users> info
    name=Sun Ray Users
    desc=For all users of Sun Rays
    defaultpriv=basic,!proc_info,
    limitpriv=basic,!proc_info,
    profiles=Sun Ray Basic User
```

Ejemplo 9–16 Eliminación de un privilegio básico de un perfil de derechos

En el siguiente ejemplo, tras una exhaustiva prueba, el administrador de seguridad elimina otro privilegio básico del perfil de derechos de usuarios Sun Ray. En el [Ejemplo 9–15](#), el administrador eliminó un privilegio. El perfil de derechos se modifica para eliminar dos privilegios básicos. Los usuarios a los que se asigna este perfil no pueden examinar ningún proceso fuera de su sesión actual y no pueden agregar otra sesión.

```
$ profiles -p "Sun Ray Users"
profiles:Sun Ray Users> set defaultpriv="basic,!proc_session,!proc_info"
profiles:Sun Ray Users> end
profiles:Sun Ray Users> exit
```

Ejemplo 9–17 Eliminación de los privilegios del conjunto límite de un perfil de derechos

En el siguiente ejemplo, tras una exhaustiva prueba, el administrador de seguridad elimina dos privilegios límite del perfil de derechos de usuarios Sun Ray.

```
$ profiles -p "Sun Ray Users"
profiles:Sun Ray Users> set limitpriv="all,!proc_session,!proc_info"
profiles:Sun Ray Users> end
profiles:Sun Ray Users> exit
```

Ejemplo 9–18 Creación de un perfil de derechos que incluye comandos con privilegios

En este ejemplo, el administrador de seguridad agrega privilegios a una aplicación en un perfil de derechos que crea el administrador. La aplicación admite privilegios.

```
# profiles -p SiteApp
profiles:SiteApp> set desc="Site application"
profiles:SiteApp> add cmd="/opt/site-app/bin/site-cmd"
profiles:SiteApp:site-cmd> add privs="proc_fork,proc_taskid"
profiles:SiteApp:site-cmd> end
profiles:SiteApp> exit
```

Para verificar, el administrador selecciona `site-cmd`.

```
# profiles -p SiteApp "select cmd=/opt/site-app/bin/site-cmd; info;end"
Found profile in files repository.
  id=/opt/site-app/bin/site-cmd
  privs=proc_fork,proc_taskid
```

Véase también Para solucionar problemas de asignación de atributos de seguridad, consulte [“Cómo solucionar problemas de asignación de privilegios y RBAC” en la página 182](#). Para obtener información, consulte [“Orden de búsqueda para atributos de seguridad asignados” en la página 207](#).

▼ Cómo clonar y modificar un perfil de derechos del sistema

Los perfiles de derechos que Oracle Solaris proporciona son de solo lectura. Puede clonar un perfil de derechos proporcionado para modificarlo si su colección de atributos de seguridad no es suficiente. Por ejemplo, es posible que quiera agregar la autorización `solaris.admin.edit/path-to-system-file` a un perfil de derechos proporcionado.

Antes de empezar Para crear o cambiar un perfil de derechos, debe convertirse en un administrador con el perfil de derechos de seguridad de archivos asignado. Para obtener más información, consulte [“Cómo usar los derechos administrativos que tiene asignados” en la página 164](#).

1 Cree un nuevo perfil de derechos a partir de un perfil existente.

```
# profiles -p [-S repository] existing-profile-name
```

- **Para mejorar un perfil de derechos existente, cree un nuevo perfil.**

Agregue el perfil de derechos existente como perfil de derechos suplementario y, a continuación, agregue las mejoras. Si desea ver un ejemplo, consulte el [Ejemplo 9–19](#).

- **Para eliminar contenido de un perfil de derechos existente, clone el perfil.**

A continuación, cambie el nombre del perfil y modifíquelo. Si desea ver un ejemplo, consulte el [Ejemplo 9–20](#).

2 Modifique el nuevo perfil de derechos.

Agregue o elimine perfiles de derechos suplementarios, autorizaciones y otros atributos de seguridad.

Ejemplo 9–19 Clonación y mejora del perfil de derechos de gestión de IPsec de red

En este ejemplo, el administrador agrega varias autorizaciones `solaris.admin.edit` a un perfil de derechos de gestión de IPsec de sitio.

El administrador verifica que el perfil de derechos de gestión de IPsec de red no se puede modificar.

```
# profiles -p "Network IPsec Management"
profiles:Network IPsec Management> add auths="solaris.admin.edit/etc/hosts"
Cannot add. Profile cannot be modified
```

A continuación, el administrador crea un perfil de derechos que incluye el perfil de gestión de IPsec de red.

```
# profiles -p "Total IPsec Mgt"
... IPsec Mgt> set desc="Network IPsec Mgt plus edit authorization"
... IPsec Mgt> add profiles="Network IPsec Management"
... IPsec Mgt> add auths="solaris.admin.edit/etc/hosts"
... IPsec Mgt> add auths="solaris.admin.edit/etc/inet/ipsecinit.conf"
... IPsec Mgt> add auths="solaris.admin.edit/etc/inet/ike/config"
... IPsec Mgt> add auths="solaris.admin.edit/etc/inet/secret/ipseckeys"
... IPsec Mgt> end
... IPsec Mgt> exit
```

El administrador verifica el contenido.

```
# profiles -p "Total IPsec Mgt" info
name=Total IPsec Mgt
desc=Network IPsec Mgt plus edit authorization
auths=solaris.admin.edit/etc/hosts,
solaris.admin.edit/etc/inet/ipsecinit.conf,
solaris.admin.edit/etc/inet/ike/config,
solaris.admin.edit/etc/inet/secret/ipseckeys
profiles=Network IPsec Management
```

Ejemplo 9–20 Clonación y eliminación de atributos de seguridad de un perfil de derechos

En este ejemplo, el administrador separa la gestión de las propiedades del servicio VSCAN de la capacidad para activar y desactivar el servicio.

En primer lugar, el administrador muestra el contenido del perfil de derechos que proporciona Oracle Solaris.

```
% profiles -p "VSCAN Management" info
      name=VSCAN Management
      desc=Manage the VSCAN service
      auths=solaris.smf.manage.vscan,solaris.smf.value.vscan,
            solaris.smf.modify.application
      help=RtVscanMngmnt.html
```

Luego, el administrador crea un perfil de derechos para activar y desactivar el servicio.

```
# profiles -p "VSCAN Management"
profiles:VSCAN Management> set name="VSCAN Control"
profiles:VSCAN Control> set desc="Start and stop the VSCAN service"
... VSCAN Control> remove auths="solaris.smf.value.vscan"
... VSCAN Control> remove auths="solaris.smf.modify.application"
... VSCAN Control> end
... VSCAN Control> exit
```

Luego, el administrador crea un perfil de derechos que puede cambiar las propiedades del servicio.

```
# profiles -p "VSCAN Management"
profiles:VSCAN Management> set name="VSCAN Properties"
profiles:VSCAN Properties> set desc="Modify VSCAN service properties"
... VSCAN Properties> remove auths="solaris.smf.manage.vscan"
... VSCAN Properties> end
... VSCAN Properties> exit
```

El administrador verifica el contenido del nuevo perfil de derechos.

```
# profiles -p "VSCAN Control" info
      name=VSCAN Control
      desc=Start and stop the VSCAN service
      auths=solaris.smf.manage.vscan
# profiles -p "VSCAN Properties" info
      name=VSCAN Properties
      desc=Modify VSCAN service properties
      auths=solaris.smf.value.vscan,solaris.smf.modify.application
```

Véase también Para solucionar problemas de asignación de atributos de seguridad, consulte [“Cómo solucionar problemas de asignación de privilegios y RBAC” en la página 182](#). Para obtener información, consulte [“Orden de búsqueda para atributos de seguridad asignados” en la página 207](#).

▼ Cómo crear una autorización

Puede crear una autorización cuando las autorizaciones proporcionadas no cubren las autorizaciones que necesita. Para obtener más información sobre autorizaciones, consulte [“Autorizaciones RBAC” en la página 138](#).

Antes de empezar

Ha definido y utilizado la autorización en el programa que protege. Para obtener instrucciones, consulte *Developer's Guide to Oracle Solaris 11 Security* y *“About Authorizations” de Developer's Guide to Oracle Solaris 11 Security*.

1 (Opcional) Cree el archivo de ayuda para su nueva autorización.

Por ejemplo, cree el archivo de ayuda para que una autorización permita al usuario modificar los datos en una aplicación.

```
# pfedit /docs/helps/NewcoSiteAppModData.html
<HTML>
-- Copyright 2012 Newco. All rights reserved.
-- NewcoSiteAppModData.html
-->
<HEAD>
  <TITLE>NewCo Modify SiteApp Data Authorization</TITLE>
</HEAD>
<BODY>
The com.newco.siteapp.data.modify authorization authorizes you
to modify existing data in the application.
<p>
Only authorized accounts are permitted to modify data.
Use this authorization with care.
<p>
</BODY>
</HTML>
```

2 Cree la autorización.

Por ejemplo, cree la autorización `com.newco.siteapp.data.modify` en el sistema local.

```
# auths add -t "SiteApp Data Modify Authorized" \
-h /docs/helps/NewcoSiteAppModData.html com.newco.siteapp.data.modify
```

Ahora puede agregar la autorización a un perfil de derechos y asignar al perfil un rol o un usuario.

Ejemplo 9–21 Agregación de autorizaciones a un perfil de derechos

En este ejemplo, el administrador agrega una autorización que una aplicación de sitio comprueba antes de permitir que un usuario ejecute la aplicación.

Después de crear la autorización, el administrador de seguridad agrega la autorización `com.newco.siteapp.data.modify` a un perfil de derechos existente. El administrador creó el perfil en el [Ejemplo 9–18](#).


```
# profiles -p "SiteApp"
profiles:SiteApp> add auths="com.newco.siteapp.data.modify"
profiles:SiteApp> end
profiles:SiteApp> exit
```

Para realizar una verificación, el administrador muestra el contenido del perfil.

```
# profiles -p SiteApp
Found profile in files repository.
  id=/opt/site-app/bin/site-cmd
  auths=com.newco.siteapp.data.modify
```

▼ Cómo agregar propiedades RBAC a las aplicaciones antiguas

Una aplicación antigua es un comando o un conjunto de comandos. Los atributos de seguridad se definen para cada comando en un perfil de derechos asignado a un rol. Un usuario que asume el rol puede ejecutar la aplicación antigua con los atributos de seguridad.

Antes de empezar

Para crear el perfil de derechos, debe convertirse en un administrador con el perfil de derechos de seguridad de la información o de gestión de derechos asignado. Para asignar el perfil de derechos, debe convertirse en un administrador con el perfil de derechos de seguridad de usuario asignado. El rol `root` puede realizar cada tarea en este procedimiento. Para obtener más información, consulte [“Cómo usar los derechos administrativos que tiene asignados” en la página 164](#).

1 Agregue atributos de seguridad a los comandos que implementan la aplicación antigua.

Agregue los atributos de seguridad a una aplicación antigua del mismo modo que lo haría para cualquier comando. Debe agregar el comando con atributos de seguridad a un perfil de derechos. Para un comando antiguo, proporcione los atributos de seguridad `euid=0` o `uid=0`. Para obtener detalles del procedimiento, consulte [“Cómo crear un perfil de derechos” en la página 175](#).

a. Cree un nuevo perfil de derechos para la aplicación antigua.

Para conocer los pasos, consulte [“Cómo crear un perfil de derechos” en la página 175](#).

b. Agregue los comandos con los atributos de seguridad necesarios.

Si desea ver un ejemplo, consulte el [Ejemplo 9–18](#).

2 Incluya el perfil de derechos en la lista de perfiles de un rol.

Para asignar un perfil de derechos a un rol, consulte el [Ejemplo 9–14](#).

Ejemplo 9–22 Agregación de atributos de seguridad a comandos en una secuencia de comandos

Si un comando de una secuencia de comandos necesita tener el conjunto de bits `setgid` o `setuid` para ejecutarse correctamente, el archivo ejecutable de la secuencia y el comando deben tener los atributos de seguridad agregados en un perfil de derechos. Luego, el perfil de derechos se asigna a un rol, y el rol se asigna a un usuario. Cuando el usuario asume el rol y ejecuta la secuencia de comandos, el comando se ejecuta con los atributos de seguridad.

Ejemplo 9–23 Comprobación de autorizaciones en una secuencia de comandos o un programa

Para comprobar autorizaciones, escriba una prueba basada en el comando `auths`. Para obtener información detallada sobre este comando, consulte la página del comando `man auths(1)`.

Por ejemplo, la siguiente línea verifica si el usuario tiene la autorización que se proporciona como argumento `$1`:

```
if [ '/usr/bin/auths|usr/xpg4/bin/grep $1' ]; then
    echo Auth granted
else
    echo Auth denied
fi
```

Para que la prueba sea más completa, debe incluir una lógica que compruebe el uso de caracteres comodín. Por ejemplo, para verificar si el usuario tiene la autorización `solaris.system.date`, debe comprobar las siguientes cadenas:

- `solaris.system.date`
- `solaris.system.*`
- `solaris.*`

Si está escribiendo un programa, utilice la función `getauthattr()` para comprobar la autorización.

▼ Cómo solucionar problemas de asignación de privilegios y RBAC

Varios factores pueden afectar el motivo por el que los procesos de un usuario o rol no se ejecutan con atributos de seguridad asignados. Este procedimiento lo ayuda a depurar asignaciones de atributos de seguridad con errores. Muchos de los pasos están basados en [“Orden de búsqueda para atributos de seguridad asignados” en la página 207](#).

Antes de empezar

Debe asumir el rol `root`. Para obtener más información, consulte [“Cómo usar los derechos administrativos que tiene asignados” en la página 164](#).

1 Verifique y reinicie el servicio de nombres.

- a. Verifique que las asignaciones de seguridad para el usuario o el rol estén en el servicio de nombres que esté activado en el sistema.

```
# svccfg -s name-service/switch
svc:/system/name-service/switch> listprop config
config                                application
config/value_authorization           astring    solaris.smf.value.name-service.switch
config/default                       astring    files ldap
config/host                          astring    "files dns mdns ldap"
config/netgroup                      astring    ldap
config/printer                       astring    "user files"
```

En esta salida, todos los servicios que no se mencionan explícitamente heredan el valor predeterminado, `files ldap`. Por lo tanto, `passwd` (y por consiguiente `user_attr`), `auth_attr` y `prof_attr` se buscan primero en los archivos, luego en LDAP.

- b. Reinicie la caché del servicio de nombres, `svc:/system/name-service/cache`.

El daemon `nsd` puede tener un intervalo de tiempo de vida prolongado. Mediante el reinicio del daemon, actualiza el servicio de nombres con los datos actuales.

```
# svcadm restart name-service/cache
```

2 Determine dónde un atributo de seguridad se asigna al usuario.

Utilice el atributo de seguridad como el valor para el comando `userattr -v`. Por ejemplo, los siguientes comandos indican qué atributos de seguridad se asignan y cuándo la asignación se creó para el usuario `jdoe`:

```
# userattr -v audit_flags jdoe      Indicates modified system defaults
user_attr: fw:no
# userattr -v auths jdoe            Indicates no added auths
Basic Solaris User :solaris.mail.mailq,solaris.network.autoconf.read,
solaris.admin.wusb.read
Console User :solaris.system.shutdown,solaris.device.cdrw,
solaris.device.mount.removable,solaris.smf.manage.vbiosd,solaris.smf.value.vbiosd
# userattr -v defaultpriv jdoe      Indicates basic user privileges only
# userattr -v limitpriv jdoe        Indicates default limit privileges
# userattr -v lock_after_retries jdoe Indicates no automatic lockout
# userattr -v pam_policy jdoe       Assigned per-user PAM policy
# userattr -v profiles jdoe         Indicates assigned rights profiles
user_attr: Audit Review,Stop
# userattr roles jdoe               Assigned roles
user_attr : cryptomgt,infosec
```

La salida indica que `jdoe` tiene asignado directamente indicadores de auditoría, dos perfiles de derechos y dos roles. Por lo tanto, cualquier valor de indicador de auditoría en los perfiles de derechos no se tiene en cuenta. Después de asumir un rol, los indicadores de auditoría en ese rol reemplazan a los indicadores de auditoría para el usuario.

3 Verifique que las autorizaciones asignadas estén escritas correctamente.

El origen de una asignación de autorización no es importante, ya que las autorizaciones se acumulan para los usuarios. Sin embargo, una autorización mal escrita produce un error sin notificación.

4 Para perfiles de derechos que ha creado, compruebe que ha asignado los atributos de seguridad adecuados a los comandos en ese perfil.

Por ejemplo, algunos comandos necesitan `uid=0` en lugar de `euid=0` para que el proceso se realice con éxito. Además, las opciones para algunos comandos pueden necesitar autorizaciones.

5 Compruebe lo siguiente si los atributos de seguridad no están disponibles para un usuario.

a. Compruebe si los atributos de seguridad están asignados directamente al usuario.

Use el comando `userattr`, tal como se muestra en el [Paso 2](#).

b. Si los atributos de seguridad no están asignados directamente, compruebe los perfiles de derechos que están asignados directamente al usuario.

i. En orden, compruebe la asignación de atributos de seguridad en la lista de perfiles de derechos.

El valor del atributo en el primer perfil de derechos de la lista es el valor en el núcleo. Si este valor es incorrecto, cambie el valor de ese perfil de derechos o vuelva a asignar los perfiles en el orden correcto.

Para comandos con privilegios, compruebe si un privilegio se asigna a la palabra clave `defaultpriv` o se elimina de la palabra clave `limitpriv`.

ii. Si no se muestra ninguna asignación de atributos, compruebe los roles que el usuario tiene asignados.

Si el atributo está asignado a un rol, el usuario debe asumir el rol para obtener los atributos de seguridad. Si el atributo está asignado a más de un rol, la asignación en el primer rol de la lista está en vigor. Si este valor es incorrecto, asigne el valor correcto al primer rol de la lista o vuelva a asignar los roles en el orden correcto.

6 Si ha asignado un privilegio directamente a un usuario o rol, compruebe si un comando que falló requiere autorizaciones para que el proceso se realice con éxito.

a. Compruebe si una opción para el comando necesita autorización.

En lugar de asignar directamente un privilegio, asigne el privilegio al comando que lo requiere, agregue las autorizaciones necesarias, coloque el comando y las autorizaciones en un perfil de derechos y asigne el perfil al usuario.

b. Compruebe si existe un perfil de derechos que incluye la autorización necesaria.

Si existe, asigne el perfil al usuario. Ordene el perfil de derechos antes que cualquier otro perfil de derechos que incluye el comando.

7 Compruebe lo siguiente si un comando falla para un usuario.**a. Verifique que el usuario esté ejecutando el comando en un shell de perfil.**

Los comandos administrativos se deben ejecutar en un shell de perfil. Para mitigar errores del usuario, puede asignar un shell de perfil como el shell de inicio de sesión del usuario. También puede recordar al usuario que ejecute comandos administrativos en un shell de perfil.

b. Compruebe si alguno de los atributos de seguridad que están asignados directamente al usuario impiden que el comando se ejecute correctamente.

En concreto, compruebe los valores de los atributos `defaultpriv` y `limitpriv` del usuario.

c. Determine qué perfil de derechos o rol incluye el comando.**i. En orden, compruebe el comando con atributos de seguridad en la lista de perfiles de derechos.**

El primer valor de la lista de perfiles de derechos es el valor en el núcleo. Si este valor es incorrecto, cambie el valor de ese perfil de derechos o vuelva a asignar los perfiles en el orden correcto.

En concreto, compruebe los valores de los atributos `defaultpriv` y `limitpriv` del perfil.

ii. Si no se muestra ninguna asignación de atributos, compruebe los roles que el usuario tiene asignados.

Si el comando está asignado a un rol, el usuario debe asumir el rol para obtener los atributos de seguridad. Si el atributo está asignado a más de un rol, la asignación en el primer rol de la lista está en vigor. Si el valor es incorrecto, asigne el valor correcto al primer rol de la lista o vuelva a asignar los roles en el orden correcto.

8 Compruebe lo siguiente si un comando falla para un rol.

Los comandos administrativos requieren privilegios para ejecutarse con éxito. Las opciones para algunos comandos pueden necesitar autorización. Se recomienda asignar un perfil de derechos que incluye el comando administrativo.

a. Compruebe si alguno de los atributos de seguridad que están asignados directamente al rol impiden que el comando se ejecute correctamente.

En concreto, compruebe los valores de los atributos `defaultpriv` y `limitpriv` del rol.

b. En orden, compruebe el comando con atributos de seguridad en la lista de perfiles de derechos.

El primer valor de la lista de perfiles de derechos es el valor en el núcleo. Si este valor es incorrecto, cambie el valor de ese perfil de derechos o vuelva a asignar los perfiles en el orden correcto.

Gestión de RBAC (tareas)

Una vez que configura y usa RBAC, utilice los procedimientos siguientes para mantener y modificar RBAC en los sistemas.

Gestión de RBAC (mapa de tareas)

El siguiente mapa de tareas hace referencia a los procedimientos para mantener el control de acceso basado en roles (RBAC) después de la implementación inicial de RBAC.

Tarea	Descripción	Para obtener instrucciones
Cambiar la contraseña del rol.	El rol root cambia la contraseña del rol.	“Cómo cambiar la contraseña de un rol” en la página 187
Modificar los derechos asignados de un rol.	Modifica los atributos de seguridad de un rol.	“Cómo cambiar los atributos de seguridad de un rol” en la página 188 Ejemplo 9–26
Modificar un perfil de derechos.	Modifica valores de atributos de seguridad en un perfil de derechos, como privilegios límite y privilegios predeterminados.	Ejemplo 9–17 Ejemplo 9–8
Volver a ordenar la asignación de perfil de derechos.	Garantiza que los atributos de seguridad asignados están disponibles para un usuario o un rol.	“Cómo volver a ordenar atributos de seguridad asignados” en la página 189
Crear un shell de perfil restringido.	Impide que los usuarios o roles tengan acceso completo a todos los comandos en el software.	“Cómo restringir a un administrador a derechos asignados explícitamente” en la página 190
Restringir los privilegios de un usuario.	Limita el conjunto básico o límite de privilegios del usuario.	Ejemplo 9–8
Eliminar derechos predeterminados de un sistema.	Crea un sistema para usos especiales.	Ejemplo 9–28

Tarea	Descripción	Para obtener instrucciones
Permitir que un usuario proporcione la contraseña del usuario para asumir un rol.	Modifica los atributos de seguridad de un usuario para que la contraseña del usuario autentique el usuario para un rol. Este comportamiento es similar al comportamiento del rol de Linux.	“Cómo permitir que un usuario use su propia contraseña para asumir un rol” en la página 191
Cambiar el rol root a un usuario.	Antes de retirar un sistema, cambie el rol root a un usuario.	“Cómo cambiar el rol root a un usuario” en la página 192
Restringir las acciones del usuario en el escritorio.	Si bien estas acciones no requieren RBAC, proporcionan seguridad al sistema.	Capítulo 11, “Desactivación de funciones en el sistema Oracle Solaris Desktop” de <i>Guía del administrador de Oracle Solaris 11.1 Desktop</i>

Estos procedimientos gestionan atributos de seguridad en usuarios, roles y perfiles de derechos. Para conocer los procedimientos de gestión de usuario básico, consulte el [Capítulo 1, “Gestión de cuentas de usuario y entornos de usuario \(descripción general\)”](#) de *Gestión de las cuentas de usuario y los entornos de usuario en Oracle Solaris 11.1*.

▼ Cómo cambiar la contraseña de un rol

Debido a que un rol se puede asignar a varios usuarios, los usuarios a los que se asigna un rol no pueden cambiar la contraseña del rol.

Antes de empezar Debe asumir el rol root. Para obtener más información, consulte [“Cómo usar los derechos administrativos que tiene asignados” en la página 164](#).

● Ejecute el comando `passwd`.

```
# passwd [-r naming-service] rolename
```

`-r naming-service` Aplica el cambio de contraseña al repositorio `files` o `ldap`. El repositorio predeterminado es `files`. Si no especifica un repositorio, se cambia la contraseña en todos los repositorios.

`rolename` Nombre de un rol existente que desea modificar.

Para conocer más opciones de comandos, consulte la página del comando `man passwd(1)`.

Ejemplo 9–24 Cambio de contraseña de un rol

En este ejemplo, el rol root cambia la contraseña del rol `devmgt` local.

```
# passwd -r files devmgt
New password:      Type new password
Confirm password:  Retype new password
```

En este ejemplo, el rol root cambia la contraseña del rol devmgt en el servicio de directorios LDAP.

```
# passwd -r ldap devmgt
New password:      Type new password
Confirm password:  Retype new password
```

En este ejemplo, el rol root cambia la contraseña del rol devmgt en el archivo y LDAP.

```
# passwd devmgt
New password:      Type new password
Confirm password:  Retype new password
```

▼ Cómo cambiar los atributos de seguridad de un rol

Antes de empezar

Debe convertirse en un administrador con el perfil de derechos de seguridad de usuario asignado para cambiar la mayoría de los atributos de seguridad de un rol. Para asignar indicadores de auditoría o cambiar la contraseña de un rol, debe asumir el rol root. Para obtener más información, consulte [“Cómo usar los derechos administrativos que tiene asignados” en la página 164](#).

1 Utilice el comando `rolemod`.

Este comando modifica los atributos de un rol definido en el servicio de nombres local o en LDAP. Los valores de las opciones -A, -P y -R pueden ser modificados por - o +. El signo - indica que se va a restar el valor de los valores asignados actualmente. El signo + indica que se va a sumar el valor a los valores asignados actualmente.

Para obtener más información sobre el comando `rolemod`, consulte lo siguiente:

- Para obtener una descripción breve, consulte la descripción del comando `roleadd` en [“Cómo crear un rol” en la página 171](#).
- Para conocer todos los argumentos de este comando, consulte la página del comando `man rolemod(1M)`.
- Para obtener la lista de valores de claves para la opción -K, consulte la página del comando `man user_attr(4)`.

El siguiente comando agrega dos perfiles de derechos al rol devmgt en el repositorio LDAP:

```
$ rolemod -P +"Device Management,File Management" -S ldap devadmin
```

2 Para cambiar la contraseña del rol, consulte [“Cómo cambiar la contraseña de un rol” en la página 187](#).

Ejemplo 9–25 Cambio de los atributos de seguridad de un rol local

En este ejemplo, el administrador de seguridad modifica el rol `prtmgt` para incluir el perfil de derechos de gestión de VSCAN.

```
$ rolemod -c "Handles printers and virus scanning" \
-P "Printer Management,VSCAN Management,All" prtmgt
```

Ejemplo 9–26 Asignación de privilegios directamente a un rol

En este ejemplo, el administrador de seguridad confía al rol `system` un privilegio muy específico que afecta la hora del sistema.

```
$ rolemod -K defaultpriv='proc_clock_highres' system
```

Los valores de la palabra clave `defaultpriv` se encuentran en la lista de privilegios de los procesos del rol en todo momento.

▼ Cómo volver a ordenar atributos de seguridad asignados

Oracle Solaris lee perfiles de derechos en orden de asignación, como se describe en [“Orden de búsqueda para atributos de seguridad asignados” en la página 207](#). En este proceso, puede volver a ordenar perfiles de derechos.

Antes de empezar

Debe convertirse en un administrador con el perfil de derechos de seguridad de usuario asignado. Para obtener más información, consulte [“Cómo usar los derechos administrativos que tiene asignados” en la página 164](#).

1 Visualice la lista de perfiles de derechos asignados actualmente al usuario o al rol.

La lista se muestra en orden.

```
$ profiles username|rolename
```

2 Asigne los perfiles de derechos en el orden correcto.

```
$ usermod | rolemod -P "list-of-profiles"
```

Ejemplo 9–27 Asignación de perfiles de derechos en un orden específico

En este ejemplo, el administrador determina que un perfil de derechos con comandos con privilegios se muestra después del perfil de todos los derechos para el rol `devadmin`.

```
$ profiles devadmin
  Basic Solaris User
  All
  Device Management
```

Por lo tanto, el rol `devadmin` no puede ejecutar los comandos de gestión de dispositivo con sus privilegios asignados.

El administrador reasigna los perfiles de derechos para `devadmin`. Con el nuevo orden de asignación, `devadmin` puede ejecutar los comandos de dispositivo con sus privilegios asignados.

```
$ rolemod -P "Device Management,Basic Solaris User,All"
$ profiles devadmin
  Device Management
  Basic Solaris User
  All
```

▼ Cómo restringir a un administrador a derechos asignados explícitamente

Puede restringir un rol o un usuario a un número limitado de acciones administrativas de dos formas.

- Puede utilizar el perfil de derechos de detención.
El perfil de derechos de detención es la forma más sencilla de crear un shell restringido. Las autorizaciones y los perfiles de derechos que están asignados en el archivo `policy.conf` no se consultan. Por lo tanto, al rol o al usuario no se le asigna el perfil de derechos de usuario básico de Solaris, el perfil de derechos de usuario de consola ni la autorización `solaris.device.cdrw`.
- Puede modificar el archivo `policy.conf` en un sistema y requerir que el rol o el usuario utilice ese sistema para tareas administrativas.

Antes de empezar Debe asumir el rol `root`. Para obtener más información, consulte [“Cómo usar los derechos administrativos que tiene asignados” en la página 164](#).

- **Agregue el perfil de derechos de detención como el último perfil en la lista de perfiles que asigna.**

Por ejemplo, puede limitar al rol `auditrev` a realizar sólo revisiones de auditoría.

```
# rolemod -P "Audit Review,Stop" auditrev
```

Debido a que el rol `auditrev` no tiene el perfil de derechos de usuario de consola, el auditor no puede cerrar el sistema. Debido a que este rol no tiene la autorización `solaris.device.cdrw`, el auditor no puede leer o escribir en la unidad de CD-ROM. Debido a que este rol no tiene el perfil de derechos de usuario básico de Solaris, ningún comando que no sean los comandos en el

perfil de derechos de revisión de auditoría se puede ejecutar en este rol. Por ejemplo, el comando `ls` no se ejecutará. El rol utiliza el explorador de archivos para ver los archivos de auditoría.

Para obtener más información, consulte [“Perfiles de derechos” en la página 205](#) y [“Orden de búsqueda para atributos de seguridad asignados” en la página 207](#).

El comando `rolemod` modifica los atributos de un rol definido en el servicio de nombres local o en LDAP. Para conocer los argumentos de este comando, consulte la página del comando `man rolemod(1M)`. La lista de argumentos de RBAC es similar a la lista para el comando `roleadd`, como se describe en [“Cómo crear un rol” en la página 171](#).

Ejemplo 9–28 Modificación de un sistema para limitar los derechos disponibles a sus usuarios

En este ejemplo, el administrador crea un sistema que sólo es útil para administrar la red. El administrador elimina el perfil de derechos de usuario básico de Solaris y cualquier autorización del archivo `policy.conf`. El perfil de derechos de usuario de consola no se elimina. Las líneas afectadas en el archivo `policy.conf` resultante son las siguientes:

```
...
#AUTHS_GRANTED=
#PROFS_GRANTED=Basic Solaris User
CONSOLE_USER=Console User
...
```

Sólo un usuario que ha sido asignado de forma explícita autorizaciones, comandos o perfiles de derechos puede usar este sistema. Después de iniciar sesión, el usuario autorizado puede realizar tareas administrativas. Si el usuario autorizado se encuentra en la consola del sistema, el usuario tiene los derechos del usuario de consola.

▼ Cómo permitir que un usuario use su propia contraseña para asumir un rol

De manera predeterminada, los usuarios deben escribir la contraseña del rol para asumir un rol. Realice este procedimiento para que asumir un rol en Oracle Solaris sea similar a asumir un rol en un entorno Linux.

Antes de empezar Asume un rol que incluye el perfil de derechos de seguridad de usuario. Este rol no puede ser el rol cuyo valor `roleauth` desea cambiar.

- **Permita que una contraseña de usuario autentique un rol.**

```
$ rolemod -K roleauth=user rolename
```

Para asumir este rol, los usuarios asignados pueden usar ahora su propia contraseña, no la contraseña que se ha creado específicamente para el rol.

Ejemplo 9–29 Activación de un rol para utilizar la contraseña del usuario asignado al utilizar un perfil de derechos

En este ejemplo, el rol root cambia el valor de roleauth por el rol secadmin en el sistema local.

```
$ profiles -p "Local System Administrator"
profiles:Local System Administrator> set roleauth="user"
profiles:Local System Administrator> end
profiles:Local System Administrator> exit
```

Cuando un usuario al que se le asigna el perfil de derechos de administrador de seguridad desea asumir el rol, se le solicita una contraseña. En la secuencia siguiente, el nombre de rol es secadmin:

```
% su - secadmin
Password:      Type user password
$              /** You are now in a profile shell with administrative rights**/
```

Si se le han asignado otros roles, el usuario tiene su propia contraseña para autenticarse ante esos roles también.

Ejemplo 9–30 Cambio del valor de roleauth por un rol en el repositorio LDAP

En este ejemplo, el rol root permite a todos los usuarios que pueden asumir el rol secadmin utilizar su propia contraseña al asumir un rol. Esta capacidad se concede a estos usuarios para todos los sistemas que están gestionados por el servidor LDAP.

```
# rolemod -S ldap -K roleauth=user secadmin
```

Errores más frecuentes

Si se establece roleauth=user para el rol, la contraseña de usuario permite que el rol autenticado acceda a todos los derechos que están asignados a ese rol. La palabra clave depende de la búsqueda. Para obtener más información, consulte [“Orden de búsqueda para atributos de seguridad asignados” en la página 207](#).

▼ Cómo cambiar el rol root a un usuario

Un administrador puede cambiar root a un usuario al retirar un sistema que se ha eliminado de la red. En esta instancia, iniciar sesión en el sistema como root simplifica la limpieza.

Antes de empezar Debe convertirse en root. Para obtener más información, consulte [“Cómo usar los derechos administrativos que tiene asignados” en la página 164.](#)

1 Elimine la asignación del rol root de los usuarios locales.

Por ejemplo, elimine la asignación de rol de dos usuarios.

```
% su - root
Password: a!2@3#4$5%6^7
# roles jdoe
root
# roles kdoe
root
# roles ldoe
secadmin
# usermod -R "" jdoe
# usermod -R "" kdoe
#
```

2 Cambie el rol root a un usuario.

```
# rolemod -K type=normal root
```

Los usuarios que están actualmente en el rol root lo siguen estando. Otros usuarios que tienen acceso de usuario root pueden cambiar su a root o pueden iniciar sesión en el sistema como el usuario root.

3 Verifique el cambio.

Puede utilizar uno de los siguientes comandos.

```
# getent user_attr root
root:::auths=solaris.*;profiles=All;audit_flags=lo\:no;lock_after_retries=no;
min_label=admin_low;clearance=admin_high
```

Si falta la palabra clave type en la salida o es igual a normal, la cuenta no es un rol.

```
# userattr type root
```

Si la salida está vacía o muestra normal, la cuenta no es un rol.

Ejemplo 9–31 Prevención de que el rol root se utilice para configurar un sistema

En este ejemplo, la política de seguridad del sitio requiere que se evite que la cuenta root mantenga el sistema. El administrador ha creado y probado los roles que mantienen el sistema. Estos roles incluyen cada perfil de seguridad y el perfil de derechos de administrador del sistema. Se ha asignado a un usuario de confianza un rol que puede restaurar una copia de seguridad. Ningún rol puede cambiar los indicadores de auditoría para el sistema, un usuario o un perfil de derechos.

Para evitar que la cuenta root se utilice para mantener el sistema, el administrador de seguridad elimina la asignación del rol root. Debido a que la cuenta root debe poder iniciar sesión en el sistema en modo de un solo usuario, la cuenta retiene una contraseña.

```
# usermod -K roles= jdoe
# userattr roles jdoe
```

Ejemplo 9–32 Cambio de usuario root a rol root

En este ejemplo, el usuario root devuelve el usuario root a un rol.
Primero, el usuario root cambia la cuenta root a un rol y verifica el cambio.

```
# usermod -K type=role root
# getent user_attr root
root:::type=role;auths=solaris.*;profiles=All;audit_flags=lo\:no;
lock_after_retries=no;min_label=admin_low;clearance=admin_high
```

A continuación, root asigna el rol root a un usuario local.

```
# usermod -R root jdoe
```

Errores más frecuentes

En un entorno de escritorio, no puede iniciar sesión directamente como root cuando root es un rol. Un mensaje de diagnóstico indica que root es un rol en el sistema.

Si no tiene una cuenta local que pueda asumir el rol root, cree una. Como root, inicie sesión en el sistema en el modo de un solo usuario, cree una cuenta de usuario local y una contraseña, y asigne el rol root a la nueva cuenta. A continuación, inicie sesión como el nuevo usuario y asuma el rol root.

Uso de privilegios (tareas)

Los privilegios pueden permitir a los usuarios realizar tareas específicas con derechos administrativos. Los privilegios también se pueden utilizar para limitar a los usuarios a que realicen solamente las tareas que pueden llevar a cabo.

El siguiente mapa de tareas hace referencia a instrucciones paso a paso para ver privilegios, gestionar y usar privilegios en el sistema.

Tarea	Descripción	Para obtener instrucciones
Ver los privilegios definidos.	Enumera los privilegios y sus definiciones en Oracle Solaris.	“Cómo enumerar los privilegios en el sistema” en la página 195
Ver los privilegios como usuario en cualquier shell.	Muestra sus privilegios directamente asignados. Todos sus procesos se ejecutan con estos privilegios.	“Cómo determinar los privilegios que se le asignaron directamente” en la página 196

Tarea	Descripción	Para obtener instrucciones
Ver los comandos con privilegios en un shell de perfil.	Muestra los comandos con privilegios que puede ejecutar mediante un perfil de derechos asignado.	“Cómo determinar los comandos con privilegios que puede ejecutar” en la página 198
Limite el acceso de agresores a un sistema cuando se ejecuta con éxito un ataque sobre una aplicación.	Protege un sistema contra ataques aplicando la política de privilegio extendida al puerto NTP.	“Cómo aplicar una política de privilegio extendida a un puerto” en la página 202
Determinar los privilegios que hay en un proceso.	Muestra el conjunto vigente, heredable, permitido y límite de privilegios de un proceso.	“Cómo determinar los privilegios de un proceso” en la página 199
Determinar los privilegios que faltan en un proceso.	Muestra los privilegios que un proceso con errores necesita para ejecutarse correctamente.	“Cómo determinar los privilegios que necesita un programa” en la página 201
Limite el acceso de agresores a un sistema cuando se ejecuta con éxito un ataque sobre una aplicación.	Crea una política extendida para el servicio NTP.	“Cómo aplicar una política de privilegio extendida a un puerto” en la página 202
Agregar privilegios a un comando.	Agrega privilegios a un comando en un perfil de derechos. El perfil de derechos se puede asignar a usuarios o roles. Los usuarios luego pueden ejecutar el comando con los privilegios asignados en un shell de perfil.	Ejemplo 9–18
Asignar privilegios a un usuario o rol.	Amplía el conjunto heredable de privilegios de un usuario o rol. Utilice este procedimiento con precaución.	Ejemplo 9–9
Restringir los privilegios de un usuario.	Limita el conjunto básico de privilegios del usuario. Utilice este procedimiento con precaución.	Ejemplo 9–16
Ejecutar una secuencia de comandos de shell con privilegios.	Agrega privilegios a una secuencia de comandos de shell y a los comandos de la secuencia de comandos de shell. A continuación, ejecuta la secuencia de comandos en un shell de perfil.	“Cómo ejecutar una secuencia de comandos de shell con comandos con privilegios” en la página 203

▼ Cómo enumerar los privilegios en el sistema

El procedimiento siguiente muestra cómo visualizar los nombres y las definiciones de privilegios.

- En una ventana de terminal, puede ver privilegios en línea.
 - Enumere todos los privilegios mediante la visualización de la página del comando **man privileges(5)**.

```
% man privileges
Standards, Environments, and Macros           privileges(5)

NAME
  privileges - process privilege model
...
  The defined privileges are:

  PRIV_CONTRACT_EVENT

      Allow a process to request reliable delivery of events
      to an event endpoint.

      Allow a process to include events in the critical event
      set term of a template which could be generated in
      volume by the user.
...
```

Este formato de privilegio es utilizado por desarrolladores.

- Enumere los privilegios mediante el comando **ppriv**.

```
% ppriv -lv | more
contract_event
    Allows a process to request critical events without limitation.
    Allows a process to request reliable delivery of all events on
    any event queue.
...
win_upgrade_sl
    Allows a process to set the sensitivity label of a window
    resource to a sensitivity label that dominates the existing
    sensitivity label.
    This privilege is interpreted only if the system is configured
    with Trusted Extensions.
```

Este formato de privilegio se utiliza para asignar privilegios a usuarios y roles con los comandos **useradd**, **roleadd**, **usermod** y **rolemod**, y a perfiles de derechos con el comando **profiles**.

▼ Cómo determinar los privilegios que se le asignaron directamente

El siguiente procedimiento muestra cómo determinar si se le asignaron privilegios directamente.



Precaución – El uso inadecuado de los privilegios asignados directamente puede generar infracciones de seguridad involuntarias. Para ver una explicación, consulte [“Consideraciones de seguridad al asignar directamente atributos de seguridad”](#) en la página 143.

1 Enumere los privilegios que los procesos pueden utilizar.

Consulte [“Cómo determinar los privilegios de un proceso”](#) en la página 199 para conocer el procedimiento.

2 Invoque acciones y ejecute comandos en cualquier shell.

Los privilegios que se muestran en el conjunto vigente están en vigor a lo largo de la sesión. Si se le asignaron privilegios directamente, además del conjunto básico, los privilegios se muestran en el conjunto vigente.

Ejemplo 9–33 Determinación de los privilegios asignados directamente

En este ejemplo, se ha asignado el privilegio `proc_clock_highres` directamente al usuario, por lo que el privilegio está disponible en todos los procesos que son propiedad del usuario.

```
% ppriv -v $$
1800:  pfksh
flags = <none>
      E: file_link_any,...,proc_clock_highres,proc_session
      I: file_link_any,...,proc_clock_highres,proc_session
      P: file_link_any,...,proc_clock_highres,proc_session
      L: cpc_cpu,dtrace_kernel,dtrace_proc,dtrace_user,...,sys_time
% ppriv -vl proc_clock_highres
      Allows a process to use high resolution timers.
```

Ejemplo 9–34 Determinación de los privilegios asignados directamente de un rol

En el siguiente ejemplo, al rol `realtime` se le asignaron privilegios directamente para gestionar los programas relacionados con la fecha y hora.

```
% su - realtime
Password:  <Type realtime password>
$ ppriv -v $$
1600:  pfksh
flags = <none>
      E: file_link_any,...,proc_clock_highres,proc_session,sys_time
      I: file_link_any,...,proc_clock_highres,proc_session,sys_time
      P: file_link_any,...,proc_clock_highres,proc_session,sys_time
      L: cpc_cpu,dtrace_kernel,dtrace_proc,dtrace_user,...,sys_time
```

▼ Cómo determinar los comandos con privilegios que puede ejecutar

Por lo general, los usuarios y los roles tienen acceso a comandos con privilegios mediante un perfil de derechos. Los comandos de un perfil de derechos se deben ejecutar en un shell de perfil.

1 Determine los perfiles de derechos que se le asignaron.

En el siguiente ejemplo, se asigna al usuario varios perfiles de derechos. El sistema lee los perfiles de derechos y su contenido en orden. Para todos los atributos excepto las autorizaciones, el primer valor de atributo definido explícitamente es el que se utiliza. Para obtener más información, consulte [“Orden de búsqueda para atributos de seguridad asignados” en la página 207.](#)

```
% profiles
Audit Review
Console User
Suspend To RAM
Suspend To Disk
Brightness
CPU Power Management
Network Autoconf
Desktop Print Management
Network Wifi Info
Desktop Removable Media User
Basic Solaris User
All
```

2 Determine sus derechos del perfil de revisión de auditoría.

```
profiles -l
Audit Review

solaris.audit.read

/usr/sbin/auditreduce  euid=0
/usr/sbin/auditstat   euid=0
/usr/sbin/praudit     euid=0
```

El perfil de derechos de revisión de auditoría permite ejecutar los comandos `auditreduce`, `auditstat` y `praudit` con el UID efectivo de 0, y le asigna la autorización `solaris.audit.read`.

Ejemplo 9–35 Determinación de comandos con privilegios de un rol

En este ejemplo, un usuario asume un rol asignado y enumera los comandos que se incluyen en uno de los perfiles de derechos.

```
% roles
devadmin
% su - devadmin
Password:      Type devadmin password
$ profiles -l
```

```

Device Security
    /usr/bin/kbd          uid=0;gid=sys
    /usr/sbin/add_allocatable  euid=0
    /usr/sbin/add_drv        uid=0
    /usr/sbin/devfsadm        uid=0
    /usr/sbin/eeprom          uid=0
    /usr/sbin/list_devices    euid=0
    /usr/sbin/rem_drv         uid=0
    /usr/sbin/remove_allocatable  euid=0
    /usr/sbin/strace          euid=0
    /usr/sbin/update_drv      uid=0

```

Ejemplo 9–36 Ejecución de los comandos con privilegios en su rol

En el siguiente ejemplo, el rol `admin` puede cambiar los permisos en el archivo `useful.script`.

```

% whoami
jdoe
% ls -l useful.script
-rwxr-xr-- 1 elsee eng 262 Apr 2 10:52 useful.script
% chgrp admin useful.script
chgrp: useful.script: Not owner
% su - admin
Password:      <Type admin password>
$ chgrp admin useful.script
$ chown admin useful.script
$ ls -l useful.script
-rwxr-xr-- 1 admin admin 262 Apr 2 10:53 useful.script

```

▼ Cómo determinar los privilegios de un proceso

Este procedimiento muestra cómo determinar los privilegios que están disponibles para los procesos. La lista no incluye privilegios que se asignaron a comandos específicos.

● Enumere los privilegios que están disponibles para el proceso del shell.

```
% ppriv [-v] pid
```

pid El número de proceso. Utilice un signo de dólar doble (\$\$) para transferir el número de proceso del shell principal al comando.

-v Proporciona una lista detallada de los nombres de privilegios.

Ejemplo 9–37 Determinación de los privilegios en el shell actual

En el siguiente ejemplo, se enumeran los privilegios del proceso principal del shell del usuario. En el segundo ejemplo, se enumeran los nombres completos de los privilegios. Las letras individuales que se visualizan hacen referencia a los siguientes conjuntos de privilegios:

- E El conjunto vigente de privilegios.
- I El conjunto heredable de privilegios.
- P El conjunto permitido de privilegios.
- L El conjunto límite de privilegios.

```
% ppriv $$
1200:  -csh
flags = <none>
      E: basic
      I: basic
      P: basic
      L: all

% ppriv -v $$
1200:  -csh
flags = <none>
      E: file_link_any,net_access,proc_exec,proc_fork,proc_info,proc_session
      I: file_link_any,net_access,proc_exec,proc_fork,proc_info,proc_session
      P: file_link_any,net_access,proc_exec,proc_fork,proc_info,proc_session
      L: cpc_cpu,dtrace_kernel,dtrace_proc,dtrace_user,...,sys_time
```

Ejemplo 9–38 Determinación de los privilegios de un rol que puede asumir

En el siguiente ejemplo, el rol sysadmin no tiene privilegios asignados directamente.

```
% su - sysadmin
Password:  <Type sysadmin password>
$ /usr/bin/whoami
sysadmin
$ ppriv -v $$
1400:  pfksh
flags = <none>
      E: file_link_any,file_read,file_write,net_access,proc_exec,proc_fork,
        proc_info,proc_session
      I: file_link_any,file_read,file_write,net_access,proc_exec,proc_fork,
        proc_info,proc_session
      P: file_link_any,file_read,file_write,net_access,proc_exec,proc_fork,
        proc_info,proc_session
      L: cpc_cpu,dtrace_kernel,dtrace_proc,dtrace_user,...,win_upgrade_sl
```

▼ Cómo determinar los privilegios que necesita un programa

Antes de empezar

El comando o proceso debe fallar para que este procedimiento de depuración funcione.

- 1 **Escriba el comando con errores como un argumento del comando de depuración `ppriv`.**

```
% ppriv -eD touch /etc/acct/yearly
touch[5245]: missing privilege "file_dac_write"
(euid = 130, syscall = 224) needed at zfs_zaccess+0x258
touch: cannot create /etc/acct/yearly: Permission denied
```

- 2 **Para determinar qué llamada del sistema falla, busque el número `syscall` en el archivo `/etc/name_to_sysnum`.**

```
% grep 224 /etc/name_to_sysnum
creat64                224
```

Ejemplo 9-39 Utilización del comando `truss` para examinar el uso de privilegios

El comando `truss` puede depurar el uso de privilegios en un shell común. Por ejemplo, el siguiente comando depura el proceso con errores `touch`:

```
% truss -t creat touch /etc/acct/yearly
creat64("/etc/acct/yearly", 0666)
Err#13 EACCES [file_dac_write]
touch: /etc/acct/yearly cannot create
```

Las interfaces ampliadas `/proc` informan el privilegio faltante después del código de error en la salida del comando `truss`.

Ejemplo 9-40 Utilización del comando `ppriv` para examinar el uso de privilegios en un shell de perfil

En este ejemplo, el usuario `jdoe` puede asumir el rol `objadmin`. El rol `objadmin` incluye el perfil de derechos de gestión de acceso a objetos. Este perfil de derechos permite al rol `objadmin` cambiar permisos en archivos que no son propiedad de `objadmin`.

En el fragmento siguiente, `jdoe` no puede cambiar los permisos en el archivo `useful.script`:

```
jdoe% ls -l useful.script
-rw-r--r-- 1 aloa staff 2303 Apr 10 10:10 useful.script
jdoe% chown objadmin useful.script
chown: useful.script: Not owner
jdoe% ppriv -eD chown objadmin useful.script
chown[11444]: missing privilege "file_chown"
(euid = 130, syscall = 16) needed at zfs_zaccess+0x258
chown: useful.script: Not owner
```

Cuando jdoe asume el rol objadmin, se modifican los permisos en el archivo:

```
jdoe% su - objadmin
Password: <Type objadmin password>
$ ls -l useful.script
-rw-r--r-- 1 aloa staff 2303 Apr 10 10:10 useful.script
$ chown objadmin useful.script
$ ls -l useful.script
-rw-r--r-- 1 objadmin staff 2303 Apr 10 10:10 useful.script
$ chgrp admin useful.script
$ ls -l objadmin.script
-rw-r--r-- 1 objadmin admin 2303 Apr 10 10:11 useful.script
```

Ejemplo 9–41 Modificación de un archivo que es propiedad del usuario root

Este ejemplo ilustra la protección contra la escalada de privilegios. Para ver una explicación, consulte [“Cómo evitar la escalada de privilegios” en la página 217](#). El archivo es propiedad del usuario root. El rol menos poderoso, el rol objadmin, necesita todos los privilegios para cambiar la propiedad del archivo, por lo que la operación no se ejecuta correctamente.

```
jdoe% su - objadmin
Password: <Type objadmin password>
$ cd /etc; ls -l system
-rw-r--r-- 1 root sys 1883 Oct 10 10:20 system
$ chown objadmin system
chown: system: Not owner
$ ppriv -eD chown objadmin system
chown[11481]: missing privilege "ALL"
(euid = 101, syscall = 16) needed at zfs_zaccess+0x258
chown: system: Not owner
```

▼ Cómo aplicar una política de privilegio extendida a un puerto

El servicio para el protocolo de hora de red (NTP) utiliza el puerto con privilegios 123 para el tráfico udp. Este procedimiento protege otros puertos del acceso por parte de usuarios malintencionados que podrían obtener los privilegios asignados a este puerto.

1 Lea la entrada de manifiesto de servicio predeterminada para el puerto.

Desde la siguiente entrada `/lib/svc/manifest/network/ntp.xml`, los privilegios `net_privaddr`, `proc_lock_memory` y `sys_time` pueden utilizarse en otros procesos.

```
privileges='basic,!file_link_any,!proc_info,!proc_session,
net_privaddr,proc_lock_memory,sys_time'
```

Los privilegios eliminados evitan que el servicio indique u observe cualquier otro proceso, y evitan la creación de enlaces físicos como una manera de renombrar archivos.

Es decir, el proceso que inicia el servicio solamente se puede enlazar con el puerto específico 123, y no se puede enlazar con ningún otro puerto con privilegios. Si un pirata informático quisiera aprovechar el servicio para iniciar otro proceso, el proceso secundario no podría establecer un enlace a ningún otro puerto con privilegios.

2 Limite el privilegio `net_privaddr` a este puerto solamente.

La política de privilegio extendida, que aparece resaltada en el siguiente fragmento, impide el acceso de este servicio a otros puertos con privilegios:

```
privileges='basic,!file_link_any,!proc_info,!proc_session,
{net_privaddr}:123/udp,proc_lock_memory,sys_time'
```

▼ Cómo ejecutar una secuencia de comandos de shell con comandos con privilegios

Al crear una secuencia de comandos de shell que ejecuta comandos que requieren privilegios, el perfil de derechos adecuado debe contener los comandos con privilegios asignados a ellos.

Antes de empezar

Debe asumir el rol root. Para obtener más información, consulte [“Cómo usar los derechos administrativos que tiene asignados” en la página 164](#).

1 Inicie la secuencia de comandos con `/bin/pfsh`, o cualquier otro shell de perfil, en la primera línea.

```
#!/bin/pfsh
# Copyright (c) 2012 by Oracle
```

2 Determine los privilegios que necesitan los comandos de la secuencia de comandos.

```
% ppriv -eD script-full-path
```

3 Conviértase en administrador con los atributos de seguridad necesarios.

Para obtener más información, consulte [“Cómo usar los derechos administrativos que tiene asignados” en la página 164](#).

4 Cree o modifique un perfil de derechos para la secuencia de comandos.

Agregue la secuencia de comandos de shell y los comandos en la secuencia de comandos de shell con sus atributos de seguridad necesarios al perfil de derechos. Para conocer los pasos, consulte [“Cómo crear un perfil de derechos” en la página 175](#).

5 Agregue el perfil de derechos a un rol y asigne el rol a un usuario.

Para ejecutar la secuencia de comandos, el usuario asume el rol y ejecuta la secuencia de comandos en el shell de perfil del rol.

- Para agregar un perfil de derechos a un rol, consulte [“Cómo cambiar los atributos de seguridad de un rol” en la página 188](#).
- Para asignar el rol a un usuario, consulte [“Cómo cambiar los atributos de seguridad de un usuario” en la página 162](#).

Atributos de seguridad en Oracle Solaris (referencia)

En este capítulo, se proporciona material de referencia sobre RBAC y privilegios:

- “Perfiles de derechos” en la página 205
- “Orden de búsqueda para atributos de seguridad asignados” en la página 207
- “Autorizaciones” en la página 208
- “Bases de datos RBAC” en la página 209
- “Comandos de RBAC” en la página 213
- “Comandos administrativos para la gestión de privilegios” en la página 215
- “Archivos con información de privilegios” en la página 216
- “Privilegios y auditoría” en la página 217
- “Cómo evitar la escalada de privilegios” en la página 217
- “Aplicaciones antiguas y el modelo de privilegios” en la página 218

Para obtener más información sobre el uso de RBAC, consulte el [Capítulo 9, “Uso del control de acceso basado en roles \(tareas\)”](#). Para obtener información general, consulte “Control de acceso basado en roles (descripción general)” en la página 131.

Para utilizar privilegios, consulte “Uso de privilegios (tareas)” en la página 194. Para obtener información general, consulte “Privilegios (descripción general)” en la página 144.

Perfiles de derechos

En esta sección, se describen algunos perfiles de derechos típicos. Los perfiles de derechos son colecciones útiles de autorizaciones y otros atributos de seguridad, comandos con atributos de seguridad y perfiles de derechos suplementarios. Oracle Solaris proporciona muchos perfiles de derechos. Si no son suficientes para sus necesidades, puede modificar los existentes y crear otros nuevos.

Los perfiles de derechos deben estar asignados en orden, del más al menos potente. Para obtener más información, consulte “Orden de búsqueda para atributos de seguridad asignados” en la página 207.

- **Perfil de derechos de administrador del sistema:** proporciona un perfil que puede realizar la mayoría de las tareas que no están relacionadas con la seguridad. Este perfil incluye varios perfiles diferentes para crear un rol poderoso. Tenga en cuenta que el perfil de derechos "todos" se asigna al final de la lista de perfiles de derechos complementarios. El comando `profiles` muestra los contenidos del perfil.

% `profiles -p "System Administrator" info`

- **Perfil de derechos de operador:** proporciona capacidades limitadas para gestionar archivos y medios sin conexión. Este perfil incluye perfiles de derechos complementarios para crear un rol simple. El comando `profiles` muestra los contenidos del perfil.

% `profiles -p Operator info`

- **Perfil de derechos de gestión de impresoras:** proporciona un número limitado de comandos y autorizaciones para gestionar la impresión. Este perfil es uno de los tantos perfiles que abarcan una sola área de administración. El comando `profiles` muestra los contenidos del perfil.

% `profiles -p "Printer Management" info`

- **Perfil de derechos de usuario de Solaris básico:** permite a los usuarios utilizar el sistema dentro de los límites de la política de seguridad. Este perfil aparece de manera predeterminada en el archivo `policy.conf`. Tenga en cuenta que la comodidad que ofrece el perfil de derechos de usuario de Solaris básico debe equilibrarse con los requisitos de seguridad del sitio. Es posible que los sitios que necesitan una seguridad más estricta prefieran eliminar este perfil del archivo `policy.conf` o asignar el perfil de derechos de detención. El comando `profiles` muestra los contenidos del perfil.

% `profiles -p "Basic Solaris User" info`

- **Perfil de derechos de usuario de la consola:** para el propietario de la estación de trabajo, proporciona acceso a autorizaciones, comandos y acciones para la persona sentada en el equipo. El comando `profiles` muestra los contenidos del perfil.

% `profiles -p "Console User" info`

- **Perfil de derechos "todos":** para los roles, proporciona acceso a los comandos que no tienen atributos de seguridad. Este perfil puede ser apropiado para los usuarios con derechos limitados. El comando `profiles` muestra los contenidos del perfil.

% `profiles -p All info`

- **Perfil de derechos de detención:** es un perfil de derechos especial que detiene la evaluación de otros perfiles. Este perfil impide la evaluación de las variables `AUTHS_GRANTED`, `PROFS_GRANTED` y `CONSOLE_USER` en el archivo `policy.conf`. Con este perfil, puede proporcionar a roles y a usuarios un shell de perfil restringido.

Nota – El perfil de detención afecta la asignación de privilegios indirectamente. Los perfiles que se enumeran posteriormente al perfil de detención no se evalúan. Por lo tanto, los comandos con privilegios en esos perfiles no están vigentes. Para utilizar este perfil, consulte [“Cómo restringir a un administrador a derechos asignados explícitamente” en la página 190.](#)

El comando `profiles` muestra los contenidos del perfil.

% **profiles -p Stop info**

Cada perfil de derechos tiene un archivo de ayuda asociado. Los archivos de ayuda están en formato HTML y se pueden personalizar. Los archivos residen en el directorio `/usr/lib/help/profiles/locale/C.`

Visualización del contenido de los perfiles de derechos

Dispone de tres vistas en los contenidos de perfiles de derechos.

- El comando `getent` le permite visualizar los contenidos de todos los perfiles de derechos en el sistema. Para ver una salida de ejemplo, consulte [“Cómo visualizar todos los atributos de seguridad definidos” en la página 157.](#)
- El comando `profiles -p "Profile Name" info` le permite visualizar los contenidos de un perfil de derechos específico.
- El comando `profiles -laccount-name` le permite visualizar los contenidos de los perfiles de derechos asignados a un usuario o rol específico.

Para obtener más información, consulte las páginas del comando `man getent(1M)` y `profiles(1)`.

Orden de búsqueda para atributos de seguridad asignados

A un usuario o rol se pueden asignar atributos de seguridad directamente o mediante un perfil de derechos. El orden de búsqueda afecta el valor de atributo de seguridad que se debe utilizar. Se utiliza el valor de la primera instancia encontrada del atributo.

Nota – El orden de autorizaciones no es importante. Las autorizaciones son acumulativas.

Cuando un usuario inicia sesión, los atributos de seguridad se asignan en el siguiente orden de búsqueda:

- **Atributos de seguridad** que se asignan al usuario con los comandos `useradd` y `usermod`. Para obtener una lista, consulte [“Base de datos `user\_attr`” en la página 210](#).
- **Perfiles de derechos** que se asignan al usuario con los comandos `useradd` y `usermod`. Estas asignaciones se buscan en orden.
El orden es el primer perfil de la lista, luego su respectiva lista de perfiles de derechos; el segundo perfil de la lista, luego su respectiva lista de perfiles, y así sucesivamente. La primera instancia de un valor es el que el sistema utiliza, excepto para los valores `auths`, que son acumulativos. Los atributos en los perfiles de derechos incluyen todos los atributos de seguridad para los usuarios y perfiles suplementarios. Para obtener una lista, consulte [“Base de datos `user\_attr`” en la página 210](#).
- Valor de **perfil de derechos de usuario de la consola**. Para obtener una descripción, consulte [“Perfiles de derechos” en la página 205](#).
- Si se asigna el **perfil de derechos de detención**, la evaluación de los atributos de seguridad se detiene. No se asignan atributos después de que se asigna el perfil de detención. El perfil de detención se evalúa después del perfil de derechos de usuario de la consola y antes de otros atributos de seguridad en el archivo `policy.conf`, incluido `AUTHS_GRANTED`. Para obtener una descripción, consulte [“Perfiles de derechos” en la página 205](#).
- Valor de **perfil de derechos de usuario de Solaris básico** en el archivo `policy.conf`.
- Valor `AUTHS_GRANTED` en el archivo `policy.conf`.
- Valor `PROFS_GRANTED` en el archivo `policy.conf`.
- Valor `PRIV_DEFAULT` en el archivo `policy.conf`.
- Valor `PRIV_LIMIT` en el archivo `policy.conf`.

Autorizaciones

Una *autorización* RBAC es un derecho perfectamente definido que se puede otorgar a un rol o a un usuario. Las aplicaciones compatibles con RBAC comprueban las autorizaciones antes de que un usuario obtenga acceso a la aplicación u operaciones específicas dentro de la aplicación.

Las autorizaciones son a nivel de usuario, por lo tanto se pueden ampliar. Puede escribir un programa que requiere autorización, agregar las autorizaciones al sistema, crear un perfil de derechos para estas autorizaciones y asignar el perfil de derechos a los usuarios o a los roles que tienen permiso de utilizar el programa.

Convenciones de denominación de autorizaciones

Una autorización tiene un nombre que se utiliza internamente. Por ejemplo, `solaris.system.date` es el nombre de una autorización. Una autorización tiene una

descripción breve, que aparece en las interfaces gráficas de usuario (GUI). Por ejemplo, Set Date & Time es la descripción de la autorización `solaris.system.date`.

Por convención, todos los nombres de autorizaciones constan del orden inverso del nombre del proveedor en Internet, el área temática, las subáreas y la función. Las partes del nombre de la autorización están separados por puntos. Un ejemplo sería `com.xyzcorp.device.access`. Las excepciones a esta convención son las autorizaciones de Oracle, que utilizan el prefijo `solaris` en lugar de un nombre de Internet. La convención de denominación permite a los administradores aplicar autorizaciones de un modo jerárquico. Un carácter comodín (*) puede representar cualquier cadena a la derecha de un punto.

Como un ejemplo de cómo se utilizan las autorizaciones, tenga en cuenta lo siguiente: el perfil de derechos de seguridad de enlaces de red sólo tiene la autorización `solaris.network.link.security`, en cambio, el perfil de derechos seguridad de la red tiene el perfil de derechos de seguridad de enlaces de red como un perfil suplementario, además de las autorizaciones `solaris.network.*` y `solaris.smf.manage.ssh`.

Autoridad de delegación en autorizaciones

Una autorización que finaliza con el sufijo `delegate` permite a un usuario o rol delegar a otros usuarios las autorizaciones asignadas que comienzan con el mismo prefijo.

La autorización `solaris.auth.delegate` permite a un usuario o rol delegar a otros usuarios cualquier autorización que estos usuarios o roles tengan asignada.

Por ejemplo un rol con las autorizaciones `solaris.auth.delegate` y `solaris.network.wifi.wep` puede delegar la autorización `solaris.network.wifi.wep` a otro usuario o rol.

Bases de datos RBAC

Las siguientes bases de datos almacenan los datos de los elementos de RBAC:

- **Base de datos de atributos de usuario extendidos** (`user_attr`): asocia usuarios y roles con autorizaciones, privilegios, palabras clave y perfiles de derechos.
- **Base de datos de atributos de perfil de derechos** (`prof_attr`): define perfiles de derechos, enumera autorizaciones asignadas de perfiles, privilegios y palabras clave, e identifica el archivo de ayuda asociado.
- **Base de datos de atributos de autorización** (`auth_attr`): define autorizaciones y sus atributos, e identifica el archivo de ayuda asociado.
- **Base de datos de atributos de ejecución** (`exec_attr`): identifica los comandos con atributos de seguridad que están asignados a perfiles de derechos específicos.

La base de datos `policy.conf` contiene autorizaciones, privilegios y perfiles de derechos que se aplican a todos los usuarios. Para obtener más información, consulte [“Archivo `policy.conf`” en la página 212](#).

Bases de datos de RBAC y servicios de nombres

El ámbito del servicio de nombres de las bases de datos RBAC se define en el servicio SMF para el cambio de servicio de nombres, `svc:/system/name-service/switch`. Las propiedades de este servicio para las bases de datos RBAC son `auth_attr`, `password` y `prof_attr`. La propiedad `password` establece la precedencia del servicio de nombres para las bases de datos `passwd` y `user_attr`. La propiedad `prof_attr` establece la precedencia del servicio de nombres para las bases de datos `prof_attr` y `exec_attr`.

En la siguiente salida, no se muestran las entradas `auth_attr`, `password` y `prof_attr`. Por lo tanto, las bases de datos RBAC utilizan el servicio de nombres `files`.

```
# svccfg -s name-service/switch listprop config
config                                application
config/value_authorization           astring      solaris.smf.value.name-service.switch
config/default                       astring      files
config/host                           astring      "files ldap dns"
config/printer                       astring      "user files ldap"
```

Base de datos `user_attr`

La base de datos `user_attr` contiene información de usuarios y roles que complementa las bases de datos `passwd` y `shadow`.

Los siguientes atributos de seguridad se pueden configurar mediante los comandos `roleadd`, `rolemod`, `useradd`, `usermod` y `profiles`:

- Para un usuario, la palabra clave `roles` asigna uno o más roles definidos.
- Para un rol, el valor `user` para la palabra clave `roleauth` permite al rol autenticar con la contraseña de usuario en lugar de con la contraseña del rol. De manera predeterminada, el valor es `role`.
- Para un usuario o rol, se pueden establecer los siguientes atributos:
 - Palabra clave `audit_flags`: modifica la máscara de auditoría. Para obtener información de referencia, consulte la página del comando `man audit_flags(5)`.
 - Palabra clave `auths`: asigna autorizaciones. Para obtener información de referencia, consulte la página del comando `man auths(1)`.
 - Palabra clave `defaultpriv`: agrega privilegios o los elimina del conjunto de privilegios básico predeterminado. Para obtener información de referencia, consulte [“Cómo se implementan los privilegios” en la página 148](#).

- Palabra clave `limitpriv`: agrega privilegios o los elimina del conjunto de privilegios límite predeterminado. Para obtener información de referencia, consulte [“Cómo se implementan los privilegios” en la página 148](#).
Estos privilegios están siempre en vigencia, no son atributos de un comando. Para obtener información de referencia, consulte la página del comando `man privileges(5)` y [“Cómo se implementan los privilegios” en la página 148](#).
- Palabra clave `project`: agrega un proyecto predeterminado. Para obtener información de referencia, consulte la página del comando `man project(4)`.
- Palabra clave `lock_after_retries`: si el valor es `yes`, el sistema se bloquea después de que el número de intentos exceda el número permitido en el archivo `/etc/default/login`.
- Palabra clave `profiles`: asigna perfiles de derechos.

Para obtener más información, consulte la página del comando `man user_attr(4)`. Para ver los contenidos de esta base de datos, utilice el comando `getent user_attr`. Para obtener más información, consulte la página del comando `man getent(1M)` y [“Cómo visualizar todos los atributos de seguridad definidos” en la página 157](#).

Base de datos `auth_attr`

Todas las autorizaciones se almacenan en la base de datos `auth_attr`. Las autorizaciones se pueden asignar a usuarios, roles o perfiles de derechos. El método preferido es colocar las autorizaciones en un perfil de derechos, incluir el perfil en la lista de perfiles de un rol y, a continuación, asignar el rol a un usuario.

Para ver los contenido de esta base de datos, utilice el comando `getent auth_attr`. Para obtener más información, consulte la página del comando `man getent(1M)` y [“Cómo visualizar todos los atributos de seguridad definidos” en la página 157](#).

Base de datos `prof_attr`

La base de datos `prof_attr` almacena el nombre, la descripción, la ubicación del archivo de ayuda, los privilegios y las autorizaciones que se asignan a los perfiles de derechos. Los comandos y los atributos de seguridad que se asignan a los perfiles de derechos se almacenan en la base de datos `exec_attr`. Para obtener más información, consulte [“Base de datos `exec\_attr`” en la página 212](#).

Para obtener más información, consulte la página del comando `man prof_attr(4)`. Para ver los contenidos de esta base de datos, utilice el comando `getent exec_attr`. Para obtener más información, consulte la página del comando `man getent(1M)` y [“Cómo visualizar todos los atributos de seguridad definidos” en la página 157](#).

Base de datos `exec_attr`

La base de datos `exec_attr` define los comandos que requieren atributos de seguridad para ejecutarse correctamente. Los comandos forman parte de un perfil de derechos. Un comando con sus atributos de seguridad puede ser ejecutado por los roles o usuarios a los que se asignó el perfil.

Para obtener más información, consulte la página del comando `man exec_attr(4)`. Para ver los contenido de esta base de datos, utilice el comando `getent`. Para obtener más información, consulte la página del comando `man getent(1M)` y [“Cómo visualizar todos los atributos de seguridad definidos” en la página 157](#).

Archivo `policy.conf`

El archivo `policy.conf` ofrece una manera de otorgar perfiles de derechos específicos, autorizaciones específicas y privilegios específicos a todos los usuarios. Las entradas pertinentes del archivo constan de pares *key=value*:

- `AUTHS_GRANTED=authorizations`: hace referencia a una o varias autorizaciones.
- `PROFS_GRANTED=rights profiles`: hace referencia a uno o varios perfiles de derechos.
- `CONSOLE_USER=Console User`: hace referencia al perfil de derechos de usuario de la consola. Este perfil se proporciona con un conjunto útil de autorizaciones para el usuario de la consola. Puede personalizar este perfil. Para ver los contenidos del perfil, consulte [“Perfiles de derechos” en la página 205](#).
- `PRIV_DEFAULT=privileges`: hace referencia a uno o varios privilegios.
- `PRIV_LIMIT=privileges`: hace referencia a todos los privilegios.

El siguiente ejemplo muestra algunos valores típicos de una base de datos `policy.conf`:

```
# grep AUTHS /etc/security/policy
AUTHS_GRANTED=solaris.device.cdrw

# grep PROFS /etc/security/policy
PROFS_GRANTED=Basic Solaris User

# grep PRIV /etc/security/policy

#PRIV_DEFAULT=basic
#PRIV_LIMIT=all
```

Para obtener más información sobre los privilegios, consulte [“Privilegios \(descripción general\)” en la página 144](#).

Comandos de RBAC

Esta sección muestra los comandos que se utilizan para administrar RBAC. También se incluye una tabla de los comandos cuyo acceso se puede controlar mediante autorizaciones.

Comandos que gestionan RBAC

Los siguientes comandos recuperan y establecen información de RBAC.

TABLA 10-1 Comandos de administración de RBAC

Página del comando man	Descripción
auths(1)	Muestra las autorizaciones de un usuario.
getent(1M)	Interfaz que muestra los contenidos de las bases de datos <code>user_attr</code> , <code>prof_attr</code> y <code>exec_attr</code> .
nscd(1M)	Daemon de caché de servicio de nombres, útil para el almacenamiento en la caché de las bases de datos <code>user_attr</code> , <code>prof_attr</code> y <code>exec_attr</code> . Utilice el comando <code>svcadm</code> para reiniciar el daemon.
pam_roles(5)	Módulo de gestión de cuentas de rol para PAM. Comprueba la autorización para asumir el rol.
pfedit(1M)	Se usa para que usuarios no root editen los sistemas de archivos cuando tienen asignada la autorización <code>solaris.admin.edit/path-to-system-file</code> .
pfexec(1)	Utilizado por los shells de perfil para ejecutar los comandos con atributos de seguridad especificados en la base de datos <code>exec_attr</code> .
policy.conf(4)	Archivo de configuración para la política de seguridad del sistema. Enumera las autorizaciones otorgadas, los privilegios concedidos y otra información de seguridad.
profiles(1)	Muestra perfiles de derechos para un usuario determinado. Crea o modifica un perfil de derechos en un sistema local o una red LDAP.
roles(1)	Muestra los roles que un usuario específico puede asumir.
roleadd(1M)	Agrega un rol a un sistema local o a una red LDAP.
roleadd(1M)	Agrega un rol a un sistema local o a una red LDAP.
rolemod(1M)	Modifica las propiedades de un rol en un sistema local o en una red LDAP.
userattr(1)	Muestra el valor de un derecho específico asignado a una cuenta de rol o usuario.
useradd(1M)	Agrega una cuenta de usuario al sistema o a una red LDAP. La opción <code>-R</code> asigna un rol a la cuenta de un usuario.
userdel(1M)	Suprime el inicio de sesión de un usuario del sistema o de una red LDAP.

TABLA 10-1 Comandos de administración de RBAC (Continuación)

Página del comando man	Descripción
usermod(1M)	Modifica las propiedades de la cuenta de un usuario en el sistema.

Comandos seleccionados que requieren autorizaciones

La siguiente tabla proporciona ejemplos acerca de cómo las autorizaciones se utilizan para limitar las opciones de comandos en un sistema Oracle Solaris. Para ver una explicación más detallada de las autorizaciones, consulte [“Autorizaciones” en la página 208](#).

TABLA 10-2 Comandos y autorizaciones asociadas

Página del comando man	Requisitos de autorización
at(1)	<code>solaris.jobs.user</code> se requiere para todas las opciones (cuando no existen los archivos <code>at.allow</code> ni <code>at.deny</code>).
atq(1)	<code>solaris.jobs.admin</code> se requiere para todas las opciones.
cdrw(1)	<code>solaris.device.cdrw</code> se requiere para todas las opciones y se otorga de manera predeterminada en el archivo <code>policy.conf</code> .
crontab(1)	<code>solaris.jobs.user</code> se requiere para la opción que permite ejecutar un trabajo (cuando no existen los archivos <code>crontab.allow</code> ni <code>crontab.deny</code>). <code>solaris.jobs.admin</code> se requiere para las opciones que permiten mostrar o modificar los archivos <code>crontab</code> de otros usuarios.
allocate(1)	<code>solaris.device.allocate</code> (u otra autorización, según se especifique en el archivo <code>device_allocate</code>) se requiere para asignar un dispositivo. <code>solaris.device.revoke</code> (u otra autorización, según se especifique en el archivo <code>device_allocate</code>) se requiere para asignar un dispositivo a otro usuario (opción <code>-F</code>).
deallocate(1)	<code>solaris.device.allocate</code> (u otra autorización, según se especifique en el archivo <code>device_allocate</code>) se requiere para desasignar el dispositivo de otro usuario. <code>solaris.device.revoke</code> (u otra autorización, según se especifique en el archivo <code>device_allocate</code>) se requiere para forzar la desasignación del dispositivo especificado (opción <code>-F</code>) o de todos los dispositivos (opción <code>-I</code>).
list_devices(1)	<code>solaris.device.revoke</code> se requiere para mostrar los dispositivos de otro usuario (opción <code>-U</code>).
roleadd(1M)	<code>solaris.user.manage</code> se requiere para crear un rol. <code>solaris.account.activate</code> se requiere para establecer una contraseña inicial. <code>solaris.account.setpolicy</code> se requiere para establecer una política de contraseñas, como el bloqueo de cuentas y la caducidad de las contraseñas.

TABLA 10-2 Comandos y autorizaciones asociadas (Continuación)

Página del comando man	Requisitos de autorización
roledel(1M)	La autorización <code>solaris.passwd.assign</code> se requiere para suprimir la contraseña.
rolemod(1M)	La autorización <code>solaris.passwd.assign</code> se requiere para cambiar la contraseña. <code>solaris.account.setpolicy</code> se requiere para modificar la política de contraseñas, como el bloqueo de cuentas y la caducidad de las contraseñas.
sendmail(1M)	<code>solaris.mail</code> se requiere para acceder a las funciones del subsistema de correo; <code>solaris.mail.mailq</code> se requiere para ver la cola de correo.
useradd(1M)	<code>solaris.user.manage</code> se requiere para crear un usuario. <code>solaris.account.activate</code> se requiere para definir la contraseña inicial. <code>solaris.account.setpolicy</code> se requiere para definir la política de contraseñas, como el bloqueo de cuentas y la caducidad de las contraseñas.
userdel(1M)	La autorización <code>solaris.passwd.assign</code> se requiere para suprimir la contraseña.
usermod(1M)	La autorización <code>solaris.passwd.assign</code> se requiere para cambiar la contraseña. <code>solaris.account.setpolicy</code> se requiere para modificar la política de contraseñas, como el bloqueo de cuentas y la caducidad de las contraseñas.

Con privilegios

Los procesos que restringen privilegios se implementan en el núcleo y pueden restringir los procesos a nivel de comando, de usuario, de rol o de sistema.

Comandos administrativos para la gestión de privilegios

La siguiente tabla muestra los comandos que están disponibles para gestionar privilegios.

TABLA 10-3 Comandos para la gestión de privilegios

Finalidad	Comando	Página de comando man
Examinar privilegios de proceso	<code>ppriv -v pid</code>	ppriv(1)
Definir privilegios de proceso	<code>ppriv -s spec</code>	
Enumerar los privilegios del sistema	<code>ppriv -l</code>	
Enumerar un privilegio y su descripción	<code>ppriv -lv priv</code>	
Agregar política de privilegio extendido a un UID, proceso, o puerto.	<code>ppriv -r rule</code>	Use -X para eliminar la política. privileges(5)

TABLA 10-3 Comandos para la gestión de privilegios (Continuación)

Finalidad	Comando	Página de comando man
Mostrar política de privilegio extendido a un UID, proceso, o puerto.	<code>ppriv -lv extended-policy</code>	ppriv(1)
Depurar error en privilegio	<code>ppriv -eD failed-operation</code>	
Asignar privilegios a un usuario nuevo	<code>useradd</code>	useradd(1M)
Agregar privilegios a un usuario existente	<code>usermod</code>	usermod(1M)
Asignar privilegios a un perfil de derechos	<code>profiles</code>	profiles(1)
Asignar privilegios a un rol nuevo	<code>roleadd</code>	roleadd(1M)
Agregar privilegios a un rol existente	<code>rolemod</code>	rolemod(1M)
Ver política de dispositivos	<code>getdevpolicy</code>	getdevpolicy(1M)
Definir política de dispositivos	<code>devfsadm</code>	devfsadm(1M)
Actualizar política de dispositivos en dispositivos abiertos	<code>update_drv -p policy driver</code>	update_drv(1M)
Agregar política de dispositivos a un dispositivo	<code>add_drv -p policy driver</code>	add_drv(1M)

Archivos con información de privilegios

Los siguientes archivos contienen información sobre privilegios.

TABLA 10-4 Archivos que contienen información de privilegios

Archivo y página del comando man	Información sobre privilegios	Descripción
/etc/security/policy.conf policy.conf(4)	<code>PRIV_DEFAULT</code>	Conjunto heredable de privilegios para el sistema
	<code>PRIV_LIMIT</code>	Conjunto límite de privilegios para el sistema
syslog.conf syslog.conf(4)	Archivo de registro del sistema para mensajes de depuración	Registro de depuración de privilegios
	Ruta definida en la entrada <code>priv.debug</code>	

Privilegios y auditoría

El uso de privilegios se puede auditar. Cada vez que un proceso utiliza un privilegio, el uso del privilegio se registra en la pista de auditoría, en el token de auditoría `upriv`. Cuando los nombres de privilegios forman parte del registro, se utiliza su representación textual. Los siguientes eventos de auditoría registran el uso del privilegio:

- **Evento de auditoría** `AUE_SETPPRIV`: el evento genera un registro de auditoría cuando se modifica un conjunto de privilegios. El evento de auditoría `AUE_SETPPRIV` está en la clase `pm`.
- **Evento de auditoría** `AUE_MODALLOCPRIV`: el evento de auditoría genera un registro de auditoría cuando se agrega un privilegio desde afuera del núcleo. El evento de auditoría `AUE_MODALLOCPRIV` está en la clase `ad`.
- **Evento de auditoría** `AUE_MODDEVPLCY`: el evento de auditoría genera un registro de auditoría cuando se modifica la política de dispositivos. El evento de auditoría `AUE_MODDEVPLCY` está en la clase `ad`.
- **Evento de auditoría** `AUE_PFEXEC`: el evento de auditoría genera un registro de auditoría cuando se realiza una llamada a `execve()` con `pfexec()` activada. El evento de auditoría `AUE_PFEXEC` está en las clases de auditoría `as`, `ex`, `ps` y `ua`. Los nombres de los privilegios se incluyen en el registro de auditoría.

El uso correcto de privilegios que se encuentran en el conjunto básico no se audita. El intento de utilizar un privilegio básico que se eliminó del conjunto básico de un usuario se audita.

Cómo evitar la escalada de privilegios

El núcleo impide la *escalada de privilegios*. La escalada de privilegios se produce cuando un privilegio permite a un proceso realizar más tareas de las que debe hacer. Para evitar que un proceso obtenga más privilegios de los que debe tener, las modificaciones vulnerables del sistema requieren el conjunto completo de privilegios. Por ejemplo, un archivo o un proceso que es propiedad de `root` (`UID=0`) sólo puede ser modificado por un proceso con el conjunto completo de privilegios. La cuenta `root` no requiere privilegios para modificar un archivo que es propiedad de `root`. Sin embargo, un usuario que no es `root` debe tener todos los privilegios para modificar un archivo que es propiedad de `root`.

De modo similar, las operaciones que proporcionan acceso a dispositivos requieren todos los privilegios del conjunto vigente.

Los privilegios `file_chown_self` y `proc_owner` están sujetos a la escalada de privilegios. El privilegio `file_chown_self` permite a un proceso delegar sus archivos. El privilegio `proc_owner` permite a un proceso inspeccionar los procesos que no son de su propiedad.

El privilegio `file_chown_self` está limitado por la variable del sistema `rstchown`. Cuando la variable `rstchown` se define en cero, el privilegio `file_chown_self` se elimina del conjunto heredable inicial del sistema y de todos los usuarios. Para obtener más información sobre la variable del sistema `rstchown`, consulte la página del comando `man chown(1)`.

El privilegio `file_chown_self` se asigna de forma más segura a un comando concreto, se coloca en un perfil y se asigna a un rol para su uso en un shell de perfil.

El privilegio `proc_owner` no es suficiente para cambiar un UID de proceso a 0. Para cambiar un proceso de cualquier UID a `UID=0`, se requieren todos los privilegios. Como el privilegio `proc_owner` otorga acceso de lectura sin restricciones a todos los archivos del sistema, el privilegio se asigna de forma más segura a un comando concreto, se coloca en un perfil y se asigna a un rol para su uso en un shell de perfil.



Precaución – La cuenta de un usuario se puede modificar para incluir el privilegio `file_chown_self` o el privilegio `proc_owner` en el conjunto heredable inicial del usuario. Debe tener un motivo de seguridad importante para colocar esos privilegios tan poderosos en el conjunto heredable de privilegios para cualquier usuario, rol o sistema.

Para obtener detalles sobre cómo se evita la escalada de privilegios para los dispositivos, consulte [“Privilegios y dispositivos” en la página 152](#).

Aplicaciones antiguas y el modelo de privilegios

Para adaptarse a las aplicaciones antiguas, la implementación de privilegios funciona con el modelo de superusuario y el modelo de privilegios. El núcleo realiza automáticamente un seguimiento del indicador `PRIV_AWARE`, que señala que un programa se ha diseñado para trabajar con privilegios. Piense en un proceso secundario que no reconoce privilegios. Los privilegios que se heredaron del proceso principal están disponibles en el conjunto permitido y el conjunto vigente del proceso secundario. Si el proceso secundario define un UID en 0, es posible que el proceso secundario no tenga capacidades completas de superusuario. El conjunto vigente y el conjunto permitido del proceso están restringidos a los privilegios del conjunto límite del proceso secundario. Por lo tanto, el conjunto límite de un proceso que reconoce privilegios restringe los privilegios raíz de los procesos secundarios que no reconocen privilegios.

P A R T E I V

Servicios criptográficos

En esta sección se describen las funciones de tecnología de clave pública y criptográficas centralizadas que proporciona Oracle Solaris.

- Capítulo 11, “Estructura criptográfica (descripción general)”
- Capítulo 12, “Estructura criptográfica (tareas)”
- Capítulo 13, “Estructura de gestión de claves”

Estructura criptográfica (descripción general)

En este capítulo, se describe la función de estructura criptográfica de Oracle Solaris y se tratan los siguientes temas:

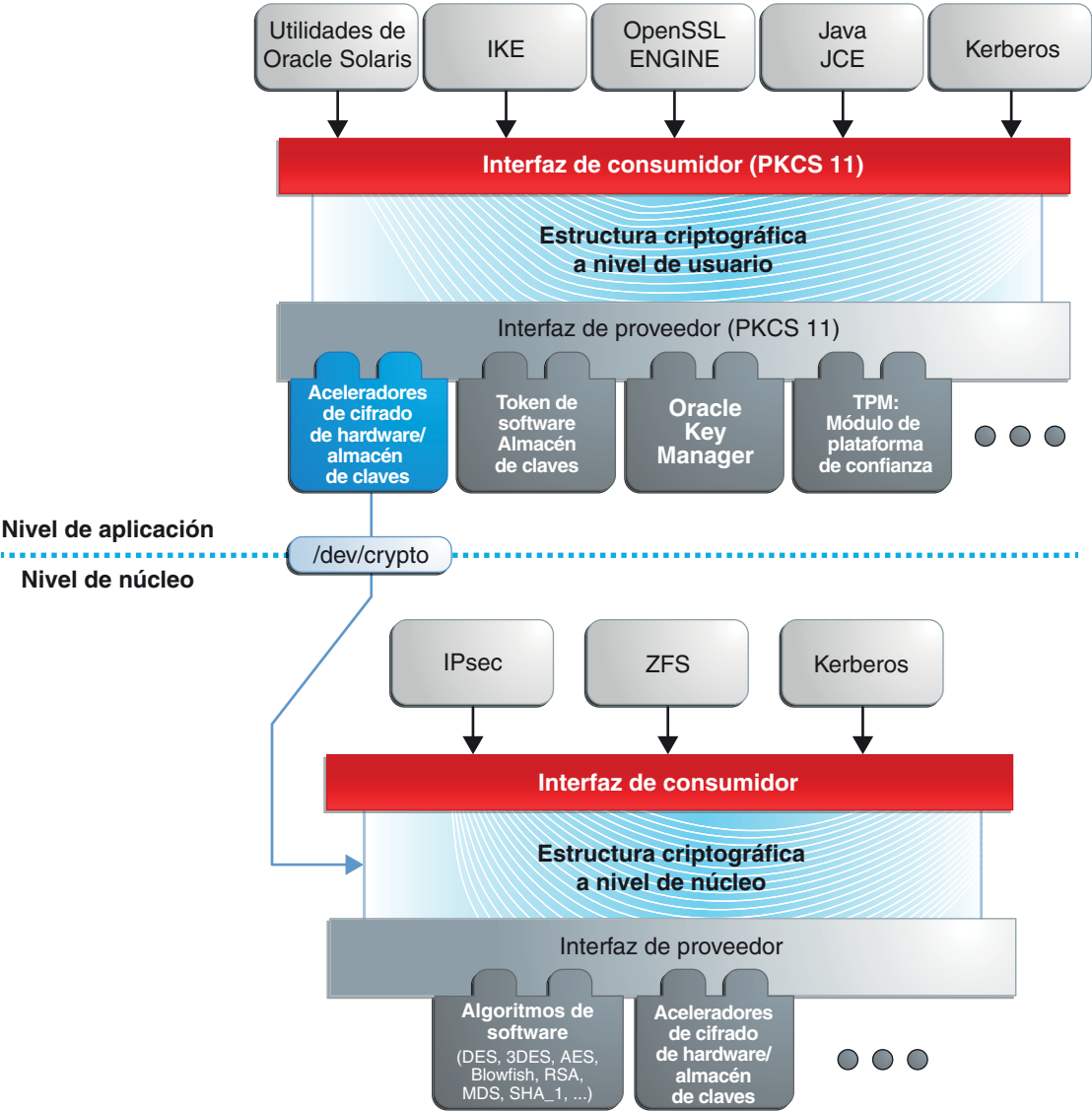
- “Introducción a la estructura criptográfica” en la página 221
- “Terminología de la estructura criptográfica” en la página 223
- “Ámbito de la estructura criptográfica” en la página 225
- “Zonas y servicios criptográficos” en la página 227
- “Estructura criptográfica y FIPS-140” en la página 228
- “Estructura criptográfica y servidores SPARC T-Series en esta versión” en la página 228

Para administrar y utilizar la estructura criptográfica, consulte el [Capítulo 12, “Estructura criptográfica \(tareas\)”](#).

Introducción a la estructura criptográfica

La estructura criptográfica proporciona un almacén común de algoritmos y bibliotecas PKCS #11 para manejar los requisitos criptográficos. Las bibliotecas PKCS #11 se implementan según el estándar siguiente: RSA Security Inc. PKCS #11 Cryptographic Token Interface (Cryptoki).

FIGURA 11-1 Niveles de estructura criptográfica



En el nivel de núcleo, la estructura actualmente maneja los requisitos criptográficos para Kerberos e IPsec. Los consumidores de nivel de usuario incluyen `libsasl` e IKE. El proxy de SSL de núcleo (`kssl`) utiliza la estructura criptográfica. Para obtener más información, consulte “Proxy SSL en el nivel del núcleo cifra las comunicaciones con el servidor web” de *Protección de la red en Oracle Solaris 11.1* y la página del comando `man ksslcfg(1M)`.

La ley de exportación de los Estados Unidos exige que el uso de interfaces criptográficas abiertas sea bajo licencia. La estructura criptográfica cumple con la ley actual mediante la solicitud de que los proveedores criptográficos de núcleo y los proveedores criptográficos de PKCS #11 estén registrados. Para obtener más información, consulte [“Firmas binarias para software de terceros” en la página 227](#).

La estructura permite a los *proveedores* de servicios criptográficos que muchos *consumidores* utilicen sus servicios en Oracle Solaris. Otro nombre para los proveedores es *complementos*. La estructura permite tres tipos de complementos:

- **Complementos de nivel de usuario:** objetos compartidos que prestan servicios mediante bibliotecas PKCS #11, como `pkcs11_softtoken.so.1`.
- **Complemento de nivel de núcleo:** módulos de núcleo que proporcionan implementaciones de algoritmos criptográficos en software, como [AES](#).

Muchos de los algoritmos de la estructura están optimizados para x86 con el conjunto de instrucciones SSE2 y para hardware SPARC.

- **Complementos de hardware:** controladores de dispositivos y sus aceleradores de hardware asociados. Los chips Niagara, los controladores de dispositivos `n2cp` y `nnp`, son un ejemplo. Un acelerador de hardware descarga funciones criptográficas que consumen muchos recursos del sistema operativo. La placa Sun Crypto Accelerator 6000 es un ejemplo.

La estructura implementa una interfaz estándar, la biblioteca PKCS #11, v2.20 enmienda 3, para proveedores de nivel de usuario. La biblioteca puede ser utilizada por aplicaciones de terceros para acceder a los proveedores. Terceros también pueden agregar bibliotecas registradas, módulos de algoritmos de núcleo registrados y controladores de dispositivos registrados a la estructura. Estos complementos se agregan cuando la utilidad `pkgadd` instala el software de terceros. Para ver un diagrama de los componentes principales de la estructura, consulte el [Capítulo 8, “Introduction to the Oracle Solaris Cryptographic Framework” de *Developer’s Guide to Oracle Solaris 11 Security*](#).

Terminología de la estructura criptográfica

La siguiente lista de definiciones y ejemplos es útil para trabajar con la estructura criptográfica.

- **Algoritmos:** algoritmos criptográficos. Estos son procedimientos informáticos establecidos y recursivos que cifran la entrada o le aplican hash. Los algoritmos de cifrado pueden ser simétricos o asimétricos. Los algoritmos simétricos utilizan la misma clave para el cifrado y el descifrado. Los algoritmos asimétricos, que se utilizan en la criptografía de claves públicas, necesitan dos claves. Las funciones de hashing también son algoritmos.

Ejemplos de algoritmos:

- Algoritmos simétricos, como AES y ARCFOUR
- Algoritmos asimétricos, como Diffie-Hellman y RSA
- Funciones de hashing, como MD5

- **Consumidores:** usuarios de los servicios criptográficos prestados por los proveedores. Los consumidores pueden ser aplicaciones, usuarios finales u operaciones de núcleo.

Ejemplos de consumidores:

- Aplicaciones, como IKE
- Usuarios finales, como un usuario común que ejecuta el comando `encrypt`
- Operaciones de núcleo, como IPsec
- **Almacén de claves:** en la estructura criptográfica, es el almacenamiento persistente para los objetos de token (se suele utilizar indistintamente con **token**). Para obtener información sobre un almacén de claves reservado, consulte **Metarranura** en esta lista de definiciones.
- **Mecanismo:** es la aplicación de un modo de un algoritmo para un fin particular.
Por ejemplo, un mecanismo DES que se aplica a la autenticación, como CKM_DES_MAC, es un mecanismo distinto de un mecanismo DES que se aplica al cifrado, CKM_DES_CBC_PAD.
- **Metarranura:** es una ranura única que presenta una unión de las capacidades de otras ranuras que se cargan en la estructura. La metarranura facilita la tarea de manejar todas las capacidades de los proveedores que están disponibles mediante la estructura. Cuando una aplicación que utiliza la metarranura solicita una operación, la metarranura averigua qué ranura debe realizar la operación. Las capacidades de la metarranura son configurables, pero no se requiere configuración. La metarranura está activada de manera predeterminada. Para configurar la metarranura, consulte la página del comando `man cryptoadm(1M)`.
La metarranura no tiene su propio almacén de claves. En su lugar, la metarranura se reserva el uso de un almacén de claves a partir de las ranuras reales en la estructura criptográfica. De manera predeterminada, la metarranura se reserva el almacén de claves Sun Crypto Soft token. El almacén de claves que utiliza la metarranura no se muestra como una de las ranuras disponibles.
Los usuarios pueden especificar un almacén de claves alternativo para la metarranura mediante la configuración de las variables de entorno `_${METASLOT_OBJECTSTORE_SLOT}` y `_${METASLOT_OBJECTSTORE_TOKEN}` o mediante la ejecución del comando `cryptoadm`. Para obtener más información, consulte las páginas del comando `man libpkcs11(3LIB)`, `pkcs11_softtoken(5)` y `cryptoadm(1M)`.
- **Modo:** es una versión de un algoritmo criptográfico. Por ejemplo, CBC (Cipher Block Chaining) es un modo distinto de ECB (Electronic Code Book). El algoritmo AES tiene dos modos, CKM_AES_ECB y CKM_AES_CBC.
- **Política:** es la elección, por parte de un administrador, de qué mecanismos estarán disponibles para su uso. De manera predeterminada, todos los proveedores y todos los mecanismos están disponibles para su uso. La desactivación de cualquier mecanismo sería una aplicación de la política. La activación de un mecanismo desactivado también sería una aplicación de la política.
- **Proveedores:** servicios criptográficos que utilizan los consumidores. Los proveedores se conectan a la estructura, por lo que también se denominan *complementos*.

Ejemplos de proveedores:

- Bibliotecas PKCS #11, como `pkcs11_softtoken.so`
- Módulos de los algoritmos criptográficos, como `aes` y `arcfour`
- Controladores de dispositivos y aceleradores de hardware asociados, como el controlador `mca` para Sun Crypto Accelerator 6000
- **Ranura:** es una interfaz de uno o más dispositivos criptográficos. Cada ranura, que corresponde a un lector físico o a otra interfaz de dispositivo, puede contener un token. Un token proporciona una vista lógica de un dispositivo criptográfico en la estructura.
- **Token:** en una ranura, un token proporciona una vista lógica de un dispositivo criptográfico en la estructura.

Ámbito de la estructura criptográfica

La estructura proporciona comandos para los administradores, los usuarios y los desarrolladores que suministran proveedores:

- **Comandos administrativos:** el comando `cryptoadm` proporciona un subcomando `list` para mostrar los proveedores disponibles y sus capacidades. Los usuarios comunes pueden ejecutar los comandos `cryptoadm list` y `cryptoadm --help`.

Para todos los demás subcomandos `cryptoadm` es necesario que asuma un rol que incluya el perfil de derechos de gestión de criptografía o que se convierta en superusuario. Los subcomandos como `disable`, `install` y `uninstall` están disponibles para administrar la estructura. Para obtener más información, consulte la página del comando `man cryptoadm(1M)`.

El comando `svcadm` se utiliza para gestionar el daemon `kcfd` y para actualizar la política criptográfica en el núcleo. Para obtener más información, consulte la página del comando `man svcadm(1M)`.

- **Comandos de nivel de usuario:** los comandos `digest` y `mac` proporcionan servicios de integridad de archivos. Los comandos `encrypt` y `decrypt` protegen los archivos contra intrusos. Para utilizar estos comandos, consulte “[Protección de archivos con la estructura criptográfica \(mapa de tareas\)](#)” en la página 229.

Comandos administrativos de la estructura criptográfica

El comando `cryptoadm` administra una estructura criptográfica en ejecución. El comando forma parte del perfil de derechos de gestión de criptografía. Este perfil se puede asignar a un rol para una administración segura de la estructura criptográfica. El comando `cryptoadm` gestiona lo siguiente:

- Visualización de información del proveedor de servicios criptográficos
- Desactivación o activación de mecanismos del proveedor
- Desactivación o activación de la metarranura

El comando `svcadm` se utiliza para activar, refrescar y desactivar el daemon de servicios criptográficos, `kcf.d`. Este comando forma parte de la función de utilidad de gestión de servicios (SMF) de Oracle Solaris. `svc:/system/cryptosvcs` es la instancia de servicio para la estructura criptográfica. Para obtener más información, consulte las páginas del comando `man smf(5)` y `svcadm(1M)`.

Comandos de nivel de usuario de la estructura criptográfica

La estructura criptográfica proporciona comandos de nivel de usuario para comprobar la integridad de los archivos, cifrar archivos y descifrar archivos. Un comando independiente, `elfsign`, permite a los proveedores registrar archivos binarios para utilizarlos en la estructura.

- Comando `digest` : procesa un [resumen de mensaje](#) para uno o varios archivos o para `stdin`. Un resumen es útil para verificar la integridad de un archivo. [SHA1](#) y [MD5](#) son ejemplos de funciones de resumen.
- Comando `mac` : procesa un [código de autenticación de mensajes \(MAC\)](#) para uno o varios archivos o para `stdin`. Un MAC asocia datos con un mensaje autenticado. Un MAC le permite a un receptor verificar que el mensaje provenga del remitente y no haya sido alterado. Los mecanismos `sha1_mac` y `md5_hmac` pueden procesar un MAC.
- Comando `encrypt`: cifra los archivos o `stdin` con un cifrado simétrico. El comando `encrypt -l` muestra los algoritmos que están disponibles. Los mecanismos incluidos en una biblioteca de nivel de usuario están disponibles para el comando `encrypt`. La estructura proporciona mecanismos AES, DES, 3DES (Triple-DES) y ARCFOUR para el cifrado del usuario.
- Comando `decrypt`: descifra archivos o `stdin` que se cifraron con el comando `encrypt`. El comando `decrypt` utiliza la misma clave y el mismo mecanismo que se utilizaron para cifrar el archivo original.

Firmas binarias para software de terceros

El comando `elfsign` proporciona un medio para firmar los proveedores que se utilizarán en la estructura criptográfica. Normalmente, este comando es ejecutado por el desarrollador de un proveedor.

El comando `elfsign` tiene subcomandos para solicitar un certificado, firmar binarios y verificar la firma en un binario. Los archivos binarios no registrados no pueden ser utilizados por la estructura criptográfica. Los proveedores que tengan binarios firmados verificables pueden utilizar la estructura.

Complementos de la estructura criptográfica

Los terceros pueden conectar sus proveedores a la estructura criptográfica. Un proveedor de terceros puede ser uno de los siguientes objetos:

- Biblioteca compartida PKCS #11
- Módulo de software de núcleo cargable, como un algoritmo de cifrado, una función MAC o una función de resumen
- Controlador de dispositivo de núcleo para un acelerador de hardware

Los objetos de un proveedor se deben firmar con un certificado de Oracle. La solicitud de certificados se basa en una clave privada que un tercero selecciona y un certificado que proporciona Oracle. La solicitud de certificado se envía a Oracle, que registra al tercero y, a continuación, expide el certificado. El tercero, a continuación, registra su objeto de proveedor con el certificado de Oracle.

Los módulos de software de núcleo cargables y los controladores de dispositivos de núcleo para aceleradores de hardware también se deben registrar en el núcleo. El registro se lleva a cabo mediante la interfaz del proveedor de servicios (SPI) de la estructura criptográfica

Zonas y servicios criptográficos

La zona global y cada zona no global tienen su propio servicio `/system/cryptosvc`. Cuando se activa o se actualiza el servicio criptográfico en la zona global, se inicia el daemon `kcfd` en la zona global, se define la política de nivel de usuario para la zona global y se establece la política de núcleo para el sistema. Cuando se activa o se actualiza el servicio en una zona no global, se inicia el daemon `kcfd` en la zona y se define la política de nivel de usuario para la zona. La política de núcleo fue definida por la zona global.

Para obtener más información sobre zonas, consulte la [Parte II, “Zonas de Oracle Solaris” de Administración de Oracle Solaris 11.1: zonas de Oracle Solaris, zonas de Oracle Solaris 10 y gestión de recursos](#). Para obtener más información sobre el uso de la SMF para gestionar aplicaciones persistentes, consulte el [Capítulo 1, “Gestión de servicios \(descripción general\)” de Gestión de servicios y errores en Oracle Solaris 11.1](#) y la página del comando `man smf(5)`.

Estructura criptográfica y FIPS-140

FIPS-140 es un estándar de seguridad informática del Gobierno de los Estados Unidos para módulos criptográficos. Para utilizar la estructura criptográfica en el modo FIPS-140 (FIPS), consulte “[Cómo utilizar la estructura criptográfica en modo FIPS-140](#)” en la página 248.

Nota – La presencia de este modo no significa que está trabajando en una materia que cumple con FIPS-140. Para que se cumpla el estándar, debe seguir la política de seguridad NIST para esta implementación. Para conocer la política, haga clic en el enlace de política de seguridad en entrada de la estructura criptográfica para Oracle en el sitio web [Validated FIPS 140-1 and FIPS 140-2 Cryptographic Modules \(http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm\)](http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm).

Estructura criptográfica y servidores SPARC T-Series en esta versión

La estructura criptográfica le proporciona mecanismos criptográficos a los sistemas SPARC T-Series y optimiza algunos mecanismos para estos servidores. Hay tres mecanismos criptográficos optimizados para datos en reposo y en movimiento: AES -CBC, AES -CFB128 y ARCFOUR. Hay varios mecanismos criptográficos optimizados para OpenSSL: DES, y mediante la optimización de aritmética de precisión arbitraria (bignum), RSA y DSA. Otras optimizaciones incluyen el rendimiento de paquetes pequeños para establecimientos de comunicación y datos en movimiento.

Los siguientes mecanismos criptográficos están disponibles en esta versión:

- AES -XTS: se usa para los datos en reposo
- SHA -224: mecanismo SHA2
- AES -XCBC -MAC: se usa para IPsec

Estructura criptográfica (tareas)

En este capítulo se describe cómo utilizar la estructura criptográfica y se tratan los siguientes temas:

- “Protección de los archivos con la estructura criptográfica (tareas)” en la página 229
- “Administración de la estructura criptográfica (tareas)” en la página 241

Protección de los archivos con la estructura criptográfica (tareas)

En esta sección, se describe cómo generar claves simétricas, cómo crear sumas de comprobación para la integridad de archivos y cómo proteger los archivos contra intrusos. Los comandos incluidos en esta sección pueden ser ejecutados por usuarios comunes. Los desarrolladores pueden escribir secuencias de comandos que utilicen estos comandos.

Protección de archivos con la estructura criptográfica (mapa de tareas)

La estructura criptográfica puede ayudar a proteger los archivos. En el siguiente mapa de tareas se hace referencia a los procedimientos para mostrar los algoritmos disponibles y para proteger los archivos criptográficamente.

Tarea	Descripción	Para obtener instrucciones
Generar una clave simétrica.	Genera una clave de la longitud especificada por el usuario. También puede almacenar la clave en un archivo, en un almacén de claves PKCS #11 o en un almacén de claves NSS.	“Cómo generar una clave simétrica con el comando <code>pktool</code>” en la página 230

Tarea	Descripción	Para obtener instrucciones
Proporcionar una suma de comprobación que garantice la integridad de un archivo.	Verifica que la copia de un archivo del receptor sea idéntica al archivo que se envió.	“Cómo calcular un resumen de un archivo” en la página 234
Proteger un archivo con un código de autenticación de mensajes (MAC).	Le comprueba al receptor del mensaje que usted era el remitente.	“Cómo calcular un MAC de un archivo” en la página 236
Cifrar un archivo y, a continuación, descifrar el archivo cifrado.	Protege el contenido de los archivos al cifrar el archivo. Proporciona los parámetros de cifrado para descifrar el archivo.	“Cómo cifrar y descifrar un archivo” en la página 238

▼ Cómo generar una clave simétrica con el comando `pktool`

Algunas aplicaciones requieren una clave simétrica para el cifrado y el descifrado de las comunicaciones. En este procedimiento, se crea una clave simétrica y se la almacena.

Si su sitio cuenta con un generador de números aleatorios, puede utilizar el generador para crear un número aleatorio para la clave. Este procedimiento no utiliza el generador de números aleatorios de su sitio.

- 1 (Opcional) Si tiene previsto utilizar un almacén de claves, créelo.
 - Para crear e inicializar un almacén de claves PKCS #11, consulte [“Cómo generar una frase de contraseña mediante el comando `pktool setpin`” en la página 267](#).
 - Para crear e inicializar una base de datos NSS, consulte el [Ejemplo 13–5](#).

2 Genere un número aleatorio para usarlo como clave simétrica.

Utilice uno de los métodos siguientes.

- **Genere una clave y almacénela en un archivo.**

La ventaja de almacenar una clave en un archivo es que se puede extraer la clave de este archivo para usarla en el archivo de claves de una aplicación, como el archivo `/etc/inet/secret/ipseckeys` o IPsec. La instrucción de uso muestra los argumentos.

```
% pktool genkey keystore=file
...genkey keystore=file
      outkey=key-fn
      [ keytype=aes|arcfour|des|3des|generic ]
      [ keylen=key-size (AES, ARCFOUR or GENERIC only)]
      [ print=y|n ]
```

`outkey=key-fn`

El nombre de archivo donde se almacena la clave.

keytype=specific-symmetric-algorithm

Para una clave simétrica de cualquier longitud, el valor es *generic*. Para un algoritmo determinado, especifique *aes*, *arcfour*, *des* o *3des*.

keylen=size-in-bits

Es la longitud de la clave en bits. El número debe ser divisible por 8. No especificar para *des* ni *3des*.

print=n

Imprime la clave en la ventana de terminal. De manera predeterminada, el valor de *print* es *n*.

■ Genere una clave y almacénela en un almacén de claves PKCS #11.

La ventaja del almacén de claves PKCS #11 es que se puede recuperar la clave por su etiqueta. Este método es útil para las claves para cifrar y descifrar archivos. Debe completar el [Paso 1](#) antes de utilizar este método. La instrucción de uso muestra los argumentos. Los corchetes alrededor del argumento del almacén de claves indican que cuando el argumento de almacén de claves no está especificado, la clave se almacena en el almacén de claves PKCS #11.

```
$ pktool genkey
...genkey [ keystore=pkcs11 ]
           label=key-label
           [ keytype=aes|arcfour|des|3des|generic ]
           [ keylen=key-size (AES, ARCFOUR or GENERIC only) ]
           [ token=token[:manuf[:serial]] ]
           [ sensitive=y|n ]
           [ extractable=y|n ]
           [ print=y|n ]
```

label=key-label

Es una etiqueta especificada por el usuario para la clave. La clave se puede recuperar del almacén de claves por su etiqueta.

keytype=specific-symmetric-algorithm

Para una clave simétrica de cualquier longitud, el valor es *generic*. Para un algoritmo determinado, especifique *aes*, *arcfour*, *des* o *3des*.

keylen=size-in-bits

Es la longitud de la clave en bits. El número debe ser divisible por 8. No especificar para *des* ni *3des*.

token=token

Es el nombre del token. De manera predeterminada, el token es Sun Software PKCS#11 softtoken.

sensitive=n

Especifica la sensibilidad de la clave. Cuando el valor es *y*, la clave no se puede imprimir utilizando el argumento *print=y*. De manera predeterminada, el valor de *sensitive* es *n*.

`extractable=y`

Especifica que la clave se puede extraer del almacén de claves. Especifique `n` para evitar que se extraiga la clave.

`print=n`

Imprime la clave en la ventana de terminal. De manera predeterminada, el valor de `print` es `n`.

- **Genere una clave y almacénela en un almacén de claves NSS.**

Debe completar el [Paso 1](#) antes de utilizar este método. La instrucción de uso muestra los argumentos.

```
$ pktool genkey keystore=nss
...genkey keystore=nss
    label=key-label
    [ keytype=aes|arcfour|des|3des|generic ]
    [ keylen=key-size (AES, ARCFOUR or GENERIC only) ]
    [ token=token[:manuf[:serial]] ]
    [ dir=directory-path ]
    [ prefix=DBprefix ]
```

`label=key-label`

Es una etiqueta especificada por el usuario para la clave. La clave se puede recuperar del almacén de claves por su etiqueta.

`keytype=symmetric-algorithm`

Para una clave simétrica de cualquier longitud, el valor es `generic`. Para un algoritmo determinado, especifique `aes`, `arcfour`, `des` o `3des`.

`keylen=size-in-bits`

Es la longitud de la clave en bits. El número debe ser divisible por 8. No especificar para `des` ni `3des`.

`token=token`

Es el nombre del token. De manera predeterminada, el token es el token interno NSS.

`dir=directory`

Es la ruta de directorio a la base de datos NSS. De manera predeterminada, el valor de `directorio` es el directorio actual.

`prefix=directory`

Es el prefijo de la base de datos NSS. El valor predeterminado es sin prefijo.

3 (Opcional) Compruebe que la clave exista.

Utilice uno de los siguientes comandos, según dónde haya guardado la clave.

- **Verifique la clave en el archivo `key-fn`.**

```
% pktool list keystore=file objtype=key [infile=key-fn]
Found n keys.
Key #1 - keytype:location (keylen)
```

- **Verifique la clave en el almacén de claves PKCS #11 o NSS.**

```
$ pktool list objtype=key
Enter PIN for keystore:
Found n keys.
Key #1 - keytype:location (keylen)
```

Ejemplo 12-1 Creación de una clave simétrica con el comando pktool

En el siguiente ejemplo, un usuario crea un almacén de claves PKCS #11 por primera vez y, a continuación, genera una clave simétrica de gran tamaño para una aplicación. Por último, el usuario verifica que la clave se encuentre en el almacén de claves.

```
# pktool setpin
Create new passphrase:    Type easily-remembered-hard-to-detect-password
Re-enter new passphrase:  Retype password
Passphrase changed.
% pktool genkey label=specialappkey keytype=generic keylen=1024
Enter PIN for Sun Software PKCS#11 softtoken :    Type password

% pktool list objtype=key
Enter PIN for Sun Software PKCS#11 softtoken :    Type password

Found 1 keys.
Key #1 - symmetric: specialappkey (1024 bits)
```

Ejemplo 12-2 Creación de una clave DES con el comando pktool

En el siguiente ejemplo, se crea una clave secreta para el algoritmo DES. La clave se almacena en un archivo local para un posterior descifrado. El comando protege el archivo con 400 permisos. Cuando se crea la clave, la opción print=y muestra la clave generada en la ventana de terminal.

Los mecanismos DES utilizan una clave de 64 bits. El usuario que posee el archivo de claves recupera la clave mediante el comando od.

```
% pktool genkey keystore=file outkey=64bit.file1 keytype=des print=y
Key Value ="a3237b2c0a8ff9b3"
% od -x 64bit.file1
00000000 a323 7b2c 0a8f f9b3
```

Ejemplo 12-3 Creación de una clave simétrica para las asociaciones de seguridad IPsec

En el siguiente ejemplo, el administrador crea manualmente el material clave para las asociaciones de seguridad de IPsec y las almacena en archivos. A continuación, el administrador copia las claves al archivo /etc/inet/secret/ipseckeys y destruye los archivos originales.

- En primer lugar, el administrador crea y muestra las claves que la política IPsec requiere:

```
# pktool genkey keystore=file outkey=ipencrin1 keytype=generic keylen=192 print=y
Key Value ="294979e512cb8e79370dabecadc3fcbb849e78d2d6bd2049"
# pktool genkey keystore=file outkey=ipencrout1 keytype=generic keylen=192 print=y
Key Value ="9678f80e33406c86e3d1686e50406bd0434819c20d09d204"
# pktool genkey keystore=file outkey=ipspi1 keytype=generic keylen=32 print=y
Key Value ="acbeaa20"
# pktool genkey keystore=file outkey=ipspi2 keytype=generic keylen=32 print=y
Key Value ="19174215"
# pktool genkey keystore=file outkey=ipsha21 keytype=generic keylen=256 print=y
Key Value ="659c20f2d6c3f9570bcee93e96d95e2263aca4eeb3369f72c5c786af4177fe9e"
# pktool genkey keystore=file outkey=ipsha22 keytype=generic keylen=256 print=y
Key Value ="b041975a0e1fce0503665c3966684d731fa3dbb12fcf87b0a837b2da5d82c810"
```

- A continuación, el administrador crea el siguiente archivo /etc/inet/secret/ipseckey:

```
## SPI values require a leading 0x.
## Backslashes indicate command continuation.
##
## for outbound packets on this system
add esp spi 0xacbeaa20 \
src 192.168.1.1 dst 192.168.2.1 \
encr_alg aes auth_alg sha256 \
encrkey 294979e512cb8e79370dabecadc3fcbb849e78d2d6bd2049 \
authkey 659c20f2d6c3f9570bcee93e96d95e2263aca4eeb3369f72c5c786af4177fe9e
##
## for inbound packets
add esp spi 0x19174215 \
src 192.168.2.1 dst 192.168.1.1 \
encr_alg aes auth_alg sha256 \
encrkey 9678f80e33406c86e3d1686e50406bd0434819c20d09d204 \
authkey b041975a0e1fce0503665c3966684d731fa3dbb12fcf87b0a837b2da5d82c810
```

- Después de verificar que la sintaxis del archivo ipseckey sea válida, el administrador destruye los archivos de claves originales.

```
# ipseckey -c /etc/inet/secret/ipseckey
# rm ipencrin1 ipencrout1 ipspi1 ipspi2 ipsha21 ipsha22
```

- El administrador copia el archivo ipseckey al sistema de comunicación mediante el comando ssh u otro mecanismo seguro. En el sistema de comunicación, las protecciones se revierten. La primera entrada en el archivo ipseckey protege los paquetes entrantes y la segunda entrada protege los paquetes salientes. No se generan claves en el sistema de comunicación.

▼ Cómo calcular un resumen de un archivo

Cuando se calcula un resumen de un archivo, se puede comprobar que el archivo no haya sido alterado comparando los resultados del resumen. Un resumen no modifica el archivo original.

1 Muestre los algoritmos de resumen disponibles.

```
% digest -l
md5
sha1
sha224
```

```
sha256
sha384
sha512
```

2 Calcule el resumen del archivo y guarde la lista de resumen.

Proporcione un algoritmo con el comando `digest`.

```
% digest -v -a algorithm input-file > digest-listing
```

`-v` Muestra el resultado en el siguiente formato:

```
algorithm (input-file) = digest
```

`-a algorithm` Es el algoritmo que se utilizará para calcular un resumen del archivo. Escriba el algoritmo tal como aparece en el resultado del [Paso 1](#).

`input-file` Es el archivo de entrada para el comando `digest`.

`digest-listing` Es el archivo de salida para el comando `digest`.

Ejemplo 12-4 Cálculo de un resumen con el mecanismo MD5

En el ejemplo siguiente, el comando `digest` usa el mecanismo MD5 para calcular un resumen de un anexo de correo electrónico.

```
% digest -v -a md5 email.attach >> $HOME/digest.emails.05.07
% cat ~/digest.emails.05.07
md5 (email.attach) = 85c0a53d1a5cc71ea34d9ee7b1b28b01
```

Cuando no se utiliza la opción `-v`, el resumen se guarda sin información adicional:

```
% digest -a md5 email.attach >> $HOME/digest.emails.05.07
% cat ~/digest.emails.05.07
85c0a53d1a5cc71ea34d9ee7b1b28b01
```

Ejemplo 12-5 Cálculo de un resumen con el mecanismo SHA1

En el ejemplo siguiente, el comando `digest` usa el mecanismo SHA1 para proporcionar una lista de directorios. Los resultados se colocarán en un archivo.

```
% digest -v -a sha1 docs/* > $HOME/digest.docs.legal.05.07
% more ~/digest.docs.legal.05.07
sha1 (docs/legal1) = 1df50e8ad219e34f0b911e097b7b588e31f9b435
sha1 (docs/legal2) = 68efa5a636291bde8f33e046eb33508c94842c38
sha1 (docs/legal3) = 085d991238d61bd0cfa2946c183be8e32cccf6c9
sha1 (docs/legal4) = f3085eae7e2c8d008816564fdf28027d10e1d983
```

▼ Cómo calcular un MAC de un archivo

Un código de autenticación de mensajes, o MAC, calcula un resumen del archivo y utiliza una clave secreta para proteger aún más el resumen. Un MAC no modifica el archivo original.

1 Muestre los mecanismos disponibles.

```
% mac -l
Algorithm      Keysize:  Min    Max
-----
des_mac        64      64
sha1_hmac      8       512
md5_hmac       8       512
sha224_hmac    8       512
sha256_hmac    8       512
sha384_hmac    8      1024
sha512_hmac    8      1024
```

2 Genere una clave simétrica de la longitud adecuada.

Dispone de dos opciones. Puede proporcionar una [frase de contraseña](#) a partir de la cual se generará una clave. O bien, puede proporcionar una clave.

- Si proporciona una frase contraseña, deberá almacenarla o recordarla. Si almacena la frase de contraseña en línea, sólo usted debe poder leer el archivo de frases de contraseña.
- Si proporciona una clave, ésta debe ser del tamaño correcto para el mecanismo. Puede utilizar el comando `pktool`. Para conocer el procedimiento y algunos ejemplos, consulte [“Cómo generar una clave simétrica con el comando pktool” en la página 230](#).

3 Cree un MAC para un archivo.

Proporcione una clave y utilice un algoritmo de clave simétrico con el comando `mac`.

```
% mac [-v] -a algorithm [-k keyfile | -K key-label [-T token]] input-file
```

- v** Muestra el resultado en el siguiente formato:
- ```
algorithm (input-file) = mac
```
- a *algorithm*** Es el algoritmo que se utiliza para calcular el MAC. Escriba el algoritmo tal como aparece en el resultado del comando `mac -l`.
- k *keyfile*** Es el archivo que contiene una clave con la longitud especificada por el algoritmo.
- K *key-label*** Es la etiqueta de la clave en el almacén de claves PKCS #11.
- T *token*** Es el nombre del token. De manera predeterminada, el token es Sun Software PKCS#11 soft token. Sólo se utiliza cuando la opción **-K *key-label*** se utiliza.
- input-file*** Es el archivo de entrada para el MAC.



**Ejemplo 12-6** Cálculo de un MAC con DES\_MAC y una frase de contraseña

En el ejemplo siguiente, el anexo de correo electrónico se autentica con el mecanismo DES\_MAC y una clave que se obtiene a partir de una frase de contraseña. La lista de MAC se guarda en un archivo. Si la frase de contraseña se almacena en un archivo, el usuario debe ser la única persona que pueda leer el archivo.

```
% mac -v -a des_mac email.attach
Enter passphrase: <Type passphrase>
des_mac (email.attach) = dd27870a
% echo "des_mac (email.attach) = dd27870a" >> ~/desmac.daily.05.07
```

**Ejemplo 12-7** Cálculo de un MAC con MD5\_HMAC y un archivo de claves

En el ejemplo siguiente, el anexo de correo electrónico se autentica con el mecanismo MD5\_HMAC y una clave secreta. La lista de MAC se guarda en un archivo.

```
% mac -v -a md5_hmac -k $HOME/keyf/05.07.mack64 email.attach
md5_hmac (email.attach) = 02df6eb6c123ff25d78877eb1d55710c
% echo "md5_hmac (email.attach) = 02df6eb6c123ff25d78877eb1d55710c" \
>> ~/mac.daily.05.07
```

**Ejemplo 12-8** Cálculo de un MAC con SHA1\_HMAC y un archivo de claves

En el ejemplo siguiente, el manifiesto de directorio se autentica con el mecanismo SHA1\_HMAC y una clave secreta. Los resultados se colocarán en un archivo.

```
% mac -v -a sha1_hmac \
-k $HOME/keyf/05.07.mack64 docs/* > $HOME/mac.docs.legal.05.07
% more ~/mac.docs.legal.05.07
sha1_hmac (docs/legal1) = 9b31536d3b3c0c6b25d653418db8e765e17fe07a
sha1_hmac (docs/legal2) = 865af61a3002f8a457462a428cdb1a88c1b51ff5
sha1_hmac (docs/legal3) = 076c944cb2528536c9aebd3b9fbe367e07b61dc7
sha1_hmac (docs/legal4) = 7aede27602ef6e4454748cbd3821e0152e45beb4
```

**Ejemplo 12-9** Cálculo de un MAC con SHA1\_HMAC y una etiqueta de clave

En el ejemplo siguiente, el manifiesto de directorio se autentica con el mecanismo SHA1\_HMAC y una clave secreta. Los resultados se ubican en el almacén de claves PKCS #11 del usuario. El usuario creó inicialmente el almacén de claves y la contraseña para el almacén de claves mediante el comando `pktool setpin`.

```
% mac -a sha1_hmac -K legaldocs0507 docs/*
Enter pin for Sun Software PKCS#11 softtoken: Type password
```

Para recuperar el MAC desde el almacén de claves, el usuario utiliza la opción detallada y proporciona la etiqueta de clave y el nombre del directorio que se ha autenticado.

```
% mac -v -a sha1_hmac -K legaldocs0507 docs/*
Enter pin for Sun Software PKCS#11 softtoken: Type password
sha1_hmac (docs/legal1) = 9b31536d3b3c0c6b25d653418db8e765e17fe07a
sha1_hmac (docs/legal2) = 865af61a3002f8a457462a428cdb1a88c1b51ff5
sha1_hmac (docs/legal3) = 076c944cb2528536c9aebd3b9fbe367e07b61dc7
sha1_hmac (docs/legal4) = 7aede27602ef6e4454748cbd3821e0152e45beb4
```

## ▼ Cómo cifrar y descifrar un archivo

Al cifrar un archivo, el archivo original no se elimina ni modifica. Se cifra el archivo de salida.

Para ver las soluciones a los errores comunes del comando `encrypt`, consulte sección que aparece a continuación de los ejemplos.

### 1 Cree una clave simétrica de la longitud adecuada.

Existen dos opciones. Puede proporcionar una [frase de contraseña](#) a partir de la cual se generará una clave. O bien, puede proporcionar una clave.

- Si proporciona una frase contraseña, deberá almacenarla o recordarla. Si almacena la frase de contraseña en línea, sólo usted debe poder leer el archivo de frases de contraseña.
- Si proporciona una clave, ésta debe ser del tamaño correcto para el mecanismo. Puede utilizar el comando `pktool`. Para conocer el procedimiento y algunos ejemplos, consulte [“Cómo generar una clave simétrica con el comando pktool” en la página 230.](#)

### 2 Cifre un archivo.

Proporcione una clave y utilice un algoritmo de clave simétrico con el comando `encrypt`.

```
% encrypt -a algorithm [-v] \
[-k keyfile | -K key-label [-T token]] [-i input-file] [-o output-file]
```

- |                              |                                                                                                                                                                                                            |
|------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>-a <i>algorithm</i></b>   | Es el algoritmo que se utiliza para cifrar el archivo. Escriba el algoritmo tal como aparece en el resultado del comando <code>encrypt -l</code> .                                                         |
| <b>-k <i>keyfile</i></b>     | Es el archivo que contiene una clave con la longitud especificada por el algoritmo. La longitud de la clave para cada algoritmo se muestra, en bits, en el resultado del comando <code>encrypt -l</code> . |
| <b>-K <i>key-label</i></b>   | Es la etiqueta de una clave en el almacén de claves PKCS #11.                                                                                                                                              |
| <b>-T <i>token</i></b>       | Es el nombre del token. De manera predeterminada, el token es Sun Software PKCS#11 softtoken. Sólo se utiliza cuando la opción <b>-K <i>key-label</i></b> se utiliza.                                      |
| <b>-i <i>input-file</i></b>  | Es el archivo de entrada que desea cifrar. Este archivo no es modificado por el comando.                                                                                                                   |
| <b>-o <i>output-file</i></b> | Es el archivo de salida, que es el formato cifrado del archivo de entrada.                                                                                                                                 |

**Ejemplo 12-10** Creación de una clave AES para cifrar los archivos

En el siguiente ejemplo, un usuario crea y almacena una clave AES en un almacén de claves PKCS #11 existente para utilizar en el cifrado y descifrado. El usuario puede comprobar que la clave existe y puede usar la clave, pero no puede verla.

```
% pktool genkey label=MyAESkeynumber1 keytype=aes keylen=256
Enter PIN for Sun Software PKCS#11 softtoken : Type password

% pktool list objtype=key
Enter PIN for Sun Software PKCS#11 softtoken : <Type password>
Found 1 key
Key #1 - Sun Software PKCS#11 softtoken: MyAESkeynumber1 (256)
```

Para utilizar la clave para cifrar un archivo, el usuario recupera la clave por su etiqueta.

```
% encrypt -a aes -K MyAESkeynumber1 -i encryptthisfile -o encryptedthisfile
```

Para descifrar el archivo encryptedthisfile, el usuario recupera la clave por su etiqueta.

```
% decrypt -a aes -K MyAESkeynumber1 -i encryptedthisfile -o sameasencryptthisfile
```

**Ejemplo 12-11** Cifrado y descifrado con AES y una frase de contraseña

En el ejemplo siguiente, se cifra un archivo con el algoritmo AES. La clave se genera a partir de una frase de contraseña. Si la frase de contraseña se almacena en un archivo, el usuario debe ser la única persona que pueda leer el archivo.

```
% encrypt -a aes -i ticket.to.ride -o ~/enc/e.ticket.to.ride
Enter passphrase: <Type passphrase>
Re-enter passphrase: Type passphrase again
```

El archivo de entrada, ticket.to.ride, todavía existe en su formato original.

Para descifrar el archivo de salida, el usuario utiliza la misma frase de contraseña y el mismo mecanismo de cifrado que utilizó para cifrar el archivo.

```
% decrypt -a aes -i ~/enc/e.ticket.to.ride -o ~/d.ticket.to.ride
Enter passphrase: <Type passphrase>
```

**Ejemplo 12-12** Cifrado y descifrado con AES y un archivo de claves

En el ejemplo siguiente, se cifra un archivo con el algoritmo AES. Los mecanismos AES utilizan una clave de 128 bits o 16 bytes.

```
% encrypt -a aes -k ~/keyf/05.07.aes16 \
-i ticket.to.ride -o ~/enc/e.ticket.to.ride
```

El archivo de entrada, `ticket.to.ride`, todavía existe en su formato original.

Para descifrar el archivo de salida, el usuario utiliza la misma clave y el mismo mecanismo de cifrado que utilizó para cifrar el archivo.

```
% decrypt -a aes -k ~/keyf/05.07.aes16 \
-i ~/enc/e.ticket.to.ride -o ~/d.ticket.to.ride
```

### Ejemplo 12-13 Cifrado y descifrado con ARCFOUR y un archivo de claves

En el ejemplo siguiente, se cifra un archivo con el algoritmo ARCFOUR. El algoritmo ARCFOUR acepta una clave de 8 bits (1 byte), 64 bits (8 bytes) o 128 bits (16 bytes).

```
% encrypt -a arcfour -i personal.txt \
-k ~/keyf/05.07.rc4.8 -o ~/enc/e.personal.txt
```

Para descifrar el archivo de salida, el usuario utiliza la misma clave y el mismo mecanismo de cifrado que utilizó para cifrar el archivo.

```
% decrypt -a arcfour -i ~/enc/e.personal.txt \
-k ~/keyf/05.07.rc4.8 -o ~/personal.txt
```

### Ejemplo 12-14 Cifrado y descifrado con 3DES y un archivo de claves

En el ejemplo siguiente, se cifra un archivo con el algoritmo 3DES. El algoritmo 3DES requiere una clave de 192 bits o 24 bytes.

```
% encrypt -a 3des -k ~/keyf/05.07.des24 \
-i ~/personal2.txt -o ~/enc/e.personal2.txt
```

Para descifrar el archivo de salida, el usuario utiliza la misma clave y el mismo mecanismo de cifrado que utilizó para cifrar el archivo.

```
% decrypt -a 3des -k ~/keyf/05.07.des24 \
-i ~/enc/e.personal2.txt -o ~/personal2.txt
```

#### Errores más frecuentes

Los siguientes mensajes indican que la clave proporcionada al comando `encrypt` no está permitida por el algoritmo que está utilizando.

- `encrypt: unable to create key for crypto operation: CKR_ATTRIBUTE_VALUE_INVALID`
- `encrypt: failed to initialize crypto operation: CKR_KEY_SIZE_RANGE`

Si utiliza una clave que no cumple con los requisitos del algoritmo, debe proporcionar una clave mejor.

- Una opción es utilizar una frase de contraseña. La estructura proporciona una clave que cumple con los requisitos.
- La segunda opción es utilizar un tamaño de clave que sea aceptado por el algoritmo. Por ejemplo, el algoritmo DES requiere una clave de 64 bits. El algoritmo 3DES requiere una clave de 192 bits.

# Administración de la estructura criptográfica (tareas)

En esta sección se describe cómo administrar proveedores de software y hardware en la estructura criptográfica. Los proveedores de software y hardware se pueden eliminar para no ser utilizados cuando se desee. Por ejemplo, puede desactivar la implementación de un algoritmo de un proveedor de software. A continuación, puede forzar al sistema a utilizar el algoritmo de otro proveedor de software.

## Administración de la estructura criptográfica (mapa de tareas)

En el siguiente mapa de tareas se hace referencia a los procedimientos para administrar a los proveedores de software y hardware en la estructura criptográfica.

| Tarea                                                       | Descripción                                                                                                                              | Para obtener instrucciones                                                                    |
|-------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------|
| Mostrar los proveedores en la estructura criptográfica.     | Muestra los algoritmos, las bibliotecas y los dispositivos de hardware que están disponibles para su uso en la estructura criptográfica. | <a href="#">“Cómo mostrar los proveedores disponibles” en la página 242</a>                   |
| Activar el modo FIPS-140.                                   | Ejecuta la estructura criptográfica para un estándar del gobierno de EE. UU. para módulos de criptografía.                               | <a href="#">“Cómo utilizar la estructura criptográfica en modo FIPS-140” en la página 248</a> |
| Agregar un proveedor de software.                           | Agrega una biblioteca PKCS #11 o un módulo de núcleo a la estructura criptográfica. El proveedor debe estar registrado.                  | <a href="#">“Cómo agregar un proveedor de software” en la página 246</a>                      |
| Evitar el uso de un mecanismo de nivel de usuario.          | Elimina un mecanismo de software para que no sea utilizado. El mecanismo se puede volver a activar.                                      | <a href="#">“Cómo evitar el uso de un mecanismo de nivel de usuario” en la página 249</a>     |
| Desactivar temporalmente mecanismos de un módulo de núcleo. | Elimina temporalmente un mecanismo para que no sea utilizado. Se suele utilizar para realizar pruebas.                                   | <a href="#">“Cómo evitar el uso de un proveedor de software de núcleo” en la página 251</a>   |
| Desinstalar una biblioteca.                                 | Elimina un proveedor de software de nivel de usuario para que no sea utilizado.                                                          | <a href="#">Ejemplo 12-21</a>                                                                 |

| Tarea                                                  | Descripción                                                                                                                         | Para obtener instrucciones                                                                          |
|--------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------|
| Desinstalar un proveedor del núcleo.                   | Elimina un proveedor de software de núcleo para que no sea utilizado.                                                               | <a href="#">Ejemplo 12-23</a>                                                                       |
| Mostrar los proveedores de hardware disponibles.       | Muestra el hardware conectado, los mecanismos que proporciona el hardware y los mecanismos que están activados para ser utilizados. | <a href="#">“Cómo mostrar proveedores de hardware” en la página 254</a>                             |
| Desactivar los mecanismos de un proveedor de hardware. | Garantiza que los mecanismos seleccionados en un acelerador de hardware no sean utilizados.                                         | <a href="#">“Cómo desactivar funciones y mecanismos del proveedor de hardware” en la página 255</a> |
| Reiniciar o actualizar los servicios criptográficos.   | Garantiza que los servicios criptográficos estén disponibles.                                                                       | <a href="#">“Cómo actualizar o reiniciar todos los servicios criptográficos” en la página 256</a>   |

## ▼ Cómo mostrar los proveedores disponibles

La estructura criptográfica proporciona algoritmos para diversos tipos de consumidores:

- Los proveedores de nivel de usuario brindan una interfaz criptográfica PKCS #11 a las aplicaciones que están enlazadas a la biblioteca `libpkcs11`
- Los proveedores de software de núcleo brindan algoritmos para IPsec, Kerberos y otros componentes de núcleo de Oracle Solaris
- Los proveedores de hardware de núcleo brindan algoritmos que están disponibles para los consumidores del núcleo y para las aplicaciones por medio de la biblioteca `pkcs11_kernel`

### 1 Muestre los proveedores en un formato breve.

**Nota** – El contenido y el formato de la lista de proveedores varía para las distintas versiones y plataformas de Oracle Solaris. Ejecute el comando `cryptoadm list` en el sistema, para ver los proveedores que admite el sistema.

Sólo los mecanismos de nivel de usuario están disponibles para ser utilizados por los usuarios comunes.

```
% cryptoadm list
User-level providers:
Provider: /usr/lib/security/$ISA/pkcs11_kernel.so
Provider: /usr/lib/security/$ISA/pkcs11_softtoken.so
Provider: /usr/lib/security/$ISA/pkcs11_tpm.so

Kernel software providers:
 des
 aes
 arcfour
 blowfish
 ecc
 sha1
```

```

sha2
md4
md5
rsa
swrand
n2rng/0
ncp/0
n2cp/0

```

## 2 Muestre los proveedores y sus mecanismos en la estructura criptográfica.

Todos los mecanismos se muestran en el siguiente resultado. Sin embargo, es posible que algunos de los mecanismos de la lista no estén disponibles para su uso. Para incluir en la lista sólo los mecanismos que el administrador ha aprobado para su uso, consulte el [Ejemplo 12–16](#).

La salida se trunca con fines de visualización.

```

% cryptoadm list -m
User-level providers:
=====

```

```

Provider: /usr/lib/security/$ISA/pkcs11_kernel.so

```

```

Mechanisms:
CKM_DSA
CKM_RSA_X_509
CKM_RSA_PKCS
...
CKM_SHA256_HMAC_GENERAL
CKM_SSL3_MD5_MAC

```

```

Provider: /usr/lib/security/$ISA/pkcs11_softtoken.so

```

```

Mechanisms:
CKM_DES_CBC
CKM_DES_CBC_PAD
CKM_DES_ECB
CKM_DES_KEY_GEN
CKM_DES_MAC_GENERAL
...
CKM_ECDSA_SHA1
CKM_ECDH1_DERIVE

```

```

Provider: /usr/lib/security/$ISA/pkcs11_tpm.so
/usr/lib/security/$ISA/pkcs11_tpm.so: no slots presented.

```

```

Kernel providers:
=====

```

```

des: CKM_DES_ECB,CKM_DES_CBC,CKM_DES3_ECB,CKM_DES3_CBC
aes: CKM_AES_ECB,CKM_AES_CBC,CKM_AES_CTR,CKM_AES_CCM,CKM_AES_GCM,CKM_AES_GMAC,
CKM_AES_CFB128,CKM_AES_XTS,CKM_AES_XCBC_MAC
arcfour: CKM_RC4
blowfish: CKM_BLOWFISH_ECB,CKM_BLOWFISH_CBC
ecc: CKM_EC_KEY_PAIR_GEN,CKM_ECDH1_DERIVE,CKM_ECDSA,CKM_ECDSA_SHA1
sha1: CKM_SHA_1,CKM_SHA_1_HMAC,CKM_SHA_1_HMAC_GENERAL
sha2: CKM_SHA224,CKM_SHA224_HMAC,...CKM_SHA512_256_HMAC_GENERAL

```

```

md4: CKM_MD4
md5: CKM_MD5,CKM_MD5_HMAC,CKM_MD5_HMAC_GENERAL

```

```

rsa: CKM_RSA_PKCS,CKM_RSA_X_509,CKM_MD5_RSA_PKCS,CKM_SHA1_RSA_PKCS,CKM_SHA224_RSA_PKCS,
CKM_SHA256_RSA_PKCS,CKM_SHA384_RSA_PKCS,CKM_SHA512_RSA_PKCS
swrand: No mechanisms presented.
n2rng/0: No mechanisms presented.
ncp/0: CKM_DSA,CKM_RSA_X_509,CKM_RSA_PKCS,CKM_RSA_PKCS_KEY_PAIR_GEN,
CKM_DH_PKCS_KEY_PAIR_GEN,CKM_DH_PKCS_DERIVE,CKM_EC_KEY_PAIR_GEN,
CKM_ECDH1_DERIVE,CKM_ECDSA
n2cp/0: CKM_DES_CBC,CKM_DES_CBC_PAD,CKM_DES_ECB,CKM_DES3_CBC,...CKM_SSL3_SHA1_MAC

```

### Ejemplo 12-15 Búsqueda de los mecanismos criptográficos existentes

En el siguiente ejemplo, se muestran todos los mecanismos que ofrece la biblioteca de nivel de usuario, `pkcs11_softtoken`.

```

% cryptoadm list -m provider=/usr/lib/security/\$ISA/pkcs11_softtoken.so
Mechanisms:
CKM_DES_CBC
CKM_DES_CBC_PAD
CKM_DES_ECB
CKM_DES_KEY_GEN
CKM_DES_MAC_GENERAL
CKM_DES_MAC
...
CKM_ECDSA
CKM_ECDSA_SHA1
CKM_ECDH1_DERIVE

```

### Ejemplo 12-16 Búsqueda de los mecanismos criptográficos disponibles

La política determina qué mecanismos están disponibles para su uso. El administrador define la política. Un administrador puede elegir desactivar los mecanismos de un proveedor determinado. La opción `-p` muestra la lista de los mecanismos permitidos por la política que el administrador ha definido.

```

% cryptoadm list -p
User-level providers:
=====
/usr/lib/security/\$ISA/pkcs11_kernel.so: all mechanisms are enabled.random is enabled.
/usr/lib/security/\$ISA/pkcs11_softtoken.so: all mechanisms are enabled, random is enabled.
/usr/lib/security/\$ISA/pkcs11_tpm.so: all mechanisms are enabled.

```

```

Kernel providers:
=====
des: all mechanisms are enabled.
aes: all mechanisms are enabled.
arcfour: all mechanisms are enabled.
blowfish: all mechanisms are enabled.
ecc: all mechanisms are enabled.
sha1: all mechanisms are enabled.
sha2: all mechanisms are enabled.
md4: all mechanisms are enabled.
md5: all mechanisms are enabled.
rsa: all mechanisms are enabled.

```



```
swrand: random is enabled.
n2rng/0: all mechanisms are enabled. random is enabled.
ncp/0: all mechanisms are enabled.
n2cp/0: all mechanisms are enabled.
```

### Ejemplo 12-17 Determinación de qué mecanismo criptográfico realiza cada función

Los mecanismos realizan funciones criptográficas específicas, como la firma o generación de claves. Las opciones `-v` y `-m` muestran cada mecanismo y sus funciones.

En esta instancia, el administrador desea determinar para qué funciones los mecanismos CKM\_ECDSA\* se pueden utilizar.

```
% cryptoadm list -vm
User-level providers:
=====
Provider: /usr/lib/security/$ISA/pkcs11_kernel.so
Number of slots: 3
Slot #2
Description: ncp/0 Crypto Accel Asym 1.0
...
CKM_ECDSA 163 571 X . . . X . X
...

Provider: /usr/lib/security/$ISA/pkcs11_softtoken.so
...
CKM_ECDSA 112 571 X . X
CKM_ECDSA_SHA1 112 571 X . X
...
Kernel providers:
=====
...
ecc: CKM_EC_KEY_PAIR_GEN,CKM_ECDH1_DERIVE,CKM_ECDSA,CKM_ECDSA_SHA1
...
```

La lista indica que estos mecanismos están disponibles de los siguientes proveedores de nivel de usuario:

- CKM\_ECDSA y CKM\_ECDSA\_SHA1: como una implementación de software en la biblioteca `/usr/lib/security/$ISA/pkcs11_softtoken.so`.
- CKM\_ECDSA: acelerado por ncp/0 Crypto Accel Asym 1.0 en la biblioteca `/usr/lib/security/$ISA/pkcs11_kernel.so`.

Cada artículo en una entrada representa una parte de la información sobre el mecanismo. Para estos mecanismos ECC, la lista indica lo siguiente:

- Longitud mínima: 112 bytes.
- Longitud máxima: 571 bytes.
- Hardware: está disponible o no está disponible en el hardware.
- Cifrar: no se utiliza para cifrar datos.
- Descifrar: no se utiliza para descifrar datos.

- Resumir: no se utiliza para crear resúmenes de mensajes.
- Firmar: se utiliza para firmar datos.
- Firmar + recuperar: no se utiliza para firmar datos, donde los datos se pueden recuperar de la firma.
- Verificar: se utiliza para verificar datos firmados.
- Verificar + recuperar: no se utiliza para verificar los datos que se pueden recuperar de la firma.
- Generación de claves: no se utiliza para generar una clave privada.
- Generación de par: no se utiliza para generar un par de claves.
- Ajustar: no se utiliza para ajustar. Es decir, cifrar una clave existente.
- Desajustar: no se utiliza para desajustar una clave ajustada.
- Derivar: no se utiliza para derivar una nueva clave de una clave de base.
- Funciones EC: funciones EC ausentes que no se tratan en elementos anteriores.

## ▼ Cómo agregar un proveedor de software

### Antes de empezar

Debe convertirse en un administrador con el perfil de derechos de gestión de criptografía asignado. Para obtener más información, consulte [“Cómo usar los derechos administrativos que tiene asignados” en la página 164.](#)

### 1 Muestre los proveedores de software que están disponibles para el sistema.

```
% cryptoadm list
User-level providers:
Provider: /usr/lib/security/$ISA/pkcs11_kernel.so
Provider: /usr/lib/security/$ISA/pkcs11_softtoken.so
/usr/lib/security/$ISA/pkcs11_tpm.so: all mechanisms are enabled.

Kernel software providers:
des
aes
arcfour
blowfish
sha1
sha2
md4
md5
rsa
swrand
n2rng/0
ncp/0
n2cp/0
```

### 2 Agregue el proveedor de un repositorio.

Oracle ha emitido un certificado al proveedor de software existente.

**3 Actualice los proveedores.**

Si agregó un proveedor de software o si agregó hardware y especificó una política para el hardware, debe refrescar los proveedores.

```
svcadm refresh svc:/system/cryptosvc
```

**4 Ubique al nuevo proveedor en la lista.**

En este caso, se instaló un nuevo proveedor de software de núcleo.

```
cryptoadm list
...
Kernel software providers:
 des
 aes
 arcfour
 blowfish
 ecc
 sha1
 sha2
 md4
 md5
 rsa
 swrand
 sha3 <-- added provider
...
```

**Ejemplo 12–18 Agregación de un proveedor de software de nivel de usuario**

En el ejemplo siguiente, se instala una biblioteca PKCS #11 registrada.

```
pkgadd -d /cdrom/cdrom0/SolarisNew
 Answer the prompts
svcadm refresh system/cryptosvc
cryptoadm list
user-level providers:
=====
 /usr/lib/security/$ISA/pkcs11_kernel.so
 /usr/lib/security/$ISA/pkcs11_softtoken.so
 /usr/lib/security/$ISA/pkcs11_tpm.so
 /opt/lib/$ISA/libpkcs11.so.1 <-- added provider
```

Los desarrolladores que estén probando una biblioteca con la estructura criptográfica pueden instalar la biblioteca manualmente.

```
cryptoadm install provider=/opt/lib/$ISA/libpkcs11.so.1
```

## ▼ Cómo utilizar la estructura criptográfica en modo FIPS-140

De manera predeterminada, el modo FIPS-140 está desactivado en Oracle Solaris. En este procedimiento, puede crear un nuevo entorno de inicio (BE) para el modo FIPS-140 y luego activar FIPS-140 en el nuevo entorno de inicio. Este método le permite recuperarse de una situación crítica del sistema que puede surgir de pruebas de cumplimiento de FIPS-140. Para obtener más información, consulte la página del comando `man cryptoadm(1M)` y [“Estructura criptográfica y FIPS-140” en la página 228](#).

**Antes de empezar** Debe asumir el rol root. Para obtener más información, consulte [“Cómo usar los derechos administrativos que tiene asignados” en la página 164](#).

### 1 Determine si el sistema está en modo FIPS-140.

```
% cryptoadm list fips-140
User-level providers:
=====
/usr/lib/security/$ISA/pkcs11_softtoken: FIPS-140 mode is disabled.

Kernel software providers:
=====
des: FIPS-140 mode is disabled.
aes: FIPS-140 mode is disabled.
ecc: FIPS-140 mode is disabled.
sha1: FIPS-140 mode is disabled.
sha2: FIPS-140 mode is disabled.
rsa: FIPS-140 mode is disabled.
swrand: FIPS-140 mode is disabled.

Kernel hardware providers:
=====;
```

### 2 Cree un nuevo entorno de inicio para su versión de FIPS-140 de la estructura criptográfica.

Antes de activar el modo FIPS-140, debe primero crear, activar e iniciar un nuevo entorno de inicio utilizando el comando `beadm`. Un sistema compatible con FIPS-140 ejecuta pruebas de cumplimiento que pueden mostrar un aviso grave en caso de error. Por lo tanto, es importante tener un entorno de inicio disponible que pueda iniciar para poner el sistema en funcionamiento mientras depura problemas con el límite FIPS-140.

#### a. Cree un entorno de inicio basado en el entorno de inicio actual.

En este ejemplo, se crea un entorno de inicio denominado `S11.1-FIPS`.

```
beadm create S11.1-FIPS-140
```

#### b. Active el entorno de inicio.

```
beadm activate S11.1-FIPS-140
```

#### c. Reinicie el sistema.

d. **Active el modo FIPS-140 en el nuevo entorno de inicio.**

```
cryptoadm enable fips-140
```

**Nota** – Este subcomando no desactiva los algoritmos aprobados que no pertenecen a FIPS-140 de la biblioteca `pkcs11_softtoken` de nivel de usuario y de los proveedores de software de núcleo. Los consumidores de la estructura son responsables del uso de algoritmos aprobados por FIPS-140.

Para obtener más información sobre los efectos del modo FIPS-140, consulte la página del comando `man cryptoadm(1M)`.

3 **Cuando desea trabajar sin el modo FIPS-140 activado, desactívelo.**

Puede reiniciar el entorno de inicio original o desactivar FIPS-140 en el entorno de inicio actual.

■ **Inicie el entorno de inicio original.**

```
beadm list
BE Active Mountpoint Space Policy Created
-- -
S11.1 - - 48.22G static 2012-10-10 10:10
S11.1-FIPS-140 NR / 287.01M static 2012-11-18 18:18
beadm activate S11.1
beadm list
BE Active Mountpoint Space Policy Created
-- -
S11.1 R - 48.22G static 2012-10-10 10:10
S11.1-FIPS-140 N / 287.01M static 2012-11-18 18:18
reboot
```

■ **Desactive el modo FIPS-140 en el entorno de inicio actual y reinicie el sistema.**

```
cryptoadm disable fips-140
```

El modo FIPS-140 permanece en funcionamiento hasta que se reinicie el sistema.

```
reboot
```

▼ **Cómo evitar el uso de un mecanismo de nivel de usuario**

Si algunos de los mecanismos criptográficos de un proveedor de biblioteca no se deben utilizar, puede eliminar los mecanismos seleccionados. Este procedimiento utiliza el mecanismo DES en la biblioteca `pkcs11_softtoken` como ejemplo.

**Antes de empezar**

Debe convertirse en un administrador con el perfil de derechos de gestión de criptografía asignado. Para obtener más información, consulte [“Cómo usar los derechos administrativos que tiene asignados” en la página 164.](#)

**1 Muestre los mecanismos ofrecidos por un proveedor de software de nivel de usuario determinado.**

```
% cryptoadm list -m provider=/usr/lib/security/\$ISA/pkcs11_softtoken.so
/usr/lib/security/\$ISA/pkcs11_softtoken.so:
CKM_DES_CBC,CKM_DES_CBC_PAD,CKM_DES_ECB,CKM_DES_KEY_GEN,
CKM_DES3_CBC,CKM_DES3_CBC_PAD,CKM_DES3_ECB,CKM_DES3_KEY_GEN,
CKM_AES_CBC,CKM_AES_CBC_PAD,CKM_AES_ECB,CKM_AES_KEY_GEN,
...
```

**2 Muestre los mecanismos que están disponibles para su uso.**

```
$ cryptoadm list -p
user-level providers:
=====
...
/usr/lib/security/\$ISA/pkcs11_softtoken.so: all mechanisms are enabled.
random is enabled.
...
```

**3 Desactive los mecanismos que no se deben utilizar.**

```
$ cryptoadm disable provider=/usr/lib/security/\$ISA/pkcs11_softtoken.so \
> mechanism=CKM_DES_CBC,CKM_DES_CBC_PAD,CKM_DES_ECB
```

**4 Muestre los mecanismos que están disponibles para su uso.**

```
$ cryptoadm list -p provider=/usr/lib/security/\$ISA/pkcs11_softtoken.so
/usr/lib/security/\$ISA/pkcs11_softtoken.so: all mechanisms are enabled,
except CKM_DES_ECB,CKM_DES_CBC_PAD,CKM_DES_CBC. random is enabled.
```

**Ejemplo 12–19 Activación de un mecanismo de proveedor de software de nivel de usuario**

En el ejemplo siguiente, un mecanismo DES desactivado se vuelve a poner a disposición para su uso.

```
$ cryptoadm list -m provider=/usr/lib/security/\$ISA/pkcs11_softtoken.so
/usr/lib/security/\$ISA/pkcs11_softtoken.so:
CKM_DES_CBC,CKM_DES_CBC_PAD,CKM_DES_ECB,CKM_DES_KEY_GEN,
CKM_DES3_CBC,CKM_DES3_CBC_PAD,CKM_DES3_ECB,CKM_DES3_KEY_GEN,
...
$ cryptoadm list -p provider=/usr/lib/security/\$ISA/pkcs11_softtoken.so
/usr/lib/security/\$ISA/pkcs11_softtoken.so: all mechanisms are enabled,
except CKM_DES_ECB,CKM_DES_CBC_PAD,CKM_DES_CBC. random is enabled.
$ cryptoadm enable provider=/usr/lib/security/\$ISA/pkcs11_softtoken.so \
> mechanism=CKM_DES_ECB
$ cryptoadm list -p provider=/usr/lib/security/\$ISA/pkcs11_softtoken.so
/usr/lib/security/\$ISA/pkcs11_softtoken.so: all mechanisms are enabled,
except CKM_DES_CBC_PAD,CKM_DES_CBC. random is enabled.
```

**Ejemplo 12–20 Activación de todos los mecanismos de proveedor de software de nivel de usuario**

En el ejemplo siguiente, se activan todos mecanismos de la biblioteca de nivel de usuario.

```
$ cryptoadm enable provider=/usr/lib/security/\$ISA/pkcs11_softtoken.so all
$ cryptoadm list -p provider=/usr/lib/security/\$ISA/pkcs11_softtoken.so
/usr/lib/security/\$ISA/pkcs11_softtoken.so: all mechanisms are enabled.
random is enabled.
```

### Ejemplo 12–21 Eliminación permanente de la disponibilidad del proveedor de software de nivel de usuario

En el ejemplo siguiente, se elimina la biblioteca `libpkcs11.so.1`.

```
$ cryptoadm uninstall provider=/opt/lib/\$ISA/libpkcs11.so.1
$ cryptoadm list
user-level providers:
 /usr/lib/security/\$ISA/pkcs11_kernel.so
 /usr/lib/security/\$ISA/pkcs11_softtoken.so
 /usr/lib/security/\$ISA/pkcs11_tpm.so

kernel providers:
...
```

## ▼ Cómo evitar el uso de un proveedor de software de núcleo

Si la estructura criptográfica proporciona múltiples modos de un proveedor como AES, puede eliminar un mecanismo lento para no utilizarlo o un mecanismo dañado. Este procedimiento utiliza el algoritmo AES como ejemplo.

**Antes de empezar** Debe convertirse en un administrador con el perfil de derechos de gestión de criptografía asignado. Para obtener más información, consulte [“Cómo usar los derechos administrativos que tiene asignados” en la página 164](#).

#### 1 Muestre los mecanismos ofrecidos por un proveedor de software de núcleo determinado.

```
$ cryptoadm list -m provider=aes
aes: CKM_AES_ECB,CKM_AES_CBC,CKM_AES_CTR,CKM_AES_CCM,CKM_AES_GCM,CKM_AES_GMAC,
CKM_AES_CFB128,CKM_AES_XTS,CKM_AES_XCBC_MAC
```

#### 2 Muestre los mecanismos que están disponibles para su uso.

```
$ cryptoadm list -p provider=aes
aes: all mechanisms are enabled.
```

#### 3 Desactive el mecanismo que no se debe utilizar.

```
$ cryptoadm disable provider=aes mechanism=CKM_AES_ECB
```

#### 4 Muestre los mecanismos que están disponibles para su uso.

```
$ cryptoadm list -p provider=aes
aes: all mechanisms are enabled, except CKM_AES_ECB.
```

**Ejemplo 12-22** Activación de un mecanismo de proveedor de software de núcleo

En el ejemplo siguiente, un mecanismo AES desactivado se vuelve a poner a disposición para su uso.

```
cryptoadm list -m provider=aes
aes: CKM_AES_ECB,CKM_AES_CBC,CKM_AES_CTR,CKM_AES_CCM,
CKM_AES_GCM,CKM_AES_GMAC,CKM_AES_CFB128,CKM_AES_XTS,CKM_AES_XCBC_MAC
$ cryptoadm list -p provider=aes
aes: all mechanisms are enabled, except CKM_AES_ECB.
$ cryptoadm enable provider=aes mechanism=CKM_AES_ECB
$ cryptoadm list -p provider=aes
aes: all mechanisms are enabled.
```

**Ejemplo 12-23** Eliminación temporal de la disponibilidad de un proveedor de software de núcleo

En el siguiente ejemplo, se elimina temporalmente el proveedor AES para no utilizarlo. El subcomando `unload` es útil para evitar que un proveedor se cargue automáticamente mientras el proveedor se está desinstalando. Por ejemplo, el subcomando `unload` se utilizaría durante la instalación de un parche que afecte al proveedor.

```
$ cryptoadm unload provider=aes
```

```
$ cryptoadm list
...
Kernel software providers:
 des
 aes (inactive)
 arcfour
 blowfish
 ecc
 sha1
 sha2
 md4
 md5
 rsa
 swrand
 n2rng/0
 ncp/0
 n2cp/0
```

El proveedor AES no estará disponible hasta que la estructura criptográfica se haya refrescado.

```
$ svcadm refresh system/cryptosvc
```

```
$ cryptoadm list
...
Kernel software providers:
 des
 aes
 arcfour
 blowfish
 ecc
```



```

sha1
sha2
md4
md5
rsa
swrand
n2rng/0
ncp/0
n2cp/0

```

Si un consumidor de núcleo está utilizando el proveedor de software de núcleo, el software no se descarga. Se muestra un mensaje de error y el proveedor sigue estando disponible para su uso.

### Ejemplo 12-24 Eliminación permanente de la disponibilidad de un proveedor de software

En el siguiente ejemplo, se elimina el proveedor AES para no utilizarlo. Una vez eliminado, el proveedor AES no aparece en la lista de la política de los proveedores de software de núcleo.

```
$ cryptoadm uninstall provider=aes
```

```

$ cryptoadm list
...
Kernel software providers:
 des
 arcfour
 blowfish
 ecc
 sha1
 sha2
 md4
 md5
 rsa
 swrand
 n2rng/0
 ncp/0
 n2cp/0

```

Si el consumidor de núcleo está utilizando el proveedor de software de núcleo, se muestra un mensaje de error y el proveedor sigue estando disponible para su uso.

### Ejemplo 12-25 Reinstalación de un proveedor de software de núcleo eliminado

En el siguiente ejemplo, se reinstala el proveedor de software de núcleo AES.

```

$ cryptoadm install provider=aes \
mechanism=CKM_AES_ECB,CKM_AES_CBC,CKM_AES_CTR,CKM_AES_CCM,
CKM_AES_GCM,CKM_AES_GMAC,CKM_AES_CFB128,CKM_AES_XTS,CKM_AES_XCBC_MAC

$ cryptoadm list
...
Kernel software providers:
 des
 aes

```

```
arcfour
blowfish
ecc
sha1
sha2
md4
md5
rsa
swrand
n2rng/0
ncp/0
n2cp/0
```

## ▼ Cómo mostrar proveedores de hardware

Los proveedores de hardware se ubican y cargan automáticamente. Para obtener más información, consulte la página del comando `man driver.conf(4)`.

### Antes de empezar

Cuando cuenta con hardware que piensa usar dentro de la estructura criptográfica, el hardware se registra con el SPI en el núcleo. La estructura comprueba que el controlador de hardware esté registrado. Específicamente, la estructura comprueba que el archivo de objeto del controlador esté registrado con un certificado emitido por Sun.

Por ejemplo, la placa Sun Crypto Accelerator 6000 (mca), el controlador ncp para el acelerador criptográfico en los procesadores UltraSPARC T1 y T2 (ncp), y el controlador n2cp para los procesadores UltraSPARC T2 (n2cp) conectan los mecanismos de hardware a la estructura.

Para obtener información sobre cómo registrar a su proveedor, consulte “[Firmas binarias para software de terceros](#)” en la página 227.

### 1 Muestre los proveedores de hardware que están disponibles en el sistema.

```
% cryptoadm list
...
kernel hardware providers:
ncp/0
```

### 2 Muestre los mecanismos que el chip o la placa proporcionan.

```
% cryptoadm list -m provider=ncp/0
ncp/0:
CKM_DSA
CKM_RSA_X_509
...
CKM_ECDH1_DERIVE
CKM_ECDSA
```

### 3 Muestre los mecanismos que están disponibles para su uso en el chip o la placa.

```
% cryptoadm list -p provider=ncp/0
ncp/0: all mechanisms are enabled.
```

## ▼ Cómo desactivar funciones y mecanismos del proveedor de hardware

Puede desactivar de manera selectiva los mecanismos y la función de números aleatorios de un proveedor de hardware. Para activarlos nuevamente, consulte el [Ejemplo 12-26](#). El hardware de este ejemplo, la placa Crypto Accelerator 1000 de Sun, proporciona un generador de números aleatorios.

### Antes de empezar

Debe convertirse en un administrador con el perfil de derechos de gestión de criptografía asignado. Para obtener más información, consulte [“Cómo usar los derechos administrativos que tiene asignados” en la página 164](#).

### ● Seleccione los mecanismos o la función que desea desactivar.

Muestre el proveedor de hardware.

```
cryptoadm list
...
Kernel hardware providers:
 dca/0
```

#### ■ Desactive los mecanismos seleccionados.

```
cryptoadm list -m provider=dca/0
dca/0: CKM_RSA_PKCS, CKM_RSA_X_509, CKM_DSA, CKM_DES_CBC, CKM_DES3_CBC
random is enabled.
cryptoadm disable provider=dca/0 mechanism=CKM_DES_CBC,CKM_DES3_CBC
cryptoadm list -p provider=dca/0
dca/0: all mechanisms are enabled except CKM_DES_CBC,CKM_DES3_CBC.
random is enabled.
```

#### ■ Desactive el generador de números aleatorios.

```
cryptoadm list -p provider=dca/0
dca/0: all mechanisms are enabled. random is enabled.
cryptoadm disable provider=dca/0 random
cryptoadm list -p provider=dca/0
dca/0: all mechanisms are enabled. random is disabled.
```

#### ■ Desactive todos los mecanismos. No desactive el generador de números aleatorios.

```
cryptoadm list -p provider=dca/0
dca/0: all mechanisms are enabled. random is enabled.
cryptoadm disable provider=dca/0 mechanism=all
cryptoadm list -p provider=dca/0
dca/0: all mechanisms are disabled. random is enabled.
```

#### ■ Desactive todas las funciones y los mecanismos en el hardware.

```
cryptoadm list -p provider=dca/0
dca/0: all mechanisms are enabled. random is enabled.
cryptoadm disable provider=dca/0 all
cryptoadm list -p provider=dca/0
dca/0: all mechanisms are disabled. random is disabled.
```

**Ejemplo 12–26 Activación de mecanismos y funciones en un proveedor de hardware**

En los siguientes ejemplos, los mecanismos desactivados en una herramienta de hardware se activan de manera selectiva.

```
cryptoadm list -p provider=dca/0
dca/0: all mechanisms are enabled except CKM_DES_ECB,CKM_DES3_ECB

.
random is enabled.
cryptoadm enable provider=dca/0 mechanism=CKM_DES3_ECB
cryptoadm list -p provider=dca/0
dca/0: all mechanisms are enabled except CKM_DES_ECB.
random is enabled.
```

En el ejemplo siguiente, sólo se activa el generador aleatorio.

```
cryptoadm list -p provider=dca/0
dca/0: all mechanisms are enabled, except CKM_MD5,CKM_MD5_HMAC,...
random is disabled.
cryptoadm enable provider=dca/0 random
cryptoadm list -p provider=dca/0
dca/0: all mechanisms are enabled, except CKM_MD5,CKM_MD5_HMAC,...
random is enabled.
```

En el ejemplo siguiente, sólo se activan los mecanismos. El generador aleatorio continúa desactivado.

```
cryptoadm list -p provider=dca/0
dca/0: all mechanisms are enabled, except CKM_MD5,CKM_MD5_HMAC,...
random is disabled.
cryptoadm enable provider=dca/0 mechanism=all
cryptoadm list -p provider=dca/0
dca/0: all mechanisms are enabled. random is disabled.
```

En el ejemplo siguiente, se activan todas las funciones y los mecanismos de la placa.

```
cryptoadm list -p provider=dca/0
dca/0: all mechanisms are enabled, except CKM_DES_ECB,CKM_DES3_ECB.
random is disabled.
cryptoadm enable provider=dca/0 all
cryptoadm list -p provider=dca/0
dca/0: all mechanisms are enabled. random is enabled.
```

## ▼ **Cómo actualizar o reiniciar todos los servicios criptográficos**

De manera predeterminada, la estructura criptográfica está activada. Cuando el daemon `kcfd` falla por cualquier motivo, la utilidad de gestión de servicios (SMF) se puede utilizar para reiniciar los servicios criptográficos. Para obtener más información, consulte las páginas del

comando `man smf(5)` y `svcadm(1M)`. Para ver el efecto del reinicio de servicios criptográficos en las zonas, consulte [“Zonas y servicios criptográficos” en la página 227](#).

**Antes de empezar**

Debe convertirse en un administrador con el perfil de derechos de gestión de criptografía asignado. Para obtener más información, consulte [“Cómo usar los derechos administrativos que tiene asignados” en la página 164](#).

**1 Compruebe el estado de los servicios criptográficos.**

```
% svcs cryptosvc
STATE STIME FMRI
offline Dec_09 svc:/system/cryptosvc:default
```

**2 Active los servicios criptográficos.**

```
svcadm enable svc:/system/cryptosvc
```

**Ejemplo 12–27 Actualización de los servicios criptográficos**

En el siguiente ejemplo, se actualizan los servicios criptográficos en la zona global. Por lo tanto, también se actualiza la política criptográfica de nivel de núcleo de cada zona no global.

```
svcadm refresh system/cryptosvc
```



## Estructura de gestión de claves

---

La estructura de gestión de claves (KMF) de Oracle Solaris proporciona herramientas e interfaces de programación para gestionar objetos de clave pública. Los objetos de clave pública incluyen certificados X. 509 y pares de claves públicas o privadas. Los formatos para almacenar estos objetos pueden variar. KMF también proporciona una herramienta para administrar políticas que definan el uso de certificados X. 509 por parte de las aplicaciones. KMF admite complementos de terceros

- “Administración de tecnologías de clave pública (descripción general)” en la página 259
- “Utilidades de la estructura de gestión de claves” en la página 260
- “Uso de la estructura de gestión de claves (tareas)” en la página 262

### Administración de tecnologías de clave pública (descripción general)

La estructura de gestión de claves (KMF) ofrece un enfoque unificado para administrar tecnologías de clave pública (PKI). Oracle Solaris tiene varias aplicaciones que utilizan tecnologías PKI. Cada aplicación proporciona su propias interfaces de programación, mecanismos de almacenamiento de claves y utilidades administrativas. Si una aplicación proporciona un mecanismo de cumplimiento de políticas, el mecanismo se aplica sólo a esa aplicación. Con KMF, las aplicaciones utilizan un conjunto unificado de herramientas administrativas, un conjunto único de interfaces de programación y un mecanismo único de cumplimiento de políticas. Estas funciones gestionan las necesidades de PKI de todas las aplicaciones que adoptan estas interfaces.

KMF unifica la gestión de tecnologías de clave pública con las siguientes interfaces:

- **Comando `pktool`:** este comando administra objetos PKI, como certificados, en una variedad de almacenes de claves.
- **Comando `kmfcfg`:** este comando gestiona la base de datos de políticas PKI y complementos de terceros.

Las decisiones de políticas PKI incluyen operaciones, como el método de validación para una operación. Además, una política PKI puede limitar el ámbito de un certificado. Por ejemplo, una política PKI puede afirmar que un certificado sólo se puede utilizar para fines específicos. Una política de ese tipo puede impedir que ese certificado se utilice para otras solicitudes.

- **Biblioteca KMF:** esta biblioteca contiene interfaces de programación que abstraen el mecanismo subyacente de almacenes de claves.

Las aplicaciones no tienen que elegir un determinado mecanismo de almacenes de claves, sino que pueden migrar de un mecanismo a otro. Los almacenes de claves admitidos son PKCS #11, NSS y OpenSSL. La biblioteca incluye una estructura conectable de modo que puedan agregarse mecanismos de almacenes de claves nuevos. Por lo tanto, las aplicaciones que utilizan los mecanismos nuevos requerirían sólo pequeñas modificaciones para poder utilizar un almacén de claves nuevo.

---

**Nota** – Para determinar la versión de OpenSSL que está en ejecución, escriba `openssl version`. La salida es similar a la siguiente:

```
OpenSSL 1.0.0i 19 Apr 2012
```

---

## Utilidades de la estructura de gestión de claves

KMF proporciona métodos para administrar el almacenamiento de claves y proporciona la política global para utilizar esas claves. KMF administra la política, las claves y los certificados para tres tecnologías de clave pública:

- Tokens de los proveedores PKCS #11, es decir, de la estructura criptográfica
- NSS, es decir, servicios de seguridad de red
- OpenSSL, un almacén de claves basado en archivos

La herramienta `kmfcfg` puede crear, modificar o suprimir entradas de políticas KMF. La herramienta también gestiona complementos para la estructura. KMF administra almacenes de claves a través del comando `pktool`. Para obtener más información, consulte las páginas del comando `man kmfcfg(1)` y `pktool(1)`, y las siguientes secciones.



## Gestión de políticas KMF

La política KMF se almacena en una base de datos. Todas las aplicaciones que utilizan las interfaces de programación KMF acceden internamente a esta base de datos de políticas. La base de datos puede restringir el uso de las claves y los certificados administrados por la biblioteca KMF. Cuando una aplicación intenta verificar un certificado, la aplicación comprueba la base de datos de políticas. El comando `kmfcfg` modifica la base de datos de políticas.

## Gestión de complementos de KMF

El comando `kmfcfg` proporciona los siguientes subcomandos para complementos:

- `list plugin`: enumera complementos gestionados por KMF.
- `install plugin`: instala el complemento por nombre de ruta del módulo y crea un almacén de claves para el complemento. Para eliminar el complemento de KMF, elimine el almacén de claves.
- `uninstall plugin`: elimina el complemento de KMF eliminando su almacén de claves.
- `modify plugin`: permite que se ejecute el complemento con una opción definida en el código para el complemento, como `debug`.

Para obtener más información, consulte la página del comando `man kmfcfg(1)`. Para conocer el procedimiento, consulte [“Cómo gestionar complementos de terceros en KMF” en la página 273](#).

## Gestión de almacenes de claves KMF

KMF gestiona los almacenes de claves para tres tecnologías de clave pública: tokens PKCS #11, NSS y OpenSSL. Para todas estas tecnologías, el comando `pktool` permite realizar las tareas siguientes:

- Generar un certificado autofirmado.
- Generar una solicitud de certificado.
- Generar una clave simétrica.
- Generar un par de claves públicas/privadas.
- Generar una solicitud de firma de certificado (CSR) PKCS #10 para que se envíe a una autoridad de certificado (CA) para que la firme.
- Firmar una solicitud de firma de certificado PKCS #10.
- Importar objetos al almacén de claves.
- Enumerar los objetos del almacén de claves.
- Suprimir objetos del almacén de claves.

- Descargar una CRL.

Para las tecnologías PKCS #11 y NSS, el comando `pktool` también permite definir un PIN generando una frase de contraseña:

- Generar una frase de contraseña para el almacén de claves.
- Generar una frase de contraseña para un objeto del almacén de claves.

Para ver ejemplos de cómo usar la utilidad `pktool`, consulte la página del comando `man pktool(1)` y [“Uso de la estructura de gestión de claves \(mapa de tareas\)”](#) en la página 262.

## Uso de la estructura de gestión de claves (tareas)

En esta sección, se describe cómo utilizar el comando `pktool` para gestionar los objetos de clave pública, como contraseñas, frases de contraseña, archivos, almacenes de claves, certificados y CRL.

### Uso de la estructura de gestión de claves (mapa de tareas)

La estructura de gestión de claves (KMF) permite gestionar de manera centralizada las tecnologías de clave pública.

| Tarea                            | Descripción                                                                                                              | Para obtener instrucciones                                                                                             |
|----------------------------------|--------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------|
| Crear un certificado.            | Crea un certificado para uso de PKCS #11, NSS u OpenSSL.                                                                 | <a href="#">“Cómo crear un certificado con el comando <code>pktool gencert</code>”</a> en la página 263                |
| Exportar un certificado.         | Crea un archivo con el certificado y sus claves admitidas. El archivo puede protegerse con una contraseña.               | <a href="#">“Cómo exportar un certificado y una clave privada en formato PKCS #12”</a> en la página 266                |
| Importar un certificado.         | Importa un certificado desde otro sistema.                                                                               | <a href="#">“Cómo importar un certificado al almacén de claves”</a> en la página 264                                   |
|                                  | Importa un certificado en formato PKCS #12 desde otro sistema.                                                           | Ejemplo 13–2                                                                                                           |
| Generar una frase de contraseña. | Genera una frase de contraseña para acceder a un almacén de claves PKCS #11 o a un almacén de claves NSS.                | <a href="#">“Cómo generar una frase de contraseña mediante el comando <code>pktool setpin</code>”</a> en la página 267 |
| Generar una clave simétrica.     | Genera claves simétricas para utilizar en el cifrado archivos, la creación de un MAC de un archivo, y para aplicaciones. | <a href="#">“Cómo generar una clave simétrica con el comando <code>pktool</code>”</a> en la página 230                 |

| Tarea                                                   | Descripción                                                                                                                | Para obtener instrucciones                                                                                                      |
|---------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------|
| Generar un par de claves.                               | Genera un par de claves públicas/privadas para utilizar con aplicaciones.                                                  | <a href="#">“Cómo generar un par de claves utilizando el comando <code>pktool genkeypair</code>” en la página 268</a>           |
| Generar una solicitud de firma de certificado PKCS #10. | Genera una solicitud de firma de certificado (CSR) PKCS #10 para que una autoridad de certificación (CA) externa la firme. | Página del comando <code>man pktool(1)</code>                                                                                   |
| Firmar una solicitud de firma de certificado PKCS #10.  | Firma una solicitud de firma de certificado PKCS #10.                                                                      | <a href="#">“Cómo firmar una solicitud de certificación utilizando el comando <code>pktool signcsr</code>” en la página 272</a> |
| Agregar un complemento a KMF.                           | Instala, modifica y muestra un complemento. También, elimina el complemento de la KMF.                                     | <a href="#">“Cómo gestionar complementos de terceros en KMF” en la página 273</a>                                               |

## ▼ Cómo crear un certificado con el comando `pktool gencert`

Este procedimiento crea un certificado autofirmado y almacena el certificado en el almacén de claves PKCS #11. Como parte de esta operación, también se crea un par de claves RSA públicas/privadas. La clave privada está almacenada en el almacén de claves con el certificado.

### 1 Generar un certificado autofirmado.

```
% pktool gencert [keystore=keystore] label=label-name \
subject=subject-DN serial=hex-serial-number
```

`keystore=keystore` Especifica el almacén de claves por tipo de objeto de clave pública. El valor puede ser `nss`, `pkcs11` o `file`. La palabra clave es opcional.

`label=label-name` Especifica un nombre único que el emisor asigna al certificado.

`subject=subject-DN` Especifica el nombre distintivo para el certificado.

`serial=hex-serial-number` Especifica el número de serie en formato hexadecimal. El emisor del certificado elige el número, como `0x0102030405`.

### 2 Verifique el contenido del almacén de claves.

```
% pktool list
Found number certificates.
1. (X.509 certificate)
 Label: label-name
 ID: Fingerprint that binds certificate to private key
 Subject: subject-DN
 Issuer: distinguished-name
 Serial: hex-serial-number
n. ...
```

Este comando muestra todos los certificados del almacén de claves. En el ejemplo siguiente, el almacén de claves contiene un solo certificado.

### Ejemplo 13-1 Creación de un certificado autofirmado mediante `pktool`

En el ejemplo siguiente, un usuario de My Company crea un certificado autofirmado y almacena el certificado en un almacén de claves para objetos PKCS #11. El almacén de claves está vacío inicialmente. Si el almacén de claves no se inicializó, el PIN para el token de software es `changeme`.

```
% pktool gencert keystore=pkcs11 label="My Cert" \
subject="C=US, O=My Company, OU=Security Engineering Group, CN=MyCA" \
serial=0x00000001
Enter pin for Sun Software PKCS#11 softtoken: Type PIN for token

% pktool list
Found 1 certificates.
1. (X.509 certificate)
 Label: My Cert
 ID: 12:82:17:5f:80:78:eb:44:8b:98:e3:3c:11:c0:32:5e:b6:4c:ea:eb
 Subject: C=US, O=My Company, OU=Security Engineering Group, CN=MyCA
 Issuer: C=US, O=My Company, OU=Security Engineering Group, CN=MyCA
 Serial: 0x01
```

## ▼ Cómo importar un certificado al almacén de claves

Este procedimiento describe cómo importar al almacén de claves un archivo con información PKI que se codifica con PEM o con DER sin procesar. Para un procedimiento de exportación, consulte el [Ejemplo 13-4](#).

### 1 Importe el certificado.

```
% pktool import keystore=keystore infile=infile-name label=label-name
```

### 2 Si va a importar objetos PKI privados, proporcione contraseñas cuando se le solicite.

#### a. En la petición de datos, proporcione la contraseña para el archivo.

Si está importando información PKI que es privada, como un archivo de exportación en formato PKCS #12, el archivo requiere una contraseña. El creador del archivo que está importando proporciona la contraseña PKCS #12.

```
Enter password to use for accessing the PKCS12 file: Type PKCS #12 password
```

#### b. En la petición de datos, escriba la contraseña para el almacén de claves.

```
Enter pin for Sun Software PKCS#11 softtoken: Type PIN for token
```

### 3 Verifique el contenido del almacén de claves.

```
% pktool list
Found number certificates.
1. (X.509 certificate)
 Label: label-name
 ID: Fingerprint that binds certificate to private key
 Subject: subject-DN
 Issuer: distinguished-name
 Serial: hex-serial-number
2. ...
```

#### Ejemplo 13-2 Importación de un archivo PKCS #12 al almacén de claves

En el ejemplo siguiente, el usuario importa un archivo PKCS #12 de terceros. El comando `pktool import` extrae la clave privada y el certificado del archivo `gracedata.p12`, y los almacena en el almacén de claves preferido del usuario.

```
% pktool import keystore=pkcs11 infile=gracedata.p12 label=GraceCert
Enter password to use for accessing the PKCS12 file: Type PKCS #12 password
Enter pin for Sun Software PKCS#11 softtoken: Type PIN for token
Found 1 certificate(s) and 1 key(s) in gracedata.p12
% pktool list
Found 1 certificates.
1. (X.509 certificate)
 Label: GraceCert
 ID: 12:82:17:5f:80:78:eb:44:8b:98:e3:3c:11:c0:32:5e:b6:4c:ea:eb
 Subject: C=US, O=My Company, OU=Security Engineering Group, CN=MyCA
 Issuer: C=US, O=My Company, OU=Security Engineering Group, CN=MyCA
 Serial: 0x01
```

#### Ejemplo 13-3 Importación de un certificado X.509 al almacén de claves

En el ejemplo siguiente, el usuario importa un certificado X.509 en formato PEM al almacén de claves preferido del usuario. Este certificado público no está protegido con una contraseña. El almacén de claves del usuario tampoco está protegido con una contraseña.

```
% pktool import keystore=pkcs11 infile=somecert.pem label="TheirCompany Root Cert"
% pktool list
Found 1 certificates.
1. (X.509 certificate)
 Label: TheirCompany Root Cert
 ID: 21:ae:83:98:24:d1:1f:cb:65:5b:48:75:d0:24:7f:cf:98:1f:ec:a0
 Subject: C=US, O=TheirCompany, OU=Security, CN=TheirCompany Root CA
 Issuer: C=US, O=TheirCompany, OU=Security, CN=TheirCompany Root CA
 Serial: 0x01
```

## ▼ Cómo exportar un certificado y una clave privada en formato PKCS #12

Puede crear un archivo en formato PKCS #12 para exportar a otros sistemas las claves privadas y su certificado X.509 asociado. El acceso al archivo está protegido con una contraseña.

### 1 Encuentre el certificado para exportar.

```
% pktool list
Found number certificates.
1. (X.509 certificate)
 Label: label-name
 ID: Fingerprint that binds certificate to private key
 Subject: subject-DN
 Issuer: distinguished-name
 Serial: hex-serial-number
2. ...
```

### 2 Exporte las claves y el certificado.

Utilice el almacén de claves y la etiqueta del comando `pktool list`. Proporcione un nombre de archivo para el archivo de exportación. Si el nombre contiene un espacio, escríbalo entre comillas dobles.

```
% pktool export keystore=keystore outfile=outfile-name label=label-name
```

### 3 Proteja el archivo de exportación con una contraseña.

En la petición de datos, escriba la contraseña actual para el almacén de claves. En este punto, puede crear una contraseña para el archivo de exportación. El destinatario debe proporcionar esta contraseña al importar el archivo.

```
Enter pin for Sun Software PKCS#11 softtoken: Type PIN for token
Enter password to use for accessing the PKCS12 file: Create PKCS #12 password
```

---

**Consejo** – Envíe la contraseña por separado del archivo de exportación. De acuerdo con las prácticas recomendadas, es aconsejable proporcionar la contraseña fuera de banda, por ejemplo, durante una llamada telefónica.

---

## Ejemplo 13–4 Exportación de un certificado y una clave privada en formato PKCS #12

En el siguiente ejemplo, un usuario exporta las claves privadas con su certificado X.509 asociado a un archivo PKCS #12 estándar. Este archivo se puede importar a otros almacenes de claves. La contraseña PKCS #11 protege el almacén de claves de origen. La contraseña PKCS #12 se utiliza para proteger los datos privados en el archivo PKCS #12. Esta contraseña es necesaria para importar el archivo.

```
% pktool list
Found 1 certificates.
```

```
1. (X.509 certificate)
Label: My Cert
ID: 12:82:17:5f:80:78:eb:44:8b:98:e3:3c:11:c0:32:5e:b6:4c:ea:eb
Subject: C=US, O=My Company, OU=Security Engineering Group, CN=MyCA
Issuer: C=US, O=My Company, OU=Security Engineering Group, CN=MyCA
Serial: 0x01
```

```
% pktool export keystore=pkcs11 outfile=mydata.p12 label="My Cert"
Enter pin for Sun Software PKCS#11 softtoken: Type PIN for token
Enter password to use for accessing the PKCS12 file: Create PKCS #12 password
```

A continuación, el usuario llama por teléfono al destinatario y proporciona la contraseña PKCS #12.

## ▼ Cómo generar una frase de contraseña mediante el comando `pktool setpin`

Puede generar una frase de contraseña para un objeto de un almacén de claves y para el almacén de claves en sí. La frase de contraseña es necesaria para acceder al objeto o al almacén de claves. Para ver un ejemplo de generación de una frase de contraseña para un objeto de un almacén de claves, consulte el [Ejemplo 13-4](#).

### 1 Genere una frase de contraseña para acceder a un almacén de claves.

```
% pktool setpin keystore=nss|pkcs11 dir=directory
```

La contraseña inicial para un almacén de claves PKCS #11 es `changeme`. La contraseña inicial para un almacén de claves NSS es una contraseña vacía.

### 2 Responda a las peticiones de datos.

Cuando se le solicite el token de frase de contraseña actual, escriba el PIN para un almacén de claves PKCS #11 o presione la tecla Intro para un almacén de claves NSS.

```
Enter current token passphrase: Type PIN or press the Return key
Create new passphrase: Type the passphrase that you want to use
Re-enter new passphrase: Retype the passphrase
Passphrase changed.
```

El almacén de claves está ahora protegido por la *frase de contraseña*. Si pierde la frase de contraseña, perderá el acceso a los objetos del almacén de claves.

## Ejemplo 13-5 Protección de un almacén de claves con una frase de contraseña

El ejemplo siguiente muestra cómo establecer la frase de contraseña para una base de datos NSS. Debido a que no se creó ninguna frase de contraseña, el usuario presiona la tecla de retorno en la primera petición de datos.

```
% pktool setpin keystore=nss dir=/var/nss
Enter current token passphrase: Press the Return key
Create new passphrase: has8n0NdaH
Re-enter new passphrase: has8n0NdaH
Passphrase changed.
```

## ▼ Cómo generar un par de claves utilizando el comando `pktool genkeypair`

Algunas aplicaciones requieren un par de claves públicas/privadas. En este procedimiento, podrá crear estos pares de claves y almacenarlos.

- 1 (Opcional) Si tiene previsto utilizar un almacén de claves, cree el almacén de claves.
  - Para crear e inicializar un almacén de claves PKCS #11, consulte [“Cómo generar una frase de contraseña mediante el comando `pktool setpin`” en la página 267](#).
  - Para crear e inicializar un almacén de claves NSS, consulte el [Ejemplo 13–5](#).

- 2 Cree el par de claves.

Utilice uno de los métodos siguientes.

- Cree el par de claves y almacene el par de claves en un archivo.

Las claves basadas en archivos se crean para aplicaciones que leen claves directamente de archivos en el disco. Normalmente, las aplicaciones que utilizan directamente bibliotecas criptográficas OpenSSL requieren que almacene las claves y los certificados de la aplicación en archivos.

---

**Nota** – El almacén de claves `file` no admite claves y certificados de curva elíptica (`ec`).

---

```
% pktool genkeypair keystore=file outkey=key-filename \
[format=der|pem] [keytype=rsa|dsa] [keylen=key-size]
```

`keystore=file`

El valor `file` especifica la ubicación de almacenamiento de tipo archivo para la clave.

`outkey=key-filename`

Especifica el nombre del archivo donde el par de claves se almacena.

`format=der|pem`

Especifica el formato de codificación del par de claves. La salida `der` es binaria y la salida `pem` es ASCII.



`keytype=rsa|dsa`

Especifica el tipo de par de claves que se puede almacenar en un almacén de claves `file`. Para obtener definiciones, consulte [DSA](#) y [RSA](#).

`keylen=key-size`

Especifica la longitud de la clave en bits. El número debe ser divisible por 8. Para determinar los posibles tamaños de clave, utilice el comando `cryptoadm list -vm`.

#### ■ Cree el par de claves y almacénelo en un almacén de claves PKCS #11.

Debe completar el [Paso 1](#) antes de utilizar este método.

El almacén de claves PKCS #11 se utiliza para almacenar objetos en un dispositivo de hardware. El dispositivo puede ser una tarjeta Sun Crypto Accelerator 6000, un dispositivo de módulo de plataforma de confianza (TPM) o una tarjeta inteligente que se conecta a la estructura criptográfica. PKCS #11 se puede utilizar para almacenar objetos en `softtoken`, o token basado en software, que almacena los objetos en un subdirectorio privado en el disco. Para obtener más información, consulte la página del comando `man pkcs11_softtoken(5)`.

Puede recuperar el par de claves del almacén de claves mediante una etiqueta que especifique.

```
% pktool genkeypair label=key-label \
[token=token[:manuf[:serial]]] \
[keytype=rsa|dsa|ec] [curve=ECC-Curve-Name]\
[keylen=key-size] [listcurves]
```

`label=key-label`

Especifica una etiqueta para el par de claves. El par de claves se puede recuperar del almacén de claves por su etiqueta.

`token=token[:manuf[:serial]]`

Especifica el nombre del token. De manera predeterminada, el nombre del token es Sun Software PKCS#11 softtoken.

`keytype=rsa|dsa|ec [curve=ECC-Curve-Name]`

Especifica el tipo de par de claves. Para el tipo de curva elíptica (`ec`), especifica opcionalmente un nombre de curva. Los nombres de curva se muestran como salida a la opción `listcurves`.

`keylen=key-size`

Especifica la longitud de la clave en bits. El número debe ser divisible por 8.

`listcurves`

Muestra los nombres de curva elíptica que se pueden utilizar como valores para la opción `curve=` para un tipo de clave `ec`.

#### ■ Genere un par de claves y almacénelo en un almacén de claves NSS.

El almacén de claves NSS es utilizado por servidores que dependen de NSS como interfaz criptográfica primaria.

Debe completar el [Paso 1](#) antes de utilizar este método.

```
% pktool keystore=nss genkeypair label=key-nickname \
[token=token[:manuf[:serial]]] \
[dir=directory-path] [prefix=database-prefix] \
[keytype=rsa|dsa|ec] [curve=ECC-Curve-Name] \
[keylen=key-size] [listcurves]
```

**keystore=nss**

El valor *nss* especifica la ubicación de almacenamiento de tipo NSS para la clave.

**label=nickname**

Especifica una etiqueta para el par de claves. El par de claves se puede recuperar del almacén de claves por su etiqueta.

**token=token[:manuf[:serial]]**

Especifica el nombre del token. De manera predeterminada, el token es Sun Software PKCS#11 softtoken.

**dir=directory**

Especifica la ruta de directorio a la base de datos NSS. De manera predeterminada, el valor de *directory* es el directorio actual.

**prefix=database-prefix**

Especifica el prefijo a la base de datos NSS. El valor predeterminado es sin prefijo.

**keytype=rsa|dsa|ec [curve=ECC-Curve-Name]**

Especifica el tipo de par de claves. Para el tipo de curva elíptica, especifica opcionalmente un nombre de curva. Los nombres de curva se muestran como salida a la opción *listcurves*.

**keylen=key-size**

Especifica la longitud de la clave en bits. El número debe ser divisible por 8.

**listcurves**

Muestra los nombres de curva elíptica que se pueden utilizar como valores para la opción *curve=* para un tipo de clave *ec*.

### 3 (Opcional) Compruebe que la clave exista.

Utilice uno de los siguientes comandos, según dónde haya guardado la clave:

- **Verifique la clave en el archivo *key-filename*.**

```
% pktool list keystore=file objtype=key infile=key-filename
Found n keys.
Key #1 - keytype:location (keylen)
```

- **Verifique la clave en el almacén de claves PKCS #11.**

```
$ pktool list objtype=key
Enter PIN for keystore:
Found n keys.
Key #1 - keytype:location (keylen)
```

- **Verifique la clave en el almacén de claves NSS.**

```
% pktool list keystore=nss dir=directory objtype=key
```

### Ejemplo 13–6 Creación de un par de claves utilizando el comando pktool

En el siguiente ejemplo, un usuario crea un almacén de claves PKCS #11 por primera vez. Después de determinar los tamaños de clave para los pares de claves RSA, el usuario genera un par de claves para una aplicación. Por último, el usuario verifica que el par de claves se encuentre en el almacén de claves. El usuario nota que la segunda instancia del par de claves RSA se puede almacenar en el hardware. Dado que el usuario no especifica un argumento token, el par de claves se almacena como un Sun Software PKCS#11 softtoken.

```
pktool setpin
Create new passphrase: Easily remembered, hard-to-detect password
Re-enter new passphrase: Retype password
Passphrase changed.
% cryptoadm list -vm | grep PAIR
...
CKM_DSA_KEY_PAIR_GEN 512 3072 X
CKM_RSA_PKCS_KEY_PAIR_GEN 256 8192 X
...
CKM_RSA_PKCS_KEY_PAIR_GEN 256 2048 X X
ecc: CKM_EC_KEY_PAIR_GEN,CKM_ECDH1_DERIVE,CKM_ECDSA,CKM_ECDSA_SHA1
% pktool genkeypair label=specialappkeypair keytype=rsa keylen=2048
Enter PIN for Sun Software PKCS#11 softtoken : Type password

% pktool list
Enter PIN for Sun Software PKCS#11 softtoken : Type password

Found 1 keys.
Key #1 - keypair: specialappkeypair (2048 bits)
```

### Ejemplo 13–7 Creación de un par de claves que utiliza el algoritmo de curva elíptica

En el siguiente ejemplo, un usuario agrega un par de claves de curva elíptica (ec) al almacén de claves, especifica un nombre de curva y verifica que el par de claves se encuentre en el almacén de claves.

```
% pktool genkeypair listcurves
secp112r1, secp112r2, secp128r1, secp128r2, secp160k1
.
.
.
c2pnb304w1, c2tnb359v1, c2pnb368w1, c2tnb431r1, prime192v2
prime192v3
% pktool genkeypair label=eckeypair keytype=ec curves=c2tnb431r1
% pktool list
Enter PIN for Sun Software PKCS#11 softtoken : Type password
```

Found 2 keys.

Key #1 - keypair: specialappkeypair (2048 bits)

Key #2 - keypair: eckeypair (c2tnb431r1)

## ▼ Cómo firmar una solicitud de certificación utilizando el comando `pktool signcsr`

Este procedimiento se utiliza para firmar una solicitud de firma de certificado (CSR) PKCS #10. CSR puede estar en formato PEM o DER. El proceso de firma emite un certificado X.509 v3. Para generar una CSR PKCS #10, consulte la página del comando `man pktool(1)`.

### Antes de empezar

Es una autoridad de certificación (CA), ha recibido una CSR y está almacenada en un archivo.

#### 1 Recopile la siguiente información para los argumentos necesarios en el comando `pktool signcsr`:

`signkey` Si ha almacenado la clave del firmante en un almacén de claves PKCS #11, `signkey` es la *etiqueta* que recupera esta clave privada.

Si ha almacenado la clave del firmante en un almacén de claves NSS o un almacén de claves de archivos, `signkey` es el nombre de archivo que alberga esta clave privada.

`csr` Especifica el nombre de archivo de la CSR.

`serial` Especifica el número de serie del certificado firmado.

`outcer` Especifica el nombre de archivo para el certificado firmado.

`issuer` Especifica el nombre del emisor de CA en formato de nombre distinguido (DN).

Para obtener más información sobre argumentos opcionales para el subcomando `signcsr`, consulte la página del comando `man pktool(1)`.

#### 2 Firme la solicitud y emita el certificado.

Por ejemplo, el siguiente comando firma el certificado con la clave del firmante del repositorio PKCS #11:

```
pktool signcsr signkey=CASigningKey \
csr=fromExampleCoCSR \
serial=0x12345678 \
outcert=ExampleCoCert2010 \
issuer="O=Oracle Corporation, \
OU=Oracle Solaris Security Technology, L=Redwood City, ST=CA, C=US, \
CN=rootsign Oracle"
```

El siguiente comando firma el certificado con la clave del firmante de un archivo:

```
pktool signcsr signkey=CASigningKey \
csr=fromExampleCoCSR \
serial=0x12345678 \
outcert=ExampleCoCert2010 \
issuer="O=Oracle Corporation, \
 OU=Oracle Solaris Security Technology, L=Redwood City, ST=CA, C=US, \
 CN=rootsign Oracle"
```

### 3 Envíe el certificado al solicitante.

Puede utilizar el correo electrónico, un sitio web u otro mecanismo para entregar el certificado al solicitante.

Por ejemplo, puede utilizar el correo electrónico para enviar el archivo `ExampleCoCert2010` al solicitante.

## ▼ Cómo gestionar complementos de terceros en KMF

Identifica el complemento proporcionándole un nombre de almacén de claves. Al agregar el complemento a KMF, el software lo identifica por su nombre de almacén de claves. El complemento se puede definir para aceptar una opción. Este procedimiento incluye cómo eliminar el complemento de KMF.

### 1 Instale el complemento.

```
% /usr/bin/kmfcfg install keystore=keystore-name \
modulepath=path-to-plugin [option="option-string"]
```

Donde

*keystore-name*: especifica un nombre único para el almacén de claves que proporciona.

*path-to-plugin*: especifica la ruta completa al objeto de biblioteca compartida para el complemento KMF.

*option-string*: especifica un argumento opcional a un objeto de biblioteca compartida.

### 2 Enumere los complementos.

```
% kmfcfg list plugin
keystore-name:path-to-plugin [(built-in)] | [;option=option-string]
```

### 3 Para eliminar el complemento, desinstálelo y verifique que se haya quitado.

```
% kmfcfg uninstall keystore=keystore-name
% kmfcfg plugin list
```

**Ejemplo 13-8** Llamada a un complemento KMF con una opción

En el siguiente ejemplo, el administrador almacena un complemento KMF en un directorio específico de sitio. El complemento se define para aceptar una opción debug. El administrador agrega el complemento y verifica que el complemento esté instalado.

```
/usr/bin/kmfcfg install keystore=mykmfplug \
modulepath=/lib/security/site-modules/mykmfplug.so
kmfcfg list plugin
KMF plugin information:

pkcs11:kmf_pkcs11.so.1 (built-in)
file:kmf_openssl.so.1 (built-in)
nss:kmf_nss.so.1 (built-in)
mykmfplug:/lib/security/site-modules/mykmfplug.so
kmfcfg modify plugin keystore=mykmfplug option="debug"
kmfcfg list plugin
KMF plugin information:

...
mykmfplug:/lib/security/site-modules/mykmfplug.so;option=debug
```

El complemento ahora se ejecuta en modo de depuración.

## P A R T E V

# Servicios de autenticación y comunicación segura

En esta sección se tratan los servicios de autenticación que se pueden configurar en un sistema que no está conectado a la red o entre dos sistemas.

- [Capítulo 14, “Uso de módulos de autenticación conectables”](#)
- [Capítulo 15, “Uso de Secure Shell”](#)
- [Capítulo 16, “Secure Shell \(referencia\)”](#)
- [Capítulo 17, “Uso de autenticación simple y capa de seguridad”](#)
- [Capítulo 18, “Autenticación de servicios de red \(tareas\)”](#)

Para configurar una red de usuarios autenticados y sistemas, consulte la [Parte VI](#).





## Uso de módulos de autenticación conectables

---

En este capítulo, se trata la estructura del módulo de autenticación conectable (PAM, Pluggable Authentication Module). PAM proporciona un método para “conectar” servicios de autenticación en el SO Oracle Solaris. PAM proporciona compatibilidad para varios servicios de autenticación al acceder a un sistema.

- “PAM (descripción general)” en la página 277
- “PAM (tareas)” en la página 279
- “Configuración de PAM (referencia)” en la página 285

### PAM (descripción general)

La estructura del módulo de autenticación conectable (PAM) permite “conectar” nuevos servicios de autenticación sin modificar los servicios del sistema, como `login`, `su` y `ssh`. También puede utilizar PAM para integrar el inicio de sesión de UNIX con otros mecanismos de seguridad, como Kerberos. También se pueden “conectar” mediante esta estructura mecanismos para la gestión de cuentas, credenciales, sesiones y contraseñas.

### Ventajas del uso de PAM

La estructura PAM permite configurar el uso de servicios del sistema (como `su`, `login` o `ssh`) para la autenticación del usuario. Algunas ventajas que ofrece PAM son:

- Política de configuración flexible
  - Política de autenticación por aplicación
  - Política de autenticación por usuario
  - La capacidad de elegir un mecanismo de autenticación predeterminado
  - La capacidad de requerir varias autorizaciones en sistemas de seguridad elevada
- Facilidad de uso para el usuario final

- La capacidad de no tener que volver a escribir las contraseñas si son iguales para diferentes servicios de autenticación
- La capacidad de solicitar al usuario contraseñas para varios servicios de autenticación sin necesidad de que el usuario escriba varios comandos
- La capacidad de transferir opciones a los servicios de autenticación de usuario.
- La capacidad de implementar una política de seguridad específico del sitio sin tener que cambiar los servicios de entrada del sistema

## Introducción a la estructura PAM

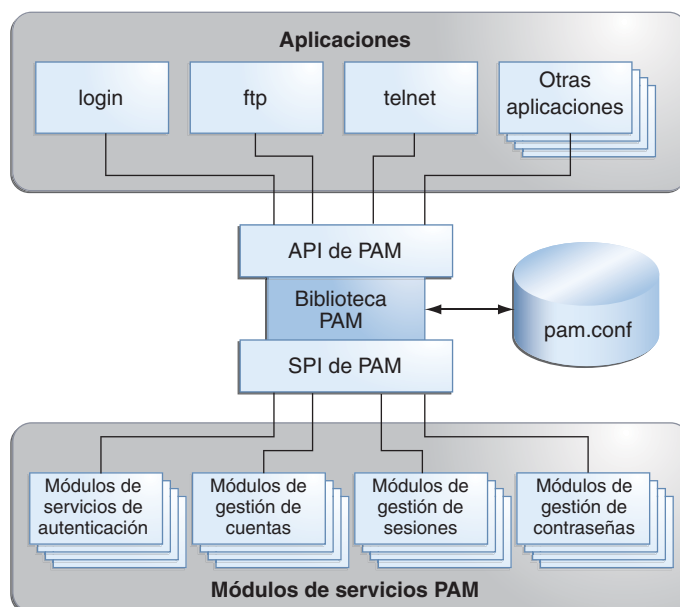
La estructura PAM consta de cuatro partes:

- Consumidores PAM
- Biblioteca PAM
- Configuración PAM
- Módulos de servicios PAM, también denominados proveedores

La estructura proporciona un modo uniforme para llevar a cabo las actividades relacionadas con la autenticación. Este enfoque permite a los desarrolladores de aplicaciones usar los servicios PAM sin tener que conocer la semántica de la política. Los algoritmos se proporcionan de forma centralizada. Los algoritmos se pueden modificar independientemente de las aplicaciones individuales. Con PAM, los administradores pueden adaptar el proceso de autenticación a las necesidades de un determinado sistema sin tener que cambiar ninguna aplicación. Los ajustes se realizan a través de la configuración PAM.

La siguiente figura ilustra la arquitectura PAM. Las aplicaciones se comunican con la biblioteca PAM a través de la interfaz de programación de aplicaciones (API) de PAM. Los módulos PAM se comunican con la biblioteca PAM a través de la interfaz del proveedor de servicios (SPI) de PAM. Por lo tanto, la biblioteca PAM permite a las aplicaciones y los módulos comunicarse entre sí.

FIGURA 14-1 Arquitectura PAM



## Cambios en PAM para esta versión

La estructura PAM incluida en la versión Oracle Solaris 11.1 incluye varias características nuevas, entre las que se incluyen:

- Indicador de control definitive
- Configuración por servicio
- Configuración por usuario

## PAM (tareas)

En esta sección, se tratan algunas tareas que pueden ser necesarias para que la estructura PAM use una determinada política de seguridad. Debe tener en cuenta algunos problemas de seguridad asociados a los archivos de configuración PAM. Para obtener información sobre los problemas de seguridad, consulte [“Planificación de la implementación de PAM” en la página 280](#).

## PAM (mapa de tareas)

| Tarea                                                     | Descripción                                                                                                                                                                                                  | Para obtener instrucciones                                                                             |
|-----------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------|
| Planificar la instalación de PAM                          | Tenga en cuenta los problemas de configuración y tome decisiones acerca de ellos antes de iniciar el proceso de configuración de software.                                                                   | <a href="#">“Planificación de la implementación de PAM” en la página 280</a>                           |
| Agregar nuevos módulos PAM                                | A veces, se deben escribir e instalar módulos específicos del sitio para satisfacer requisitos que no forman parte del software genérico. Este procedimiento explica cómo instalar estos nuevos módulos PAM. | <a href="#">“Cómo agregar un módulo PAM” en la página 281</a>                                          |
| Asignar una nueva política PAM a un usuario.              | Se establecen requisitos de autenticación específicos para varios servicios que se van a asignar a un determinado usuario.                                                                                   | <a href="#">“Cómo asignar una política PAM personalizada a un usuario” en la página 283</a>            |
| Asignar un nuevo perfil de derechos a todos los usuarios. | Se establecen requisitos de autenticación específicos para varios servicios que se van a asignar a todos los usuarios en el sistema.                                                                         | <a href="#">“Cómo asignar una nueva política de derechos a todos los usuarios” en la página 284</a>    |
| Bloquear el acceso a través de ~/.rhosts                  | Se impide el acceso a través de ~/.rhosts para mejorar aún más la seguridad.                                                                                                                                 | <a href="#">“Cómo evitar el acceso de tipo .rhost desde sistemas remotos con PAM” en la página 282</a> |
| Iniciar el registro de errores                            | Inicie el registro de mensajes de error relacionados con PAM mediante syslog.                                                                                                                                | <a href="#">“Cómo registrar los informes de errores de PAM” en la página 282</a>                       |

## Planificación de la implementación de PAM

Tal como se suministra, el archivo de configuración PAM implementa la política de seguridad estándar. Esta política funciona en diversas situaciones. Si debe implementar una política de seguridad distinta, aquí se muestran los problemas en los que se debe centrar:

- Determine cuáles son sus necesidades, especialmente qué módulos de servicios PAM debe seleccionar.
- Identifique los servicios que necesitan opciones de configuración especiales. Use el nombre de servicio `other` para proporcionar valores predeterminados para los servicios, si es apropiado.
- Decida el orden en que se deben ejecutar los módulos.
- Seleccione el indicador de control para cada módulo. Consulte [“Cómo funciona el apilamiento PAM” en la página 287](#) para obtener más información sobre todos los indicadores de control.
- Seleccione las opciones que son necesarias para cada módulo. La página del comando `man` de cada módulo debe enumerar las opciones especiales.

A continuación, exponemos algunas sugerencias que se deben tener en cuenta antes de cambiar la configuración PAM:

- Use entradas de nombre de servicio `other` para cada tipo de módulo para que cada aplicación no tenga que ser incluida en la configuración PAM.
- Asegúrese de tener en cuenta las implicaciones de seguridad de los indicadores de control.
- Revise las páginas del comando `man` que están asociadas a los módulos. Estas páginas del comando `man` puede ayudar a comprender cómo funciona cada módulo, qué opciones están disponibles y las interacciones entre los módulos apilados.




---

**Precaución** – Si la configuración PAM no está configurada correctamente o se daña, es posible que ningún usuario pueda iniciar sesión. Como el comando `su` `login` no utiliza PAM, se necesita la contraseña de usuario `root` para iniciar el equipo en modo de usuario único y corregir el problema.

---

Después de cambiar la configuración PAM, revise el archivo lo más posible mientras sigue teniendo acceso al sistema para corregir problemas. Pruebe todos los comandos que posiblemente hayan sido afectados por los cambios.

## ▼ Cómo agregar un módulo PAM

Este procedimiento muestra cómo agregar un nuevo módulo PAM. Es posible crear nuevos módulos para satisfacer políticas de seguridad específicas del sitio o para admitir aplicaciones de terceros.

### Antes de empezar

Debe asumir el rol `root`. Para obtener más información, consulte [“Cómo usar los derechos administrativos que tiene asignados” en la página 164](#).

- 1 **Determine qué indicadores de control y qué opciones se deben utilizar.**  
Consulte [“Cómo funciona el apilamiento PAM” en la página 287](#) para obtener información sobre los indicadores de control.
- 2 **Asegúrese de que la propiedad y los permisos estén definidos de modo que el archivo del módulo sea propiedad de `root` y los permisos sean `555`.**
- 3 **Use `pfedit` para editar un archivo de configuración PAM apropiado y agregue este módulo a los servicios apropiados.**

Se pueden realizar cambios a `/etc/pam.conf` o `/etc/pam.d/service`.

#### 4 Verifique que el módulo se haya agregado correctamente.

Es necesario realizar una comprobación en caso de que el archivo de configuración no esté configurado correctamente. Inicie sesión con un servicio directo, como ssh, y ejecute el comando su.

## ▼ Cómo evitar el acceso de tipo .rhost desde sistemas remotos con PAM

---

**Nota** – El servicio rsh no está activado de manera predeterminada. Para proporcionar una conexión segura, use el comando ssh en su lugar.

---

**Antes de empezar** Debe asumir el rol root. Para obtener más información, consulte [“Cómo usar los derechos administrativos que tiene asignados” en la página 164.](#)

#### 1 Elimine todas las líneas que incluyen rhosts\_auth.so.1 de los archivos de configuración PAM.

Este paso impide la lectura de los archivos ~/.rhosts durante una sesión rlogin. Por lo tanto, este paso impide el acceso no autenticado al sistema local desde sistemas remotos. Cualquier acceso rlogin requiere una contraseña, independientemente de la presencia o el contenido de los archivos ~/.rhosts o /etc/hosts.equiv.

#### 2 Desactive el servicio rsh.

Para evitar el acceso no autenticado al sistema, recuerde desactivar el servicio rsh.

```
svcadm disable network/shell:default
```

#### 3 Desactive el servicio rlogin.

Desactive también el servicio rlogin, si es necesario.

```
svcadm disable network/login:rlogin
```

## ▼ Cómo registrar los informes de errores de PAM

**Antes de empezar** Debe asumir el rol root. Para obtener más información, consulte [“Cómo usar los derechos administrativos que tiene asignados” en la página 164.](#)

#### 1 Determine qué instancia del servicio system-log está en línea.

```
svcs system-log
STATE STIME FMRI
disabled 13:11:55 svc:/system/system-log:rsyslog
online 13:13:27 svc:/system/system-log:default
```

---

**Nota** – Si la instancia de servicio `rsyslog` está en línea, modifique el archivo `rsyslog.conf`.

---

## 2 Configure el archivo `/etc/syslog.conf` para el nivel de registro que necesite.

Consulte la página del comando `man syslog.conf(4)` para obtener más información sobre niveles de registro. La mayoría de los informes de errores PAM se realiza para la utilidad `LOG_AUTH`.

## 3 Refresque la información de configuración para el servicio `system-log`.

```
svcadm refresh system-log:default
```

---

**Nota** – Refresque la instancia de servicio `system-log:rsyslog` si el servicio `rsyslog` está en línea.

---

# ▼ Cómo asignar una política PAM personalizada a un usuario

## Antes de empezar

Debe asumir el rol `root`. Para obtener más información, consulte “[Cómo usar los derechos administrativos que tiene asignados](#)” en la página 164.

## 1 Cree un nuevo archivo de configuración de política PAM.

Consulte los comentarios en el texto siguiente para obtener una descripción de los efectos que produce el archivo.

```
cat /etc/opt/pam_policy/custom-config
#
PAM configuration which uses UNIX authentication for console logins,
LDAP for SSH keyboard-interactive logins, and denies telnet logins.
#
login auth requisite pam_authtok_get.so.1
login auth required pam_dhkeys.so.1
login auth required pam_unix_auth.so.1
login auth required pam_unix_cred.so.1
login auth required pam_dial_auth.so.1
#
sshd-kbdint auth requisite pam_authtok_get.so.1
sshd-kbdint auth binding pam_unix_auth.so.1 server_policy
sshd-kbdint auth required pam_unix_cred.so.1
sshd-kbdint auth required pam_ldap.so.1
#
telnet auth requisite pam_deny.so.1
telnet account requisite pam_deny.so.1
telnet session requisite pam_deny.so.1
telnet password requisite pam_deny.so.1
```

**2 Compruebe los permisos de archivo en el nuevo archivo.**

El archivo debe ser propiedad de root y no puede ser escrito por grupos ni por cualquier persona.

```
ls -l /etc/opt/pam_policy
total 5
-r--r--r-- 1 root 4570 Jun 21 12:08 custom-config
```

**3 Asigne la nueva política PAM a un usuario.**

El archivo custom-config en /etc/opt/pam\_policy está asignado al usuario denominado jill.

```
useradd -K pam_policy=/etc/opt/pam_policy/custom-config jill
```

## ▼ Cómo asignar una nueva política de derechos a todos los usuarios

**Antes de empezar**

Debe asumir el rol root. Para obtener más información, consulte [“Cómo usar los derechos administrativos que tiene asignados” en la página 164](#).

**1 Cree una nueva política de derechos.**

En este ejemplo, se utiliza la política PAM ldap.

```
profiles -p "PAM Per-User Policy of LDAP" \
 'set desc="Profile which sets pam_policy=ldap";
 set pam_policy=ldap; exit;'
```

**2 Asigne un nuevo perfil de derechos a todos los usuarios.**

Use pfedit para agregar la nueva política a la declaración PROFS\_GRANTED.

```
cat /etc/security/policy.conf
.
.

AUTHS_GRANTED=
PROFS_GRANTED=Basic Solaris User,PAM Per-User Policy of LDAP
CONSOLE_USER=Console User
```

**Ejemplo 14–1 Asignación de un perfil de derechos a un usuario**

Si se ha creado un perfil como se mostró en el paso 1 del procedimiento anterior, ese perfil de derechos puede asignarse a un usuario mediante el siguiente comando:

```
usermod -P +"PAM Per-User Policy of LDAP" jill
```



## Configuración de PAM (referencia)

Las aplicaciones del sistema, como ssh, que usan el servicio PAM están configuradas en los archivos de configuración PAM. Consulte la página del comando `man pam.conf(4)` para obtener más información. Estos archivos de configuración incluyen el archivo `/etc/pam.conf`, así como archivos específicos del servicio ubicados en `/etc/pam.d`. Los cambios que se realizan en estos archivos afectan a todos los usuarios del sistema. Los archivos de configuración PAM específicos del servicio constituyen el mecanismo preferido para la configuración PAM, ya que su granularidad implica que un error en un archivo solamente afecta a ese servicio. También, la agregación de nuevos servicios PAM se simplifica a la copia de un único archivo. Los archivos específicos del servicio permiten una mejor interoperabilidad con otras aplicaciones PAM entre plataformas, ya que `/etc/pam.d` es la configuración predeterminada en la mayoría de las implementaciones PAM.

Además, los archivos de política PAM pueden utilizarse para crear políticas de autenticación para servicios individuales y asignar esas políticas tanto a un individuo, un grupo de individuos o a todos los usuarios, según sea necesario. Los archivos de política PAM predeterminados se ubican en `/etc/security/pam_policy`. Los archivos de política PAM ofrecen la posibilidad de establecer o cambiar la política de autenticación para uno o más usuarios de manera segura y fiable.

El administrador del sistema gestiona los archivos de configuración PAM. Un orden incorrecto de las entradas en estos archivos puede provocar efectos secundarios imprevistos. Por ejemplo, un archivo configurado incorrectamente puede bloquear los usuarios de manera que el modo de usuario único resulta necesario para su reparación. Para obtener una descripción acerca de cómo establecer el orden, consulte “[Cómo funciona el apilamiento PAM](#)” en la [página 287](#).

## Orden de búsqueda de configuración PAM

La información de configuración PAM de los archivos de configuración PAM es recopilada por la biblioteca PAM en el siguiente orden:

1. El nombre del servicio se busca en `/etc/pam.conf`.
2. Se comprueba `/etc/pam.d/service`.
3. El nombre de servicio `other` se comprueba en `/etc/pam.conf`.
4. Se comprueba el archivo `/etc/pam.d/other`.

Este orden permite que un archivo `/etc/pam.conf` existente trabaje con los archivos de configuración PAM por servicio ubicados en `/etc/pam.d`.

## Sintaxis de archivo de configuración de PAM

El archivo `/etc/pam.conf` y los archivos de política PAM usan una sintaxis que es diferente a la de los archivos específicos del servicio. La sintaxis de cada uno de estos archivos se describe a continuación.

Las entradas en `/etc/pam.conf` o en los archivos de política PAM se encuentran en uno de los siguientes formatos:

*service-name module-type control-flag module-path module-options*

*service-name module-type include path-to-included-PAM-configuration*

*service-name* El nombre del servicio que no distingue mayúsculas de minúsculas, por ejemplo, `login` o `passwd`. Una aplicación puede utilizar distintos nombres para los servicios que la aplicación proporciona. Por ejemplo, el daemon de shell seguro de Oracle Solaris utiliza estos nombres de servicio: `sshd - none`, `sshd - password`, `sshd - kbdint`, `sshd - pubkey` y `sshd - hostbased`.

El nombre de servicio `other` es un nombre predefinido que se usa como un nombre de servicio comodín. Si no se encuentra un determinado nombre de servicio en el archivo de configuración, se utiliza la configuración de `other`.

*module-type* El tipo de servicio, es decir, `auth`, `account`, `session` o `password`.

*control-flag* Indica el rol del módulo en la determinación del valor de éxito o error integrado del servicio. Los indicadores de control válidos son: `binding`, `definitive`, `include`, `optional`, `required`, `requisite` y `sufficient`. Consulte [“Cómo funciona el apilamiento PAM” en la página 287](#) para obtener información sobre el uso de estos indicadores.

*module-path* La ruta del objeto de la biblioteca que implementa el servicio. Si el nombre de la ruta no es absoluto, se asume que es relativo a `/usr/lib/security/$ISA/`. Utilice la macro dependiente de la arquitectura `$ISA` para que `libpam` busque en el directorio la arquitectura específica de la aplicación.

*module-options* Opciones que se transfieren a los módulos de servicios. La página del comando `man` de un módulo describe las opciones aceptadas por ese módulo. Las opciones típicas del módulo incluyen `nowarn` y `debug`.

*path-to-included-PAM-configuration* Proporciona la ruta completa para un archivo de configuración PAM independiente o un nombre de

ruta relativo al archivo `/usr/lib/security`.

Los archivos de configuración por servicio ubicados en `/etc/pam.d` usan la misma sintaxis que `pam.conf`, pero no incluyen el nombre de servicio. Al utilizar los archivos de configuración por servicio, el nombre del archivo es el nombre del servicio. Por ejemplo, `/etc/pam.d/cron` incluye la configuración PAM para el comando `cron`.

## Política de autenticación por usuario

El módulo PAM `pam_user_policy` permite a los administradores del sistema especificar configuraciones PAM en función de cada usuario. La clave `pam_policy` para el usuario necesita proporcionar la ruta para un archivo de configuración PAM específico del usuario. Consulte la página del comando `man pam_user_policy(5)` para obtener más información.

A continuación, se indican algunas maneras de establecer una política de autenticación por usuario:

- Cree un nuevo archivo de política PAM para un usuario y, luego, use el comando `usermod` para asignar la política al usuario. Hay información sobre este procedimiento disponible en [“Cómo asignar una política PAM personalizada a un usuario” en la página 283](#).
- Use el comando `usermod` para asignar una política predefinida a un usuario.
- Asigne un perfil de derechos que incluya una clave `pam_policy` para un usuario utilizando la opción `-P` para el comando `usermod`.
- Asigne un perfil de derechos que incluya una clave `pam_policy` para todos los usuarios agregándola a la clave `PROFS_GRANTED` en `/etc/security/policy.conf`. Hay información sobre este procedimiento disponible en [“Cómo asignar una nueva política de derechos a todos los usuarios” en la página 284](#).

## Cómo funciona el apilamiento PAM

Cuando una aplicación llama a una de las siguientes funciones, `libpam` lee los archivos de configuración PAM para determinar qué módulos participan en la operación para este servicio:

- `pam_authenticate(3PAM)`
- `pam_acct_mgmt(3PAM)`
- `pam_setcred(3PAM)`
- `pam_open_session(3PAM)`
- `pam_close_session(3PAM)`
- `pam_chauthtok(3PAM)`

Si los archivos de configuración contienen solamente un módulo para una operación para este servicio, como la autenticación o la gestión de cuentas, el resultado de ese módulo determina el

resultado de la operación. Por ejemplo, la operación de autenticación predeterminada para la aplicación `passwd` contiene un módulo, `pam_passwd_auth.so.1`:

```
passwd auth required pam_passwd_auth.so.1
```

Por otro lado, si hay varios módulos definidos para la operación del servicio, se dice que esos módulos están *apilados* y que existe una *pila PAM* para ese servicio. Por ejemplo, analice la situación en la que `/etc/pam.d/login` contiene las siguientes entradas:

```
auth definitive pam_user_policy.so.1
auth requisite pam_authtok_get.so.1
auth required pam_unix_auth.so.1
auth required pam_dhkeys.so.1
auth required pam_unix_cred.so.1

auth required pam_dial_auth.so.1
```

Estas entradas representan un ejemplo de pila `auth` para el servicio `login`. Para determinar el resultado de esta pila, los códigos de resultado de los módulos individuales requieren un *proceso de integración*. En el proceso de integración, los módulos se ejecutan en orden, como se especifica en el archivo. Cada código de éxito o error se integra en el resultado general según el indicador de control del módulo. El indicador de control puede provocar la finalización anticipada de la pila. Por ejemplo, es posible que un módulo `requisite` o `definitive` falle, o un módulo `sufficient`, `definitive` o `binding` tenga éxito. Después del procesamiento de la pila, los resultados individuales se combinan en un único resultado general que se proporciona a la aplicación.

El indicador de control señala el rol que un módulo PAM tiene en la determinación del acceso al servicio. Los indicadores de control y sus efectos son:

- **Binding:** el éxito en el cumplimiento de los requisitos de un módulo "binding" devuelve inmediatamente un valor de éxito a la aplicación si no ha fallado ningún módulo "required" anterior. Si se cumplen estas condiciones, no se produce ninguna ejecución adicional de módulos. Un fallo provoca el registro de un fallo de `required` y la continuación del procesamiento de los módulos.
- **Definitive:** el éxito en el cumplimiento de los requisitos de un módulo "definitive" devuelve inmediatamente un valor de éxito a la aplicación si no ha fallado ningún módulo "required" anterior. Si falló un módulo "required" anterior, ese fallo se devuelve inmediatamente a la aplicación, sin ejecuciones adicionales de módulos. Un fallo provoca la devolución inmediata de error sin ejecuciones adicionales de módulos.
- **Include:** agrega líneas de un archivo de configuración PAM independiente que se utilizará en este punto en la pila PAM. Este indicador no controla el comportamiento de éxito o error. Cuando se lee un archivo nuevo, la pila PAM incluye aumenta. Cuando finaliza la comprobación de la pila en el nuevo archivo, el valor de la pila incluye disminuye. Cuando se llega al final de un archivo y la pila PAM incluye es 0, finaliza el procesamiento de la pila. El número máximo de la pila PAM incluye es 32.

- **Optional:** el éxito en el cumplimiento de los requisitos de un módulo "optional" no es necesario para utilizar el servicio. Un fallo provoca el registro de un fallo de optional.
- **Required:** el éxito en el cumplimiento de los requisitos de un módulo "required" es necesario para utilizar el servicio. Un fallo provoca la devolución de un error tras la ejecución de los módulos restantes de este servicio. El éxito final del servicio se devuelve solamente si ningún módulo binding o required ha informado fallos.
- **Requisite:** el éxito en el cumplimiento de los requisitos de un módulo "requisite" es necesario para utilizar el servicio. Un fallo provoca la devolución inmediata de error un sin ejecuciones adicionales de módulos. Todos los módulos requisite de un servicio deben devolver un valor de éxito para que la función pueda devolver un valor de éxito a la aplicación.
- **Sufficient:** si no se han producido fallos anteriores de "required", el éxito de un módulo "sufficient" devuelve un valor de éxito a la aplicación inmediatamente, sin ejecuciones adicionales de módulos. Un fallo provoca el registro de un fallo de optional.

Los dos diagramas siguientes muestran cómo se determina el acceso en el proceso de integración. El primer diagrama indica cómo se registra el éxito o error para cada tipo de indicador de control. El segundo diagrama muestra cómo se determina el valor integrado.

Administración de Oracle Solaris 11.1: servicios de seguridad • Febrero de 2014

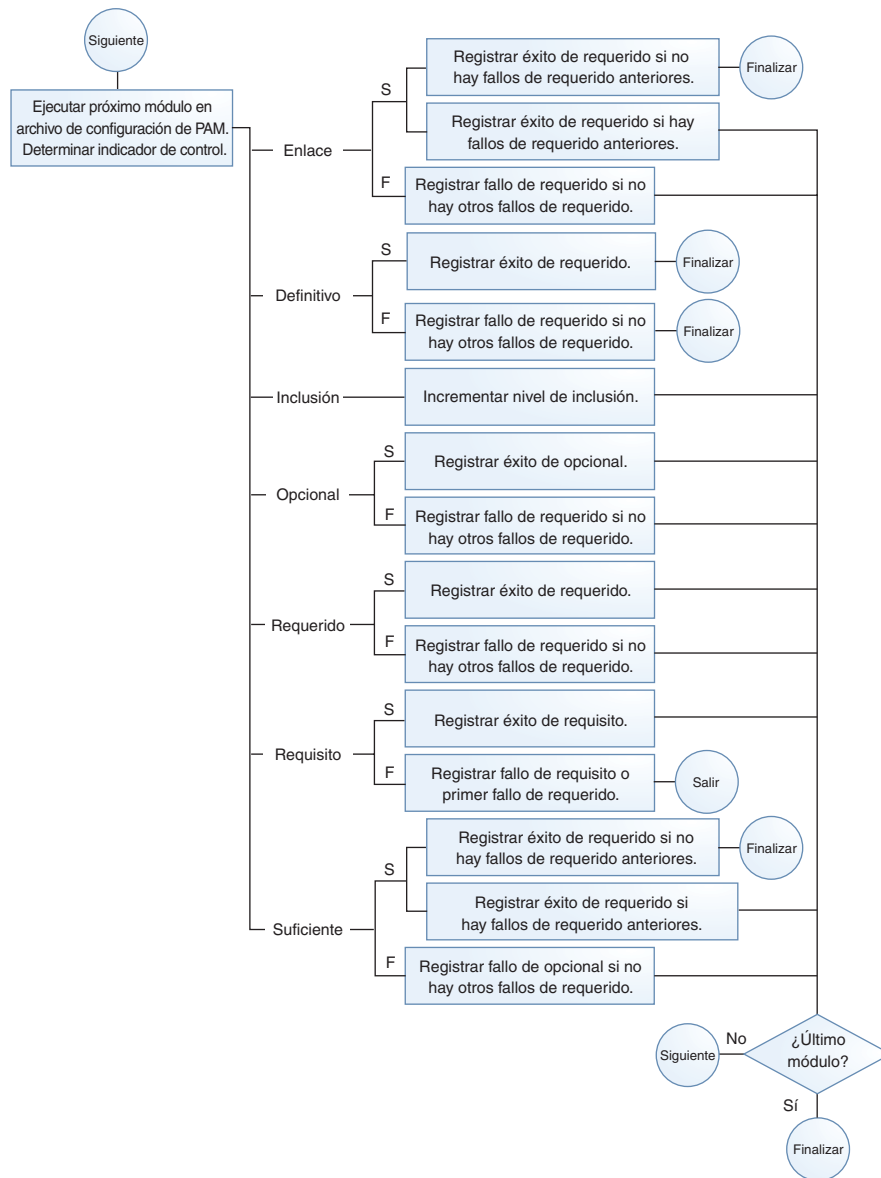
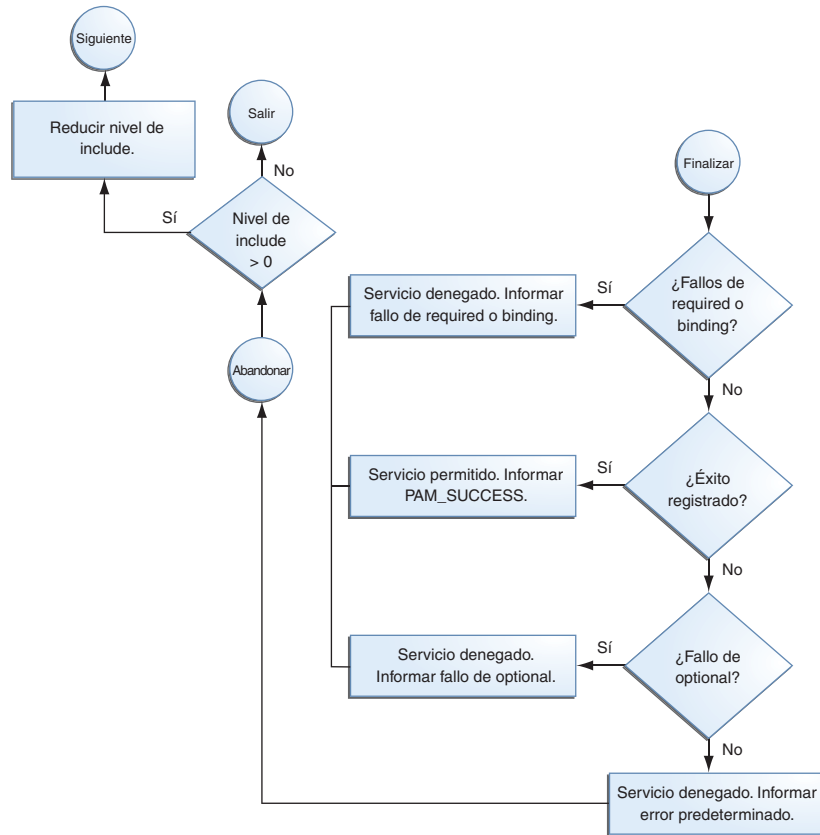


FIGURA 14-3 Apilamiento PAM: cómo se determina el valor integrado



## Ejemplo de apilamiento PAM

En este ejemplo se muestran las definiciones predeterminadas para la gestión de autenticación en el archivo `/etc/pam.d/other`. Estas definiciones se utilizan si no se han configurado definiciones específicas del servicio.

```

#
Default definitions for Authentication management
Used when service name is not explicitly mentioned for authentication
#
auth definitive pam_user_policy.so.1
auth requisite pam_authtok_get.so.1
auth required pam_dhkeys.so.1
auth required pam_unix_auth.so.1
auth required pam_unix_cred.so.1

```

En primer lugar, la política de seguridad para el usuario se comprueba mediante el módulo `pam_user_policy`. El indicador de control `definitive` selecciona que si la evaluación de la

política de seguridad se realiza con éxito, el servicio devuelve un aviso de éxito a la aplicación, ya que ningún otro módulo se habrá comprobado en ese punto. Si la solicitud falla, se envía un mensaje de error a la aplicación y no se realizan más comprobaciones. Si no hay ninguna política definida para el usuario, se ejecuta el módulo siguiente.

Si no se especifica una política PAM por usuario para este usuario, se ejecuta el módulo `pam_authtok_get`. El indicador de control de este módulo se estableció en `required`. Si `pam_authtok_get` falla, finaliza el proceso de autenticación y se devuelve un valor de error al servicio.

Si `pam_authtok_get` no falla, se ejecutan los tres próximos módulos. Estos módulos están configurados con el indicador de control `required`, para que el proceso continúe independientemente de si se devuelve un fallo individual. Después de que se ejecuta `pam_unix_cred` no queda ningún módulo. En este punto, si todos los módulos no presentan fallos, se concede acceso al usuario. Si `pam_dhkeys`, `pam_unix_auth` o `pam_unix_cred` devuelve un error, no se permite el acceso al usuario.



## Uso de Secure Shell

---

La función Secure Shell de Oracle Solaris proporciona acceso seguro a un host remoto por medio de una red no segura. El shell proporciona comandos para el inicio de sesión remoto y la transferencia de archivos remota. En este capítulo, se tratan los siguientes temas:

- “Secure Shell (descripción general)” en la página 293
- “Secure Shell y el proyecto OpenSSH” en la página 296
- “Secure Shell y FIPS-140” en la página 297
- “Configuración de Secure Shell (tareas)” en la página 298
- “Uso de Secure Shell (tareas)” en la página 304

Para obtener información de referencia, consulte el [Capítulo 16, “Secure Shell \(referencia\)”](#).

### Secure Shell (descripción general)

Secure Shell en Oracle Solaris se crea a partir del Kit de herramientas de código abierto, OpenSSL, que implementa la capa de sockets seguros y la seguridad de capa de transporte.

Dos versiones distintas del kit de herramientas están disponibles en Oracle Solaris.

- La versión 1.0.0 es la versión predeterminada donde se ejecuta Secure Shell.
- La versión 0.9.8 implementa FIPS-140, un estándar de seguridad informática del Gobierno de los EE. UU. para módulos de cifrado.

Para utilizar Secure Shell en el modo FIPS-140 (FIPS), consulte [“Secure Shell y FIPS-140” en la página 297](#).

En Secure Shell, la autenticación la proporciona el uso de contraseñas, claves públicas o ambas. Todo el tráfico de la red está cifrado. Por lo tanto, Secure Shell impide que un posible intruso pueda leer una comunicación interceptada. Secure Shell también impide que un adversario falsifique el sistema.

Secure Shell también puede utilizarse como una [red privada virtual \(VPN\)](#) a petición. Una VPN puede reenviar tráfico de sistemas de ventanas X o puede conectar números de puerto individuales entre los equipos locales y remotos mediante un enlace de red cifrado.

Con Secure Shell, puede realizar estas acciones:

- Iniciar sesión en otro host de forma segura por medio de una red no segura.
- Copiar archivos de forma segura entre los dos hosts.
- Ejecutar comandos de forma segura en el host remoto.

En el lado del servidor, Secure Shell admite la versión 2 (v2) del protocolo Secure Shell. En el cliente, además de v2, se admite la versión 1 (v1). Para obtener más información sobre v1, consulte [System Administration Guide: Security Services](#).

## Autenticación de Secure Shell

Secure Shell proporciona métodos de clave pública y contraseña para autenticar la conexión al host remoto. La autenticación de clave pública es un mecanismo de autenticación más potente que la autenticación de contraseña, porque la clave privada nunca viaja por medio de la red.

Los métodos de autenticación se prueban en el siguiente orden: cuando la configuración no satisface un método de autenticación, se prueba el siguiente método.

- **GSS-API:** utiliza credenciales para mecanismos GSS-API, como `mech_krb5` (Kerberos V) y `mech_dh` (AUTH\_DH), para autenticar clientes y servidores. Para obtener más información sobre GSS-API, consulte “[Introduction to GSS-API](#)” de *Developer’s Guide to Oracle Solaris 11 Security*.
- **Autenticación basada en host:** utiliza claves de host y archivos `rhhosts`. Utiliza las claves de host públicas y privadas RSA y DSA del cliente para autenticar el cliente. Utiliza los archivos `rhhosts` para autorizar clientes a usuarios.
- **Autenticación de clave pública:** autentica a los usuarios con sus claves públicas y privadas RSA y DSA.
- **Autenticación de contraseña:** utiliza PAM para autenticar a los usuarios. El método de autenticación de teclado en v2 permite la solicitud arbitraria por PAM. Para obtener más información, consulte la sección SECURITY en la página del comando `man sshd(1M)`.

En la siguiente tabla, se muestran los requisitos para autenticar a un usuario que está intentando iniciar sesión en un host remoto. El usuario está en el host local, el cliente. El host remoto, el servidor, está ejecutando el daemon `sshd`. En la tabla, se muestran los métodos de autenticación de Secure Shell, las versiones de protocolo compatibles y los requisitos de host.

TABLA 15-1 Métodos de autenticación para Secure Shell

| Método de autenticación                       | Requisitos de host local (cliente)                                                                                                                                               | Requisitos de host remoto (servidor)                                                                                                                                                                                                                                                                                |
|-----------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| GSS-API                                       | Credenciales de iniciador para el mecanismo GSS                                                                                                                                  | Credenciales de aceptador para el mecanismo GSS<br>Para obtener más información, consulte <a href="#">“Adquisición de credenciales GSS en Secure Shell” en la página 318.</a>                                                                                                                                       |
| Basado en host                                | Cuenta de usuario<br><br>Clave privada de host local en<br>/etc/ssh/ssh_host_rsa_key o<br>/etc/ssh/ssh_host_dsa_key<br><br>HostbasedAuthentication yes en<br>/etc/ssh/ssh_config | Cuenta de usuario<br><br>Clave pública de host local en<br>/etc/ssh/known_hosts o ~/.ssh/known_hosts<br><br>HostbasedAuthentication yes en<br>/etc/ssh/sshd_config<br><br>IgnoreRhosts no en /etc/ssh/sshd_config<br><br>Entrada de host local en /etc/ssh/shosts.equiv,<br>/etc/hosts.equiv, ~/.rhosts o ~/.shosts |
| Clave pública RSA o DSA                       | Cuenta de usuario<br><br>Clave privada en ~/.ssh/id_rsa o ~/.ssh/id_dsa<br><br>Clave pública del usuario en ~/.ssh/id_rsa.pub o<br>~/.ssh/id_dsa.pub                             | Cuenta de usuario<br><br>Clave pública del usuario en<br>~/.ssh/authorized_keys                                                                                                                                                                                                                                     |
| Basado en contraseña                          | Cuenta de usuario                                                                                                                                                                | Cuenta de usuario<br><br>Admite PAM                                                                                                                                                                                                                                                                                 |
| .rhosts con RSA (v1) en el servidor solamente | Cuenta de usuario<br><br>Clave pública de host local en<br>/etc/ssh/ssh_host_rsa1_key                                                                                            | Cuenta de usuario<br><br>Clave pública de host local en<br>/etc/ssh/ssh_known_hosts o<br>~/.ssh/known_hosts<br><br>IgnoreRhosts no en /etc/ssh/sshd_config<br><br>Entrada de host local en /etc/ssh/shosts.equiv,<br>/etc/hosts.equiv, ~/.shosts o ~/.rhosts                                                        |

## Secure Shell en la empresa

Para obtener una descripción completa de Secure Shell en un sistema Oracle Solaris, consulte *Secure Shell in the Enterprise* (Shell seguro en la empresa), por Jason Reid, ISBN 0-13-142900-0, junio de 2003. El libro forma parte de Sun BluePrints Series, publicado por Sun Microsystems Press.

## Secure Shell y el proyecto OpenSSH

Secure Shell es una bifurcación del proyecto [OpenSSH](http://www.openssh.com) (<http://www.openssh.com>). Las correcciones de seguridad para las vulnerabilidades que se detectan en versiones posteriores de OpenSSH se integran en Secure Shell, ya que son funciones y correcciones de errores individuales. El desarrollo interno continúa en la bifurcación de Secure Shell.

Las siguientes funciones se han implementado para el protocolo v2 en esta versión de Secure Shell:

- Palabra clave `ForceCommand`: fuerza la ejecución de los comandos especificados independientemente de lo que escriba el usuario en la línea de comandos. Esta palabra clave es muy útil dentro de un bloque `Match`. Esta opción de configuración `sshd_config` es similar a la opción `command="..."` en `$HOME/.ssh/authorized_keys`.
- Protección de frase de contraseña AES-128: en esta versión, las claves privadas generadas por el comando `ssh-keygen` están protegidas con el algoritmo AES-128. Este algoritmo protege las claves recientemente generadas y las claves que se volvieron a cifrar, por ejemplo, cuando se cambia la frase de contraseña.
- Opción `-u` para el comando `sftp-server`: permite al usuario establecer una `umask` explícita en archivos y directorios. Esta opción sustituye la `umask` predeterminada del usuario. Para ver un ejemplo, consulte la descripción de `Subsystem` en la página del comando `man sshd_config(4)`.
- Palabras clave adicionales para bloques `Match`: `AuthorizedKeysFile`, `ForceCommand` y `HostbasedUsesNameFromPacketOnly` se admiten dentro de bloques `Match`. De manera predeterminada, el valor de `AuthorizedKeysFile` es `$HOME/.ssh/authorized_keys` y de `HostbasedUsesNameFromPacketOnly` es no. Para utilizar bloques `Match`, consulte “Cómo crear excepciones de host y usuario para valores predeterminados de Secure Shell” en la página 302.

Si bien los ingenieros de Oracle Solaris proporcionan correcciones de errores para el proyecto, también han integrado las siguientes funciones de Oracle Solaris en la bifurcación de Secure Shell:

- PAM: Secure Shell utiliza PAM. La opción de configuración `UsePAM` de OpenSSH no se admite.
- Separación de privilegios: Secure Shell no utiliza el código de separación de privilegios del proyecto OpenSSH. Secure Shell separa el procesamiento de auditoría, conservación de registros y restablecimiento de claves del procesamiento de protocolos de sesión.  
El código de separación de privilegios de Secure Shell siempre está activado y no se puede desactivar. La opción `UsePrivilegeSeparation` de OpenSSH no se admite.
- Configuración regional: Secure Shell admite completamente la negociación de idiomas, como se define en RFC 4253, *Secure Shell Transfer Protocol* (Protocolo de transferencia de shell seguro). Después de que el usuario inicia sesión, el perfil del shell de inicio de sesión del usuario puede sustituir la configuración regional negociada de Secure Shell.

- Auditoría: Secure Shell está totalmente integrado en el servicio de auditoría de Solaris. Para obtener más información sobre el servicio de auditoría, consulte la [Parte VII](#).
- Compatibilidad con GSS-API: la GSS-API se puede utilizar para la autenticación de usuario y para el intercambio de claves inicial. La GSS-API se define en RFC4462, *Generic Security Service Application Program Interface* (Interfaz de programa de aplicación de servicios de seguridad genéricos).
- Comandos de proxy: Secure Shell proporciona comandos de proxy para protocolos SOCKS5 y HTTP. Para ver un ejemplo, consulte [“Cómo configurar conexiones Secure Shell predeterminadas a hosts fuera de un cortafuegos” en la página 314](#).

En las versiones de Oracle Solaris, Secure Shell resincroniza el indicador de compatibilidad `SSH_OLD_FORWARD_ADDR` del proyecto OpenSSH. A partir de marzo de 2011, la versión de SSH; es 1.5.

## Secure Shell y FIPS-140

Oracle Solaris proporciona una opción de FIPS-140 para el servidor y el cliente. El modo FIPS, donde Secure Shell utiliza el modo FIPS-140 de OpenSSL, no es el predeterminado. Puede invocar el modo FIPS en la línea de comandos, como en `ssh -o "UseFIPS140 yes" remote-host`. Como alternativa, se puede definir una palabra clave en los archivos de configuración.

Brevemente, la implementación consta de los siguientes elementos:

- Los siguientes cifrados aprobados por FIPS están disponibles en el servidor y en el cliente: `aes128-cbc`, `aes192-cbc` y `aes256-cbc`.  
`3des-cbc` está disponible de manera predeterminada en el cliente, pero no está en la lista de cifrado del servidor debido a posibles riesgos de seguridad.
- Están disponibles los siguientes códigos de autenticación de mensajes (MAC) aprobados por FIPS:
  - `hmac-sha1`, `hmac-sha1-96`
  - `hmac-sha2-256`, `hmac-sha2-256-96`
  - `hmac-sha2-512`, `hmac-sha2-512-96`
- Se admiten cuatro configuraciones de servidor-cliente:
  - Ningún modo FIPS en cliente o servidor
  - Modo FIPS en el cliente y en el servidor
  - Modo FIPS en el servidor, pero no en el cliente
  - Ningún modo FIPS en el servidor, pero sí en el cliente
- El comando `ssh-keygen` tiene una opción para generar la clave privada del usuario en el formato PKCS n° 8 que requieren los clientes Secure Shell en modo FIPS. Para obtener más información, consulte la página del comando `man ssh-keygen(1)`.

Para obtener más información sobre las operaciones de FIPS en Secure Shell, consulte las páginas del comando `man sshd(1M)`, `sshd_config(4)`, `ssh(1)` y `ssh_config(4)`.

Cuando utiliza una tarjeta Sun Crypto Accelerator 6000 para operaciones Secure Shell, Secure Shell se ejecuta con compatibilidad de FIPS-140 en el nivel 3. El hardware de nivel 3 está certificado para evitar la alteración física, utilizar autenticación basada en identidad y aislar las interfaces que gestionan parámetros de seguridad críticos de otras interfaces de hardware.

## Configuración de Secure Shell (tareas)

Secure Shell se configura durante la instalación. Para cambiar los valores predeterminados, se requiere la intervención del administrador. Las siguientes tareas muestran cómo cambiar algunos de los valores predeterminados.

### Configuración de Secure Shell (mapa de tareas)

En el siguiente mapa de tareas, se indican procedimientos para configurar Secure Shell.

| Tarea                                                                         | Descripción                                                                                                                                    | Para obtener instrucciones                                                                                                                                                      |
|-------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Configurar autenticación basada en host.                                      | Configura la autenticación basada en host en el cliente y el servidor.                                                                         | <a href="#">“Cómo configurar la autenticación basada en host para Secure Shell” en la página 298</a>                                                                            |
| Aumentar tamaño del búfer para controlar la latencia de conexión.             | Genera el valor de la propiedad TCP <code>recv_buf</code> para ancho de banda alto y redes de latencia alta.                                   | <a href="#">“Cambio del tamaño de la memoria intermedia de recepción de TCP” de <i>Conexión de sistemas mediante la configuración de redes fijas en Oracle Solaris 11.1</i></a> |
| Configurar reenvío del puerto.                                                | Permite a los usuarios utilizar el reenvío del puerto.                                                                                         | <a href="#">“Cómo configurar el reenvío del puerto en Secure Shell” en la página 301</a>                                                                                        |
| Configurar excepciones para valores predeterminados del sistema Secure Shell. | Para usuarios, hosts, grupos y direcciones, especifica una configuración de Secure Shell diferente de los valores predeterminados del sistema. | <a href="#">“Cómo crear excepciones de host y usuario para valores predeterminados de Secure Shell” en la página 302</a>                                                        |
| Aislar un entorno root para transferencias sftp.                              | Proporciona un directorio protegido para las transferencias de archivos.                                                                       | <a href="#">“Cómo crear un directorio aislado para archivos sftp” en la página 303</a>                                                                                          |

### ▼ Cómo configurar la autenticación basada en host para Secure Shell

El siguiente procedimiento configura un sistema de clave pública en el que la clave pública del cliente se utiliza para la autenticación en el servidor. El usuario también debe crear un par de clave pública y clave privada.

En el procedimiento, los términos *cliente* y *host local* hacen referencia al equipo en el que un usuario introduce el comando `ssh`. Los términos *servidor* y *host remoto* hacen referencia al equipo al que el cliente está intentando acceder.

**Antes de empezar** Debe asumir el rol `root`. Para obtener más información, consulte [“Cómo usar los derechos administrativos que tiene asignados” en la página 164](#).

**1 En el cliente, active la autenticación basada en host.**

En el archivo de configuración del cliente, `/etc/ssh/ssh_config`, escriba la siguiente entrada:

```
HostbasedAuthentication yes
```

Para ver la sintaxis del archivo, consulte la página del comando `man ssh_config(4)`.

**2 En el servidor, active la autenticación basada en host.**

En el archivo de configuración del servidor, `/etc/ssh/sshd_config`, escriba la misma entrada:

```
HostbasedAuthentication yes
```

Para ver la sintaxis del archivo, consulte la página del comando `man sshd_config(4)`.

**3 En el servidor, configure un archivo que permita que el cliente se reconozca como un host de confianza.**

Para obtener más información, consulte la sección `FILES` de la página del comando `man sshd(1M)`.

- **Agregue el cliente como una entrada al archivo `/etc/ssh/hosts.equiv` del servidor.**

```
client-host
```

- **También puede indicar a los usuarios que agreguen una entrada para el cliente a sus archivos `~/.hosts` en el servidor.**

```
client-host
```

**4 En el servidor, asegúrese de que el daemon `sshd` pueda acceder a la lista de hosts de confianza.**

Establezca `IgnoreRhosts` en `no` en el archivo `/etc/ssh/sshd_config`.

```
sshd_config
IgnoreRhosts no
```

**5 Asegúrese de que los usuarios de Secure Shell en su sitio tengan cuentas en ambos hosts.**

**6 Realice una de las siguientes acciones para colocar la clave pública del cliente en el servidor.**

- **Modifique el archivo `sshd_config` en el servidor y luego indique a sus usuarios que agreguen las claves de host públicas del cliente a sus archivos `~/.ssh/known_hosts`.**

```
sshd_config
IgnoreUserKnownHosts no
```

Para obtener instrucciones para el usuario, consulte [“Cómo generar un par de clave pública y clave privada para utilizar con Secure Shell” en la página 305.](#)

- **Copie la clave pública del cliente en el servidor.**

Las claves de host se almacenan en el directorio `/etc/ssh`. Las claves suelen ser generadas por el daemon `sshd` al iniciar por primera vez.

- a. **Agregue la clave al archivo `/etc/ssh/ssh_known_hosts` en el servidor.**

En el cliente, escriba el comando en una línea sin barra diagonal inversa.

```
cat /etc/ssh/ssh_host_dsa_key.pub | ssh RemoteHost \
'cat >> /etc/ssh/ssh_known_hosts && echo "Host key copied"'
```

- b. **Cuando se le pida, proporcione la contraseña de inicio de sesión.**

Cuando el archivo se copia, se muestra el mensaje “Host key copied” (clave de host copiada).

Cada línea en el archivo `/etc/ssh/ssh_known_hosts` consta de campos que están separados por espacios:

```
hostnames algorithm-name publickey comment
```

- c. **Edite el archivo `/etc/ssh/ssh_known_hosts` y agregue `RemoteHost` como el primer campo en la entrada copiada.**

```
/etc/ssh/ssh_known_hosts File
RemoteHost <copied entry>
```

## Ejemplo 15–1 Configuración de autenticación basada en host

En el siguiente ejemplo, cada host está configurado como servidor y como cliente. Un usuario en cualquiera de los hosts puede iniciar una conexión `ssh` al otro host. La siguiente configuración hace que cada host sea un servidor y un cliente:

- En cada host, los archivos de configuración de Secure Shell contienen las siguientes entradas:

```
/etc/ssh/ssh_config
HostBasedAuthentication yes
#
/etc/ssh/sshd_config
HostBasedAuthentication yes
IgnoreRhosts no
```

- En cada host, el archivo `shosts.equiv` contiene una entrada para el otro host:

```
/etc/ssh/shosts.equiv on machine2
machine1

/etc/ssh/shosts.equiv on machine1
machine2
```

- La clave pública de cada host está en el archivo `/etc/ssh/ssh_known_hosts` del otro host:



```
/etc/ssh/ssh_known_hosts on machine2
... machine1

/etc/ssh/ssh_known_hosts on machine1
... machine2
```

- Los usuarios tienen una cuenta en ambos hosts:

```
/etc/passwd on machine1
jdoe:x:3111:10:J Doe:/home/jdoe:/bin/sh

/etc/passwd on machine2
jdoe:x:3111:10:J Doe:/home/jdoe:/bin/sh
```

## ▼ Cómo configurar el reenvío del puerto en Secure Shell

El reenvío del puerto permite que un puerto local sea reenviado a un host remoto. Efectivamente, un socket se asigna para escuchar el puerto en el lado local. De forma similar, un puerto se puede especificar en el lado remoto.

---

**Nota** – El reenvío del puerto de Secure Shell debe utilizar conexiones TCP. Secure Shell no admite conexiones UDP para el reenvío del puerto.

---

### Antes de empezar

Debe asumir el rol root. Para obtener más información, consulte [“Cómo usar los derechos administrativos que tiene asignados” en la página 164](#).

#### 1 Configure un valor de Secure Shell en el servidor remoto para permitir el reenvío del puerto.

Cambie el valor de `AllowTcpForwarding` a `yes` en el archivo `/etc/ssh/sshd_config`.

```
Port forwarding
AllowTcpForwarding yes
```

#### 2 Reinicie el servicio Secure Shell.

```
remoteHost# svcadm restart network/ssh:default
```

Para obtener información sobre la gestión de servicios persistentes, consulte el [Capítulo 1, “Gestión de servicios \(descripción general\)” de \*Gestión de servicios y errores en Oracle Solaris 11.1\*](#) y la página del comando `man svcadm(1M)`.

#### 3 Verifique que el reenvío del puerto se pueda utilizar.

```
remoteHost# /usr/bin/pgrep -lf sshd
1296 ssh -L 2001:remoteHost:23 remoteHost
```

## ▼ Cómo crear excepciones de host y usuario para valores predeterminados de Secure Shell

Este procedimiento agrega un bloque Match condicional después de la sección global del archivo `/etc/ssh/sshd_config`. Los pares de valores de palabras clave a continuación del bloque Match especifican excepciones para el usuario, grupo, host o dirección que se especifica como coincidencia.

### Antes de empezar

Debe convertirse en un administrador con la autorización `solaris.admin.edit/etc/ssh/sshd_config` asignada. De manera predeterminada, el rol `root` tiene esta autorización. Para obtener más información, consulte [“Cómo usar los derechos administrativos que tiene asignados” en la página 164](#).

- 1 **Edite el archivo `/etc/ssh/sshd_config`.**
- 2 **Configure un usuario, grupo, host o dirección para que utilice una configuración de Secure Shell diferente de la configuración predeterminada.**

Coloque los bloques Match después de la configuración global.

---

**Nota** – La sección global del archivo puede o no mostrar la configuración predeterminada. Para conocer los valores predeterminados, consulte la página del comando `man sshd_config(4)`.

---

Es posible que tenga usuarios que no deberían poder utilizar el reenvío TCP. En el siguiente ejemplo, cualquier usuario en el grupo `public` y cualquier nombre de usuario que comienza con `test` no puede utilizar el reenvío TCP:

```
sshd_config file
Global settings

Example (reflects default settings):
#
Host *
ForwardAgent no
ForwardX11 no
PubkeyAuthentication yes
PasswordAuthentication yes
FallBackToRsh no
UseRsh no
BatchMode no
CheckHostIP yes
StrictHostKeyChecking ask
EscapeChar ~
Match Group public
 AllowTcpForwarding no
Match User test*
 AllowTcpForwarding no
```

Para obtener más información sobre la sintaxis del bloque Match, consulte la página del comando `man sshd_config(4)`.

## ▼ Cómo crear un directorio aislado para archivos sftp

Este procedimiento configura un directorio `sftponly` creado específicamente para transferencias `sftp`. Los usuarios no pueden ver los archivos o directorios fuera del directorio de transferencia.

**Antes de empezar** Debe asumir el rol `root`. Para obtener más información, consulte [“Cómo usar los derechos administrativos que tiene asignados” en la página 164](#).

### 1 En el servidor Secure Shell cree el directorio aislado como un entorno `chroot`.

```
groupadd sftp
useradd -m -G sftp -s /bin/false sftponly
chown root:root /export/home/sftponly
mkdir /export/home/sftponly/www
chown sftponly:staff /export/home/sftponly/www
```

En esta configuración, `/export/home/sftponly` es el directorio `chroot` al que sólo tiene acceso la cuenta `root`. El usuario tiene permiso de escritura en el subdirectorio `sftponly/www`.

### 2 Todavía en el servidor, configure un bloque de coincidencia para el grupo `sftp`.

En el archivo `/etc/ssh/sshd_config`, busque la entrada `sftp subsystem` y modifique el archivo de la siguiente forma:

```
pfedit /etc/ssh/sshd_config
...
sftp subsystem
#Subsystem sftp /usr/lib/ssh/sftp-server
Subsystem sftp internal-sftp
...
Match Group for Subsystem
At end of file, to follow all global options
Match Group sftp
 ChrootDirectory %h
 ForceCommand internal-sftp
 AllowTcpForwarding no
```

Puede usar las siguientes variables para especificar la ruta `chroot`:

- `%h`: especifica el directorio raíz.
- `%u`: especifica el nombre de usuario del usuario autenticado.
- `%:`: omite el signo `%`.

### 3 En el cliente, compruebe que la configuración funcione correctamente.

Los archivos en el entorno `chroot` pueden ser diferentes.

```
root@client:~# ssh sftponly@server
This service allows sftp connections only.
```

```
Connection to server closed. No shell access, sftp is enforced.
root@client:~# sftp sftponly@server
sftp> pwd sftp access granted
Remote working directory: / chroot directory looks like root directory
sftp> ls
WWW local.cshrc local.login local.profile
sftp> get local.cshrc
Fetching /local.cshrc to local.cshrc
/local.cshrc 100% 166 0.2KB/s 00:00 user can read contents
sftp> put /etc/motd
Uploading /etc/motd to /motd
Couldn't get handle: Permission denied user cannot write to / directory
sftp> cd WWW
sftp> put /etc/motd
Uploading /etc/motd to /WWW/motd
/etc/motd 100% 118 0.1KB/s 00:00 user can write to WWW directory
sftp> ls -l
-rw-r--r-- 1 101 10 118 Jul 20 09:07 motd successful transfer
sftp>
```

## Uso de Secure Shell (tareas)

Secure Shell proporciona acceso seguro entre un shell local y un shell remoto. Para obtener más información, consulte las páginas del comando man [ssh\\_config\(4\)](#) y [ssh\(1\)](#).

## Uso de Secure Shell (mapa de tareas)

En el siguiente mapa de tareas, se indican procedimientos de usuario para usar Secure Shell.

| Tarea                                                                 | Descripción                                                                                   | Para obtener instrucciones                                                                                             |
|-----------------------------------------------------------------------|-----------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------|
| Crear un par de clave pública y clave privada.                        | Permite el acceso a Secure Shell para sitios que requieren la autenticación de clave pública. | <a href="#">“Cómo generar un par de clave pública y clave privada para utilizar con Secure Shell” en la página 305</a> |
| Cambiar la frase de contraseña.                                       | Cambia la frase que autentica la clave privada.                                               | <a href="#">“Cómo cambiar la frase de contraseña de una clave privada de Secure Shell” en la página 307</a>            |
| Iniciar sesión con Secure Shell.                                      | Proporciona comunicación de Secure Shell cifrada cuando se inicia sesión de manera remota.    | <a href="#">“Cómo iniciar sesión en un host remoto con Secure Shell” en la página 307</a>                              |
| Iniciar sesión en Secure Shell sin que se le solicite una contraseña. | Permite iniciar sesión mediante un agente que proporciona la contraseña a Secure Shell.       | <a href="#">“Cómo reducir indicadores de contraseñas en Secure Shell” en la página 309</a>                             |

| Tarea                                                                                           | Descripción                                                                                                                        | Para obtener instrucciones                                                                                                 |
|-------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------|
| Conectarse a Secure Shell como root.                                                            | Permite iniciar sesión como root para los comandos send y receive de ZFS.                                                          | <a href="#">“Cómo administrar ZFS con Secure Shell de forma remota” en la página 310</a>                                   |
| Utilizar el reenvío del puerto en Secure Shell.                                                 | Especifica un puerto local o un puerto remoto que se utilizará en una conexión de Secure Shell por TCP.                            | <a href="#">“Cómo utilizar el reenvío del puerto en Secure Shell” en la página 312</a>                                     |
| Copiar archivos con Secure Shell.                                                               | Copia archivos entre hosts de manera segura.                                                                                       | <a href="#">“Cómo copiar archivos con Secure Shell” en la página 313</a>                                                   |
| Conectarse de forma segura de un host dentro de un cortafuegos a un host fuera del cortafuegos. | Utiliza comandos de Secure Shell que son compatibles con HTTP o SOCKS5 para conectar hosts que están separados por un cortafuegos. | <a href="#">“Cómo configurar conexiones Secure Shell predeterminadas a hosts fuera de un cortafuegos” en la página 314</a> |

## ▼ Cómo generar un par de clave pública y clave privada para utilizar con Secure Shell

Los usuarios deben generar un par de clave pública y clave privada cuando su sitio implementa la autenticación basada en host o la autenticación de clave pública de usuario. Para obtener opciones adicionales, consulte la página del comando man [ssh-keygen\(1\)](#).

### Antes de empezar

Consulte al administrador del sistema si se ha configurado la autenticación basada en host.

#### 1 Inicie el programa de generación de claves.

```
myLocalHost% ssh-keygen -t rsa
Generating public/private rsa key pair.
...
```

Donde -t es el tipo de algoritmo, uno de rsa, dsa o rsa1.

#### 2 Especifique la ruta al archivo que contendrá la clave.

De manera predeterminada, el nombre de archivo id\_rsa, que representa una clave v2 RSA, aparece entre paréntesis. Puede seleccionar este archivo presionando la tecla de retorno. O puede escribir un nombre de archivo alternativo.

Enter file in which to save the key (/home/jdoe/.ssh/id\_rsa): *<Press Return>*

El nombre de archivo de la clave pública se crea automáticamente adjuntando la cadena .pub al nombre del archivo de clave privada.

#### 3 Escriba una frase de contraseña para usar la clave.

Esta frase de contraseña se utiliza para cifrar la clave privada. Se *desaconseja* el uso de una entrada nula. Tenga en cuenta que la frase de contraseña no se muestra cuando la escribe.

Enter passphrase (empty for no passphrase): *<Type passphrase>*

**4 Vuelva a escribir la frase de contraseña para confirmarla.**

```
Enter same passphrase again: <Type passphrase>
Your identification has been saved in /home/jdoe/.ssh/id_rsa.
Your public key has been saved in /home/jdoe/.ssh/id_rsa.pub.
The key fingerprint is:
0e:fb:3d:57:71:73:bf:58:b8:eb:f3:a3:aa:df:e0:d1 jdoe@myLocalHost
```

**5 Compruebe los resultados.**

Compruebe que la ruta al archivo de claves sea correcta.

```
% ls ~/.ssh
id_rsa
id_rsa.pub
```

En este punto, ha creado un par de clave pública y clave privada.

**6 Elija la opción adecuada:**

- Si el administrador ha configurado la autenticación basada en host, es posible que necesite copiar la clave pública del host local en el host remoto.

Ahora puede iniciar sesión en el host remoto. Para obtener detalles, consulte [“Cómo iniciar sesión en un host remoto con Secure Shell” en la página 307.](#)

**a. Escriba el comando en una línea sin barra diagonal inversa.**

```
% cat /etc/ssh/ssh_host_dsa_key.pub | ssh RemoteHost \
'cat >> ~/.ssh/known_hosts && echo "Host key copied"'
```

**b. Cuando se le pida, proporcione la contraseña de inicio de sesión.**

```
Enter password: <Type password>
Host key copied
%
```

- Si su sitio utiliza la autenticación de usuario con claves públicas, rellene el archivo `authorized_keys` en el host remoto.

**a. Copie la clave pública en el host remoto.**

Escriba el comando en una línea sin barra diagonal inversa.

```
myLocalHost% cat $HOME/.ssh/id_rsa.pub | ssh myRemoteHost \
'cat >> .ssh/authorized_keys && echo "Key copied"'
```

**b. Cuando se le pida, proporcione la contraseña de inicio de sesión.**

Cuando el archivo se copia, se muestra el mensaje “Key copied” (clave copiada).

```
Enter password: Type login password
Key copied
myLocalHost%
```

## 7 (Opcional) Reduzca la solicitud de frases de contraseña.

Para obtener un procedimiento, consulte “[Cómo reducir indicadores de contraseñas en Secure Shell](#)” en la página 309. Para obtener más información, consulte las páginas del comando `man ssh-agent(1)` y `ssh-add(1)`.

## ▼ Cómo cambiar la frase de contraseña de una clave privada de Secure Shell

El siguiente procedimiento no cambia la clave privada. El procedimiento cambia el mecanismo de autenticación para la clave privada, la frase de contraseña. Para obtener más información, consulte la página del comando `man ssh-keygen(1)`.

### ● Cambie la frase de contraseña.

Escriba el comando `ssh-keygen` con la opción `-p` y responda a las solicitudes.

```
myLocalHost% ssh-keygen -p
Enter file which contains the private key (/home/jdoe/.ssh/id_rsa): <Press Return>
Enter passphrase (empty for no passphrase): <Type passphrase>
Enter same passphrase again: <Type passphrase>
```

Donde `-p` solicita cambiar la frase de contraseña de un archivo de clave privada.

## ▼ Cómo iniciar sesión en un host remoto con Secure Shell

### 1 Inicie una sesión de Secure Shell.

Escriba el comando `ssh` y especifique el nombre del host remoto y de inicio de sesión.

```
myLocalHost% ssh myRemoteHost -l username
```

Una solicitud cuestiona la autenticidad del host remoto:

```
The authenticity of host 'myRemoteHost' can't be established.
RSA key fingerprint in md5 is: 04:9f:bd:fc:3d:3e:d2:e7:49:fd:6e:18:4f:9c:26
Are you sure you want to continue connecting(yes/no)?
```

Esta solicitud es normal para conexiones iniciales a hosts remotos.

### 2 Si se le solicita, verifique la autenticidad de la clave del host remoto.

- Si no puede confirmar la autenticidad del host remoto, escriba `no` y póngase en contacto con el administrador del sistema.

```
Are you sure you want to continue connecting(yes/no)? no
```

El administrador es responsable de actualizar el archivo `/etc/ssh/ssh_known_hosts` global. Un archivo `ssh_known_hosts` actualizado impide que esta solicitud aparezca.

- **Si confirma la autenticidad del host remoto, responda la solicitud y continúe con el siguiente paso.**

Are you sure you want to continue connecting(yes/no)? **yes**

### 3 Auténtíquese en Secure Shell.

- a. **Cuando se le solicite, escriba la frase de contraseña.**

Enter passphrase for key '/home/jdoe/.ssh/id\_rsa': *<Type passphrase>*

- b. **Cuando se le solicite, escriba la contraseña de su cuenta.**

```
jdoe@myRemoteHost's password: <Type password>
Last login: Wed Sep 7 09:07:49 2011 from myLocalHost
Oracle Corporation SunOS 5.11 September 2011
myRemoteHost%
```

### 4 Realice transacciones en el host remoto.

Los comandos que envía están cifrados. Ninguna respuesta que recibe está cifrada.

### 5 Cierre la conexión de Secure Shell.

Cuando haya terminado, escriba salir (**exit**) o utilice el método habitual para salir de su shell.

```
myRemoteHost% exit
myRemoteHost% logout
Connection to myRemoteHost closed
myLocalHost%
```

## Ejemplo 15-2 Visualización de interfaz gráfica de usuario remoto en Secure Shell

En este ejemplo, `jdoe` es el usuario inicial en ambos sistemas, por lo que se le asigna el perfil de derechos de instalación de software. `jdoe` desea usar la interfaz gráfica de usuario de Package Manager en el sistema remoto. El valor predeterminado de la palabra clave `X11Forwarding` sigue siendo `yes`, y el paquete `xauth` se instala en el sistema remoto.

```
% ssh -l jdoe -X myRemoteHost
jdoe@myRemoteHost's password: <Type password>
Last login: Wed Sep 7 09:07:49 2011 from myLocalHost
Oracle Corporation SunOS 5.11 September 2011
myRemoteHost% packagemanager &
```



## ▼ Cómo reducir indicadores de contraseñas en Secure Shell

Si no desea escribir la frase de contraseña ni la contraseña para utilizar Secure Shell, puede utilizar el daemon del agente. Inicie el daemon al comienzo de la sesión. A continuación, almacene las claves privadas con el daemon del agente mediante el comando `ssh-add`. Si tiene cuentas diferentes en hosts diferentes, agregue las claves que necesita para la sesión.

Puede iniciar el daemon del agente manualmente cuando sea necesario, como se describe en el siguiente procedimiento.

### 1 Inicie el daemon del agente.

```
myLocalHost% eval 'ssh-agent'
Agent pid 9892
```

### 2 Verifique que el daemon del agente se haya iniciado.

```
myLocalHost% pgrep ssh-agent
9892
```

### 3 Agregue la clave privada al daemon del agente.

Escriba el comando `ssh-add`.

```
myLocalHost% ssh-add
Enter passphrase for /home/jdoe/.ssh/id_rsa: <Type passphrase>
Identity added: /home/jdoe/.ssh/id_rsa(/home/jdoe/.ssh/id_rsa)
myLocalHost%
```

### 4 Inicie una sesión de Secure Shell.

```
myLocalHost% ssh myRemoteHost -l jdoe
```

No se le solicita una frase de contraseña.

## Ejemplo 15-3 Uso de opciones de `ssh-add`

En este ejemplo, `jdoe` agrega dos claves al daemon del agente. La opción `-l` se utiliza para enumerar todas las claves que se almacenan en el daemon. Al final de la sesión, la opción `-D` se usa para eliminar todas las claves del daemon del agente.

```
myLocalHost% ssh-agent
myLocalHost% ssh-add
Enter passphrase for /home/jdoe/.ssh/id_rsa: <Type passphrase>
Identity added: /home/jdoe/.ssh/id_rsa(/home/jdoe/.ssh/id_rsa)
myLocalHost% ssh-add /home/jdoe/.ssh/id_dsa
Enter passphrase for /home/jdoe/.ssh/id_dsa: <Type passphrase>
Identity added:
/home/jdoe/.ssh/id_dsa(/home/jdoe/.ssh/id_dsa)
```

```
myLocalHost% ssh-add -l
md5 1024 0e:fb:3d:53:71:77:bf:57:b8:eb:f7:a7:aa:df:e0:d1
/home/jdoe/.ssh/id_rsa(RSA)
md5 1024 c1:d3:21:5e:40:60:c5:73:d8:87:09:3a:fa:5f:32:53
/home/jdoe/.ssh/id_dsa(DSA)
```

*User conducts Oracle Solaris Secure Shell transactions*

```
myLocalHost% ssh-add -D
Identity removed:
/home/jdoe/.ssh/id_rsa(/home/jdoe/.ssh/id_rsa.pub)
/home/jdoe/.ssh/id_dsa(DSA)
```

## ▼ Cómo administrar ZFS con Secure Shell de forma remota

De manera predeterminada, el rol root no puede iniciar sesión de forma remota con Secure Shell. Históricamente, la raíz ha utilizado Secure Shell para las tareas importantes, como el envío de datos agrupados de ZFS para su almacenamiento en un sistema remoto. En este procedimiento, el rol root crea un usuario que puede actuar como administrador remoto de ZFS.

**Antes de empezar** Debe asumir el rol root. Para obtener más información, consulte [“Cómo usar los derechos administrativos que tiene asignados” en la página 164.](#)

### 1 Cree el usuario en ambos sistemas.

Por ejemplo, cree el usuario zfsroot y proporcione una contraseña.

```
source # useradd -c "Remote ZFS Administrator" -u 1201 -d /home/zfsroot zfsroot
source # passwd zfsroot
Enter password:
Retype password:
#
```

```
dest # useradd -c "Remote ZFS Administrator" -u 1201 -d /home/zfsroot zfsroot
dest # passwd zfsroot
...
```

El usuario zfsroot debe estar definido de idéntica manera en ambos sistemas.

### 2 Cree el par de claves del usuario para la autenticación de Secure Shell.

El par de claves se crea en el sistema de origen. A continuación, la clave pública se copia al usuario zfsroot en el sistema de destino.

#### a. Genere el par de claves y colóquelo en el archivo id\_migrate.

```
ssh-keygen -t rsa -P "" -f ~/id_migrate
Generating public/private rsa key pair.
```

```
Your identification has been saved in /root/id_migrate.
Your public key has been saved in /root/id_migrate.pub.
The key fingerprint is:
3c:7f:40:ef:ec:63:95:b9:23:a2:72:d5:ea:d1:61:f0 root@source
```

**b. Envíe la parte pública del par de claves al sistema de destino.**

```
scp ~/id_migrate.pub zfsroot@dest:
The authenticity of host 'dest (10.134.76.126)' can't be established.
RSA key fingerprint is 44:37:ab:4e:b7:2f:2f:b8:5f:98:9d:e9:ed:6d:46:80.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'dest,10.134.76.126' (RSA) to the list of known hosts.
Password:
id_migrate.pub 100% |*****| 399 00:00
```

**3 En ambos sistemas, asigne el perfil de derechos de administración de archivos ZFS a zfsroot.**

```
source # usermod -P +'ZFS File System Management' -S files zfsroot
dest # usermod -P +'ZFS File System Management' -S files zfsroot
```

**4 Verifique que el sistema de destino tiene asignado el perfil de derechos.**

```
dest # profiles zfsroot
zfsroot:
ZFS File System Management
Basic Solaris User
All
```

**5 En el sistema de destino, mueva la parte pública del par de claves al directorio privado /home/zfsroot/.ssh.**

```
root@dest # su - zfsroot
Oracle Corporation SunOS 5.11 11.1 May 2012
zfsroot@dest $ mkdir -m 700 .ssh
zfsroot@dest $ cat id_migrate.pub >> .ssh/authorized_keys
```

**6 Verifique que la configuración funciona.**

```
root@source# ssh -l zfsroot -i ~/id_migrate dest \
pfexec /usr/sbin/zfs snapshot zones@test
root@source# ssh -l zfsroot -i ~/id_migrate dest \
pfexec /usr/sbin/zfs destroy zones@test
```

**7 (Opcional) Verifique que puede crear una instantánea y replicar los datos.**

```
root@source# zfs snapshot -r rpool/zones@migrate-all
root@source# zfs send -rc rpool/zones@migrate-all | \
ssh -l zfsroot -i ~/id_migrate dest pfexec /usr/sbin/zfs recv -F zones
```

**8 (Opcional) Elimine la capacidad de usar la cuenta zfsroot para la administración de ZFS.**

```
root@dest# usermod -P -'ZFS File System Management' zfsroot
root@dest# su - zfsroot
zfsroot@dest# cp .ssh/authorized_keys .ssh/authorized_keys.bak
zfsroot@dest# grep -v root@source .ssh/authorized_keys.bak > .ssh/authorized_keys
```

## ▼ Cómo utilizar el reenvío del puerto en Secure Shell

Puede especificar que un puerto local se reenvíe a un host remoto. Efectivamente, un socket se asigna para escuchar el puerto en el lado local. La conexión desde este puerto se realiza mediante un canal seguro al host remoto. Por ejemplo, puede especificar el puerto 143 para obtener correo electrónico remotamente con IMAP4. De forma similar, un puerto se puede especificar en el lado remoto.

### Antes de empezar

Para utilizar el reenvío del puerto, el administrador debe tener activado el reenvío del puerto en el servidor remoto de Secure Shell. Para obtener detalles, consulte [“Cómo configurar el reenvío del puerto en Secure Shell” en la página 301](#).

### ● Para usar el reenvío del puerto seguro, elija una de las siguientes opciones:

- **Para establecer que un puerto local reciba una comunicación segura de un puerto remoto, especifique ambos puertos.**

Especifique el puerto local que escucha para la comunicación remota. Además, especifique el host remoto y el puerto remoto que reenvían la comunicación.

```
myLocalHost% ssh -L localPort:remoteHost:remotePort
```

- **Para establecer que un puerto remoto reciba una conexión segura de un puerto local, especifique ambos puertos.**

Especifique el puerto remoto que escucha para la comunicación remota. Además, especifique el host local y el puerto local que reenvían la comunicación.

```
myLocalHost% ssh -R remotePort:localhost:localPort
```

### Ejemplo 15-4 Uso del reenvío del puerto local para recibir correo

El ejemplo siguiente muestra cómo puede utilizar el reenvío del puerto local para recibir correo de manera segura desde un servidor remoto.

```
myLocalHost% ssh -L 9143:myRemoteHost:143 myRemoteHost
```

Este comando reenvía conexiones del puerto 9143 en myLocalHost al puerto 143. El puerto 143 es el puerto del servidor v2 IMAP en myRemoteHost. Cuando el usuario inicia una aplicación de correo, el usuario especifica el número de puerto local para el servidor IMAP, como en localhost:9143.

No confunda localhost con myLocalHost. myLocalHost es un nombre de host hipotético. localhost es una palabra clave que identifica el sistema local.

### Ejemplo 15-5 Uso del reenvío del puerto remoto para comunicarse fuera de un cortafuegos

En el siguiente ejemplo, se muestra cómo un usuario en un entorno empresarial puede reenviar conexiones desde un host en una red externa hasta un host dentro de un cortafuegos corporativo.

```
myLocalHost% ssh -R 9022:myLocalHost:22 myOutsideHost
```

Este comando reenvía conexiones desde el puerto 9022 en myOutsideHost hasta el puerto 22, el servidor sshd, en el host local.

```
myOutsideHost% ssh -p 9022 localhost
myLocalHost%
```

## ▼ Cómo copiar archivos con Secure Shell

El siguiente procedimiento muestra cómo usar el comando `scp` para copiar archivos cifrados entre hosts. Puede copiar archivos cifrados ya sea entre un host local y un host remoto, o entre dos hosts remotos. El comando `scp` solicita autenticación. Para obtener más información, consulte la página del comando [man scp\(1\)](#).

También puede utilizar el programa de transferencia de archivos segura `sftp`. Para obtener más información, consulte la página del comando [man sftp\(1\)](#). Si desea ver un ejemplo, consulte el [Ejemplo 15-6](#).

---

**Nota** – El servicio de auditoría puede auditar transacciones `sftp` a través de la clase de auditoría `ft`. Para `scp`, el servicio de auditoría puede auditar acceso y salida para la sesión `ssh`.

---

#### 1 Inicie el programa de copia segura.

Especifique el archivo de origen, el nombre de usuario en el destino remoto y el directorio de destino.

```
myLocalHost% scp myfile.1 jdoe@myRemoteHost:~
```

#### 2 Indique la frase de contraseña cuando se le solicite.

```
Enter passphrase for key '/home/jdoe/.ssh/id_rsa': <Type passphrase>
myfile.1 25% |***** | 640 KB 0:20 ETA
myfile.1
```

Después de escribir la frase de contraseña, se muestra un indicador de progreso. Consulte la segunda línea en el resultado anterior. El indicador de progreso muestra:

- El nombre del archivo
- El porcentaje del archivo que se ha transferido
- Una serie de asteriscos que indican el porcentaje del archivo que se ha transferido

- La cantidad de datos transferidos
- El tiempo calculado de llegada, o ETA, del archivo completo (es decir, la cantidad restante de tiempo)

#### **Ejemplo 15-6** Especificación de un puerto cuando se utiliza el comando `sftp`

En este ejemplo, el usuario desea que el comando `sftp` utilice un puerto concreto. El usuario utiliza la opción `-o` para especificar el puerto.

```
% sftp -o port=2222 guest@RemoteFileServer
```

## ▼ **Cómo configurar conexiones Secure Shell predeterminadas a hosts fuera de un cortafuegos**

Puede utilizar Secure Shell para establecer una conexión desde un host dentro de un cortafuegos hasta un host fuera del cortafuegos. Esta tarea se realiza especificando un comando de proxy para `ssh` en un archivo de configuración o como una opción en la línea de comandos. Para la opción de línea de comandos, consulte el [Ejemplo 15-7](#).

En general, puede personalizar las interacciones de `ssh` mediante un archivo de configuración.

- Puede personalizar su propio archivo personal en `~/.ssh/config`.
- O puede utilizar los valores en el archivo de configuración administrativo, `/etc/ssh/ssh_config`.

Los archivos se pueden personalizar con dos tipos de comandos de proxy. Un comando de proxy es para conexiones HTTP. El otro comando de proxy es para conexiones SOCKS5. Para obtener más información, consulte la página del comando `man ssh_config(4)`.

### **1 Especifique los comandos de proxy y los hosts en un archivo de configuración.**

Utilice la sintaxis siguiente para agregar tantas líneas como sea necesario:

```
[Host outside-host]
ProxyCommand proxy-command [-h proxy-server] \
[-p proxy-port] outside-host | %h outside-port | %p
```

**Host** *outside-host*

Limita la especificación del comando de proxy a instancias cuando un nombre de host remoto se especifica en la línea de comandos. Si utiliza un carácter comodín para *outside-host*, aplica la especificación del comando de proxy a un conjunto de hosts.

**proxy-command**

Especifica el comando de proxy.

El comando puede ser cualquiera de los siguientes:

- `/usr/lib/ssh/ssh-http-proxy-connect` para conexiones HTTP
- `/usr/lib/ssh/ssh-socks5-proxy-connect` para conexiones SOCKS5

`-h proxy-server y -p proxy-port`

Estas opciones especifican un servidor proxy y un puerto proxy, respectivamente. Si están presentes, los proxies sustituyen cualquier variable de entorno que especifica servidores proxy y puertos proxy, como HTTPPROXY, HTTPPROXYPORT, SOCKS5\_PORT, SOCKS5\_SERVER y http\_proxy. La variable http\_proxy especifica una URL. Si las opciones no se usan, las variables de entorno relevantes se deben definir. Para obtener más información, consulte las páginas del comando `man ssh-socks5-proxy-connect(1)` y `ssh-http-proxy-connect(1)`.

*outside-host*

Designa un host específico para conectarse. Utilice el argumento de sustitución %h para especificar el host en la línea de comandos.

*outside-port*

Designa un puerto específico para conectarse. Utilice el argumento de sustitución %p para especificar el puerto en la línea de comandos. Al especificar %h y %p sin utilizar la opción `Host outside-host`, el comando de proxy se aplica al argumento de host cada vez que se invoca el comando `ssh`.

## 2 Ejecute Secure Shell especificando el host externo.

Escriba, por ejemplo:

```
myLocalHost% ssh myOutsideHost
```

Este comando busca una especificación de comando de proxy para myOutsideHost en su archivo de configuración personal. Si la especificación no se ha encontrado, el comando busca en el archivo de configuración de todo el sistema, `/etc/ssh/ssh_config`. El comando de proxy se sustituye por el comando `ssh`.

### Ejemplo 15–7 Conexión a hosts fuera de un cortafuegos desde la línea de comandos de Secure Shell

“Cómo configurar conexiones Secure Shell predeterminadas a hosts fuera de un cortafuegos” en la [página 314](#) explica cómo especificar un comando de proxy en un archivo de configuración. En este ejemplo, un comando de proxy se especifica en la línea de comandos `ssh`.

```
% ssh -o'Proxycommand=/usr/lib/ssh/ssh-http-proxy-connect \
-h myProxyServer -p 8080 myOutsideHost 22' myOutsideHost
```

La opción `-o` para el comando `ssh` proporciona un método de línea de comandos para especificar un comando de proxy. En este ejemplo, el comando realiza lo siguiente:

- Sustituye el comando de proxy HTTP para `ssh`
- Utiliza el puerto 8080 y myProxyServer como el servidor proxy
- Se conecta al puerto 22 en myOutsideHost





## Secure Shell (referencia)

---

En este capítulo, se describen las opciones de configuración de la función Secure Shell de Oracle Solaris y se tratan los siguientes temas:

- “Una sesión de Secure Shell típica” en la página 317
- “Configuración de cliente y servidor en Secure Shell” en la página 320
- “Palabras clave en Secure Shell” en la página 320
- “Mantenimiento de hosts conocidos en Secure Shell” en la página 326
- “Archivos de Secure Shell” en la página 326
- “Comandos de Secure Shell” en la página 329

Si desea obtener procedimientos para configurar Secure Shell, consulte el [Capítulo 15, “Uso de Secure Shell”](#).

### Una sesión de Secure Shell típica

El daemon de Secure Shell (`sshd`) se inicia, normalmente, durante el inicio cuando los servicios de red se inician. El daemon escucha conexiones de clientes. Una sesión de Secure Shell empieza cuando el usuario ejecuta un comando `ssh`, `scp` o `sftp`. Un daemon `sshd` nuevo se bifurca para cada conexión entrante. Los daemons bifurcados manejan intercambio de claves, cifrado, autenticación, ejecución de comandos e intercambio de datos con el cliente. Estas características de la sesión son determinadas por archivos de configuración del lado del cliente y archivos de configuración del lado del servidor. Los argumentos de la línea de comandos pueden sustituir los valores de los archivos de configuración.

El cliente y el servidor deben autenticarse entre ellos. Tras una autenticación con éxito, el usuario puede ejecutar comandos de manera remota y copiar datos entre hosts.

## Características de la sesión en Secure Shell

El comportamiento del lado del servidor del daemon `sshd` se controla mediante valores de palabra clave en el archivo `/etc/ssh/sshd_config`. Por ejemplo, el archivo `sshd_config` controla los tipos de autenticación que se permiten para acceder al servidor. El comportamiento del lado del servidor también se puede controlar mediante las opciones de línea de comandos cuando el daemon `sshd` se inicia.

El comportamiento en el lado del cliente está controlado por palabras clave de Secure Shell en este orden de prioridad:

- Opciones de línea de comandos
- Archivo de configuración del usuario, `~/.ssh/config`
- Archivo de configuración de todo el sistema, `/etc/ssh/ssh_config`

Por ejemplo, un usuario puede sustituir el valor `Ciphers` de la configuración de todo el sistema, que prefiere `aes128-ctr`, especificando `-c aes256-ctr,aes128-ctr,arcfour` en la línea de comandos. Ahora se prefiere el primer cifrado, `aes256-ctr`.

## Autenticación e intercambio de claves en Secure Shell

El protocolo de Secure Shell admite autenticación de host/usuario de cliente y autenticación de host de servidor. Las claves criptográficas se cambian para la protección de sesiones de Secure Shell. Secure Shell proporciona varios métodos de autenticación e intercambio de claves. Algunos métodos son opcionales. Los mecanismos de autenticación de clientes se muestran en la [Tabla 15–1](#). Los servidores se autentican con claves públicas de host conocidas.

Para la autenticación, Secure Shell admite la autenticación de usuario y la autenticación interactiva genérica, que generalmente involucra contraseñas. Secure Shell también admite la autenticación con claves públicas de usuario y con claves públicas de host de confianza. Las claves pueden ser RSA o [DSA](#). Los intercambios de claves de sesión constan de intercambios de claves efímeras Diffie-Hellman que se firman en el paso de autenticación de servidor. Además, Secure Shell puede usar credenciales GSS para la autenticación.

### Adquisición de credenciales GSS en Secure Shell

A fin de utilizar la GSS-API para la autenticación en Secure Shell, el servidor debe tener credenciales de aceptador GSS-API y el cliente debe tener credenciales de iniciador GSS-API. Se admiten los mecanismos `mech_dh` y `mech_krb5`.

Para `mech_dh`, el servidor tiene credenciales de aceptador GSS-API si `root` ha ejecutado el comando `keylogin`.

Para `mech_krb5`, el servidor tiene credenciales de aceptador GSS-API cuando el principal host que corresponde al servidor tiene una entrada válida en `/etc/krb5/krb5.keytab`.

El cliente tiene credenciales de iniciador para `mech_dh` si se ha realizado una de las siguientes acciones:

- El comando `keylogin` se ha ejecutado.
- El módulo `pam_dhkeys` se utiliza en el archivo `pam.conf`.

El cliente tiene credenciales de iniciador para `mech_krb5` si se ha realizado una de las siguientes acciones:

- El comando `kinit` se ha ejecutado.
- El módulo `pam_krb5` se utiliza en el archivo `pam.conf`.

Para el uso de `mech_dh` en una RPC segura, consulte el [Capítulo 18, “Autenticación de servicios de red \(tareas\)”](#). Para el uso de `mech_krb5`, consulte el [Capítulo 19, “Introducción al servicio Kerberos”](#). Para obtener más información sobre los mecanismos, consulte las páginas del comando `man mech(4)` y `man mech_spnego(5)`.

## Ejecución de comandos y reenvío de datos en Secure Shell

Una vez completada la autenticación, el usuario puede utilizar Secure Shell, generalmente, mediante la solicitud de un shell o la ejecución de un comando. Mediante las opciones del comando `ssh`, el usuario puede realizar solicitudes. Las solicitudes pueden incluir la asignación de un pseudo-tty, el reenvío de conexiones X11 o conexiones TCP/IP, o la activación de un programa de autenticación `ssh-agent` por medio de una conexión segura.

Los componentes básicos de una sesión de usuario son los siguientes:

1. El usuario solicita un shell o la ejecución de un comando, que inicia el modo de sesión.  
En este modo, los datos se envían o se reciben por medio del terminal en el lado del cliente. En el lado del servidor, los datos se envían por medio del shell o de un comando.
2. Cuando la transferencia de datos se completa, el programa de usuario finaliza.
3. Todos los reenvíos de X11 y de TCP/IP se detienen, excepto para las conexiones que ya existen. Las conexiones X11 y TCP/IP existentes permanecen abiertas.
4. El servidor envía un mensaje de estado de salida al cliente. Cuando todas las conexiones están cerradas, como los puertos reenviados que habían permanecido abiertos, el cliente cierra la conexión al servidor. A continuación, el cliente se cierra.

# Configuración de cliente y servidor en Secure Shell

Las características de una sesión de Secure Shell son controladas por los archivos de configuración. Los archivos de configuración se pueden sustituir a un cierto grado por opciones en la línea de comandos.

## Configuración de clientes en Secure Shell

En la mayoría de los casos, las características del lado del cliente de una sesión de Secure Shell son determinadas por el archivo de configuración de todo el sistema, `/etc/ssh/ssh_config`. Los valores del archivo `ssh_config` se pueden sustituir por el archivo de configuración del usuario, `~/.ssh/config`. Además, el usuario puede sustituir ambos archivos de configuración en la línea de comandos.

Los valores en el archivo `/etc/ssh/sshd_config` del servidor determinan qué solicitudes de clientes son permitidas por el servidor. Para obtener una lista de valores de configuración del servidor, consulte [“Palabras clave en Secure Shell” en la página 320](#). Para obtener información detallada, consulte la página del comando `man sshd_config(4)`.

Las palabras clave en el archivo de configuración del cliente se muestran en [“Palabras clave en Secure Shell” en la página 320](#). Si la palabra clave tiene un valor predeterminado, el valor se proporciona. Estas palabras clave se describen detalladamente en las páginas del comando `man ssh(1)`, `scp(1)`, `sftp(1)` y `ssh_config(4)`. Para obtener una lista de palabras clave en orden alfabético y sus valores de sustitución de línea de comando equivalentes, consulte la [Tabla 16–8](#).

## Configuración de servidores en Secure Shell

Las características del lado del servidor de una sesión de Secure Shell son determinadas por el archivo `/etc/ssh/sshd_config`. Las palabras clave en el archivo de configuración del servidor se muestran en [“Palabras clave en Secure Shell” en la página 320](#). Si la palabra clave tiene un valor predeterminado, el valor se proporciona. Para obtener una descripción completa de las palabras clave, consulte la página del comando `man sshd_config(4)`.

## Palabras clave en Secure Shell

En las tablas siguientes, se enumeran las palabras clave y sus valores predeterminados (si hay). Las palabras clave están en orden alfabético. Las palabras clave que se aplican al cliente están en el archivo `ssh_config`. Las palabras clave que se aplican al servidor están en el archivo `sshd_config`. Algunas palabras clave se establecen en ambos archivos. Las palabras clave para un servidor de Secure Shell que ejecuta el protocolo v1 están marcadas.

TABLA 16-1 Palabras clave en archivos de configuración de Secure Shell (de A a Escape)

| Palabra clave       | Valor predeterminado                                    | Ubicación |
|---------------------|---------------------------------------------------------|-----------|
| AllowGroups         | No hay valor predeterminado                             | Servidor  |
| AllowTcpForwarding  | yes                                                     | Servidor  |
| AllowUsers          | No hay valor predeterminado                             | Servidor  |
| AuthorizedKeysFile  | ~/.ssh/authorized_keys                                  | Servidor  |
| Banner              | /etc/issue                                              | Servidor  |
| Batchmode           | no                                                      | Cliente   |
| BindAddress         | No hay valor predeterminado                             | Cliente   |
| CheckHostIP         | yes                                                     | Cliente   |
| ChrootDirectory     | no                                                      | Servidor  |
| Cipher              | blowfish, 3des                                          | Cliente   |
| Ciphers             | aes128-ctr, aes128-cbc, 3des-cbc, blowfish-cbc, arcfour | Ambos     |
| ClearAllForwardings | no                                                      | Cliente   |
| ClientAliveCountMax | 3                                                       | Servidor  |
| ClientAliveInterval | 0                                                       | Servidor  |
| Compression         | no                                                      | Ambos     |
| CompressionLevel    | No hay valor predeterminado                             | Cliente   |
| ConnectionAttempts  | 1                                                       | Cliente   |
| ConnectTimeout      | Tiempo de espera de TCP de sistema                      | Cliente   |
| DenyGroups          | No hay valor predeterminado                             | Servidor  |
| DenyUsers           | No hay valor predeterminado                             | Servidor  |
| DisableBanner       | no                                                      | Cliente   |
| DynamicForward      | No hay valor predeterminado                             | Cliente   |
| EscapeChar          | ~                                                       | Cliente   |

TABLA 16-2 Palabras clave en archivos de configuración de Secure Shell (de Fall a Local)

| Palabra clave | Valor predeterminado | Ubicación |
|---------------|----------------------|-----------|
| FallBackToRsh | no                   | Cliente   |

**TABLA 16-2** Palabras clave en archivos de configuración de Secure Shell (de Fall a Local)  
(Continuación)

| Palabra clave                   | Valor predeterminado                                                                                                     | Ubicación    |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------|--------------|
| ForwardAgent                    | no                                                                                                                       | Cliente      |
| ForwardX11                      | no                                                                                                                       | Cliente      |
| ForwardX11Trusted               | yes                                                                                                                      | Cliente      |
| GatewayPorts                    | no                                                                                                                       | Ambos        |
| GlobalKnownHostsFile            | /etc/ssh/ssh_known_hosts                                                                                                 | Cliente      |
| GSSAPIAuthentication            | yes                                                                                                                      | Ambos        |
| GSSAPIDelegateCredentials       | no                                                                                                                       | Cliente      |
| GSSAPIKeyExchange               | yes                                                                                                                      | Ambos        |
| GSSAPIStoreDelegateCredentials  | yes                                                                                                                      | Servidor     |
| HashKnownHosts                  | no                                                                                                                       | Cliente      |
| Host                            | * Para obtener más información, consulte <a href="#">“Parámetros específicos de host Secure Shell” en la página 325.</a> | Cliente      |
| HostbasedAuthentication         | no                                                                                                                       | Ambos        |
| HostbasedUsesNameFromPacketOnly | no                                                                                                                       | Servidor     |
| HostKey                         | /etc/ssh/ssh_host_key                                                                                                    | Servidor, v1 |
| HostKey                         | /etc/ssh/host_rsa_key,<br>/etc/ssh/host_dsa_key                                                                          | Servidor     |
| HostKeyAlgorithms               | ssh-rsa, ssh-dss                                                                                                         | Cliente      |
| HostKeyAlias                    | No hay valor predeterminado                                                                                              | Cliente      |
| HostName                        | No hay valor predeterminado                                                                                              | Cliente      |
| IdentityFile                    | ~/.ssh/id_dsa, ~/.ssh/id_rsa                                                                                             | Cliente      |
| IgnoreIfUnknown                 | No hay valor predeterminado                                                                                              | Cliente      |
| IgnoreRhosts                    | yes                                                                                                                      | Servidor     |
| IgnoreUserKnownHosts            | yes                                                                                                                      | Servidor     |
| KbdInteractiveAuthentication    | yes                                                                                                                      | Ambos        |
| KeepAlive                       | yes                                                                                                                      | Ambos        |
| KeyRegenerationInterval         | 3600 (segundos)                                                                                                          | Servidor     |

**TABLA 16-2** Palabras clave en archivos de configuración de Secure Shell (de Fall a Local)  
(Continuación)

| Palabra clave | Valor predeterminado        | Ubicación |
|---------------|-----------------------------|-----------|
| ListenAddress | No hay valor predeterminado | Servidor  |
| LocalForward  | No hay valor predeterminado | Cliente   |

**TABLA 16-3** Palabras clave en archivos de configuración de Secure Shell (de Login a R)

| Palabra clave                    | Valor predeterminado                                 | Ubicación |
|----------------------------------|------------------------------------------------------|-----------|
| LoginGraceTime                   | 120 (segundos)                                       | Servidor  |
| LogLevel                         | info                                                 | Ambos     |
| LookupClientHostnames            | yes                                                  | Servidor  |
| MACs                             | hmac-sha1, hmac-md5                                  | Ambos     |
| Match                            | No hay valor predeterminado                          | Servidor  |
| MaxStartups                      | 10:30:60                                             | Servidor  |
| NoHostAuthenticationForLocalHost | no                                                   | Cliente   |
| NumberOfPasswordPrompts          | 3                                                    | Cliente   |
| PAMServiceName                   | No hay valor predeterminado                          | Servidor  |
| PAMServicePrefix                 | No hay valor predeterminado                          | Servidor  |
| PasswordAuthentication           | yes                                                  | Ambos     |
| PermitEmptyPasswords             | no                                                   | Servidor  |
| PermitRootLogin                  | no                                                   | Servidor  |
| PermitUserEnvironment            | no                                                   | Servidor  |
| PidFile                          | /system/volatile/sshd.pid                            | Servidor  |
| Port                             | 22                                                   | Ambos     |
| PreferredAuthentications         | hostbased, publickey, keyboard-interactive, password | Cliente   |
| PreUserauthHook                  | No hay valor predeterminado                          | Servidor  |
| PrintLastLog                     | yes                                                  | Servidor  |
| PrintMotd                        | no                                                   | Servidor  |
| Protocol                         | 2,1                                                  | Ambos     |
| ProxyCommand                     | No hay valor predeterminado                          | Cliente   |

**TABLA 16-3** Palabras clave en archivos de configuración de Secure Shell (de Login a R) *(Continuación)*

| Palabra clave           | Valor predeterminado        | Ubicación    |
|-------------------------|-----------------------------|--------------|
| PubkeyAuthentication    | yes                         | Ambos        |
| RekeyLimit              | 1G a 4G                     | Cliente      |
| RemoteForward           | No hay valor predeterminado | Cliente      |
| RhostsAuthentication    | no                          | Servidor, v1 |
| RhostsRSAAuthentication | no                          | Servidor, v1 |
| RSAAuthentication       | no                          | Servidor, v1 |

**TABLA 16-4** Palabras clave en archivos de configuración de Secure Shell (de S a X)

| Palabra clave         | Valor predeterminado          | Ubicación    |
|-----------------------|-------------------------------|--------------|
| ServerAliveCountMax   | 3                             | Cliente      |
| ServerAliveInterval   | 0                             | Cliente      |
| ServerKeyBits         | 512 a 768                     | Servidor, v1 |
| StrictHostKeyChecking | ask                           | Cliente      |
| StrictModes           | yes                           | Servidor     |
| Subsystem             | sftp /usr/lib/ssh/sftp-server | Servidor     |
| SyslogFacility        | auth                          | Servidor     |
| UseFIPS140            | no                            | Ambos        |
| UseOpenSSLEngine      | yes                           | Ambos        |
| UsePrivilegedPort     | no                            | Ambos        |
| User                  | No hay valor predeterminado   | Cliente      |
| UserKnownHostsFile    | ~/.ssh/known_hosts            | Cliente      |
| UseRsh                | no                            | Cliente      |
| VerifyReverseMapping  | no                            | Servidor     |
| X11DisplayOffset      | 10                            | Servidor     |
| X11Forwarding         | yes                           | Servidor     |
| X11UseLocalHost       | yes                           | Servidor     |
| XAuthLocation         | /usr/bin/xauth                | Ambos        |



## Parámetros específicos de host Secure Shell

Si es útil tener diferentes características de Secure Shell para diferentes hosts locales, el administrador puede definir conjuntos separados de parámetros en el archivo `/etc/ssh/ssh_config` que se aplicarán según la expresión regular o de host. Esta tarea se realiza mediante la agrupación de entradas en el archivo por la palabra clave `Host`. Si la palabra clave `Host` no se utiliza, las entradas en el archivo de configuración del cliente se aplican a cualquier host local en el que un usuario está trabajando.

## Secure Shell y variables de entorno de inicio de sesión

Cuando las siguientes palabras clave de Secure Shell no están establecidas en el archivo `sshd_config` obtienen el valor de entradas equivalentes en el archivo `/etc/default/login`.

| Entrada en <code>/etc/default/login</code>               | Palabra clave y valor en <code>sshd_config</code>                             |
|----------------------------------------------------------|-------------------------------------------------------------------------------|
| <code>CONSOLE=*</code>                                   | <code>PermitRootLogin=without-password</code>                                 |
| <code>#CONSOLE=*</code>                                  | <code>PermitRootLogin=yes</code>                                              |
| <code>PASSREQ=YES</code>                                 | <code>PermitEmptyPasswords=no</code>                                          |
| <code>PASSREQ=NO</code>                                  | <code>PermitEmptyPasswords=yes</code>                                         |
| <code>#PASSREQ</code>                                    | <code>PermitEmptyPasswords=no</code>                                          |
| <code>TIMEOUT=segundos</code>                            | <code>LoginGraceTime=segundos</code>                                          |
| <code>#TIMEOUT</code>                                    | <code>LoginGraceTime=120</code>                                               |
| <code>RETRIES</code> y <code>SYSLOG_FAILED_LOGINS</code> | Sólo se aplican a métodos de autenticación de password y keyboard-interactive |

Cuando las siguientes variables están establecidas por las secuencias de comandos de inicialización del shell de inicio de sesión del usuario, el daemon `sshd` utiliza dichos valores. Cuando las variables no están establecidas, el daemon utiliza el valor predeterminado.

|          |                                                                                                                                                                                                                                                                                              |
|----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| TIMEZONE | Controla la configuración de la variable de entorno TZ. Cuando no está establecida, el daemon <code>sshd</code> utiliza el valor de TZ cuando se inició el daemon.                                                                                                                           |
| ALTSHELL | Controla la configuración de la variable de entorno SHELL. El valor predeterminado es <code>ALTSHELL=YES</code> , donde el daemon <code>sshd</code> utiliza el valor del shell del usuario. Cuando el valor predeterminado es <code>ALTSHELL=NO</code> , el valor SHELL no está establecido. |
| PATH     | Controla la configuración de la variable de entorno PATH. Cuando el valor no está establecido, la ruta predeterminada es <code>/usr/bin</code> .                                                                                                                                             |

**SUPATH** Controla la configuración de la variable de entorno PATH para root. Cuando el valor no está establecido, la ruta predeterminada es /usr/sbin:/usr/bin.

Para obtener más información, consulte las páginas del comando man [login\(1\)](#) y [sshd\(1M\)](#).

## Mantenimiento de hosts conocidos en Secure Shell

Cada host que necesita comunicarse de manera segura con otro host debe tener la clave pública del servidor almacenada en el archivo /etc/ssh/ssh\_known\_hosts del host local. Aunque una secuencia de comandos podría utilizarse para actualizar los archivos /etc/ssh/ssh\_known\_hosts, esta práctica es fuertemente desalentada, porque una secuencia de comandos abre una importante vulnerabilidad de seguridad.

El archivo /etc/ssh/ssh\_known\_hosts sólo debería ser distribuido por un mecanismo seguro, de la siguiente manera:

- Por medio de una conexión segura, como Secure Shell, IPsec o ftp Kerberizado de un equipo conocido y de confianza
- En el tiempo de instalación del sistema

Para evitar la posibilidad de que un intruso obtenga acceso insertando claves públicas falsas en un archivo known\_hosts, debe utilizar un origen conocido y de confianza del archivo ssh\_known\_hosts. El archivo ssh\_known\_hosts se puede distribuir durante la instalación. Más tarde, las secuencias de comandos que utiliza el comando scp se pueden utilizar para obtener la última versión.

## Archivos de Secure Shell

En la siguiente tabla, se muestran los principales archivos de Secure Shell y los permisos de archivo sugeridos.

TABLA 16-5 Archivos de Secure Shell

| Nombre de archivo                                        | Descripción                                                                                                                                              | Permisos sugeridos y propietario |
|----------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------|
| /etc/ssh/sshd_config                                     | Contiene datos de configuración para sshd, el daemon de Secure Shell.                                                                                    | -rw-r--r-- root                  |
| /etc/ssh/ssh_host_dsa_key o<br>/etc/ssh/ssh_host_rsa_key | Contiene la clave privada de host.                                                                                                                       | -rw----- root                    |
| host-private-key.pub                                     | Contiene la clave pública de host, por ejemplo, /etc/ssh/ssh_host_rsa_key.pub. Se utiliza para copiar la clave del host en el archivo known_hosts local. | -rw-r--r-- root                  |

TABLA 16-5 Archivos de Secure Shell (Continuación)

| Nombre de archivo         | Descripción                                                                                                                                                                                                                                                                                            | Permisos sugeridos y propietario |
|---------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------|
| /system/volatile/sshd.pid | Contiene el ID de proceso del daemon de Secure Shell, <code>sshd</code> . Si hay varios daemons en ejecución, el archivo contiene el último daemon que se ha iniciado.                                                                                                                                 | -rw-r--r-- root                  |
| ~/.ssh/authorized_keys    | Contiene las claves públicas del usuario que tiene permitido iniciar sesión en la cuenta de usuario.                                                                                                                                                                                                   | -rw-r--r-- username              |
| /etc/ssh/ssh_known_hosts  | Contiene las claves públicas de host de todos los hosts con los que el cliente puede comunicarse de forma segura. El archivo es rellenado por el administrador.                                                                                                                                        | -rw-r--r-- root                  |
| ~/.ssh/known_hosts        | Contiene las claves públicas de host de todos los hosts con los que el cliente puede comunicarse de forma segura. El archivo se mantiene automáticamente. Cada vez que el usuario se conecta con un host desconocido, la clave del host remoto se agrega al archivo.                                   | -rw-r--r-- username              |
| /etc/default/login        | Proporciona valores predeterminados para el daemon <code>sshd</code> cuando los parámetros <code>sshd_config</code> correspondientes no están establecidos.                                                                                                                                            | -r--r--r-- root                  |
| /etc/nologin              | Si el archivo existe, el daemon <code>sshd</code> sólo permite que <code>root</code> inicie sesión. El contenido de este archivo se muestra a los usuarios que intentan iniciar sesión.                                                                                                                | -rw-r--r-- root                  |
| ~/.rhosts                 | Contiene los pares de host y nombre de usuario que especifican los hosts en los que el usuario puede iniciar sesión sin una contraseña. Este archivo también es utilizado por los daemons <code>rlogind</code> y <code>rshd</code> .                                                                   | -rw-r--r-- username              |
| ~/.shosts                 | Contiene los pares de host y nombre de usuario que especifican los hosts en los que el usuario puede iniciar sesión sin una contraseña. Este archivo no es utilizado por otras utilidades. Para obtener más información, consulte la página del comando <code>man sshd(1M)</code> en la sección FILES. | -rw-r--r-- username              |
| /etc/hosts.equiv          | Contiene los hosts que se utilizan en la autenticación <code>.rhosts</code> . Este archivo también es utilizado por los daemons <code>rlogind</code> y <code>rshd</code> .                                                                                                                             | -rw-r--r-- root                  |
| /etc/ssh/shosts.equiv     | Contiene los hosts que se utilizan en la autenticación basada en host. Este archivo no es utilizado por otras utilidades.                                                                                                                                                                              | -rw-r--r-- root                  |
| ~/.ssh/environment        | Contiene asignaciones iniciales en el momento del inicio de sesión. De manera predeterminada, este archivo no se lee. La palabra clave <code>PermitUserEnvironment</code> en el archivo <code>sshd_config</code> se debe establecer en <code>yes</code> para que este archivo se lea.                  | -rw-r--r-- username              |
| ~/.ssh/rc                 | Contiene las rutinas de inicialización que se ejecutan antes de que el shell del usuario se inicie. Para ver un ejemplo de rutina de inicialización, consulte la página del comando <code>man sshd(1M)</code> .                                                                                        | -rw-r--r-- username              |

TABLA 16-5 Archivos de Secure Shell (Continuación)

| Nombre de archivo   | Descripción                                                                                        | Permisos sugeridos y propietario |
|---------------------|----------------------------------------------------------------------------------------------------|----------------------------------|
| /etc/ssh/sshrcc     | Contiene rutinas de inicialización específicas de host que son especificadas por un administrador. | -rw-r--r-- root                  |
| /etc/ssh/ssh_config | Configura los valores del sistema en el sistema cliente.                                           | -rw-r--r-- root                  |
| ~/.ssh/config       | Configura los valores del usuario que sustituyen los valores del sistema.                          | -rw-r--r-- username              |

**Nota** – El archivo `sshd_config` se pueden sustituir por un archivo de un paquete personalizado para el sitio. Para obtener más información, consulte la definición de atributo de archivo `overlay` en la página del comando `man pkg(5)`.

En la siguiente tabla, se muestran los archivos de Secure Shell que se pueden sustituir por palabras clave u opciones de comandos.

TABLA 16-6 Valores de sustitución para la ubicación de archivos de Secure Shell

| Nombre de archivo           | Valor de sustitución de palabra clave | Valor de sustitución de línea de comandos                                        |
|-----------------------------|---------------------------------------|----------------------------------------------------------------------------------|
| /etc/ssh/ssh_config         |                                       | ssh -F <i>archivo de configuración</i><br>scp -F <i>archivo de configuración</i> |
| ~/.ssh/config               |                                       | ssh -F <i>archivo de configuración</i>                                           |
| /etc/ssh/host_rsa_key       | HostKey                               |                                                                                  |
| /etc/ssh/host_dsa_key       |                                       |                                                                                  |
| ~/.ssh/identity             | IdentityFile                          | ssh -i <i>archivo de identidad</i>                                               |
| ~/.ssh/id_dsa,~/.ssh/id_rsa |                                       | scp -i <i>archivo de identidad</i>                                               |
| ~/.ssh/authorized_keys      | AuthorizedKeysFile                    |                                                                                  |
| /etc/ssh/ssh_known_hosts    | GlobalKnownHostsFile                  |                                                                                  |
| ~/.ssh/known_hosts          | UserKnownHostsFile                    |                                                                                  |
|                             | IgnoreUserKnownHosts                  |                                                                                  |

# Comandos de Secure Shell

En la siguiente tabla, se resumen los principales comandos de Secure Shell.

TABLA 16-7 Comandos en Secure Shell

| Página del comando man          | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">ssh(1)</a>          | Inicia sesión de un usuario en un equipo remoto y ejecuta de manera segura comandos en un equipo remoto. El comando <code>ssh</code> permite comunicaciones cifradas seguras entre dos hosts que no son de confianza por medio de una red no segura. Las conexiones X11 y los puertos TCP/IP arbitrarios también se pueden reenviar por medio del canal seguro.                                                                                                                                                  |
| <a href="#">sshd(1M)</a>        | Es el daemon para Secure Shell. El daemon escucha conexiones de clientes y permite comunicaciones cifradas seguras entre dos hosts que no son de confianza por medio de una red no segura.                                                                                                                                                                                                                                                                                                                       |
| <a href="#">ssh-add(1)</a>      | Agrega identidades RSA o DSA al agente de autenticación, <code>ssh-agent</code> . Las identidades también se denominan <i>claves</i> .                                                                                                                                                                                                                                                                                                                                                                           |
| <a href="#">ssh-agent(1)</a>    | Contiene claves privadas que se utilizan para la autenticación de clave pública. El programa <code>ssh-agent</code> se inicia al principio de una sesión X o de una sesión de inicio de sesión. Todas las demás ventanas y otros programas se inician como clientes del programa <code>ssh-agent</code> . Mediante el uso de variables de entorno, el agente se puede localizar y utilizar para la autenticación cuando los usuarios utilizan el comando <code>ssh</code> para iniciar sesión en otros sistemas. |
| <a href="#">ssh-keygen(1)</a>   | Genera y gestiona claves de autenticación para Secure Shell.                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <a href="#">ssh-keyscan(1)</a>  | Recopila las claves públicas de un número de hosts de Secure Shell. Ayuda en la generación y la verificación de archivos <code>ssh_known_hosts</code> .                                                                                                                                                                                                                                                                                                                                                          |
| <a href="#">ssh-keysign(1M)</a> | Es utilizado por el comando <code>ssh</code> para acceder a las claves de host en el host local. Genera la firma digital que se requiere durante la autenticación basada en host con Secure Shell v2. El comando es invocado por el comando <code>ssh</code> , no por el usuario.                                                                                                                                                                                                                                |
| <a href="#">scp(1)</a>          | Copia de manera segura archivos entre hosts en una red por medio de un transporte <code>ssh</code> cifrado. A diferencia del comando <code>rcp</code> , el comando <code>scp</code> solicita contraseñas o frases de contraseña si la información de contraseña es necesaria para la autenticación.                                                                                                                                                                                                              |
| <a href="#">sftp(1)</a>         | Es un programa de transferencia de archivos interactivo similar al comando <code>ftp</code> . A diferencia del comando <code>ftp</code> , el comando <code>sftp</code> realiza todas las operaciones por medio de un transporte <code>ssh</code> cifrado. El comando se conecta, inicia sesión en el nombre de host especificado y, a continuación, introduce el modo de comando interactivo.                                                                                                                    |

En la siguiente tabla, se muestran las opciones de comandos que sustituyen palabras clave de Secure Shell. Las palabras clave se especifican en los archivos `ssh_config` y `sshd_config`.

TABLA 16-8 Equivalentes de línea de comandos para palabras clave de Secure Shell

| Palabra clave | Valor de sustitución de línea de comandos ssh | Valor de sustitución de línea de comandos scp |
|---------------|-----------------------------------------------|-----------------------------------------------|
| BatchMode     |                                               | <code>scp -B</code>                           |

TABLA 16–8 Equivalentes de línea de comandos para palabras clave de Secure Shell (Continuación)

| Palabra clave  | Valor de sustitución de línea de comandos ssh           | Valor de sustitución de línea de comandos scp |
|----------------|---------------------------------------------------------|-----------------------------------------------|
| BindAddress    | ssh -b <i>dirección de enlace</i>                       | scp -a <i>dirección de enlace</i>             |
| Cipher         | ssh -c <i>cifrado</i>                                   | scp -c <i>cifrado</i>                         |
| Ciphers        | ssh -c <i>especificación de cifrado</i>                 | scp -c <i>especificación de cifrado</i>       |
| Compression    | ssh -C                                                  | scp -C                                        |
| DynamicForward | ssh -D <i>puerto SOCKS4</i>                             |                                               |
| EscapeChar     | ssh -e <i>carácter de escape</i>                        |                                               |
| ForwardAgent   | ssh -A para activar<br>ssh -a para desactivar           |                                               |
| ForwardX11     | ssh -X para activar<br>ssh -x para desactivar           |                                               |
| GatewayPorts   | ssh -g                                                  |                                               |
| IPv4           | ssh -4                                                  | scp -4                                        |
| IPv6           | ssh -6                                                  | scp -6                                        |
| LocalForward   | ssh -L<br><i>puerto_local:host_remoto:puerto_remoto</i> |                                               |
| MACS           | ssh -m <i>especificación de mac</i>                     |                                               |
| Port           | ssh -p <i>puerto</i>                                    | scp -P <i>puerto</i>                          |
| Protocol       | ssh -2 sólo para v2                                     |                                               |
| RemoteForward  | ssh -R<br><i>puerto_remoto:host_local:puerto_local</i>  |                                               |

## Uso de autenticación simple y capa de seguridad

---

En este capítulo se incluye información sobre la autenticación sencilla y capa de seguridad (SASL).

- “SASL (descripción general)” en la página 331
- “SASL (referencia)” en la página 332

### SASL (descripción general)

La autenticación sencilla y capa de seguridad (SASL) es una estructura que proporciona autenticación y servicios de seguridad opcionales a los protocolos de red. Una aplicación llama a la biblioteca SASL, `/usr/lib/libsasl.so`, que proporciona una capa intermedia entre la aplicación y los distintos mecanismos de SASL. Los mecanismos se utilizan en el proceso de autenticación y para la prestación servicios de seguridad opcionales. La versión de SASL proviene de Cyrus SASL con algunos cambios.

SASL proporciona los siguientes servicios:

- Carga de cualquier complemento
- Determinación de las opciones de seguridad necesarias de la aplicación para ayudar a elegir un mecanismo de seguridad
- Listado de los complementos que están disponibles para la aplicación
- Elección del mejor mecanismo de una lista de los mecanismos disponibles para un determinado intento de autenticación
- Enrutamiento de datos de autenticación entre la aplicación y el mecanismo elegido
- Información sobre la negociación de SASL de nuevo a la aplicación

## SASL (referencia)

En la siguiente sección se proporciona información sobre la implementación de SASL.

### Complementos de SASL

Los complementos de SASL admiten mecanismos de seguridad, canonización del usuario y recuperación de propiedad auxiliar. De manera predeterminada, los complementos de 32 bits cargados dinámicamente se instalan en `/usr/lib/sasl`, y los complementos de 64 bits se instalan en `/usr/lib/sasl/ $ISA`. Se proporcionan los siguientes complementos de mecanismo de seguridad:

|                             |                                                                                                                                                                    |
|-----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>crammd5.so.1</code>   | CRAM-MD5, que admite sólo autenticación, no autorización.                                                                                                          |
| <code>digestmd5.so.1</code> | DIGEST-MD5, que admite autenticación, integridad, privacidad y autorización.                                                                                       |
| <code>gssapi.so.1</code>    | GSSAPI, que admite autenticación, integridad, privacidad y autorización. El mecanismo de seguridad GSSAPI requiere una infraestructura Kerberos en funcionamiento. |
| <code>plain.so.1</code>     | PLAIN, que admite autenticación y autorización.                                                                                                                    |

Además, el complemento de mecanismo de seguridad EXTERNAL y el complemento de canonización de usuario INTERNAL están integrados en `libsasl.so.1`. El mecanismo EXTERNAL admite la autenticación y la autorización. El mecanismo admite integridad y privacidad, si el origen de la seguridad externa la proporciona. El complemento INTERNAL agrega el nombre de dominio al nombre de usuario, si es necesario.

La versión de Oracle Solaris no suministra ningún complemento `auxprop` en este momento. Para que los complementos de mecanismo CRAM-MD5 y DIGEST-MD5 funcionen plenamente en el servidor, el usuario debe proporcionar un complemento `auxprop` para recuperar contraseñas de texto sin cifrar. El complemento PLAIN requiere asistencia adicional para verificar la contraseña. La asistencia para la verificación de la contraseña puede ser una de las siguientes opciones: una devolución de llamada a la aplicación del servidor, un complemento `auxprop`, `saslauthd` o `pwcheck`. Los daemons `saslauthd` y `pwcheck` no se proporcionan en las versiones de Oracle Solaris. Para obtener una mejor interoperabilidad, restrinja las aplicaciones del servidor a los mecanismos que sean totalmente operativos mediante la opción de SASL `mech_list`.

### Variable de entorno de SASL

De manera predeterminada, el nombre de autenticación del cliente se establece en `getenv("LOGNAME")`. Esta variable puede ser restablecida por el cliente o por el complemento.



## Opciones de SASL

El comportamiento de `libsasl` y los complementos se pueden modificar en el servidor mediante las opciones que se pueden establecer en el archivo `/etc/sasl/app.conf`. La variable *app* es el nombre definido por el servidor para la aplicación. La documentación de la *aplicación* del servidor debe especificar el nombre de la aplicación.

Se admiten las siguientes opciones:

|                                |                                                                                                                                                                                                                                                                       |
|--------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>auto_transition</code>   | Pasa al usuario automáticamente a otros mecanismos cuando el usuario realiza una autenticación de texto sin formato correcta.                                                                                                                                         |
| <code>auxprop_login</code>     | Muestra el nombre de los complementos de propiedad auxiliar que se van a utilizar.                                                                                                                                                                                    |
| <code>canon_user_plugin</code> | Selecciona el complemento <code>canon_user</code> que se va a utilizar.                                                                                                                                                                                               |
| <code>mech_list</code>         | Muestra los mecanismos que la aplicación del servidor tiene permitido utilizar.                                                                                                                                                                                       |
| <code>pwcheck_method</code>    | Muestra los mecanismos utilizados para verificar las contraseñas. Actualmente, <code>auxprop</code> es el único valor permitido.                                                                                                                                      |
| <code>reauth_timeout</code>    | Ajusta el tiempo, en minutos, durante el cual la información de autenticación se almacena en la caché para una nueva autenticación rápida. Esta opción es utilizada por el complemento DIGEST-MD5. Al definir esta opción en 0, se desactiva una nueva autenticación. |

Las siguientes opciones no se admiten:

|                             |                                                                                                                                                                                                                                                                       |
|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>plugin_list</code>    | Muestra los mecanismos disponibles. No se utiliza porque la opción cambia el comportamiento de la carga dinámica de los complementos.                                                                                                                                 |
| <code>saslauthd_path</code> | Define la ubicación de la puerta <code>saslauthd</code> , que se utiliza para la comunicación con el daemon <code>saslauthd</code> . El daemon <code>saslauthd</code> no se incluye en la versión de Oracle Solaris. Por lo tanto, esta opción tampoco está incluida. |
| <code>keytab</code>         | Define la ubicación del archivo <code>keytab</code> usado por el complemento GSSAPI. Utilice la variable de entorno <code>KRB5_KTNAME</code> en su lugar para establecer la ubicación predeterminada de <code>keytab</code> .                                         |

Las siguientes son opciones que no se encuentran en Cyrus SASL. Sin embargo, se agregaron a la versión de Oracle Solaris:

|                         |                                                                                                                                                                                                                                    |
|-------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>use_authid</code> | Adquiere las credenciales del cliente en lugar de utilizar las credenciales predeterminadas al crear el contexto de seguridad del cliente GSS. De manera predeterminada, se utiliza la identidad Kerberos del cliente por defecto. |
| <code>log_level</code>  | Establece el nivel deseado de registro para un servidor.                                                                                                                                                                           |



## Autenticación de servicios de red (tareas)

---

En este capítulo, se proporciona información sobre cómo utilizar RPC segura para autenticar un host y un usuario en un montaje NFS, y se incluyen los siguientes temas:

- “Descripción general de RPC segura” en la página 335
- “Administración de autenticación con RPC segura (tareas)” en la página 340

### Descripción general de RPC segura

RPC segura (llamada de procedimiento remoto) protege los procedimientos remotos con un mecanismo de autenticación. El mecanismo de autenticación Diffie-Hellman autentica tanto el host como el usuario que realiza una solicitud para un servicio. El mecanismo de autenticación utiliza el cifrado Estándar de cifrado de datos (DES). Entre las aplicaciones que utilizan RPC segura se incluyen NFS y el servicio de nombres NIS.

### Servicios NFS y RPC segura

NFS permite que varios hosts compartan archivos mediante la red. En el servicio NFS, un servidor contiene los datos y recursos para varios clientes. Los clientes tienen acceso a los sistemas de archivos que el servidor comparte con los clientes. Los usuarios conectados a los sistemas cliente pueden acceder a los sistemas de archivos mediante el montaje de sistemas de archivos del servidor. Para el usuario en el sistema cliente, los archivos se ven como locales para el cliente. Uno de los usos más comunes de NFS permite que los sistemas se instalen en oficinas mientras se almacenan todos los archivos de usuario en una ubicación central. Algunas de las funciones del servicio NFS, como la opción `-nosuid` para el comando `mount`, se pueden utilizar para prohibir la apertura de dispositivos y sistemas de archivos por parte de usuarios no autorizados.

El servicio NFS utiliza RPC segura para autenticar a los usuarios que realizan solicitudes a través de la red. Este proceso se conoce como *NFS seguro*. El mecanismo de autenticación Diffie-Hellman, AUTH\_DH, usa cifrado DES para garantizar el acceso autorizado. El mecanismo AUTH\_DH también se ha denominado AUTH\_DES. Para obtener más información, consulte lo siguiente:

- Para configurar y administrar Secure NFS, consulte [“Administración de sistema NFS seguro” de Gestión de sistemas de archivos de red en Oracle Solaris 11.1](#).
- Para una descripción de las transacciones implicadas en la autenticación RPC, consulte [“Implementación de autenticación Diffie-Hellman” en la página 337](#).

## Autenticación Kerberos

Kerberos es un sistema de autenticación desarrollado en MIT. Algunos cifrados en Kerberos se basan en DES. El soporte de Kerberos V4 ya no se proporciona como parte de RPC segura. Sin embargo, una implementación por parte del cliente y por parte del servidor de Kerberos V5, que utiliza RPCSEC\_GSS, se incluye con esta versión. Para obtener más información, consulte [“Cómo configurar servidores NFS con Kerberos” en la página 399](#).

## Cifrado DES con NFS seguro

Las funciones de cifrado del Estándar de cifrado de datos (DES) utiliza una clave de 56 bits para cifrar los datos. Si dos principales o usuarios de credenciales conocen la misma clave DES, pueden comunicarse en privado mediante la clave para cifrar y descifrar texto. DES es un mecanismo de cifrado relativamente rápido.

El riesgo de usar sólo la clave DES es que un intruso puede recopilar suficientes mensajes de texto cifrado que se cifraron con la misma clave para poder descubrir la clave y descifrar los mensajes. Por este motivo, los sistemas de seguridad como NFS seguro necesitan cambiar las claves con frecuencia.

## Autenticación Diffie-Hellman y RPC segura

El método de autenticación de un usuario Diffie-Hellman (DH) no es trivial para un intruso que quiere ingresar. El cliente y el servidor tienen sus propias claves privadas, las cuales se utilizan con la clave pública para crear una clave común. La clave privada también se conoce como *clave secreta*. El cliente y el servidor utilizan la clave común para comunicarse entre sí. La clave común se cifra con una función de cifrado acordada, como DES.

La autenticación se basa en la capacidad del sistema emisor de utilizar la clave común para cifrar la hora actual. A continuación, el sistema receptor puede descifrar y comprobar la hora actual.

La hora en el cliente y el servidor debe estar sincronizada. Para obtener más información, consulte “[Gestión del protocolo de hora de red \(tarear\)](#)” de *Introducción a los servicios de red de Oracle Solaris 11*.

Las claves públicas y privadas se almacenan en una base de datos de NIS. NIS almacena las claves en el mapa `publickey`. Este archivo contiene la clave pública y la clave privada para todos los usuarios potenciales.

El administrador del sistema es responsable de configurar mapas NIS y de generar una clave pública y una clave privada para cada usuario. La clave privada se almacena en formato cifrado con la contraseña del usuario. Este proceso hace que sólo el usuario conozca la clave privada.

## Implementación de autenticación Diffie-Hellman

En esta sección, se describe la serie de transacciones en una sesión cliente-servidor que utiliza autenticación Diffie-Hellman (`AUTH_DH`).

### Generación de las claves públicas y las claves secretas para RPC segura

A veces, antes de una transacción, el administrador ejecuta el comando `newkey` o el comando `nisaddcred` para generar una clave pública y una clave secreta. Cada usuario tiene una clave pública y una clave secreta únicas. La clave pública se almacena en una base de datos pública. La clave secreta se almacena en formato cifrado en la misma base de datos. El comando `chkey` cambia el par de claves.

### Ejecución del comando `keylogin` para RPC segura

Normalmente, la contraseña de inicio de sesión es idéntica a la contraseña de RPC segura. En este caso, el comando `keylogin` no es necesario. Sin embargo, si las contraseñas son distintas, los usuarios tienen que iniciar sesión y, a continuación, ejecutar el comando `keylogin`.

El comando `keylogin` le solicita al usuario una contraseña de RPC segura. El comando utiliza la contraseña para descifrar la clave secreta. El comando `keylogin` pasa la clave secreta descifrada al programa *servidor de claves*. El servidor de claves es un servicio RPC con una instancia local en cada equipo. El servidor de claves guarda la clave secreta descifrada y espera a que el usuario inicie una transacción RPC segura con un servidor.

Si la contraseña de inicio de sesión y la contraseña de RPC son iguales, el proceso de inicio de sesión pasa la clave secreta al servidor de claves. Si las contraseñas deben ser diferentes, el usuario debe ejecutar siempre el comando `keylogin`. Cuando el comando `keylogin` se incluye en el archivo de configuración del entorno del usuario, como el archivo `~/.login`, `~/.cshrc` o `~/.profile`, el comando `keylogin` se ejecuta automáticamente siempre que el usuario inicia sesión.

## Generación de clave de conversación para RPC segura

Cuando el usuario inicia una transacción con un servidor, ocurre lo siguiente:

1. El servidor de claves genera aleatoriamente una clave de conversación.
2. El núcleo usa la clave de conversación junto con otros materiales para cifrar la indicación de hora del cliente.
3. El servidor de claves busca la clave pública del servidor en la base de datos de claves públicas. Para obtener más información, consulte la página del comando `man publickey(4)`.
4. El servidor de claves utiliza la clave secreta del cliente y la clave pública del servidor para crear una clave común.
5. El servidor de claves cifra la clave de conversación con la clave común.

## Ponerse en contacto inicialmente con el servidor en RPC segura

La transmisión, que incluye la indicación de hora cifrada y la clave de conversación cifrada, se envía al servidor. La transmisión incluye una credencial y un verificador. La credencial contiene tres componentes:

- El nombre de red del cliente
- La clave de conversación, que se cifra con la clave común
- Una "ventana", que se cifra con la clave de conversación

La ventana es la diferencia en tiempo que el cliente afirma que se debe permitir entre el reloj del servidor y la indicación de hora del cliente. Si la diferencia entre el reloj del servidor y la indicación de hora es mayor que la ventana, el servidor rechaza la solicitud del cliente. En circunstancias normales, este rechazo no se produce porque el cliente primero se sincroniza con el servidor antes de iniciar la sesión RPC.

El verificador del cliente contiene lo siguiente:

- La indicación de hora cifrada
- Un verificador cifrado de la ventana especificada, que se reduce a 1

El verificador de ventana es necesario en caso de que alguien desee asumir la personalidad de un usuario. El imitador puede escribir un programa que, en lugar de completar los campos cifrados de la credencial y el verificador, sólo inserte bits de manera aleatoria. El servidor descifra la clave de conversación en alguna clave aleatoria. El servidor utiliza la clave para intentar descifrar la ventana y la indicación de hora. El resultado son números aleatorios. Después de miles de intentos, sin embargo, el par ventana/indicación de hora aleatorio podría pasar el sistema de autenticación. El verificador de ventana disminuye la posibilidad de que una credencial falsa se pueda autenticar.

## Descifrado de la clave de conversación en RPC segura

Cuando el servidor recibe la transmisión del cliente, se produce lo siguiente:

1. El servidor de claves local del servidor busca la clave pública del cliente en la base de datos de claves públicas.
2. El servidor de claves utiliza la clave pública del cliente y la clave secreta del servidor para deducir la clave común. La clave común es la misma clave común que el cliente procesa. Sólo el servidor y el cliente pueden calcular la clave común porque el cálculo requiere que se conozca una de las claves secretas.
3. El núcleo usa la clave común para descifrar la clave de conversación.
4. El núcleo llama al servidor de claves para descifrar la indicación de hora del cliente con la clave de conversación descifrada.

## Almacenamiento de información en el servidor en RPC segura

Después de que el servidor descifra la indicación de hora del cliente, el servidor almacena cuatro elementos de información en una tabla de credenciales:

- El nombre de equipo del cliente
- La clave de conversación
- La ventana
- La indicación de hora del cliente

El servidor almacena los primeros tres elementos para su uso futuro. El servidor almacena la indicación de hora del cliente para evitar que se realicen reproducciones. El servidor acepta sólo indicaciones de hora que son cronológicamente mayores que la última indicación de hora vista. Como resultado, cualquier transacción reproducida seguramente sea rechazada.

---

**Nota** – El nombre del emisor de llamada está implícito en las transacciones. El emisor se debe autenticar de alguna manera. El servidor de claves no puede usar la autenticación DES para autenticar el emisor de llamada porque el uso de DES por parte del servidor de claves crearía un interbloqueo. Para evitar un interbloqueo, el servidor de claves almacena las claves secretas por ID de usuario (UID) y otorga solicitudes sólo a procesos root locales.

---

## Devolución del verificador al cliente en RPC segura

El servidor devuelve un verificador al cliente, que incluye lo siguiente:

- El ID de índice, que el servidor registra en su caché de credenciales
- La indicación de hora del cliente menos 1, que se cifra mediante la clave de conversación

El motivo para sustraer 1 de la indicación de hora del cliente es para asegurarse de que la indicación de hora esté desactualizada. Una indicación de hora desactualizada no puede volver a utilizarse como un verificador de cliente.

### Autenticación del servidor en RPC segura

El cliente recibe el verificador y autentica el servidor. El cliente sabe que sólo el servidor pudo haber enviado el verificador ya que sólo el servidor conoce la indicación de hora que el cliente envió.

### Manejo de transacciones en RPC segura

Con cada transacción después de la primera transacción, el cliente devuelve el ID de índice al servidor en su siguiente transacción. El cliente también envía otra indicación de hora cifrada. El servidor envía de vuelta la indicación de hora del cliente menos 1, que se cifra mediante la clave de conversación.

## Administración de autenticación con RPC segura (tareas)

Al requerir autenticación para el uso de sistemas de archivos NFS montados, aumenta la seguridad de la red.

### Administración de RPC segura (mapa de tareas)

El siguiente mapa de tareas indica los procedimientos que configuran RPC segura para NIS y NFS.

| Tarea                                       | Descripción                                                                                                         | Para obtener instrucciones                                                                      |
|---------------------------------------------|---------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------|
| 1. Iniciar el servidor de claves            | Asegura que se puedan crear claves para que se puedan autenticar los usuarios.                                      | <a href="#">“Cómo reiniciar el servidor de claves RPC segura” en la página 340</a>              |
| 2. Configurar credenciales en un host NIS   | Asegura que el usuario root en un host se pueda autenticar en un entorno NIS.                                       | <a href="#">“Cómo configurar una clave Diffie-Hellman para un host NIS” en la página 341</a>    |
| 3. Otorgar una clave a un usuario NIS       | Permite que se autentique un usuario en un entorno NIS.                                                             | <a href="#">“Cómo configurar una clave Diffie-Hellman para un usuario NIS” en la página 342</a> |
| 4. Compartir archivos NFS con autenticación | Permite a un servidor NFS proteger de manera segura los sistemas de archivos compartidos mediante la autenticación. | <a href="#">“Cómo compartir archivos NFS con autenticación Diffie-Hellman” en la página 343</a> |

### ▼ Cómo reiniciar el servidor de claves RPC segura

**Antes de empezar** Debe asumir el rol root. Para obtener más información, consulte [“Cómo usar los derechos administrativos que tiene asignados” en la página 164](#).



## 1 Verifique que el daemon `key serv` esté en ejecución.

```
svcs *key serv*
STATE STIME FMRI
disabled Dec_14 svc:/network/rpc/key serv
```

## 2 Active el servicio de servidor de claves si el servidor no está en línea.

```
svcadm enable network/rpc/key serv
```

# ▼ Cómo configurar una clave Diffie-Hellman para un host NIS

Este procedimiento debe realizarse en cada host en el dominio NIS.

### Antes de empezar

Debe asumir el rol `root`. Para obtener más información, consulte [“Cómo usar los derechos administrativos que tiene asignados” en la página 164](#).

## 1 Si el servicio de nombres predeterminado no es NIS, agregue el mapa `publickey` al servicio de nombres.

### a. Verifique que el valor de `config/default` para el servicio de nombres no sea `nis`.

```
svccfg -s name-service/switch listprop config
config application
config/value_authorization astring solaris.smf.value.name-service.switch
config/default astring files
config/host astring "files nis dns"
config/printer astring "user files nis"
```

Si el valor de `config/default` es `nis`, puede detenerse aquí.

### b. Establezca el servicio de nombres para `publickey` en `nis`.

```
svccfg
svccfg -s name-service/switch setprop config/publickey = astring: "nis"
svccfg -s name-service/switch:default refresh
```

### c. Confirme el valor `publickey`.

```
svccfg
svccfg -s name-service/switch listprop
config application
config/value_authorization astring solaris.smf.value.name-service.switch
config/default astring files
config/host astring "files nis dns"
config/printer astring "user files nis"
config/publickey astring nis
```

En este sistema, el valor de `publickey` se muestra porque es diferente del predeterminado, `files`.

**2 Cree un nuevo par de claves mediante el comando newkey.**

```
newkey -h hostname
```

Donde *hostname* es el nombre del cliente.

**Ejemplo 18-1 Configuración de una nueva clave para root en un cliente NIS**

En el siguiente ejemplo, *earth* se configura como un cliente NIS seguro. Se asigna al administrador el perfil de derechos de seguridad del servicio de nombres.

```
newkey -h earth
Adding new key for unix.earth@example.com
New Password: <Type password>
Retype password: <Retype password>
Please wait for the database to get updated...
Your new key has been successfully stored away.
#
```

## ▼ Cómo configurar una clave Diffie-Hellman para un usuario NIS

Este procedimiento debe realizarse para cada usuario en el dominio NIS.

**Antes de empezar**

Sólo los administradores del sistema, cuando inician sesión en el servidor maestro NIS, pueden generar una nueva clave para un usuario. Los administradores deben tener asignado el perfil de derechos de seguridad del servicio de nombres.

**1 Conviértase en administrador con los atributos de seguridad necesarios.**

Para obtener más información, consulte [“Cómo usar los derechos administrativos que tiene asignados” en la página 164](#).

**2 Cree una nueva clave para un usuario.**

```
newkey -u username
```

Done *username* es el nombre del usuario. El sistema solicita una contraseña. Puede escribir una contraseña genérica. La clave privada se almacena en formato cifrado mediante la contraseña genérica.

**3 Indique al usuario que inicie sesión y escriba el comando chkey -p.**

Este comando permite a los usuarios volver a cifrar sus claves privadas con una contraseña que sólo ellos conozcan.

---

**Nota** – El comando `chkey` se puede utilizar para crear un nuevo par de claves para un usuario.

---

### Ejemplo 18–2 Configuración y cifrado de una nueva clave de usuario en NIS

En este ejemplo, el superusuario configura la clave.

```
newkey -u jdoe
Adding new key for unix.12345@example.com
New Password: <Type password>
Retype password: <Retype password>
Please wait for the database to get updated...
Your new key has been successfully stored away.
#
```

Luego el usuario `jdoe` vuelve a cifrar la clave con una contraseña privada.

```
% chkey -p
Updating nis publickey database.
Reencrypting key for unix.12345@example.com
Please enter the Secure-RPC password for jdoe: <Type password>
Please enter the login password for jdoe: <Type password>
Sending key change request to centralexample...
```

## ▼ Cómo compartir archivos NFS con autenticación Diffie-Hellman

Este procedimiento protege los sistemas de archivos compartidos en un servidor NFS mediante la solicitud de autenticación para acceso.

#### Antes de empezar

La autenticación de clave pública Diffie-Hellman debe estar activada en la red. Para activar la autenticación en la red, complete [“Cómo configurar una clave Diffie-Hellman para un host NIS” en la página 341](#).

Para realizar esta tarea, debe convertirse en un administrador con el perfil de derechos de administración del sistema asignado. Para obtener más información, consulte [“Cómo usar los derechos administrativos que tiene asignados” en la página 164](#).

#### 1 En el servidor NFS, comparta un sistema de archivos con autenticación Diffie-Hellman.

```
share -F nfs -o sec=dh /filesystem
```

Donde *filesystem* es el sistema de archivos que se va a compartir.

La opción `-o sec=dh` significa que la autenticación `AUTH_DH` ahora es necesaria para acceder al sistema de archivos.

**2 En un cliente NFS, monte un sistema de archivos con autenticación Diffie-Hellman.**

**# mount -F nfs -o sec=dh server:filesystem mount-point**

*server* Es el nombre del sistema que comparte *filesystem*

*filesystem* Es el nombre del sistema de archivos que se comparte, como *opt*

*mount-point* Es el nombre del punto de montaje, como */opt*

La opción **-o sec=dh** monta el sistema de archivos con autenticación AUTH\_DH.

## P A R T E V I

# Servicio Kerberos

En esta sección se proporciona información acerca de la configuración, la gestión y el uso del servicio Kerberos en los siguientes capítulos:

- Capítulo 19, “Introducción al servicio Kerberos”
- Capítulo 20, “Planificación del servicio Kerberos”
- Capítulo 21, “Configuración del servicio Kerberos (tareas)”
- Capítulo 22, “Mensajes de error y resolución de problemas de Kerberos”
- Capítulo 23, “Administración de las políticas y los principales de Kerberos (tareas)”
- Capítulo 24, “Uso de aplicaciones Kerberos (tareas)”
- Capítulo 25, “El servicio Kerberos (referencia)”



## Introducción al servicio Kerberos

---

En este capítulo, se brinda una introducción al servicio Kerberos. A continuación, se presenta la información general que se incluye en este capítulo.

- “¿Qué es el servicio Kerberos?” en la página 347
- “Cómo funciona el servicio Kerberos” en la página 348
- “Servicios de seguridad de Kerberos” en la página 355
- “Componentes de las distintas versiones de Kerberos” en la página 356

### ¿Qué es el servicio Kerberos?

El servicio *Kerberos* es una arquitectura cliente-servidor que proporciona seguridad a las transacciones en las redes. El servicio ofrece una sólida autenticación de usuario y también integridad y privacidad. La *autenticación* garantiza que las identidades del remitente y del destinatario de las transacciones de la red sean verdaderas. El servicio también puede verificar la validez de los datos que se transfieren de un lugar a otro (*integridad*) y cifrar los datos durante la transmisión (*privacidad*). Con el servicio Kerberos, puede iniciar sesión en otros equipos, ejecutar comandos, intercambiar datos y transferir archivos de manera segura. Además, Kerberos proporciona servicios de *autorización*, que permiten a los administradores restringir el acceso a los servicios y los equipos. Asimismo, como usuario de Kerberos, puede regular el acceso de otras personas a su cuenta.

El servicio Kerberos es un sistema de *inicio de sesión único*. Esto significa que sólo debe autenticarse con el servicio una vez por sesión, y todas las transacciones realizadas posteriormente durante la sesión se aseguran de manera automática. Una vez que el servicio lo autenticó, no necesita volver a autenticarse cada vez que utiliza un comando basado en Kerberos, como ftp o ssh, o accede a datos en un sistema de archivos NFS. Por lo tanto, no es necesario que envíe la contraseña a través de la red, donde puede ser interceptada, cada vez que utiliza estos servicios.

El servicio Kerberos en la versión de Oracle Solaris se basa en el protocolo de autenticación de red Kerberos V5, que fue desarrollado en el Instituto Tecnológico de Massachusetts (MIT,

Massachusetts Institute of Technology). A quienes hayan utilizado el producto Kerberos V5, la versión de Oracle Solaris les resultará muy familiar. Dado que el protocolo Kerberos V5 es un estándar *de facto* para la seguridad de la red en la industria, la versión de Oracle Solaris promueve la interoperabilidad con otros sistemas. En otras palabras, como el servicio Kerberos en la versión de Oracle Solaris funciona con sistemas que usan el protocolo Kerberos V5, el servicio favorece las transacciones seguras incluso en redes heterogéneas. Además, el servicio proporciona autenticación y seguridad tanto entre dominios como dentro de un único dominio.

El servicio Kerberos brinda flexibilidad para la ejecución de las aplicaciones de Oracle Solaris. Puede configurar el servicio para permitir solicitudes de servicios de red que se basen o no en Kerberos, como el servicio NFS, `telnet` y `ftp`. Como resultado, las aplicaciones actuales seguirán funcionando, incluso si se ejecutan en sistemas en que el servicio Kerberos no se encuentre activado. Igualmente, puede configurar el servicio Kerberos para permitir únicamente solicitudes de red que se basen en Kerberos.

El servicio Kerberos ofrece un mecanismo de seguridad que permite el uso de Kerberos para la autenticación, la integridad y la privacidad cuando se utilizan aplicaciones que emplean Generic Security Service Application Programming Interface (GSS-API). Sin embargo, no es necesario que las aplicaciones permanezcan comprometidas con el servicio Kerberos si se desarrollan otros mecanismos de seguridad. Como el servicio está diseñado para integrarse en GSS-API de manera modular, las aplicaciones que utilizan GSS-API pueden emplear el mecanismo de seguridad que mejor se ajuste a sus necesidades.

## Cómo funciona el servicio Kerberos

A continuación, se ofrece una descripción general del sistema de autenticación Kerberos. Para obtener una descripción más detallada, consulte [“Cómo funciona el sistema de autenticación Kerberos” en la página 537](#).

Desde el punto de vista del usuario, una vez que se inició la sesión Kerberos, el servicio Kerberos queda invisible la mayor parte del tiempo. Los comandos, como `ssh` o `ftp`, funcionan de manera similar. Normalmente, para inicializar una sesión Kerberos sólo se debe iniciar sesión y proporcionar una contraseña de Kerberos.

El sistema Kerberos se basa en el concepto de *tickets*. Un ticket es un conjunto de información electrónica que identifica a un usuario o servicio, como el servicio NFS. Así como su licencia de conducir lo identifica e indica qué privilegios tiene para conducir un automóvil, el ticket lo identifica e indica qué privilegios tiene para acceder a la red. Cuando realiza una transacción que se basa en Kerberos (por ejemplo, si inicia sesión en otro equipo de manera remota), envía de manera transparente una solicitud de un ticket a un *Centro de distribución de claves* (KDC). El KDC accede a una base de datos para autenticar su identidad y devuelve un ticket que le concede permiso para acceder a otro equipo. La expresión "de manera transparente" implica que no necesita solicitar un ticket de manera explícita. La solicitud forma parte de la actividad



del comando `rlogin`. Debido a que sólo los clientes que están autenticados pueden obtener un ticket para un servicio específico, los demás clientes no pueden usar `rlogin` con una identidad asumida.

Los tickets tienen ciertos atributos asociados a ellos. Por ejemplo, un ticket puede ser *reenviable*, lo que significa que se puede utilizar en otro equipo sin que se realice un nuevo proceso de autenticación. Asimismo, un ticket puede ser *posfechado*, que significa que no adquiere validez hasta un momento especificado. El modo de uso de los tickets, por ejemplo, para especificar qué usuarios pueden obtener los distintos tipos de tickets, se establece mediante *políticas*. Las políticas se determinan durante la instalación o administración del servicio Kerberos.

---

**Nota** – Con frecuencia verá los términos *credencial* y *ticket*. En el ámbito de Kerberos en general, estos términos se utilizan de manera indistinta. Sin embargo, técnicamente, una credencial es un ticket con una *clave de sesión* para una sesión determinada. Esta diferencia se explica en profundidad en [“Obtención de acceso a un servicio con Kerberos” en la página 537](#).

---

Las siguientes secciones explican más detalladamente el proceso de autenticación Kerberos.

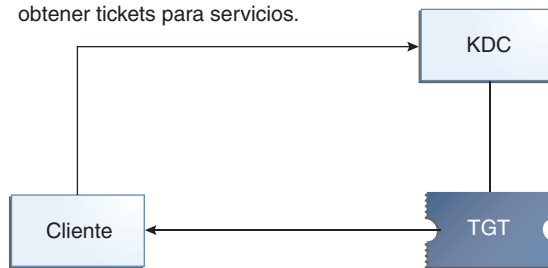
## Autenticación inicial: el ticket de otorgamiento de tickets

La autenticación de Kerberos tiene dos fases: una autenticación inicial que permite que se lleven a cabo todas las autenticaciones posteriores y las autenticaciones posteriores en sí mismas.

La siguiente figura muestra cómo se lleva a cabo la autenticación inicial.

**FIGURA 19-1** Autenticación inicial para una sesión Kerberos

1. En el inicio de sesión (o con `kinit`), el cliente solicita un TGT que le permite obtener tickets para servicios.



3. El cliente usa la contraseña para descifrar, por lo tanto, proporciona la identidad. Ahora puede usar el TGT para obtener otros tickets.
2. El KDC comprueba la base de datos y envía el TGT.

TGT = ticket de otorgamiento de tickets  
KDC = centro de distribución de claves

1. Un cliente (un usuario o un servicio como NFS) comienza una sesión Kerberos mediante la solicitud de un *ticket de otorgamiento de tickets* (TGT) desde el Centro de distribución de claves (KDC). Esta solicitud se suele llevar a cabo automáticamente en el inicio de sesión.

Se necesita un ticket de otorgamiento de tickets para obtener otros tickets de servicios específicos. El ticket de otorgamiento de tickets funciona de manera similar a un pasaporte. Como el pasaporte, el ticket de otorgamiento de tickets lo identifica y le permite obtener muchas “visas” (tickets), que en este caso no son para entrar en países extranjeros sino en equipos remotos o servicios de red. Como los pasaportes y las visas, el ticket de otorgamiento de tickets y otros tickets diversos tienen una duración limitada. La diferencia radica en que los comandos “Kerberizados” detectan que tiene un pasaporte y entonces obtienen las visas para usted. No es necesario que se encargue de efectuar las transacciones.

También puede establecerse un analogía entre el ticket de otorgamiento de tickets y un pase de esquí por tres días que sirve para acceder a cuatro centros de esquí diferentes. Puede exhibir el pase en cualquiera de los centros al que quiera acceder y así obtener un ticket de ascenso para dicho centro, siempre que el pase no esté vencido. Una vez que tenga el ticket de ascenso, puede esquiar cuanto quiera en el centro que eligió. Si el día siguiente quiere ir a otro centro, vuelve a exhibir el pase para conseguir otro ticket de ascenso para ese nuevo centro. La diferencia radica en que los comandos basados en Kerberos detectan que tiene un pase de esquí para el fin de semana y entonces obtienen un ticket de ascenso para usted. No es necesario que se encargue de efectuar las transacciones.

2. El KDC crea un ticket de otorgamiento de tickets y lo envía de vuelta al cliente en formato cifrado. El cliente descifra el ticket de otorgamiento de tickets con la contraseña del cliente.

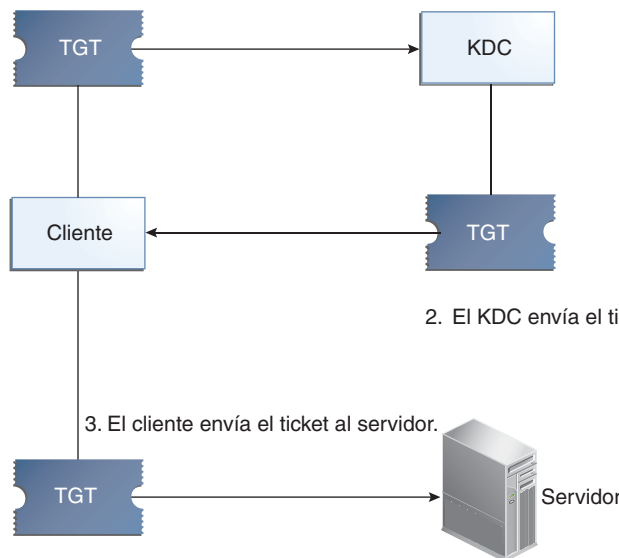
3. Con un ticket de otorgamiento de tickets válido, el cliente puede solicitar tickets para todo tipo de operaciones de red, como `rlogin` o `telnet`, durante todo el período de validez del ticket de otorgamiento de tickets. Por lo general, este ticket dura algunas horas. Cada vez que el cliente realiza una operación de red única, solicita al KDC un ticket para esa operación.

## Autenticaciones Kerberos posteriores

Una vez que el cliente ha recibido la autenticación inicial, cada autenticación posterior sigue el patrón que se muestra en la siguiente figura.

FIGURA 19-2 Obtención de acceso a un servicio con la autenticación Kerberos

1. El cliente solicita el ticket para el servidor y envía el TGT al KDC como prueba de identidad.



2. El KDC envía el ticket al cliente para el servidor.

3. El cliente envía el ticket al servidor.

4. El servidor permite el acceso del cliente.

TGT = ticket de otorgamiento de tickets  
KDC = centro de distribución de claves

1. El cliente solicita al KDC un ticket para un servicio en particular; por ejemplo, para iniciar sesión en otro equipo de manera remota. Para ello, envía al KDC su ticket de otorgamiento de tickets como prueba de identidad.
2. El KDC envía el ticket por el servicio específico al cliente.

Por ejemplo, suponga que el usuario joe quiere acceder a un sistema de archivos NFS que se ha compartido con la autenticación krb5 requerida. Como ya se encuentra autenticado (es decir, ya tiene un ticket de otorgamiento de tickets), cuando intenta acceder a los archivos, el sistema de cliente NFS obtiene un ticket del KDC de manera automática y transparente para el servicio NFS.

Por ejemplo, suponga que el usuario joe utiliza `rlogin` en el servidor `boston`. Como ya se encuentra autenticado, (es decir, ya tiene un ticket de otorgamiento de tickets), obtiene un ticket de manera automática y transparente mediante el comando `rlogin`. Este ticket le permite iniciar sesión de manera remota en `boston` tantas veces como quiera hasta que el ticket caduque. Si joe inicia sesión de manera remota en el equipo `denver`, obtiene otro ticket, como en el paso 1.

3. El cliente envía el ticket al servidor.

Cuando se usa el servicio NFS, el cliente NFS envía el ticket de manera automática y transparente al servidor NFS para el servicio NFS.

4. El servidor permite el acceso de clientes.

Según estos pasos, parece que el servidor nunca se comunica con el KDC. Sin embargo, el servidor sí se comunica. Se registra con el KDC, como lo hace el primer cliente. A fin de simplificar el proceso, esa parte se excluye.

## Aplicaciones remotas de Kerberos

Los comandos basados en Kerberos (o “Kerberizados”) que un usuario como joe puede utilizar son los siguientes:

- `ftp`
- `rcp`, `rlogin`, `rsh`
- `ssh`, `scp`, `sftp`
- `telnet`

Estas aplicaciones son iguales a las aplicaciones de Solaris que tienen el mismo nombre. Sin embargo, se han ampliado a fin de utilizar los principales de Kerberos para autenticar las transacciones y proporcionar así una seguridad basada en Kerberos. Consulte [“Principales de Kerberos” en la página 352](#) para obtener información sobre los principales.

Estos comandos se analizan detalladamente en [“Comandos de usuario de Kerberos” en la página 520](#).

## Principales de Kerberos

Un cliente en el servicio Kerberos se identifica con su *principal*. Un principal es una identidad única a la que el KDC puede asignar tickets. Un principal puede ser un usuario, como joe, o un servicio, como `nfs` o `telnet`.

Por convención, el nombre de principal consta de tres componentes: el *nombre primario*, la *instancia* y el *dominio*. Un principal de Kerberos típico sería, por ejemplo, `joe/admin@ENG.EXAMPLE.COM`. En este ejemplo:

- `joe` es el nombre primario. El nombre primario puede ser un nombre de usuario, como se muestra aquí, o un servicio, como `nfs`. El nombre primario también puede ser la palabra `host`, lo cual significa que el principal es un principal de servicio que está configurado para proporcionar distintos servicios de red, `ftp`, `scp`, `ssh`, etc.
- `admin` es la instancia. La instancia es opcional en el caso de los principales de usuario, pero es necesaria para los principales de servicio. Por ejemplo, si el usuario `joe` a veces actúa como administrador del sistema, puede utilizar `joe/admin` para distinguirse de su identidad de usuario habitual. Del mismo modo, si `joe` tiene cuentas en dos hosts diferentes, puede utilizar dos nombres de principal con instancias diferentes, por ejemplo, `joe/denver.example.com` y `joe/boston.example.com`. Tenga en cuenta que el servicio Kerberos trata `joe` y `joe/admin` como dos principales completamente diferentes.

En el caso de un principal de servicio, la instancia es el nombre de host completo. Un ejemplo de una instancia así es `bigmachine.eng.example.com`. La combinación nombre primario/instancia para este ejemplo podría ser `ftp/bigmachine.eng.example.com` o `host/bigmachine.eng.example.com`.

- `ENG.EXAMPLE.COM` es el dominio de Kerberos. En [“Dominios de Kerberos” en la página 353](#), se analizan los dominios.

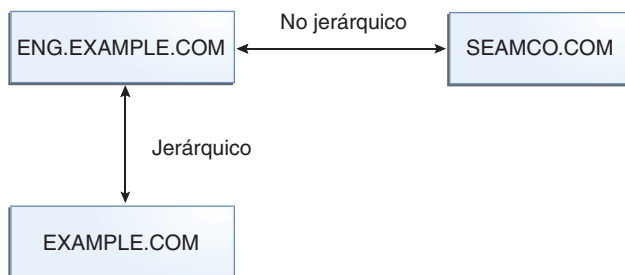
Todos los nombres de principal que aparecen a continuación son válidos:

- `joe`
- `joe/admin`
- `joe/admin@ENG.EXAMPLE.COM`
- `nfs/host.eng.example.com@ENG.EXAMPLE.COM`
- `host/eng.example.com@ENG.EXAMPLE.COM`

## Dominios de Kerberos

Un *dominio* es una red lógica, similar a un dominio, que define un grupo de sistemas con el mismo KDC *principal*. La [Figura 19–3](#) muestra el modo en que los dominios pueden relacionarse entre sí. Algunos dominios son jerárquicos, lo que implica que un dominio es un superconjunto de los otros dominios. De lo contrario, los dominios son no jerárquicos (o “directos”), y la asignación entre los dos dominios debe definirse. Una característica del servicio Kerberos es que permite la autenticación entre dominios. Cada dominio sólo necesita una entrada de principal para el otro dominio en su KDC. Esta función de Kerberos se denomina *autenticación entre dominios*.

FIGURA 19-3 Dominios de Kerberos



## Servidores Kerberos

Cada dominio debe incluir un servidor que mantenga la copia maestra de la base de datos del principal. Este servidor se llama *servidor KDC maestro*. Además, cada dominio debe contener por lo menos un *servidor KDC esclavo*, que contenga las copias duplicadas de la base de datos del principal. Tanto el servidor KDC maestro como el servidor KDC esclavo crean tickets que se utilizan para establecer la autenticación.

El dominio también puede incluir un *servidor de aplicaciones* Kerberos. Este servidor proporciona acceso a los servicios Kerberizados (como ftp, telnet, ssh y NFS). Si tiene instalado SEAM 1.0 o 1.0.1, puede que el dominio incluya un servidor de aplicaciones de red Kerberos, pero este software no viene incluido con estas versiones.

La siguiente figura muestra lo que un dominio hipotético puede llegar a contener.

FIGURA 19-4 Un dominio de Kerberos típico



## Servicios de seguridad de Kerberos

Además de proporcionar autenticación segura a los usuarios, el servicio Kerberos proporciona dos servicios de seguridad:

- **Integridad:** así como la autenticación garantiza que los clientes de una red sean quienes dicen ser, la integridad garantiza que los datos que estos envían sean válidos y que no se hayan alterado durante la transmisión. La integridad se lleva a cabo mediante la comprobación criptográfica de los datos. La integridad también incluye la autenticación de usuario.
- **Privacidad:** la privacidad es un paso más avanzado en torno a la seguridad. La privacidad no incluye solamente la verificación de la integridad de los datos transmitidos, sino que también cifra los datos antes de la transmisión para protegerlos de los intrusos. Además, la privacidad autentica a los usuarios.

Los desarrolladores pueden diseñar sus aplicaciones basadas en RPC para seleccionar un servicio de seguridad con la interfaz de programación RPCSEC\_GSS.

# Componentes de las distintas versiones de Kerberos

En varias de las versiones, se incluyen componentes del servicio Kerberos. Originalmente, el servicio Kerberos y los cambios realizados en el sistema operativo básico para que se admita el servicio Kerberos se lanzaron con el nombre de producto “Sun Enterprise Authentication Mechanism”, que se abrevió como SEAM. A medida que se fueron incluyendo más componentes del producto SEAM en el software de Oracle Solaris, los contenidos de la versión de SEAM fueron disminuyendo. A partir de la versión Oracle Solaris 10, se incluyen todos los componentes del producto SEAM, por lo que el producto SEAM ya no es necesario. El nombre del producto SEAM existe en la documentación por razones históricas.

En la tabla siguiente, se describen los componentes que se incluyen en cada versión. Las versiones de producto se enumeran en orden cronológico. En las secciones siguientes, se describen todos los componentes.

TABLA 19-1    Contenidos de las versiones de Kerberos

| Nombre de la versión                                          | Contenido                                                                 |
|---------------------------------------------------------------|---------------------------------------------------------------------------|
| SEAM 1.0 en Solaris Easy Access Server 3.0                    | Versión completa del servicio Kerberos para las versiones Solaris 2.6 y 7 |
| Servicio Kerberos en la versión Solaris 8                     | Software de cliente Kerberos únicamente                                   |
| SEAM 1.0.1 en Solaris 8 Admin Pack                            | KDC de Kerberos y aplicaciones remotas para la versión Solaris 8          |
| Servicio Kerberos en la versión Solaris 9                     | KDC de Kerberos y software de cliente únicamente                          |
| SEAM 1.0.2                                                    | Aplicaciones remotas de Kerberos para la versión Solaris 9                |
| El servicio Kerberos a partir de la versión Oracle Solaris 10 | Versión completa del servicio Kerberos con mejoras                        |

Para obtener más información sobre las mejoras incluidas en la versión Oracle Solaris 10, consulte [“Kerberos Components” de System Administration Guide: Security Services](#).

## Componentes de Kerberos

De manera similar a la distribución del producto Kerberos V5 del MIT, el servicio Kerberos en la versión de Oracle Solaris incluye lo siguiente:

- Centro de distribución de claves (KDC):
  - Daemon de administración de bases de datos de Kerberos: kadmind.
  - Daemon de procesamiento de tickets de Kerberos: krb5kdc.



- Programas de administración de bases de datos: `kadmin` (maestro solamente), `kadmin.local` y `kdb5_util`.
- Software de propagación de bases de datos: `kprop` (esclavo solamente) y `kpropd`.
- Programas de usuario para gestionar credenciales: `kinit`, `klist` y `kdestroy`.
- Programa de usuario para cambiar la contraseña de Kerberos: `kpasswd`.
- Aplicaciones remotas: `ftp`, `rcp`, `rlogin`, `rsh`, `scp`, `sftp`, `ssh` y `telnet`.
- Daemons de aplicaciones remotas: `ftpd`, `rlogind`, `rshd`, `sshd` y `telnetd`.
- Utilidad de administración `keytab`: `ktutil`.
- Generic Security Service Application Programming Interface (GSS-API): permite que las aplicaciones utilicen varios mecanismos de seguridad sin solicitarle que vuelva a compilar la aplicación cada vez que se agrega un mecanismo nuevo. GSS-API utiliza interfaces estándar que permiten que las aplicaciones puedan emplearse en varios sistemas operativos. GSS-API proporciona aplicaciones que pueden incluir servicios de seguridad de la integridad y la privacidad, y también autenticación. Tanto `ftp` como `ssh` utilizan GSS-API.
- RPCSEC\_GSS Application Programming Interface (API): permite que los servicios NFS usen la autenticación Kerberos. RPCSEC\_GSS es un tipo de seguridad que proporciona servicios de seguridad que son independientes de los mecanismos que se utilizan. RPCSEC\_GSS se sitúa en la parte superior de la capa de GSS-API. Cualquier mecanismo de seguridad basado en GSS-API que sea conectable puede utilizarse mediante las aplicaciones que usan RPCSEC\_GSS.

Además, el servicio Kerberos en la versión de Oracle Solaris incluye lo siguiente:

- Una herramienta basada en la interfaz gráfica de usuario de administración de Kerberos (`gkadmin`): permite administrar los principales y las políticas de los principales. Esta interfaz gráfica de usuario basada en la tecnología Java es una alternativa al comando `kadmin`.
- Módulo de servicio Kerberos V5 para PAM: proporciona la autenticación y la gestión de cuentas, la gestión de sesiones y la gestión de contraseñas para el servicio Kerberos. Este módulo puede utilizarse para hacer que la autenticación Kerberos sea transparente para el usuario.
- Módulos del núcleo: proporcionan implementaciones del servicio Kerberos basadas en el núcleo para que las utilice el servicio NFS a fin de mejorar considerablemente el rendimiento.

## Acerca de Kerberos en esta versión

En esta sección figuran los cambios que están disponibles en la versión Oracle Solaris 11.1.

- El software de Kerberos se ha sincronizado con la versión 1.8 del MIT. Se han incluido las siguientes funciones:
  - Los tipos de cifrado débil `arcfour-hmac-md5-exp`, `des-cbc-md5` y `des-cbc-crc` no se permiten de manera predeterminada. La declaración `allow_weak_crypto = true` en el archivo `/etc/krb5/krb5.conf` se puede agregar para permitir el uso de algoritmos de cifrado más débiles.
  - En el archivo `/etc/krb5/krb5.conf`, la relación `permitted_enctypes` puede tomar una palabra clave opcional `DEFAULT` con `+` o `-` `enctype_family` para agregar o quitar un tipo de cifrado específico del conjunto predeterminado.
  - En la mayoría de los casos, puede eliminar la necesidad de la tabla de asignación `domain_realm` del lado del cliente implementando compatibilidad de referencia mínima en KDC y proporcionando información de asignación a clientes a través de ese protocolo. Los clientes pueden funcionar sin ninguna tabla de asignación `domain_realm` enviando solicitudes para el principal de servicio `name/service/canonical-fqdn@LOCAL.REALM` al KDC local y solicitando referencias. Esta capacidad se puede limitar a nombres de principal de servicio con tipos de nombres específicos o en formas específicas. El KDC sólo pueden utilizar su tabla de asignación `domain_realm`. No se pueden presentar consultas de bloque para DNS.
  - Puede crear alias para entradas principales si utiliza un LDAP secundario para la base de datos de Kerberos. La compatibilidad de alias principal es útil si se puede acceder a un servicio mediante nombres de host diferentes o si DNS no está disponible para poner en forma canónica el nombre de host, lo que significa que se utiliza la forma corta. Puede utilizar un alias para los distintos nombres de principal con los que se conoce un servicio y el sistema sólo necesita un conjunto de claves para el principal de servicio real en su archivo `keytab`.
  - Puede utilizar la utilidad `kvno` para diagnosticar problemas con claves de principal de servicio que se almacenan en `/etc/krb5/krb5.keytab`.
  - El comando `kadmin ktadd` admite la opción `-norandkey` que evita que el comando `kadmin` cree una nueva clave al azar. La opción `-norandkey` puede resultar útil cuando se desea crear una tabla de claves para un principal que tiene una clave derivada de una contraseña. Puede crear una tabla de claves que puede utilizarse para ejecutar el comando `kinit` sin necesidad de especificar una contraseña.
  - Los principales se pueden bloquear después de un determinado número de errores de autenticación previa dentro de un plazo determinado. Consulte [“Cómo configurar el bloqueo de cuenta” en la página 422](#) para obtener más información.

- El indicador OK\_AS\_DELEGATE permite al KDC comunicar la política de dominio local con un cliente respecto de si un servidor intermedio es de confianza para aceptar credenciales delegadas. Consulte [“Confianza de servicios para la delegación” en la página 369](#) para obtener más información.
- El servicio Kerberos se ha actualizado para proporcionarle capacidad a un cliente Solaris, para que realice actualizaciones en un entorno maestro de varios KDC. Consulte [Ejemplo 21–15](#) para obtener más información.
- El daemon ktkk\_warnd se ha mejorado para registrar los elementos principales con las credenciales existentes y para permitir que se envíe correo a los usuarios sin necesidad de tener que especificar cada usuario. Además, el servicio ahora lo puede configurar el usuario. Consulte [“Cómo renovar automáticamente todos los tickets de otorgamiento de tickets \(TGT\)” en la página 423](#) para obtener ejemplos de funcionamiento.



## Planificación del servicio Kerberos

---

Este capítulo debe ser estudiado por los administradores que participan en la instalación y el mantenimiento del servicio Kerberos. En el capítulo se explican diferentes opciones de instalación y configuración que los administradores deben determinar antes de instalar o configurar el servicio.

Esta es una lista de los temas que un administrador del sistema u otros profesionales de asistencia expertos deberían estudiar:

- “¿Por qué planificar implementaciones Kerberos?” en la página 362
- “Planificación de dominios Kerberos” en la página 362
- “Asignación de nombres de host en dominios” en la página 363
- “Nombres de principal de servicio y cliente” en la página 364
- “Puertos para KDC y servicios de administración” en la página 365
- “El número de KDC esclavos” en la página 365
- “Qué sistema de propagación de base de datos se debe utilizar” en la página 367
- “Sincronización de reloj dentro de un dominio” en la página 367
- “Opciones de configuración de cliente” en la página 367
- “Mejora de seguridad de inicio de sesión de cliente” en la página 368
- “Opciones de configuración de KDC” en la página 368
- “Confianza de servicios para la delegación” en la página 369
- “Tipos de cifrado Kerberos” en la página 369
- “URL de ayuda en pantalla en la herramienta gráfica de administración de Kerberos” en la página 370

## ¿Por qué planificar implementaciones Kerberos?

Antes de instalar el servicio Kerberos, debe resolver varios problemas de configuración. Aunque el cambio de configuración después de la instalación inicial es posible, algunos cambios pueden ser difíciles de implementar. Además, algunos cambios necesitan que se reconstruya el KDC, por lo que es mejor considerar objetivos a largo plazo cuando planifique la configuración de Kerberos.

Desplegar una infraestructura Kerberos implica ciertas tareas, como la instalación de KDC, la creación de claves para sus hosts y la migración de usuarios. Reconfigurar una implementación Kerberos puede ser tan complicado como realizar una implementación inicial, por lo tanto, planifique una implementación cuidadosamente para evitar tener que volver a configurarla.

## Planificación de dominios Kerberos

Un *dominio* es una red lógica, que define un grupo de sistemas que están bajo el mismo KDC maestro. Al igual que al establecer un nombre de dominio DNS, cuestiones como el nombre de dominio, el número y el tamaño de cada dominio, y la relación de un dominio con otros para autenticación entre dominios deberían resolverse antes de configurar el servicio Kerberos.

### Nombres de dominio

Los nombres de dominio pueden constar de cualquier cadena ASCII. Normalmente, el nombre de dominio es el mismo que el nombre de dominio DNS, excepto que el nombre de dominio está en mayúscula. Esta convención puede ayudar a diferenciar problemas con el servicio Kerberos de problemas con el espacio de nombres DNS al tiempo que se utiliza un nombre que es familiar. Si no utiliza DNS o decide utilizar una cadena diferente, puede utilizar cualquier cadena. Sin embargo, el proceso de configuración requiere más trabajo. Se aconseja el uso de nombres de dominio que siguen la estructura de nombres de Internet estándar.

### Número de dominios

El número de dominios que su instalación requiere depende de varios factores:

- El número de clientes que se deben admitir. Demasiados clientes en un dominio hacen que la administración sea más difícil y, finalmente, que sea necesario dividir el dominio. Los factores principales que determinan el número de clientes que se pueden admitir son los siguientes:
  - La cantidad de tráfico de Kerberos que cada cliente genera.
  - El ancho de banda de la red física.
  - La velocidad de los hosts.

Debido a que cada instalación tendrá diferentes limitaciones, no existe ninguna regla para determinar el número máximo de clientes.

- Qué tan alejados están los clientes. La configuración de varios dominios pequeños podría tener sentido si los clientes estuvieran en diferentes regiones geográficas.
- El número de hosts disponibles para ser instalados como KDC. Cada dominio debe tener, al menos, dos servidores KDC, un servidor maestro y un servidor esclavo.

Se recomienda la alineación de dominios Kerberos con dominios administrativos. Tenga en cuenta que un dominio Kerberos V puede abarcar varios subdominios del dominio DNS al que corresponde el dominio.

## Jerarquía de dominios

Cuando configura varios dominios para autenticación entre dominios, debe decidir cómo relacionar los dominios. Puede establecer una relación jerárquica entre los dominios, que proporciona rutas automáticas a los dominios relacionados. Por supuesto, todos los dominios en la cadena jerárquica deben estar correctamente configurados. La rutas automáticas pueden facilitar la carga de administración. Sin embargo, si hay muchos niveles de dominios, es posible que no desee utilizar la ruta predeterminada porque requiere demasiadas transacciones.

También puede decidir establecer la relación de confianza directamente. Una relación de confianza directa es más útil cuando existen demasiados niveles entre dos dominios jerárquicos o cuando no existe ninguna relación jerárquica. La conexión debe definirse en el archivo `/etc/krb5/krb5.conf` en todos los hosts que utilicen la conexión. Por lo tanto, se requiere trabajo adicional. La relación de confianza directa también se denomina como una relación transitiva. Para ver una introducción, consulte [“Dominios de Kerberos” en la página 353](#). Para conocer los procedimientos de configuración de varios dominios, consulte [“Configuración de autenticación entre dominios” en la página 393](#).

## Asignación de nombres de host en dominios

La asignación de nombres de host en los nombres de dominio se define en la sección `domain_realm` del archivo `krb5.conf`. Estas asignaciones se pueden definir para todo un dominio y para hosts individuales, según los requisitos.

DNS también se puede utilizar para buscar información sobre los KDC. El uso de DNS hace que sea más fácil cambiar la información porque no será necesario editar el archivo `krb5.conf` en todos los clientes cada vez que se realice un cambio. Consulte la página del comando `man krb5.conf(4)` para obtener más información.

Los clientes de Kerberos de Solaris pueden interoperar mejor con servidores de Active Directory. Los servidores de Active Directory se pueden configurar para proporcionar el dominio para asignación de hosts.

## Nombres de principal de servicio y cliente

Cuando se utiliza el servicio Kerberos, DNS debe estar habilitado en todos los hosts. Con DNS, el principal debe contener el nombre de dominio completo (FQDN) de cada host. Por ejemplo, si el nombre de host es `boston`, el nombre de dominio DNS es `example.com` y el nombre de dominio es `EXAMPLE.COM`, entonces el nombre de principal para el host debe ser `host/boston.example.com@EXAMPLE.COM`. Los ejemplos de este manual requieren que DNS esté configurado y el uso de FQDN para cada host.

El servicio Kerberos pone en forma canónica nombres de alias de host a través de DNS y utiliza la forma canónica (cname) al construir el principal de servicio para el servicio asociado. Por lo tanto al crear un principal de servicio, el componente de nombre de host de nombres de principal de servicio debe ser la forma canónica del nombre de host del sistema donde se aloja el servicio.

A continuación, se muestra un ejemplo de cómo el servicio Kerberos pone en forma canónica el nombre de host. Si un usuario ejecuta el comando `ssh alpha.example.com` donde `alpha.example.com` es un alias de host DNS para el cname `beta.example.com`. Cuando `ssh` llama a Kerberos y solicita un ticket de servicio de host para `alpha.example.com`, el servicio Kerberos aplica el formato canónico a `alpha.example.com` y lo convierte en `beta.example.com`, y solicita un ticket para el principal de servicio `host/beta.example.com` desde el KDC.

Para los nombres de principal que incluyen el FQDN de un host, es importante hacer coincidir la cadena que describe el nombre de dominio DNS en el archivo `/etc/resolv.conf`. El servicio Kerberos requiere que el nombre de dominio DNS esté en letras minúsculas cuando se especifica el FQDN para un principal. El nombre de dominio DNS puede incluir letras mayúsculas y minúsculas, pero sólo utilice letras minúsculas cuando cree un principal de host. Por ejemplo, no importa si el nombre de dominio DNS es `example.com`, `Example.COM` o cualquier otra variación. El nombre de principal para el host seguiría siendo `host/boston.example.com@EXAMPLE.COM`.

Además, la utilidad de gestión de servicios se ha configurado de modo que muchos de los daemons o comandos no se inicien si el servicio de cliente DNS no está en ejecución. Los daemons `kdb5_util`, `kadmind` y `kpropd`, y el comando `kprop` están configurados para depender del servicio DNS. Para utilizar completamente las funciones disponibles mediante el servicio Kerberos y SMF, debe habilitar el servicio de cliente DNS en todos los hosts.



## Puertos para KDC y servicios de administración

De manera predeterminada, el puerto 88 y el puerto 750 se utilizan para el KDC, y el puerto 749 se utiliza para el daemon de administración KDC. Se pueden utilizar diferentes números de puerto. Sin embargo, si cambia los números de puerto, los archivos `/etc/services` y `/etc/krb5/krb5.conf` se deben cambiar en cada cliente. Además de estos archivos, se debe actualizar el archivo `/etc/krb5/kdc.conf` en cada KDC.

## El número de KDC esclavos

Los KDC esclavos generan credenciales para los clientes al igual que el KDC maestro. Los KDC esclavos proporcionan copia de seguridad si el maestro deja de estar disponible. Cada dominio debe tener al menos un KDC esclavo. Es posible que se requieran KDC esclavos adicionales según estos factores:

- El número de segmentos físicos en el dominio. Normalmente, la red debe configurarse para que cada segmento pueda funcionar, al menos mínimamente, sin el resto del dominio. Para ello, un KDC debe ser accesible desde cada segmento. El KDC en esta instancia puede ser maestro o esclavo.
- El número de clientes en el dominio. Mediante la adición de más servidores KDC, puede reducir la carga en los servidores actuales.

Es posible agregar demasiados KDC esclavos. Recuerde que la base de datos KDC se debe propagar para cada servidor, por lo tanto, cuantos más servidores KDC se instalen, mayor es el tiempo que se tarda en obtener los datos actualizados en el dominio. También, como cada esclavo retiene una copia de la base de datos KDC, una mayor cantidad de esclavos aumenta el riesgo de una infracción de seguridad.

Además, uno o más KDC esclavos pueden configurarse fácilmente para ser intercambiados con el KDC maestro. La ventaja de configurar al menos un KDC esclavo de este modo es que si el KDC maestro falla por cualquier motivo, tendrá un sistema preconfigurado que será fácil de intercambiar como KDC maestro. Para obtener instrucciones sobre cómo configurar un KDC esclavo intercambiable, consulte [“Intercambio de un KDC maestro y un KDC esclavo” en la página 425](#).

## Asignación de credenciales GSS a credenciales UNIX

El servicio Kerberos proporciona una asignación predeterminada de nombres de credenciales GSS a IDs de usuario UNIX (UIDs) para aplicaciones GSS que requieren esta asignación, por ejemplo NFS. Los nombres de credenciales GSS son equivalentes a los nombres de principal de Kerberos cuando se utiliza el servicio Kerberos. El algoritmo de asignación predeterminado es tomar un componente de nombre de principal de Kerberos y utilizar ese componente, que es el nombre principal del principal, para buscar el UID. La búsqueda se produce en el dominio predeterminado o en cualquier dominio permitido mediante el parámetro `auth_to_local_realm` en `/etc/krb5/krb5.conf`. Por ejemplo, el nombre de principal de usuario `bob@EXAMPLE.COM` se asigna al UID del usuario UNIX denominado `bob` con la tabla de contraseña. El nombre de principal de usuario `bob/admin@EXAMPLE.COM` no se puede asignar, porque el nombre de principal incluye un componente de la instancia de `admin`. Si las asignaciones predeterminadas para las credenciales de usuario son suficientes, no es necesario completar la tabla de credenciales GSS. En versiones anteriores, era necesario completar la tabla de credenciales GSS para que el servicio NFS funcionara. Si la asignación predeterminada no es suficiente, por ejemplo, si desea asignar un nombre de principal que contenga un componente de instancia, se deberían utilizar otros métodos. Para más información, consulte:

- [“Cómo crear una tabla de credenciales” en la página 401](#)
- [“Cómo agregar una única entrada a la tabla de credenciales” en la página 401](#)
- [“Cómo proporcionar asignación de credenciales entre dominios” en la página 402](#)
- [“Observación de asignación de credenciales GSS a credenciales UNIX” en la página 469](#)

## Migración de usuario automática a dominio Kerberos

Los usuarios UNIX que no tengan cuentas de usuario válidas en el dominio Kerberos predeterminado se pueden migrar automáticamente mediante la estructura PAM. Específicamente, el módulo `pam_krb5_migrate` se utilizaría en la pila de autenticación del servicio PAM. Los servicios se configurarían de manera que siempre que un usuario, que no tiene un principal de Kerberos, lleve a cabo un inicio de sesión correcto en un sistema utilizando su contraseña, un principal de Kerberos se crearía de manera automática para dicho usuario. La nueva contraseña de principal sería la misma que la contraseña de UNIX. Consulte [“Cómo configurar la migración automática de usuarios en un dominio Kerberos” en la página 420](#) para obtener instrucciones sobre cómo utilizar el módulo `pam_krb5_migrate`.

## Qué sistema de propagación de base de datos se debe utilizar

La base de datos que se almacena en el KDC maestro se debe propagar regularmente a los KDC esclavos. Puede configurar la propagación de la base de datos para que sea gradual. El proceso gradual propaga sólo información actualizada a los KDC esclavos, en lugar de a toda la base de datos. Para obtener más información sobre la propagación de base de datos, consulte [“Administración de la base de datos de Kerberos” en la página 430](#).

Si no utiliza propagación gradual, uno de los primeros problemas que debe resolver es la frecuencia de actualización de los KDC esclavos. La necesidad de contar con información actualizada disponible para todos los clientes se debe considerar con la cantidad de tiempo que se tarda en completar la actualización.

En las instalaciones de gran tamaño con muchos KDC en un dominio, uno o más esclavos pueden propagar los datos de forma que el proceso se realice en paralelo. Esta estrategia reduce la cantidad de tiempo que tarda la actualización, pero también aumenta el nivel de complejidad de administración del dominio. Para obtener una descripción completa de esta estrategia, consulte [“Configuración de propagación en paralelo” en la página 442](#).

## Sincronización de reloj dentro de un dominio

Todos los hosts que participan en el sistema de autenticación de Kerberos deben tener sus relojes internos sincronizados dentro un máximo de tiempo especificado. Conocida como *sesgo de reloj*, esta función proporciona otra comprobación de seguridad de Kerberos. Si el sesgo de reloj se excede entre cualquiera de los hosts participantes, las solicitudes se rechazan.

Una manera de sincronizar todos los relojes es utilizar el software de protocolo de hora de red (NTP). Consulte [“Sincronización de relojes entre clientes Kerberos y KDC” en la página 424](#) para obtener más información. Otras maneras de sincronizar los relojes están disponibles, por lo tanto, el uso de NTP no es necesario. Sin embargo, alguna forma de sincronización se debe utilizar para evitar errores de acceso debido al sesgo de reloj.

## Opciones de configuración de cliente

La utilidad de configuración `kclient` se puede ejecutar en el modo interactivo o no interactivo. En el modo interactivo, se le solicita al usuario valores de parámetros específicos de Kerberos, que permiten al usuario realizar cambios en la instalación existente al configurar el cliente. En el modo no interactivo, se utiliza un archivo con valores de parámetros previamente configurados. Además, las opciones de línea de comandos se pueden utilizar en el modo no interactivo. Ambos modos necesitan menos pasos que el proceso manual, lo que debería hacer que el proceso sea más rápido y menos proclive a errores.

Se han realizado cambios para permitir un cliente Kerberos de configuración cero. Si estas reglas se siguen en el entorno, entonces no es necesario un procedimiento de configuración explícito para un cliente Solaris Kerberos:

- DNS está configurado para devolver registros SRV para los KDC.
- El nombre de dominio coincide con el nombre de dominio DNS o KDC admite referencias.
- El cliente Kerberos no necesita un archivo `keytab`.

En algunos casos, puede que sea mejor configurar explícitamente el cliente Kerberos:

- Si las referencias no se utilizan, la lógica de configuración cero depende del nombre de dominio DNS del host para determinar el dominio. Esto presenta un pequeño riesgo de seguridad, pero el riesgo es mucho menor que si se activa `dns_lookup_realm`.
- El módulo `pam_krb5` se basa en una entrada de clave de host en la `keytab`. Es posible que este requisito esté deshabilitado en el archivo `krb5.conf`, sin embargo no se recomienda por razones de seguridad. Consulte la página del comando `man krb5.conf(4)`.
- El proceso de configuración cero es menos eficaz que la configuración directa y tiene una mayor dependencia de DNS. El proceso realiza más búsquedas de DNS que un cliente configurado directamente.

Consulte “[Configuración de clientes Kerberos](#)” en la [página 405](#) para obtener una descripción de todos los procesos de configuración de cliente.

## Mejora de seguridad de inicio de sesión de cliente

En el inicio de sesión, un cliente, mediante el módulo `pam_krb5`, verifica que el KDC que emitió los últimos TGT sea el mismo KDC que emitió el principal de host de cliente que se almacena en `/etc/krb5/krb5.keytab`. El módulo `pam_krb5` verifica el KDC cuando el módulo está configurado en la pila de autenticación. Para algunas configuraciones, como los clientes DHCP que no almacenan un principal de host de cliente, esta verificación se debe deshabilitar. Para desactivar esta verificación, debe definir la opción `verify_ap_req_nofail` en el archivo `krb5.conf` como falsa. Consulte “[Cómo desactivar la verificación del ticket de otorgamiento de tickets](#)” en la [página 418](#) para obtener más información.

## Opciones de configuración de KDC

Hay varias maneras de configurar un KDC. Las maneras más sencillas utilizan la utilidad `kdcmgr` para configurar el KDC automáticamente o interactivamente. La versión automática requiere que utilice las opciones de línea de comandos para definir los parámetros de configuración. Este método es especialmente útil para las secuencias de comandos. La versión interactiva le solicita toda la información que se necesita. Consulte la [Tabla 21–1](#) para obtener referencias a instrucciones para el uso de este comando.

También está disponible la compatibilidad para utilizar LDAP para gestionar los archivos de base de datos para Kerberos. Consulte [“Cómo configurar un KDC para utilizar un servidor de datos LDAP” en la página 380](#) para obtener instrucciones. El uso de LDAP simplifica la administración de sitios que requieren mejor coordinación entre las bases de datos Kerberos y la configuración de servidor de directorios existente.

## Confianza de servicios para la delegación

Para algunas aplicaciones, es posible que un cliente necesite delegar autoridad a un servidor para que actúe en su nombre para ponerse en contacto con otros servicios. El cliente debe reenviar las credenciales a un servidor intermedio. La capacidad del cliente de obtener un ticket de servicio para un servidor no transmite ninguna información al cliente sobre si se debería confiar en el servidor para aceptar credenciales delegadas. La opción `ok_to_auth_as_delegate` para el comando `kadmin` proporciona una manera de que un KDC comunique la política de dominio local a un cliente con respecto a si un servidor intermedio es de confianza para aceptar dichas credenciales.

La copia de indicadores de tickets de credenciales en la parte cifrada de la respuesta de KDC puede tener la opción `ok_to_auth_as_delegate` establecida para indicar al cliente que la política del dominio ha determinado que el servidor especificado en el ticket es un destinatario de delegación adecuado. Un cliente puede utilizar la presencia de esta información para determinar si delegar credenciales (concediendo un proxy o TGT reenviado) a este servidor. Al definir esta opción, un administrador debe considerar la seguridad y ubicación del servidor en que se ejecuta el servicio, así como si el servicio requiere el uso de credenciales delegadas.

## Tipos de cifrado Kerberos

Un *tipo de cifrado* es un identificador que especifica el algoritmo de cifrado, el modo de cifrado y los algoritmos hash que se usan en el servicio Kerberos. Las claves en el servicio Kerberos tienen un tipo de cifrado asociado para identificar el algoritmo criptográfico y el modo que se utilizará cuando el servicio realice operaciones criptográficas con la clave. Aquí se muestran los tipos de cifrado admitidos:

- `des-cbc-md5`
- `des-cbc-crc`
- `des3-cbc-sha1-kd`
- `arcfour-hmac-md5`
- `arcfour-hmac-md5-exp`
- `aes128-cts-hmac-sha1-96`
- `aes256-cts-hmac-sha1-96`

---

**Nota** – En las versiones anteriores a la versión Solaris 10 8/07, el tipo de cifrado `aes256-cts-hmac-sha1-96` se puede utilizar con el servicio Kerberos si los paquetes de criptografía resistente que están desempaquetados se encuentran instalados.

---

Si desea cambiar el tipo de cifrado, debería hacerlo al crear una nueva base de datos de principal. Debido a la interacción entre el KDC, el servidor y el cliente, es difícil cambiar el tipo de cifrado en la base de datos existente. Deje estos parámetros sin configurar a menos que vuelva a crear la base de datos. Consulte “[Uso de los tipos de cifrado de Kerberos](#)” en la [página 541](#) para obtener más información.

---

**Nota** – Si tiene instalado un KDC maestro que no ejecuta la versión Solaris 10, los KDC esclavos deben actualizarse a la versión Solaris 10 antes de actualizar el KDC maestro. Un KDC maestro de Solaris 10 utilizará los nuevos tipos de cifrado, que un esclavo anterior no podrá manejar.

---

De manera predeterminada, los tipos de cifrado débil `arcfour-hmac-md5-exp`, `des-cbc-md5` y `des-cbc-crc` no se permiten en la versión Oracle Solaris 11. Si necesita seguir utilizando estos tipos de cifrado, en especial para telnet, establezca `allow_weak_crypto = true` en la sección `libdefaults` del archivo `/etc/krb5/krb5.conf`.

## URL de ayuda en pantalla en la herramienta gráfica de administración de Kerberos

La URL de ayuda en pantalla es utilizada por la herramienta gráfica de administración de Kerberos, `gkadmin`, por lo que la URL debe estar definida correctamente para activar el menú “Contenidos de ayuda” para trabajar. La versión HTML de este manual se puede instalar en cualquier servidor adecuado. También puede decidir si desea utilizar las colecciones en <http://www.oracle.com/technetwork/indexes/documentation/index.html>.

La URL se especifica en el archivo `krb5.conf` al configurar un host para utilizar el servicio Kerberos. La URL debe señalar la sección titulada “[Herramienta SEAM](#)” en la [página 472](#) en el capítulo *Administración de principales y políticas de Kerberos (tareas)* de este manual. Se puede seleccionar otra página HTML, si otra ubicación es más adecuada.

## Configuración del servicio Kerberos (tareas)

---

En este capítulo, se proporcionan procedimientos de configuración para servidores KDC, servidores de aplicaciones de red, servidores NFS y clientes Kerberos. Muchos de esos procedimientos necesitan acceso de superusuario, por lo que deben ser utilizados por administradores del sistema o usuarios avanzados. También se incluyen procedimientos de configuración entre dominios y otros temas relacionados con servidores KDC.

Se tratan los temas siguientes.

- “Configuración del servicio Kerberos (mapa de tareas)” en la página 371
- “Configuración de servidores KDC” en la página 373
- “Configuración de clientes Kerberos” en la página 405
- “Configuración de autenticación entre dominios” en la página 393
- “Configuración de servidores de aplicaciones de red de Kerberos” en la página 395
- “Configuración de servidores NFS con Kerberos” en la página 398
- “Sincronización de relojes entre clientes Kerberos y KDC” en la página 424
- “Intercambio de un KDC maestro y un KDC esclavo” en la página 425
- “Administración de la base de datos de Kerberos” en la página 430
- “Aumento de la seguridad en servidores Kerberos” en la página 448

## Configuración del servicio Kerberos (mapa de tareas)

Las partes del proceso de configuración dependen de otras partes y deben realizarse en un orden específico. Estos procedimientos, a menudo, establecen servicios que son necesarios para utilizar el servicio Kerberos. Otros procedimientos no dependen de ningún orden y pueden realizarse cuando corresponde. El siguiente mapa de tareas muestra un orden sugerido para una instalación de Kerberos.

| Tarea                                                       | Descripción                                                                                                                                                                                                                             | Para obtener instrucciones                                                                 |
|-------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------|
| 1. Planificar la instalación de Kerberos                    | Permite resolver problemas de configuración antes de iniciar el proceso de configuración de software. La planificación anticipada permite ahorrar tiempo y otros recursos a la larga.                                                   | <a href="#">Capítulo 20, “Planificación del servicio Kerberos”</a>                         |
| 2. Instalar el NTP (opcional)                               | Configura el software de protocolo de hora de red (NTP) u otro protocolo de sincronización de relojes. Para que el servicio Kerberos funcione correctamente, los relojes de todos los sistemas en el dominio deben estar sincronizados. | <a href="#">“Sincronización de relojes entre clientes Kerberos y KDC” en la página 424</a> |
| 3. Configurar los servidores KDC                            | Configura y genera los servidores KDC maestros y los servidores KDC esclavos, y la base de datos KDC de un dominio.                                                                                                                     | <a href="#">“Configuración de servidores KDC” en la página 373</a>                         |
| 4. Aumentar la seguridad en los servidores KDC (opcional)   | Evita infracciones de seguridad en los servidores KDC.                                                                                                                                                                                  | <a href="#">“Cómo restringir el acceso a servidores KDC” en la página 449</a>              |
| 5. Configurar los servidores KDC intercambiables (opcional) | Facilita la tarea de intercambio del servidor KDC maestro y un servidor KDC esclavo.                                                                                                                                                    | <a href="#">“Cómo configurar un KDC esclavo intercambiable” en la página 425</a>           |

# Configuración de servicios Kerberos adicionales (mapa de tareas)

Una vez que se hayan completado los pasos necesarios, se podrán utilizar los procedimientos siguientes, cuando corresponda.

| Tarea                                              | Descripción                                                                                             | Para obtener instrucciones                                                                        |
|----------------------------------------------------|---------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------|
| Configurar la autenticación entre dominios         | Permite comunicaciones de un dominio a otro dominio.                                                    | <a href="#">“Configuración de autenticación entre dominios” en la página 393</a>                  |
| Configurar los servidores de aplicaciones Kerberos | Permite que un servidor admita servicios, como ftp, telnet y rsh, utilizando la autenticación Kerberos. | <a href="#">“Configuración de servidores de aplicaciones de red de Kerberos” en la página 395</a> |
| Configurar los clientes Kerberos                   | Permite que un cliente utilice servicios Kerberos.                                                      | <a href="#">“Configuración de clientes Kerberos” en la página 405</a>                             |
| Configurar el servidor NFS con Kerberos            | Permite que un servidor comparta un sistema de archivos que requiere la autenticación Kerberos.         | <a href="#">“Configuración de servidores NFS con Kerberos” en la página 398</a>                   |



## Configuración de servidores KDC

Después de instalar el software Kerberos, debe configurar los servidores KDC. La configuración de un servidor KDC maestro y de, al menos, un servidor KDC esclavo proporciona el servicio que emite credenciales. Estas credenciales son la base para el servicio Kerberos, por lo que los KDC se deben instalar antes de intentar otras tareas.

La diferencia más importante entre un KDC maestro y un KDC esclavo es que sólo el KDC maestro puede manejar solicitudes de administración de bases de datos. Por ejemplo, el cambio de una contraseña o la adición de un nuevo principal se deben realizar en el KDC maestro. Estos cambios, luego, se pueden propagar a los KDC esclavos. Tanto el KDC esclavo como el KDC maestro generan credenciales. Esta función proporciona redundancia en el caso de que el KDC maestro no pueda responder.

**TABLA 21-1** Configuración de servidores KDC (mapa de tareas)

| Tarea                               | Descripción                                                                                                                                                          | Para obtener instrucciones                                                                        |
|-------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------|
| Configurar un KDC maestro.          | Configura y crea el servidor KDC maestro y la base de datos para un dominio mediante un proceso automático, que es bueno para las secuencias de comandos.            | <a href="#">“Cómo configurar automáticamente un KDC maestro” en la página 374</a>                 |
|                                     | Configura y crea el servidor KDC maestro y la base de datos para un dominio mediante un proceso interactivo, que es suficiente para la mayoría de las instalaciones. | <a href="#">“Cómo configurar interactivamente un KDC maestro” en la página 375</a>                |
|                                     | Configura y genera el servidor KDC maestro y la base de datos para un dominio mediante un proceso manual, que se necesita para instalaciones más complejas.          | <a href="#">“Cómo configurar manualmente un KDC maestro” en la página 376</a>                     |
|                                     | Configura y genera el servidor KDC maestro y la base de datos para un dominio mediante un proceso manual y un LDAP para el KDC.                                      | <a href="#">“Cómo configurar un KDC para utilizar un servidor de datos LDAP” en la página 380</a> |
| Configurar un servidor KDC esclavo. | Configura y crea un servidor KDC esclavo para un dominio mediante un proceso automático, que es bueno para las secuencias de comandos.                               | <a href="#">“Cómo configurar automáticamente un KDC esclavo” en la página 386</a>                 |
|                                     | Configura y crea un servidor KDC esclavo para un dominio mediante un proceso interactivo, que es suficiente para la mayoría de las instalaciones.                    | <a href="#">“Cómo configurar interactivamente un KDC esclavo” en la página 387</a>                |
|                                     | Configura y genera un servidor KDC esclavo para un dominio mediante un proceso manual, que se necesita para instalaciones más complejas.                             | <a href="#">“Cómo configurar manualmente un KDC esclavo” en la página 388</a>                     |

TABLA 21–1 Configuración de servidores KDC (mapa de tareas) (Continuación)

| Tarea                                                 | Descripción                                                                               | Para obtener instrucciones                                                                                                  |
|-------------------------------------------------------|-------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------|
| Refrescar las claves de principal en un servidor KDC. | Actualiza la clave de la sesión en un servidor KDC para utilizar nuevos tipos de cifrado. | <a href="#">“Cómo refrescar las claves del servicio de otorgamiento de tickets en un servidor maestro” en la página 392</a> |

## ▼ Cómo configurar automáticamente un KDC maestro

En la versión Oracle Solaris 11, un KDC maestro se puede configurar automáticamente mediante el siguiente procedimiento.

**Antes de empezar** Debe asumir el rol root. Para obtener más información, consulte [“Cómo usar los derechos administrativos que tiene asignados” en la página 164](#).

● **Cree el KDC.**

Ejecute la utilidad `kdcmgr` para crear el KDC. Debe proporcionar la contraseña de clave maestra y la contraseña para el principal administrativo.

```
kdc1# kdcmgr -a kws/admin -r EXAMPLE.COM create master
```

```
Starting server setup
```

```

Setting up /etc/krb5/kdc.conf
```

```
Setting up /etc/krb5/krb5.conf
```

```
Initializing database '/var/krb5/principal' for realm 'EXAMPLE.COM',
master key name 'K/M@EXAMPLE.COM'
```

```
You will be prompted for the database Master Password.
```

```
It is important that you NOT FORGET this password.
```

```
Enter KDC database master key: <Type the password>
```

```
Re-enter KDC database master key to verify: <Type it again>
```

```
Authenticating as principal root/admin@EXAMPLE.COM with password.
```

```
WARNING: no policy specified for kws/admin@EXAMPLE.COM; defaulting to no policy
```

```
Enter password for principal "kws/admin@EXAMPLE.COM": <Type the password>
```

```
Re-enter password for principal "kws/admin@EXAMPLE.COM": <Type it again>
```

```
Principal "kws/admin@EXAMPLE.COM" created.
```

```
Setting up /etc/krb5/kadm5.acl.
```

```

Setup COMPLETE.
```

```
kdc1#
```

## ▼ Cómo configurar interactivamente un KDC maestro

En la versión Oracle Solaris, un KDC maestro se puede configurar interactivamente mediante el siguiente procedimiento.

**Antes de empezar** Debe asumir el rol root. Para obtener más información, consulte [“Cómo usar los derechos administrativos que tiene asignados” en la página 164](#).

### ● Cree el KDC.

Ejecute la utilidad `kdcmgr` para crear el KDC. Necesita proporcionar la contraseña de clave maestra y la contraseña para el principal administrativo.

```
kdc1# kdcmgr create master
```

```
Starting server setup
```

```
Enter the Kerberos realm: EXAMPLE.COM
```

```
Setting up /etc/krb5/kdc.conf
```

```
Setting up /etc/krb5/krb5.conf
```

```
Initializing database '/var/krb5/principal' for realm 'EXAMPLE.COM',
master key name 'K/M@EXAMPLE.COM'
```

```
You will be prompted for the database Master Password.
```

```
It is important that you NOT FORGET this password.
```

```
Enter KDC database master key: <Type the password>
```

```
Re-enter KDC database master key to verify: <Type it again>
```

```
Enter the krb5 administrative principal to be created: kws/admin
```

```
Authenticating as principal root/admin@EXAMPLE.COM with password.
```

```
WARNING: no policy specified for kws/admin@EXAMPLE.COM; defaulting to no policy
```

```
Enter password for principal "kws/admin@EXAMPLE.COM": <Type the password>
```

```
Re-enter password for principal "kws/admin@EXAMPLE.COM": <Type it again>
```

```
Principal "kws/admin@EXAMPLE.COM" created.
```

```
Setting up /etc/krb5/kadm5.acl.
```

```

Setup COMPLETE.
```

```
kdc1#
```

### Ejemplo 21–1 Visualización del estado de un servidor KDC

El comando `kdcmgr estado` se puede utilizar para mostrar información sobre un servidor KDC maestro o esclavo.

## ▼ Cómo configurar manualmente un KDC maestro

En este procedimiento, se configura la propagación incremental. Además, se utilizan los siguientes parámetros de configuración:

- Nombre de dominio = `EXAMPLE.COM`
- Nombre de dominio DNS = `example.com`
- KDC maestro = `kdc1.example.com`
- Principal admin = `kws/admin`
- URL de ayuda en pantalla =  
`http://docs.oracle.com/cd/E23824_01/html/821-1456/aadmin-23.html`

---

**Nota** – Ajuste la dirección URL para que establezca un enlace a la sección, como se describe en [“URL de ayuda en pantalla en la herramienta gráfica de administración de Kerberos” en la página 370](#).

---

### Antes de empezar

Este procedimiento requiere que el host esté configurado para usar DNS. Para obtener instrucciones específicas de nomenclatura si este maestro se va a intercambiar, consulte [“Intercambio de un KDC maestro y un KDC esclavo” en la página 425](#).

Debe asumir el rol root. Para obtener más información, consulte [“Cómo usar los derechos administrativos que tiene asignados” en la página 164](#).

### 1 Edite el archivo de configuración de Kerberos (`krb5.conf`).

Necesita cambiar los nombres de dominio y los nombres de los servidores. Consulte la página del comando `man krb5.conf(4)` para obtener una descripción completa de este archivo.

```
kdc1 # cat /etc/krb5/krb5.conf
[libdefaults]
 default_realm = EXAMPLE.COM

[realms]
 EXAMPLE.COM = {
 kdc = kdc1.example.com
 admin_server = kdc1.example.com
 }

[domain_realm]
 .example.com = EXAMPLE.COM

#
if the domain name and realm name are equivalent,
this entry is not needed
#
[logging]
 default = FILE:/var/krb5/kdc.log
 kdc = FILE:/var/krb5/kdc.log

[appdefaults]
```

```
gkadmin = {
 help_url = http://docs.oracle.com/cd/E23824_01/html/821-1456/aadmin-23.html
}
```

En este ejemplo, se modificaron las líneas para las entradas `default_realm`, `kdc`, `admin_server` y `domain_realm`. Además, se editó la línea que define `help_url`.

---

**Nota** – Si desea restringir los tipos de cifrado, puede definir las líneas `default_tkt_enctypes` o `default_tgs_enctypes`. Consulte [“Uso de los tipos de cifrado de Kerberos” en la página 541](#) para obtener una descripción de los problemas relacionados con la restricción de los tipos de cifrado.

---

## 2 Edite el archivo de configuración de KDC (`kdc.conf`).

Necesita cambiar el nombre de dominio. Consulte la página del comando `man kdc.conf(4)` para obtener una descripción completa de este archivo.

```
kdc1 # cat /etc/krb5/kdc.conf
[kdcdefaults]
 kdc_ports = 88,750

[realms]
 EXAMPLE.COM = {
 profile = /etc/krb5/krb5.conf
 database_name = /var/krb5/principal
 acl_file = /etc/krb5/kadm5.acl
 kadmind_port = 749
 max_life = 8h 0m 0s
 max_renewable_life = 7d 0h 0m 0s
 sunw_dbprop_enable = true
 sunw_dbprop_master_ulogsize = 1000
 }
```

En este ejemplo, se modificó la definición del nombre de dominio en la sección `realms`. Además, en la sección `realms`, se agregaron líneas para permitir la propagación incremental y para seleccionar el número de actualizaciones que el KDC maestro mantiene en el registro.

---

**Nota** – Si desea restringir los tipos de cifrado, puede definir las líneas `permitted_enctypes`, `supported_enctypes` o `master_key_type`. Consulte [“Uso de los tipos de cifrado de Kerberos” en la página 541](#) para obtener una descripción de los problemas relacionados con la restricción de los tipos de cifrado.

---

## 3 Cree la base de datos KDC mediante el comando `kdb5_util`.

El comando `kdb5_util` crea la base de datos KDC. Además, cuando se utiliza con la opción `-s`, este comando crea un archivo intermedio que se utiliza para autenticar el KDC para él mismo antes de que los daemons `kadmind` y `krb5kdc` se inicien.

```
kdc1 # /usr/sbin/kdb5_util create -s
Initializing database '/var/krb5/principal' for realm 'EXAMPLE.COM'
master key name 'K/M@EXAMPLE.COM'
You will be prompted for the database Master Password.
```

```
It is important that you NOT FORGET this password.
Enter KDC database master key: <Type the key>
Re-enter KDC database master key to verify: <Type it again>
```

#### 4 Edite el archivo de la lista de control de acceso de Kerberos (kadm5 . acl).

Una vez que se rellena, el archivo /etc/krb5/kadm5 . acl debe contener todos los nombres de principales que tienen permitido administrar el KDC.

```
kws/admin@EXAMPLE.COM *
```

La entrada da al principal kws/admin en el dominio EXAMPLE . COM la capacidad de modificar los principales o las políticas en el KDC. La instalación predeterminada incluye un asterisco (\*) para que concuerde con todos los principales admin. Este valor predeterminado puede ser un riesgo de seguridad, por lo que es más seguro incluir una lista de todos los principales admin. Consulte la página del comando man [kadm5 . acl\(4\)](#) para obtener más información.

#### 5 Agregue principales de administración a la base de datos.

Puede agregar tantos principales admin como necesite. Debe agregar, al menos, un principal admin para completar el proceso de configuración del KDC. Para este ejemplo, se agrega un principal kws/admin. Puede sustituir un nombre de principal adecuado en lugar de “kws”.

```
kadmin.local: addprinc kws/admin
Enter password for principal kws/admin@EXAMPLE.COM: <Type the password>
Re-enter password for principal kws/admin@EXAMPLE.COM: <Type it again>
Principal "kws/admin@EXAMPLE.COM" created.
kadmin.local:
```

#### 6 Inicie los daemons Kerberos.

```
kdc1 # svcadm enable -r network/security/krb5kdc
kdc1 # svcadm enable -r network/security/kadmin
```

#### 7 Inicie kadmin y agregue más principales.

En este punto, puede agregar principales con la herramienta gráfica de administración de Kerberos. Para ello, debe iniciar sesión con uno de los nombres de principales admin creados anteriormente en este procedimiento. Sin embargo, el siguiente ejemplo de línea de comandos se muestra para que resulte más sencillo.

```
kdc1 # /usr/sbin/kadmin -p kws/admin
Enter password: <Type kws/admin password>
kadmin:
```

##### a. Cree el principal host del KDC maestro.

El principal host es utilizado por aplicaciones Kerberizadas, como kprop, para propagar los cambios a los KDC esclavos. Este principal también se utiliza para proporcionar acceso remoto seguro al servidor KDC mediante aplicaciones, como ssh. Tenga en cuenta que

cuando la instancia de principal es un nombre de host, el FQDN se debe especificar en letras minúsculas, independientemente de si el nombre de dominio está en mayúsculas o minúsculas en el servicio de nombres.

```
kadmin: addprinc -randkey host/kdc1.example.com
Principal "host/kdc1.example.com@EXAMPLE.COM" created.
kadmin:
```

#### b. (Opcional) Cree el principal `clnt`.

Este principal es utilizado por la utilidad `clnt` durante la instalación de un cliente Kerberos. Si no planea utilizar esta utilidad, no tiene que agregar el principal. Los usuarios de la utilidad `clnt` necesitan usar esta contraseña.

```
kadmin: addprinc clntconfig/admin
Enter password for principal clntconfig/admin@EXAMPLE.COM: <Type the password>
Re-enter password for principal clntconfig/admin@EXAMPLE.COM: <Type it again>
Principal "clntconfig/admin@EXAMPLE.COM" created.
kadmin:
```

#### c. Agregue el principal `host` del KDC maestro al archivo `keytab` del KDC maestro.

La adición del principal `host` al archivo `keytab` permite que este principal sea utilizado por servidores de aplicaciones, como `sshd`, automáticamente.

```
kadmin: ktadd host/kdc1.example.com
Entry for principal host/kdc1.example.com with kvno 3, encryption type AES-256 CTS mode
with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal host/kdc1.example.com with kvno 3, encryption type AES-128 CTS mode
with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal host/kdc1.example.com with kvno 3, encryption type Triple DES cbc
mode with HMAC/sha1 added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal host/kdc1.example.com with kvno 3, encryption type ArcFour
with HMAC/md5 added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal host/kdc1.example.com with kvno 3, encryption type DES cbc mode
with RSA-MD5 added to keytab WRFILE:/etc/krb5/krb5.keytab.
kadmin:
```

#### d. Salga de `kadmin`.

```
kadmin: quit
```

### 8 (Opcional) Sincronice el reloj de los KDC maestros mediante NTP u otro mecanismo de sincronización de relojes.

No es necesario instalar ni utilizar el protocolo de hora de red (NTP). Sin embargo, cada reloj debe estar dentro de la hora predeterminada que está definida en la sección `libdefaults` del archivo `krb5.conf` para que la autenticación se realice con éxito. Consulte [“Sincronización de relojes entre clientes Kerberos y KDC” en la página 424](#) para obtener información sobre el NTP.

### 9 Configure los KDC esclavos.

Para proporcionar redundancia, asegúrese de instalar, al menos, un KDC esclavo. Consulte [“Cómo configurar manualmente un KDC esclavo” en la página 388](#) para obtener instrucciones específicas.

## ▼ Cómo configurar un KDC para utilizar un servidor de datos LDAP

Utilice el siguiente procedimiento para configurar un KDC para utilizar un servidor de datos LDAP.

En este procedimiento, se utilizan los siguientes parámetros de configuración:

- Nombre de dominio = `EXAMPLE.COM`
- Nombre de dominio DNS = `example.com`
- KDC maestro = `kdc1.example.com`
- Servidor de directorios = `dsserver.example.com`
- Principal admin = `kws/admin`
- FMRI para el servicio LDAP =  
`svc:/application/sun/ds:ds--var-opt-SUNWdsee-dsins1`
- URL de ayuda en pantalla =  
`http://docs.oracle.com/cd/E23824_01/html/821-1456/aadmin-23.html`

---

**Nota** – Ajuste la dirección URL para que establezca un enlace a la sección, como se describe en [“URL de ayuda en pantalla en la herramienta gráfica de administración de Kerberos” en la página 370.](#)

---

### Antes de empezar

Este procedimiento también requiere que el host esté configurado para usar DNS. Para obtener un mejor rendimiento, instale el KDC y el servicio de directorios LDAP en el mismo servidor. Además, un servidor de directorios debe estar en ejecución. El siguiente procedimiento funciona con servidores que utilizan la versión Sun Directory Server Enterprise Edition 7.0.

Debe asumir el rol root en el servidor KDC. Para obtener más información, consulte [“Cómo usar los derechos administrativos que tiene asignados” en la página 164.](#)

### 1 Configure el KDC maestro para utilizar SSL para alcanzar el servidor de directorios.

Siga los pasos a continuación para configurar un KDC con el fin de utilizar el certificado autofirmado de Directory Server. Si el certificado ha caducado, siga las instrucciones para renovar un certificado en [“To Manage Self-Signed Certificates”](#).

#### a. En el servidor de directorios, exporte el certificado de servidor de directorios autofirmado.

```
/export/sun-ds6.1/ds6/bin/dsadm show-cert -F der /export/sun-ds6.1/directory2 \
defaultCert > /tmp/defaultCert.cert.der
```

#### b. En el KDC maestro, importe el certificado de servidor de directorios.

```
pktool setpin keystore=nss dir=/var/ldap
chmod a+r /var/ldap/*.db
```



```
pktool import keystore=nss objtype=cert trust="CT" infile=/tmp/defaultCert.certutil.der \
 label=defaultCert dir=/var/ldap
```

**c. En el KDC maestro, compruebe que SSL esté funcionado.**

En este ejemplo se da por sentado que la entrada `cn=directory manager` tiene privilegios de administración.

```
/usr/bin/ldapsearch -Z -P /var/ldap -D "cn=directory manager" \
 -h dsserver.example.com -b "" -s base objectclass='*'
Subject:
 "CN=dsserver.example.com,CN=636,CN=Directory Server,O=Example Corporation
```

Tenga en cuenta que la entrada `CN=dsserver.example.com` debería incluir el nombre de host calificado completo, no una versión corta.

**2 Rellene el directorio LDAP si es necesario.**

**3 Agregue el esquema Kerberos al esquema existente.**

```
ldapmodify -h dsserver.example.com -D "cn=directory manager" -f /usr/share/lib/ldif/kerberos.ldif
```

**4 Cree el contenedor Kerberos en el directorio LDAP.**

Agregue las entradas siguientes al archivo `krb5.conf`.

**a. Defina el tipo de base de datos.**

Agregue una entrada para definir `database_module` para la sección `realms`.

```
database_module = LDAP
```

**b. Defina el módulo de la base de datos.**

```
[dbmodules]
LDAP = {
 ldap_kerberos_container_dn = "cn=krbcontainer,dc=example,dc=com"
 db_library = kldap
 ldap_kdc_dn = "cn=kdc service,ou=profile,dc=example,dc=com"
 ldap_kadmin_dn = "cn=kadmin service,ou=profile,dc=example,dc=com"
 ldap_cert_path = /var/ldap
 ldap_servers = ldaps://dsserver.example.com
}
```

**c. Cree el KDC en el directorio LDAP.**

Este comando crea `krbcontainer` y varios otros objetos. También crea un archivo intermedio de clave maestra `/var/krb5/.k5.EXAMPLE.COM`.

```
kdb5_ldap_util -D "cn=directory manager" create -P abcd1234 -r EXAMPLE.COM -s
```

**5 Guarde las contraseñas del nombre distintivo del vínculo (DN) del KDC.**

Estas contraseñas son utilizadas por el KDC cuando se enlaza al DS. El KDC utiliza diferentes roles según el tipo de acceso que el KDC está utilizando.

```
kdb5_ldap_util stashesrvpw "cn=kdc service,ou=profile,dc=example,dc=com"
kdb5_ldap_util stashesrvpw "cn=kadmin service,ou=profile,dc=example,dc=com"
```

## 6 Agregue roles de servicio KDC.

### a. Cree un archivo `kdc_roles.ldif` con contenido como el siguiente:

```
dn: cn=kdc service,ou=profile,dc=example,dc=com
cn: kdc service
sn: kdc service
objectclass: top
objectclass: person
userpassword: test123

dn: cn=kadmin service,ou=profile,dc=example,dc=com
cn: kadmin service
sn: kadmin service
objectclass: top
objectclass: person
userpassword: test123
```

### b. Cree las entradas de rol en el directorio LDAP.

```
ldapmodify -a -h dsserver.example.com -D "cn=directory manager" -f kdc_roles.ldif
```

## 7 Defina las ACL para los roles relacionados con el KDC.

```
cat << EOF | ldapmodify -h dsserver.example.com -D "cn=directory manager"
Set kadmin ACL for everything under krbcontainer.
dn: cn=krbcontainer,dc=example,dc=com
changetype: modify
add: aci
aci: (target="ldap:///cn=krbcontainer,dc=example,dc=com")(targetattr="krb*")(version 3.0;\
 acl kadmin_ACL; allow (all)\
 userdn = "ldap:///cn=kadmin service,ou=profile,dc=example,dc=com";)

Set kadmin ACL for everything under the people subtree if there are
mix-in entries for krb princs:
dn: ou=people,dc=example,dc=com
changetype: modify
add: aci
aci: (target="ldap:///ou=people,dc=example,dc=com")(targetattr="krb*")(version 3.0;\
 acl kadmin_ACL; allow (all)\
 userdn = "ldap:///cn=kadmin service,ou=profile,dc=example,dc=com";)
EOF
```

## 8 Edite el archivo de configuración de Kerberos (`krb5.conf`).

Necesita cambiar los nombres de dominio y los nombres de los servidores. Consulte la página del comando `man krb5.conf(4)` para obtener una descripción completa de este archivo.

```
kdc1 # cat /etc/krb5/krb5.conf
[libdefaults]
 default_realm = EXAMPLE.COM

[realms]
 EXAMPLE.COM = {
 kdc = kdc1.example.com
 admin_server = kdc1.example.com
 }
```

```
[domain_realm]
 .example.com = EXAMPLE.COM
#
if the domain name and realm name are equivalent,
this entry is not needed
#
[logging]
 default = FILE:/var/krb5/kdc.log
 kdc = FILE:/var/krb5/kdc.log

[appdefaults]
 gkadmin = {
 help_url = http://docs.oracle.com/cd/E23824_01/html/821-1456/aadmin-23.html
 }
```

En este ejemplo, se modificaron las líneas para las entradas `default_realm`, `kdc`, `admin_server` y `domain_realm`. Además, se editó la línea que define `help_url`.

---

**Nota** – Si desea restringir los tipos de cifrado, puede definir las líneas `default_tkt_enctypes` o `default_tgs_enctypes`. Consulte [“Uso de los tipos de cifrado de Kerberos” en la página 541](#) para obtener una descripción de los problemas relacionados con la restricción de los tipos de cifrado.

---

## 9 Edite el archivo de configuración de KDC (`kdc.conf`).

Necesita cambiar el nombre de dominio. Consulte la página del comando `man kdc.conf(4)` para obtener una descripción completa de este archivo.

```
kdc1 # cat /etc/krb5/kdc.conf
[kdcdefaults]
 kdc_ports = 88,750

[realms]
 EXAMPLE.COM = {
 profile = /etc/krb5/krb5.conf
 database_name = /var/krb5/principal
 acl_file = /etc/krb5/kadm5.acl
 kadmind_port = 749
 max_life = 8h 0m 0s
 max_renewable_life = 7d 0h 0m 0s
 sunw_dbprop_enable = true
 sunw_dbprop_master_uologsize = 1000
 }
```

En este ejemplo, se modificó la definición del nombre de dominio en la sección `realms`. Además, en la sección `realms`, se agregaron líneas para permitir la propagación incremental y para seleccionar el número de actualizaciones que el KDC maestro mantiene en el registro.

**Nota** – Si desea restringir los tipos de cifrado, puede definir las líneas `permitted_enctypes`, `supported_enctypes` o `master_key_type`. Consulte [“Uso de los tipos de cifrado de Kerberos” en la página 541](#) para obtener una descripción de los problemas relacionados con la restricción de los tipos de cifrado.

---

## 10 Edite el archivo de la lista de control de acceso de Kerberos (`kadm5.ac1`).

Una vez que se rellena, el archivo `/etc/krb5/kadm5.ac1` debe contener todos los nombres de principales que tienen permitido administrar el KDC.

```
kws/admin@EXAMPLE.COM *
```

La entrada `da` al principal `kws/admin` en el dominio `EXAMPLE.COM` la capacidad de modificar los principales o las políticas en el KDC. La instalación predeterminada incluye un asterisco (\*) para que concuerde con todos los principales `admin`. Este valor predeterminado puede ser un riesgo de seguridad, por lo que es más seguro incluir una lista de todos los principales `admin`. Consulte la página del comando `man kadm5.ac1(4)` para obtener más información.

## 11 Inicie el comando `kadmin.local` y agregue principales.

Los próximos pasos secundarios crean los principales que son utilizados por el servicio Kerberos.

```
kdc1 # /usr/sbin/kadmin.local
kadmin.local:
```

### a. Agregue principales de administración a la base de datos.

Puede agregar tantos principales `admin` como necesite. Debe agregar, al menos, un principal `admin` para completar el proceso de configuración del KDC. Para este ejemplo, se agrega un principal `kws/admin`. Puede sustituir un nombre de principal adecuado en lugar de “`kws`”.

```
kadmin.local: addprinc kws/admin
Enter password for principal kws/admin@EXAMPLE.COM: <Type the password>
Re-enter password for principal kws/admin@EXAMPLE.COM: <Type it again>
Principal "kws/admin@EXAMPLE.COM" created.
kadmin.local:
```

### b. Salga de `kadmin.local`.

Ha agregado todos los principales necesarios para los pasos siguientes.

```
kadmin.local: quit
```

## 12 (Opcional) Configure las dependencias LDAP para servicios Kerberos.

Si los servidores LDAP y KDC se están ejecutando en el mismo host y si el servicio LDAP está configurado con un FMRI de SMF, agregue una dependencia al servicio LDAP para los daemons Kerberos. Esta dependencia reiniciará el servicio KDC si el servicio LDAP se reinicia.

### a. Agregue la dependencia al servicio krb5kdc.

```
svccfg -s security/krb5kdc
svc:/network/security/krb5kdc> addpg dsins1 dependency
svc:/network/security/krb5kdc> setprop dsins1/entities = \
 fmri: "svc:/application/sun/ds:ds--var-opt-SUNWdsee-dsins1"
svc:/network/security/krb5kdc> setprop dsins1/grouping = astring: "require_all"
svc:/network/security/krb5kdc> setprop dsins1/restart_on = astring: "restart"
svc:/network/security/krb5kdc> setprop dsins1/type = astring: "service"
svc:/network/security/krb5kdc> exit
```

### b. Agregue la dependencia al servicio kadmind.

```
svccfg -s security/kadmind
svc:/network/security/kadmind> addpg dsins1 dependency
svc:/network/security/kadmind> setprop dsins1/entities = \
 fmri: "svc:/application/sun/ds:ds--var-opt-SUNWdsee-dsins1"
svc:/network/security/kadmind> setprop dsins1/grouping = astring: "require_all"
svc:/network/security/kadmind> setprop dsins1/restart_on = astring: "restart"
svc:/network/security/kadmind> setprop dsins1/type = astring: "service"
svc:/network/security/kadmind> exit
```

## 13 Inicie los daemons Kerberos.

```
kdc1 # svcadm enable -r network/security/krb5kdc
kdc1 # svcadm enable -r network/security/kadmind
```

## 14 Inicie kadmind y agregue más principales.

En este punto, puede agregar principales con la herramienta de interfaz gráfica de usuario de administración de Kerberos. Para ello, debe iniciar sesión con uno de los nombres de principales admin creados anteriormente en este procedimiento. Sin embargo, el siguiente ejemplo de línea de comandos se muestra para que resulte más sencillo.

```
kdc1 # /usr/sbin/kadmind -p kws/admin
Enter password: <Type kws/admin password>
kadmind:
```

### a. Cree el principal host del KDC maestro.

El principal host es utilizado por aplicaciones Kerberizadas, como klist y kprop. Los clientes utilizan este principal cuando montan un sistema de archivos NFS autenticado. Tenga en cuenta que cuando la instancia de principal es un nombre de host, el FQDN se debe especificar en letras minúsculas, independientemente de si el nombre de dominio está en mayúsculas o minúsculas en el servicio de nombres.

```
kadmind: addprinc -randkey host/kdc1.example.com
Principal "host/kdc1.example.com@EXAMPLE.COM" created.
kadmind:
```

**b. (Opcional) Cree el principal `kcLient`.**

Este principal es utilizado por la utilidad `kcLient` durante la instalación de un cliente Kerberos. Si no planea utilizar esta utilidad, no tiene que agregar el principal. Los usuarios de la utilidad `kcLient` necesitan usar esta contraseña.

```
kadmin: addprinc clntconfig/admin
Enter password for principal clntconfig/admin@EXAMPLE.COM: <Type the password>
Re-enter password for principal clntconfig/admin@EXAMPLE.COM: <Type it again>
Principal "clntconfig/admin@EXAMPLE.COM" created.
kadmin:
```

**c. Agregue el principal `host` del KDC maestro al archivo `keytab` del KDC maestro.**

La agregación del principal `host` al archivo `keytab` permite que este principal se utilice automáticamente.

```
kadmin: ktadd host/kdc1.example.com
Entry for principal host/kdc1.example.com with kvno 3, encryption type AES-256 CTS mode
with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal host/kdc1.example.com with kvno 3, encryption type AES-128 CTS mode
with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal host/kdc1.example.com with kvno 3, encryption type Triple DES cbc
mode with HMAC/sha1 added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal host/kdc1.example.com with kvno 3, encryption type ArcFour
with HMAC/md5 added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal host/kdc1.example.com with kvno 3, encryption type DES cbc mode
with RSA-MD5 added to keytab WRFILE:/etc/krb5/krb5.keytab.
kadmin:
```

**d. Salga de `kadmin`.**

```
kadmin: quit
```

**15 (Opcional) Sincronice el reloj de los KDC maestros mediante NTP u otro mecanismo de sincronización de relojes.**

No es necesario instalar ni utilizar el protocolo de hora de red (NTP). Sin embargo, cada reloj debe estar dentro de la hora predeterminada que está definida en la sección `libdefaults` del archivo `krb5.conf` para que la autenticación se realice con éxito. Consulte [“Sincronización de relojes entre clientes Kerberos y KDC” en la página 424](#) para obtener información sobre el NTP.

**16 Configure los KDC esclavos.**

Para proporcionar redundancia, asegúrese de instalar, al menos, un KDC esclavo. Consulte [“Cómo configurar manualmente un KDC esclavo” en la página 388](#) para obtener instrucciones específicas.

**▼ Cómo configurar automáticamente un KDC esclavo**

En la versión Oracle Solaris, un KDC esclavo se puede configurar automáticamente mediante el siguiente procedimiento.

**Antes de empezar** Debe asumir el rol root. Para obtener más información, consulte [“Cómo usar los derechos administrativos que tiene asignados” en la página 164.](#)

- **Cree el KDC.**

Ejecute la utilidad `kdcmgr` para crear el KDC. Debe proporcionar la contraseña de clave maestra y la contraseña para el principal administrativo.

```
kdc2# kdcmgr -a kws/admin -r EXAMPLE.COM create -m kdc1 slave
```

```
Starting server setup
```

```

```

```
Setting up /etc/krb5/kdc.conf
```

```
Setting up /etc/krb5/krb5.conf
```

```
Obtaining TGT for kws/admin ...
```

```
Password for kws/admin@EXAMPLE.COM: <Type the password>
```

```
Setting up /etc/krb5/kadm5.acl.
```

```
Setting up /etc/krb5/kpropd.acl.
```

```
Waiting for database from master...
```

```
Waiting for database from master...
```

```
Waiting for database from master...
```

```
kdb5_util: Cannot find/read stored master key while reading master key
```

```
kdb5_util: Warning: proceeding without master key
```

```
Enter KDC database master key: <Type the password>
```

```

```

```
Setup COMPLETE.
```

```
kdc2#
```

## ▼ **Cómo configurar interactivamente un KDC esclavo**

Utilice el siguiente procedimiento para configurar interactivamente un KDC esclavo.

**Antes de empezar** Debe asumir el rol root. Para obtener más información, consulte [“Cómo usar los derechos administrativos que tiene asignados” en la página 164.](#)

- **Cree el KDC.**

Ejecute la utilidad `kdcmgr` para crear el KDC. Debe proporcionar la contraseña de clave maestra y la contraseña para el principal administrativo.

```
kdc1# kdcmgr create slave
```

```
Starting server setup
```

```

Enter the Kerberos realm: EXAMPLE.COM
What is the master KDC's host name?: kdc1

Setting up /etc/krb5/kdc.conf

Setting up /etc/krb5/krb5.conf
Obtaining TGT for kws/admin ...
Password for kws/admin@EXAMPLE.COM: <Type the password>

Setting up /etc/krb5/kadm5.acl.

Setting up /etc/krb5/kpropd.acl.

Waiting for database from master...
Waiting for database from master...
Waiting for database from master...
kdb5_util: Cannot find/read stored master key while reading master key
kdb5_util: Warning: proceeding without master key
Enter KDC database master key: <Type the password>

Setup COMPLETE.

kdc2#
```

## ▼ Cómo configurar manualmente un KDC esclavo

En este procedimiento, se configura un nuevo KDC esclavo denominado `kdc2`. Además, se configura la propagación incremental. Este procedimiento utiliza los siguientes parámetros de configuración:

- Nombre de dominio = `EXAMPLE.COM`
- Nombre de dominio DNS = `example.com`
- KDC maestro = `kdc1.example.com`
- KDC esclavo = `kdc2.example.com`
- Principal admin = `kws/admin`

### Antes de empezar

El KDC maestro debe estar configurado. Para obtener instrucciones específicas si este esclavo se va a intercambiar, consulte [“Intercambio de un KDC maestro y un KDC esclavo” en la página 425](#).

Debe asumir el rol root en el servidor KDC. Para obtener más información, consulte [“Cómo usar los derechos administrativos que tiene asignados” en la página 164](#).



**1 En el KDC maestro, inicie kadmin.**

Debe iniciar sesión con uno de los nombres de principales admin que creó cuando configuró el KDC maestro.

```
kdc1 # /usr/sbin/kadmin -p kws/admin
Enter password: <Type kws/admin password>
kadmin:
```

**a. En el KDC maestro, agregue principales host esclavos a la base de datos si aún no lo ha hecho.**

Para que el esclavo funcione, debe tener un principal host. Tenga en cuenta que cuando la instancia de principal es un nombre de host, el FQDN se debe especificar en letras minúsculas, independientemente de si el nombre de dominio está en mayúsculas o minúsculas en el servicio de nombres.

```
kadmin: addprinc -randkey host/kdc2.example.com
Principal "host/kdc2.example.com@EXAMPLE.COM" created.
kadmin:
```

**b. En el KDC maestro, cree el principal kiprop.**

El principal kiprop se utiliza para autorizar la propagación incremental del KDC maestro.

```
kadmin: addprinc -randkey kiprop/kdc2.example.com
Principal "kiprop/kdc2.example.com@EXAMPLE.COM" created.
kadmin:
```

**c. Salga de kadmin.**

```
kadmin: quit
```

**2 En el KDC maestro, edite el archivo de configuración de Kerberos (krb5.conf).**

Debe agregar una entrada para cada esclavo. Consulte la página del comando `man krb5.conf(4)` para obtener una descripción completa de este archivo.

```
kdc1 # cat /etc/krb5/krb5.conf
.
.
[realms]
 EXAMPLE.COM = {
 kdc = kdc1.example.com
 kdc = kdc2.example.com
 admin_server = kdc1.example.com
 }
```

**3 En el KDC maestro, agregue una entrada kiprop a kadm5.acl.**

Esta entrada permite que el KDC maestro reciba solicitudes de propagación incremental para el servidor kdc2.

```
kdc1 # cat /etc/krb5/kadm5.acl
*/admin@EXAMPLE.COM *
kiprop/kdc2.example.com@EXAMPLE.COM p
```

- 4 En el KDC maestro, reinicie kadmind para utilizar las nuevas entradas en el archivo kadm5 . ac l.**

```
kdc1 # svcadm restart network/security/kadmin
```

- 5 En todos los KDC esclavos, copie los archivos de administración KDC del servidor KDC maestro.**

Este paso se debe realizar en todos los KDC esclavos, ya que el servidor KDC maestro ha actualizado información que cada servidor KDC necesita. Puede utilizar ftp o un mecanismo de transferencia similar para capturar copias de los siguientes archivos del KDC maestro:

- /etc/krb5/krb5.conf
- /etc/krb5/kdc.conf

- 6 En todos los KDC esclavos, agregue una entrada para el KDC maestro y cada KDC esclavo en el archivo de configuración de propagación de bases de datos, kpropd . ac l.**

Esta información se debe actualizar en todos los servidores KDC esclavos.

```
kdc2 # cat /etc/krb5/kpropd.ac l
host/kdc1.example.com@EXAMPLE.COM
host/kdc2.example.com@EXAMPLE.COM
```

- 7 En todos los KDC esclavos, asegúrese de que el archivo de la lista de control de acceso de Kerberos, kadm5 . ac l, no esté relleno.**

Un archivo kadm5 . ac l sin modificaciones sería de la siguiente manera:

```
kdc2 # cat /etc/krb5/kadm5.ac l
*/admin@___default_realm___ *
```

Si el archivo tiene entradas kprop, elimínelas.

- 8 En el nuevo esclavo, cambie una entrada en kdc . conf.**

Reemplace la entrada sunw\_dbprop\_master\_ologsize por una entrada que defina sunw\_dbprop\_slave\_poll. La entrada establece el tiempo de sondeo en dos minutos.

```
kdc1 # cat /etc/krb5/kdc.conf
[kdcdefaults]
 kdc_ports = 88,750

[realms]
 EXAMPLE.COM= {
 profile = /etc/krb5/krb5.conf
 database_name = /var/krb5/principal
 acl_file = /etc/krb5/kadm5.ac l
 kadmind_port = 749
 max_life = 8h 0m 0s
 max_renewable_life = 7d 0h 0m 0s
 sunw_dbprop_enable = true
 sunw_dbprop_slave_poll = 2m
 }
```

## 9 En el nuevo esclavo, inicie el comando `kadmin`.

Debe iniciar sesión con uno de los nombres de principales `admin` que creó cuando configuró el KDC maestro.

```
kdc2 # /usr/sbin/kadmin -p kws/admin
Enter password: <Type kws/admin password>
kadmin:
```

### a. Agregue el principal `host` del esclavo al archivo `keytab` del esclavo mediante `kadmin`.

Esta entrada permite que `kprop` y otras aplicaciones Kerberizadas funcionen. Tenga en cuenta que cuando la instancia de principal es un nombre de `host`, el FQDN se debe especificar en letras minúsculas, independientemente de si el nombre de dominio está en mayúsculas o minúsculas en el servicio de nombres.

```
kadmin: ktadd host/kdc2.example.com
Entry for principal host/kdc2.example.com with kvno 3, encryption type AES-256 CTS mode
with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal host/kdc2.example.com with kvno 3, encryption type AES-128 CTS mode
with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal host/kdc2.example.com with kvno 3, encryption type Triple DES cbc
mode with HMAC/sha1 added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal host/kdc2.example.com with kvno 3, encryption type ArcFour
with HMAC/md5 added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal host/kdc2.example.com with kvno 3, encryption type DES cbc mode
with RSA-MD5 added to keytab WRFILE:/etc/krb5/krb5.keytab.
kadmin:
```

### b. Agregue el principal `kiprop` al archivo `keytab` del KDC esclavo.

La adición del principal `kiprop` al archivo `krb5.keytab` permite que el comando `kpropd` se autentique cuando se inicia la propagación incremental.

```
kadmin: ktadd kiprop/kdc2.example.com
Entry for principal kiprop/kdc2.example.com with kvno 3, encryption type AES-256 CTS mode
with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal kiprop/kdc2.example.com with kvno 3, encryption type AES-128 CTS mode
with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal kiprop/kdc2.example.com with kvno 3, encryption type Triple DES cbc
mode with HMAC/sha1 added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal kiprop/kdc2.example.com with kvno 3, encryption type ArcFour
with HMAC/md5 added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal kiprop/kdc2.example.com with kvno 3, encryption type DES cbc mode
with RSA-MD5 added to keytab WRFILE:/etc/krb5/krb5.keytab.
kadmin:
```

### c. Salga de `kadmin`.

```
kadmin: quit
```

## 10 En el nuevo esclavo, inicie el daemon de propagación de Kerberos.

```
kdc2 # svcadm enable network/security/krb5_prop
```

## 11 En el nuevo esclavo, cree un archivo intermedio con `kdb5_util`.

```
kdc2 # /usr/sbin/kdb5_util stash
kdb5_util: Cannot find/read stored master key while reading master key
```

```
kdb5_util: Warning: proceeding without master key
```

```
Enter KDC database master key: <Type the key>
```

**12 (Opcional) En el nuevo KDC esclavo, sincronice el reloj del KDC maestro mediante NTP u otro mecanismo de sincronización de relojes.**

No es necesario instalar ni utilizar el protocolo de hora de red (NTP). Sin embargo, cada reloj debe estar dentro de la hora predeterminada que está definida en la sección `libdefaults` del archivo `krb5.conf` para que la autenticación se realice con éxito. Consulte [“Sincronización de relojes entre clientes Kerberos y KDC” en la página 424](#) para obtener información sobre el NTP.

**13 En el nuevo esclavo, inicie el daemon del KDC (krb5kdc).**

```
kdc2 # svcadm enable network/security/krb5kdc
```

## ▼ **Cómo refrescar las claves del servicio de otorgamiento de tickets en un servidor maestro**

Cuando el principal de servicio de otorgamiento de tickets (TGS) sólo tiene una clave DES, que es el caso de los servidores KDC creados antes de la versión Solaris 10, la clave restringe el tipo de cifrado de la clave de sesión de otorgamiento de tickets (TGT) a DES. Si un KDC se actualiza a una versión que admite otros tipos de cifrado más seguros, el administrador puede esperar que un cifrado más seguro se utilice para todas las claves de sesión generadas por el KDC. Sin embargo, si al principal TGS existente no se le refrescan las claves para incluir los nuevos tipos de cifrado, la clave de sesión TGT seguirá estando limitada a DES. El siguiente procedimiento refresca la clave para que se puedan utilizar tipos de cifrado adicionales.

- **Actualice la clave del principal del servicio TGS.**

```
kdc1 % /usr/sbin/kadmin -p kws/admin
Enter password: <Type kws/admin password>
kadmin: cpw -randkey krbtgt/EXAMPLE.COM@EXAMPLE.COM
```

### **Ejemplo 21-2 Actualización de claves de principales de un servidor maestro**

Si ha iniciado sesión en el KDC maestro como `root`, puede actualizar el principal del servicio TGS con el siguiente comando:

```
kdc1 # kadmin.local -q 'cpw -randkey krbtgt/EXAMPLE.COM@EXAMPLE.COM'
```

# Configuración de autenticación entre dominios

Existen varias maneras de enlazar dominios para que los usuarios de un dominio se puedan autenticar en otro dominio. La autenticación entre dominios se lleva a cabo mediante el establecimiento de una clave secreta que se comparte entre dos dominios. La relación de los dominios puede ser jerárquica o direccional (consulte [“Jerarquía de dominios” en la página 363](#)).

## ▼ Cómo establecer la autenticación entre dominios jerárquica

El ejemplo de este procedimiento utiliza dos dominios, ENG.EAST.EXAMPLE.COM y EAST.EXAMPLE.COM. La autenticación entre dominios se establecerá en ambas direcciones. Este procedimiento debe realizarse en el KDC maestro de ambos dominios.

### Antes de empezar

El KDC maestro para cada dominio debe estar configurado. Para probar completamente el proceso de autenticación, varios clientes Kerberos deben estar configurados.

Debe asumir el rol root en ambos servidores KDC. Para obtener más información, consulte [“Cómo usar los derechos administrativos que tiene asignados” en la página 164](#).

### 1 Cree principales de servicio de ticket de otorgamiento de tickets para los dos dominios.

Debe iniciar sesión con uno de los nombres de principales admin que creó cuando configuró el KDC maestro.

```
/usr/sbin/kadmin -p kws/admin
Enter password: <Type kws/admin password>
kadmin: addprinc krbtgt/ENG.EAST.EXAMPLE.COM@EAST.EXAMPLE.COM
Enter password for principal krgtgt/ENG.EAST.EXAMPLE.COM@EAST.EXAMPLE.COM: <Type password>
kadmin: addprinc krbtgt/EAST.EXAMPLE.COM@ENG.EAST.EXAMPLE.COM
Enter password for principal krgtgt/EAST.EXAMPLE.COM@ENG.EAST.EXAMPLE.COM: <Type password>
kadmin: quit
```

---

**Nota** – La contraseña que se ha especificado para cada principal de servicio debe ser idéntica en ambos KDC. Por lo tanto, la contraseña para el principal de servicio `krbtgt/ENG.EAST.EXAMPLE.COM@EAST.EXAMPLE.COM` debe ser la misma en ambos dominios.

---

### 2 Agregue entradas al archivo de configuración de Kerberos (`krb5.conf`) para definir nombres de dominio para cada dominio.

```
cat /etc/krb5/krb5.conf
[libdefaults]
.
```

```
[domain_realm]
 .eng.east.example.com = ENG.EAST.EXAMPLE.COM
 .east.example.com = EAST.EXAMPLE.COM
```

En este ejemplo, se definen nombres de dominio para los dominios ENG.EAST.EXAMPLE.COM y EAST.EXAMPLE.COM. Es importante incluir el subdominio en primer lugar, puesto que el archivo se busca de arriba abajo.

**3 Copie el archivo de configuración de Kerberos en todos los clientes de este dominio.**

Para que la autenticación entre dominios funcione, todos los sistemas (incluidos los KDC esclavos y otros servidores) deben tener instalada la nueva versión del archivo de configuración de Kerberos (/etc/krb5/krb5.conf).

**4 Repita todos estos pasos en el segundo dominio.**

## ▼ **Cómo establecer la autenticación entre dominios directa**

El ejemplo de este procedimiento utiliza dos dominios, ENG.EAST.EXAMPLE.COM y SALES.WEST.EXAMPLE.COM. La autenticación entre dominios se establecerá en ambas direcciones. Este procedimiento debe realizarse en el KDC maestro de ambos dominios.

**Antes de empezar**

El KDC maestro para cada dominio debe estar configurado. Para probar completamente el proceso de autenticación, varios clientes Kerberos deben estar configurados.

Debe asumir el rol root en ambos servidores KDC. Para obtener más información, consulte [“Cómo usar los derechos administrativos que tiene asignados” en la página 164](#).

**1 Cree principales de servicio de ticket de otorgamiento de tickets para los dos dominios.**

Debe iniciar sesión con uno de los nombres de principales admin que creó cuando configuró el KDC maestro.

```
/usr/sbin/kadmin -p kws/admin
Enter password: <Type kws/admin password>
kadmin: addprinc krbtgt/ENG.EAST.EXAMPLE.COM@SALES.WEST.EXAMPLE.COM
Enter password for principal
 krgtgt/ENG.EAST.EXAMPLE.COM@SALES.WEST.EXAMPLE.COM: <Type the password>
kadmin: addprinc krbtgt/SALES.WEST.EXAMPLE.COM@ENG.EAST.EXAMPLE.COM
Enter password for principal
 krgtgt/SALES.WEST.EXAMPLE.COM@ENG.EAST.EXAMPLE.COM: <Type the password>
kadmin: quit
```

---

**Nota** – La contraseña que se ha especificado para cada principal de servicio debe ser idéntica en ambos KDC. Por lo tanto, la contraseña para el principal de servicio `krbtgt/ENG.EAST.EXAMPLE.COM@SALES.WEST.EXAMPLE.COM` debe ser la misma en ambos dominios.

---

**2 Agregue entradas en el archivo de configuración de Kerberos para definir la ruta directa al dominio remoto.**

En este ejemplo, se muestran los clientes en el dominio `ENG.EAST.EXAMPLE.COM`. Debe intercambiar los nombres de dominio para obtener las definiciones adecuadas en el dominio `SALES.WEST.EXAMPLE.COM`.

```
cat /etc/krb5/krb5.conf
[libdefaults]
.
.
[capaths]
 ENG.EAST.EXAMPLE.COM = {
 SALES.WEST.EXAMPLE.COM = .
 }

 SALES.WEST.EXAMPLE.COM = {
 ENG.EAST.EXAMPLE.COM = .
 }
```

**3 Copie el archivo de configuración de Kerberos en todos los clientes del dominio actual.**

Para que la autenticación entre dominios funcione, todos los sistemas (incluidos los KDC esclavos y otros servidores) deben tener instalada la nueva versión del archivo de configuración de Kerberos (`/etc/krb5/krb5.conf`).

**4 Repita todos estos pasos para el segundo dominio.**

## Configuración de servidores de aplicaciones de red de Kerberos

Los servidores de aplicaciones de red son hosts que proporcionan acceso mediante una o más de las siguientes aplicaciones de red: `ftp`, `rcp`, `rlogin`, `rsh`, `ssh` y `telnet`. Sólo se requieren unos pocos pasos para habilitar la versión de Kerberos de estos comandos en un servidor.

## ▼ Cómo configurar un servidor de aplicaciones de red de Kerberos

Este procedimiento utiliza los siguientes parámetros de configuración:

- Servidor de aplicaciones = boston
- Principal admin = kws/admin
- Nombre de dominio DNS = example.com
- Nombre de dominio = EXAMPLE.COM

### Antes de empezar

Este procedimiento requiere que el KDC maestro se haya configurado. Para probar completamente el proceso, varios clientes Kerberos deben estar configurados.

Debe asumir el rol root en el servidor de aplicación. Para obtener más información, consulte [“Cómo usar los derechos administrativos que tiene asignados” en la página 164](#).

### 1 (Opcional) Instale el cliente NTP u otro mecanismo de sincronización de relojes.

Consulte [“Sincronización de relojes entre clientes Kerberos y KDC” en la página 424](#) para obtener información sobre el NTP.

### 2 Agregue principales para el nuevo servidor y actualice el archivo keytab del servidor.

El siguiente comando informa la existencia del principal host:

```
boston # klist -k |grep host
4 host/boston.example.com@EXAMPLE.COM
4 host/boston.example.com@EXAMPLE.COM
4 host/boston.example.com@EXAMPLE.COM
4 host/boston.example.com@EXAMPLE.COM
```

Si el comando no devuelve un principal, cree nuevos principales mediante los siguientes pasos.

Si desea obtener información sobre cómo utilizar la herramienta de interfaz gráfica de usuario de administración de Kerberos para agregar un principal, consulte [“Cómo crear un nuevo principal de Kerberos” en la página 482](#). El ejemplo de los siguientes pasos muestra cómo agregar los principales necesarios mediante la línea de comandos. Debe iniciar sesión con uno de los nombres de principales admin que creó cuando configuró el KDC maestro.

```
boston # /usr/sbin/kadmin -p kws/admin
Enter password: <Type kws/admin password>
kadmin:
```

#### a. Cree el principal host del servidor.



El principal host se utiliza de las siguientes maneras:

- Para autenticar el tráfico al utilizar los comandos remotos, como `rsh` y `ssh`.
- Por `pam_krb5` para evitar ataques de falsificación de KDC mediante el principal host a fin de verificar que la credencial de Kerberos de un usuario se haya obtenido de un KDC de confianza.
- Para permitir que el usuario `root` adquiera automáticamente una credencial de Kerberos sin necesidad de que exista un principal `root`. Esto puede ser útil al realizar un montaje de NFS manual donde el recurso compartido requiere una credencial de Kerberos.

Este principal es necesario si el tráfico que utiliza la aplicación remota se va a autenticar mediante el servicio Kerberos. Si el servidor tiene varios nombres de host asociados con él, cree un principal para cada nombre de host utilizando el formato de FQDN del nombre de host.

```
kadmin: addprinc -randkey host/boston.example.com
Principal "host/boston.example.com" created.
kadmin:
```

#### b. Agregue el principal host del servidor al archivo keytab del servidor.

Si el comando `kadmin` no se está ejecutando, reinicielo con un comando similar al siguiente:

```
/usr/sbin/kadmin -p kws/admin
```

Si el servidor tiene varios nombres de host asociados con él, agregue un principal al archivo `keytab` para cada nombre de host.

```
kadmin: ktadd host/boston.example.com
Entry for principal host/boston.example.com with kvno 3, encryption type AES-256 CTS mode
with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal host/boston.example.com with kvno 3, encryption type AES-128 CTS mode
with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal host/boston.example.com with kvno 3, encryption type Triple DES cbc
mode with HMAC/sha1 added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal host/boston.example.com with kvno 3, encryption type ArcFour
with HMAC/md5 added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal host/boston.example.com with kvno 3, encryption type DES cbc mode
with RSA-MD5 added to keytab WRFILE:/etc/krb5/krb5.keytab.
kadmin:
```

#### c. Salga de `kadmin`.

```
kadmin: quit
```

## ▼ Cómo utilizar el servicio de seguridad genérico con Kerberos al ejecutar FTP

El servicio de seguridad genérico (GSS) se puede utilizar en aplicaciones para utilizar fácilmente Kerberos para autenticación, integridad y privacidad. Los pasos siguientes muestran cómo activar el servicio GSS para ProFTPD.

**Antes de empezar** Debe asumir el rol root en el servidor FTP. Para obtener más información, consulte [“Cómo usar los derechos administrativos que tiene asignados” en la página 164](#).

**1 Agregue principales para el servidor FTP y cree el archivo keytab del servidor.**

Estas medidas podrían no ser necesarias si los cambios se realizaron anteriormente.

**a. Inicie el comando kadmin.**

```
ftpserver1 # /usr/sbin/kadmin -p kws/admin
Enter password: <Type kws/admin password>
kadmin:
```

**b. Agregue el principal de servicio ftp al servidor FTP.**

```
kadmin: ank -randkey ftp/ftpserver1.example.com
```

**c. Agregue el principal de servicio ftp a un nuevo archivo keytab.**

La creación de un nuevo archivo keytab, permite que esta información esté disponible para el servicio ftp, sin exponer toda la información del archivo keytab para el servidor.

```
kadmin: ktadd -k /etc/krb5/ftp.keytab ftp/ftpserver1.example.com
```

**2 Cambie la propiedad del nuevo archivo keytab.**

```
ftpserver1 # chown ftp:ftp /etc/krb5/ftp.keytab
```

**3 Active GSS para el servidor FTP.**

Realice los siguientes cambios en el archivo `/etc/proftpd.conf`.

```
cat /etc/proftpd.conf
LoadModule mod_gss.c

GSSEngine on
GSSKeytab /etc/krb5/ftp.keytab
```

**4 Reinicie el servidor FTP.**

```
svcadm restart network/ftp
```

## Configuración de servidores NFS con Kerberos

Los servicios NFS utilizan ID de usuario (UID) de UNIX para identificar a un usuario y no pueden utilizar directamente credenciales GSS. Para traducir la credencial a un UID, es posible que se deba crear una tabla de credenciales que asigne credenciales de usuario a UID de UNIX. Consulte [“Asignación de credenciales GSS a credenciales UNIX” en la página 366](#) para obtener más información sobre la asignación predeterminada de credenciales. Los procedimientos de esta sección se centran en las tareas que se necesitan para configurar un servidor NFS con Kerberos, administrar la tabla de credenciales e iniciar los modos de seguridad de Kerberos para sistemas de archivos montados en NFS. En el siguiente mapa de tareas, se describen las tareas que se tratan en esta sección.

**TABLA 21-2** Configuración de servidores NFS con Kerberos (mapa de tareas)

| Tarea                                                                             | Descripción                                                                                                                                                                       | Para obtener instrucciones                                                                                         |
|-----------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------|
| Configurar un servidor NFS con Kerberos                                           | Permite que un servidor comparta un sistema de archivos que requiere la autenticación Kerberos.                                                                                   | <a href="#">“Cómo configurar servidores NFS con Kerberos” en la página 399</a>                                     |
| Crear una tabla de credenciales                                                   | Genera una tabla de credenciales que se puede utilizar para proporcionar asignación de credenciales GSS a ID de usuario de UNIX si la asignación predeterminada no es suficiente. | <a href="#">“Cómo crear una tabla de credenciales” en la página 401</a>                                            |
| Cambiar la tabla de credenciales que asigna credenciales de usuario a UID de UNIX | Actualiza la información en la tabla de credenciales.                                                                                                                             | <a href="#">“Cómo agregar una única entrada a la tabla de credenciales” en la página 401</a>                       |
| Crear asignaciones de credenciales entre dos dominios similares                   | Proporciona instrucciones sobre cómo asignar UID de un dominio a otro si los dominios comparten un archivo de contraseña.                                                         | <a href="#">“Cómo proporcionar asignación de credenciales entre dominios” en la página 402</a>                     |
| Compartir un sistema de archivos con autenticación Kerberos                       | Comparte un sistema de archivos con modos de seguridad, de manera que la autenticación Kerberos es necesaria.                                                                     | <a href="#">“Cómo configurar un entorno NFS seguro con varios modos de seguridad de Kerberos” en la página 403</a> |

## ▼ Cómo configurar servidores NFS con Kerberos

En este procedimiento, se utilizan los siguientes parámetros de configuración:

- Nombre de dominio = `EXAMPLE.COM`
- Nombre de dominio DNS = `example.com`
- Servidor NFS = `denver.example.com`
- Principal admin = `kws/admin`

**Antes de empezar** Debe asumir el rol root en el servidor NFS. Para obtener más información, consulte [“Cómo usar los derechos administrativos que tiene asignados” en la página 164](#).

### 1 Complete los requisitos para configurar un servidor NFS con Kerberos.

El KDC maestro debe estar configurado. Para probar completamente el proceso, necesita varios clientes.

### 2 (Opcional) Instale el cliente NTP u otro mecanismo de sincronización de relojes.

No es necesario instalar ni utilizar el protocolo de hora de red (NTP). Sin embargo, cada reloj debe estar sincronizado con la hora en el servidor KDC dentro de una diferencia máxima definida por la relación `clockskew` en el archivo `krb5.conf` para que la autenticación se realice con éxito. Consulte [“Sincronización de relojes entre clientes Kerberos y KDC” en la página 424](#) para obtener información sobre el NTP.

### 3 Configure el servidor NFS como un cliente Kerberos.

Siga las instrucciones en [“Configuración de clientes Kerberos” en la página 405](#).

### 4 Inicie kadmin.

Si desea obtener información sobre cómo utilizar la herramienta gráfica de administración de Kerberos para agregar un principal, consulte [“Cómo crear un nuevo principal de Kerberos” en la página 482](#). Para ello, debe iniciar sesión con uno de los nombres de principales admin que creó cuando configuró el KDC maestro. Sin embargo, el siguiente ejemplo muestra cómo agregar los principales necesarios mediante la línea de comandos.

```
denver # /usr/sbin/kadmin -p kws/admin
Enter password: <Type kws/admin password>
kadmin:
```

#### a. Cree el principal de servicio NFS del servidor.

Tenga en cuenta que cuando la instancia de principal es un nombre de host, el FQDN se debe especificar en letras minúsculas, independientemente de si el nombre de dominio está en mayúsculas o minúsculas en el servicio de nombres.

Repita este paso para cada interfaz única en el sistema que pueda ser utilizada para acceder a datos de NFS. Si un host tiene varias interfaces con nombres únicos, cada nombre único debe tener su propio principal de servicio NFS.

```
kadmin: addprinc -randkey nfs/denver.example.com
Principal "nfs/denver.example.com" created.
kadmin:
```

#### b. Agregue el principal de servicio NFS del servidor al archivo keytab del servidor.

Repita este paso para cada principal de servicio único creado en el [Paso a](#).

```
kadmin: ktadd nfs/denver.example.com
Entry for principal nfs/denver.example.com with kvno 3, encryption type AES-256 CTS mode
with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal nfs/denver.example.com with kvno 3, encryption type AES-128 CTS mode
with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal nfs/denver.example.com with kvno 3, encryption type Triple DES cbc
mode with HMAC/sha1 added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal nfs denver.example.com with kvno 3, encryption type ArcFour
with HMAC/md5 added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal nfs/denver.example.com with kvno 3, encryption type DES cbc mode
with RSA-MD5 added to keytab WRFILE:/etc/krb5/krb5.keytab.
kadmin:
```

#### c. Salga de kadmin.

```
kadmin: quit
```

### 5 (Opcional) Cree asignaciones de credenciales GSS especiales si es necesario.

Normalmente, el servicio Kerberos genera asignaciones adecuadas entre las credenciales GSS y los UID de UNIX. La asignación predeterminada se describe en [“Asignación de credenciales](#)

[GSS a credenciales UNIX](#) en la página 366. Si la asignación predeterminada no es suficiente, consulte [“Cómo crear una tabla de credenciales” en la página 401](#) para obtener más información.

## 6 Comparta el sistema de archivos NFS con modos de seguridad de Kerberos.

Consulte [“Cómo configurar un entorno NFS seguro con varios modos de seguridad de Kerberos” en la página 403](#) para obtener más información.

## ▼ Cómo crear una tabla de credenciales

La tabla de credenciales `gsscred` es utilizada por un servidor NFS para asignar credenciales Kerberos a un UID. De manera predeterminada, la parte principal del nombre del principal se compara con un nombre de inicio de sesión de UNIX. Para que los clientes NFS monten sistemas de archivos de un servidor NFS con autenticación Kerberos, esta tabla se debe crear si la asignación predeterminada no es suficiente.

**Antes de empezar** Debe asumir el rol `root` en el servidor NFS. Para obtener más información, consulte [“Cómo usar los derechos administrativos que tiene asignados” en la página 164](#).

### 1 Edite `/etc/gss/gsscred.conf` y cambie el mecanismo de seguridad.

Cambie el mecanismo a `files`.

### 2 Cree la tabla de credenciales mediante el comando `gsscred`.

```
gsscred -m kerberos_v5 -a
```

El comando `gsscred` recopila información de todos los orígenes que se muestran con la entrada `passwd` en el servicio `svc:/system/name-service/switch:default`. Es posible que necesite eliminar temporalmente la entrada `files` si no desea las entradas de contraseñas locales incluidas en la tabla de credenciales. Consulte la página del comando [man `gsscred\(1M\)`](#) para obtener más información.

## ▼ Cómo agregar una única entrada a la tabla de credenciales

**Antes de empezar** Este procedimiento requiere que la tabla `gsscred` ya se haya creado en el servidor NFS. Consulte [“Cómo crear una tabla de credenciales” en la página 401](#) para obtener instrucciones.

Debe asumir el rol `root` en el servidor NFS. Para obtener más información, consulte [“Cómo usar los derechos administrativos que tiene asignados” en la página 164](#).

### ● Agregue una entrada a la tabla de credenciales mediante el comando `gsscred`.

```
gsscred -m mech [-n name [-u uid]] -a
```

|             |                                                                                   |
|-------------|-----------------------------------------------------------------------------------|
| <i>mec</i>  | Define el mecanismo de seguridad que se va a utilizar.                            |
| <i>name</i> | Define el nombre de principal para el usuario, como se define en el KDC.          |
| <i>uid</i>  | Define el UID para el usuario, como se define en la base de datos de contraseñas. |
| <i>-a</i>   | Agrega el UID a la asignación del nombre de principal.                            |

### **Ejemplo 21–3** Adición de un principal de componente múltiple a la tabla de credenciales

En el siguiente ejemplo, se agrega una entrada para un principal denominado `sandy/admin`, que está asignado al UID 3736.

```
gsscred -m kerberos_v5 -n sandy/admin -u 3736 -a
```

### **Ejemplo 21–4** Adición de un principal de un dominio diferente en la tabla de credenciales

En el siguiente ejemplo, se agrega una entrada para un principal denominado `sandy/admin@EXAMPLE.COM`, que está asignado al UID 3736.

```
gsscred -m kerberos_v5 -n sandy/admin@EXAMPLE.COM -u 3736 -a
```

## ▼ **Cómo proporcionar asignación de credenciales entre dominios**

Este procedimiento proporciona una asignación de credenciales apropiada entre dominios que utilizan el mismo archivo de contraseña. En este ejemplo, los dominios `CORP.EXAMPLE.COM` y `SALES.EXAMPLE.COM` utilizan el mismo archivo de contraseña. Las credenciales para `bob@CORP.EXAMPLE.COM` y `bob@SALES.EXAMPLE.COM` están asignadas al mismo UID.

**Antes de empezar** Debe asumir el rol `root` en el sistema cliente. Para obtener más información, consulte [“Cómo usar los derechos administrativos que tiene asignados” en la página 164](#).

- **En el sistema cliente, agregue entradas al archivo `krb5.conf`.**

```
cat /etc/krb5/krb5.conf
[libdefaults]
 default_realm = CORP.EXAMPLE.COM
.
[realms]
 CORP.EXAMPLE.COM = {
 .
 auth_to_local_realm = SALES.EXAMPLE.COM
 .
 }
```

### Ejemplo 21-5 Asignación de credenciales entre dominios mediante el mismo archivo de contraseña

Este ejemplo proporciona una asignación de credenciales apropiada entre dominios que utilizan el mismo archivo de contraseña. En este ejemplo, los dominios CORP.EXAMPLE.COM y SALES.EXAMPLE.COM utilizan el mismo archivo de contraseña. Las credenciales para bob@CORP.EXAMPLE.COM y bob@SALES.EXAMPLE.COM están asignadas al mismo UID. En el sistema cliente, agregue entradas al archivo krb5.conf.

```
cat /etc/krb5/krb5.conf
[libdefaults]
 default_realm = CORP.EXAMPLE.COM

[realms]
 CORP.EXAMPLE.COM = {
 .
 auth_to_local_realm = SALES.EXAMPLE.COM
 .
 }
```

#### Errores más frecuentes

Consulte [“Observación de asignación de credenciales GSS a credenciales UNIX” en la página 469](#) para obtener ayuda con el proceso de resolución de problemas de asignación de credenciales.

## ▼ Cómo configurar un entorno NFS seguro con varios modos de seguridad de Kerberos

Este procedimiento permite que un servidor NFS proporcione acceso seguro al NFS mediante diferentes tipos o modos de seguridad. Cuando un cliente negocia un tipo de seguridad con el servidor NFS, se utiliza el primer tipo ofrecido por el servidor al cual el cliente tiene acceso. Este tipo se utiliza para todas las solicitudes de cliente posteriores del sistema de archivos compartidas por el servidor NFS.

#### Antes de empezar

Debe asumir el rol root en el servidor NFS. Para obtener más información, consulte [“Cómo usar los derechos administrativos que tiene asignados” en la página 164](#).

#### 1 Verifique que exista un principal de servicio NFS en el archivo keytab.

El comando `klist` informa si hay un archivo keytab y muestra los principales. Si los resultados muestran que no existe ningún archivo keytab o que no existe ningún principal de servicio NFS, debe verificar que se hayan completado todos los pasos en [“Cómo configurar servidores NFS con Kerberos” en la página 399](#).

```
klist -k
Keytab name: FILE:/etc/krb5/krb5.keytab
KVNO Principal
```

```

3 nfs/denver.example.com@EXAMPLE.COM
3 nfs/denver.example.com@EXAMPLE.COM
3 nfs/denver.example.com@EXAMPLE.COM
3 nfs/denver.example.com@EXAMPLE.COM
```

## 2 Active los modos de seguridad de Kerberos en el archivo `/etc/nfssec.conf`.

Edita el archivo `/etc/nfssec.conf` y elimine el símbolo “#” que se encuentra delante de los modos de seguridad de Kerberos.

```
cat /etc/nfssec.conf
.

Uncomment the following lines to use Kerberos V5 with NFS

krb5 390003 kerberos_v5 default - # RPCSEC_GSS
krb5i 390004 kerberos_v5 default integrity # RPCSEC_GSS
krb5p 390005 kerberos_v5 default privacy # RPCSEC_GSS
```

## 3 Comparta los sistemas de archivos con los modos de seguridad apropiados.

```
share -F nfs -o sec=mode file-system
```

*modo*                      Especifica los modos de seguridad que se utilizarán al compartir el sistema de archivos. Cuando se utilizan varios modos de seguridad, el primero en la lista se utiliza de manera predeterminada.

*sistema\_archivos*        Define la ruta al sistema de archivos que se va a compartir.

Todos los clientes que intentan acceder a los archivos desde el sistema de archivos especificado requieren autenticación Kerberos. Para acceder a los archivos, el principal de usuario en el cliente NFS debe autenticarse.

## 4 (Opcional) Si el montador automático se está utilizando, edite la base de datos `auto_master` para seleccionar un modo de seguridad distinto del predeterminado.

No es necesario que siga este procedimiento si no está utilizando el montador automático para acceder al sistema de archivos o si la selección predeterminada para el modo de seguridad es aceptable.

```
file-system auto_home -nosuid,sec=mode
```

## 5 (Opcional) Emita manualmente el comando `mount` para acceder al sistema de archivos mediante un modo que no esté predeterminado.

Como alternativa, puede utilizar el comando `mount` para especificar el modo de seguridad, pero esta alternativa no aprovecha el montador automático.

```
mount -F nfs -o sec=mode file-system
```



**Ejemplo 21–6**    Uso compartido de un sistema de archivos con un modo de seguridad de Kerberos

En este ejemplo, la autenticación de Kerberos debe realizarse correctamente antes de que se pueda acceder a cualquier archivo mediante el servicio NFS.

```
share -F nfs -o sec=krb5 /export/home
```

**Ejemplo 21–7**    Uso compartido de un sistema de archivos con varios modos de seguridad de Kerberos

En este ejemplo, los tres modos de seguridad de Kerberos se han seleccionado. El modo que se utiliza se negocia entre el cliente y el servidor NFS. Si falla el primer modo en el comando, se intenta con el siguiente. Consulte la página del comando `man nfssec(5)` para obtener más información.

```
share -F nfs -o sec=krb5:krb5i:krb5p /export/home
```

# Configuración de clientes Kerberos

Los clientes Kerberos incluyen cualquier host, que no es un servidor KDC, en la red que necesita utilizar servicios Kerberos. Esta sección proporciona procedimientos para instalar un cliente Kerberos, así como información específica sobre el uso de la autenticación de root para montar sistemas de archivos NFS.

## Configuración de clientes Kerberos (mapa de tareas)

El siguiente mapa de tareas incluye todos los procedimientos asociados con la configuración de clientes Kerberos. Cada fila incluye un identificador de tarea y una descripción del motivo por el que desea realizar la tarea, seguidos de un enlace a la tarea.

| Tarea                                                   | Descripción                                                                                                                                                                                                                                                                                         | Para obtener instrucciones                                                                                                                                                       |
|---------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Establecer un perfil de instalación de cliente Kerberos | Genera un perfil de instalación de cliente que se puede utilizar para instalar automáticamente un cliente Kerberos.                                                                                                                                                                                 | <a href="#">“Cómo crear un perfil de instalación de cliente Kerberos” en la página 406</a>                                                                                       |
| Configurar un cliente Kerberos                          | Instala manualmente un cliente Kerberos. Utilizar este procedimiento si la instalación de cada cliente requiere parámetros de instalación únicos.<br><br>Instala automáticamente un cliente Kerberos. Utilice este procedimiento si los parámetros de instalación para cada cliente son los mismos. | <a href="#">“Cómo configurar manualmente un cliente Kerberos” en la página 412</a><br><br><a href="#">“Cómo configurar automáticamente un cliente Kerberos” en la página 406</a> |

| Tarea                                                                                                   | Descripción                                                                                                                                                                                                                                                                    | Para obtener instrucciones                                                                                                                                                                                 |
|---------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                                         | Instala interactivamente un cliente Kerberos. Utilice este procedimiento si sólo algunos de los parámetros de instalación deben cambiarse.<br><br>Instala automáticamente un cliente Kerberos de un servidor de Active Directory.                                              | <a href="#">“Cómo configurar interactivamente un cliente Kerberos” en la página 408</a><br><br><a href="#">“Cómo configurar un cliente Kerberos para un servidor de Active Directory” en la página 411</a> |
| Permitir que un cliente acceda a un sistema de archivos NFS como el usuario root                        | Crea un principal root en el cliente, para que el cliente pueda montar un sistema de archivos NFS compartido con el acceso root. Además, permite que el cliente configure acceso root no interactivo al sistema de archivos NFS, de modo que se puedan ejecutar trabajos cron. | <a href="#">“Cómo acceder a un sistema de archivos NFS protegido con Kerberos como el usuario root” en la página 419</a>                                                                                   |
| Desactivar la verificación del KDC que ha emitido un ticket de otorgamiento de tickets (TGT) de cliente | Permite a los clientes que no tienen un principal host almacenado en el archivo keytab local omitir la comprobación de seguridad que verifica que el KDC que ha emitido el TGT sea el mismo servidor que ha emitido el principal host.                                         | <a href="#">“Cómo desactivar la verificación del ticket de otorgamiento de tickets” en la página 418</a>                                                                                                   |

## ▼ Cómo crear un perfil de instalación de cliente Kerberos

Este procedimiento crea un perfil kclient que se puede utilizar al instalar un cliente Kerberos. Mediante el perfil kclient, se reducen las probabilidades de errores de escritura. Asimismo, el uso del perfil reduce la intervención del usuario, en comparación con el proceso interactivo.

1 **Conviértase en superusuario.**

2 **Cree un perfil de instalación kclient.**

Un ejemplo de perfil kclient podría ser similar al siguiente:

```
client# cat /net/denver.example.com/export/install/profile
REALM EXAMPLE.COM
KDC kdc1.example.com
ADMIN clntconfig
FILEPATH /net/denver.example.com/export/install/krb5.conf
NFS 1
DNSLOOKUP none
```

## ▼ Cómo configurar automáticamente un cliente Kerberos

**Antes de empezar** Este procedimiento utiliza un perfil de instalación. Consulte [“Cómo crear un perfil de instalación de cliente Kerberos” en la página 406](#).

Para completar esta tarea, debe asumir el rol root. Para obtener más información, consulte [“Cómo usar los derechos administrativos que tiene asignados” en la página 164.](#)

- **Ejecute la secuencia de comandos de instalación de `kclient`.**

Debe proporcionar la contraseña para el principal `clntconfig` con el fin de completar el proceso.

```
client# /usr/sbin/kclient -p /net/denver.example.com/export/install/profile
```

```
Starting client setup
```

```

```

```
kdc1.example.com
```

```
Setting up /etc/krb5/krb5.conf.
```

```
Obtaining TGT for clntconfig/admin ...
```

```
Password for clntconfig/admin@EXAMPLE.COM: <Type the password>
```

```
nfs/client.example.com entry ADDED to KDC database.
```

```
nfs/client.example.com entry ADDED to keytab.
```

```
host/client.example.com entry ADDED to KDC database.
```

```
host/client.example.com entry ADDED to keytab.
```

```
Copied /net/denver.example.com/export/install/krb5.conf.
```

```

```

```
Setup COMPLETE.
```

```
client#
```

## **Ejemplo 21–8** Configuración automática de un cliente Kerberos con valores de sustitución de línea de comandos

El siguiente ejemplo sustituye los parámetros `DNSARG` y `KDC` que se establecen en el perfil de instalación.

```
/usr/sbin/kclient -p /net/denver.example.com/export/install/profile\
```

```
-d dns_fallback -k kdc2.example.com
```

```
Starting client setup
```

```

```

```
kdc1.example.com
```

```
Setting up /etc/krb5/krb5.conf.
```

```
Obtaining TGT for clntconfig/admin ...
```

```
Password for clntconfig/admin@EXAMPLE.COM: <Type the password>
```

```
nfs/client.example.com entry ADDED to KDC database.
nfs/client.example.com entry ADDED to keytab.

host/client.example.com entry ADDED to KDC database.
host/client.example.com entry ADDED to keytab.

Copied /net/denver.example.com/export/install/krb5.conf.

Setup COMPLETE.

client#
```

## ▼ **Cómo configurar interactivamente un cliente Kerberos**

Este procedimiento utiliza la utilidad de instalación `kclient` sin un perfil de instalación. En la versión Oracle Solaris 11, la utilidad `kclient` incrementó la facilidad de uso y la capacidad de trabajar con servidores de Active Directory. Consulte [“Cómo configurar un cliente Kerberos para un servidor de Active Directory” en la página 411](#) para obtener más información. Consulte el [Ejemplo 21–10](#) para obtener un ejemplo de ejecución de `kclient` en una versión anterior.

**Antes de empezar** Para completar esta tarea, debe asumir el rol root. Para obtener más información, consulte [“Cómo usar los derechos administrativos que tiene asignados” en la página 164](#).

### ● **Ejecute la secuencia de comandos de instalación de `kclient`.**

Necesita proporcionar la siguiente información:

- Nombre de dominio Kerberos
- Nombre de host de KDC maestro
- Nombres de host de KDC esclavos
- Dominios que se van a asignar al dominio local
- Nombres de servicio PAM y opciones que se utilizarán para la autenticación Kerberos

#### **a. Indique si el servidor KDC no ejecuta una versión Oracle Solaris.**

Si el sistema es un cliente de un servidor KDC que no ejecuta una versión Oracle Solaris, es necesario definir el tipo de servidor que está ejecutando el KDC. Los servidores disponibles son: Microsoft Active Directory, servidor KDC MIT, servidor KDC Heimdal y servidor KDC Shishi.

**b. Seleccione si DNS se debe utilizar para las consultas de Kerberos.**

Si utiliza el DNS para las consultas de Kerberos, deberá introducir la opción de consulta de DNS que desea utilizar. Las opciones válidas son `dns_lookup_kdc`, `dns_lookup_realm` y `dns_fallback`. Consulte la página del comando `man krb5.conf(4)` para obtener más información sobre estos valores.

**c. Defina el nombre del dominio de Kerberos y el nombre de host de KDC maestro.**

Esta información se ha agregado al archivo de configuración `/etc/krb5/krb5.conf`.

**d. Seleccione si existen KDC esclavos.**

Si hay KDC esclavos en el dominio, entonces es necesario introducir los nombres de host de KDC esclavos. Esta información se utiliza para crear entradas KDC adicionales en el archivo de configuración del cliente.

**e. Indique si el servicio o las claves de host son necesarios.**

Normalmente, el servicio o las claves de host no son necesarios, a menos que el sistema cliente aloje servicios kerberizados.

**f. Especifique si el cliente es un miembro de un clúster.**

Si el cliente es un miembro de un clúster, entonces tendrá que proporcionar el nombre lógico del clúster. El nombre de host lógico se utiliza al crear claves de servicio, que es necesario cuando se alojan servicios Kerberos de los clústeres.

**g. Identifique cualquier host o dominio que se va a asignar al dominio actual.**

Esta asignación permite que otros dominios pertenezcan al dominio predeterminado del cliente.

**h. Especifique si el cliente utilizará NFS Kerberizado.**

Las claves de servicio NFS se deben crear si el cliente alojará servicios NFS mediante Kerberos.

**i. Indique si se debe crear una nueva política de PAM.**

Esta opción permite al usuario definir qué servicios PAM utilizan Kerberos para la autenticación. Es necesario introducir el nombre del servicio y un indicador que determine cómo se utilizará la autenticación Kerberos. Las opciones de indicadores válidos son:

- `first`: utilice primero la autenticación Kerberos y sólo utilice UNIX si la autenticación Kerberos falla
- `only`: utilice sólo autenticación Kerberos
- `optional`: utilice autenticación Kerberos de manera optativa

**j. Seleccione esta opción si el archivo `/etc/krb5/krb5.conf` maestro se debe copiar.**

Esta opción permite que se utilice información de configuración específica cuando los argumentos para `kclient` no son suficientes.

### **Ejemplo 21-9 Ejecución de la utilidad de instalación `kclient`**

```
client# /usr/sbin/kclient

Starting client setup

Is this a client of a non-Solaris KDC ? [y/n]: n
 No action performed.
Do you want to use DNS for kerberos lookups ? [y/n]: n
 No action performed.
Enter the Kerberos realm: EXAMPLE.COM
Specify the KDC hostname for the above realm: kdc1.example.com

Note, this system and the KDC's time must be within 5 minutes of each other for
Kerberos to function. Both systems should run some form of time synchronization
system like Network Time Protocol (NTP).
Do you have any slave KDC(s) ? [y/n]: y
Enter a comma-separated list of slave KDC host names: kdc2.example.com

Will this client need service keys ? [y/n]: n
 No action performed.
Is this client a member of a cluster that uses a logical host name ? [y/n]: n
 No action performed.
Do you have multiple domains/hosts to map to realm ? [y/n]: y
Enter a comma-separated list of domain/hosts to map to the default realm: engineering.example.com, \
example.com

Setting up /etc/krb5/krb5.conf.

Do you plan on doing Kerberized nfs ? [y/n]: y
Do you want to update /etc/pam.conf ? [y/n]: y
Enter a comma-separated list of PAM service names in the following format:
service:{first|only|optional}: xscreensaver:first
Configuring /etc/pam.conf.

Do you want to copy over the master krb5.conf file ? [y/n]: n
 No action performed.

Setup COMPLETE.
```

### **Ejemplo 21-10 Ejecución de la utilidad de instalación `kclient` en la versión Oracle Solaris 10**

A continuación, se muestra la salida de los resultados de la ejecución del comando `kclient`.

```
client# /usr/sbin/kclient

Starting client setup

```

```

Do you want to use DNS for kerberos lookups ? [y/n]: n
 No action performed.
Enter the Kerberos realm: EXAMPLE.COM
Specify the KDC hostname for the above realm: kdc1.example.com

Setting up /etc/krb5/krb5.conf.

Enter the krb5 administrative principal to be used: clntconfig/admin
Obtaining TGT for clntconfig/admin ...
Password for clntconfig/admin@EXAMPLE.COM: <Type the password>
Do you plan on doing Kerberized nfs ? [y/n]: n

host/client.example.com entry ADDED to KDC database.
host/client.example.com entry ADDED to keytab.

Do you want to copy over the master krb5.conf file ? [y/n]: y
Enter the pathname of the file to be copied: \
/net/denver.example.com/export/install/krb5.conf

Copied /net/denver.example.com/export/install/krb5.conf.

Setup COMPLETE !
#

```

## ▼ Cómo configurar un cliente Kerberos para un servidor de Active Directory

Este procedimiento utiliza la utilidad de instalación `kcLient` sin un perfil de instalación.

**Antes de empezar** Debe asumir el rol root. Para obtener más información, consulte [“Cómo usar los derechos administrativos que tiene asignados” en la página 164](#).

### 1 (Opcional) Active la creación de registros de recursos DNS para el cliente.

```
client# sharectl set -p ddns_enable=true smb
```

### 2 Ejecute la utilidad `kcLient`.

La opción `-T` selecciona un tipo de servidor KDC. En este caso se selecciona un servidor de Active Directory.

```
client# kcLient -T ms_ad
```

De manera predeterminada, deberá proporcionar la contraseña del administrador principal.

**Ejemplo 21–11 Configuración de un cliente Kerberos para un servidor de Active Directory mediante `kclient`**

La siguiente salida muestra los resultados de la ejecución del comando `kclient` mediante el argumento de tipo de servidor `ms_ad` (Microsoft Active Directory). El cliente se unirá al dominio de Active Directory denominado `EXAMPLE.COM`.

```
client# /usr/sbin/kclient -T ms_ad

Starting client setup

Attempting to join 'CLIENT' to the 'EXAMPLE.COM' domain.
Password for Administrator@EXAMPLE.COM: <Type the password>
Forest name found: example.com
Looking for local KDCs, DCs and global catalog servers (SVR RRs).

Setting up /etc/krb5/krb5.conf

Creating the machine account in AD via LDAP.

Setup COMPLETE.
#
```

## ▼ Cómo configurar manualmente un cliente Kerberos

En este procedimiento, se utilizan los siguientes parámetros de configuración:

- Nombre de dominio = `EXAMPLE.COM`
- Nombre de dominio DNS = `example.com`
- KDC maestro = `kdc1.example.com`
- KDC esclavo = `kdc2.example.com`
- Servidor NFS = `denver.example.com`
- Cliente = `client.example.com`
- Principal admin = `kws/admin`
- Principal de usuario = `mre`
- URL de ayuda en pantalla =  
`http://docs.oracle.com/cd/E23824_01/html/821-1456/aadmin-23.html`

---

**Nota** – Ajuste la dirección URL para que establezca un enlace a la sección, como se describe en “[URL de ayuda en pantalla en la herramienta gráfica de administración de Kerberos](#)” en la página 370.

---



**Antes de empezar** Debe asumir el rol root. Para obtener más información, consulte [“Cómo usar los derechos administrativos que tiene asignados” en la página 164.](#)

## 1 Edite el archivo de configuración de Kerberos (krb5.conf).

Para cambiar el archivo de la versión predeterminada de Kerberos, debe cambiar los nombres de dominios y los nombres de servidores. También tiene que identificar la ruta a los archivos de ayuda para gkadmin.

```
kdc1 # cat /etc/krb5/krb5.conf
[libdefaults]
 default_realm = EXAMPLE.COM

[realms]
 EXAMPLE.COM = {
 kdc = kdc1.example.com
 kdc = kdc2.example.com
 admin_server = kdc1.example.com
 }

[domain_realm]
 .example.com = EXAMPLE.COM

#
if the domain name and realm name are equivalent,
this entry is not needed
#
[logging]
 default = FILE:/var/krb5/kdc.log
 kdc = FILE:/var/krb5/kdc.log

[appdefaults]
 gkadmin = {
 help_url = http://docs.oracle.com/cd/E23824_01/html/821-1456/aadmin-23.html
```

---

**Nota** – Si desea restringir los tipos de cifrado, puede definir las líneas `default_tkt_encypes` o `default_tgs_encypes`. Consulte [“Uso de los tipos de cifrado de Kerberos” en la página 541](#) para obtener una descripción de los problemas relacionados con la restricción de los tipos de cifrado.

---

## 2 (Opcional) Cambie el proceso utilizado para ubicar los KDC.

De manera predeterminada, el dominio de Kerberos para la asignación KDC se determina en el siguiente orden:

- La definición en la sección `realms`, en `krb5.conf`.
- Mediante la búsqueda de registros SRV en DNS.

Puede cambiar este comportamiento agregando `dns_lookup_kdc` o `dns_fallback` a la sección `libdefaults` del archivo `krb5.conf`. Consulte la página del comando `man krb5.conf(4)` para obtener más información. Tenga en cuenta que las referencias siempre se intentan en primer lugar.

## 3 (Opcional) Cambie el proceso que se utiliza para determinar el dominio para un host.

De manera predeterminada, el host para la asignación de dominio se determina en el siguiente orden:

- Si el KDC admite referencias, el KDC puede informar al cliente a qué dominio pertenece el host.
- Por la definición de `domain_realm` en el archivo `krb5.conf`.
- El nombre de dominio DNS del host.
- El dominio predeterminado.

Puede cambiar este comportamiento agregando `dns_lookup_kdc` o `dns_fallback` a la sección `libdefaults` del archivo `krb5.conf`. Consulte la página del comando `man krb5.conf(4)` para obtener más información. Tenga en cuenta que las referencias siempre se intentarán en primer lugar.

#### **4 (Opcional) Sincronice el reloj del cliente con el reloj del KDC maestro mediante NTP u otro mecanismo de sincronización de relojes.**

No es necesario instalar ni utilizar el protocolo de hora de red (NTP). Sin embargo, cada reloj debe estar sincronizado con la hora en el servidor KDC dentro de una diferencia máxima definida por la relación `clockskew` en el archivo `krb5.conf` para que la autenticación se realice con éxito. Consulte “[Sincronización de relojes entre clientes Kerberos y KDC](#)” en la página 424 para obtener información sobre el NTP.

#### **5 Inicie `kadmin`.**

Si desea obtener información sobre cómo utilizar la herramienta gráfica de administración de Kerberos para agregar un principal, consulte “[Cómo crear un nuevo principal de Kerberos](#)” en la página 482. Para ello, debe iniciar sesión con uno de los nombres de principales `admin` que creó cuando configuró el KDC maestro. Sin embargo, el siguiente ejemplo muestra cómo agregar los principales necesarios mediante la línea de comandos.

```
denver # /usr/sbin/kadmin -p kws/admin
Enter password: <Type kws/admin password>
kadmin:
```

##### **a. (Opcional) Cree un principal de usuario si aún no existe ningún principal de usuario.**

Necesita crear un principal de usuario sólo si el usuario asociado con este host no tiene un principal asignado a él.

```
kadmin: addprinc mre
Enter password for principal mre@EXAMPLE.COM: <Type the password>
Re-enter password for principal mre@EXAMPLE.COM: <Type it again>
kadmin:
```

##### **b. (Opcional) Cree un principal `root` y agregue el principal al archivo `keytab` del servidor.**

Este paso es necesario para que el cliente pueda tener acceso `root` a sistemas de archivos montados mediante el servicio NFS. Este paso también es necesario si se necesita acceso `root` no interactivo, por ejemplo, la ejecución de trabajos cron como `root`.

Si el cliente no requiere acceso root a un sistema de archivos remoto que está montado mediante el servicio NFS, puede omitir este paso. El principal root debe ser un principal de dos componentes, donde el segundo componente es el nombre de host del sistema cliente Kerberos, para evitar la creación de un principal root de todo el dominio. Tenga en cuenta que cuando la instancia de principal es un nombre de host, el FQDN se debe especificar en letras minúsculas, independientemente de si el nombre de dominio está en mayúsculas o minúsculas en el servicio de nombres.

```
kadmin: addprinc -randkey root/client.example.com
Principal "root/client.example.com" created.
kadmin: ktadd root/client.example.com
Entry for principal root/client.example.com with kvno 3, encryption type AES-256 CTS mode
with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal root/client.example.com with kvno 3, encryption type AES-128 CTS mode
with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal root/client.example.com with kvno 3, encryption type Triple DES cbc
mode with HMAC/sha1 added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal root/client.example.com with kvno 3, encryption type ArcFour
with HMAC/md5 added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal root/client.example.com with kvno 3, encryption type DES cbc mode
with RSA-MD5 added to keytab WRFILE:/etc/krb5/krb5.keytab.
kadmin:
```

### c. Cree un principal host y agregue el principal al archivo keytab del servidor.

El principal host es utilizado por servicios de acceso remoto para proporcionar autenticación. El principal permite que root adquiera una credencial si ya no hay una en el archivo keytab.

```
kadmin: addprinc -randkey host/denver.example.com
Principal "host/denver.example.com@EXAMPLE.COM" created.
kadmin: ktadd host/denver.example.com
Entry for principal host/denver.example.com with kvno 3, encryption type AES-256 CTS mode
with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal host/denver.example.com with kvno 3, encryption type AES-128 CTS mode
with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal host/denver.example.com with kvno 3, encryption type Triple DES cbc
mode with HMAC/sha1 added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal host/denver.example.com with kvno 3, encryption type ArcFour
with HMAC/md5 added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal host/denver.example.com with kvno 3, encryption type DES cbc mode
with RSA-MD5 added to keytab WRFILE:/etc/krb5/krb5.keytab.
kadmin:
```

### d. (Opcional) Agregue el principal de servicio NFS del servidor al archivo keytab del servidor.

Este paso sólo es necesario si el cliente necesita acceder a sistemas de archivos NFS utilizando la autenticación Kerberos.

```
kadmin: ktadd nfs/denver.example.com
Entry for principal nfs/denver.example.com with kvno 3, encryption type AES-256 CTS mode
with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal nfs/denver.example.com with kvno 3, encryption type AES-128 CTS mode
with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal nfs/denver.example.com with kvno 3, encryption type Triple DES cbc
mode with HMAC/sha1 added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal nfs/denver.example.com with kvno 3, encryption type ArcFour
```

```
with HMAC/md5 added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal nfs/denver.example.com with kvno 3, encryption type DES cbc mode
with RSA-MD5 added to keytab WRFILE:/etc/krb5/krb5.keytab.
kadmin:
```

**e. Salga de kadmin.**

```
kadmin: quit
```

**6 (Opcional) Habilite Kerberos con NFS.**

**a. Active los modos de seguridad de Kerberos en el archivo /etc/nfssec.conf.**

Edite el archivo /etc/nfssec.conf y elimine el símbolo “#” que se encuentra delante de los modos de seguridad de Kerberos.

```
cat /etc/nfssec.conf
.

Uncomment the following lines to use Kerberos V5 with NFS

krb5 390003 kerberos_v5 default - # RPCSEC_GSS
krb5i 390004 kerberos_v5 default integrity # RPCSEC_GSS
krb5p 390005 kerberos_v5 default privacy # RPCSEC_GSS
```

**b. Active el DNS.**

Si el servicio `svc:/network/dns/client:default` no está activado, debe activarlo. Consulte la página del comando `man resolv.conf(4)` para obtener más información.

**c. Reinicie el servicio gssd.**

```
svcadm restart network/rpc/gss
```

**7 Si desea que el cliente renueve automáticamente el TGT o advierta a los usuarios acerca de la caducidad del ticket Kerberos, cree una entrada en el archivo /etc/krb5/warn.conf.**

Consulte la página del comando `man warn.conf(4)` para obtener más información.

## **Ejemplo 21–12 Configuración de un cliente Kerberos mediante un KDC que no sea Solaris**

Un cliente Kerberos se puede configurar para trabajar con un KDC que no sea Solaris. En este caso, se debe incluir una línea en el archivo /etc/krb5/krb5.conf, en la sección `realms`. Esta línea cambia el protocolo que se utiliza cuando el cliente se comunica con el servidor de cambio de contraseña de Kerberos. A continuación, se indica el formato de esta línea.

```
[realms]
 EXAMPLE.COM = {
 kdc = kdc1.example.com
 kdc = kdc2.example.com
 admin_server = kdc1.example.com
 kpasswd_protocol = SET_CHANGE
 }
```

**Ejemplo 21–13** Registros TXT de DNS para la asignación de nombre de host y dominio al dominio Kerberos

```
@ IN SOA kdc1.example.com root.kdc1.example.com (
 1989020501 ;serial
 10800 ;refresh
 3600 ;retry
 3600000 ;expire
 86400) ;minimum

 IN NS kdc1.example.com.
kdc1 IN A 192.146.86.20
kdc2 IN A 192.146.86.21

_kerberos.example.com. IN TXT "EXAMPLE.COM"
_kerberos.kdc1.example.com. IN TXT "EXAMPLE.COM"
_kerberos.kdc2.example.com. IN TXT "EXAMPLE.COM"
```

**Ejemplo 21–14** Registros SRV de DNS para ubicaciones del servidor Kerberos

En este ejemplo, se definen los registros para la ubicación de los KDC, el servidor admin y el servidor kpasswd, respectivamente.

```
@ IN SOA kdc1.example.com root.kdc1.example.com (
 1989020501 ;serial
 10800 ;refresh
 3600 ;retry
 3600000 ;expire
 86400) ;minimum

 IN NS kdc1.example.com.
kdc1 IN A 192.146.86.20
kdc2 IN A 192.146.86.21

_kerberos._udp.EXAMPLE.COM IN SRV 0 0 88 kdc2.example.com
_kerberos._tcp.EXAMPLE.COM IN SRV 0 0 88 kdc2.example.com
_kerberos._udp.EXAMPLE.COM IN SRV 1 0 88 kdc1.example.com
_kerberos._tcp.EXAMPLE.COM IN SRV 1 0 88 kdc1.example.com
_kerberos-adm._tcp.EXAMPLE.COM IN SRV 0 0 749 kdc1.example.com
_kpasswd._udp.EXAMPLE.COM IN SRV 0 0 749 kdc1.example.com
```

**Ejemplo 21–15** Configuración de un cliente Solaris para trabajar con un múltiplo KDC principal

El servicio Kerberos de Microsoft Active Directory, proporciona un KDC que se ejecuta en varios maestros. Para que un cliente Solaris pueda actualizar información la declaración `admin_server` o `kpasswd_server` en `/etc/krb5/krb5.conf` debe estar actualizada para mostrar todos los servidores. En este ejemplo, se muestra cómo permitir al cliente actualizar información en el KDC compartido entre `kdc1` y `kdc2`.

```
[realms]
EXAMPLE.COM = {
 kdc = kdc1.example.com
 kdc = kdc2.example.com
```

```
admin_server = kdc1.example.com
admin_server = kdc2.example.com
}
```

## ▼ Cómo desactivar la verificación del ticket de otorgamiento de tickets

Este procedimiento desactiva la comprobación de seguridad que comprueba que el KDC del principal de host almacenado en el archivo `/etc/krb5/krb5.keytab` local sea el mismo KDC que ha emitido el ticket de otorgamiento de tickets (TGT). Esta comprobación impide ataques de falsificación de DNS. Sin embargo, para algunas configuraciones de clientes, el principal host puede no estar disponible, por lo que esta comprobación debería ser desactivada para permitir que el cliente funcione. Éstas son las configuraciones que requieren que esta comprobación esté desactivada:

- La dirección IP del cliente se asigna dinámicamente. Por ejemplo, un cliente DHCP.
- El cliente no está configurado para hospedar servicios, por lo que no se ha creado ningún principal host.
- La clave del host no se almacena en el cliente.

**Antes de empezar** Debe asumir el rol root. Para obtener más información, consulte [“Cómo usar los derechos administrativos que tiene asignados” en la página 164](#).

### ● Cambie el archivo `krb5.conf`.

Si la opción `verify_ap_req_nofail` se establece en `false`, el proceso de verificación de TGT no está activado. Consulte la página del comando `man krb5.conf(4)` para obtener más información sobre esta opción.

```
client # cat /etc/krb5/krb5.conf
[libdefaults]
 default_realm = EXAMPLE.COM
 verify_ap_req_nofail = false
...
```

---

**Nota** – La opción `verify_ap_req_nofail` se puede introducir en la sección `[libdefaults]` o `[realms]` del archivo `krb5.conf`. Si la opción está en la sección `[libdefaults]`, el valor se utiliza para todos los dominios. Si la opción está en la sección `[realms]`, el valor sólo se aplica al dominio definido.

---

## ▼ Cómo acceder a un sistema de archivos NFS protegido con Kerberos como el usuario root

Este procedimiento permite a un cliente acceder a un sistema de archivos NFS que requiere la autenticación Kerberos con el privilegio de ID root. En particular, cuando el sistema de archivos NFS está compartido con opciones, como: `-o sec=krb5, root=client1.sun.com`.

### ● Inicie kadmin.

Si desea obtener información sobre cómo utilizar la herramienta de interfaz gráfica de usuario de administración de Kerberos para agregar un principal, consulte [“Cómo crear un nuevo principal de Kerberos” en la página 482](#). Para ello, debe iniciar sesión con uno de los nombres de principales admin que creó cuando configuró el KDC maestro. Sin embargo, el siguiente ejemplo muestra cómo agregar los principales necesarios mediante la línea de comandos.

```
denver # /usr/sbin/kadmin -p kws/admin
Enter password: <Type kws/admin password>
kadmin:
```

#### a. Cree un principal root para el cliente NFS.

Este principal se utiliza para proporcionar acceso equivalente a root a sistemas de archivos montados en NFS que requieren la autenticación Kerberos. El principal root debe ser un principal de dos componentes, donde el segundo componente es el nombre de host del sistema cliente Kerberos, para evitar la creación de un principal root de todo el dominio. Tenga en cuenta que cuando la instancia de principal es un nombre de host, el FQDN se debe especificar en letras minúsculas, independientemente de si el nombre de dominio está en mayúsculas o minúsculas en el servicio de nombres.

```
kadmin: addprinc -randkey root/client.example.com
Principal "root/client.example.com" created.
kadmin:
```

#### b. Agregue el principal root al archivo keytab del servidor.

Este paso es necesario si ha agregado un principal root para que el cliente pueda tener acceso root a sistemas de archivos montados mediante el servicio NFS. Este paso también es necesario si se necesita acceso root no interactivo, por ejemplo, la ejecución de trabajos cron como root.

```
kadmin: ktadd root/client.example.com
Entry for principal root/client.example.com with kvno 3, encryption type AES-256 CTS mode
with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal root/client.example.com with kvno 3, encryption type AES-128 CTS mode
with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal root/client.example.com with kvno 3, encryption type Triple DES cbc
mode with HMAC/sha1 added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal root/client.example.com with kvno 3, encryption type ArcFour
with HMAC/md5 added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal root/client.example.com with kvno 3, encryption type DES cbc mode
with RSA-MD5 added to keytab WRFILE:/etc/krb5/krb5.keytab.
kadmin:
```

**c. Salga de kadmin.**

```
kadmin: quit
```

## ▼ Cómo configurar la migración automática de usuarios en un dominio Kerberos

Los usuarios, que no tienen un principal de Kerberos, se pueden migrar automáticamente a un dominio Kerberos existente. La migración se logra utilizando la estructura PAM para el servicio en uso mediante el apilamiento del módulo `pam_krb5_migrate` en la pila de autenticación del servicio, en los archivos de configuración de PAM.

En este ejemplo, los nombres de servicio PAM `gdm` y `other` se configuran para usar la migración automática. Se utilizan los siguientes parámetros de configuración:

- Nombre de dominio = `EXAMPLE.COM`
- KDC maestro = `kdc1.example.com`
- Equipo que hospeda el servicio de migración = `server1.example.com`
- Principal de servicio de migración = `host/server1.example.com`

**Antes de empezar**

Configure `server1` como un cliente Kerberos del dominio `EXAMPLE.COM`. Consulte [“Configuración de clientes Kerberos” en la página 405](#) para obtener más información.

Debe asumir el rol `root`. Para obtener más información, consulte [“Cómo usar los derechos administrativos que tiene asignados” en la página 164](#).

**1 Compruebe si existe un principal de servicio de host para server1.**

El principal de servicio de host en el archivo `keytab` de `server1` se utiliza para autenticar el servidor en el KDC maestro.

```
server1 # klist -k
Keytab name: FILE:/etc/krb5/krb5.keytab
KVNO Principal

 3 host/server1.example.com@EXAMPLE.COM
 3 host/server1.example.com@EXAMPLE.COM
 3 host/server1.example.com@EXAMPLE.COM
 3 host/server1.example.com@EXAMPLE.COM
```

**2 Realice cambios en el archivo de configuración de PAM.****a. Actualice las entradas del servicio gdm.**

```
cat /etc/pam.d/gdm
.
.

auth definitive pam_user_policy.so.1
auth requisite pam_authtok_get.so.1
```



```

auth required pam_dhkeys.so.1
auth sufficient pam_krb5.so.1
auth requisite pam_unix_auth.so.1
auth required pam_unix_cred.so.1
auth optional pam_krb5_migrate.so.1

```

**b. (Opcional) Fuerce un cambio inmediato de contraseña si es necesario.**

Las cuentas de Kerberos recién creadas pueden tener el tiempo de caducidad de contraseña establecido en la hora actual (ahora) para forzar un cambio inmediato de contraseña Kerberos. Para establecer el tiempo de caducidad en la hora actual, agregue la opción `expire_pw` a las líneas que utilizan el módulo `pam_krb5_migrate`. Consulte la página del comando `man pam_krb5_migrate(5)` para obtener más información.

```

cat /etc/pam.d/gdm
.
.
auth optional pam_krb5_migrate.so.1 expire_pw

```

**c. Agregue el módulo `pam_krb5` a la pila de cuentas.**

Esta adición permite la caducidad de la contraseña en Kerberos para bloquear el acceso.

```

cat /etc/pam.d/other
.
.
#
Default definition for Account management
Used when service name is not explicitly mentioned for account management
#
account requisite pam_roles.so.1
account definitive pam_user_policy.so.1
account required pam_krb5.so.1
account required pam_unix_account.so.1
account required pam_tsol_account.so.1
#

```

**d. Agregue el módulo `pam_krb5` a la pila de contraseñas.**

Esta adición permite que las contraseñas se actualicen cuando la contraseña caduca.

```

cat /etc/pam.d/other
.
.
#
Default definition for Password management
#
password include pam_authtok_common
password sufficient pam_krb5.so.1
password required pam_authtok_store.so.1

```

**3 En el KDC maestro, actualice el archivo de control de acceso.**

Las entradas siguientes otorgan privilegios de migración y consulta al principal de servicio `host/server1.example.com` para todos los usuarios, excepto el usuario `root`. Es importante que los usuarios que no se deben migrar se enumeren en el archivo `kadm5.acl` utilizando el

privilegio U. Estas entradas deben estar antes de la entrada ui o permitir todo. Consulte la página del comando man `kadm5.acl(4)` para obtener más información.

```
kdc1 # cat /etc/krb5/kadm5.acl
host/server1.example.com@EXAMPLE.COM U root
host/server1.example.com@EXAMPLE.COM ui *
*/admin@EXAMPLE.COM *
```

#### 4 En el KDC maestro, reinicie el daemon de administración Kerberos.

Este paso permite al daemon `kadmind` utilizar las nuevas entradas `kadm5.acl`.

```
kdc1 # svcadm restart network/security/kadmin
```

#### 5 En el KDC maestro, agregue entradas al archivo `pam.conf`.

Las entradas siguientes permiten que el daemon `kadmind` utilice el servicio PAM `k5migrate` para validar la contraseña de usuario de UNIX para las cuentas que necesitan migración.

```
grep k5migrate /etc/pam.conf
k5migrate auth required pam_unix_auth.so.1
k5migrate account required pam_unix_account.so.1
```

## ▼ Cómo configurar el bloqueo de cuenta

### ● Inicie `kadmin`.

```
% /usr/sbin/kadmin -p kws/admin
Enter password: <Type kws/admin password>
kadmin:
```

#### a. Cree una política con parámetros de bloqueo de cuenta.

En el ejemplo siguiente, el subcomando `add_policy` se utiliza para crear una política denominada `default`. Tres fallos de autenticación durante un máximo de 300 segundos provocarán un bloqueo de cuenta de 900 segundos.

```
kadmin: add_policy -maxfailure 3 -failurecountinterval "300 seconds" \
-lockoutduration "900 seconds" default
```

#### b. Salga de `kadmin`.

```
kadmin: quit
```

### Ejemplo 21–16 Desbloqueo de principal bloqueado

En el siguiente ejemplo, un principal de usuario se desbloquea:

```
/usr/sbin/kadmin -p kws/admin
Enter password: <Type kws/admin password>
kadmin: modify_principal -unlock principal
```

## ▼ Cómo renovar automáticamente todos los tickets de otorgamiento de tickets (TGT)

### Antes de empezar

Debe asumir el rol root. Para obtener más información, consulte [“Cómo usar los derechos administrativos que tiene asignados” en la página 164](#).

#### 1 Edite el archivo de configuración warnd.

Agregue una entrada como la siguiente para renovar el TGT 30 minutos antes de que el ticket caduque y registre el mensaje en los terminales de usuario cuando la renovación falle o se realice correctamente:

```
cat /etc/krb5/warn.conf
* renew:log terminal 30m
```

#### 2 Reinicie el servicio.

```
svcadm restart network/security/ktkt_warn
```

### Ejemplo 21-17 Configuración de mensajes de caducidad de TGT en un servidor

El siguiente ejemplo muestra varias formas de configurar la renovación y el sistema de mensajes para TGT.

```
cat /etc/krb5/warn.conf
#
renew the TGT 30 minutes before expiration and send message to users terminal
#
gtb@EXAMPLE.COM renew:log terminal 30m
#
send a warning message to a specific email address 20 minutes before TGT expiration
#
mre@EXAMPLE.COM mail 20m mre@example2.com
#
renew the TGT 20 minutes before expiration and send an email message on failure
#
bricker@EXAMPLE.COM renew:log-failure mail 20m &
#
catch-all: any principal not matched above will get an email warning
* mail 20m &
```

### Ejemplo 21-18 Configuración de mensajes de caducidad de TGT para un usuario

Además de configurar una entrada para cada usuario en el nivel del sistema, cada usuario puede configurar un archivo de configuración warnd individual, que se denomina `/var/user/$USER/krb-warn.conf`. Por ejemplo:

```
% cat /var/user/gtb/krb-warn.conf
gtb@EXAMPLE.COM renew:log mail 30m &
```

## Sincronización de relojes entre clientes Kerberos y KDC

Todos los hosts que participan en el sistema de autenticación Kerberos deben tener los relojes internos sincronizados dentro de una cantidad de tiempo máxima especificada (conocida como *desfase de reloj*). Este requisito proporciona otra comprobación de seguridad de Kerberos. Si el desfase del reloj se supera entre cualquiera de los hosts que participan, las solicitudes de los clientes se rechazan.

El desfase del reloj también determina el tiempo durante el cual los servidores de aplicaciones deben realizar un seguimiento de todos los mensajes del protocolo Kerberos a fin de reconocer y rechazar solicitudes reproducidas. Por lo tanto, cuanto más grande es el valor del desfase del reloj, más información tienen que recopilar los servidores de aplicaciones.

El valor predeterminado para el desfase máximo del reloj es de 300 s (5 min). Puede cambiar este valor predeterminado en la sección `libdefaults` del archivo `krb5.conf`.

---

**Nota** – Por motivos de seguridad, no aumente el desfase del reloj más allá de 300 s.

---

Debido a que mantener los relojes sincronizados entre los clientes Kerberos y los KDC es importante, debe utilizar el software de protocolo de hora de red (NTP) para sincronizarlos. El software de dominio público NTP de la Universidad de Delaware se incluye en el software Oracle Solaris.

---

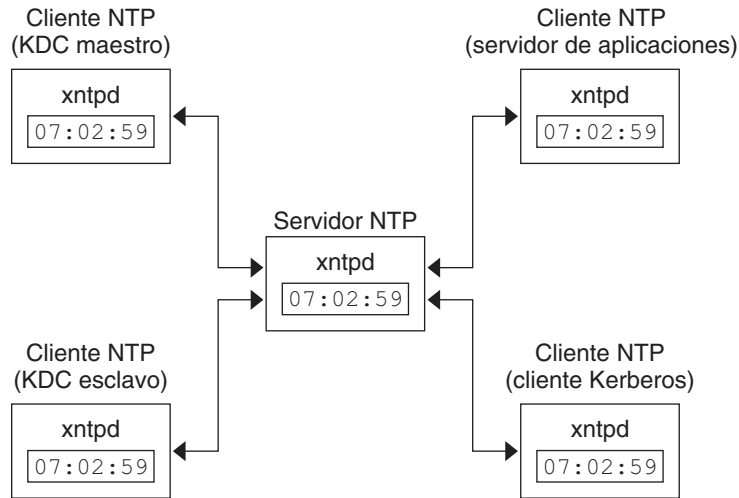
**Nota** – Otra forma de sincronizar los relojes es utilizar el comando `rdate` y los trabajos `cron`, un proceso que puede ser menos involucrado que utilizar el NTP. Sin embargo, esta sección se centra en el uso del NTP. Y, si utiliza la red para sincronizar los relojes, el protocolo de sincronización de relojes debe ser seguro.

---

El NTP permite gestionar la sincronización de relojes de red o el tiempo preciso, o ambos, en un entorno de red. El NTP es, básicamente, una implementación de servidor y cliente. Elija un sistema para que sea el reloj maestro (el servidor NTP). A continuación, configure todos los otros sistemas (los clientes NTP) para sincronizar sus relojes con el reloj principal.

Para sincronizar los relojes, el NTP utiliza el daemon `xntpd`, que establece y mantiene una hora del día del sistema UNIX de acuerdo con los servidores de hora estándar de Internet. A continuación, se muestra un ejemplo de esta implementación de NTP de servidor y cliente.

FIGURA 21-1 Sincronización de relojes mediante el NTP



Asegurarse de que los clientes Kerberos y los KDC mantengan relojes sincronizados implica la implementación de los siguientes pasos:

1. Configure un servidor NTP en la red. Este servidor puede ser cualquier sistema, excepto el KDC maestro. Consulte [“Gestión del protocolo de hora de red \(tareas\)” de Introducción a los servicios de red de Oracle Solaris 11](#) para buscar la tarea del servidor NTP.
2. Al realizar la configuración de los clientes Kerberos y los KDC en la red, configúrelos para que sean clientes NTP del servidor NTP. Consulte [“Gestión del protocolo de hora de red \(tareas\)” de Introducción a los servicios de red de Oracle Solaris 11](#) para buscar la tarea del cliente NTP.

## Intercambio de un KDC maestro y un KDC esclavo

Debe utilizar los procedimientos de esta sección para facilitar el intercambio de un KDC maestro con un KDC esclavo. Debe intercambiar el KDC maestro con un KDC esclavo sólo si el servidor KDC maestro falla por algún motivo o si el KDC maestro debe volver a instalarse (por ejemplo, porque se instaló un nuevo hardware).

### ▼ Cómo configurar un KDC esclavo intercambiable

Realice este procedimiento en el servidor KDC esclavo que desea que esté disponible para convertirse en el KDC maestro. Este procedimiento supone que utiliza la propagación incremental.

**Antes de empezar** Debe asumir el rol root. Para obtener más información, consulte [“Cómo usar los derechos administrativos que tiene asignados” en la página 164](#).

**1 Utilice nombres de alias para el KDC maestro y el KDC esclavo intercambiable durante la instalación del KDC.**

Al definir los nombres de host para los KDC, asegúrese de que cada sistema tenga un alias incluido en DNS. Asimismo, utilice los nombres de alias al definir los hosts en el archivo `/etc/krb5/krb5.conf`.

**2 Siga los pasos para instalar un KDC esclavo.**

Antes de realizar un intercambio, este servidor debe funcionar como cualquier otro KDC esclavo en el dominio. Consulte [“Cómo configurar manualmente un KDC esclavo” en la página 388](#) para obtener instrucciones.

**3 Mueva los comandos del KDC maestro.**

Para evitar que los comandos del KDC maestro se ejecuten desde este KDC esclavo, mueva los comandos `kprop`, `kadmin` y `kadmin.local` a un lugar reservado.

```
kdc4 # mv /usr/lib/krb5/kprop /usr/lib/krb5/kprop.save
kdc4 # mv /usr/lib/krb5/kadmin /usr/lib/krb5/kadmin.save
kdc4 # mv /usr/sbin/kadmin.local /usr/sbin/kadmin.local.save
```

## ▼ **Cómo intercambiar un KDC maestro y un KDC esclavo**

En este procedimiento, el servidor KDC maestro que se está intercambiando se denomina `kdc1`. El KDC esclavo que se convertirá en el nuevo KDC maestro se denomina `kdc4`. Este procedimiento supone que utiliza la propagación incremental.

**Antes de empezar** Este procedimiento requiere que el servidor KDC esclavo se haya configurado como un esclavo intercambiable. Para obtener más información, consulte [“Cómo configurar un KDC esclavo intercambiable” en la página 425](#)).

Debe asumir el rol root. Para obtener más información, consulte [“Cómo usar los derechos administrativos que tiene asignados” en la página 164](#).

**1 En el nuevo KDC maestro, inicie kadmin.**

```
kdc4 # /usr/sbin/kadmin -p kws/admin
Enter password: <Type kws/admin password>
kadmin:
```

**a. Cree nuevos principales para el servicio kadmind.**

El ejemplo siguiente muestra el primer comando `addprinc` en dos líneas, pero debe escribirse en una línea.

```
kadmin: addprinc -randkey -allow_tgs_req +password_changing_service -clearpolicy \
changepw/kdc4.example.com
Principal "changepw/kdc4.example.com@ENG.SUN.COM" created.
kadmin: addprinc -randkey -allow_tgs_req -clearpolicy kadmin/kdc4.example.com
Principal "kadmin/kdc4.example.com@EXAMPLE.COM" created.
kadmin:
```

**b. Salga de kadmin.**

```
kadmin: quit
```

**2 En el nuevo KDC maestro, fuerce la sincronización.**

Los siguientes pasos fuerzan una actualización completa del KDC en el servidor esclavo.

```
kdc4 # svcadm disable network/security/krb5kdc
kdc4 # rm /var/krb5/principal.ulong
```

**3 En el nuevo KDC maestro, verifique que la actualización se haya completado.**

```
kdc4 # /usr/sbin/kproplog -h
```

**4 En el nuevo KDC maestro, reinicie el servicio KDC.**

```
kdc4 # svcadm enable -r network/security/krb5kdc
```

**5 En el nuevo KDC maestro, borre el registro de actualización.**

Estos pasos reinician el registro de actualización para el nuevo servidor KDC maestro.

```
kdc4 # svcadm disable network/security/krb5kdc
kdc4 # rm /var/krb5/principal.ulong
```

**6 En el KDC maestro antiguo, termine los procesos kadmind y krb5kdc.**

Al terminar el proceso `kadmind`, evita que se realicen cambios en la base de datos del KDC.

```
kdc1 # svcadm disable network/security/kadmin
kdc1 # svcadm disable network/security/krb5kdc
```

**7 En el KDC maestro antiguo, especifique el tiempo de sondeo para solicitar propagaciones.**

Elimine el comentario de la entrada `sunw_dbprop_master_ologsize` en `/etc/krb5/kdc.conf` y agregue una entrada que defina `sunw_dbprop_slave_poll`. La entrada establece el tiempo de sondeo en dos minutos.

```
kdc1 # cat /etc/krb5/kdc.conf
[kdcdefaults]
 kdc_ports = 88,750
```

```
[realms]
 EXAMPLE.COM= {
 profile = /etc/krb5/krb5.conf
 database_name = /var/krb5/principal
 acl_file = /etc/krb5/kadm5.acl
 kadmind_port = 749
 max_life = 8h 0m 0s
 max_renewable_life = 7d 0h 0m 0s
 sunw_dbprop_enable = true
 sunw_dbprop_master_ulogsize = 1000
 sunw_dbprop_slave_poll = 2m
 }
```

## 8 En el KDC maestro antiguo, mueva los comandos del KDC maestro y el archivo `kadm5.acl`.

Para evitar que los comandos del KDC maestro se ejecuten, mueva los comandos `kprop`, `kadmind` y `kadmin.local` a un lugar reservado.

```
kdc1 # mv /usr/lib/krb5/kprop /usr/lib/krb5/kprop.save
kdc1 # mv /usr/lib/krb5/kadmind /usr/lib/krb5/kadmind.save
kdc1 # mv /usr/sbin/kadmin.local /usr/sbin/kadmin.local.save
kdc1 # mv /etc/krb5/kadm5.acl /etc/krb5/kadm5.acl.save
```

## 9 En el servidor DNS, cambie los nombres de alias del KDC maestro.

Para cambiar los servidores, edite el archivo de zona `example.com` y cambie la entrada para `masterkdc`.

```
masterkdc IN CNAME kdc4
```

## 10 En el servidor DNS, reinicie el servidor de nombres de dominio de Internet.

Ejecute el siguiente comando para volver a cargar la nueva información de alias:

```
svcadm refresh network/dns/server
```

## 11 En el nuevo KDC maestro, mueva los comandos del KDC maestro y el archivo `kpropd.acl` esclavo.

```
kdc4 # mv /usr/lib/krb5/kprop.save /usr/lib/krb5/kprop
kdc4 # mv /usr/lib/krb5/kadmind.save /usr/lib/krb5/kadmind
kdc4 # mv /usr/sbin/kadmin.local.save /usr/sbin/kadmin.local
kdc4 # mv /etc/krb5/kpropd.acl /etc/krb5/kpropd.acl.save
```

## 12 En el nuevo KDC maestro, cree el archivo de la lista de control de acceso de Kerberos (`kadm5.acl`).

Una vez que se rellena, el archivo `/etc/krb5/kadm5.acl` debe contener todos los nombres de principales que tienen permitido administrar el KDC. El archivo también debe mostrar todos los esclavos que realizan solicitudes de propagación incremental. Consulte la página del comando `man kadm5.acl(4)` para obtener más información.

```
kdc4 # cat /etc/krb5/kadm5.acl
kws/admin@EXAMPLE.COM *
kiprop/kdc1.example.com@EXAMPLE.COM p
```



### 13 En el nuevo KDC maestro, especifique el tamaño de registro de actualización en el archivo `kdc.conf`.

Elimine el comentario de la entrada `sunw_dbprop_slave_poll` y agregue una entrada que defina `sunw_dbprop_master_ulogsize`. La entrada establece el tamaño de registro en 1000 entradas.

```
kdc1 # cat /etc/krb5/kdc.conf
[kdcdefaults]
 kdc_ports = 88,750

[realms]
 EXAMPLE.COM= {
 profile = /etc/krb5/krb5.conf
 database_name = /var/krb5/principal
 acl_file = /etc/krb5/kadm5.acl
 kadmind_port = 749
 max_life = 8h 0m 0s
 max_renewable_life = 7d 0h 0m 0s
 sunw_dbprop_enable = true
 sunw_dbprop_slave_poll = 2m
 sunw_dbprop_master_ulogsize = 1000
 }
```

### 14 En el KDC maestro antiguo, inicie `kadmind` y `krb5kdc`.

```
kdc4 # svcadm enable -r network/security/krb5kdc
kdc4 # svcadm enable -r network/security/kadmind
```

### 15 En el KDC maestro antiguo, agregue el principal de servicio `kiprop`.

La adición del principal `kiprop` al archivo `krb5.keytab` permite que el daemon `kpropd` se autentique para el servicio de propagación incremental.

```
kdc1 # /usr/sbin/kadmin -p kws/admin
Authenticating as principal kws/admin@EXAMPLE.COM with password.
Enter password: <Type kws/admin password>
kadmin: ktadd kiprop/kdc1.example.com
Entry for principal kiprop/kdc1.example.com with kvno 3, encryption type AES-256 CTS mode
with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal kiprop/kdc1.example.com with kvno 3, encryption type AES-128 CTS mode
with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal kiprop/kdc1.example.com with kvno 3, encryption type Triple DES cbc
mode with HMAC/sha1 added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal kiprop/kdc1.example.com with kvno 3, encryption type ArcFour
with HMAC/md5 added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal kiprop/kdc1.example.com with kvno 3, encryption type DES cbc mode
with RSA-MD5 added to keytab WRFILE:/etc/krb5/krb5.keytab.
kadmin: quit
```

### 16 En el KDC maestro antiguo, agregue una entrada para cada KDC que aparece en `krb5.conf` al archivo de configuración de propagación, `kpropd.acl`.

```
kdc1 # cat /etc/krb5/kpropd.acl
host/kdc1.example.com@EXAMPLE.COM
```

```
host/kdc2.example.com@EXAMPLE.COM
host/kdc3.example.com@EXAMPLE.COM
host/kdc4.example.com@EXAMPLE.COM
```

**17 En el KDC maestro antiguo, inicie kpropd y krb5kdc.**

```
kdc1 # svcadm enable -r network/security/krb5_prop
kdc1 # svcadm enable -r network/security/krb5kdc
```

## Administración de la base de datos de Kerberos

La base de datos de Kerberos es la red principal de Kerberos y se debe mantener correctamente. En esta sección, se proporcionan algunos procedimientos sobre cómo administrar la base de datos de Kerberos, como la copia de seguridad y restauración de la base de datos, la configuración de la propagación incremental o en paralelo, y la administración del archivo intermedio. Los pasos para configurar inicialmente la base de datos se detallan en [“Cómo configurar manualmente un KDC maestro” en la página 376](#).

### Copia de seguridad y propagación de la base de datos de Kerberos

La propagación de la base de datos de Kerberos desde el KDC maestro hasta los KDC esclavos es una de las tareas de configuración más importantes. Si la propagación no ocurre con suficiente frecuencia, el KDC maestro y los KDC esclavos pierden la sincronización. Por lo tanto, si el KDC maestro deja de funcionar, los KDC esclavos no tendrán la información más reciente de la base de datos. Además, si un KDC esclavo se ha configurado como un KDC maestro con fines de equilibrio de carga, los clientes que utilicen ese KDC esclavo como KDC maestro no tendrán la información más reciente. Por lo tanto, debe asegurarse de que la propagación se produzca con suficiente frecuencia o configurar los servidores para la propagación incremental en función de la frecuencia con la que se cambia la base de datos de Kerberos. La propagación incremental se prefiere frente a la propagación manual porque hay más sobrecarga administrativa cuando se propaga manualmente la base de datos. También hay ineficacias cuando se realiza la propagación completa de la base de datos.

Al configurar el KDC maestro, se configura el comando `kprop_script` en un trabajo `cron` para realizar automáticamente una copia de seguridad de la base de datos de Kerberos en el archivo de volcado `/var/krb5/slave_datatrans` y propagarlo a los KDC esclavos. No obstante, como con cualquier archivo, la base de datos de Kerberos puede dañarse. Si se dañan los datos en un KDC esclavo, es posible que nunca lo note, porque la próxima propagación automática de la base de datos instala una copia nueva. Sin embargo, si se dañan los datos en el KDC maestro, la base de datos dañada se propaga a todos los KDC esclavos durante la siguiente propagación. Por lo tanto, la copia de seguridad dañada sobrescribe el archivo de copia de seguridad anterior que no está dañado en el KDC maestro.

Debido a que no hay ninguna copia de seguridad “segura” en este escenario, también debe configurar un trabajo `cron` para copiar periódicamente el archivo de volcado `slave_datatrans` en otra ubicación o para crear otra copia de seguridad separada mediante el comando `dump` de `kdb5_util`. De este modo, si se daña su base de datos, puede restaurar la copia de seguridad más reciente en el KDC maestro mediante el comando `load` de `kdb5_util`.

Otra nota importante: debido a que el archivo de volcado de la base de datos contiene claves de principales, necesita proteger el archivo contra el acceso de usuarios no autorizados. De manera predeterminada, el archivo de volcado de la base de datos tiene permisos de lectura y escritura sólo como `root`. Para protegerlo contra el acceso no autorizado, utilice sólo el comando `kprop` para propagar el archivo de volcado de la base de datos, que cifra los datos que se transfieren. Además, `kprop` propaga los datos sólo a los KDC esclavos, lo cual minimiza la posibilidad de enviar accidentalmente el archivo de volcado de la base de datos a hosts no autorizados.



---

**Precaución** – Si la base de datos de Kerberos se actualiza después de ser propagada y si la base se daña posteriormente antes de la siguiente propagación, los KDC esclavos no contendrán las actualizaciones. Las actualizaciones se perderán. Por este motivo, si agrega actualizaciones importantes a la base de datos de Kerberos antes de una propagación programada con regularidad, debe propagar manualmente la base de datos para evitar pérdidas de datos.

---

## El archivo `kpropd.ac1`

El archivo `kpropd.ac1` en un KDC esclavo proporciona una lista de nombres de principales `host`, un nombre por línea, que especifica los sistemas desde los cuales el KDC puede recibir una base de datos actualizada mediante la propagación. Si el KDC maestro se utiliza para propagar todos los KDC esclavos, el archivo `kpropd.ac1` de cada esclavo necesita contener sólo el nombre del principal `host` del KDC maestro.

Sin embargo, la instalación de Kerberos y los pasos de configuración posteriores en este manual le indican que agregue el mismo archivo `kpropd.ac1` al KDC maestro y a los KDC esclavos. Este archivo contiene todos los nombres de principales `host` del KDC. Esta configuración permite propagar desde cualquier KDC, en caso de que los KDC que se propagan no estén disponibles temporalmente. De este modo, al conservar una copia idéntica en todos los KDC, hace que la configuración sea fácil de mantener.

## El comando `kprop_script`

El comando `kprop_script` usa el comando `kprop` para propagar la base de datos de Kerberos a otros KDC. Si el comando `kprop_script` se ejecuta en un KDC esclavo, propaga la copia del KDC esclavo de la base de datos de Kerberos a otros KDC. El comando `kprop_script` acepta una lista de nombres de `host` para argumentos, separados por espacios, que indican los KDC para propagar.

Cuando `kprop_script` se ejecuta, crea una copia de seguridad de la base de datos de Kerberos en el archivo `/var/krb5/slave_datatrans` y copia el archivo en los KDC especificados. La base de datos de Kerberos se bloquea hasta que la propagación se termina.

## ▼ Cómo realizar copias de seguridad de la base de datos de Kerberos

**Antes de empezar** Debe asumir el rol root. Para obtener más información, consulte [“Cómo usar los derechos administrativos que tiene asignados” en la página 164.](#)

- Realice una copia de seguridad de la base de datos de Kerberos mediante el comando `dump` del comando `kdb5_util`.

```
/usr/sbin/kdb5_util dump [-verbose] [-d dbname] [filename [principals...]]
```

*-verbose* Imprime el nombre de cada principal y política a los que se está realizando una copia de seguridad.

*nombre\_base\_datos* Define el nombre de la base de datos para realizar copia de seguridad. Tenga en cuenta que puede especificar una ruta absoluta para el archivo. Si la opción `-d` no está especificada, el nombre de la base de datos predeterminado es `/var/krb5/principal`.

*nombre\_archivo* Define el archivo que se utiliza para realizar la copia de seguridad de la base de datos. Puede especificar una ruta absoluta para el archivo. Si no especifica un archivo, la base de datos se vuelca a una salida estándar.

*principales* Define una lista de uno o más principales (separados por un espacio) para realizar copia de seguridad. Debe utilizar nombres completos de principales. Si no especifica ningún principal, se realiza una copia de seguridad de la base de datos completa.

### Ejemplo 21–19 Copia de seguridad de la base de datos de Kerberos

En el siguiente ejemplo, se realiza una copia de seguridad de la base de datos de Kerberos en un archivo denominado `dumpfile`. Debido a que la opción `-verbose` está especificada, cada principal se imprime a medida que se le realiza una copia de seguridad.

```
kdb5_util dump -verbose dumpfile
kadmin/kdc1.eng.example.com@ENG.EXAMPLE.COM
krbtgt/ENG.EXAMPLE.COM@ENG.EXAMPLE.COM
kadmin/history@ENG.EXAMPLE.COM
pak/admin@ENG.EXAMPLE.COM
pak@ENG.EXAMPLE.COM
changepw/kdc1.eng.example.com@ENG.EXAMPLE.COM
```

En el ejemplo siguiente, se realiza una copia de seguridad de los principales `pak` y `pak/admin` de la base de datos de Kerberos.

```
kdb5_util dump -verbose dumpfile pak/admin@ENG.EXAMPLE.COM pak@ENG.EXAMPLE.COM
pak/admin@ENG.EXAMPLE.COM
pak@ENG.EXAMPLE.COM
```

## ▼ Cómo restaurar la base de datos de Kerberos

**Antes de empezar** En KDC maestro, debe asumir el rol root. Para obtener más información, consulte [“Cómo usar los derechos administrativos que tiene asignados” en la página 164](#).

### 1 En el maestro, detenga los daemons del KDC.

```
kdc1 # svcadm disable network/security/krb5kdc
kdc1 # svcadm disable network/security/kadmin
```

### 2 Restaure la base de datos de Kerberos mediante el comando `load` del comando `kdb_util`.

```
/usr/sbin/kdb5_util load [-verbose] [-d dbname] [-update] [filename]
```

`-verbose` Imprime el nombre de cada principal y política que se están restaurando.

`nombre_base_datos` Define el nombre de la base de datos para restaurar. Tenga en cuenta que puede especificar una ruta absoluta para el archivo. Si la opción `-d` no está especificada, el nombre de la base de datos predeterminado es `/var/krb5/principal`.

`-update` Actualiza la base de datos existente. De lo contrario, se crea una base de datos nueva o la base de datos existente se sobrescribe.

`nombre_archivo` Define el archivo desde el cual se va a restaurar la base de datos. Puede especificar una ruta absoluta para el archivo.

### 3 Inicie los daemons del KDC.

```
kdc1 # svcadm enable -r network/security/krb5kdc
kdc1 # svcadm enable -r network/security/kadmin
```

## Ejemplo 21–20 Restauración de la base de datos de Kerberos

En el ejemplo siguiente, la base de datos denominada `database1` se restaura en el directorio actual del archivo `dumpfile`. Debido a que la opción `-update` no está especificada, se crea una base de datos nueva con la restauración.

```
kdb5_util load -d database1 dumpfile
```

## ▼ Cómo convertir una base de datos de Kerberos después de una actualización de servidor

Si la base de datos del KDC se ha creado en un servidor que ejecuta la versión Solaris 8 o Solaris 9, la conversión de la base de datos permite aprovechar el formato de base de datos mejorado.

**Antes de empezar**

Asegúrese de que la base de datos esté utilizando un formato antiguo.

En KDC maestro, debe asumir el rol root. Para obtener más información, consulte [“Cómo usar los derechos administrativos que tiene asignados” en la página 164](#).

**1 En el maestro, detenga los daemons del KDC.**

```
kdc1 # svcadm disable network/security/krb5kdc
kdc1 # svcadm disable network/security/kadmin
```

**2 Cree un directorio para almacenar una copia temporal de la base de datos.**

```
kdc1 # mkdir /var/krb5/tmp
kdc1 # chmod 700 /var/krb5/tmp
```

**3 Vuelque la base de datos del KDC.**

```
kdc1 # kdb5_util dump /var/krb5/tmp/prdb.txt
```

**4 Guarde copias de los archivos de la base de datos actual.**

```
kdc1 # cd /var/krb5
kdc1 # mv princ* tmp/
```

**5 Cargue la base de datos.**

```
kdc1 # kdb5_util load /var/krb5/tmp/prdb.txt
```

**6 Inicie los daemons del KDC.**

```
kdc1 # svcadm enable -r network/security/krb5kdc
kdc1 # svcadm enable -r network/security/kadmin
```

## ▼ **Cómo reconfigurar un KDC maestro para utilizar la propagación incremental**

Los pasos de este procedimiento se pueden utilizar para volver a configurar un KDC maestro existente a fin de utilizar la propagación incremental. En este procedimiento, se utilizan los siguientes parámetros de configuración:

- Nombre de dominio = EXAMPLE.COM
- Nombre de dominio DNS = example.com
- KDC maestro = kdc1.example.com
- KDC esclavo = kdc2.example.com
- Principal admin = kws/admin

**Antes de empezar**

Debe asumir el rol root. Para obtener más información, consulte [“Cómo usar los derechos administrativos que tiene asignados” en la página 164](#).

## 1 Agregue entradas a `kdc.conf`.

Necesita activar la propagación incremental y seleccionar el número de actualizaciones que el KDC maestro mantiene en el registro. Consulte la página del comando `man kdc.conf(4)` para obtener más información.

```
kdc1 # cat /etc/krb5/kdc.conf
[kdcdefaults]
 kdc_ports = 88,750

[realms]
 EXAMPLE.COM= {
 profile = /etc/krb5/krb5.conf
 database_name = /var/krb5/principal
 acl_file = /etc/krb5/kadm5.acl
 kadmind_port = 749
 max_life = 8h 0m 0s
 max_renewable_life = 7d 0h 0m 0s
 sunw_dbprop_enable = true
 sunw_dbprop_master_ulogsize = 1000
 }
```

## 2 Cree el principal `kiprop`.

El principal `kiprop` se utiliza para autenticar el servidor KDC maestro y para autorizar las actualizaciones del KDC maestro.

```
kdc1 # /usr/sbin/kadmin -p kws/admin
Enter password: <Type kws/admin password>
kadmin: addprinc -randkey kiprop/kdc1.example.com
Principal "kiprop/kdc1.example.com@EXAMPLE.COM" created.
kadmin: addprinc -randkey kiprop/kdc2.example.com
Principal "kiprop/kdc2.example.com@EXAMPLE.COM" created.
kadmin:
```

## 3 En el KDC maestro, agregue una entrada `kiprop` a `kadm5.acl`.

Esta entrada permite que el KDC maestro reciba solicitudes de propagación incremental del servidor `kdc2`.

```
kdc1 # cat /etc/krb5/kadm5.acl
*/admin@EXAMPLE.COM *
kiprop/kdc2.example.com@EXAMPLE.COM p
```

## 4 Elimine el comentario de la línea `kprop` en el archivo `crontab root`.

Este paso impide que el KDC maestro propague su copia de la base de datos del KDC.

```
kdc1 # crontab -e
#ident "@(#)root 1.20 01/11/06 SMI"
#
The root crontab should be used to perform accounting data collection.
#
The rtc command is run to adjust the real time clock if and when
daylight savings time changes.
#
10 3 * * * /usr/sbin/logadm
```

```
15 3 * * 0 /usr/lib/fs/nfs/nfsfind
1 2 * * * [-x /usr/sbin/rtc] && /usr/sbin/rtc -c > /dev/null 2>&1
30 3 * * * [-x /usr/lib/gss/gsscred_clean] && /usr/lib/gss/gsscred_clean
#10 3 * * * /usr/lib/krb5kprop_script kdc2.example.sun.com #SUNWkr5ma
```

## 5 Reinicie kadmind.

```
kdc1 # svcadm restart network/security/kadmin
```

## 6 Reconfigure todos los servidores KDC esclavos que utilicen la propagación incremental.

Consulte [“Cómo reconfigurar un KDC esclavo para utilizar la propagación incremental” en la página 436](#) para obtener instrucciones completas.

# ▼ Cómo reconfigurar un KDC esclavo para utilizar la propagación incremental

**Antes de empezar** Debe asumir el rol root. Para obtener más información, consulte [“Cómo usar los derechos administrativos que tiene asignados” en la página 164](#).

## 1 Agregue entradas a kdc.conf.

La primera nueva entrada permite la propagación progresiva. La segunda nueva entrada establece el tiempo de sondeo en dos minutos.

```
kdc2 # cat /etc/krb5/kdc.conf
[kdcdefaults]
 kdc_ports = 88,750

[realms]
 EXAMPLE.COM= {
 profile = /etc/krb5/krb5.conf
 database_name = /var/krb5/principal
 acl_file = /etc/krb5/kadm5.acl
 kadmind_port = 749
 max_life = 8h 0m 0s
 max_renewable_life = 7d 0h 0m 0s
 sunw_dbprop_enable = true
 sunw_dbprop_slave_poll = 2m
 }
```

## 2 Agregue el principal kprop al archivo krb5.keytab.

```
kdc2 # /usr/sbin/kadmin -p kws/admin
Enter password: <Type kws/admin password>
kadmin: ktadd kprop/kdc2.example.com
Entry for principal kprop/kdc2.example.com with kvno 3, encryption type AES-256 CTS mode
with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal kprop/kdc2.example.com with kvno 3, encryption type AES-128 CTS mode
with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal kprop/kdc2.example.com with kvno 3, encryption type Triple DES cbc
```



```
mode with HMAC/sha1 added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal kiprop/kdc2.example.com with kvno 3, encryption type ArcFour
with HMAC/md5 added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal kiprop/kdc2.example.com with kvno 3, encryption type DES cbc mode
with RSA-MD5 added to keytab WRFILE:/etc/krb5/krb5.keytab.
kadmin: quit
```

### 3 Reinicie kpropd.

```
kdc2 # svcadm restart network/security/krb5_prop
```

## ▼ Cómo configurar un KDC esclavo para utilizar la propagación completa

En este procedimiento se muestra cómo reconfigurar un servidor KDC esclavo que ejecuta la versión Solaris 10 para utilizar la propagación completa. Normalmente, el procedimiento sólo se debe utilizar si el servidor KDC maestro ejecuta la versión Solaris 9 o una versión anterior. En este caso, el servidor KDC maestro no puede admitir la propagación incremental, por lo que el esclavo debe estar configurado para que la propagación funcione.

En este procedimiento, se configura un KDC esclavo denominado kdc3. Este procedimiento utiliza los siguientes parámetros de configuración:

- Nombre de dominio = EXAMPLE.COM
- Nombre de dominio DNS = example.com
- KDC maestro = kdc1.example.com
- KDC esclavo = kdc2.example.com y kdc3.example.com
- Principal admin = kws/admin
- URL de ayuda en pantalla =  
[http://docs.oracle.com/cd/E23824\\_01/html/821-1456/aadmin-23.html](http://docs.oracle.com/cd/E23824_01/html/821-1456/aadmin-23.html)

---

**Nota** – Ajuste la dirección URL para que establezca un enlace a la sección, como se describe en [“URL de ayuda en pantalla en la herramienta gráfica de administración de Kerberos” en la página 370](#).

---

#### Antes de empezar

El KDC maestro debe estar configurado. Para obtener instrucciones específicas si este esclavo se va a intercambiar, consulte [“Intercambio de un KDC maestro y un KDC esclavo” en la página 425](#).

En KDC maestro, debe asumir el rol root. Para obtener más información, consulte [“Cómo usar los derechos administrativos que tiene asignados” en la página 164](#).

**1 En el KDC maestro, inicie kadmin.**

Debe iniciar sesión con uno de los nombres de principales admin que creó cuando configuró el KDC maestro.

```
kdc1 # /usr/sbin/kadmin -p kws/admin
Enter password: <Type kws/admin password>
kadmin:
```

**a. En el KDC maestro, agregue principales host esclavos a la base de datos si aún no lo ha hecho.**

Para que el esclavo funcione, debe tener un principal host. Tenga en cuenta que cuando la instancia de principal es un nombre de host, el FQDN se debe especificar en letras minúsculas, independientemente de si el nombre de dominio está en mayúsculas o minúsculas en el servicio de nombres.

```
kadmin: addprinc -randkey host/kdc3.example.com
Principal "host/kdc3@EXAMPLE.COM" created.
kadmin:
```

**b. Salga de kadmin.**

```
kadmin: quit
```

**2 En el KDC maestro, edite el archivo de configuración de Kerberos (krb5.conf).**

Debe agregar una entrada para cada esclavo. Consulte la página del comando `man krb5.conf(4)` para obtener una descripción completa de este archivo.

```
kdc1 # cat /etc/krb5/krb5.conf
.
.
[realms]
 EXAMPLE.COM = {
 kdc = kdc1.example.com
 kdc = kdc2.example.com
 kdc = kdc3.example.com
 admin_server = kdc1.example.com
 }
```

**3 En el KDC maestro, agregue una entrada para el KDC maestro y cada KDC esclavo en el archivo kpropd.acl.**

Consulte la página del comando `man kpropd(1M)` para obtener una descripción completa de este archivo.

```
kdc1 # cat /etc/krb5/kpropd.acl
host/kdc1.example.com@EXAMPLE.COM
host/kdc2.example.com@EXAMPLE.COM
host/kdc3.example.com@EXAMPLE.COM
```

**4 En todos los KDC esclavos, copie los archivos de administración KDC del servidor KDC maestro.**

Este paso se debe realizar en todos los KDC esclavos, ya que el servidor KDC maestro ha actualizado información que cada servidor KDC necesita. Puede utilizar `ftp` o un mecanismo de transferencia similar para capturar copias de los siguientes archivos del KDC maestro:

- `/etc/krb5/krb5.conf`
- `/etc/krb5/kdc.conf`
- `/etc/krb5/kpropd.acl`

**5 En todos los KDC esclavos, asegúrese de que el archivo de la lista de control de acceso de Kerberos, `kadm5.acl`, no esté relleno.**

Un archivo `kadm5.acl` sin modificaciones sería de la siguiente manera:

```
kdc2 # cat /etc/krb5/kadm5.acl
*/admin@___default_realm___ *
```

Si el archivo tiene entradas `kprop`, elimínelas.

**6 En el nuevo esclavo, inicie el comando `kadmin`.**

Debe iniciar sesión con uno de los nombres de principales `admin` que creó cuando configuró el KDC maestro.

```
kdc2 # /usr/sbin/kadmin -p kws/admin
Enter password: <Type kws/admin password>
kadmin:
```

**a. Agregue el principal `host` del esclavo al archivo `keytab` del esclavo mediante `kadmin`.**

Esta entrada permite que `kprop` y otras aplicaciones Kerberizadas funcionen. Tenga en cuenta que cuando la instancia de principal es un nombre de `host`, el FQDN se debe especificar en letras minúsculas, independientemente de si el nombre de dominio está en mayúsculas o minúsculas en el servicio de nombres.

```
kadmin: ktadd host/kdc3.example.com
Entry for principal host/kdc3.example.com with kvno 3, encryption type AES-256 CTS mode
with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal host/kdc3.example.com with kvno 3, encryption type AES-128 CTS mode
with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal host/kdc3.example.com with kvno 3, encryption type Triple DES cbc
mode with HMAC/sha1 added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal host/kdc3.example.com with kvno 3, encryption type ArcFour
with HMAC/md5 added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal host/kdc3.example.com with kvno 3, encryption type DES cbc mode
with RSA-MD5 added to keytab WRFILE:/etc/krb5/krb5.keytab.
kadmin:
```

**b. Salga de `kadmin`.**

```
kadmin: quit
```

- 7 En el KDC maestro, agregue el nombre del KDC esclavo al trabajo cron, que ejecuta de forma automática las copias de seguridad, ejecutando crontab -e.**

Agregue el nombre de cada servidor KDC esclavo al final de la línea kprop\_script.

```
10 3 * * * /usr/lib/krb5/kprop_script kdc2.example.com kdc3.example.com
```

Es posible que también desee cambiar la hora de las copias de seguridad. Esta entrada inicia el proceso de copia de seguridad cada día a las 3:10 a. m.

- 8 En el nuevo esclavo, inicie el daemon de propagación de Kerberos.**

```
kdc3 # svcadm enable network/security/krb5_prop
```

- 9 En el KDC maestro, realice una copia de seguridad de la base de datos y propáguela mediante kprop\_script.**

Si ya hay disponible una copia de seguridad de la base de datos, no es necesario completar otra copia de seguridad. Consulte [“Cómo propagar manualmente la base de datos de Kerberos a los KDC esclavos” en la página 442](#) para obtener más instrucciones.

```
kdc1 # /usr/lib/krb5/kprop_script kdc3.example.com
Database propagation to kdc3.example.com: SUCCEEDED
```

- 10 En el nuevo esclavo, cree un archivo intermedio con kdb5\_util.**

```
kdc3 # /usr/sbin/kdb5_util stash
kdb5_util: Cannot find/read stored master key while reading master key
kdb5_util: Warning: proceeding without master key
```

Enter KDC database master key:      *<Type the key>*

- 11 (Opcional) En el nuevo KDC esclavo, sincronice el reloj del KDC maestro mediante NTP u otro mecanismo de sincronización de relojes.**

No es necesario instalar ni utilizar el protocolo de hora de red (NTP). Sin embargo, cada reloj debe estar dentro de la hora predeterminada que está definida en la sección libdefaults del archivo krb5.conf para que la autenticación se realice con éxito. Consulte [“Sincronización de relojes entre clientes Kerberos y KDC” en la página 424](#) para obtener información sobre el NTP.

- 12 En el nuevo esclavo, inicie el daemon del KDC (krb5kdc).**

```
kdc3 # svcadm enable network/security/krb5kdc
```

## ▼ **Cómo verificar que los servidores KDC estén sincronizados**

Si la propagación incremental se ha configurado, este procedimiento garantiza que la información en el KDC esclavo se ha actualizado.

**Antes de empezar** Debe asumir el rol root. Para obtener más información, consulte [“Cómo usar los derechos administrativos que tiene asignados” en la página 164.](#)

- 1 **En el servidor KDC maestro, ejecute el comando kproplog.**  
`kdc1 # /usr/sbin/kproplog -h`
- 2 **En un servidor KDC esclavo, ejecute el comando kproplog.**  
`kdc2 # /usr/sbin/kproplog -h`
- 3 **Compruebe que el último número de serie y los últimos valores de indicación de hora coincidan.**

### Ejemplo 21–21 Verificación de que los servidores KDC estén sincronizados

A continuación, se muestra un ejemplo de resultados de la ejecución del comando kproplog en el servidor KDC maestro.

```
kdc1 # /usr/sbin/kproplog -h

Kerberos update log (/var/krb5/principal.ulong)
Update log dump:
 Log version #: 1
 Log state: Stable
 Entry block size: 2048
 Number of entries: 2500
 First serial #: 137966
 Last serial #: 140465
 First time stamp: Fri Nov 28 00:59:27 2004
 Last time stamp: Fri Nov 28 01:06:13 2004
```

A continuación, se muestra un ejemplo de resultados de la ejecución del comando kproplog en un servidor KDC esclavo.

```
kdc2 # /usr/sbin/kproplog -h

Kerberos update log (/var/krb5/principal.ulong)
Update log dump:
 Log version #: 1
 Log state: Stable
 Entry block size: 2048
 Number of entries: 0
 First serial #: None
 Last serial #: 140465
 First time stamp: None
 Last time stamp: Fri Nov 28 01:06:13 2004
```

Tenga en cuenta que los valores para el último número de serie y la última indicación de hora son idénticos, lo que indica que el esclavo está sincronizado con el servidor KDC maestro.

En la salida del servidor KDC esclavo, observe que no existen entradas de actualización en el registro de actualización del servidor KDC esclavo. No existen entradas porque el servidor KDC

esclavo no conserva un conjunto de actualizaciones, a diferencia del servidor KDC maestro. Además, el servidor KDC esclavo no incluye información sobre el primer número de serie ni la primera indicación de hora porque no es información relevante.

## ▼ Cómo propagar manualmente la base de datos de Kerberos a los KDC esclavos

Este procedimiento muestra cómo propagar la base de datos de Kerberos mediante el comando `kprop`. Utilice este procedimiento si necesita sincronizar un KDC esclavo con el KDC maestro fuera del trabajo `cron` periódico. A diferencia de `kprop_script`, puede utilizar `kprop` para propagar sólo la copia de seguridad de la base de datos actual sin realizar primero una nueva copia de seguridad de la base de datos de Kerberos.

---

**Nota** – No utilice este procedimiento si está usando la propagación incremental.

---

**Antes de empezar** Debe asumir el rol `root`. Para obtener más información, consulte [“Cómo usar los derechos administrativos que tiene asignados” en la página 164](#).

- 1 (Opcional) Cree una copia de seguridad de la base de datos mediante el comando `kdb5_util`.  
`# /usr/sbin/kdb5_util dump /var/krb5/slave_datatrans`
- 2 Propague la base de datos a un KDC esclavo mediante el comando `kprop`.  
`# /usr/lib/krb5/kprop -f /var/krb5/slave_datatrans slave-KDC`

**Ejemplo 21–22** Propagación manual de la base de datos de Kerberos a los KDC esclavos mediante `kprop_script`

Si desea realizar una copia de seguridad de la base de datos y propagarla a un KDC esclavo fuera del trabajo `cron` periódico, también puede utilizar el comando `kprop_script`, como se indica a continuación:

```
/usr/lib/krb5/kprop_script slave-KDC
```

## Configuración de propagación en paralelo

En la mayoría de los casos, el KDC maestro se utiliza, exclusivamente, para propagar su base de datos de Kerberos a los KDC esclavos. Sin embargo, si su sitio tiene muchos KDC esclavos, es posible que deba considerar el uso compartido de carga del proceso de propagación, conocido como *propagación en paralelo*.

---

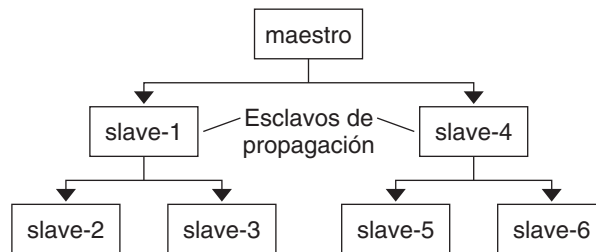
**Nota** – No utilice este procedimiento si está usando la propagación incremental.

---

La propagación en paralelo permite que KDC esclavos específicos compartan las tareas de propagación con el KDC maestro. Este uso compartido de tareas permite que la propagación se realice más rápido y alivie el trabajo para el KDC maestro.

Por ejemplo, suponga que su sitio tiene un KDC maestro y seis KDC esclavos (que se muestran en la [Figura 21–2](#)), donde del `slave-1` al `slave-3` constan de una agrupación lógica y del `slave-4` al `slave-6` constan de otra agrupación lógica. Para configurar la propagación en paralelo, puede hacer que el KDC maestro propague la base de datos al `slave-1` y al `slave-4`. A su vez, los KDC esclavos pueden propagar la base de datos a los KDC esclavos de su grupo.

FIGURA 21–2 Ejemplo de configuración de propagación en paralelo



## Pasos de configuración para la propagación en paralelo

A continuación, no se muestra un procedimiento detallado paso a paso, sino una lista de nivel superior con pasos de configuración para habilitar la propagación en paralelo. Estos pasos implican lo siguiente:

1. En el KDC maestro, cambie la entrada `kprop_script` en su trabajo `cron` a fin de incluir argumentos sólo para los KDC esclavos que realizarán la propagación subsiguiente (los *esclavos de propagación*).
2. En cada esclavo de propagación, agregue una entrada `kprop_script` a su trabajo `cron`, que debe incluir argumentos para que los esclavos se propaguen. Para propagar en paralelo correctamente, el trabajo `cron` se debe configurar para que se ejecute después de que el esclavo de propagación se propaga con la nueva base de datos de Kerberos.

---

**Nota** – El tiempo que tomará que un esclavo de propagación se propague depende de factores, como el ancho de banda de la red y el tamaño de la base de datos de Kerberos.

---

3. En cada KDC esclavo, configure los permisos adecuados que se van a propagar. Este paso se realiza mediante la adición del nombre del principal host del KDC de propagación al archivo `kpropd.acl`.

#### EJEMPLO 21-23 Configuración de propagación en paralelo

Mediante el ejemplo de la [Figura 21-2](#), la entrada `kprop_script` de los KDC maestros sería similar a la siguiente:

```
0 3 * * * /usr/lib/krb5/kprop_script slave-1.example.com slave-4.example.com
```

La entrada `kprop_script` de `slave-1` sería similar a la siguiente:

```
0 4 * * * /usr/lib/krb5/kprop_script slave-2.example.com slave-3.example.com
```

Tenga en cuenta que la propagación en el esclavo comienza una hora después de que es propagado por el maestro.

El archivo `kpropd.acl` en los esclavos de propagación contendría la siguiente entrada:

```
host/master.example.com@EXAMPLE.COM
```

El archivo `kpropd.acl` en los KDC esclavos que están siendo propagados por `slave-1` contendría la siguiente entrada:

```
host/slave-1.example.com@EXAMPLE.COM
```

## Administración del archivo intermedio

El *archivo intermedio* contiene la clave maestra para la base de datos de Kerberos, que se crea automáticamente al crear una base de datos de Kerberos. Si el archivo intermedio se daña, puede utilizar el comando `stash` de la utilidad `kdb5_util` para sustituir el archivo dañado. La única vez que debe eliminar un archivo intermedio es después de eliminar la base de datos de Kerberos con el comando `destroy` de `kdb5_util`. Debido a que el archivo intermedio no se elimina automáticamente con la base de datos, tiene que eliminarlo para finalizar la limpieza.

### ▼ Cómo eliminar un archivo intermedio

**Antes de empezar** Debe asumir el rol `root`. Para obtener más información, consulte [“Cómo usar los derechos administrativos que tiene asignados” en la página 164](#).

- **Elimine el archivo intermedio.**

```
rm stash-file
```



Donde *stash-file* es la ruta al archivo intermedio. De manera predeterminada, el archivo intermedio se encuentra en `/var/krb5/.k5.dominio`.

**Nota** – Si necesita volver a crear el archivo intermedio, puede utilizar la opción `-f` del comando `kdb5_util`.

## ▼ Cómo emplear una nueva clave maestra

**Antes de empezar** Debe asumir el rol `root`. Para obtener más información, consulte [“Cómo usar los derechos administrativos que tiene asignados” en la página 164](#).

### 1 Cree una nueva clave maestra.

Este comando agrega una nueva clave maestra generada aleatoriamente. La opción `-s` necesita que la nueva clave maestra se almacene en el archivo `keytab` predeterminado.

```
kdb5_util add_mkey -s
```

```
Creating new master key for master key principal 'K/M@EXAMPLE.COM'
You will be prompted for a new database Master Password.
It is important that you NOT FORGET this password.
Enter KDC database master key: <Type the password>
Re-enter KDC database master key to verify: <Type it again>
```

### 2 Verifique que exista la nueva clave maestra.

```
kdb5_util list_mkeys
Master keys for Principal: K/M@EXAMPLE.COM
KNVO: 2, Enctype: AES-128 CTS mode with 96-bit SHA-1 HMAC, No activate time set
KNVO: 1, Enctype: DES cbc mode with RSA-MD5, Active on: Wed Dec 31 18:00:00 CST 2001 *
```

El asterisco en esta salida identifica la clave maestra actualmente activa.

### 3 Defina un tiempo para que la clave maestra creada recientemente se active.

```
date
Fri Jul 1 17:57:00 CDT 2011
kdb5_util use_mkey 2 'now+2days'
kdb5_util list_mkeys
Master keys for Principal: K/M@EXAMPLE.COM
KNVO: 2, Enctype: AES-128 CTS mode with 96-bit SHA-1 HMAC, Active on: Sun Jul 03 17:57:15 CDT 2011
KNVO: 1, Enctype: DES cbc mode with RSA-MD5, Active on: Wed Dec 31 18:00:00 CST 2001 *
```

En este ejemplo, se define la fecha a dos días antes para darle tiempo a la nueva clave maestra a que se propague a todos los KDC. Ajuste la fecha de manera adecuada para su entorno.

### 4 (Opcional) Después de crear un principal nuevo, verifique que la nueva clave maestra esté en uso.

```
kadmin.local -q 'getprinc jimf' |egrep 'Principal|MKey'
Authenticating as principal root/admin@EXAMPLE.COM with password.
```

```
Principal: jimf@EXAMPLE.COM
MKey: vno 2
```

En este ejemplo, MKey: vno 2 indica que la clave secreta del principal está protegida por la clave maestra creada recientemente, 2.

## 5 Vuelva a cifrar las claves secretas de principal de usuario con la nueva clave maestra.

Si agregar un argumento de patrón al final del comando, los principales que coincidan con el patrón se actualizarán. Agregue la opción -n a esta sintaxis de comando para identificar qué principales se actualizarán.

```
kdb5_util update_princ_encryption -f -v
Principals whose keys WOULD BE re-encrypted to master key vno 2:
updating: host/kdc1.example.com@EXAMPLE.COM
skipping: jimf@EXAMPLE.COM
updating: kadmin/changepw@EXAMPLE.COM
updating: kadmin/history@EXAMPLE.COM
updating: kdc/admin@EXAMPLE.COM
updating: host/kdc2.example.com@EXAMPLE.COM
6 principals processed: 5 updated, 1 already current
```

## 6 Depure la clave maestra antigua.

Después de que una clave maestra ya no se utiliza para proteger ninguna clave secreta de principal, se puede depurar del principal de clave maestra. Este comando no depura la clave si la clave aún está siendo utilizada por algún principal. Agregue la opción -n a este comando para verificar que la clave maestra correcta se depurará.

```
kdb5_util purge_mkeys -f -v
Purging the follwing master key(s) from K/M@EXAMPLE.COM:
KNVO: 1
1 key(s) purged.
```

## 7 Verifique que la clave maestra antigua se ha depurado.

```
kdb5_util list_mkeys
Master keys for Principal: K/M@EXAMPLE.COM
KNVO: 2, Enctype: AES-128 CTS mode with 96-bit SHA-1 HMAC, Active on: Sun Jul 03 17:57:15 CDT 2011 *
```

## 8 Actualice el archivo intermedio.

```
kdb5_util stash
Using existing stashed keys to update stash file.
```

## 9 Verifique que el archivo intermedio se haya actualizado.

```
klist -kt /var/krb5/.k5.EXAMPLE.COM
Keytab name: FILE:.k5.EXAMPLE.COM
KVNO Timestamp Principal

2 05/07/2011 15:08 K/M@EXAMPLE.COM
```

# Gestión de un KDC en un servidor de directorios LDAP

La mayoría de las tareas de administración del KDC que usan un servidor de directorios LDAP son las mismas que las tareas para el servidor DB2. Hay algunas tareas nuevas que son específicas para trabajar con LDAP.

TABLA 21-3 Configuración de servidores KDC para utilizar LDAP (mapa de tareas)

| Tarea                                                                                              | Descripción                                                                                                                     | Para obtener instrucciones                                                                                                               |
|----------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------|
| Configurar un KDC maestro.                                                                         | Configura y genera el servidor KDC maestro y la base de datos para un dominio mediante un proceso manual y un LDAP para el KDC. | <a href="#">“Cómo configurar un KDC para utilizar un servidor de datos LDAP” en la página 380</a>                                        |
| Mezclar atributos de principales de Kerberos con tipos de clases de objeto que no son de Kerberos. | Permite que la información almacenada con los registros de Kerberos se comparta con otras bases de datos LDAP.                  | <a href="#">“Cómo mezclar atributos de principales de Kerberos en un tipo de clase de objeto que no es de Kerberos” en la página 447</a> |
| Destruir un dominio.                                                                               | Elimina todos los datos asociados con un dominio.                                                                               | <a href="#">“Cómo destruir un dominio en un servidor de directorios LDAP” en la página 448</a>                                           |

## ▼ Cómo mezclar atributos de principales de Kerberos en un tipo de clase de objeto que no es de Kerberos

Este procedimiento permite que los atributos de principales de Kerberos se asocien con tipos de clases de objeto que no son de Kerberos. En este procedimiento, los atributos `krbprincipalaux`, `krbTicketPolicyAux` y `krbPrincipalName` están asociados con la clase de objeto de personas.

En este procedimiento, se utilizan los siguientes parámetros de configuración:

- Servidor de directorios = `dsserver.example.com`
- Principal de usuario = `willf@EXAMPLE.COM`

**Antes de empezar** Debe asumir el rol `root`. Para obtener más información, consulte [“Cómo usar los derechos administrativos que tiene asignados” en la página 164](#).

### 1 Prepare cada entrada en la clase de objeto de personas.

Repita este paso para cada entrada.

```
cat << EOF | ldapmodify -h dsserver.example.com -D "cn=directory manager"
dn: uid=willf,ou=people,dc=example,dc=com
changetype: modify
objectClass: krbprincipalaux
objectClass: krbTicketPolicyAux
```

```
krbPrincipalName: willf@EXAMPLE.COM
EOF
```

2 **Agregue un atributo de subárbol al contenedor del dominio.**

Este paso permite buscar entradas de principales en el contenedor ou=people,dc=example,dc=com, así como en el contenedor EXAMPLE.COM predeterminado.

```
kdb5_ldap_util -D "cn=directory manager" modify \
 -subtrees 'ou=people,dc=example,dc=com' -r EXAMPLE.COM
```

3 **(Opcional) Si los registros del KDC están almacenados en DB2, migre las entradas de DB2.**

a. **Vuelque las entradas de DB2.**

```
kdb5_util dump > dumpfile
```

b. **Cargue la base de datos en el servidor LDAP.**

```
kdb5_util load -update dumpfile
```

4 **(Opcional) Agregue los atributos de los principales al KDC.**

```
kadmin.local -q 'addprinc willf'
```

▼ **Cómo destruir un dominio en un servidor de directorios LDAP**

Este procedimiento se puede utilizar si un servidor de directorios LDAP distinto se ha configurado para manejar un dominio.

**Antes de empezar** Debe asumir el rol root. Para obtener más información, consulte [“Cómo usar los derechos administrativos que tiene asignados” en la página 164.](#)

● **Destruya el dominio.**

```
kdb5_ldap_util -D "cn=directory manager" destroy
```

**Aumento de la seguridad en servidores Kerberos**

Siga estos pasos para aumentar la seguridad en servidores de aplicaciones Kerberos y en servidores KDC.

TABLA 21–4 Aumento de la seguridad en servidores Kerberos (mapa de tareas)

| Tarea                                      | Descripción                                             | Para obtener instrucciones                                                    |
|--------------------------------------------|---------------------------------------------------------|-------------------------------------------------------------------------------|
| Restringir el acceso a los servidores KDC. | Aumenta la seguridad de los servidores KDC y sus datos. | <a href="#">“Cómo restringir el acceso a servidores KDC” en la página 449</a> |

TABLA 21-4 Aumento de la seguridad en servidores Kerberos (mapa de tareas) (Continuación)

| Tarea                                                                      | Descripción                                                                                            | Para obtener instrucciones                                                                                           |
|----------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------|
| Aumentar la seguridad de contraseñas utilizando un archivo de diccionario. | Aumenta la seguridad de cualquier contraseña nueva comprobando la nueva contraseña con un diccionario. | <a href="#">“Cómo utilizar un archivo de diccionario para aumentar la seguridad de contraseñas” en la página 449</a> |

## ▼ Cómo restringir el acceso a servidores KDC

Tanto los servidores KDC maestros como los servidores KDC esclavos tienen copias de la base de datos del KDC almacenadas localmente. La restricción del acceso a estos servidores para que las bases de datos sean seguras es importante para la seguridad general de la instalación de Kerberos.

**Antes de empezar** Debe asumir el rol root. Para obtener más información, consulte [“Cómo usar los derechos administrativos que tiene asignados” en la página 164](#).

### 1 Restrinja el acceso al hardware que admite el KDC.

Para restringir el acceso físico, asegúrese de que el servidor KDC y su monitor se encuentren en una instalación segura. Los usuarios no deben poder acceder a este servidor de ninguna forma.

### 2 Almacene las copias de seguridad de la base de datos del KDC en discos locales o en los KDC esclavos.

Realice copias de seguridad en cinta del KDC sólo si las cintas están almacenadas de manera segura. Siga la misma práctica para las copias de los archivos keytab. Sería mejor almacenar estos archivos en un sistema de archivos local que no esté compartido con otros sistemas. El sistema de archivos de almacenamiento puede estar en el servidor KDC maestro o en cualquier KDC esclavo.

## ▼ Cómo utilizar un archivo de diccionario para aumentar la seguridad de contraseñas

Un archivo de diccionario puede ser utilizado por el servicio Kerberos para evitar que las palabras del diccionario se usen como contraseñas al crear nuevas credenciales. Impedir el uso de términos del diccionario como contraseñas hace que sea más difícil adivinar las contraseñas. De manera predeterminada, se utiliza el archivo `/var/krb5/kadm5.dict`, pero está vacío.

**Antes de empezar** Debe asumir el rol root. Para obtener más información, consulte [“Cómo usar los derechos administrativos que tiene asignados” en la página 164](#).

## 1 Edite el archivo de configuración de KDC (`kdc.conf`).

Necesita agregar una línea para indicar al servicio que utilice un archivo de diccionario. En este ejemplo, se utiliza el diccionario que se incluye con la utilidad `spell`. Consulte la página del comando `man kdc.conf(4)` para obtener una descripción completa del archivo de configuración.

```
kdc1 # cat /etc/krb5/kdc.conf
[kdcdefaults]
 kdc_ports = 88,750

[realms]
 EXAMPLE.COM = {
 profile = /etc/krb5/krb5.conf
 database_name = /var/krb5/principal
 acl_file = /etc/krb5/kadm5.acl
 kadmind_port = 749
 max_life = 8h 0m 0s
 max_renewable_life = 7d 0h 0m 0s
 sunw_dbprop_enable = true
 sunw_dbprop_master_ulogsize = 1000
 dict_file = /usr/share/lib/dict/words
 }
```

## 2 Reinicie los daemons Kerberos.

```
kdc1 # svcadm restart -r network/security/krb5kdc
kdc1 # svcadm restart -r network/security/kadmin
```

## Mensajes de error y resolución de problemas de Kerberos

---

En este capítulo se proporcionan soluciones para mensajes de error que puede llegar a recibir cuando utiliza el servicio Kerberos. En este capítulo se brindan además algunos consejos sobre la resolución de diversos problemas. Ésta es una lista de mensajes de error e información sobre resolución de problemas de este capítulo.

- “Mensajes de error de la herramienta SEAM” en la página 451
- “Mensajes de error comunes de Kerberos (A-M)” en la página 452
- “Mensajes de error comunes de Kerberos (N-Z)” en la página 462
- “Problemas con el formato del archivo `krb5.conf`” en la página 467
- “Problemas al propagar la base de datos de Kerberos” en la página 467
- “Problemas al montar un sistema de archivos NFS Kerberizado” en la página 468
- “Problemas de autenticación como usuario `root`” en la página 468
- “Observación de asignación de credenciales GSS a credenciales UNIX” en la página 469

### Mensajes de error de Kerberos

En esta sección se proporciona información acerca de los mensajes de error de Kerberos, incluido el motivo por el cual se produce cada error y una forma de solucionarlo.

#### Mensajes de error de la herramienta SEAM

Unable to view the list of principals or policies; use the Name field.

**Causa:** el principal `admin` con el que inició sesión no tiene el privilegio de lista (`l`) en el archivo ACL de Kerberos (`kadm5.acl`). Por lo tanto, no puede ver la lista de principales o la lista de políticas.

**Solución:** debe escribir los nombres de políticas y principales en el campo Nombre para trabajar con ellos o debe iniciar sesión con un principal con los privilegios apropiados.

JNI: Java array creation failed  
JNI: Java class lookup failed  
JNI: Java field lookup failed  
JNI: Java method lookup failed  
JNI: Java object lookup failed  
JNI: Java object field lookup failed  
JNI: Java string access failed  
JNI: Java string creation failed

**Causa:** existe un problema grave con la interfaz nativa de Java que utiliza la herramienta SEAM (gkadmin).

**Solución:** salga de gkadmin y vuelva a iniciarlo. Si el problema persiste, informe acerca del error.

## Mensajes de error comunes de Kerberos (A-M)

En esta sección se proporciona una lista en orden alfabético (A-M) de mensajes de error comunes de los comandos Kerberos, los daemons Kerberos, la estructura PAM, la interfaz GSS, el servicio NFS y la biblioteca Kerberos.

All authentication systems disabled; connection refused

**Causa:** esta versión de rlogind no admite ningún mecanismo de autenticación.

**Solución:** asegúrese de que rlogind se invoque con la opción -k.

Another authentication mechanism must be used to access this host

**Causa:** la autenticación no se pudo llevar a cabo.

**Solución:** asegúrese de que el cliente use el mecanismo Kerberos V5 para la autenticación.

Authentication negotiation has failed, which is required for encryption. Good bye.

**Causa:** no se pudo negociar la autenticación con el servidor.

**Solución:** inicie la depuración de autenticación mediante la invocación del comando telnet con el comando toggle authdebug y observe los mensajes de depuración para obtener más pistas. Además, asegúrese de tener credenciales válidas.

Bad krb5 admin server hostname while initializing kadmin interface

**Causa:** se configuró un nombre de host no válido para admin\_server en el archivo krb5.conf.



**Solución:** asegúrese de que el nombre de host correcto para el KDC maestro se especifique en la línea `admin_server` en el archivo `krb5.conf`.

Bad lifetime value

**Causa:** el valor de vigencia especificado no es válido o su formato es incorrecto.

**Solución:** asegúrese de que el valor proporcionado coincida con lo establecido en la sección de formatos de hora de la página del comando `man kinit(1)`.

Bad start time value

**Causa:** el valor de hora de inicio especificado no es válido o su formato es incorrecto.

**Solución:** asegúrese de que el valor proporcionado coincida con lo establecido en la sección de formatos de hora de la página del comando `man kinit(1)`.

Cannot contact any KDC for requested realm

**Causa:** ningún KDC respondió en el dominio solicitado.

**Solución:** asegúrese de que al menos se pueda acceder a un KDC (maestro o esclavo) o que el daemon `krb5kdc` se ejecute en los KDC. Busque en el archivo `/etc/krb5/krb5.conf` la lista de KDC configurados (`kdc = kdc-name`).

Cannot determine realm for host: host is '*hostname*'

**Causa:** Kerberos no puede determinar el nombre de dominio para el host.

**Solución:** asegúrese de que haya un nombre de dominio predeterminado o que las asignaciones de nombre de dominio estén configuradas en el archivo de configuración de Kerberos (`krb5.conf`).

Cannot find a kadmin KDC entry in `krb5.conf(4)` or DNS Service Location records for realm '*realmname*'

Cannot find a kpassword KDC entry in `krb5.conf(4)` or DNS Service Location records for realm '*realmname*'

Cannot find a master KDC entry in `krb5.conf(4)` or DNS Service Location records for realm '*realmname*'

Cannot find any KDC entries in `krb5.conf(4)` or DNS Service Location records for realm '*realmname*'

**Causa:** el archivo `krb5.conf` o el registro de servidor DNS se configuraron de manera incorrecta.

**Solución:** asegúrese de que el archivo de configuración de Kerberos (`/etc/krb5/krb5.conf`) o que los registros de servidor DNS para el KDC estén configurados correctamente.

Cannot find address for '*hostname*': '*error-string*'

**Causa:** no se encontró ninguna dirección en los registros DNS para el nombre de host proporcionado.

**Solución:** corrija el registro de host en DNS o corrija el error en el proceso de búsqueda de DNS.

Cannot find KDC for requested realm

**Causa:** no se encontró ningún KDC en el dominio solicitado.

**Solución:** asegúrese de que el archivo de configuración de Kerberos (`krb5.conf`) especifique un KDC en la sección `realm`.

cannot initialize realm *realm-name*

**Causa:** el KDC podría no tener un archivo intermedio.

**Solución:** asegúrese de que el KDC tenga un archivo intermedio. En caso contrario, cree un archivo intermedio mediante el comando `kdb5_util` e intente reiniciar el comando `krb5kdc`.

Cannot resolve KDC for requested realm

**Causa:** Kerberos no puede determinar ningún KDC para el dominio.

**Solución:** asegúrese de que el archivo de configuración de Kerberos (`krb5.conf`) especifique un KDC en la sección `realm`.

Cannot resolve network address for KDCs '*hostname*' discovered via DNS Service Location records for realm '*realm-name*'

Cannot resolve network address for KDCs '*hostname*' specified in `krb5.conf(4)` for realm '*realm-name*'

**Causa:** el archivo `krb5.conf` o el registro de servidor DNS se configuró de manera incorrecta.

**Solución:** asegúrese de que el archivo de configuración de Kerberos (`/etc/krb5/krb5.conf`) y que los registros de servidor DNS para el KDC estén configurados correctamente.

Cannot reuse password

**Causa:** este principal ya ha utilizado la contraseña que especificó.

**Solución:** seleccione una contraseña que no se haya elegido antes, al menos no dentro del número de contraseñas que se mantiene en la base de datos de KDC para cada principal. La política del principal aplica esta política.

Can't get forwarded credentials

**Causa:** no se pudo establecer el reenvío de credenciales.

**Solución:** asegúrese de que el principal tenga credenciales que se puedan reenviar.

Can't open/find Kerberos configuration file

**Causa:** el archivo de configuración de Kerberos (`krb5.conf`) no estaba disponible.

**Solución:** asegúrese de que el archivo `krb5.conf` esté disponible en la ubicación correcta y tenga los permisos correctos. `root` debería poder escribir en este archivo y el resto debería poder leerlo.

Client '*principal*' not found in Kerberos database

**Causa:** el principal no se encuentra en la base de datos de Kerberos.

**Solución:** agregue el principal de cliente a la base de datos de Kerberos.

Client '*principal*' pre-authentication failed

**Causa:** falló la autenticación para el principal.

**Solución:** asegúrese de que el usuario esté utilizando la contraseña correcta.

Client did not supply required checksum--connection rejected

**Causa:** no se negoció la autenticación con suma de comprobación con el cliente. Es posible que el cliente use un protocolo Kerberos V5 obsoleto que no admite conexión inicial.

**Solución:** asegúrese de que el cliente use un protocolo Kerberos V5 que admita conexión inicial.

Client/server realm mismatch in initial ticket request: '*client-principal*' requesting ticket '*service-principal*'

**Causa:** se produjo una discrepancia de dominios entre el cliente y el servidor en la solicitud de ticket inicial.

**Solución:** asegúrese de que el servidor con el que se comunica esté en el mismo dominio que el cliente o que las configuraciones de dominios sean correctas.

Client or server has a null key

**Causa:** el principal tiene una clave nula.

**Solución:** modifique el principal para que tenga una clave no nula mediante el comando `cpw` de `kadmin`.

Clock skew too great: '*client*' requesting ticket '*service-principal*' from KDC '*KDC-hostname*' ( *KDC-time*). Skew is *value*

Clock skew too great: '*client*' AP request with ticket for '*service-principal*'. Skew is *value* (allowable *value*)

**Causa:** la diferencia entre el tiempo informado en el cliente y el servidor KDC o servidor de aplicaciones es demasiado grande.

**Solución:** configure el protocolo de tiempo de red (NTP) para mantener los relojes sincronizados. Consulte [“Sincronización de relojes entre clientes Kerberos y KDC” en la página 424](#) para obtener más información.

Communication failure with server while initializing kadmin interface

**Causa:** el host que se especificó para el servidor de administración, también denominado KDC maestro, no tiene los daemons kadmind en ejecución.

**Solución:** asegúrese de que ha especificado el nombre de host correcto para el KDC maestro. Si especificó el nombre de host correcto, asegúrese de que kadmind esté en ejecución en el KDC maestro que especificó.

Credentials cache file permissions incorrect

**Causa:** no tiene los permisos de lectura o escritura apropiados en la antememoria de credenciales (/tmp/krb5cc\_uid).

**Solución:** asegúrese de tener los permisos de lectura y escritura en la antememoria de credenciales.

Credentials cache I/O operation failed XXX

**Causa:** Kerberos tuvo un problema al escribir en la antememoria de credenciales del sistema (/tmp/krb5cc\_uid).

**Solución:** asegúrese de que la antememoria de credenciales no se haya eliminado y de que haya espacio libre en el dispositivo mediante el comando df.

Decrypt integrity check failed

**Causa:** es posible que tenga un ticket no válido.

**Solución:** verifique estas condiciones:

- asegúrese de que las credenciales sean válidas. Destruya los tickets con kdestroy y cree nuevos tickets con kinit.
- Asegúrese de que el host de destino tenga un archivo keytab con la versión correcta de la clave del servicio. Use kadmin para ver el número de versión de clave del principal de servicio (por ejemplo, host/FQDN-hostname) en la base de datos de Kerberos. Asimismo, utilice klist -k en el host de destino para asegurarse de que tenga el mismo número de versión de clave.

Decrypt integrity check failed for client 'principal' and server 'hostname'

**Causa:** es posible que tenga un ticket no válido.

**Solución:** asegúrese de que las credenciales sean válidas. Destruya los tickets con el comando kdestroy y cree nuevos tickets con el comando kinit.

Encryption could not be enabled. Goodbye.

**Causa:** no se pudo negociar el cifrado con el servidor.

**Solución:** inicie la depuración de autenticación mediante la invocación del comando `telnet` con el comando `toggle encdebug` y observe los mensajes de depuración para obtener más pistas.

Failed to find realm for *principal* in keytab

**Causa:** el nombre de dominio incluido en el *principal* no coincide con el nombre de dominio en el principal almacenado en el archivo keytab.

**Solución:** asegúrese de que los principales estén utilizando el dominio correcto.

failed to obtain credentials cache

**Causa:** durante la inicialización de `kadmin`, se produjo un error cuando `kadmin` intentó obtener credenciales para el principal `admin`.

**Solución:** asegúrese de haber utilizado el principal y la contraseña correctos cuando ejecutó `kadmin`.

Field is too long for this implementation

**Causa:** el tamaño del mensaje que enviaba una aplicación Kerberizada era demasiado largo. Este error se puede generar si el protocolo de transporte es UDP. Que tiene un tamaño máximo de mensaje de 65535 bytes de manera predeterminada. Además, hay límites en los campos individuales dentro de un mensaje de protocolo que se envía por el servicio Kerberos.

**Solución:** verifique que no haya restringido el transporte a UDP en el archivo `/etc/krb5/kdc.conf` del servidor KDC.

GSS-API (or Kerberos) error

**Causa:** este mensaje es un mensaje de error genérico de GSS-API o Kerberos y puede ser causado por diversos problemas.

**Solución:** compruebe el archivo `/var/krb5/kdc.log` para encontrar el mensaje de error más específico que se registró cuando se produjo este error.

Hostname cannot be canonicalized for '*hostname*': '*error-string*'

**Causa:** el cliente Kerberos no puede encontrar el nombre de host completo para el servidor.

**Solución:** asegúrese de que el nombre de host del servidor esté definido en DNS y que las asignaciones de nombre de host a dirección y de dirección a nombre de host sean consistentes.

Illegal cross-realm ticket

**Causa:** el ticket enviado no tenía los dominios cruzados correctos. Es posible que los dominios no tengan configuradas las relaciones de confianza correctas.

**Solución:** asegúrese de que los dominios que utilice tengan las relaciones de confianza correctas.

**Improper format of Kerberos configuration file**

**Causa:** el archivo de configuración de Kerberos tiene entradas no válidas.

**Solución:** asegúrese de que todas las relaciones en el archivo `krb5.conf` estén seguidas del signo “=” y un valor. Asimismo, verifique que los paréntesis estén presentes en pares para cada subsección.

**Inappropriate type of checksum in message**

**Causa:** el mensaje contenía un tipo de suma de comprobación no válido.

**Solución:** compruebe qué tipos de suma de comprobación se especifican en los archivos `krb5.conf` y `kdc.conf`.

**Incorrect net address**

**Causa:** existe una discrepancia en la dirección de red. La dirección de red en el ticket que se reenviaba era distinta de la dirección de red donde se procesó el ticket. Este mensaje puede aparecer cuando los tickets se reenvían.

**Solución:** asegúrese de que las direcciones de red sean correctas. Destruya los tickets con `kdestroy` y cree nuevos tickets con `kinit`.

**Invalid credential was supplied**

**Service key not available**

**Causa:** es posible que el ticket de servicio en la antememoria de credenciales sea incorrecto.

**Solución:** destruya la antememoria de credenciales actual y vuelva a ejecutar `kinit` antes de intentar utilizar este servicio.

**Invalid flag for file lock mode**

**Causa:** se produjo un error de Kerberos interno.

**Solución:** informe acerca del error.

**Invalid message type specified for encoding**

**Causa:** Kerberos no pudo reconocer el tipo de mensaje que se envió mediante la aplicación Kerberizada.

**Solución:** si utiliza una aplicación Kerberizada desarrollada por su sitio o un vendedor, asegúrese de que la aplicación utilice Kerberos correctamente.

**Invalid number of character classes**

**Causa:** la contraseña que especificó para el principal no contiene suficientes clases de contraseñas, como si se aplica mediante la política del principal.

**Solución:** asegúrese de especificar una contraseña con el número mínimo de clases de contraseñas que la política necesita.

KADM err: Memory allocation failure

**Causa:** no hay suficiente memoria para ejecutar kadmin.

**Solución:** libere memoria e intente ejecutar kadmin nuevamente.

kadmin: Bad encryption type while changing host/*FQDN*'s key

**Causa:** se incluyen más tipos de cifrado de manera predeterminada en la versión base en las versiones más nuevas. Los clientes pueden solicitar tipos de cifrado que posiblemente no sean admitidos por un KDC que ejecuta una versión anterior del software.

**Solución:** existen varias soluciones para este problema. La más fácil de implementar es la que se enumera primero:

1. Agregar los paquetes SUNWcry y SUNWcryr al servidor KDC. Esto aumenta el número de tipos de cifrado admitidos por KDC.
2. Establecer `permitted_enctypes` en `krb5.conf` en el cliente si no desea incluir el tipo de cifrado `aes256`. Será necesario realizar este paso en cada nuevo cliente.

KDC can't fulfill requested option

**Causa:** KDC no permite la opción solicitada. Un posible problema podría ser que las opciones de posfechado o reenvío se hayan solicitado y KDC no las haya permitido. Otro problema podría ser que usted solicitó la renovación de un TGT, pero no disponía de un TGT renovable.

**Solución:** determine si solicita una opción que KDC no permite o un tipo de ticket que no se encuentra disponible.

KDC policy rejects request

**Causa:** la política de KDC no permite la solicitud. Por ejemplo, la solicitud al KDC no tenía una dirección IP en su solicitud. O se solicitó el reenvío pero el KDC no lo permitía.

**Solución:** asegúrese de utilizar `kinit` con las opciones correctas. Si es necesario, modifique la política que está asociada con el principal o cambie los atributos del principal para permitir la solicitud. Puede modificar la política o el principal mediante `kadmin`.

KDC reply did not match expectation: KDC not found. Probably got an unexpected realm referral

**Causa:** la respuesta de KDC no contenía el nombre de principal esperado u otros valores en la respuesta eran incorrectos.

**Solución:** asegúrese de que el KDC con el que se comunica cumpla con RFC4120, que la solicitud que envía sea una solicitud Kerberos V5 y que el KDC esté disponible.

kdestroy: Could not obtain principal name from cache

**Causa:** la caché de credenciales no se encuentra o está dañada.

**Solución:** compruebe que la ubicación de la caché proporcionada sea correcta. Elimine y obtenga un nuevo TGT mediante kinit, si es necesario.

kdestroy: No credentials cache file found while destroying cache

**Causa:** la caché de credenciales (/tmp/krb5c\_*uid*) no se encuentra o está dañada.

**Solución:** compruebe que la ubicación de la caché proporcionada sea correcta. Elimine y obtenga un nuevo TGT mediante kinit, si es necesario.

kdestroy: TGT expire warning NOT deleted

**Causa:** la caché de credenciales no se encuentra o está dañada.

**Solución:** compruebe que la ubicación de la caché proporcionada sea correcta. Elimine y obtenga un nuevo TGT mediante kinit, si es necesario.

Kerberos authentication failed

**Causa:** la contraseña de Kerberos es incorrecta o es posible que la contraseña no esté sincronizada con la contraseña de UNIX.

**Solución:** si la contraseña no está sincronizada, debe especificar una contraseña diferente para completar la autenticación Kerberos. Es posible que el usuario haya olvidado su contraseña original.

Kerberos V5 refuses authentication

**Causa:** no se pudo negociar la autenticación con el servidor.

**Solución:** inicie la depuración de autenticación mediante la invocación del comando telnet con el comando toggle authdebug y observe los mensajes de depuración para obtener más pistas. Además, asegúrese de tener credenciales válidas.

Key table entry not found

**Causa:** no existe ninguna entrada para el principal de servicio en el archivo keytab del servidor de aplicación de red.

**Solución:** agregue el principal de servicio apropiado al archivo keytab del servidor para que pueda proporcionar el servicio Kerberizado.

Key table file '*filename*' not found

**Causa:** el archivo de tabla de claves mencionado no existe.

**Solución:** cree el archivo de tabla de claves.



Key version *number* is not available for principal *principal*

**Causa:** la versión de clave de las claves no coincide con la versión para las claves en el servidor de aplicaciones.

**Solución:** compruebe la versión de las claves en el servidor de aplicaciones mediante el comando `klist -k`

Key version number for principal in key table is incorrect

**Causa:** una versión de clave del principal en el archivo keytab es diferente de la versión en la base de datos de Kerberos. Es posible que una clave del servicio haya cambiado o que utilice un ticket de servicio antiguo.

**Solución:** si la clave del servicio ha cambiado (por ejemplo, mediante el uso de `kadmin`), deberá extraer la nueva clave y almacenarla en el archivo keytab del host donde se ejecuta el servicio.

Asimismo, es posible que utilice un ticket de servicio antiguo que tiene una clave anterior. Es posible que desee ejecutar el comando `kdestroy` y luego el comando `kinit` nuevamente.

kinit: gethostname failed

**Causa:** un error en la configuración de red local provoca el fallo de `kinit`.

**Solución:** asegúrese de que el host esté configurado correctamente.

login: load\_modules: can not open module /usr/lib/security/pam\_krb5.so.1

**Causa:** no se encuentra el módulo PAM de Kerberos o no es un binario ejecutable válido.

**Solución:** asegúrese de que el módulo PAM de Kerberos esté en el directorio `/usr/lib/security` y que sea un binario ejecutable válido. Además, asegúrese de que el archivo `/etc/pam.conf` contenga la ruta correcta a `pam_krb5.so.1`.

Looping detected getting initial creds: '*client-principal*' requesting ticket '*service-principal*'. Max loops is *value*. Make sure a KDC is available.

**Causa:** Kerberos realizó varios intentos de obtener los tickets iniciales pero no tuvo éxito.

**Solución:** asegúrese de que al menos un KDC responda a las solicitudes de autenticación.

Master key does not match database

**Causa:** el volcado de base de datos cargado no se creó a partir de una base de datos que contiene la clave maestra. La clave maestra se encuentra en `/var/krb5/.k5.REALM`.

**Solución:** asegúrese de que la clave maestra en el volcado de base de datos cargado coincida con la clave maestra ubicada en `/var/krb5/.k5.REALM`.

Matching credential not found

**Causa:** la credencial concordante para su solicitud no se ha encontrado. Su solicitud necesita credenciales que no están disponibles en la antememoria de credenciales.

**Solución:** Destruya los tickets con `kdestroy` y cree nuevos tickets con `kinit`.

Message out of order

**Causa:** mensajes que se enviaron utilizando privacidad de orden secuencial llegaron fuera de orden. Es posible que algunos mensajes se hayan perdido en el tránsito.

**Solución:** debe reinicializar la sesión de Kerberos.

Message stream modified

**Causa:** existe una discrepancia entre la suma de comprobación calculada y la suma de comprobación de mensaje. Es posible que el mensaje se haya modificado durante el tránsito, lo que puede indicar una infracción de seguridad.

**Solución:** asegúrese de que los mensajes se envíen a través de la red correctamente. Debido a que este mensaje también puede indicar la posible alteración de mensajes durante el envío, destruya los tickets mediante `kdestroy` y reinicialice los servicios Kerberos que esté utilizando.

## Mensajes de error comunes de Kerberos (N-Z)

En esta sección se proporciona una lista en orden alfabético (N-Z) de mensajes de error comunes de los comandos Kerberos, los daemons Kerberos, la estructura PAM, la interfaz GSS, el servicio NFS y la biblioteca Kerberos.

No credentials cache file found

**Causa:** Kerberos no pudo encontrar la caché de credenciales (`/tmp/krb5cc_uid`).

**Solución:** asegúrese de que el archivo de credenciales exista y se pueda leer. En caso contrario, intente ejecutar `kinit` nuevamente.

No credentials were supplied, or the credentials were unavailable or inaccessible

No credential cache found

**Causa:** la antememoria de credenciales del usuario es incorrecta o no existe.

**Solución:** el usuario debe ejecutar `kinit` antes de intentar iniciar el servicio.

No credentials were supplied, or the credentials were unavailable or inaccessible

No principal in keytab ('*filename*') matches desired name *principal*

**Causa:** se ha producido un error al intentar autenticar el servidor.

**Solución:** asegúrese de que el host o principal de servicio estén en el archivo keytab del servidor.

Operation requires “*privilege*” privilege

**Causa:** el principal admin que estaba en uso no tenía el privilegio adecuado configurado en el archivo `kadm5.acl`.

**Solución:** utilice un principal que tenga los privilegios adecuados. O bien, configure el principal que estaba en uso para que tenga los privilegios adecuados mediante la modificación del archivo `kadm5.acl`. Normalmente, un principal con `/admin` como parte de su nombre tiene los privilegios adecuados.

PAM-KRB5 (auth): `krb5_verify_init_creds` failed: Key table entry not found

**Causa:** la aplicación remota intentó leer el principal de servicio del host en el archivo local `/etc/krb5/krb5.keytab`, pero no existe.

**Solución:** agregue el principal de servicio del host al archivo keytab del host.

Password is in the password dictionary

**Causa:** la contraseña que especificó está en un diccionario de contraseñas que está en uso. La contraseña no es una buena elección para una contraseña.

**Solución:** seleccione una contraseña que tenga una mezcla de clases de contraseñas.

Permission denied in replay cache code

**Causa:** no se pudo abrir la antememoria de reproducción del sistema. Es posible que el servidor se haya ejecutado por primera vez con un ID de usuario diferente del ID de usuario actual.

**Solución:** asegúrese de que la antememoria de reproducción tenga los permisos adecuados. La antememoria de reproducción se almacena en el host donde la aplicación de servidor Kerberizada está en ejecución. El archivo de antememoria de reproducción se denomina `/var/krb5/rcache/rc_service_name_uid` para usuarios no root. Para los usuarios root, el archivo de antememoria de reproducción se denomina `/var/krb5/rcache/root/rc_nombre_servicio`.

Protocol version mismatch

**Causa:** lo más probable es que una solicitud de Kerberos V4 se haya enviado al KDC. El servicio Kerberos sólo admite el protocolo Kerberos V5.

**Solución:** asegúrese de que las aplicaciones utilicen el protocolo Kerberos V5.

Request is a replay

**Causa:** la solicitud ya se ha enviado a este servidor y ya se ha procesado. Es posible que los tickets hayan sido robados y alguien esté intentando volver a utilizar los tickets.

**Solución:** espere unos minutos y vuelva a emitir la solicitud.

Requested principal and ticket don't match: Requested principal is '*service-principal*' and TGT principal is '*TGT-principal*'

**Causa:** el principal de servicio al que se conecta y el ticket de servicio que posee no concuerdan.

**Solución:** asegúrese de que DNS funcione correctamente. Si utiliza el software de otro proveedor, asegúrese de que el software utilice los nombres de principal correctamente.

Requested protocol version not supported

**Causa:** lo más probable es que una solicitud de Kerberos V4 se haya enviado al KDC. El servicio Kerberos sólo admite el protocolo Kerberos V5.

**Solución:** asegúrese de que las aplicaciones utilicen el protocolo Kerberos V5.

Service key *service-principal* not available

**Causa:** el principal de servicio denominado no está en el archivo keytab en el servidor de aplicaciones.

**Solución:** asegúrese de que el principal de servicio coincida o se incluya en el archivo keytab en el servidor de aplicaciones.

Server refused to negotiate authentication, which is required for encryption.  
Good bye.

**Causa:** la aplicación remota no es capaz o se ha configurado para no aceptar la autenticación Kerberos del cliente.

**Solución:** proporcione una aplicación remota que puede negociar la autenticación o configurar la aplicación para que utilice los indicadores adecuados para activar la autenticación.

Server refused to negotiate encryption. Good bye.

**Causa:** no se pudo negociar el cifrado con el servidor.

**Solución:** inicie la depuración de autenticación mediante la invocación del comando `telnet` con el comando `toggle encdebug` y observe los mensajes de depuración para obtener más pistas.

Server rejected authentication (during sendauth exchange)

**Causa:** el servidor con el que intenta comunicarse rechazó la autenticación. La mayoría de las veces, este error se produce durante la propagación de la base de datos de Kerberos. Algunas de las causas comunes podrían ser problemas relacionados con el archivo `kpropd.ac1`, DNS o el archivo `keytab`.

**Solución:** si recibe este error cuando ejecuta aplicaciones que no sean kprop, investigue si el archivo keytab del servidor es correcto.

Server *service-principal* not found in Kerberos database

**Causa:** el principal de servicio no es correcto o no se encuentra en la base de datos de principal.

**Solución:** asegúrese de que el principal de servicio sea correcto y que esté en la base de datos.

Target name principal '*principal*' does not match *service-principal*

**Causa:** el principal de servicio que se está utilizando no coincide con el principal de servicio que utiliza el servidor de aplicaciones.

**Solución:** en el servidor de aplicaciones, asegúrese de que el principal de servicio se incluya en el archivo keytab. Para el cliente, asegúrese de que se utilice el principal servicio correcto.

The ticket isn't for us

Ticket/authenticator don't match

**Causa:** existe una discrepancia entre el ticket y el autenticador. Es posible que el nombre del principal en la solicitud no haya coincidido con el nombre del principal de servicio. Ya sea porque el ticket se envió con un nombre FQDN del principal mientras que el servicio esperaba un nombre no FQDN, o se envió un nombre no FQDN cuando el servicio esperaba un nombre FQDN.

**Solución:** si recibe este error cuando ejecuta aplicaciones que no sean kprop, investigue si el archivo keytab del servidor es correcto.

Ticket expired

**Causa:** el tiempo del ticket ha caducado.

**Solución:** Destruya los tickets con `kdestroy` y cree nuevos tickets con `kinit`.

Ticket is ineligible for postdating

**Causa:** el principal no permite que los tickets sean posfechados.

**Solución:** modifique el principal con `kadmin` para permitir que sea posfechado.

Ticket not yet valid: '*client-principal*' requesting ticket '*service-principal*' from '*kdc-hostname*' (*time*). TGT start time is *time*.

**Causa:** el ticket posfechado no es válido todavía.

**Solución:** cree un nuevo ticket con la fecha correcta o espere hasta que el ticket actual sea válido.

Truncated input file detected

**Causa:** el archivo de volcado de base de datos que se utilizaba en la operación no era un archivo de volcado completo.

**Solución:** cree el archivo de volcado de nuevo o utilice un archivo de volcado de base de datos diferente.

Unable to securely authenticate user ... exit

**Causa:** no se pudo negociar la autenticación con el servidor.

**Solución:** inicie la depuración de autenticación mediante la invocación del comando `telnet` con el comando `toggle authdebug` y observe los mensajes de depuración para obtener más pistas. Además, asegúrese de tener credenciales válidas.

Unknown encryption type: *name*

**Causa:** el tipo de cifrado que se incluye con la credencial no se puede utilizar.

**Solución:** determine qué tipos de cifrado utiliza el cliente con el comando `klist -e`. Asegúrese de que el servidor de aplicaciones admita al menos uno de los tipos de cifrado.

Wrong principal in request

**Causa:** había un nombre de principal no válido en el ticket. Este error puede indicar que hay un problema de DNS o FQDN.

**Solución:** asegúrese de que el principal del servicio coincida con el principal en el ticket.

## Resolución de problemas de Kerberos

En esta sección se proporciona información acerca de la resolución de problemas del software Kerberos.

### ▼ Cómo identificar problemas con números de versión de clave

A veces, el número de versión de clave (KVNO) utilizado por el KDC y las claves de principal de servicio almacenadas en `/etc/krb5/krb5.keytab` para servicios alojados en el sistema no coinciden. El KVNO puede salir de sincronización cuando un nuevo conjunto de claves se crea en el KDC sin actualizar el archivo `keytab` con las nuevas claves. Este problema se puede diagnosticar mediante el siguiente procedimiento.

**1 Enumere las entradas keytab.**

Tenga en cuenta que el KVNO para cada principal se incluye en la lista.

```
klist -k
Keytab name: FILE:/etc/krb5/krb5.keytab
KVNO Principal

2 host/denver.example.com@EXAMPLE.COM
2 host/denver.example.com@EXAMPLE.COM
2 host/denver.example.com@EXAMPLE.COM
2 nfs/denver.example.com@EXAMPLE.COM
2 nfs/denver.example.com@EXAMPLE.COM
2 nfs/denver.example.com@EXAMPLE.COM
2 nfs/denver.example.com@EXAMPLE.COM
```

**2 Adquiera una credencial inicial mediante la clave host.**

```
kinit -k
```

**3 Determine el KVNO que KDC utiliza.**

```
kvno nfs/denver.example.com
nfs/denver.example.com@EXAMPLE.COM: kvno = 3
```

Tenga en cuenta que el KVNO que se muestran aquí es 3 en lugar de 2.

## Problemas con el formato del archivo krb5.conf

Si el archivo `krb5.conf` no tiene el formato correcto, es posible que se muestre el siguiente mensaje de error en una ventana de terminal o se registre en el archivo de registro:

```
Improper format of Kerberos configuration file while initializing krb5 library
```

Si hay un problema con el formato del archivo `krb5.conf`, los servicios asociados podrían quedar vulnerables a ataques. Debe solucionar el problema antes de permitir que se utilicen funciones de Kerberos.

## Problemas al propagar la base de datos de Kerberos

Si la propagación de la base de datos de Kerberos falla, pruebe `/usr/bin/rlogin -x` entre el KDC esclavo y el KDC maestro, y del KDC maestro al servidor KDC esclavo.

Si los KDC se han configurado para restringir el acceso, `rlogin` está desactivado y no se puede utilizar para solucionar este problema. Para activar `rlogin` en un KDC, debe activar el servicio `eklogin`.

```
svcadm enable svc:/network/login:eklogin
```

Una vez solucionado el problema, es necesario desactivar el servicio `eklogin`.

Si `rlogin` no funciona, es posible que los problemas se deban a los archivos `keytab` en los KDC. Si `rlogin` funciona, el problema no está en el archivo `keytab` ni en el servicio de nombres, porque `rlogin` y el software de propagación utilizan el mismo principal `host/host-name`. En este caso, asegúrese de que el archivo `kpropd.acf` sea correcto.

## Problemas al montar un sistema de archivos NFS Kerberizado

- Si el montaje de un sistema de archivos NFS Kerberizado falla, asegúrese de que el archivo `/var/ncache/root` exista en el servidor NFS. Si el sistema de archivos no es propiedad de `root`, elimínelo e intente el montaje nuevamente.
- Si tiene un problema al acceder a un sistema de archivos NFS Kerberizado, asegúrese de que el servicio `gssd` esté habilitado en el sistema y el servidor NFS.
- Si ve el mensaje de error `invalid argument` o `bad directory` cuando intenta acceder a un sistema de archivos NFS Kerberizado, posiblemente el problema sea que no utiliza un nombre DNS completo cuando intenta montar el sistema de archivos NFS. El `host` que se monta no es el mismo que el nombre de `host` parte del principal de servicio en el archivo `keytab` del servidor.

Este problema también puede ocurrir si el servidor tiene varias interfaces Ethernet y ha configurado DNS para que utilice un esquema "nombre por interfaz" en lugar de un esquema "varios registros de dirección por host". Para el servicio Kerberos, debe configurar varios registros de dirección por host como se indica a continuación<sup>1</sup>:

|                                |                  |                            |
|--------------------------------|------------------|----------------------------|
| <code>my.host.name.</code>     | <code>A</code>   | <code>1.2.3.4</code>       |
|                                | <code>A</code>   | <code>1.2.4.4</code>       |
|                                | <code>A</code>   | <code>1.2.5.4</code>       |
| <code>my-en0.host.name.</code> | <code>A</code>   | <code>1.2.3.4</code>       |
| <code>my-en1.host.name.</code> | <code>A</code>   | <code>1.2.4.4</code>       |
| <code>my-en2.host.name.</code> | <code>A</code>   | <code>1.2.5.4</code>       |
| <code>4.3.2.1</code>           | <code>PTR</code> | <code>my.host.name.</code> |
| <code>4.4.2.1</code>           | <code>PTR</code> | <code>my.host.name.</code> |
| <code>4.5.2.1</code>           | <code>PTR</code> | <code>my.host.name.</code> |

En este ejemplo, la configuración permite una referencia a las diferentes interfaces y a un único principal de servicio en lugar de tres principales de servicio en el archivo `keytab` del servidor.

## Problemas de autenticación como usuario root

Si falla la autenticación cuando intenta convertirse en superusuario en el sistema y ya ha agregado el principal `root` al archivo `keytab` del `host`, hay dos posibles problemas que debe

<sup>1</sup> Ken Hornstein, "Kerberos FAQ" [<http://www.cmf.nrl.navy.mil/CCS/people/kenh/kerberos-faq.html#kerbdns>], se accedió el 10 de marzo de 2010.



comprobar. En primer lugar, asegúrese de que el principal root en el archivo `keytab` tenga un nombre de host completo como su instancia. Si es así, compruebe el archivo `/etc/resolv.conf` para asegurarse de que el sistema esté correctamente configurado como un cliente DNS.

## Observación de asignación de credenciales GSS a credenciales UNIX

Para poder supervisar las asignaciones de credenciales, primero elimine el comentario de esta línea del archivo `/etc/gss/gsscred.conf`.

```
SYSLOG_UID_MAPPING=yes
```

Luego, indique al servicio `gssd` que obtenga información del archivo `/etc/gss/gsscred.conf`.

```
pkill -HUP gssd
```

Ahora debería poder controlar las asignaciones de credenciales a medida que `gssd` las solicita. Las asignaciones son registradas por `syslogd` si el archivo `syslog.conf` está configurado para la utilidad de sistema `auth` con el nivel de gravedad `debug`.

## Uso de DTrace con el servicio Kerberos

El mecanismo Kerberos es compatible con varios sondeos de DTrace para decodificar varios mensajes de protocolo. Los sondeos incluyen `KRB_AP_*`, `KRB_KDC_*`, `KRB_CRED`, `KRB_ERROR`, `KRB_PRIV`, `KRB_SAFE` e información general de mensajes. Tiene una ventaja que la destaca de otros inspectores de protocolos, ya que permite al usuario con privilegios ver fácilmente los datos sin cifrar de Kerberos y de aplicaciones.

El siguiente ejemplo muestra la autenticación previa seleccionada por el cliente. El primer paso consiste en crear una secuencia de comandos de DTrace, como se muestra a continuación:

```
cat krbtrace.d
kerberos$target:::krb_message-recv
{
 printf("<- krb message recved: %s\n", args[0]->krb_message_type);
 printf("<- krb message remote addr: %s\n", args[1]->kconn_remote);
 printf("<- krb message ports: local %d remote %d\n",
 args[1]->kconn_localport, args[1]->kconn_remoteport);
 printf("<- krb message protocol: %s transport: %s\n",
 args[1]->kconn_protocol, args[1]->kconn_type);
}

kerberos$target:::krb_message-send
{
 printf(">- krb message sent: %s\n", args[0]->krb_message_type);
 printf(">- krb message remote addr: %s\n", args[1]->kconn_remote);
}
```

```
printf("-> krb message ports: local %d remote %d\n",
 args[1]->kconn_localport, args[1]->kconn_remoteport);
printf("-> krb message protocol: %s transport: %s\n",
 args[1]->kconn_protocol, args[1]->kconn_type);
printf("\n");
}

kerberos$target::krb_kdc_req-make
{
 printf("-> krb kdc_req make msg type: %s\n", args[0]->krb_message_type);
 printf("-> krb kdc_req make pre-auths: %s\n", args[1]->kdcreq_padata_types);
 printf("-> krb kdc_req make auth data: %s\n", args[1]->kdcreq_authorization_data);
 printf("-> krb kdc_req make client: %s server: %s\n", args[1]->kdcreq_client,
 args[1]->kdcreq_server);
}

kerberos$target::krb_kdc_req-read
{
 /* printf("<- krb kdc_req msg type: %s\n", args[0]->krb_message_type); */
 printf("<- krb kdc_req client: %s server: %s\n", args[1]->kdcreq_client,
 args[1]->kdcreq_server);
 printf("\n");
}

kerberos$target::krb_kdc_rep-read
{
 /* printf("<- krb kdc_rep msg type: %s\n", args[0]->krb_message_type); */
 printf("<- krb kdc_rep client: %s server: %s\n", args[1]->kdcprep_client,
 args[1]->kdcprep_enc_server);
 printf("\n");
}

kerberos$target::krb_ap_req-make
{
 printf("-> krb ap_req make server: %s client: %s\n", args[2]->kticket_server,
 args[2]->kticket_enc_client);
}

kerberos$target::krb_error-read
{
 printf("<- krb error code: %s\n", args[1]->kerror_error_code);
 printf("<- krb error client: %s server: %s\n", args[1]->kerror_client,
 args[1]->kerror_server);
 printf("<- krb error e-text: %s\n", args[1]->kerror_e_text);
 printf("\n");
}
```

A continuación, ejecute la secuencia de comandos `krbt race.d` como usuario con privilegios en el sistema Kerberos. Para ello, escriba el siguiente comando:

```
LD_BIND_NOW=1 dtrace -qs krbtrace.d -c "kinit -k"
.
.
-> krb kdc_req make pre-auths: FX_COOKIE(133) ENC_TIMESTAMP(2) REQ_ENC_PA_REP(149)
```

Los tipos de autenticación previa se mostrarán en el resultado. Para obtener más información acerca de los distintos tipos de autenticación previa, consulte [RFC 4120](#).

## Administración de las políticas y los principales de Kerberos (tareas)

---

En este capítulo se brindan los procedimientos para administrar los principales y las políticas que están relacionadas con ellos. En este capítulo, también se muestra cómo administrar un archivo keytab del host.

Este capítulo debe ser utilizado por cualquier persona que necesite administrar principales y políticas. Antes de utilizar este capítulo, debe estar familiarizado con los principales y las políticas, incluida cualquier consideración sobre la planificación. Consulte el [Capítulo 19, “Introducción al servicio Kerberos”](#) y el [Capítulo 20, “Planificación del servicio Kerberos”](#), respectivamente.

A continuación se indica la información contenida en este capítulo:

- “[Maneras de administrar las políticas y los principales de Kerberos](#)” en la página 471
- “[Herramienta SEAM](#)” en la página 472
- “[Administración de los principales de Kerberos](#)” en la página 476
- “[Administración de las políticas de Kerberos](#)” en la página 490
- “[Referencia de la herramienta SEAM](#)” en la página 499
- “[Administración de los archivos keytab](#)” en la página 504

## Maneras de administrar las políticas y los principales de Kerberos

La base de datos de Kerberos en el KDC maestro contiene todos los principales de Kerberos del dominio, sus contraseñas, sus políticas y otra información administrativa. Para crear y eliminar los principales, y modificar sus atributos, puede utilizar el comando `kadmin` o `gkadmin`.

El comando `kadmin` proporciona una interfaz de línea de comandos interactiva que le permite mantener los principales, las políticas y los archivos `keytab` de Kerberos. Hay dos versiones del comando `kadmin`:

- `kadmin`: utiliza la autenticación de Kerberos para funcionar de manera segura desde cualquier parte de la red
- `kadmin.local`: se debe ejecutar directamente en el KDC maestro

Además de que `kadmin` usa Kerberos para autenticar el usuario, las capacidades de las dos versiones son idénticas. La versión local es necesaria para que usted pueda configurar una parte suficiente de la base de datos para poder utilizar la versión remota.

Asimismo, la versión de Oracle Solaris proporciona la herramienta SEAM, `gkadmin`, que es una interfaz gráfica de usuario (GUI) interactiva que proporciona, básicamente, las mismas capacidades que el comando `kadmin`. Para obtener más información, consulte [“Herramienta SEAM” en la página 472](#).

## Herramienta SEAM

La herramienta SEAM (`gkadmin`) es una interfaz gráfica de usuario (GUI) interactiva que permite mantener los principales y las políticas de Kerberos. Esta herramienta proporciona en gran parte las mismas funciones que el comando `kadmin`. Sin embargo, la herramienta no admite la gestión de los archivos `keytab`. Debe utilizar el comando `kadmin` para administrar los archivos `keytab`, lo cual se describe en [“Administración de los archivos `keytab`” en la página 504](#).

De manera similar al comando `kadmin`, la herramienta SEAM utiliza la RPC cifrada y la autenticación de Kerberos para trabajar de manera segura en cualquier parte de la red. La herramienta SEAM le permite realizar las siguientes acciones:

- Crear nuevos principales basados en los valores predeterminados o en los principales existentes.
- Crear nuevas políticas basadas en políticas existentes.
- Agregar comentarios para los principales.
- Configurar valores predeterminados para la creación de principales nuevos.
- Iniciar sesión como otro principal sin salir de la herramienta.
- Imprimir o guardar listas de principales y listas de políticas.
- Consultar y buscar listas de principales y listas de políticas.

La herramienta SEAM también proporciona ayuda contextual y ayuda general en pantalla.

Los siguientes mapas de tareas ofrecen consejos sobre las distintas tareas que puede realizar con la herramienta SEAM:

- “Administración de los principales de Kerberos (mapa de tareas)” en la página 476
- “Administración de las políticas de Kerberos (mapa de tareas)” en la página 490

También, puede ir a “Descripción de los paneles de la herramienta SEAM” en la página 499 para obtener descripciones de todos los atributos de principales y atributos de políticas que puede especificar o ver en la herramienta SEAM.

## Equivalentes de línea de comandos de la herramienta SEAM

En esta sección se muestran los comandos `kadmin` que proporcionan las mismas capacidades que la herramienta SEAM. Estos comandos se pueden utilizar sin ejecutar un sistema de ventana X. Aunque la mayoría de los procedimientos de este capítulo utilizan la herramienta SEAM, muchos procedimientos también proporcionan ejemplos correspondientes que utilizan equivalentes de línea de comandos.

**TABLA 23-1** Equivalentes de línea de comandos de la herramienta SEAM

| Procedimiento herramienta SEAM                                   | Comando <code>kadmin</code> equivalente                      |
|------------------------------------------------------------------|--------------------------------------------------------------|
| Ver lista de principales                                         | <code>list_principals</code> o <code>get_principals</code>   |
| Ver atributos de un principal                                    | <code>get_principal</code>                                   |
| Crear un principal nuevo                                         | <code>add_principal</code>                                   |
| Duplicar un principal                                            | No hay equivalente de línea de comandos                      |
| Modificar un principal                                           | <code>modify_principal</code> o <code>change_password</code> |
| Suprimir un principal                                            | <code>delete_principal</code>                                |
| Configurar valores predeterminados para crear principales nuevos | No hay equivalente de línea de comandos                      |
| Ver lista de políticas                                           | <code>list_policies</code> o <code>get_policies</code>       |
| Ver atributos de una política                                    | <code>get_policy</code>                                      |
| Crear una política nueva                                         | <code>add_policy</code>                                      |
| Duplicar una política                                            | No hay equivalente de línea de comandos                      |
| Modificar una política                                           | <code>modify_policy</code>                                   |
| Suprimir una política                                            | <code>delete_policy</code>                                   |

## El único archivo modificado por la herramienta SEAM

El único archivo que modifica la herramienta SEAM es el archivo `$HOME/.gkadmin`. Este archivo contiene los valores predeterminados para la creación de principales nuevos. Puede actualizar este archivo seleccionando Properties en el menú Edit.

## Funciones de impresión y ayuda en pantalla de la herramienta SEAM

La herramienta SEAM proporciona funciones de impresión y de ayuda en pantalla. Desde el menú Print, puede enviar lo siguiente a una impresora o un archivo:

- Lista de los principales disponibles en el KDC maestro especificado
- Lista de políticas disponibles en el KDC maestro especificado
- El principal seleccionado actualmente o el principal cargado
- La política seleccionada actualmente o la política cargada

Desde el menú Help puede acceder a la ayuda contextual y a la ayuda general. Al seleccionar la opción Context-Sensitive Help del menú Help, aparece la ventana Context-Sensitive Help y la herramienta cambia al modo de ayuda. En el modo de ayuda, al hacer clic en cualquier campo, etiqueta o botón de la ventana, aparece ayuda sobre esa opción en la ventana Help. Para volver al modo normal de la herramienta, haga clic en Dismiss en la ventana Help.

También puede seleccionar Help Contents, que abre un explorador HTML que proporciona referencias a la descripción general y a la información sobre las tareas que se proporciona en este capítulo.

## Trabajo con listas extensas en la herramienta SEAM

A medida que su sitio comience a acumular un gran número de principales y políticas, la herramienta SEAM tardará cada vez más tiempo en cargar y mostrar las listas de principales y políticas. Por lo tanto, su productividad con la herramienta se reducirá. Existen varias maneras de solucionar este problema.

Primero, puede eliminar totalmente el tiempo de carga de las listas al no hacer que la herramienta SEAM cargue las listas. Puede establecer esta opción seleccionando Properties en el menú Edit, y desactivando el campo Show Lists. Por supuesto, si la herramienta no carga las listas, no podrá mostrar las listas, y usted ya no podrá utilizar los paneles de lista para seleccionar los principales o las políticas. En cambio, deberá escribir el nombre de un principal o una política en el nuevo campo Name proporcionado y, a continuación, seleccionar la operación que desee realizar. De hecho, escribir un nombre equivale a seleccionar un elemento de la lista.

Otra manera de trabajar con listas extensas es almacenarlas en la caché. De hecho, el almacenamiento de las listas en la caché por un tiempo limitado se define como el comportamiento predeterminado para la herramienta SEAM. La herramienta SEAM aún debe cargar inicialmente las listas en la caché. Pero después la herramienta puede utilizar la caché en lugar de recuperar las listas de nuevo. Esta opción elimina la necesidad de cargar las listas del servidor una y otra vez, que es lo que lleva mucho tiempo.

Puede establecer el almacenamiento de listas en la caché seleccionando Properties en el menú Edit. Existen dos opciones de configuración de caché. Puede elegir almacenar la lista en la caché para siempre, o puede especificar un límite de tiempo en el cual la herramienta debe volver a cargar las listas de servidor en la caché.

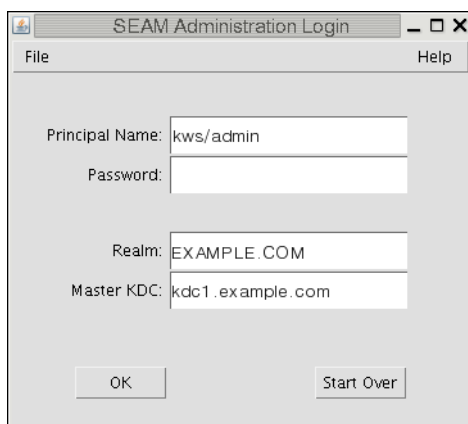
El almacenamiento de las listas en la caché permite utilizar los paneles de lista para seleccionar principales y políticas, por lo que no afecta la manera en que se puede utilizar la herramienta SEAM como lo hace la primera opción. Además, aunque el almacenamiento en la caché no le permite ver los cambios de otros usuarios, puede ver la información más reciente de la de lista según sus cambios, ya que sus cambios actualizan las listas tanto en el servidor como en la caché. Y, si desea actualizar la caché para ver otros cambios y obtener la última copia de las listas, puede utilizar el menú Refresh para actualizar la caché desde el servidor.

## ▼ Cómo iniciar la herramienta SEAM

- 1 Para iniciar la herramienta SEAM utilice el comando `gkadmin`.

```
$ /usr/sbin/gkadmin
```

Aparece la ventana SEAM Administration Login.



- 2 Si no desea utilizar los valores predeterminados, especifique nuevos valores predeterminados.

La ventana automáticamente se rellena con los valores predeterminados. El nombre de principal predeterminado se determina tomando su identidad actual de la variable de entorno

USER y anexándole /admin a ella (*username/admin*). Los valores predeterminados de los campos de dominio (Realm) y de KDC maestro (Master KDC) se seleccionan del archivo /etc/krb5/krb5.conf. Si alguna vez desea recuperar los valores predeterminados, haga clic en Start Over.

**Nota** – Las operaciones de administración que puede realizar cada nombre de principal se rigen por el archivo ACL de Kerberos, /etc/krb5/kadm5.acl. Para obtener más información sobre privilegios limitados, consulte [“Uso de la herramienta SEAM con privilegios de administración de Kerberos limitados” en la página 502.](#)

- 3    **Escriba la contraseña del nombre de principal especificado.**
- 4    **Haga clic en Aceptar.**  
Aparece una ventana en la que se muestran todos los principales.

## Administración de los principales de Kerberos

En esta sección se proporcionan instrucciones detalladas que se deben utilizar para administrar principales con la herramienta SEAM. En esta sección también se proporcionan ejemplos de equivalentes de línea de comandos, si están disponibles.

### Administración de los principales de Kerberos (mapa de tareas)

| Tarea                         | Descripción                                                                                                                                           | Para obtener instrucciones                                                            |
|-------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| Ver lista de principales      | Para ver la lista de principales, haga clic en la ficha Principals.                                                                                   | <a href="#">“Cómo ver la lista de los principales de Kerberos” en la página 478</a>   |
| Ver atributos de un principal | Para ver los atributos de un principal, seleccione el principal en la lista de principales y, a continuación, haga clic en el botón Modify.           | <a href="#">“Cómo ver los atributos de un principal de Kerberos” en la página 480</a> |
| Crear un principal nuevo      | Para crear un principal nuevo, haga clic en el botón Create New en el panel Principal List.                                                           | <a href="#">“Cómo crear un nuevo principal de Kerberos” en la página 482</a>          |
| Duplicar un principal         | Para duplicar un principal, seleccione el principal que desea duplicar en la lista de principales y, a continuación, haga clic en el botón Duplicate. | <a href="#">“Cómo duplicar un principal de Kerberos” en la página 485</a>             |



| Tarea                                                                                     | Descripción                                                                                                                                                                                                                                                                                                                                                                                        | Para obtener instrucciones                                                                                           |
|-------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------|
| Modificar un principal                                                                    | Para modificar un principal, seleccione el principal que desea modificar en la lista de principales y, a continuación, haga clic en el botón Modify.<br><br>Tenga en cuenta que no puede modificar el nombre de un principal. Para cambiar el nombre de un principal, debe duplicar el principal, especificar un nombre nuevo para él, guardarlo y, a continuación, suprimir el antiguo principal. | <a href="#">“Cómo modificar un principal de Kerberos” en la página 485</a>                                           |
| Suprimir un principal                                                                     | Para suprimir un principal, seleccione el principal que desea suprimir en la lista de principales y, a continuación, haga clic en el botón Delete.                                                                                                                                                                                                                                                 | <a href="#">“Cómo suprimir un principal de Kerberos” en la página 487</a>                                            |
| Configurar valores predeterminados para crear principales nuevos                          | Para configurar valores predeterminado para crear principales nuevos, seleccione Properties en el menú Edit.                                                                                                                                                                                                                                                                                       | <a href="#">“Cómo configurar valores predeterminados para crear nuevos principales de Kerberos” en la página 487</a> |
| Modificar los privilegios de administración de Kerberos (archivo <code>kadm5.acl</code> ) | <i>Sólo línea de comandos.</i> Los privilegios de administración de Kerberos determinan qué operaciones puede realizar un principal en la base de datos de Kerberos, por ejemplo, agregar y modificar.<br><br>Debe editar el archivo <code>/etc/krb5/kadm5.acl</code> para modificar los privilegios de administración de Kerberos para cada principal.                                            | <a href="#">“Cómo modificar los privilegios de administración de Kerberos” en la página 488</a>                      |

## Automatización de la creación de nuevos principales de Kerberos

Si bien la herramienta SEAM es fácil de usar, no ofrece una manera de automatizar la creación de nuevos principales. La automatización es especialmente útil si necesita agregar 10 o, incluso, 100 nuevos principales en un breve periodo. Sin embargo, puede utilizar el comando `kadmin.local` en una secuencia de comandos de shell Bourne para hacer exactamente eso.

La siguiente secuencia de comandos de shell es un ejemplo de cómo automatizar la creación de nuevos principales:

```
awk '{ print "ank +needchange -pw", $2, $1 }' < /tmp/princnames |
time /usr/sbin/kadmin.local> /dev/null
```

Este ejemplo está dividido en dos líneas para su legibilidad. La secuencia de comandos lee un archivo llamado `princnames` que contiene los nombres de principales y sus contraseñas, y los agrega a la base de datos de Kerberos. Usted debería crear el archivo `princnames`, que contiene un nombre de principal y su contraseña en cada línea, separados por un espacio o varios. La

opción `+needchange` configura el principal para que se le pida al usuario que introduzca una nueva contraseña la primera vez que inicia sesión con el principal. Esta práctica ayuda a garantizar que las contraseñas del archivo `princnames` no sean un riesgo de seguridad.

Puede crear secuencias de comandos más elaboradas. Por ejemplo, la secuencia de comandos podría utilizar la información del servicio de nombres para obtener la lista de nombres de usuario para los nombres de principales. Lo que usted hace y cómo lo hace está determinado por las necesidades del sitio y su experiencia en secuencias de comandos.

## ▼ **Cómo ver la lista de los principales de Kerberos**

Después de este procedimiento se muestra un ejemplo del equivalente de línea de comandos.

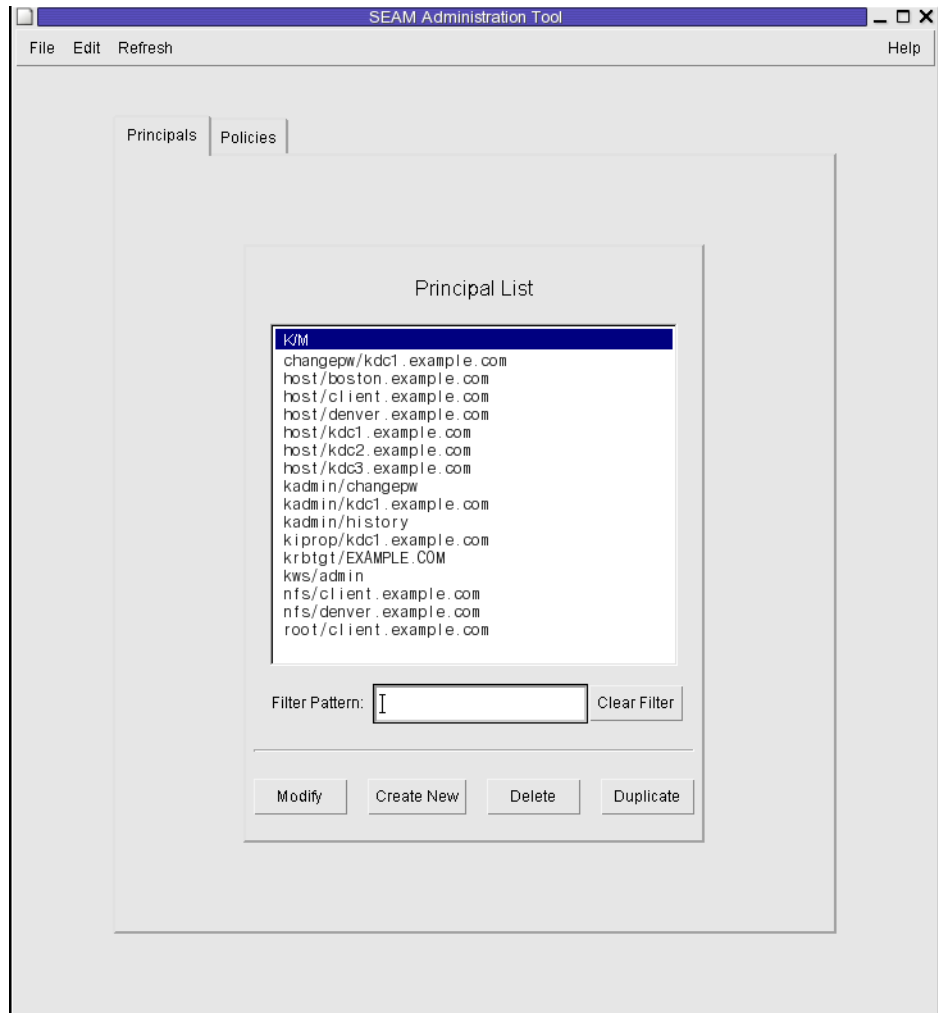
### **1 Si es necesario, inicie la herramienta SEAM.**

Para obtener más información, consulte [“Cómo iniciar la herramienta SEAM” en la página 475](#).

```
$ /usr/sbin/gkadmin
```

## 2 Haga clic en la ficha Principals.

Aparecerá la lista de principales.



## 3 Muestre un principal específico o una sublista de principales.

Escriba una cadena de filtro en el campo de filtro y, a continuación, presione la tecla de retorno. Si el filtro se realiza correctamente, se muestra la lista de principales que coinciden con el filtro.

La cadena de filtro debe estar compuesta por uno o varios caracteres. Debido a que el mecanismo de filtro distingue mayúsculas de minúsculas, deberá utilizar las letras mayúsculas y minúsculas correspondientes para el filtro. Por ejemplo, si escribe la cadena de filtro ge, el mecanismo de filtro mostrará sólo los principales que contengan la cadena ge (por ejemplo, george o edge).

Si desea que aparezca la lista completa de principales, haga clic en Clear Filter.

### **Ejemplo 23–1** Visualización de la lista de los principales de Kerberos (línea de comandos)

En el ejemplo siguiente, el comando `list_principals` de `kadmin` se utiliza para mostrar todos los principales que coinciden con `kadmin*`. Se pueden utilizar comodines con el comando `list_principals`.

```
kadmin: list_principals kadmin*
kadmin/changepw@EXAMPLE.COM
kadmin/kdc1.example.con@EXAMPLE.COM
kadmin/history@EXAMPLE.COM
kadmin: quit
```

## ▼ **Cómo ver los atributos de un principal de Kerberos**

Después de este procedimiento se muestra un ejemplo del equivalente de línea de comandos.

### **1 Si es necesario, inicie la herramienta SEAM.**

Para obtener más información, consulte [“Cómo iniciar la herramienta SEAM” en la página 475](#).

```
$ /usr/sbin/gkadmin
```

### **2 Haga clic en la ficha Principals.**

### **3 Seleccione el principal que desea ver en la lista y, a continuación, haga clic en Modify.**

Aparecerá el panel Principal Basics que contiene algunos de los atributos del principal.

### **4 A continuación, haga clic en Next para ver todos los atributos del principal.**

Tres ventanas contienen información de atributos. Para obtener información sobre los diferentes atributos de cada ventana, seleccione Context-Sensitive Help desde el menú Help. O, para ver las descripciones de todos los atributos de los principales, vaya a [“Descripción de los paneles de la herramienta SEAM” en la página 499](#).

### **5 Cuando haya terminado, haga clic en Cancel.**

### **Ejemplo 23–2** Visualización de los atributos de un principal de Kerberos

En el ejemplo siguiente, se muestra la primera ventana que se verá al visualizar el principal `jdb/admin`.

The screenshot shows the 'SEAM Administration Tool' window with a menu bar (File, Edit, Refresh, Help) and two tabs: 'Principals' and 'Policies'. The 'Principals' tab is active, displaying a 'Principal Basics' configuration form for the principal 'jdb/admin'.

**Principal Basics**

*General*

Principal Name:

Password:

Encryption Key Types:

Policy:

Account Expires:

*Admin History*

Last Principal Change: Sep 28, 2009 1:32:23 PM

Last Changed By: host/admin@EXAMPLE.COM

Comments:

Modify Principal

### Ejemplo 23-3 Visualización de los atributos de un principal de Kerberos (línea de comandos)

En el ejemplo siguiente, el comando `get_principal` de `kadmin` se utiliza para ver los atributos del principal `jdb/admin`.

```
kadmin: getprinc jdb/admin
Principal: jdb/admin@EXAMPLE.COM
```

```
Expiration date: [never]
Last password change: [never]
```

```
Password expiration date: Wed Apr 14 11:53:10 PDT 2011
Maximum ticket life: 1 day 16:00:00
Maximum renewable life: 1 day 16:00:00
```

```
Last modified: Mon Sep 28 13:32:23 PST 2009 (host/admin@EXAMPLE.COM)
Last successful authentication: [never]
Last failed authentication: [never]
Failed password attempts: 0
Number of keys: 1
Key: vno 1, AES-256 CTS mode with 96-bit SHA-1 HMAC, no salt
Key: vno 1, AES-128 CTS mode with 96-bit SHA-1 HMAC, no salt
Key: vno 1, Triple DES with HMAC/sha1, no salt
Key: vno 1, ArcFour with HMAC/md5, no salt
Key: vno 1, DES cbc mode with RSA-MD5, no salt
Attributes: REQUIRES_HW_AUTH
Policy: [none]
kadmin: quit
```

## ▼ Cómo crear un nuevo principal de Kerberos

Después de este procedimiento se muestra un ejemplo del equivalente de línea de comandos.

### 1 Si es necesario, inicie la herramienta SEAM.

Para obtener más información, consulte [“Cómo iniciar la herramienta SEAM” en la página 475](#).

---

**Nota** – Si va a crear un nuevo principal que pueda necesitar una nueva política, debe crear la nueva política antes de crear el nuevo principal. Vaya a [“Cómo crear una nueva política de Kerberos” en la página 495](#).

---

```
$ /usr/sbin/gkadmin
```

### 2 Haga clic en la ficha Principals.

### 3 Haga clic en New.

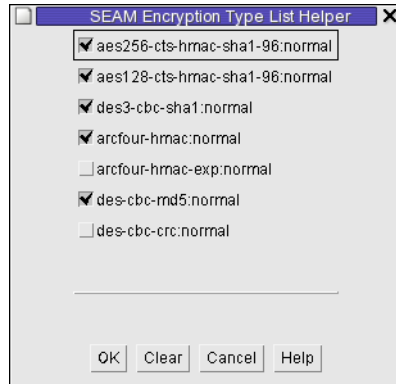
Aparecerá el panel Principal Basics que contiene algunos de los atributos del principal que se está visualizando.

### 4 Especifique un nombre de principal y una contraseña.

Tanto el nombre de principal como la contraseña son obligatorios.

### 5 Especifique los tipos de cifrado para el principal.

Haga clic en el cuadro ubicado a la derecha del campo de tipos de clave de cifrado para abrir una nueva ventana que muestre todos los tipos de clave de cifrado disponibles. Después de seleccionar los tipos de cifrado necesarios, haga clic en OK.



### 6 Especifique la política para el principal.

### 7 Especifique los valores para los atributos del principal y, a continuación, haga clic en Next para especificar más atributos.

Tres ventanas contienen información de atributos. Para obtener información sobre los diferentes atributos de cada ventana, seleccione Context-Sensitive Help desde el menú Help. O, para ver las descripciones de todos los atributos de los principales, vaya a [“Descripción de los paneles de la herramienta SEAM” en la página 499](#).

### 8 Haga clic en Save para guardar el principal, o bien, haga clic en Done en el último panel.

### 9 Si es necesario, configure los privilegios de administración de Kerberos para el nuevo principal en el archivo `/etc/krb5/kadm5.acL`.

Para obtener más detalles, consulte [“Cómo modificar los privilegios de administración de Kerberos” en la página 488](#).

## Ejemplo 23–4 Creación de un nuevo principal de Kerberos

En el siguiente ejemplo se muestra el panel Principal Basics cuando se crea un nuevo principal denominado pak. La política se establece en testuser.

The screenshot shows the SEAM Administration Tool window. The 'Principals' tab is selected. The 'Principal Basics' form is displayed with the following fields and values:

- Principal Name:** pak
- Password:** (masked with asterisks)
- Generate Random Password:** (button)
- Encryption Key Types:** aes256-cts-hmac-sha1-96:no
- Policy:** testuser
- Account Expires:** Oct 8, 2010 10:49:40 AM
- Admin History:**
  - Last Principal Change: Oct 8, 2009 11:35:10 AM
  - Last Changed By: kathys
  - Comments: (empty text box)

At the bottom of the form are buttons for 'Save', 'Previous', 'Next', and 'Cancel'. Below the form, the text 'Create New Principal- \*CHANGES\*' is visible.

### Ejemplo 23-5 Creación de un nuevo principal de Kerberos (línea de comandos)

En el ejemplo siguiente, el comando `add_principal` de `kadmin` se utiliza para crear un nuevo principal denominado `pak`. La política del principal se establece en `testuser`.

```
kadmin: add_principal -policy testuser pak
Enter password for principal "pak@EXAMPLE.COM": <Type the password>
Re-enter password for principal "pak@EXAMPLE.COM": <Type the password again>
Principal "pak@EXAMPLE.COM" created.
kadmin: quit
```



## ▼ Cómo duplicar un principal de Kerberos

En este procedimiento se explica cómo utilizar todos los atributos de un principal existente, o algunos de ellos, para crear un nuevo principal. No hay equivalente de línea de comandos para este procedimiento.

**1 Si es necesario, inicie la herramienta SEAM.**

Para obtener más información, consulte [“Cómo iniciar la herramienta SEAM” en la página 475.](#)

```
$ /usr/sbin/gkadmin
```

**2 Haga clic en la ficha Principals.**

**3 Seleccione el principal que desea duplicar en la lista y, a continuación, haga clic en Duplicate.**

Aparecerá el panel Principal Basics. Todos los atributos del principal seleccionado se duplican, excepto los campos Principal Name y Password, que están vacíos.

**4 Especifique un nombre de principal y una contraseña.**

Tanto el nombre de principal como la contraseña son obligatorios. Para realizar un duplicado exacto del principal que ha seleccionado, haga clic en Save y vaya al [Paso 7](#).

**5 Especifique diferentes valores para los atributos del principal y, a continuación, haga clic en Next para especificar más atributos.**

Tres ventanas contienen información de atributos. Para obtener información sobre los diferentes atributos de cada ventana, seleccione Context-Sensitive Help desde el menú Help. O, para ver las descripciones de todos los atributos de los principales, vaya a [“Descripción de los paneles de la herramienta SEAM” en la página 499.](#)

**6 Haga clic en Save para guardar el principal, o bien, haga clic en Done en el último panel.**

**7 Si es necesario, configure los privilegios de administración de Kerberos para el principal en el archivo `/etc/krb5/kadm5.ac1`.**

Para obtener más información, consulte [“Cómo modificar los privilegios de administración de Kerberos” en la página 488.](#)

## ▼ Cómo modificar un principal de Kerberos

Después de este procedimiento se muestra un ejemplo del equivalente de línea de comandos.

**1 Si es necesario, inicie la herramienta SEAM.**

Para obtener más información, consulte [“Cómo iniciar la herramienta SEAM” en la página 475.](#)

```
$ /usr/sbin/gkadmin
```

**2 Haga clic en la ficha Principals.****3 Seleccione el principal que desea modificar en la lista y, a continuación, haga clic en Modify.**

Aparecerá el panel Principal Basics que contiene algunos de los atributos del principal que se está visualizando.

**4 Modifique los atributos del principal y, a continuación, haga clic en Next para modificar más atributos.**

Tres ventanas contienen información de atributos. Para obtener información sobre los diferentes atributos de cada ventana, seleccione Context-Sensitive Help desde el menú Help. O, para ver las descripciones de todos los atributos de los principales, vaya a [“Descripción de los paneles de la herramienta SEAM” en la página 499](#).

---

**Nota** – No puede modificar el nombre de un principal. Para cambiar el nombre de un principal, debe duplicar el principal, especificar un nombre nuevo para él, guardarlo y, a continuación, suprimir el antiguo principal.

---

**5 Haga clic en Save para guardar el principal, o bien, haga clic en Done en el último panel.****6 Modifique los privilegios de administración de Kerberos para el principal en el archivo `/etc/krb5/kadm5.ac1`.**

Para obtener más información, consulte [“Cómo modificar los privilegios de administración de Kerberos” en la página 488](#).

**Ejemplo 23–6 Modificación de la contraseña de un principal de Kerberos (línea de comandos)**

En el ejemplo siguiente, el comando `change_password` de `kadmin` se utiliza para modificar la contraseña para el principal `jdb`. El comando `change_password` no le permitirá cambiar la contraseña por una contraseña que ya esté en el historial de contraseñas del principal.

```
kadmin: change_password jdb
Enter password for principal "jdb": <Type the new password>
Re-enter password for principal "jdb": <Type the password again>
Password for "jdb@EXAMPLE.COM" changed.
kadmin: quit
```

Para modificar otros atributos de un principal, debe utilizar el comando `modify_principal` de `kadmin`.

## ▼ Cómo suprimir un principal de Kerberos

Después de este procedimiento se muestra un ejemplo del equivalente de línea de comandos.

### 1 Si es necesario, inicie la herramienta SEAM.

Para obtener más información, consulte [“Cómo iniciar la herramienta SEAM” en la página 475.](#)

```
$ /usr/sbin/gkadmin
```

### 2 Haga clic en la ficha Principals.

### 3 Seleccione el principal que desea suprimir en la lista y, a continuación, haga clic en Delete.

Una vez que confirme la supresión, el principal se suprimirá.

### 4 Elimine el principal del archivo de la lista de control de acceso (ACL) de Kerberos, `/etc/krb5/kadm5.acl`.

Para obtener más información, consulte [“Cómo modificar los privilegios de administración de Kerberos” en la página 488.](#)

## Ejemplo 23–7 Supresión de un principal de Kerberos (línea de comandos)

En el ejemplo siguiente, el comando `delete_principal` de `kadmin` se utiliza para suprimir el principal `jdb`.

```
kadmin: delete_principal pak
Are you sure you want to delete the principal "pak@EXAMPLE.COM"? (yes/no): yes
Principal "pak@EXAMPLE.COM" deleted.
Make sure that you have removed this principal from all ACLs before reusing.
kadmin: quit
```

## ▼ Cómo configurar valores predeterminados para crear nuevos principales de Kerberos

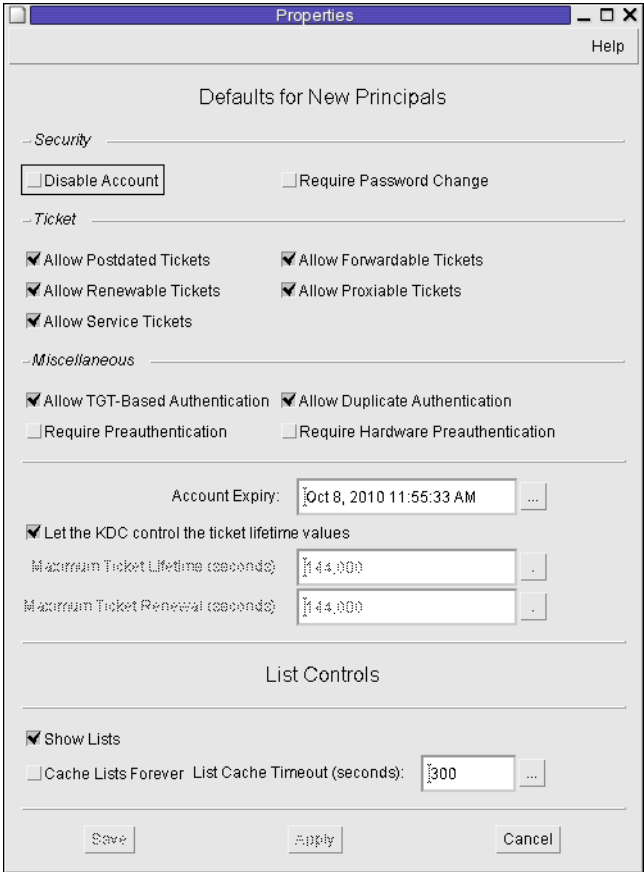
No hay equivalente de línea de comandos para este procedimiento.

### 1 Si es necesario, inicie la herramienta SEAM.

Para obtener más información, consulte [“Cómo iniciar la herramienta SEAM” en la página 475.](#)

```
$ /usr/sbin/gkadmin
```

- 2 **Elija Properties en el menú Edit.**  
Aparecerá la ventana Properties.



- 3 **Seleccione los valores predeterminados que desea utilizar para crear nuevos principales.**  
Para obtener información sobre los diferentes atributos de cada ventana, seleccione Context-Sensitive Help desde el menú Help.
- 4 **Haga clic en Guardar.**

## ▼ **Cómo modificar los privilegios de administración de Kerberos**

Aunque su sitio probablemente tenga muchos principales de usuario, en general, se prefiere que sólo unos pocos usuarios puedan administrar la base de datos de Kerberos. Los privilegios para

administrar la base de datos de Kerberos se determinan mediante el archivo de la lista de control de acceso (ACL) de Kerberos, `kadm5.ac1`. Mediante el archivo `kadm5.ac1` se pueden permitir o prohibir privilegios para cada principal. También puede utilizar el comodín `*` en el nombre del principal para especificar privilegios para grupos de principales.

**Antes de empezar** Debe asumir el rol `root`. Para obtener más información, consulte [“Cómo usar los derechos administrativos que tiene asignados” en la página 164](#).

● **Edite el archivo `/etc/krb5/kadm5.ac1`.**

Una entrada del archivo `kadm5.ac1` debe tener el siguiente formato:

*principal privileges [principal-target]*

|                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |   |                                                             |   |                                                            |   |                                                               |   |                                                                  |   |                                                                      |   |                                                                                    |       |                                                        |
|--------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|-------------------------------------------------------------|---|------------------------------------------------------------|---|---------------------------------------------------------------|---|------------------------------------------------------------------|---|----------------------------------------------------------------------|---|------------------------------------------------------------------------------------|-------|--------------------------------------------------------|
| <i>principal</i>         | <p>Especifica el principal al que se le otorgan los privilegios. Cualquier parte del nombre del principal puede incluir el comodín <code>*</code>, que es útil para proporcionar los mismos privilegios para un grupo de principales. Por ejemplo, si desea especificar todos los principales con la instancia <code>admin</code>, debe utilizar <code>*/admin@realm</code>.</p> <p>Tenga en cuenta que un uso común de una instancia <code>admin</code> es conceder privilegios independientes (por ejemplo, acceso de administración a la base de datos de Kerberos) a un principal de Kerberos individual. Por ejemplo, el usuario <code>jdb</code> puede tener un principal para su uso administrativo, denominado <code>jdb/admin</code>. De esta manera, el usuario <code>jdb</code> obtiene los tickets de <code>jdb/admin</code> sólo cuando realmente necesita utilizar esos privilegios.</p>                                                                                                                                                    |   |                                                             |   |                                                            |   |                                                               |   |                                                                  |   |                                                                      |   |                                                                                    |       |                                                        |
| <i>privileges</i>        | <p>Especifica qué operaciones puede, o no puede, realizar el principal. Este campo consta de una cadena compuesta por uno o varios caracteres de la siguiente lista, o por sus equivalentes en mayúscula. Si el carácter está en mayúscula (o no se ha especificado), la operación está prohibida. Si el carácter está en minúscula, la operación está permitida.</p> <table><tr><td>a</td><td>Permite o prohíbe la agregación de principales o políticas.</td></tr><tr><td>d</td><td>Permite o prohíbe la supresión de principales o políticas.</td></tr><tr><td>m</td><td>Permite o prohíbe la modificación de principales o políticas.</td></tr><tr><td>c</td><td>Permite o prohíbe la modificación de contraseñas de principales.</td></tr><tr><td>i</td><td>Permite o prohíbe realizar consultas a la base de datos de Kerberos.</td></tr><tr><td>l</td><td>Permite o prohíbe mostrar principales o políticas en la base de datos de Kerberos.</td></tr><tr><td>x o *</td><td>Permite todos los privilegios (<code>admcil</code>).</td></tr></table> | a | Permite o prohíbe la agregación de principales o políticas. | d | Permite o prohíbe la supresión de principales o políticas. | m | Permite o prohíbe la modificación de principales o políticas. | c | Permite o prohíbe la modificación de contraseñas de principales. | i | Permite o prohíbe realizar consultas a la base de datos de Kerberos. | l | Permite o prohíbe mostrar principales o políticas en la base de datos de Kerberos. | x o * | Permite todos los privilegios ( <code>admcil</code> ). |
| a                        | Permite o prohíbe la agregación de principales o políticas.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |   |                                                             |   |                                                            |   |                                                               |   |                                                                  |   |                                                                      |   |                                                                                    |       |                                                        |
| d                        | Permite o prohíbe la supresión de principales o políticas.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |   |                                                             |   |                                                            |   |                                                               |   |                                                                  |   |                                                                      |   |                                                                                    |       |                                                        |
| m                        | Permite o prohíbe la modificación de principales o políticas.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |   |                                                             |   |                                                            |   |                                                               |   |                                                                  |   |                                                                      |   |                                                                                    |       |                                                        |
| c                        | Permite o prohíbe la modificación de contraseñas de principales.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |   |                                                             |   |                                                            |   |                                                               |   |                                                                  |   |                                                                      |   |                                                                                    |       |                                                        |
| i                        | Permite o prohíbe realizar consultas a la base de datos de Kerberos.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |   |                                                             |   |                                                            |   |                                                               |   |                                                                  |   |                                                                      |   |                                                                                    |       |                                                        |
| l                        | Permite o prohíbe mostrar principales o políticas en la base de datos de Kerberos.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |   |                                                             |   |                                                            |   |                                                               |   |                                                                  |   |                                                                      |   |                                                                                    |       |                                                        |
| x o *                    | Permite todos los privilegios ( <code>admcil</code> ).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |   |                                                             |   |                                                            |   |                                                               |   |                                                                  |   |                                                                      |   |                                                                                    |       |                                                        |
| <i>destino_principal</i> | <p>Cuando se especifica un principal en este campo, los <i>privileges</i> se aplican al <i>principal</i> sólo cuando el <i>principal</i> opera en el <i>principal-target</i>. Cualquier parte del nombre del principal puede incluir el comodín <code>*</code>, que es útil para agrupar principales.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |   |                                                             |   |                                                            |   |                                                               |   |                                                                  |   |                                                                      |   |                                                                                    |       |                                                        |

**Ejemplo 23–8**    Modificación de los privilegios de administración de Kerberos

La siguiente entrada en el archivo `kadm5.ac1` otorga a cualquier principal del dominio `EXAMPLE.COM` con la instancia `admin` todos los privilegios de la base de datos de Kerberos:

```
*/admin@EXAMPLE.COM *
```

La siguiente entrada del archivo `kadm5.ac1` le otorga al principal `jdb@EXAMPLE.COM` los privilegios para agregar, mostrar y consultar cualquier principal que tenga la instancia `root`.

```
jdb@EXAMPLE.COM ali */root@EXAMPLE.COM
```

# Administración de las políticas de Kerberos

En esta sección se proporcionan instrucciones detalladas que se deben utilizar para administrar políticas con la herramienta SEAM. En esta sección también se proporcionan ejemplos de equivalentes de línea de comandos, si están disponibles.

## Administración de las políticas de Kerberos (mapa de tareas)

| Tarea                         | Descripción                                                                                                                                                                                                                                                                                                                                                                                                   | Para obtener instrucciones                                                            |
|-------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| Ver lista de políticas        | Para ver la lista de políticas, haga clic en la ficha <i>Policies</i> .                                                                                                                                                                                                                                                                                                                                       | <a href="#">“Cómo ver la lista de políticas de Kerberos” en la página 491</a>         |
| Ver atributos de una política | Para ver los atributos de una política, seleccione la política en la lista de políticas y, a continuación, haga clic en el botón <i>Modify</i> .                                                                                                                                                                                                                                                              | <a href="#">“Cómo ver los atributos de una política de Kerberos” en la página 493</a> |
| Crear una política nueva      | Para crear una política nueva, haga clic en el botón <i>Create New</i> en el panel <i>Policy List</i> .                                                                                                                                                                                                                                                                                                       | <a href="#">“Cómo crear una nueva política de Kerberos” en la página 495</a>          |
| Duplicar una política         | Para duplicar una política, seleccione la política que desea duplicar en la lista de políticas y, a continuación, haga clic en el botón <i>Duplicate</i> .                                                                                                                                                                                                                                                    | <a href="#">“Cómo duplicar una política de Kerberos” en la página 497</a>             |
| Modificar una política        | <p>Para modificar una política, seleccione la política que desea modificar en la lista de políticas y, a continuación, haga clic en el botón <i>Modify</i>.</p> <p>Tenga en cuenta que no puede modificar el nombre de una política. Para cambiar el nombre de una política, debe duplicar la política, especificar un nombre nuevo para ella, guardarla y, a continuación, suprimir la antigua política.</p> | <a href="#">“Cómo modificar una política de Kerberos” en la página 497</a>            |

| Tarea                 | Descripción                                                                                                                                     | Para obtener instrucciones                                                |
|-----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------|
| Suprimir una política | Para suprimir una política, seleccione la política que desea suprimir en la lista de políticas y, a continuación, haga clic en el botón Delete. | <a href="#">“Cómo suprimir una política de Kerberos” en la página 498</a> |

## ▼ Cómo ver la lista de políticas de Kerberos

Después de este procedimiento se muestra un ejemplo del equivalente de línea de comandos.

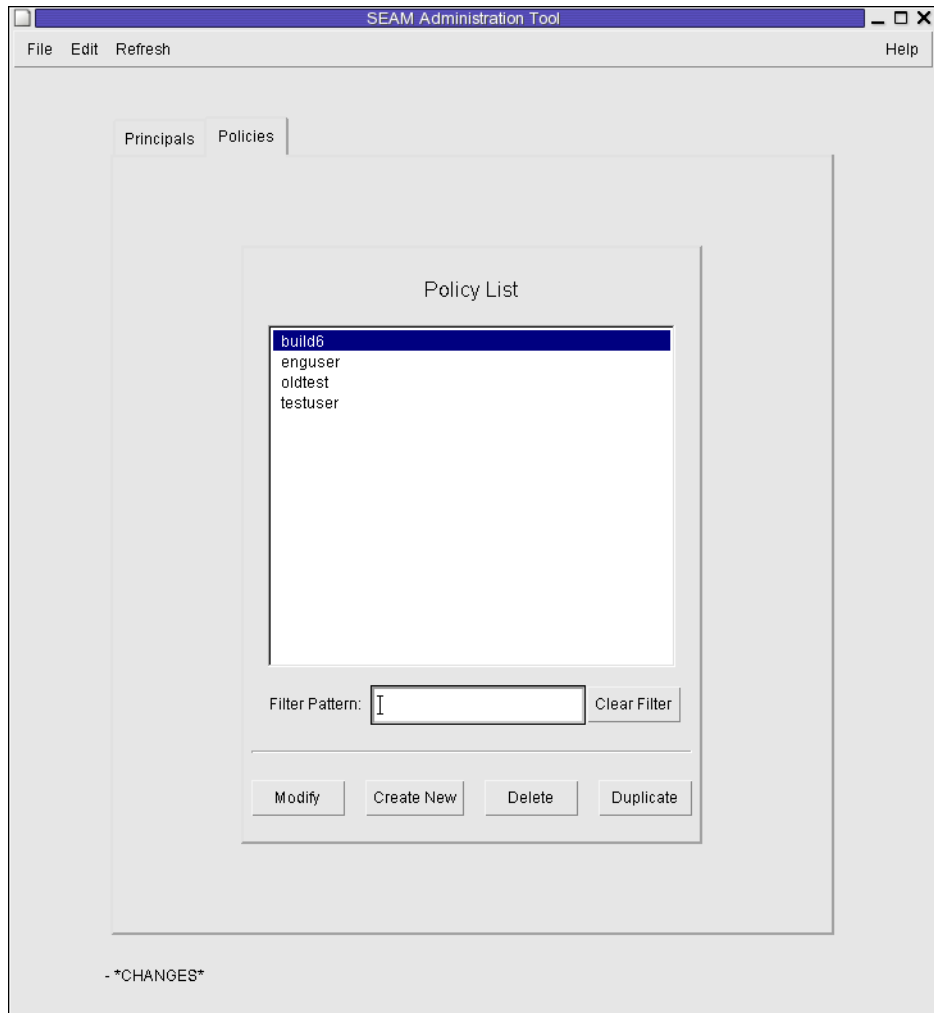
### 1 Si es necesario, inicie la herramienta SEAM.

Para obtener más información, consulte [“Cómo iniciar la herramienta SEAM” en la página 475](#).

```
$ /usr/sbin/gkadmin
```

## 2 Haga clic en la ficha Políticas.

Aparecerá la lista de políticas.



## 3 Muestre una política específica o una sublista de políticas.

Escriba una cadena de filtro en el campo de filtro y, a continuación, presione la tecla e retorno. Si el filtro se realiza correctamente, se muestra la lista de políticas que coinciden con el filtro.

La cadena de filtro debe estar compuesta por uno o varios caracteres. Debido a que el mecanismo de filtro distingue mayúsculas de minúsculas, deberá utilizar las letras mayúsculas y minúsculas correspondientes para el filtro. Por ejemplo, si escribe la cadena de filtro ge, el mecanismo de filtro mostrará sólo las políticas que contengan la cadena ge (por ejemplo, george o edge).



Si desea que aparezca la lista completa de políticas, haga clic en Clear Filter.

### **Ejemplo 23–9** Visualización de la lista de las políticas de Kerberos (línea de comandos)

En el ejemplo siguiente, el comando `list_policies` de `kadmin` se utiliza para mostrar todas las políticas que coinciden con `*user*`. Se pueden utilizar comodines con el comando `list_policies`.

```
kadmin: list_policies *user*
testuser
enguser
kadmin: quit
```

## ▼ **Cómo ver los atributos de una política de Kerberos**

Después de este procedimiento se muestra un ejemplo del equivalente de línea de comandos.

### **1** Si es necesario, inicie la herramienta SEAM.

Para obtener más información, consulte [“Cómo iniciar la herramienta SEAM” en la página 475](#).

```
$ /usr/sbin/gkadmin
```

### **2** Haga clic en la ficha Policies.

### **3** Seleccione la política que desea ver en la lista y, a continuación, haga clic en Modify.

Aparecerá el panel Policy Details.

### **4** Cuando haya terminado, haga clic en Cancel.

### **Ejemplo 23–10** Visualización de los atributos de una política de Kerberos

En el ejemplo siguiente se muestra el panel Policy Details que se verá al visualizar la política `test`.



### Ejemplo 23-11 Visualización de los atributos de una política de Kerberos (línea de comandos)

En el ejemplo siguiente, el comando `get_policy` de `kadmin` se utiliza para ver los atributos de la política `enguser`.

```
kadmin: get_policy enguser
Policy: enguser
Maximum password life: 2592000
Minimum password life: 0
Minimum password length: 8
Minimum number of password character classes: 2
Number of old keys kept: 3
Reference count: 0
kadmin: quit
```

El recuento de referencia (Reference count) es el número de los principales que utilizan esta política.

## ▼ **Cómo crear una nueva política de Kerberos**

Después de este procedimiento se muestra un ejemplo del equivalente de línea de comandos.

**1 Si es necesario, inicie la herramienta SEAM.**

Para obtener más información, consulte [“Cómo iniciar la herramienta SEAM”](#) en la página 475.

```
$ /usr/sbin/gkadmin
```

**2 Haga clic en la ficha Políticas.**

**3 Haga clic en New.**

Aparecerá el panel Policy Details.

**4 Especifique un nombre para la política en el campo Policy Name.**

El nombre de la política es obligatorio.

**5 Especifique valores para los atributos de la política.**

Para obtener información sobre los diferentes atributos de esta ventana, seleccione Context-Sensitive Help desde el menú Help. También puede ir a la [Tabla 23–5](#) para ver la descripción de todos los atributos de políticas.

**6 Haga clic en Save para guardar la política, o haga clic en Done.**

### **Ejemplo 23–12 Creación de una nueva política de Kerberos**

En el siguiente ejemplo, se crea una nueva política denominada `build11`. El valor de clases mínimas para contraseña, Minimum Password Classes, se establece en 3.



### Ejemplo 23-13 Creación de una nueva política de Kerberos (línea de comandos)

En el ejemplo siguiente, el comando `add_policy` de `kadmin` se utiliza para crear la política `build11`. Esta política requiere al menos 3 clases de caracteres en una contraseña.

```
$ kadmin
kadmin: add_policy -minclasses 3 build11
kadmin: quit
```

## ▼ Cómo duplicar una política de Kerberos

En este procedimiento se explica cómo utilizar todos los atributos de una política existente, o algunos de ellos, para crear una nueva política. No hay equivalente de línea de comandos para este procedimiento.

### 1 Si es necesario, inicie la herramienta SEAM.

Para obtener más información, consulte [“Cómo iniciar la herramienta SEAM” en la página 475](#).

```
$ /usr/sbin/gkadmin
```

### 2 Haga clic en la ficha Políticas.

### 3 Seleccione la política que desea duplicar en la lista y, a continuación, haga clic en Duplicate.

Aparecerá el panel Policy Details. Todos los atributos de la política seleccionada se duplican, excepto el campo Policy Name, que está vacío.

### 4 Especifique un nombre para la política duplicada en el campo Policy Name.

El nombre de la política es obligatorio. Para realizar un duplicado exacto de la política que ha seleccionado, vaya al [Paso 6](#).

### 5 Especifique valores diferentes para los atributos de la política.

Para obtener información sobre los diferentes atributos de esta ventana, seleccione Context-Sensitive Help desde el menú Help. También puede ir a la [Tabla 23–5](#) para ver la descripción de todos los atributos de políticas.

### 6 Haga clic en Save para guardar la política, o haga clic en Done.

## ▼ Cómo modificar una política de Kerberos

Después de este procedimiento se muestra un ejemplo del equivalente de línea de comandos.

### 1 Si es necesario, inicie la herramienta SEAM.

Para obtener detalles, consulte [“Cómo iniciar la herramienta SEAM” en la página 475](#).

```
$ /usr/sbin/gkadmin
```

### 2 Haga clic en la ficha Políticas.

### 3 Seleccione la política que desea modificar en la lista y, a continuación, haga clic en Modify.

Aparecerá el panel Policy Details.

**4 Modifique los atributos de la política.**

Para obtener información sobre los diferentes atributos de esta ventana, seleccione Context-Sensitive Help desde el menú Help. También puede ir a la [Tabla 23–5](#) para ver la descripción de todos los atributos de políticas.

---

**Nota** – No puede modificar el nombre de una política. Para cambiar el nombre de una política, debe duplicar la política, especificar un nombre nuevo para ella, guardarla y, a continuación, suprimir la antigua política.

---

**5 Haga clic en Save para guardar la política, o haga clic en Done.****Ejemplo 23–14 Modificación de una política de Kerberos (línea de comandos)**

En el ejemplo siguiente, el comando `modify_policy` de `kadmin` se utiliza para cambiar la longitud mínima de una contraseña por cinco caracteres para la política `build11`.

```
$ kadmin
kadmin: modify_policy -minlength 5 build11
kadmin: quit
```

## ▼ **Cómo suprimir una política de Kerberos**

Después de este procedimiento se muestra un ejemplo del equivalente de línea de comandos.

---

**Nota** – Antes de suprimir una política, debe cancelarla en todos los principales que la estén utilizando. Para ello, debe modificar el atributo de política de los principales correspondientes. La política no se puede suprimir si algún principal la está utilizando.

---

**1 Si es necesario, inicie la herramienta SEAM.**

Para obtener más información, consulte “[Cómo iniciar la herramienta SEAM](#)” en la [página 475](#).

```
$ /usr/sbin/gkadmin
```

**2 Haga clic en la ficha Políticas.****3 Seleccione la política que desea suprimir en la lista y, a continuación, haga clic en Delete.**

Una vez que confirme la supresión, la política se suprimirá.

**Ejemplo 23–15 Supresión de una política de Kerberos (línea de comandos)**

En el ejemplo siguiente, el comando `delete_policy` de `kadmin` se utiliza para suprimir la política `build11`.

```
kadmin: delete_policy build11
Are you sure you want to delete the policy "build11"? (yes/no): yes
kadmin: quit
```

Antes de suprimir una política, debe cancelarla en todos los principales que la estén utilizando. Para ello, debe utilizar el comando `modify_principal -policy` de `kadmin` en los principales correspondientes. El comando `delete_policy` fallará, si la política está siendo utilizada por un principal.

## Referencia de la herramienta SEAM

En esta sección, se proporcionan descripciones de cada panel de la herramienta SEAM. Asimismo, se proporciona información sobre el uso de privilegios limitados en la herramienta SEAM.

### Descripción de los paneles de la herramienta SEAM

En esta sección se ofrece la descripción de todos los atributos de los principales y las políticas que se pueden especificar o ver en la herramienta SEAM. Los atributos están organizados según el panel en el que aparecen.

**TABLA 23–2** Atributos del panel Principal Basics de la herramienta SEAM

| Atributo              | Descripción                                                                                                                                                                                                                                    |
|-----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Principal Name        | El nombre del principal (que es la parte <i>principal/instance</i> de un nombre de principal completo). Un principal es una identidad única a la que el KDC puede asignar tickets.<br><br>Si modifica un principal, no puede editar su nombre. |
| Password              | La contraseña para el principal. Puede utilizar el botón Generate Random Password para crear una contraseña aleatoria para el principal.                                                                                                       |
| Policy                | Un menú de las políticas disponibles para el principal.                                                                                                                                                                                        |
| Account Expires       | La fecha y hora en que caduca la cuenta del principal. Cuando la cuenta caduque, el principal ya no podrá obtener un ticket de otorgamiento de tickets (TGT) y quizá no pueda iniciar sesión.                                                  |
| Last Principal Change | La fecha en la que se modificó por última vez la información del principal. (Sólo lectura)                                                                                                                                                     |
| Last Changed By       | El nombre del principal que modificó por última vez la cuenta de este principal. (Sólo lectura)                                                                                                                                                |
| Comments              | Comentarios relacionados con el principal (por ejemplo, “Cuenta temporal”).                                                                                                                                                                    |

**TABLA 23–3** Atributos del panel de detalles del principal de la herramienta SEAM

| Atributo     | Descripción                                                                                    |
|--------------|------------------------------------------------------------------------------------------------|
| Last Success | La fecha y hora en que el principal inició sesión correctamente por última vez. (Sólo lectura) |

TABLA 23-3 Atributos del panel de detalles del principal de la herramienta SEAM (Continuación)

| Atributo                   | Descripción                                                                                                                  |
|----------------------------|------------------------------------------------------------------------------------------------------------------------------|
| Last Failure               | La fecha y hora en que se produjo un fallo en el inicio de sesión del principal por última vez. (Sólo lectura)               |
| Failure Count              | El número de veces que se produjeron fallos en el inicio de sesión del principal. (Sólo lectura)                             |
| Last Password Change       | La fecha y la hora en que se modificó por última vez la contraseña del principal. (Sólo lectura)                             |
| Password Expires           | La fecha y hora en que caduca la contraseña actual del principal.                                                            |
| Key Version                | El número de versión de clave del principal. En general, este atributo sólo se cambia cuando una contraseña está en peligro. |
| Maximum Lifetime (seconds) | El período máximo durante el cual un ticket se puede otorgar al principal (sin renovación).                                  |
| Maximum Renewal (seconds)  | El período máximo durante el cual un ticket existente se puede renovar para el principal.                                    |

TABLA 23-4 Atributos del panel de indicadores de principal de la herramienta SEAM

| Atributo (botones de radio) | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Disable Account             | Cuando está activado, impide que el principal inicie sesión. Este atributo proporciona una manera sencilla de congelar temporalmente una cuenta de principal.                                                                                                                                                                                                                                                                         |
| Require Password Change     | Cuando está activado, hace que caduque la contraseña actual del principal, lo cual fuerza al usuario a utilizar el comando <code>kpasswd</code> para crear una contraseña nueva. Este atributo es útil si se produce una infracción de seguridad y, como consecuencia, es necesario asegurarse de que se sustituyan las contraseñas antiguas.                                                                                         |
| Allow Postdated Tickets     | Cuando está activado, permite al principal obtener tickets posfechados.<br><br>Por ejemplo, es posible que necesite utilizar tickets posfechados para trabajos cron que se deben ejecutar fuera del horario comercial, pero no pueda obtener los tickets anticipadamente debido a la corta duración de los tickets.                                                                                                                   |
| Allow Forwardable Tickets   | Cuando está activado, permite al principal obtener tickets reenviables.<br><br>Los tickets reenviables son aquellos que se reenvían al host remoto para proporcionar una sesión de inicio único. Por ejemplo, si está utilizando tickets reenviables y se autentica a usted mismo mediante <code>ftp</code> o <code>rsh</code> , otros servicios, como los servicios NFS, estarán disponibles sin que se le solicite otra contraseña. |
| Allow Renewable Tickets     | Cuando está activado, permite al principal obtener tickets renovables.<br><br>Un principal puede ampliar automáticamente la fecha o la hora de caducidad de un ticket renovable (en lugar de tener que obtener un nuevo ticket una vez que caduca el primero). Actualmente, el servicio NFS es el servicio de tickets que puede renovar tickets.                                                                                      |



TABLA 23-4 Atributos del panel de indicadores de principal de la herramienta SEAM (Continuación)

| Atributo (botones de radio)      | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|----------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Allow Proxiable Tickets          | <p>Cuando está activado, permite al principal obtener tickets que admiten proxy.</p> <p>Un ticket que admite proxy es un ticket que puede ser utilizado por un servicio en nombre de un cliente para realizar una operación para el cliente. Con un ticket que admite proxy, un servicio puede adoptar la identidad de un cliente y obtener un ticket para otro servicio. Sin embargo, el servicio no puede obtener un ticket de otorgamiento de tickets (TGT).</p>                                                      |
| Allow Service Tickets            | <p>Cuando está activado, permite que se emitan tickets de servicio al principal.</p> <p>No debería permitir que se emitan tickets de servicio para los principales <code>kadmin/hostname</code> ni <code>changepw/hostname</code>. Esta práctica garantiza que sólo estos principales puedan actualizar la base de datos KDC.</p>                                                                                                                                                                                        |
| Allow TGT-Based Authentication   | <p>Cuando está activado, permite al principal de servicio proporcionar servicios a otro principal. Más concretamente, este atributo permite al KDC emitir un ticket de servicio para el principal de servicio.</p> <p>Este atributo sólo es válido para los principales de servicio. Cuando no está activado, los tickets de servicio no se pueden emitir para el principal de servicio.</p>                                                                                                                             |
| Allow Duplicate Authentication   | <p>Cuando está activado, permite al principal de usuario obtener tickets de servicio para otros principales de usuario.</p> <p>Este atributo sólo es válido para los principales de usuario. Cuando no está activado, el principal de usuario aún puede obtener tickets de servicio para los principales de servicio, pero no para otros principales de usuario.</p>                                                                                                                                                     |
| Required Preauthentication       | <p>Cuando está activado, el KDC sólo enviará un ticket de otorgamiento de tickets (TGT) solicitado al principal una vez que haya autenticado (mediante el software) que el principal es realmente el principal que está solicitando el TGT. Esta autenticación previa generalmente se realiza mediante una contraseña adicional, por ejemplo, de una tarjeta DES.</p> <p>Cuando no está activado, el KDC no necesita realizar una autenticación previa del principal antes de enviar un TGT solicitado al principal.</p> |
| Required Hardware Authentication | <p>Cuando está activado, el KDC sólo enviará un ticket de otorgamiento de tickets (TGT) solicitado al principal una vez que haya autenticado (mediante el hardware) que el principal es realmente el principal que está solicitando el TGT. La autenticación previa del hardware se puede llevar a cabo, por ejemplo, en un lector de anillos Java.</p> <p>Cuando no está activado, el KDC no necesita realizar una autenticación previa del principal antes de enviar un TGT solicitado al principal.</p>               |

TABLA 23-5 Atributos del panel de características básicas de la política de la herramienta SEAM

| Atributo    | Descripción                                                                                                                                                                               |
|-------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Policy Name | <p>El nombre de la política. Una política es un conjunto de reglas que rigen la contraseña y los tickets de un principal.</p> <p>Si modifica una política, no puede editar su nombre.</p> |

TABLA 23–5 Atributos del panel de características básicas de la política de la herramienta SEAM (Continuación)

| Atributo                            | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Minimum Password Length             | La longitud mínima de la contraseña del principal.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Minimum Password Classes            | <p>El número mínimo de tipos de caracteres diferentes que se deben utilizar en la contraseña del principal.</p> <p>Por ejemplo, un valor de clases mínimo de 2 significa que la contraseña debe tener al menos dos tipos de caracteres diferentes, como letras y números (hi2mom). Un valor de 3 significa que la contraseña debe tener al menos tres tipos de caracteres diferentes, como letras, números y signos de puntuación (hi2mom!). Y así sucesivamente.</p> <p>Un valor de 1 no establece ninguna restricción para el número tipos de caracteres de la contraseña.</p> |
| Saved Password History              | El número de contraseñas anteriores utilizadas por el principal, y una lista de las contraseñas anteriores que no se pueden volver a utilizar.                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Minimum Password Lifetime (seconds) | El período mínimo durante el cual se debe utilizar una contraseña antes de poder modificarla.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Maximum Password Lifetime (seconds) | El período máximo durante el cual se puede utilizar una contraseña antes de tener que modificarla.                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Principals Using This Policy        | El número de principales a los que se aplica actualmente esta política. (Sólo lectura)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

## Uso de la herramienta SEAM con privilegios de administración de Kerberos limitados

Todas las capacidades de la herramienta SEAM están disponibles si su principal admin tiene todos los privilegios para administrar la base de datos de Kerberos. Sin embargo, es posible que tenga privilegios limitados, por ejemplo, que sólo pueda ver la lista de principales o cambiar la contraseña de un principal. Con privilegios de administración de Kerberos limitados, aún puede utilizar la herramienta SEAM. Sin embargo, varias partes de la herramienta SEAM cambian según los privilegios de administración de Kerberos que no se tienen. En la [Tabla 23–6](#) se muestra cómo cambia la herramienta SEAM según los privilegios de administración de Kerberos que se tengan.

El cambio más visual de la herramienta SEAM se produce cuando no se tiene el privilegio de lista. Sin el privilegio de lista, los paneles de lista no muestran la lista de principales ni la de políticas para poder manipularlas. En cambio, debe utilizar el campo Name de los paneles de lista para especificar el principal o la política que desea manipular.

Si inicia sesión en la herramienta SEAM y no tiene suficientes privilegios para realizar tareas en ella, se muestra el siguiente mensaje y se vuelve a la ventana SEAM Administration Login:

Insufficient privileges to use gkadmin: ADMCIL. Please try using another principal.

Para cambiar los privilegios de un principal para que pueda administrar la base de datos de Kerberos, vaya a [“Cómo modificar los privilegios de administración de Kerberos” en la página 488](#).

**TABLA 23–6** Uso de la herramienta SEAM con privilegios de administración de Kerberos limitados

| Privilegio no permitido        | Cómo cambia la herramienta SEAM                                                                                                                                                                                                                                                                                                                                                  |
|--------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| a (agregar)                    | Los botones Create New y Duplicate no están disponibles en los paneles Principal List y Policy List. Si no tiene el privilegio para agregar, no puede crear principales ni políticas nuevos, ni duplicarlos.                                                                                                                                                                     |
| d (suprimir)                   | El botón Delete no está disponible en los paneles Principal List ni Policy List. Si no tiene el privilegio para suprimir, no puede suprimir principales ni políticas.                                                                                                                                                                                                            |
| m (modificar)                  | El botón Modify no está disponible en los paneles Principal List ni Policy List. Si no tiene el privilegio para modificar, no puede modificar principales ni políticas.<br><br>Además, si el botón Modify no está disponible, no puede modificar ninguna contraseña de principal, aunque tenga el privilegio para cambiar contraseñas.                                           |
| c (cambiar contraseña)         | El campo Password del panel Principal Basics es de sólo lectura y no se puede cambiar. Si no tiene el privilegio para cambiar contraseñas, no puede modificar ninguna contraseña de principal.<br><br>Tenga en cuenta que aunque tenga el privilegio para cambiar contraseñas, para poder cambiar la contraseña de un principal también debe tener el privilegio para modificar. |
| i (consultar la base de datos) | Los botones Modify y Duplicate no están disponibles en los paneles Principal List y Policy List. Si no tiene el privilegio para consultar, no puede modificar ni duplicar principales ni políticas.<br><br>Además, si el botón Modify no está disponible, no puede modificar ninguna contraseña de principal, aunque tenga el privilegio para cambiar contraseñas.               |
| l (lista)                      | Las listas de principales y políticas de los paneles de lista no están disponibles. Si no tiene el privilegio de lista, debe utilizar el campo Name de los paneles de lista para especificar el principal o la política que desea manipular.                                                                                                                                     |

## Administración de los archivos keytab

Cada host que proporciona un servicio debe tener un archivo local, denominado *keytab* (la abreviatura en inglés de “tabla de claves”). El archivo keytab contiene el principal para el servicio adecuado, denominado *clave de servicio*. La clave de servicio es utilizada por un servicio para autenticarse a sí misma en el KDC, y sólo es conocida por Kerberos y el servicio. Por ejemplo, si tiene un servidor NFS Kerberizado, ese servidor debe tener un archivo keytab que contenga su principal de servicio `nfs`.

Para agregar una clave de servicio a un archivo keytab, agregue el principal de servicio correspondiente al archivo keytab de un host mediante el comando `ktadd` de `kadmin`. Como está agregando un principal de servicio a un archivo keytab, el principal ya debe existir en la base de datos de Kerberos para que `kadmin` pueda verificar su existencia. En los servidores de aplicaciones que proporcionan servicios Kerberizados, el archivo keytab se encuentra en `/etc/krb5/krb5.keytab`, de manera predeterminada.

Un archivo keytab es análogo a la contraseña de un usuario. De la misma manera que es importante que los usuarios protejan sus contraseñas, es importante que los servidores de aplicaciones protejan sus archivos keytab. Siempre debe guardar los archivos keytab en un disco local y permitir su lectura sólo al usuario `root`. Asimismo, nunca debe enviar un archivo keytab a través una red no segura.

También hay una instancia especial en la que se debe agregar un principal `root` al archivo keytab de un host. Si desea que un usuario del cliente Kerberos monte sistemas de archivos NFS Kerberizados que requieren acceso equivalente a `root`, debe agregar el principal `root` del cliente al archivo keytab del cliente. De lo contrario, los usuarios deberán utilizar el comando `kinit` como `root` para obtener credenciales para el principal `root` del cliente cuando deseen montar un sistema de archivos NFS Kerberizado con acceso `root`, incluso cuando estén utilizando el montador automático.

Otro comando que puede utilizar para administrar los archivos keytab es el comando `ktutil`. Este comando interactivo le permite gestionar el archivo keytab de un host local sin tener privilegios de administración de Kerberos, porque `ktutil` no interactúa con la base de datos de Kerberos como lo hace `kadmin`. Por lo tanto, después de agregar un principal a un archivo keytab, puede usar `ktutil` para ver la lista de claves en un archivo keytab o para deshabilitar temporalmente la autenticación de un servicio.

---

**Nota** – Al cambiar un principal en un archivo keytab mediante el comando `ktadd` en `kadmin`, se genera una clave nueva y esta se agrega al archivo keytab.

---

## Administración de archivos keytab (mapa de tareas)

| Tarea                                                                  | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Para obtener instrucciones                                                                                    |
|------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------|
| Agregar un principal de servicio a un archivo keytab                   | Utilice el comando <code>ktadd</code> de <code>kadmin</code> para agregar un principal de servicio a un archivo keytab.                                                                                                                                                                                                                                                                                                                                                                    | <a href="#">“Cómo agregar un principal de servicio de Kerberos a un archivo keytab” en la página 505</a>      |
| Eliminar un principal de servicio de un archivo keytab                 | Utilice el comando <code>ktremove</code> de <code>kadmin</code> para eliminar un servicio de un archivo keytab.                                                                                                                                                                                                                                                                                                                                                                            | <a href="#">“Cómo eliminar un principal de servicio de un archivo keytab” en la página 506</a>                |
| Mostrar la lista de claves (lista de principales) en un archivo keytab | Utilice el comando <code>ktutil</code> para mostrar la lista de claves en un archivo keytab.                                                                                                                                                                                                                                                                                                                                                                                               | <a href="#">“Cómo visualizar la lista de claves (principales) en un archivo keytab” en la página 507</a>      |
| Desactivar temporalmente la autenticación de un servicio en un host    | <p>Este procedimiento es una manera rápida de desactivar temporalmente la autenticación de un servicio en un host sin la necesidad de contar con privilegios <code>kadmin</code>.</p> <p>Antes de utilizar <code>ktutil</code> para suprimir el principal de servicio del archivo keytab del servidor, copie el archivo keytab original en una ubicación temporal. Cuando desee habilitar el servicio nuevamente, vuelva a copiar el archivo keytab original en la ubicación correcta.</p> | <a href="#">“Cómo deshabilitar temporalmente la autenticación de un servicio en un host” en la página 508</a> |

### ▼ Cómo agregar un principal de servicio de Kerberos a un archivo keytab

- 1 Asegúrese de que el principal ya exista en la base de datos de Kerberos.

Para obtener más información, consulte [“Cómo ver la lista de los principales de Kerberos” en la página 478](#).

- 2 Asuma el rol `root` en el host que requiere un principal agregado al archivo keytab.

- 3 Inicie el comando `kadmin`.

```
/usr/sbin/kadmin
```

- 4 Agregue un principal a un archivo keytab mediante el comando `ktadd`.

```
kadmin: ktadd [-e enctype] [-k keytab] [-q] [principal | -glob principal-exp]
```

`-e tipo_cifrado`

Sustituye la lista de tipos de cifrado definida en el archivo `krb5.conf`.

|                                          |                                                                                                                                                                                                                                                                               |
|------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>-k keytab</code>                   | Especifica el archivo keytab. De manera predeterminada, se utiliza <code>/etc/krb5/krb5.keytab</code> .                                                                                                                                                                       |
| <code>-q</code>                          | Muestra menos información detallada.                                                                                                                                                                                                                                          |
| <code>principal</code>                   | Especifica el principal que se va a agregar al archivo keytab. Se pueden agregar los siguientes principales de servicio: <code>host</code> , <code>root</code> , <code>nfs</code> y <code>ftp</code> .                                                                        |
| <code>-glob expresiones_principal</code> | Especifica las expresiones de principal. Todos los principales que coinciden con las <i>expresiones_principal</i> se agregan al archivo keytab. Las reglas de expresión de principal son las mismas que para el comando <code>list_principals</code> de <code>kadmin</code> . |

## 5 Salga del comando `kadmin`.

`kadmin: quit`

### Ejemplo 23–16 Adición de un principal de servicio a un archivo keytab

En el siguiente ejemplo, el principal del `host` de `denver` se agrega al archivo keytab de `denver` para que el KDC pueda autenticar los servicios de red de `denver`.

```
denver # /usr/sbin/kadmin
kadmin: ktadd host/denver.example.com
Entry for principal host/denver.example.com with kvno 3, encryption type AES-256 CTS
mode with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal host/denver.example.com with kvno 3, encryption type AES-128 CTS mode
with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal host/denver.example.com with kvno 3, encryption type Triple DES cbc mode
with HMAC/sha1 added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal host/denver.example.com with kvno 3, encryption type ArcFour
with HMAC/md5 added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal host/denver.example.com with kvno 3, encryption type DES cbc mode
with RSA-MD5 added to keytab WRFILE:/etc/krb5/krb5.keytab.
kadmin: quit
```

## ▼ Cómo eliminar un principal de servicio de un archivo keytab

- 1 Asuma el rol `root` en el `host` con un principal de servicio que se debe eliminar de su archivo keytab.
- 2 Inicie el comando `kadmin`.

`# /usr/sbin/kadmin`

- 3 (Opcional) Para mostrar la lista actual de principales (claves) del archivo keytab, utilice el comando `ktutil`.**

Para obtener instrucciones detalladas, consulte [“Cómo visualizar la lista de claves \(principales\) en un archivo keytab” en la página 507](#).

- 4 Elimine un principal del archivo keytab con el comando `ktremove`.**

kadmin: `ktremove [-k keytab] [-q] principal [kvno | all | old]`

`-k keytab` Especifica el archivo keytab. De manera predeterminada, se utiliza `/etc/krb5/krb5.keytab`.

`-q` Muestra menos información detallada.

`principal` Especifica el principal que se va a eliminar del archivo keytab.

`kvno` Elimina todas las entradas del principal especificado cuyo número de versión de clave coincida con `kvno`.

`all` Elimina todas las entradas del principal especificado.

`old` Elimina todas las entradas del principal especificado, excepto las de los principales con el número de versión más alto.

- 5 Salga del comando `kadmin`.**

kadmin: `quit`

### **Ejemplo 23–17 Eliminación de un principal de servicio de un archivo keytab**

En el siguiente ejemplo, el principal del host de denver se elimina del archivo keytab de denver.

```
denver # /usr/sbin/kadmin
kadmin: ktremove host/denver.example.com@EXAMPLE.COM
kadmin: Entry for principal host/denver.example.com@EXAMPLE.COM with kvno 3
 removed from keytab WRFILE:/etc/krb5/krb5.keytab.
kadmin: quit
```

## **▼ Cómo visualizar la lista de claves (principales) en un archivo keytab**

- 1 Asuma el rol `root` en el host con el archivo keytab.**

---

**Nota** – Si bien puede crear archivos keytab que son propiedad de otros usuarios, para usar la ubicación predeterminada para el archivo keytab se requiere la propiedad de `root`.

---

**2 Inicie el comando ktutil.**

```
/usr/bin/ktutil
```

**3 Lea el archivo keytab en la memoria intermedia de la lista de claves con el comando read\_kt.**

```
ktutil: read_kt keytab
```

**4 Visualice la memoria intermedia de lista de claves con el comando list.**

```
ktutil: list
```

Aparece la memoria intermedia de lista de claves actual.

**5 Salga del comando ktutil.**

```
ktutil: quit
```

**Ejemplo 23–18 Visualización de la lista de claves (principales) en un archivo keytab**

En el siguiente ejemplo, se muestra la lista de claves en el archivo `/etc/krb5/krb5.keytab` en el host `denver`.

```
denver # /usr/bin/ktutil
ktutil: read_kt /etc/krb5/krb5.keytab
ktutil: list
slot KVNO Principal

1 5 host/denver@EXAMPLE.COM
ktutil: quit
```

## ▼ Cómo deshabilitar temporalmente la autenticación de un servicio en un host

En algunas ocasiones, es posible que necesite desactivar temporalmente el mecanismo de autenticación de un servicio, como `rlogin` o `ftp`, en un servidor de aplicaciones de red. Por ejemplo, es posible que desee impedir que los usuarios inicien sesión en un sistema mientras usted está realizando tareas de mantenimiento. El comando `ktutil` le permite realizar esta tarea mediante la eliminación del principal de servicio del archivo keytab del servidor, sin necesidad de privilegios `kadmin`. Para volver a activar la autenticación, sólo necesita copiar el archivo keytab original que guardó nuevamente en su ubicación original.

---

**Nota** – De manera predeterminada, la mayoría de los servicios están configurados para requerir autenticación. Si un servicio no está configurado para requerir autenticación, el servicio sigue funcionando, aunque desactive la autenticación del servicio.

---

**1 Asuma el rol root en el host con el archivo keytab.**



---

**Nota** – Si bien puede crear archivos keytab que son propiedad de otros usuarios, para usar la ubicación predeterminada para el archivo keytab se requiere la propiedad de root.

---

**2 Guarde el archivo keytab actual en un archivo temporal.**

**3 Inicie el comando `ktutil`.**

```
/usr/bin/ktutil
```

**4 Lea el archivo keytab en la memoria intermedia de la lista de claves con el comando `read_kt`.**

```
ktutil: read_kt keytab
```

**5 Visualice la memoria intermedia de lista de claves con el comando `list`.**

```
ktutil: list
```

Aparece la memoria intermedia de lista de claves actual. Anote el número de ranura para el servicio que desea deshabilitar.

**6 Para desactivar temporalmente un servicio de host, elimine el principal de servicio específico de la memoria intermedia de lista de claves con el comando `delete_entry`.**

```
ktutil: delete_entry slot-number
```

Donde *número\_ranura* especifica el número de ranura del principal de servicio que se va a suprimir, el cual se muestra mediante el comando `list`.

**7 Escriba la memoria intermedia de lista de claves en un nuevo archivo keytab mediante el comando `write_kt`.**

```
ktutil: write_kt new-keytab
```

**8 Salga del comando `ktutil`.**

```
ktutil: quit
```

**9 Mueva el nuevo archivo keytab.**

```
mv new-keytab keytab
```

**10 Cuando desee volver a habilitar el servicio, copie el archivo keytab (original) temporal nuevamente en su ubicación original.**

### **Ejemplo 23–19 Inhabilitación temporal de un servicio en un host**

En el ejemplo siguiente, el servicio de host en el host `denver` está desactivado temporalmente. Para volver a activar el servicio de host en `denver`, copie el archivo `krb5.keytab.temp` en el archivo `/etc/krb5/krb5.keytab`.

```
denver # cp /etc/krb5/krb5.keytab /etc/krb5/krb5.keytab.temp
denver # /usr/bin/ktutil
 ktutil:read_kt /etc/krb5/krb5.keytab
 ktutil:list
slot KVNO Principal

1 8 root/denver@EXAMPLE.COM
2 5 host/denver@EXAMPLE.COM
 ktutil:delete_entry 2
 ktutil:list
slot KVNO Principal

1 8 root/denver@EXAMPLE.COM
 ktutil:write_kt /etc/krb5/new.krb5.keytab
 ktutil: quit
denver # cp /etc/krb5/new.krb5.keytab /etc/krb5/krb5.keytab
```

## Uso de aplicaciones Kerberos (tareas)

---

Este capítulo está destinado para cualquiera que utiliza un sistema con el servicio Kerberos configurado. En este capítulo, se explica cómo utilizar los servicios y comandos “Kerberizados” que se proporcionan. Ya debe estar familiarizado con estos comandos (en sus versiones no Kerberizadas) antes de leer sobre ellos aquí.

Debido a que este capítulo está destinado para el lector general, se incluye información sobre cómo obtener, visualizar y destruir los tickets. Este capítulo también incluye información sobre cómo elegir o cambiar una contraseña de Kerberos.

A continuación, se indica la información contenida en este capítulo:

- “Gestión de tickets de Kerberos” en la página 511
- “Gestión de contraseñas de Kerberos” en la página 515
- “Comandos de usuario de Kerberos” en la página 520

Para obtener una descripción general del producto Kerberos de Oracle Solaris, consulte el [Capítulo 19, “Introducción al servicio Kerberos”](#).

### Gestión de tickets de Kerberos

En esta sección, se explica cómo obtener, visualizar y destruir tickets. Para obtener una introducción a los tickets, consulte [“Cómo funciona el servicio Kerberos” en la página 348](#).

### ¿Debe preocuparse por los tickets?

Con cualquiera de las versiones Oracle Solaris instalada, Kerberos se integra en el comando `login`. No obstante, para obtener los tickets de forma automática, debe configurar el servicio PAM servicios para los servicios de inicio de sesión aplicables. Para obtener más información, consulte la página del comando `man pam_krb5(5)`. Los comandos Kerberizados `rsh`, `rcp`, `telnet` y `rlogin`, por lo general, están configurados para reenviar copias de los tickets a otros

equipos, de modo que no es necesario solicitar explícitamente los tickets para obtener acceso a esos equipos. Es posible que su configuración no incluya este reenvío automático, ya que el sistema predeterminado no está configurado para que las credenciales se reenvíen. Consulte [“Descripción general de comandos Kerberizados” en la página 520](#) y [“Reenvío de tickets de Kerberos” en la página 523](#) para obtener más información sobre el reenvío de tickets.

Para obtener información sobre las duraciones de los tickets, consulte [“Duración de los tickets” en la página 534](#).

## Creación de un ticket de Kerberos

Normalmente, si el PAM se ha configurado correctamente, un ticket se crea automáticamente cuando inicia sesión, de modo que no tiene que hacer nada especial para obtener un ticket. Sin embargo, puede que necesite crear un ticket si su ticket caduca. Además, puede que necesite utilizar un principal diferente aparte del principal predeterminado, por ejemplo, si usa `rlogin -l` para iniciar sesión en un equipo como otro usuario.

Para crear un ticket, utilice el comando `kinit`.

```
% /usr/bin/kinit
```

El comando `kinit` le solicita la contraseña. Para conocer la sintaxis completa del comando `kinit`, consulte la página del comando `man kinit(1)`.

### EJEMPLO 24-1 Creación de un ticket de Kerberos

En este ejemplo, se muestra a un usuario, `jennifer`, que crea un ticket en su propio sistema.

```
% kinit
Password for jennifer@ENG.EXAMPLE.COM: <Type password>
```

Aquí, el usuario `david` crea un ticket que tiene una validez de tres horas, con la opción `-l`.

```
% kinit -l 3h david@EXAMPLE.ORG
Password for david@EXAMPLE.ORG: <Type password>
```

En este ejemplo se muestra cómo el usuario `david` crea un ticket reenviable (con la opción `-f`). Con este ticket reenviable, puede, por ejemplo, iniciar sesión en un segundo sistema y, a continuación, ejecutar el comando `telnet` para iniciar sesión en un tercer sistema.

```
% kinit -f david@EXAMPLE.ORG
Password for david@EXAMPLE.ORG: <Type password>
```

**EJEMPLO 24-1** Creación de un ticket de Kerberos (Continuación)

Para obtener más información sobre el reenvío de tickets, consulte [“Reenvío de tickets de Kerberos” en la página 523](#) y [“Tipos de tickets” en la página 532](#).

## Visualización de tickets de Kerberos

No todos los tickets son similares. Por ejemplo, un ticket puede ser *reenviable*. Otro ticket puede ser *posfechado*. Mientras que un tercer ticket puede ser reenviable y posfechado. Puede ver los tickets que tiene y sus atributos utilizando el comando `klist` con la opción `-f`:

```
% /usr/bin/klist -f
```

Los siguientes símbolos indican los atributos asociados con cada ticket, como se muestra por `klist`:

|   |                  |
|---|------------------|
| A | Preautenticado   |
| D | Posfechable      |
| d | Posfechado       |
| F | Reenviable       |
| f | Reenviado        |
| I | Inicial          |
| i | No válido        |
| P | Que admite proxy |
| p | Proxy            |
| R | Renovable        |

En la sección [“Tipos de tickets” en la página 532](#), se describen los diferentes atributos que un ticket puede tener.

**EJEMPLO 24-2** Visualización de tickets de Kerberos

En este ejemplo, se muestra que el usuario `jennifer` tiene un ticket *inicial*, que es *reenviable* (F) y *posfechado* (d), pero que aún no está validado (i).

```
% /usr/bin/klist -f
```

```
Ticket cache: /tmp/krb5cc_74287
```

```
Default principal: jennifer@EXAMPLE.COM
```

| Valid starting     | Expires            | Service principal           |
|--------------------|--------------------|-----------------------------|
| 09 Mar 04 15:09:51 | 09 Mar 04 21:09:51 | nfs/EXAMPLE.COM@EXAMPLE.COM |

**EJEMPLO 24-2** Visualización de tickets de Kerberos (Continuación)

```
renew until 10 Mar 04 15:12:51, Flags: Fdi
```

El siguiente ejemplo muestra que el usuario david tiene dos tickets que fueron *reenviados* (f) al host desde otro host. Los tickets también son *reenviables* (F).

```
% klist -f
Ticket cache: /tmp/krb5cc_74287
Default principal: david@EXAMPLE.COM

Valid starting Expires Service principal
07 Mar 04 06:09:51 09 Mar 04 23:33:51 host/EXAMPLE.COM@EXAMPLE.COM
 renew until 10 Mar 04 17:09:51, Flags: fF

Valid starting Expires Service principal
08 Mar 04 08:09:51 09 Mar 04 12:54:51 nfs/EXAMPLE.COM@EXAMPLE.COM
 renew until 10 Mar 04 15:22:51, Flags: fF
```

El ejemplo siguiente muestra cómo visualizar los tipos de cifrado de la clave de sesión y el ticket mediante la opción -e. La opción -a se utiliza para asignar la dirección de host a un nombre de host si el servicio de nombres puede realizar la conversión.

```
% klist -fea
Ticket cache: /tmp/krb5cc_74287
Default principal: david@EXAMPLE.COM

Valid starting Expires Service principal
07 Mar 04 06:09:51 09 Mar 04 23:33:51 krbtgt/EXAMPLE.COM@EXAMPLE.COM
 renew until 10 Mar 04 17:09:51, Flags: FRIA
 Etype(skey, tkt): DES cbc mode with RSA-MD5, DES cbc mode with CRC-32
 Addresses: client.example.com
```

## Destrucción de tickets de Kerberos

Si desea destruir todos los tickets de Kerberos adquiridos durante la sesión actual, utilice el comando `kdestroy`. El comando destruye la antememoria de credenciales, que destruye todas las credenciales y los tickets. Si bien esto no suele ser necesario, la ejecución de `kdestroy` reduce las posibilidades de que la antememoria de credenciales esté en riesgo en los momentos en los que no tiene ninguna sesión iniciada.

Para destruir los tickets, utilice el comando `kdestroy`.

```
% /usr/bin/kdestroy
```

El comando `kdestroy` destruye *todos* los tickets. No puede utilizar este comando para destruir de manera selectiva un determinado ticket.

Si no va a utilizar el sistema y le preocupa que un intruso use sus permisos, debe utilizar `kdestroy` o un protector de pantalla que bloquee la pantalla.

## Gestión de contraseñas de Kerberos

Con el servicio Kerberos configurado, ahora tiene dos contraseñas: la contraseña regular de Solaris y una contraseña de Kerberos. Ambas contraseñas pueden ser iguales o pueden ser diferentes.

### Consejos para elegir una contraseña

La contraseña puede incluir casi cualquier carácter que se pueda escribir. Las principales excepciones son las teclas `Ctrl` y la tecla de retorno. Una buena contraseña es una contraseña que se puede recordar con rapidez, pero que ningún otro usuario puede adivinar fácilmente. Ejemplos de contraseñas incorrectas:

- Palabras que se pueden encontrar en un diccionario
- Cualquier nombre común o popular
- El nombre de una persona famosa o un personaje
- El nombre o nombre de usuario en cualquier forma (por ejemplo: el nombre escrito hacia atrás, repetido dos veces, etc.)
- El nombre de un cónyuge, de un hijo o de una mascota
- La fecha de nacimiento o la fecha de nacimiento de un familiar
- El número de seguridad social, el número de licencia de conducir, el número de pasaporte u otro número de identificación similar
- Cualquier contraseña de ejemplo que aparece en este manual o en cualquier otro manual

Una contraseña correcta tiene, al menos, ocho caracteres de longitud. Además, una contraseña debe incluir una combinación de caracteres, como letras en mayúscula y minúscula, números y signos de puntuación. Ejemplos de contraseñas que serían correctas si no aparecieran en este manual:

- Acrónimos, como “I2LMHInSF” (que se recuerda como “I too left my heart in San Francisco”)
- Palabras sin sentido fáciles de pronunciar, como “WumpaBun” o “WangDangdoodle!”
- Frases escritas de manera incorrecta deliberadamente, como “6o'cluck” o “RrriotGrrrlsRrrule!”



---

**Precaución** – No utilice estos ejemplos. Las contraseñas que aparecen en los manuales son las primeras contraseñas que un intruso probará.

---

## Cambio de la contraseña

Si el PAM se ha configurado correctamente, puede cambiar la contraseña de Kerberos de dos maneras:

- Con el comando `passwd` de UNIX usual. Con el servicio Kerberos configurado, el comando `passwd` también solicita automáticamente una nueva contraseña de Kerberos.

La ventaja de utilizar `passwd` en lugar de `kpasswd` es que puede establecer las contraseñas de UNIX y Kerberos al mismo tiempo. Sin embargo, normalmente, no *tiene* que cambiar ambas contraseñas con `passwd`. A menudo, sólo puede cambiar su contraseña de UNIX y dejar la contraseña de Kerberos intacta, o viceversa.

---

**Nota** – El comportamiento de `passwd` depende de cómo el módulo PAM está configurado. Es posible que se le requiera que cambie las dos contraseñas en algunas configuraciones. Algunos sitios requieren que se cambie la contraseña de UNIX, mientras que otros sitios requieren que se cambie la contraseña de Kerberos.

---

- Con el comando `kpasswd`. El comando `kpasswd` es muy similar al comando `passwd`. Una diferencia es que `kpasswd` sólo cambia contraseñas de Kerberos. Debe utilizar `passwd` si desea cambiar la contraseña de UNIX.

Otra diferencia es que `kpasswd` puede cambiar una contraseña para un principal de Kerberos que no es un usuario de UNIX válido. Por ejemplo, `david/admin` es un principal de Kerberos, pero no es un usuario de UNIX real, por lo que debe utilizar `kpasswd` en lugar de `passwd`.

Después de cambiar la contraseña, el cambio tarda un tiempo en propagarse por un sistema (especialmente, en una red grande). En función de cómo está configurado el sistema, este tiempo puede ser de unos pocos minutos a una hora o más. Si necesita obtener nuevos tickets de Kerberos poco tiempo después de cambiar la contraseña, pruebe la nueva contraseña primero. Si la contraseña nueva no funciona, vuelva a intentarlo utilizando la contraseña antigua.

El protocolo Kerberos V5 permite a los administradores del sistema establecer criterios sobre contraseñas permitidas para cada usuario. Esos criterios son definidos por la *política* establecida para cada usuario (o por una política predeterminada). Consulte [“Administración de las políticas de Kerberos” en la página 490](#) para obtener más información sobre las políticas.



Por ejemplo, suponga que la política del usuario `jennifer` (denomínela `jenpol`) exige que las contraseñas deben tener, como mínimo, ocho caracteres y deben incluir una combinación de, al menos, dos tipos de caracteres. Por lo tanto, `kpasswd` rechazará un intento de utilizar “`sloth`” como contraseña.

```
% kpasswd
kpasswd: Changing password for jennifer@ENG.EXAMPLE.COM.
Old password: <Jennifer types her existing password>
kpasswd: jennifer@ENG.EXAMPLE.COM's password is controlled by
the policy jenpol
which requires a minimum of 8 characters from at least 2 classes
(the five classes are lowercase, uppercase, numbers, punctuation,
and all other characters).
New password: <Jennifer types 'sloth'>
New password (again): <Jennifer re-types 'sloth'>
kpasswd: New password is too short.
Please choose a password which is at least 4 characters long.
```

Aquí, `jennifer` utiliza “`slothrop49`” como contraseña. La contraseña “`slothrop49`” cumple los criterios porque tiene más de ocho letras y contiene dos tipos diferentes de caracteres (números y letras minúsculas).

```
% kpasswd
kpasswd: Changing password for jennifer@ENG.EXAMPLE.COM.
Old password: <Jennifer types her existing password>
kpasswd: jennifer@ENG.EXAMPLE.COM's password is controlled by
the policy jenpol
which requires a minimum of 8 characters from at least 2 classes
(the five classes are lowercase, uppercase, numbers, punctuation,
and all other characters).
New password: <Jennifer types 'slothrop49'>
New password (again): <Jennifer re-types 'slothrop49'>
Kerberos password changed.
```

#### EJEMPLO 24-3 Cambio de la contraseña

En el ejemplo siguiente, el usuario `david` cambia tanto la contraseña de UNIX como la contraseña de Kerberos con `passwd`.

```
% passwd
passwd: Changing password for david
Enter login password: <Type the current UNIX password>
New password: <Type the new UNIX password>
Re-enter password: <Confirm the new UNIX password>
Old KRB5 password: <Type the current Kerberos password>
New KRB5 password: <Type the new Kerberos password>
Re-enter new KRB5 password: <Confirm the new Kerberos password>
```

**EJEMPLO 24-3** Cambio de la contraseña (Continuación)

Tenga en cuenta que `passwd` solicita tanto la contraseña de UNIX como la contraseña de Kerberos. Este comportamiento es establecido por la configuración predeterminada. En ese caso, el usuario `david` debe usar `kpasswd` para establecer la contraseña de Kerberos como otra cosa, como se muestra a continuación.

En este ejemplo, se muestra al usuario `david`, que cambia sólo su contraseña de Kerberos con `kpasswd`.

```
% kpasswd
kpasswd: Changing password for david@ENG.EXAMPLE.COM.
Old password: <Type the current Kerberos password>
New password: <Type the new Kerberos password>
New password (again): <Confirm the new Kerberos password>
Kerberos password changed.
```

En este ejemplo, el usuario `david` cambia la contraseña del principal de Kerberos `david/admin` (que no es un usuario de UNIX válido). Debe utilizar `kpasswd`.

```
% kpasswd david/admin
kpasswd: Changing password for david/admin.
Old password: <Type the current Kerberos password>
New password: <Type the new Kerberos password>
New password (again): <Type the new Kerberos password>
Kerberos password changed.
```

## Otorgamiento de acceso a su cuenta

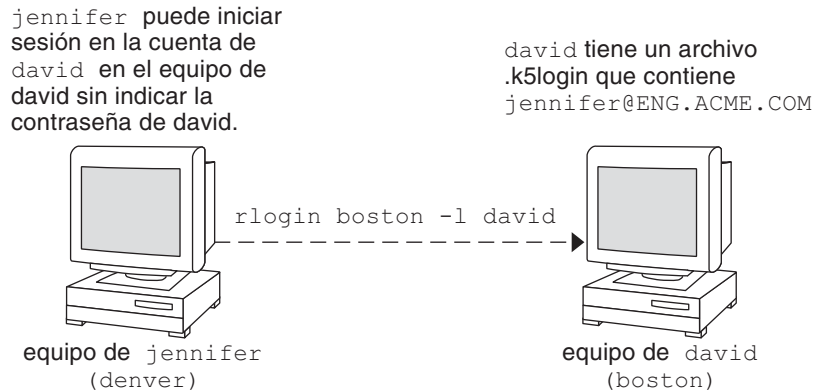
Si tiene que otorgarle a alguien acceso para que inicie sesión en su cuenta (como usted), puede hacerlo mediante Kerberos, sin revelar su contraseña, colocando un archivo `.k5login` en el directorio principal. Un archivo `.k5login` es una lista de uno o más principales de Kerberos correspondientes a cada persona a la que desea otorgar acceso. Cada principal debe estar en una línea diferente.

Suponga que el usuario `david` tiene un archivo `.k5login` en el directorio principal, como el siguiente:

```
jennifer@ENG.EXAMPLE.COM
joe@EXAMPLE.ORG
```

Este archivo permite a los usuarios *jennifer* y *joe* asumir la identidad de *david*, siempre y cuando ya tengan tickets de Kerberos en sus respectivos dominios. Por ejemplo, *jennifer* puede iniciar sesión de manera remota en el equipo de *david* (boston), como si fuera él, sin tener que indicar la contraseña de *david*.

FIGURA 24-1 Uso del archivo `.k5login` para otorgar acceso a su cuenta



En el caso donde el directorio principal de *david* está montado en NFS, mediante protocolos Kerberos V5, desde otro equipo (un tercer equipo), *jennifer* debe tener un ticket reenviable para acceder al directorio principal de *david*. Consulte [“Creación de un ticket de Kerberos” en la página 512](#) para obtener un ejemplo del uso de un ticket reenviable.

Si va a iniciar sesión en otros equipos de una red, es posible que desee incluir su propio principal de Kerberos en los archivos `.k5login` de esos equipos.

Usar un archivo `.k5login` es mucho más seguro que dar la contraseña, debido a los siguientes motivos:

- Puede quitar el acceso en cualquier momento eliminando el principal del archivo `.k5login`.
- Aunque los principales de usuarios nombrados en el archivo `.k5login` del directorio principal tengan acceso completo a su cuenta en ese equipo (o conjuntos de equipos si el archivo `.k5login` se comparte, por ejemplo, por medio de NFS). Sin embargo, cualquier servicio Kerberizado autorizará el acceso según la identidad del usuario, no la suya. Por lo tanto, *jennifer* puede iniciar sesión en el equipo de *joe* y realizar tareas allí. No obstante, si utiliza un programa Kerberizado, como `ftp` o `rlogin`, lo hace como ella misma.
- Kerberos mantiene un registro de quién obtiene tickets, por lo que un administrador del sistema puede detectar, si es necesario, quién puede utilizar su identidad de usuario en un momento concreto.

Una manera común de utilizar el archivo `.k5login` es colocarlo en el directorio principal de `root`, con lo cual se otorga a `root` acceso para ese equipo a los principales de Kerberos enumerados. Esta configuración permite que los administradores del sistema se conviertan en `root` localmente o inicien sesión de manera remota como `root` sin tener que proporcionar la contraseña de `root` y sin requerir que ningún usuario escriba la contraseña de `root` por medio de la red.

**EJEMPLO 24-4** Uso del archivo `.k5login` para otorgar acceso a su cuenta

Suponga que `jennifer` decide iniciar sesión en el equipo `boston.example.com` como `root`. Debido a que tiene una entrada para el nombre de principal en el archivo `.k5login` del directorio principal de `root` en `boston.example.com`, tampoco tiene que escribir su contraseña.

```
% rlogin boston.example.com -l root -x
This rlogin session is using DES encryption for all data transmissions.
Last login: Thu Jun 20 16:20:50 from daffodil
SunOS Release 5.7 (GENERIC) #2: Tue Nov 14 18:09:31 EST 1998
boston[root]%
```

## Comandos de usuario de Kerberos

El producto Kerberos V5 es un sistema de *inicio de sesión único*, lo que significa que sólo tiene que escribir la contraseña una vez. Los programas Kerberos V5 realizan la autenticación (y el cifrado opcional) porque Kerberos se ha integrado en cada paquete de programas de red familiares existentes. Las aplicaciones Kerberos V5 son versiones de programas de red UNIX existentes con las funciones de Kerberos agregadas.

Por ejemplo, cuando utiliza un programa Kerberizado para conectarse a un host remoto, el programa, el KDC y el host remoto realizan un conjunto de negociaciones rápidas. Cuando estas negociaciones están completas, el programa ha aprobado su identidad en su nombre para el host remoto, y el host remoto le ha otorgado acceso.

Tenga en cuenta que los comandos Kerberizados primero intentan autenticarse con Kerberos. Si la autenticación Kerberos falla, se produce un error o se intenta la autenticación UNIX, según las opciones que se utilizaron con el comando. Consulte la sección *Kerberos Security* en cada página del comando `man` del comando Kerberos para obtener información más detallada.

## Descripción general de comandos Kerberizados

Los servicios de red Kerberizados son programas que se conectan a otro equipo en algún lugar de Internet. Estos programas son los siguientes:

- `ftp`
- `rcp`

- `rlogin`
- `rsh`
- `ssh`
- `telnet`

Estos programas tienen funciones que utilizan de forma transparente los tickets de Kerberos para negociar la autenticación y el cifrado opcional con el host remoto. En la mayoría de los casos, sólo observará que ya no tiene que escribir la contraseña para utilizarlos, ya que Kerberos proporciona prueba de su identidad.

Los programas de red Kerberos V5 incluyen opciones que permiten realizar lo siguiente:

- Reenviar los tickets al otro host (si inicialmente obtuvo tickets reenviables).
- Cifrar datos transmitidos entre usted y el host remoto.

---

**Nota** – En esta sección, se asume que ya está familiarizado con las versiones no Kerberizadas de estos programas, y se resalta la funcionalidad de Kerberos agregada por el paquete Kerberos V5. Para obtener descripciones detalladas de los comandos que se describen aquí, consulte las respectivas páginas del comando `man`.

---

Las siguientes opciones de Kerberos se han agregado a `ftp`, `rcp`, `rlogin`, `rsh` y `telnet`:

- a Intenta el inicio de sesión automático usando sus tickets existentes. Utiliza el nombre de usuario devuelto por `getlogin()`, salvo que el nombre sea diferente del ID de usuario actual. Consulte la página del comando `man telnet(1)` para obtener detalles.
- f Reenvía un ticket *no reenviable* a un host remoto. Esta opción es mutuamente excluyente con la opción `-F`. No se pueden utilizar juntas en el mismo comando.

Es posible que desee reenviar un ticket si tiene motivos para creer que deberá autenticarse con otros servicios basados en Kerberos en un tercer host. Por ejemplo, es posible que desee iniciar sesión de manera remota en otro equipo y, a continuación, iniciar sesión de manera remota desde él en un tercer equipo.

Definitivamente debe usar un ticket reenviable si el directorio principal en el host remoto se monta en NFS utilizando el mecanismo Kerberos V5. De lo contrario, no podrá acceder a su directorio principal. Es decir, suponga que inicia sesión por primera vez en el sistema 1. Desde el sistema 1, inicia sesión remotamente en el equipo doméstico, el sistema 2, que monta el directorio principal del sistema

3. A menos que haya utilizado la opción -f o -F con rlogin, no podrá acceder al directorio principal porque el ticket no se puede reenviar al sistema 3.

De manera predeterminada, kinit obtiene tickets de otorgamiento de tickets (TGT) reenviables. Sin embargo, la configuración puede ser diferente en este sentido.

Para obtener más información sobre el reenvío de tickets, consulte [“Reenvío de tickets de Kerberos” en la página 523](#).

- F

Reenvía una copia *reenviable* de su TGT a un sistema remoto. Es similar a -f, pero permite el acceso a un equipo más (es decir, un cuarto o quinto equipo). La opción -F, por lo tanto, puede considerarse un conjunto universal de la opción -f. La opción -F es mutuamente excluyente con la opción -f. No se pueden utilizar juntas en el mismo comando.

Para obtener más información sobre el reenvío de tickets, consulte [“Reenvío de tickets de Kerberos” en la página 523](#).
- k *dominio*

Solicita tickets para el host remoto en el *realm* especificado, en lugar de determinar el dominio usando el archivo krb5.conf.
- K

Utiliza sus tickets para autenticarse en el host remoto, pero no inicia sesión automáticamente.
- m *mecanismo*

Especifica el mecanismo de seguridad GSS-API para utilizar, como se muestra en el archivo /etc/gss/mech. De manera predeterminada, este mecanismo es kerberos\_v5.
- x

Cifra esta sesión.
- X *tipo\_autenticación*

Desactiva el tipo de autenticación *auth-type*.

En la siguiente tabla, se muestra qué comandos tienen opciones específicas. Una "X" indica que el comando tiene esa opción.

TABLA 24-1 Opciones de Kerberos para comandos de red

|    | ftp | rcp | rlogin | rsh | telnet |
|----|-----|-----|--------|-----|--------|
| -a |     |     |        |     | X      |
| -f | X   |     | X      | X   | X      |
| -F |     |     | X      | X   | X      |
| -k |     | X   | X      | X   | X      |

TABLA 24-1 Opciones de Kerberos para comandos de red (Continuación)

|    | ftp | rcp | rlogin | rsh | telnet |
|----|-----|-----|--------|-----|--------|
| -K |     |     |        |     | X      |
| -m | X   |     |        |     |        |
| -x | X   | X   | X      | X   | X      |
| -X |     |     |        |     | X      |

Además, `ftppermite` definir el nivel de protección de una sesión en el indicador:

|                      |                                                                                                                                                                                                                                                                           |
|----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>clear</code>   | Establece el nivel de protección en “sin cifrar”, es decir, sin protección. Este nivel de protección es el valor predeterminado.                                                                                                                                          |
| <code>private</code> | Establece el nivel de protección en “private” (privado). La confidencialidad y la integridad de las transmisiones de datos se protegen mediante el cifrado. No obstante, es posible que el servicio de privacidad no esté disponible para todos los usuarios de Kerberos. |
| <code>safe</code>    | Define el nivel de protección en “safe” (seguro). La integridad de las transmisiones de datos se protege mediante la suma de comprobación criptográfica.                                                                                                                  |

También puede definir el nivel de protección en el indicador `ftp` escribiendo `protect` seguido de cualquiera de los niveles de protección mostrados anteriormente (`clear`, `private` o `safe`).

## Reenvío de tickets de Kerberos

Como se describe en [“Descripción general de comandos Kerberizados” en la página 520](#), algunos comandos permiten reenviar tickets con la opción `-f` o `-F`. El reenvío de tickets le permite “encadenar” las transacciones de la red. Puede, por ejemplo, iniciar sesión de manera remota en un equipo y, a continuación, iniciar sesión de manera remota desde él en otro equipo. La opción `-f` permite reenviar un ticket, mientras que la opción `-F` permite reenviar un ticket reenviado.

En la siguiente figura, el usuario `david` obtiene un ticket de otorgamiento de tickets (TGT) no reenviable con `kinit`. El ticket no es reenviable porque no especificó la opción `-f`. En el escenario 1, puede iniciar sesión de manera remota en el equipo B, pero no puede hacer nada más. En el escenario 2, el comando `rlogin -f` falla debido a que está intentando reenviar un ticket que no es reenviable.

FIGURA 24-2 Uso de tickets no reenviables

1. (En A): `kinit david@ACME.ORG`



2. (En A): `kinit david@ACME.ORG`



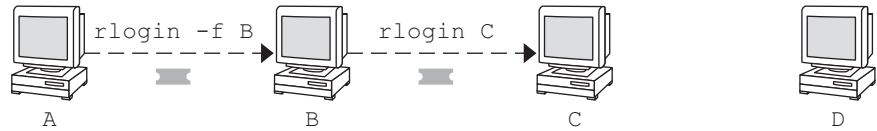
En realidad, los archivos de configuración de Kerberos están configurados para que `kinit` obtenga tickets reenviables de manera predeterminada. Sin embargo, la configuración puede diferir. Para una mejor explicación, suponga que `kinit` *no* obtiene TGT reenviables, a menos que se invoque con `kinit -f`. Por otro lado, observe que `kinit` no tiene una opción `-F`. Los TGT son reenviables o no reenviables.

En la siguiente figura, el usuario `david` obtiene TGT reenviables con `kinit -f`. En el escenario 3, puede acceder al equipo C debido a que utiliza un ticket reenviable con `rlogin`. En el escenario 4, el segundo `rlogin` falla debido a que el ticket no es reenviable. Mediante la opción `-F`, en cambio, como en el escenario 5, el segundo `rlogin` se ejecuta correctamente, y el ticket se puede reenviar al equipo D.

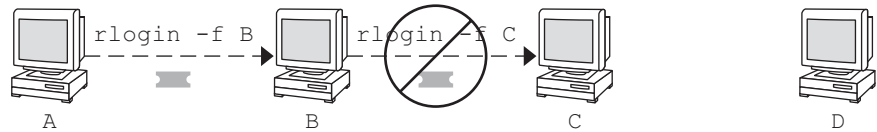


FIGURA 24-3 Uso de tickets reenviables

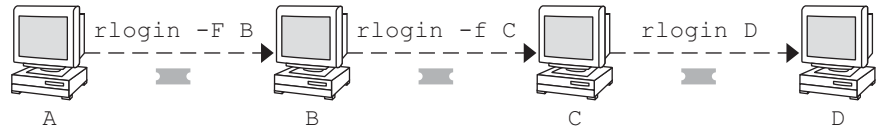
3. (En A): `kinit -f david@ACME.ORG`



4. (En A): `kinit -f david@ACME.ORG`



5. (En A): `kinit -f david@ACME.ORG`



## Uso de comandos Kerberizados (ejemplos)

Los siguientes ejemplos muestran cómo funcionan las opciones para los comandos Kerberizados.

### EJEMPLO 24-5 Uso de las opciones -a, -f y -x con telnet

En este ejemplo, el usuario david ya ha iniciado sesión y desea ejecutar el comando `telnet` para iniciar sesión en el equipo `denver.example.com`. Utiliza la opción `-f` para reenviar sus tickets, la opción `-x` para cifrar la sesión y la opción `-a` para realizar el inicio de sesión automáticamente. Debido a que no planea utilizar los servicios de un tercer host, puede utilizar `-f` en lugar de `-F`.

```
% telnet -a -f -x denver.example.com
Trying 128.0.0.5...
Connected to denver.example.com. Escape character is '^]'.
[Kerberos V5 accepts you as "david@eng.example.com"]
[Kerberos V5 accepted forwarded credentials]
SunOS 5.9: Tue May 21 00:31:42 EDT 2004 Welcome to SunOS
%
```

Tenga en cuenta que el equipo de david utilizó Kerberos para autenticarlo en `denver.example.com` e inició sesión automáticamente como él mismo. Tenía una sesión cifrada, una copia de sus tickets esperándolo y nunca tuvo que escribir su contraseña. Si hubiera utilizado una versión de `telnet` no Kerberizada, se le habría solicitado la contraseña, y la

**EJEMPLO 24-5** Uso de las opciones -a, -f y -x con telnet (Continuación)

contraseña se habría enviado por la red sin cifrar. Si un intruso hubiese estado observando el tráfico de la red en ese momento, habría visto la contraseña de david.

Si reenvía los tickets de Kerberos, telnet (así como los otros comandos proporcionados aquí) los destruye cuando se cierra.

**EJEMPLO 24-6** Uso de rlogin con la opción -F

Aquí, el usuario jennifer desea iniciar sesión en su propio equipo, boston.example.com. Reenvía sus tickets con la opción -F y cifra la sesión con la opción -x. Elige -F en lugar de -f porque, después de iniciar sesión en boston, es posible que desee realizar otras transacciones de la red que requieren que los tickets se reenvíen. Además, como está reenviando sus tickets existentes, no tiene que escribir la contraseña.

```
% rlogin boston.example.com -F -x
This rlogin session is using encryption for all transmissions.
Last login Mon May 19 15:19:49 from daffodil
SunOS Release 5.9 (GENERIC) #2 Tue Nov 14 18:09:3 EST 2003
%
```

**EJEMPLO 24-7** Configuración del nivel de protección en ftp

Suponga que joe desea usar ftp para obtener su correo desde el directorio ~joe/MAIL del equipo denver.example.com mediante el cifrado de la sesión. El intercambio sería de la siguiente manera:

```
% ftp -f denver.example.com
Connected to denver.example.com
220 denver.example.org FTP server (Version 6.0) ready.
334 Using authentication type GSSAPI; ADAT must follow
GSSAPI accepted as authentication type
GSSAPI authentication succeeded Name (daffodil.example.org:joe)
232 GSSAPI user joe@MELPOMENE.EXAMPLE.COM is authorized as joe
230 User joe logged in.
Remote system type is UNIX.
Using BINARY mode to transfer files.
ftp> protect private
200 Protection level set to Private
ftp> cd ~joe/MAIL
250 CWD command successful.
ftp> get RMAIL
227 Entering Passive Mode (128,0,0,5,16,49)
150 Opening BINARY mode data connection for RMAIL (158336 bytes).
226 Transfer complete. 158336 bytes received in 1.9 seconds (1.4e+02 Kbytes/s)
ftp> quit
%
```

Para cifrar la sesión, joe establece el nivel de protección en private.

## El servicio Kerberos (referencia)

---

En este capítulo, se enumeran muchos de los archivos, comandos y daemons que forman parte del producto Kerberos. Además, se proporciona información detallada sobre cómo funciona la autenticación Kerberos.

A continuación, se indica la información de referencia contenida en este capítulo.

- [“Archivos de Kerberos” en la página 527](#)
- [“Comandos de Kerberos” en la página 529](#)
- [“Daemons de Kerberos” en la página 530](#)
- [“Terminología de Kerberos” en la página 531](#)
- [“Cómo funciona el sistema de autenticación Kerberos” en la página 537](#)
- [“Obtención de acceso a un servicio con Kerberos” en la página 537](#)
- [“Uso de los tipos de cifrado de Kerberos” en la página 541](#)
- [“Tabla de uso de gsscred” en la página 543](#)
- [“Diferencias importantes entre Oracle Solaris Kerberos y MIT Kerberos” en la página 543](#)

## Archivos de Kerberos

En esta sección se enumeran algunos de los archivos que son utilizados por el servicio Kerberos.

TABLA 25-1 Archivos de Kerberos

| Nombre de archivo | Descripción                                                                           |
|-------------------|---------------------------------------------------------------------------------------|
| ~/ .gkadmin       | Valores predeterminados para la creación de nuevos principales en la herramienta SEAM |
| ~/ .k5login       | Lista de principales que otorgan acceso a una cuenta de Kerberos                      |

TABLA 25-1 Archivos de Kerberos (Continuación)

| Nombre de archivo              | Descripción                                                                                                                                                             |
|--------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| /etc/krb5/kadm5.acl            | Archivo de lista de control de acceso de Kerberos, que incluye los nombres de principales de los administradores de KDC y sus privilegios de administración de Kerberos |
| /etc/krb5/kadm5.keytab         | Obsoleto: este archivo se eliminó de la versión Oracle Solaris 11.                                                                                                      |
| /etc/krb5/kdc.conf             | Archivo de configuración de KDC                                                                                                                                         |
| /etc/krb5/kpropd.acl           | Archivo de configuración de propagación de bases de datos de Kerberos                                                                                                   |
| /etc/krb5/krb5.conf            | Archivo de configuración de dominios de Kerberos                                                                                                                        |
| /etc/krb5/krb5.keytab          | Archivo keytab para servidores de aplicaciones de redes                                                                                                                 |
| /etc/krb5/warn.conf            | Archivo de configuración de renovación automática y advertencia de caducidad de ticket de Kerberos                                                                      |
| /etc/pam.conf                  | Archivo de configuración de PAM                                                                                                                                         |
| /tmp/krb5cc_uid                | Antememoria de credenciales predeterminadas, en la que <i>uid</i> es el UID decimal del usuario                                                                         |
| /tmp/ovsec_adm.xxxxxx          | Antememoria de credenciales temporales por la duración de la operación para cambio de contraseña, donde <i>xxxxxx</i> es una cadena aleatoria                           |
| /var/krb5/.k5.DOMINIO          | Archivo intermedio de KDC, que contiene una copia de la clave maestra de KDC                                                                                            |
| /var/krb5/kadmin.log           | Archivo de registro para kadmin                                                                                                                                         |
| /var/krb5/kdc.log              | Archivo de registro para el KDC                                                                                                                                         |
| /var/krb5/principal            | Base de datos principal de Kerberos                                                                                                                                     |
| /var/krb5/principal.kadm5      | Base de datos administrativa de Kerberos, que contiene información sobre políticas                                                                                      |
| /var/krb5/principal.kadm5.lock | Archivo de bloqueo de bases de datos administrativas de Kerberos                                                                                                        |
| /var/krb5/principal.ok         | Archivo de inicialización de base de datos principal de Kerberos que se crea cuando la base de datos de Kerberos se inicializa con éxito                                |
| /var/krb5/principal.ulong      | Registro de actualización de Kerberos, que contiene actualizaciones para la propagación progresiva                                                                      |
| /var/krb5/slave_datatrans      | Archivo de copia de seguridad del KDC que la secuencia de comandos <i>kprop_script</i> utiliza para la propagación                                                      |

TABLA 25-1 Archivos de Kerberos (Continuación)

| Nombre de archivo                              | Descripción                                                                                                            |
|------------------------------------------------|------------------------------------------------------------------------------------------------------------------------|
| <code>/var/krb5/slave_datatrans_esclavo</code> | Archivo de volcado temporal que se crea cuando se realizan las actualizaciones completas del <i>slave</i> especificado |
| <code>/var/user/\$USER/krb-warn.conf</code>    | Advertencia de caducidad de ticket por usuario y archivo de configuración de renovación automática                     |

## Comandos de Kerberos

En esta sección, se enumeran algunos comandos que se incluyen en el producto Kerberos.

TABLA 25-2 Comandos de Kerberos

| Comando                          | Descripción                                                                                                                                            |
|----------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>/usr/bin/ftp</code>        | Programa del protocolo de transferencia de archivos                                                                                                    |
| <code>/usr/bin/kdestroy</code>   | Destruye los tickets de Kerberos                                                                                                                       |
| <code>/usr/bin/kinit</code>      | Obtiene tickets de otorgamiento de tickets de Kerberos y los almacena en la antememoria                                                                |
| <code>/usr/bin/klint</code>      | Muestra los tickets de Kerberos actuales                                                                                                               |
| <code>/usr/bin/kpasswd</code>    | Cambia una contraseña de Kerberos                                                                                                                      |
| <code>/usr/bin/ktutil</code>     | Gestiona los archivos keytab de Kerberos                                                                                                               |
| <code>/usr/bin/kvno</code>       | Enumera los números de versión de clave para los principales de Kerberos                                                                               |
| <code>/usr/bin/rcp</code>        | Programa de copia de archivos remota                                                                                                                   |
| <code>/usr/bin/rlogin</code>     | Programa de inicio de sesión remoto                                                                                                                    |
| <code>/usr/bin/rsh</code>        | Programa de shell remoto                                                                                                                               |
| <code>/usr/bin/scp</code>        | Programa de copia de archivos remota y segura                                                                                                          |
| <code>/usr/bin/sftp</code>       | Programa de transferencia de archivos segura                                                                                                           |
| <code>/usr/bin/ssh</code>        | Programa de inicio de sesión remoto y seguro                                                                                                           |
| <code>/usr/bin/telnet</code>     | Programa telnet Kerberizado                                                                                                                            |
| <code>/usr/lib/krb5/kprop</code> | Programa de propagación de bases de datos de Kerberos                                                                                                  |
| <code>/usr/sbin/gkadmin</code>   | Programa de interfaz gráfica de usuario de administración de bases de datos de Kerberos, que se utiliza para gestionar los principales y las políticas |

| TABLA 25-2 Comandos de Kerberos (Continuación) |                                                                                                                                                                                                                      |
|------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Comando                                        | Descripción                                                                                                                                                                                                          |
| /usr/sbin/gsscred                              | Gestiona las entradas de la tabla gsscred                                                                                                                                                                            |
| /usr/sbin/kadmin                               | Programa de administración de bases de datos de Kerberos remoto (se ejecuta con autenticación Kerberos), que se utiliza para gestionar los principales, las políticas y los archivos keytab                          |
| /usr/sbin/kadmin.local                         | Programa de administración de bases de datos de Kerberos local (debe ejecutarse con la autenticación Kerberos en el KDC maestro), que se utiliza para gestionar los principales, las políticas y los archivos keytab |
| /usr/sbin/kclient                              | Secuencia de comandos de instalación de cliente Kerberos que se utiliza con o sin un perfil de instalación                                                                                                           |
| /usr/sbin/kdb5_ldap_util                       | Crea contenedores LDAP para las bases de datos de Kerberos                                                                                                                                                           |
| /usr/sbin/kdb5_util                            | Crea archivos intermedios y bases de datos de Kerberos                                                                                                                                                               |
| /usr/sbin/kgcmgr                               | Configura KDC maestros y esclavos de Kerberos                                                                                                                                                                        |
| /usr/sbin/kproplog                             | Contiene un resumen de las entradas del registro de actualización                                                                                                                                                    |

## Daemons de Kerberos

La siguiente tabla enumera los daemons que utiliza el producto Kerberos.

| TABLA 25-3 Daemons de Kerberos |                                                                                  |
|--------------------------------|----------------------------------------------------------------------------------|
| Daemon                         | Descripción                                                                      |
| /usr/lib/inet/proftpd          | Daemon del protocolo de transferencia de archivos segura                         |
| /usr/lib/ssh/sshd              | Daemon de shell seguro                                                           |
| /usr/lib/krb5/kadmind          | Daemon de administración de bases de datos de Kerberos                           |
| /usr/lib/krb5/kpropd           | Daemon de propagación de bases de datos de Kerberos                              |
| /usr/lib/krb5/krb5kdc          | Daemon de procesamiento de tickets de Kerberos                                   |
| /usr/lib/krb5/ktkt_warnd       | Daemon de renovación automática y advertencia de caducidad de ticket de Kerberos |
| /usr/sbin/in.rlogind           | Daemon de inicio de sesión remoto                                                |
| /usr/sbin/in.rshd              | Daemon de shell remoto                                                           |
| /usr/sbin/in.telnetd           | Daemon telnet                                                                    |

# Terminología de Kerberos

La siguiente sección presenta los términos de Kerberos con sus definiciones. Estos términos se utilizan en toda la documentación de Kerberos. Para incorporar los conceptos de Kerberos, resulta esencial comprender estos términos.

## Terminología específica de Kerberos

Para administrar los KDC, debe comprender los términos de esta sección.

El *Centro de distribución de claves, KDC*, es el componente de Kerberos que se encarga de la emisión de credenciales. Para crear estas credenciales, se utiliza la información que está almacenada en la base de datos del KDC. Cada dominio necesita al menos dos KDC, uno que sea maestro y al menos uno que sea esclavo. Todos los KDC generan credenciales, pero únicamente el KDC maestro realiza los cambios en la base de datos del KDC.

El *archivo intermedio* contiene la clave maestra para el KDC. Esta clave se utiliza cuando se reinicia un servidor para autenticar el KDC automáticamente antes de iniciar los comandos `kadmind` y `krb5kdc`. Como este archivo contiene la clave maestra, el archivo y cualquier copia de seguridad del archivo deben permanecer seguros. El archivo se crea con permisos de sólo lectura para el usuario `root`. Para mantener el archivo seguro, no cambie los permisos. Si el archivo corre peligro, la clave podría ser utilizada para acceder a la base de datos del KDC o para modificarla.

## Terminología específica de la autenticación

Debe conocer los términos de esta sección para comprender el proceso de autenticación. Los programadores y los administradores del sistema deben estar familiarizados con estos términos.

El *cliente* es el software que se ejecuta en la estación de trabajo del usuario. El software de Kerberos que se ejecuta en el cliente realiza muchas solicitudes durante este proceso. Por lo tanto, es importante establecer la diferencia entre las acciones de este software y el usuario.

Los términos *server* y *service* suelen utilizarse de manera indistinta. El término *servidor* se utiliza para definir el sistema físico en el que se ejecuta el software de Kerberos. El término *servicio* corresponde a una determinada función que se admite en un servidor (por ejemplo, `ftp` o `nfs`). Con frecuencia, la documentación define los servidores como una parte de un servicio, pero esta definición hace que el significado de los términos sea confuso. Por lo tanto, el término *server* se refiere al sistema físico. El término *service* se refiere al software.

El producto Kerberos usa dos tipos de claves. Un tipo de clave es una clave derivada de contraseña. La clave derivada de contraseña se otorga a cada principal de usuario, y sólo el usuario y el KDC la conocen. El otro tipo de clave que el producto Kerberos utiliza es una clave

aleatoria que no está asociada con una contraseña y que, por lo tanto, no es adecuada para que la usen los principales de usuario. Por lo general, las claves aleatorias se usan para los principales de servicio que tienen entradas en un archivo keytab y claves de sesión generadas por el KDC. Los principales de servicio pueden usar claves aleatorias, ya que el servicio puede acceder a la clave que se encuentra en el archivo keytab y entonces puede ejecutarse de manera no interactiva. Las claves de sesión son generadas por el KDC (y compartidas entre el cliente y el servicio) a fin de facilitar las transacciones seguras entre un cliente y un servicio.

Un *ticket* es un paquete de información que se utiliza para transferir la identidad de un usuario a un servidor o servicio de manera segura. Un ticket es válido únicamente para un solo cliente y un servicio determinado en un servidor específico. El ticket contiene:

- Nombre de principal del servicio
- Nombre de principal del usuario
- Dirección IP del host del usuario
- Indicación de hora
- Valor que define la duración del ticket
- Copia de la clave de sesión

Todos estos datos se encuentran cifrados en la clave de servicio del servidor. Tenga en cuenta que el KDC emite el ticket integrado en una credencial, que se describe en el siguiente párrafo. Una vez que se emitió un ticket, éste puede volver a usarse hasta que caduque.

La *credencial* es un paquete de información que incluye un ticket y una clave de sesión coincidente. La credencial está cifrada con la clave del principal solicitante. Generalmente, el KDC genera una credencial en respuesta a una solicitud de ticket de un cliente.

El *autenticador* es la información utilizada por el servidor para autenticar el principal del usuario cliente. El autenticador incluye el nombre de principal del usuario, la indicación de hora y otros datos. A diferencia del ticket, el autenticador puede utilizarse sólo una vez; por lo general, cuando se solicita acceso a un servicio. El autenticador se cifra mediante la clave de sesión compartida por el cliente y el servidor. Habitualmente, el cliente crea el autenticador y lo envía con el ticket de un servidor o de un servicio para que se autentique en el servidor o el servicio.

## Tipos de tickets

Los tickets tienen propiedades que establecen el modo en que pueden utilizarse. Estas propiedades se asignan al ticket en el momento que éste se crea, pero pueden modificarse más adelante. Por ejemplo, un ticket puede cambiar de *forwardable* a *forwarded*. Puede ver las propiedades del ticket con el comando `klist`. Consulte [“Visualización de tickets de Kerberos” en la página 513](#).

Los tickets pueden describirse con uno o más de los siguientes términos:



|                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Reenviable/reenviado   | <p>Un ticket reenviable puede enviarse de un host a otro, sin la necesidad de que un cliente vuelva a autenticarse. Por ejemplo, si el usuario david obtiene un ticket reenviable cuando está en el equipo del usuario jennifer, puede iniciar sesión en su propio equipo sin obtener un ticket nuevo (ni volver a autenticarse). Consulte el <a href="#">Ejemplo 24–1</a> para ver un ejemplo de un ticket reenviable.</p>                                                                                                                                                                                                                                                                                                                                                           |
| Inicial                | <p>Un ticket inicial es un ticket que se emite directamente en lugar de emitirse por medio de un ticket de otorgamiento de tickets. Algunos servicios, como las aplicaciones que cambian las contraseñas, posiblemente requieran que los tickets se marquen como iniciales para garantizar que el cliente pueda demostrar que conoce su clave secreta. El ticket inicial indica que, recientemente, el cliente se ha autenticado por sí mismo, en lugar de recurrir al ticket de otorgamiento de tickets, que quizás haya estado funcionando durante mucho tiempo.</p>                                                                                                                                                                                                                |
| No válido              | <p>Un ticket no válido es un ticket posfechado que todavía no se puede usar. Un servidor de aplicaciones rechaza un ticket no válido hasta que se valide. Para validar un ticket, el cliente debe presentarlo al KDC en una solicitud de ticket de otorgamiento de tickets, con el indicador VALIDATE definido, después de que haya pasado la hora de inicio.</p>                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Posfechable/posfechado | <p>Un ticket posfechado no es válido hasta que transcurra un tiempo especificado tras su creación. Un ticket de este tipo es útil, por ejemplo, para los trabajos por lotes que deben ejecutarse tarde por la noche, ya que si el ticket es robado, no se puede utilizar hasta que se ejecute el trabajo por lotes. Los tickets posfechados se emiten como no válidos y siguen teniendo ese estado hasta que haya pasado su hora de inicio, y el cliente solicite la validación por parte del KDC. Generalmente, un ticket posfechado es válido hasta la hora de vencimiento del ticket de otorgamiento de tickets. Sin embargo, si el ticket se marca como renovable, su duración suele definirse para que coincida con la duración total del ticket de otorgamiento de tickets.</p> |
| Que admite proxy/proxy | <p>A veces, es necesario que un principal permita que un servicio realice una operación en su nombre. El nombre de principal del proxy debe estar especificado cuando se crea el ticket. La versión de Oracle Solaris no es compatible con tickets que admiten proxy ni con tickets proxy.</p> <p>Un ticket que admite proxy es similar al ticket reenviable, excepto en que sólo es válido para un único servicio, mientras que el ticket</p>                                                                                                                                                                                                                                                                                                                                        |

reenviable otorga al servicio el uso total de la identidad del cliente. Por lo tanto, el ticket reenviable se puede considerar como una especie de superproxy.

#### Renovable

Debido a que los tickets con duraciones muy largas constituyen un riesgo de seguridad, los tickets se pueden designar como renovables. Un ticket renovable tiene dos horas de vencimiento: la hora de vencimiento de la instancia actual del ticket y la duración máxima de cualquier ticket, que es de una semana. Si un cliente desea seguir utilizando un ticket, debe renovarlo antes del primer vencimiento. Por ejemplo, un ticket puede ser válido por una hora, pero todos los tickets tienen una duración máxima de 10 h. Si el cliente que tiene el ticket desea conservarlo durante más de una hora, debe renovarlo dentro de esa hora. Cuando un ticket alcanza la duración máxima (10 h), vence automáticamente y no se puede renovar.

Para obtener más información sobre cómo ver los atributos de tickets, consulte [“Visualización de tickets de Kerberos” en la página 513](#).

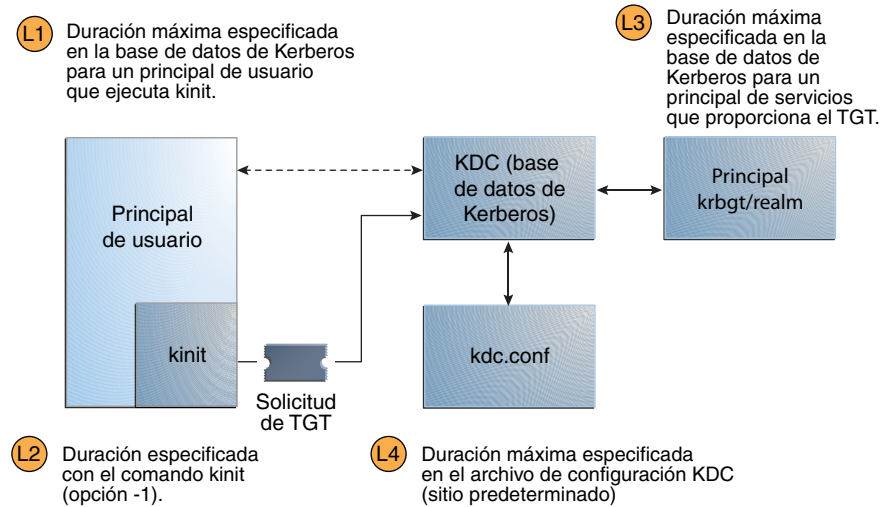
## Duración de los tickets

En cualquier momento que un principal obtenga un ticket, incluido un ticket de otorgamiento de tickets (TGT), la duración del ticket se establece como el menor de los siguientes valores de duración:

- El valor de duración que establece la opción `-l` de `kinit`, si se usa `kinit` para obtener el ticket. De manera predeterminada, `kinit` usó el valor de duración máxima.
- El valor de duración máxima (`max_life`) que se encuentra especificado en el archivo `kdc.conf`.
- El valor de duración máxima que se especifica en la base de datos de Kerberos para el principal de servicio que proporciona el ticket. En el caso de `kinit`, el principal de servicio es `krbtgt/realm`.
- El valor de duración máxima que se especifica en la base de datos de Kerberos para el principal de usuario que solicita el ticket.

La [Figura 25–1](#) muestra cómo se determina la duración de un TGT y de dónde provienen los cuatro valores de duración. Aunque esta figura muestra cómo se determina la duración de un TGT, básicamente, ocurre lo mismo cuando algún principal obtiene un ticket. Las únicas diferencias radican en que `kinit` no proporciona un valor de duración, y el principal de servicio que otorga el ticket proporciona un valor de duración máxima (en lugar del principal `krbtgt/realm`).

FIGURA 25-1 Cómo se determina la duración de un TGT



Duración del ticket = valor mínimo de L1, L2, L3 y L4

La duración del ticket renovable también se determina a partir del mínimo de los cuatro valores, pero en su lugar se utilizan los valores de duración renovables, de la siguiente manera:

- El valor de duración renovable que especifica la opción -r de kinit, si kinit se utiliza para obtener o renovar el ticket.
- El valor de duración máxima renovable (max\_renewable\_life) que se especifica en el archivo kdc.conf.
- El valor de duración máxima renovable que se especifica en la base de datos de Kerberos para el principal de servicio que proporciona el ticket. En el caso de kinit, el principal de servicio es krbtgt/realm.
- El valor de duración máxima renovable que se especifica en la base de datos de Kerberos para el principal de usuario que solicita el ticket.

## Nombres de principales de Kerberos

Cada ticket se identifica con un nombre de principal. El nombre de principal puede identificar un usuario o un servicio. A continuación se muestran ejemplos de varios nombres de principal.

TABLA 25–4 Ejemplos de nombres de principales de Kerberos

| Nombre de principal                      | Descripción                                                                                                                                                                                                                                                                                                                                                                   |
|------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| changepw/kdc1.example.com@EXAMPLE.COM    | Un principal para el servidor KDC maestro que permite el acceso al KDC cuando se cambian las contraseñas.                                                                                                                                                                                                                                                                     |
| clntconfig/admin@EXAMPLE.COM             | Un principal que es empleado por la utilidad de instalación kclnt.                                                                                                                                                                                                                                                                                                            |
| ftp/boston.example.com@EXAMPLE.COM       | Un principal que es empleado por el servicio ftp. Este principal puede utilizarse en lugar de un principal de host.                                                                                                                                                                                                                                                           |
| host/boston.example.com@EXAMPLE.COM      | Un principal que es empleado por las aplicaciones de Kerberos (por ejemplo, klist y kprop) y los servicios (como ftp y telnet). Este principal se llama principal de host o de servicio. El principal se utiliza para autenticar los montajes de NFS. Este principal también lo utilizan los clientes para verificar que el TGT que reciben provenga del KDC correspondiente. |
| K/M@EXAMPLE.COM                          | El nombre de principal clave maestro. Se asocia un nombre de principal clave maestro con cada KDC maestro.                                                                                                                                                                                                                                                                    |
| kadmin/history@EXAMPLE.COM               | Un principal que incluye una clave utilizada para mantener los historiales de las contraseñas de otros principales. Cada KDC maestro tiene uno de los siguientes principales.                                                                                                                                                                                                 |
| kadmin/kdc1.example.com@EXAMPLE.COM      | Un principal para el servidor KDC maestro que permite el acceso al KDC con kadmin.                                                                                                                                                                                                                                                                                            |
| kadmin/changepw.example.com@EXAMPLE.COM  | Un principal que se utiliza para aceptar solicitudes de cambio de contraseña de clientes que no están ejecutando una versión de Oracle Solaris.                                                                                                                                                                                                                               |
| krbtgt/EXAMPLE.COM@EXAMPLE.COM           | Este principal se utiliza cuando se genera un ticket de otorgamiento de tickets.                                                                                                                                                                                                                                                                                              |
| krbtgt/EAST.EXAMPLE.COM@WEST.EXAMPLE.COM | Este principal es un ejemplo de un ticket de otorgamiento de tickets entre dominios.                                                                                                                                                                                                                                                                                          |
| nfs/boston.example.com@EXAMPLE.COM       | Un principal que emplea el servicio NFS. Este principal puede utilizarse en lugar de un principal de host.                                                                                                                                                                                                                                                                    |
| root/boston.example.com@EXAMPLE.COM      | Un principal que está asociado a la cuenta root en un cliente. Este principal se denomina principal de root y proporciona acceso root a los sistemas de archivos montados en NFS.                                                                                                                                                                                             |
| username@EXAMPLE.COM                     | Un principal para un usuario.                                                                                                                                                                                                                                                                                                                                                 |
| nombre_de_usuario/admin@EXAMPLE.COM      | Un principal de admin que se puede utilizar para administrar la base de datos del KDC.                                                                                                                                                                                                                                                                                        |

## Cómo funciona el sistema de autenticación Kerberos

Las aplicaciones le permiten iniciar sesión en un sistema remoto si puede proporcionar un ticket que demuestre su identidad y una clave de sesión coincidente. La clave de sesión contiene información que es específica del usuario y del servicio al que se accede. El KDC crea un ticket y una clave de sesión para todos los usuarios cuando inician sesión por primera vez. El ticket y la clave de sesión coincidente constituyen una credencial. Mientras utilice varios servicios de red, el usuario puede recopilar muchas credenciales. El usuario debe tener una credencial para cada servicio que se ejecute en un servidor determinado. Por ejemplo, para acceder al servicio `ftp` en un servidor que se llama `boston` se requiere una credencial. Para acceder al servicio `ftp` en otro servidor se necesita la credencial correspondiente.

El proceso de creación y almacenamiento de las credenciales es transparente. Las credenciales las crea el KDC que las envía al solicitante. Cuando se recibe, la credencial se almacena en una antememoria de credenciales.

## Cómo interactúa el servicio Kerberos con DNS y el servicio nsswitch

El servicio Kerberos se compila a fin de usar el DNS para resolver nombres de host. El servicio `nsswitch` no se verifica nunca cuando la resolución del nombre de host está lista.

## Obtención de acceso a un servicio con Kerberos

Para acceder a un servicio específico en un servidor específico, el usuario debe obtener dos credenciales. La primera credencial es para el ticket de otorgamiento de tickets (conocido como el TGT). Una vez que el servicio de otorgamiento de tickets descifra esta credencial, el servicio crea una segunda credencial para el servidor al que el usuario solicita acceso. Esta segunda credencial se puede utilizar para solicitar acceso al servicio en el servidor. Después de que el servidor descifra correctamente la segunda credencial, se le otorga el acceso al usuario. En las siguientes secciones, se describe este proceso de manera más detallada.

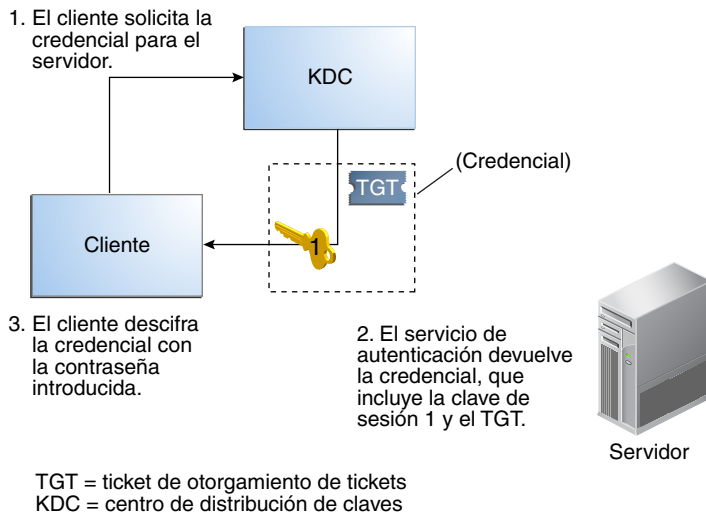
## Obtención de una credencial para el servicio de otorgamiento de tickets

1. A fin de iniciar el proceso de autenticación, el cliente envía una solicitud al servidor de autenticación para un principal de usuario específico. Esta solicitud se envía sin cifrado. En la solicitud no se incluye ninguna información que deba permanecer segura, por lo que no es necesario utilizar el cifrado.

2. Una vez que el servicio de autenticación recibe la solicitud, el nombre de principal del usuario se consulta en la base de datos del KDC. Si un principal coincide con la entrada en la base de datos, el servicio de autenticación obtiene la clave privada de ese principal. Luego, el servicio de autenticación genera una clave de sesión que utilizarán el cliente y el servicio de otorgamiento de tickets (Clave de sesión 1) y un ticket para el servicio de otorgamiento de tickets (Ticket 1). A este ticket también se lo conoce como *ticket de otorgamiento de tickets* (TGT). Tanto la clave de sesión como el ticket se cifran con la clave privada del usuario, y la información se envía de vuelta al cliente.
3. El cliente utiliza esta información para descifrar la Clave de sesión 1 y el Ticket 1 con la clave privada para el principal de usuario. Como únicamente el usuario y la base de datos del KDC deben conocer la clave privada, la información que se encuentra en el paquete debe permanecer segura. El cliente almacena la información en la antememoria de credenciales.

Durante este proceso, por lo general, al usuario se le solicita una contraseña. Si la contraseña que el usuario especifica es la misma que la que se ha utilizado para crear la clave privada almacenada en la base de datos del KDC, el cliente puede descifrar correctamente la información que envía el servicio de autenticación. Así, el cliente obtiene una credencial para utilizar con el servicio de otorgamiento de tickets. El cliente está listo para solicitar una credencial para un servidor.

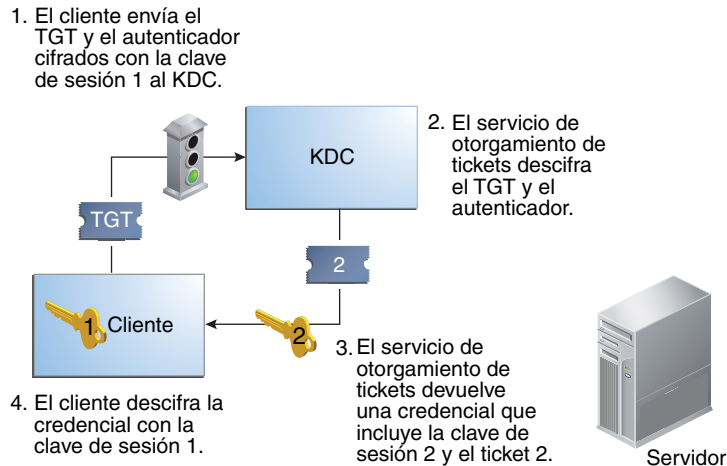
FIGURA 25-2 Obtención de una credencial para el servicio de otorgamiento de tickets



## Obtención de una credencial para un servidor

1. Para solicitar acceso a un servidor específico, el cliente debe haber obtenido primero una credencial para ese servidor desde el servicio de autenticación. Consulte [“Obtención de una credencial para el servicio de otorgamiento de tickets” en la página 537](#). Luego, el cliente envía una solicitud al servicio de otorgamiento de tickets, que incluye el nombre de principal del servicio (Ticket 1) y un autenticador que fue cifrado con la Clave de sesión 1. Originalmente, el servicio de autenticación cifró el Ticket 1 con la clave de servicio del servicio de otorgamiento de tickets.
2. El Ticket 1 se puede descifrar porque el servicio de otorgamiento de tickets conoce la clave de servicio del servicio de otorgamiento de tickets. La información del Ticket 1 incluye la Clave de sesión 1, por lo que el servicio de otorgamiento de tickets puede descifrar el autenticador. En este punto, el principal de usuario se autentica con el servicio de otorgamiento de tickets.
3. Una vez que la autenticación se realiza correctamente, el servicio de otorgamiento de tickets genera una clave de sesión para el principal de usuario y para el servidor (Clave de sesión 2), y un ticket para el servidor (Ticket 2). Luego, la Clave de sesión 2 y el Ticket 2 se cifran con la Clave de sesión 1. Como sólo el cliente y el servicio de otorgamiento de tickets conocen la Clave de sesión 1, esta información es segura y se puede enviar a través de la red con seguridad.
4. Cuando recibe este paquete de información, el cliente descifra la información con la Clave de sesión 1, que había almacenado en la antememoria de credenciales. El cliente obtuvo una credencial para usarla con el servidor. Ahora el cliente está listo para solicitar acceso a un servicio determinado en ese servidor.

FIGURA 25-3 Obtención de una credencial para un servidor



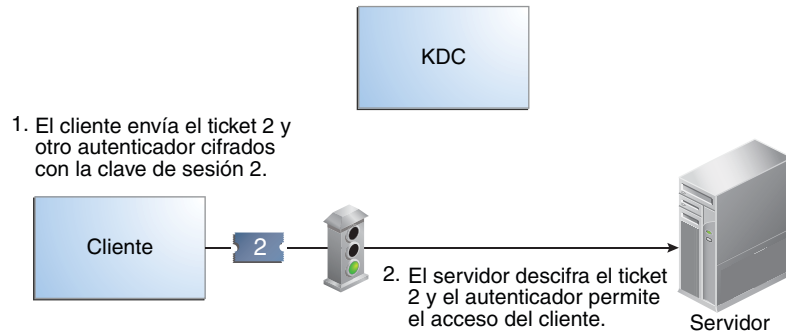
TGT = ticket de otorgamiento de tickets  
KDC = centro de distribución de claves

## Obtención de acceso a un servicio específico

1. Para solicitar acceso a un servicio específico, el cliente debe haber obtenido antes una credencial para el servicio de otorgamiento de tickets del servidor de autenticación y un servidor credenciales del servicio de otorgamiento de tickets. Consulte [“Obtención de una credencial para el servicio de otorgamiento de tickets” en la página 537](#) y [“Obtención de una credencial para un servidor” en la página 539](#). A continuación, el cliente puede enviar al servidor una solicitud que incluya el Ticket 2 y otro autenticador. El autenticador se cifra con la Clave de sesión 2.
2. El Ticket 2 se cifró mediante el servicio de otorgamiento de tickets con la clave de servicio para el servicio. Como el principal de servicio conoce la clave de servicio, el servicio puede descifrar el Ticket 2 y obtener la Clave de sesión 2. Luego, la Clave de sesión 2 puede usarse para descifrar el autenticador. Si el autenticador se descifra correctamente, el cliente obtiene acceso al servicio.



FIGURA 25-4 Obtención de acceso a un servicio específico



## Uso de los tipos de cifrado de Kerberos

Los tipos de cifrado identifican los algoritmos criptográficos y el modo en que se deben usar cuando se realizan las operaciones criptográficas. Los tipos de cifrado `aes`, `des3-cbc-sha1` y `rc4-hmac` permiten la creación de claves que se pueden utilizar para las operaciones criptográficas más resistentes. Estas operaciones más resistentes mejoran la seguridad general del servicio Kerberos.

Cuando un cliente solicita un ticket del KDC, el KDC debe usar claves cuyo tipo de cifrado sea compatible tanto con el cliente como con el servidor. Mientras que el protocolo Kerberos permite al cliente solicitar que el KDC utilice determinados tipos de cifrado para la parte del cliente de la respuesta de ticket, el protocolo no permite que el servidor especifique tipos de cifrado para el KDC.

**Nota** – Si tiene instalado un KDC maestro que no ejecuta la versión Solaris 10, los KDC esclavos deben actualizarse a la versión Solaris 10 antes de actualizar el KDC maestro. Un KDC maestro de Solaris 10 utilizará los nuevos tipos de cifrado, que un esclavo anterior no podrá manejar.

A continuación se enumeran algunos de los problemas que deben tenerse en cuenta antes de cambiar los tipos de cifrado.

- El KDC supone que el servidor admite el primer tipo de cifrado/clave asociado a la entrada de principal de servidor en la base de datos de principal.
- En el KDC, debe asegurarse de que las claves generadas para el principal sean compatibles con los sistemas en los que se autenticará el principal. De manera predeterminada, el comando `kadmin` crea claves para todos los tipos de cifrado admitidos. Si los sistemas en los que se utiliza el principal no admiten este conjunto de tipos de cifrado predeterminado, debe restringir los tipos de cifrado cuando crea un principal. Puede restringir los tipos de cifrado mediante el uso del indicador `-e` en `kadmin addprinc` o la definición del parámetro `supported_ectypes` en el archivo `kdc.conf` de este subconjunto. El parámetro

`supported_etypes` debe utilizarse cuando la mayoría de los sistemas de un dominio Kerberos admiten un subconjunto del conjunto predeterminado de tipos de cifrado. Al definir `supported_etypes`, se especifica el conjunto predeterminado de tipos de cifrado que `kadmin addprinc` utiliza cuando crea un principal para un dominio en particular. Como regla general, es mejor controlar los tipos de cifrado utilizados por Kerberos con alguno de estos dos métodos.

- Cuando vaya a determinar los tipos de cifrado que admite un sistema, tenga en cuenta la versión de Kerberos que se ejecuta en el sistema y los algoritmos criptográficos que admite la aplicación de servidor para la que se crea un principal de servidor. Por ejemplo, cuando se crea un principal de servicio `nfs/hostname`, debe restringir los tipos de cifrado para los tipos que admite el servidor NFS en ese host. Tenga en cuenta que, en la versión Solaris 10, el servidor NFS también admite todos los tipos de cifrado de Kerberos.
- El parámetro `master_key_etype` del archivo `kdc.conf` se puede utilizar para controlar el tipo de cifrado de la clave maestra que cifra las entradas de la base de datos del principal. No utilice este parámetro si la base de datos del principal del KDC ya se ha creado. El parámetro `master_key_etype` se puede usar en el momento de la creación de la base de datos para cambiar el tipo de cifrado predeterminado para la clave maestra, de `des-cbc-crc` a un tipo de cifrado más resistente. Cuando configure los KDC esclavos, asegúrese de que todos admitan el tipo de cifrado seleccionado y tengan una entrada `master_key_etype` idéntica en su archivo `kdc.conf`. Asimismo, asegúrese de que `master_key_etype` se encuentre definido en uno de los tipos de cifrado en `supported_etypes` si `supported_etypes` está definido en `kdc.conf`. Si alguno de estos problemas no se trata adecuadamente, es posible que el KDC maestro no pueda trabajar con los KDC esclavos.
- En el cliente, puede controlar qué tipos de cifrado el cliente solicita cuando obtiene los tickets procedentes del KDC mediante algunos parámetros de `krb5.conf`. El parámetro `default_tkt_etypes` especifica los tipos de cifrado que el cliente está dispuesto a utilizar cuando el cliente solicita un ticket de otorgamiento de tickets (TGT) desde el KDC. El cliente utiliza el TGT para adquirir otros tickets del servidor con más eficacia. Se define `default_tkt_etypes` a fin de otorgarle al cliente un poco de control sobre los tipos de cifrado que se utilizan para proteger la comunicación entre el cliente y el KDC cuando el cliente solicita un ticket de servidor con el TGT (esto se llama solicitud TGS). Tenga en cuenta que los tipos de cifrado especificados en `default_tkt_etypes` deben coincidir, al menos, con uno de los tipos de cifrado de la clave de principal en la base de datos del principal que se almacena en el KDC. De lo contrario, la solicitud TGT fallará. En la mayoría de las situaciones, es mejor no definir `default_tkt_etypes` porque este parámetro puede generar problemas de interoperabilidad. De manera predeterminada, el código de cliente pide que todos los tipos de cifrado admitidos y el KDC seleccionen los tipos de cifrado en función de las claves que el KDC encuentre en la base de datos del principal.
- El parámetro `default_tgs_etypes` restringe los tipos de cifrado que el cliente solicita en sus solicitudes TGS, que se utilizan para adquirir tickets de servidor. Este parámetro también restringe los tipos de cifrado que el KDC utiliza cuando crea la clave de sesión que el cliente y el servidor comparten. Por ejemplo, si un cliente quiere usar solamente el cifrado 3DES cuando emplea NFS seguro, debe definir `default_tgs_etypes = des3-cbc-sha1`.

Asegúrese de que los principales de servidor y de cliente tengan una clave des-3-cbc-sha1 en la base de datos del principal. Al igual que con `default_tkt_enctype`, probablemente sea mejor, en la mayoría de los casos, no establecer esto, ya que puede provocar problemas de interoperabilidad si las credenciales no están configuradas correctamente en el KDC o en el servidor.

- En el servidor, puede controlar los tipos de cifrado aceptados por el servidor con `permitted_enctypes` en `kdcc.conf`. Además, puede especificar los tipos de cifrado utilizados en la creación de entradas `keytab`. Por lo general, es mejor no utilizar ninguno de estos métodos para controlar los tipos de cifrado y, en su lugar, dejar que el KDC determine los tipos de cifrado que se usarán, porque el KDC no se comunica con la aplicación del servidor para determinar qué clave o tipo de cifrado se usarán.

## Tabla de uso de `gsscred`

Un servidor NFS utiliza la tabla `gsscred` cuando el servidor intenta identificar un usuario de Kerberos si las asignaciones predeterminadas no son suficientes. El servicio NFS utiliza los ID de UNIX para identificar a los usuarios. Estos ID no forman parte de un principal de usuario ni de una credencial. La tabla `gsscred` proporciona asignaciones adicionales de las credenciales GSS a los UID de UNIX (desde el archivo de contraseñas). La tabla debe crearse y administrarse una vez que se haya rellenado la base de datos del KDC. Consulte [“Asignación de credenciales GSS a credenciales UNIX” en la página 366](#) para obtener más información.

Cuando se recibe una solicitud de cliente, el servicio NFS intenta asignar el nombre de la credencial a un ID de UNIX. Si la asignación falla, se comprueba la tabla `gsscred`.

## Diferencias importantes entre Oracle Solaris Kerberos y MIT Kerberos

La versión de Solaris 10 del servicio Kerberos se basa en la versión 1.2.1 de MIT Kerberos. A continuación, se enumeran las mejoras incluidas en la versión de Solaris 10 que no se incluyen en la versión 1.2.1 del MIT:

- Compatibilidad de Kerberos con las aplicaciones remotas de Oracle Solaris
- Propagación progresiva para la base de datos del KDC
- Secuencia de comandos de configuración del cliente
- Mensajes de errores localizados
- Compatibilidad del registro de auditoría de Oracle Solaris
- Uso seguro de subprocesos de Kerberos con GSS-API
- Uso de la estructura de cifrado para la criptografía

Además, esta versión incluye algunas correcciones de errores posteriores al MIT Kerberos 1.2.1. En especial, se incorporaron correcciones de errores de 1.2.5 `btrees` y la admisión de 1.3 TCP.



## P A R T E V I I

# Auditoría en Oracle Solaris

En esta sección se proporciona información acerca de la configuración, la gestión y el uso del subsistema de auditoría.

- Capítulo 26, “Auditoría (descripción general)”
- Capítulo 27, “Planificación de la auditoría”
- Capítulo 28, “Gestión de auditoría (tareas)”
- Capítulo 29, “Auditoría (referencia)”



## Auditoría (descripción general)

---

El subsistema de auditoría de Oracle Solaris mantiene un registro de cómo se está utilizando el sistema. El servicio de auditoría incluye herramientas para ayudar con el análisis de los datos de auditoría.

En este capítulo, se presenta cómo funciona la auditoría en el Oracle Solaris:

- “¿Qué es la auditoría?” en la página 547
- “Conceptos y terminología de auditoría” en la página 548
- “¿Cómo se relaciona la auditoría con la seguridad?” en la página 558
- “¿Cómo funciona la auditoría?” en la página 559
- “¿Cómo se configura la auditoría?” en la página 560
- “Auditoría en un sistema con zonas de Oracle Solaris” en la página 561
- “Acerca del servicio de auditoría en esta versión” en la página 562

Para obtener sugerencias de planificación, consulte el [Capítulo 27, “Planificación de la auditoría”](#). Para obtener información sobre procedimientos para configurar la auditoría en su sitio, consulte el [Capítulo 28, “Gestión de auditoría \(tareas\)”](#). Para obtener información de referencia, consulte el [Capítulo 29, “Auditoría \(referencia\)”](#).

### ¿Qué es la auditoría?

La auditoría es la recopilación de datos sobre el uso de los recursos del sistema. Los datos de auditoría proporcionan un registro de los eventos del sistema relacionados con la seguridad. Estos datos se pueden utilizar para asignar responsabilidad para acciones que ocurren en un host. La auditoría correcta comienza con dos funciones de seguridad: identificación y autenticación. En cada inicio de sesión, después de que un usuario proporciona un nombre de usuario y la autenticación PAM se realiza correctamente, se genera un *ID de usuario de auditoría* único e inmutable y se lo asocia con el usuario, y se genera un ID de sesión de auditoría único y se lo asocia con el proceso del usuario. El ID de sesión de auditoría es heredado por cada proceso que se inicia durante esa sesión de inicio de sesión. Cuando un usuario cambia a otro usuario, a todas las acciones del usuario se les realiza un seguimiento con

el mismo ID de usuario de auditoría. Para obtener más detalles sobre cómo cambiar la identidad, consulte la página del comando `man su(1M)`. Tenga en cuenta que, de manera predeterminada, ciertas acciones como el inicio y cierre del sistema siempre se auditan.

El servicio de auditoría hace que lo siguiente sea posible:

- Supervisión de eventos relacionados con la seguridad que ocurren en el host
- Registro de los eventos en una pista de auditoría de toda la red
- Detección de uso incorrecto o actividad no autorizada
- Revisión de patrones de acceso e historiales de acceso de personas y objetos
- Detección de intentos para eludir los mecanismos de protección
- Detección de uso ampliado de privilegio que se produce cuando un usuario cambia la identidad

# Conceptos y terminología de auditoría

Los siguientes términos se usan para describir el servicio de auditoría. Algunas definiciones incluyen enlaces a descripciones más completas.

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                  |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| clase de auditoría              | <p>Una agrupación de eventos de auditoría. Las clases de auditoría proporcionan una forma de seleccionar un grupo de eventos que se van a auditar.</p> <p>Para obtener más información, consulte “<a href="#">Clases de auditoría y preselección</a>” en la página 552 y las páginas del comando <code>man audit_flags(5)</code>, <code>audit_class(4)</code> y <code>audit_event(4)</code>.</p> |
| sistema de archivo de auditoría | <p>Un repositorio de archivos de auditoría en formato binario.</p> <p>Para obtener más información, consulte “<a href="#">Registros de auditoría</a>” en la página 555 y la página del comando <code>man audit.log(4)</code>.</p>                                                                                                                                                                |
| evento de auditoría             | <p>Una acción del sistema relacionada con la seguridad que se puede auditar. Para una mayor facilidad de selección, los eventos se agrupan en clases de auditoría.</p> <p>Para obtener más información, consulte “<a href="#">Eventos de auditoría</a>” en la página 551 y la página del comando <code>man audit_event(4)</code>.</p>                                                            |
| indicador de auditoría          | <p>Una clase de auditoría que se proporciona como un argumento para un comando o palabra clave. Un indicador puede estar precedido de un signo más o signo menos para</p>                                                                                                                                                                                                                        |



|                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|--------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                          | <p>indicar que la clase se audita para determinar si es correcta (+) o tiene fallos (-). Un signo de intercalación (^) indica que no se debe auditar una clase correcta (^+) o que no se debe auditar una clase con fallos (^-).</p> <p>Para obtener más información, consulte la página del comando <code>man audit_flags(5)</code> y <a href="#">“Sintaxis de la clase de auditoría” en la página 646</a>.</p>                                                                                                                                                                                                                                                                                                                                                                                                                     |
| complemento de auditoría | <p>Un módulo que transfiere los registros de auditoría de la cola a una ubicación especificada. El complemento <code>audit_binfile</code> crea archivos de auditoría binarios. Los archivos de auditoría binarios incluyen la pista de auditoría, que está almacenada en sistemas de archivos de auditoría. El complemento <code>audit_remote</code> envía registros de auditoría binarios a un repositorio remoto. El complemento <code>audit_syslog</code> realiza un resumen de todos los registros de auditoría en los registros <code>syslog</code>.</p> <p>Para obtener más información, consulte <a href="#">“Módulos de complemento de auditoría” en la página 554</a> y las páginas del comando <code>man</code> de módulo, <code>audit_binfile(5)</code>, <code>audit_remote(5)</code> y <code>audit_syslog(5)</code>.</p> |
| política de auditoría    | <p>Un conjunto de opciones de auditoría que puede activar o desactivar en el sitio. Estas opciones incluyen si se desean registrar o no determinados tipos de datos de auditoría. Las opciones también incluyen si se desean suspender o no acciones auditables cuando la cola de auditoría está llena.</p> <p>Para obtener más información, consulte <a href="#">“Comprensión de la política de auditoría” en la página 571</a> y la página del comando <code>man auditconfig(1M)</code>.</p>                                                                                                                                                                                                                                                                                                                                       |
| registro de auditoría    | <p>Datos de auditoría que se recopilan en la cola de auditoría. Un registro de auditoría describe un único evento de auditoría. Cada registro de auditoría se compone de tokens de auditoría.</p> <p>Para obtener más información, consulte <a href="#">“Registros de auditoría y tokens de auditoría” en la página 553</a> y la página del comando <code>man audit.log(4)</code>.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| token de auditoría       | <p>Un campo de un evento o registro de auditoría. Cada token de auditoría describe un atributo de un evento de auditoría, como un usuario, un programa u otro objeto.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

|                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|---------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                     | <p>Para obtener más información, consulte <a href="#">“Formatos de token de auditoría” en la página 653</a> y la página del comando <code>man audit.log(4)</code>.</p>                                                                                                                                                                                                                                                                                                                                                                          |
| pista de auditoría  | <p>Una colección de uno o más archivos de auditoría que almacenan los datos de auditoría de todos los sistemas auditados que utilizan el complemento predeterminado, <code>audit_binfile</code>.</p>                                                                                                                                                                                                                                                                                                                                            |
|                     | <p>Para obtener más información, consulte <a href="#">“Pista de auditoría” en la página 651</a>.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| auditoría local     | <p>Recopilación de registros de auditoría que se generan en el sistema local. Los registros se pueden generar en la zona global, en las zonas no globales o en ambos lugares.</p>                                                                                                                                                                                                                                                                                                                                                               |
|                     | <p>Para obtener más información, consulte <a href="#">“Módulos de complemento de auditoría” en la página 554</a>.</p>                                                                                                                                                                                                                                                                                                                                                                                                                           |
| selección posterior | <p>La elección de qué eventos de auditoría se deben examinar en la pista de auditoría. El complemento activo predeterminado, <code>audit_binfile</code>, crea la pista de auditoría. Una herramienta de selección posterior, el comando <code>audit_reduce</code>, selecciona registros de la pista de auditoría.</p>                                                                                                                                                                                                                           |
|                     | <p>Para obtener más información, consulte las páginas del comando <code>man auditreduce(1M)</code> y <code>praudit(1M)</code>.</p>                                                                                                                                                                                                                                                                                                                                                                                                              |
| preselección        | <p>La elección de qué clases de auditoría se deben supervisar. Los eventos de auditoría de clases de auditoría preseleccionadas se recopilan en la cola de auditoría. Las clases de auditoría que no se preseleccionan no se auditan, por lo que sus eventos no aparecen en la cola.</p>                                                                                                                                                                                                                                                        |
|                     | <p>Para obtener más información, consulte <a href="#">“Clases de auditoría y preselección” en la página 552</a> y las páginas del comando <code>man audit_flags(5)</code> y <code>auditconfig(1M)</code>.</p>                                                                                                                                                                                                                                                                                                                                   |
| objeto público      | <p>Un archivo que es propiedad del usuario <code>root</code> y que todo el mundo puede leer. Por ejemplo, los archivos en el directorio <code>/etc</code> y el directorio <code>/usr/bin</code> son objetos públicos. Los objetos públicos no se auditan en eventos de sólo lectura. Por ejemplo, incluso si la clase de auditoría <code>file_read (fr)</code> está preseleccionada, la lectura de objetos públicos no se audita. Puede sustituir el valor predeterminado cambiando la opción de política de auditoría <code>public</code>.</p> |

**auditoría remota**

Servidor de auditoría remota (Audit Remote Server, ARS) que recibe y almacena los registros de auditoría de un sistema que se está auditando y se configura con un complemento `audit_remote` activo. Para distinguir un sistema auditado de un ARS, se puede hacer referencia al sistema auditado como “sistema auditado localmente”.

Para obtener más información, consulte las opciones `-set remote` en la página del comando `man auditconfig(1M)` y en “Servidor de auditoría remoto” en la página 648.

## Eventos de auditoría

Los eventos de auditoría representan acciones que se pueden auditar en un sistema. Los eventos de auditoría se muestran en el archivo `/etc/security/audit_event`. Cada evento de auditoría está conectado a una llamada del sistema o comando de usuario, y está asignado a una o más clases de auditoría. Para obtener una descripción del formato del archivo `audit_event`, consulte la página del comando `man audit_event(4)`.

Por ejemplo, el evento de auditoría `AUE_EXECVE` audita la llamada del sistema `execve()`. El comando `auditrecord -e execve` muestra esta entrada:

```
execve
 system call execve See execve(2)
 event ID 23 AUE_EXECVE
 class ps,ex (0x0000000040100000)
 header
 path
 [attribute] omitted on error
 [exec_arguments] output if argv policy is set
 [exec_environment] output if arge policy is set
 subject
 [use_of_privilege]
 return
```

Cuando preselecciona la clase de auditoría `ps` o la clase de auditoría `ex`, entonces cada llamada del sistema `execve()` se registra en la cola de auditoría.

La auditoría maneja eventos *atribuibles* y *no atribuibles*. La política de auditoría divide los eventos en *síncronos* y *asíncronos*, de la siguiente manera:

- **Eventos atribuibles:** eventos que se pueden atribuir a un usuario. La llamada del sistema `execve()` se puede atribuir a un usuario, por lo tanto, se considera un evento atribuible. Todos los eventos atribuibles son eventos síncronos.
- **Eventos no atribuibles:** eventos que ocurren en el nivel de interrupción del núcleo o antes de que un usuario sea autenticado. La clase de auditoría `na` maneja los eventos de auditoría que no son atribuibles. Por ejemplo, el inicio del sistema es un evento no atribuible. La mayoría de los eventos no atribuibles son eventos asíncronos. Sin embargo, los eventos no atribuibles que tienen procesos asociados, como inicios de sesión fallidos, son eventos síncronos.
- **Eventos síncronos:** eventos que están asociados con un proceso en el sistema. La mayoría de los eventos del sistema son eventos síncronos.
- **Eventos asíncronos:** eventos que no están asociados con ningún proceso, por lo que no hay ningún proceso disponible para bloquear y más tarde reactivar. Los eventos de salida y entrada de la PROM, y de inicio del sistema inicial son ejemplos de eventos asíncronos.

Además de los eventos de auditoría que define el servicio de auditoría, las aplicaciones de terceros pueden generar eventos de auditoría. Los números de evento de auditoría de 32768 a 65535 están disponibles para aplicaciones de terceros. Los proveedores necesitan ponerse en contacto con sus representantes de Oracle Solaris para reservar números de evento y obtener acceso a las interfaces de auditoría.

## Clases de auditoría y preselección

Cada uno de los eventos de auditoría pertenece a una *clase de auditoría* o a clases de auditoría. Las clases de auditoría son contenedores prácticos para un gran número de eventos de auditoría. Cuando se *preselecciona* una clase para auditar, todos los eventos de esa clase se registran en la cola de auditoría. Por ejemplo, cuando preselecciona la clase de auditoría `ps`, se registran `execve()`, `fork()` y otras llamadas del sistema.

Puede preseleccionar para eventos de un sistema y para eventos iniciados por un usuario concreto.

- **Preselección en todo el sistema:** especifique los valores predeterminados en todo el sistema para auditoría mediante las opciones `-setflags` y `-setnaflags` para el comando `auditconfig`.

---

**Nota** – Si la política `perzone` está establecida, se pueden especificar las clases de auditoría predeterminadas en cada zona. Para la auditoría `perzone`, los valores predeterminados son para toda la zona y no para todo el sistema.

---

- **Preselección específica del usuario:** especifique diferencias de valores predeterminados de auditoría en todo el sistema para usuarios individuales mediante la configuración de los indicadores de auditoría para el usuario. Los comandos `useradd`, `roleadd`, `usermod` y `rolemod` ubican el atributo de seguridad `audit_flags` en la base de datos `user_attr`. El comando `profiles` ubica indicadores de auditoría para los perfiles de derechos en la base de datos `prof_attr`.

La máscara de preselección de auditoría determina las clases de eventos que se auditarán para un usuario. Para obtener una descripción de la máscara de preselección de usuario, consulte [“Características del proceso de auditoría” en la página 650](#). Para conocer los indicadores de auditoría configurados que se utilizan, consulte [“Orden de búsqueda para atributos de seguridad asignados” en la página 207](#).

Las clases de auditoría se definen en el archivo `/etc/security/audit_class`. Cada entrada contiene la máscara de auditoría para la clase, el nombre para la clase y un nombre descriptivo para la clase. Por ejemplo, las definiciones de clase `lo` y `ps` aparecen en el archivo `audit_class`, de la siguiente manera:

```
0x00000000000000000000000000000000:lo:login or logout
0x00000000000000000000000000000000:ps:process start/stop
```

Las clases de auditoría incluyen dos clases globales: `all` y `no`. Las clases de auditoría se describen en la página del comando `man audit_class(4)`. Para la lista de clases, lea el archivo `/etc/security/audit_class`.

La asignación de eventos de auditoría a clases es configurable. Puede eliminar eventos de una clase, agregar eventos a una clase y crear una nueva clase para colocar eventos seleccionados. Para conocer el procedimiento, consulte [“Cómo cambiar una pertenencia a clase de un evento de auditoría” en la página 591](#). Para ver los eventos que se asignan a una clase, utilice el comando `auditrecord -c clase`.

## Registros de auditoría y tokens de auditoría

Cada *registro de auditoría* registra la aparición de un único evento auditado. El registro incluye información, como quién realizó la acción, qué archivos fueron afectados, qué acción se intentó realizar y dónde y cuándo ocurrió la acción. El siguiente ejemplo muestra un registro de auditoría login con tres tokens: header, subject y return:

```
header,69,2,login - local,,example_system,2010-10-10 10:10:10.020 -07:00
subject,jdoe,jdoe,staff,jdoe,staff,1210,4076076536,69 2 example_system
return,success,0
```

El tipo de información que se guarda para cada uno de los eventos de auditoría se define mediante un conjunto de *tokens de auditoría*. Cada vez que un registro de auditoría se crea para un evento, el registro contiene algunos de los tokens o todos los tokens que se definen para el

evento. La naturaleza del evento determina qué tokens se registran. En el ejemplo anterior, cada línea empieza con el nombre del token de auditoría. El contenido del token de auditoría sigue al nombre del token. Juntos, los tokens de auditoría header, subject y return componen el registro de auditoría login - local. Para mostrar los tokens que componen un registro de auditoría, utilice el comando `auditrecord -e evento`.

Para obtener una descripción detallada de la estructura de cada token de auditoría con un ejemplo de salida de `praudit`, consulte [“Formatos de token de auditoría” en la página 653](#). Para obtener una descripción de la cadena binaria de tokens de auditoría, consulte la página del comando `man audit.log(4)`.

## Módulos de complemento de auditoría

Los módulos de complemento de auditoría dirigen los registros de auditoría de la cola de auditoría a un archivo o repositorio. Al menos un complemento debe estar activo. De manera predeterminada, el complemento `audit_binfile` está activo. Los complementos se configuran con el comando `auditconfig -setplugin plugin-name`.

El servicio de auditoría proporciona los siguientes complementos:

- Complemento `audit_binfile`: maneja la entrega de la cola de la auditoría a los archivos de auditoría binarios. Para obtener más información, consulte la página de comando `man audit.log(4)`.
- Complemento `audit_remote`: maneja la entrega segura de registros de auditoría binarios de la cola de auditoría a un servidor remoto configurado. El complemento `audit_remote` utiliza la biblioteca `libgss()` para autenticar el servidor. La transmisión está protegida para privacidad e integridad.
- Complemento `audit_syslog`: maneja la entrega de registros seleccionados de la cola de auditoría a los registros `syslog`.

Para configurar un complemento, consulte la página del comando `man auditconfig(1M)`. Para ver ejemplos de configuración de complementos, consulte las tareas en [“Configuración de registros de auditoría \(tareas\)” en la página 592](#). Para obtener información sobre los complementos, consulte las páginas del comando `man audit_binfile(5)`, `audit_remote(5)` y `audit_syslog(5)`.

## Registros de auditoría

Los registros de auditoría se recopilan en registros de auditoría. El servicio de auditoría proporciona tres modos de salida para los registros de auditoría.

- Los registros que se denominan *archivos de auditoría* almacenan registros de auditoría en formato binario. El conjunto de archivos de auditoría de un sistema o sitio proporciona un registro de auditoría completo. El registro de auditoría completo se denomina *pista de auditoría*. Estos registros se crean mediante el complemento `audit_binfile` y pueden ser revisados por los comandos `praudit` y `auditreduce` de selección posterior.
- El complemento `audit_remote` envía registros de auditoría a un repositorio remoto. El repositorio es responsable de mantener una pista de auditoría y de suministrar herramientas de selección posterior.
- La utilidad `syslog` recopila y almacena resúmenes de texto del registro de auditoría. Un registro `syslog` no está completo. El siguiente ejemplo muestra una entrada `syslog` para un registro de auditoría login:

```
Oct 10 10:10:20 example_system auditd: [ID 6472 audit.notice] \
login - login ok session 4076172534 by root as root:other
```

Un sitio puede configurar la auditoría para recopilar registros de auditoría en todos los formatos. Puede configurar los sistemas en su sitio para que usen el modo binario localmente, para que envíen archivos binarios a un repositorio remoto y para usar el modo `syslog`. En la siguiente tabla, se comparan registros de auditoría binarios con registros de auditoría `syslog`.

TABLA 26-1 Comparación de registros de auditoría binarios, remotos y `syslog`

| Función              | Registros binarios y remotos                                                                                                                                                                                                                | Registros <code>syslog</code>                                                                         |
|----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------|
| Protocolo            | Binario: escribe en el sistema de archivos<br><br>Remoto: envía a un repositorio remoto                                                                                                                                                     | Utiliza UDP para el registro remoto                                                                   |
| Tipo de datos        | Binarios                                                                                                                                                                                                                                    | Texto                                                                                                 |
| Longitud de registro | Sin límite                                                                                                                                                                                                                                  | Hasta 1024 caracteres por registro de auditoría                                                       |
| Ubicación            | Binario: almacenado en un zpool en el sistema<br><br>Remoto: repositorio remoto                                                                                                                                                             | Se almacenan en una ubicación que se especifica en el archivo <code>syslog.conf</code>                |
| Cómo configurar      | Binario: se define el atributo <code>p_dir</code> en el complemento <code>audit_binfile</code><br><br>Remoto: se define el atributo <code>p_hosts</code> en el complemento <code>audit_remote</code> y se hace que se active el complemento | Se activa el complemento <code>audit_syslog</code> y se configura el archivo <code>syslog.conf</code> |

TABLA 26-1 Comparación de registros de auditoría binarios, remotos y syslog (Continuación)

| Función            | Registros binarios y remotos                                                                                             | Registros syslog                                                                                                  |
|--------------------|--------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------|
| Cómo leer          | Binario: normalmente, en modo de lote, salida del explorador en XML<br><br>Remoto: el repositorio dicta el procedimiento | En tiempo real o se buscan mediante secuencias de comandos creadas para syslog<br><br>Salida de texto sin formato |
| Integridad         | Se garantiza que estén completos y que aparezcan en el orden correcto                                                    | No se garantiza que estén completos                                                                               |
| Indicación de hora | Hora universal coordinada (UTC)                                                                                          | Hora en el sistema que se audita                                                                                  |

Los registros binarios proporcionan la mayor seguridad y cobertura. La salida binaria cumple con los requisitos de las certificaciones de seguridad, como los requisitos de auditoría [Common Criteria](http://www.commoncriteriaportal.org/) (<http://www.commoncriteriaportal.org/>).

El complemento `audit_binfile` escribe los registros en un sistema de archivos que tiene protección para no ser vistos. En un único sistema, todos los registros binarios se recopilan y se muestran en orden. La indicación de hora del UTC en registros binarios permite realizar una comparación exacta cuando los sistemas en una pista de auditoría se distribuyen entre zonas horarias. El comando `praudit -x` permite ver los registros en un explorador, en XML. También puede utilizar secuencias de comandos para analizar la salida XML.

El complemento `audit_remote` escribe registros de auditoría en un repositorio remoto. El repositorio maneja el almacenamiento y la selección posterior.

En contraste, es posible que los registros `syslog` proporcionen una mayor comodidad y flexibilidad. Por ejemplo, puede recopilar los datos de `syslog` de un gran variedad de orígenes. Además, al supervisar eventos `audit.notice` en el archivo `syslog.conf`, la utilidad `syslog` registra un resumen de registros de auditoría con la indicación de hora actual. Puede utilizar las mismas herramientas de análisis y de gestión que ha desarrollado para mensajes `syslog` de una gran variedad de orígenes, incluidos estaciones de trabajo, servidores, cortafuegos y enrutadores. Los registros se pueden consultar en tiempo real y se pueden almacenar en un sistema remoto.

Si usa `syslog.conf` para almacenar registros de auditoría de manera remota, está protegiendo los datos del registro para evitar que los modifique o suprima un agresor. Por otro lado, cuando los registros de auditoría se almacenan de manera remota, los registros son susceptibles a ataques de red, como denegación de servicio y direcciones de origen simuladas. También, el UDP puede eliminar paquetes o puede entregar paquetes que no funcionan. El límite en entradas `syslog` es de 1024 caracteres, por lo que algunos registros de auditoría podrían estar truncados en el registro. En un único sistema, no se recopilan todos los registros de auditoría. Los registros podrían no aparecer en orden. Debido a que cada registro de auditoría se indica con la fecha y la hora del sistema local, no es posible basarse en la indicación de hora para construir una pista de auditoría para varios sistemas.



Para obtener más información sobre complementos y registros de auditoría, consulte lo siguiente:

- Página del comando `man audit_binfile(5)`
- Página del comando `man audit_syslog(5)`
- Página del comando `man audit.log(4)`
- “Cómo asignar espacio de auditoría para la pista de auditoría” en la página 597
- “Cómo configurar registros de auditoría `syslog`” en la página 605

## Almacenamiento y gestión de la pista de auditoría

Cuando el complemento `audit_binfile` está activo, un *sistema de archivos de auditoría* mantiene los archivos de auditoría en formato binario. Una instalación típica utiliza el sistema de archivos `/var/audit` y puede usar sistemas de archivos adicionales. El contenido de todos los sistemas de archivos de auditoría compone la *pista de auditoría*. Los registros de auditoría se almacenan en estos sistemas de archivos en el siguiente orden:

- **Sistema de archivos de auditoría primario:** el sistema `/var/audit`, el sistema de archivos predeterminado para archivos de auditoría de un sistema
- **Sistemas de archivos de auditoría secundarios:** sistemas de archivos donde los archivos de auditoría para un sistema se ubican según el criterio del administrador

Los sistemas de archivos se especifican como argumentos para el atributo `p_dir` del complemento `audit_binfile`. Un sistema de archivos no se utiliza hasta que un sistema de archivos que está antes en la lista esté lleno. Para ver un ejemplo con una lista de las entradas del sistema de archivos, consulte “Cómo crear sistemas de archivos ZFS para archivos de auditoría” en la página 593.

Colocar los archivos de auditoría en el directorio raíz de auditoría predeterminado ayuda al revisor de auditoría cuando revisa la pista de auditoría. El comando `auditreduce` usa el directorio raíz de auditoría para encontrar todos los archivos en la pista de auditoría. El directorio raíz de auditoría predeterminado es `/var/audit`. La opción `-M` para el comando `auditreduce` se puede utilizar para especificar archivos de auditoría de un equipo específico, y la opción `-S` se puede utilizar para especificar un sistema de archivos de auditoría diferente. Para obtener más información, consulte la página del comando `man auditreduce(1M)`.

El servicio de auditoría proporciona comandos para combinar y filtrar archivos de la pista de auditoría. El comando `auditreduce` puede fusionar archivos de auditoría de la pista de auditoría. El comando también puede filtrar archivos para localizar eventos particulares. El comando `praudit` lee los archivos binarios. Las opciones para el comando `praudit` ofrecen una salida que es adecuada para las secuencias de comandos y para la presentación del explorador.

## Indicaciones de hora confiables

Al fusionar registros de auditoría de varios sistemas, la fecha y la hora en esos sistemas deben ser exactas. De manera similar, al enviar registros de auditoría a un sistema remoto, el sistema de registro y sistema de repositorio deben tener relojes precisos. El protocolo de hora de red (NTP) mantiene relojes del sistema precisos y coordinados. Para obtener más información, consulte la página del comando `man` [Capítulo 3, “Servicios relacionados con el tiempo” de \*Introducción a los servicios de red de Oracle Solaris 11\*](#) and the `xntpd(1M)`.

## Gestión de un repositorio remoto

Una vez que se configura el complemento `audit_remote`, un repositorio remoto recibe los registros de auditoría. El servidor de auditoría remota (ARS) proporciona un receptor para los registros de auditoría. Los registros de auditoría pasan al ARS mediante una conexión protegida y se pueden almacenar de forma similar a como se almacenan localmente. Para configurar un ARS, consulte [“Cómo configurar un repositorio remoto para los archivos de auditoría” en la página 601](#). Para obtener una descripción del ARS, consulte la página del comando `man` [“Servidor de auditoría remoto” en la página 648](#) and the `ars(5)`.

## ¿Cómo se relaciona la auditoría con la seguridad?

La auditoría ayuda a detectar posibles brechas de seguridad al revelar patrones sospechosos o anómalos del uso del sistema. La auditoría también proporciona un medio para rastrear acciones sospechosas de un usuario concreto, lo que sirve como elemento de disuasión. Es decir, es menos probable que los usuarios que saben que sus actividades se están auditando intenten realizar actividades maliciosas.

Para proteger un sistema informático, especialmente un sistema en una red, se requieren mecanismos que controlan las actividades antes de que comiencen los procesos del sistema o del usuario. La seguridad requiere herramientas que supervisan las actividades a medida que se producen. También requiere informes de actividades después de que las actividades ocurren.

El mejor método requiere que los parámetros de auditoría se establezcan antes de que los usuarios inicien sesión o se inicien procesos del sistema, porque la mayoría de las actividades de auditoría incluyen la supervisión de eventos actuales y el registro de eventos que cumplen con parámetros especificados. Cómo el servicio de auditoría supervisa e informa estos eventos se trata detalladamente en el [Capítulo 27, “Planificación de la auditoría”](#) y el [Capítulo 28, “Gestión de auditoría \(tareas\)”](#).

La auditoría no puede evitar que los piratas informáticos entren de manera no autorizada. Sin embargo, el servicio de auditoría puede informar, por ejemplo, que un usuario específico realizó acciones específicas a una hora y en una fecha concretas. El informe de auditoría puede identificar al usuario por ruta de entrada y nombre de usuario. Dicha información se puede informar de inmediato en su terminal y en un archivo para su análisis posterior. Por lo tanto, el servicio de auditoría proporciona datos que ayudan a determinar lo siguiente:

- Cómo se comprometió la seguridad del sistema
- Qué espacios de bucle se deben cerrar para garantizar el nivel de seguridad deseado

## ¿Cómo funciona la auditoría?

La auditoría genera registros de auditoría cuando se producen eventos especificados. Habitualmente, los eventos que generan registros de auditoría incluyen los siguientes:

- Inicio y cierre del sistema
- Inicio y cierre de sesión
- Creación o destrucción de proceso, o creación o destrucción de subproceso
- Apertura, cierre, creación, destrucción o cambio de nombre de objetos
- Uso de capacidades de privilegio o control de acceso basado en roles (RBAC)
- Acciones de identificación y de autenticación
- Cambios de permiso por un proceso o usuario
- Acciones administrativas, como la instalación de un paquete
- Aplicaciones específicas de sitio

Los registros de auditoría se generan a partir de tres orígenes:

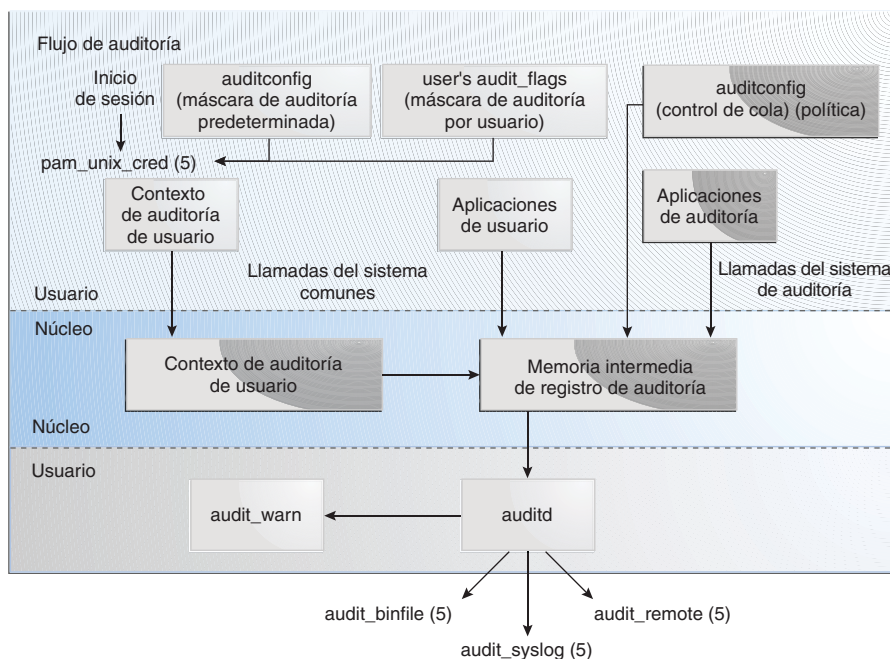
- Por una aplicación
- Como resultado de un [evento asíncrono de auditoría](#)
- Como resultado de una llamada del sistema de proceso

Una vez que la información de evento pertinente se ha capturado, la información se formatea en un registro de auditoría. En cada registro de auditoría, se incluye información que identifica el evento, qué generó el evento, la hora del evento y otra información relevante. Este registro se coloca en una cola de auditoría y se envía a los *complementos* activos para su almacenamiento. Al menos un complemento debe estar activo, aunque todos los complementos pueden estar activos. Los complementos se describen en “[¿Cómo se configura la auditoría?](#)” en la página 560 y en “[Módulos de complemento de auditoría](#)” en la página 554.

## ¿Cómo se configura la auditoría?

Durante la configuración del sistema, *preselecciona* las clases de registros de auditoría que desea supervisar. También puede ajustar el grado de auditoría que se realiza para usuarios individuales. En la siguiente figura, se muestran los detalles del flujo de auditoría en Oracle Solaris.

FIGURA 26-1 El flujo de auditoría



Después de que los datos de auditoría se recopilan en el núcleo, los complementos distribuyen los datos a las ubicaciones adecuadas.

- El complemento `audit_binfile` ubica registros de auditoría binarios en el sistema de archivos `/var/audit`. De manera predeterminada, el complemento `audit_binfile` está activo. Las herramientas de selección posterior permiten examinar partes interesantes de la pista de auditoría.

Los archivos de auditoría se pueden almacenar en una o más agrupaciones ZFS. Estas agrupaciones pueden estar en diferentes sistemas y en redes diferentes pero que estén relacionadas. La recopilación de archivos de auditoría que están enlazados se considera una *pista de auditoría*.

- El complemento `audit_remote` envía registros de auditoría binarios a través de un enlace protegido a un repositorio remoto.
- El complemento `audit_syslog` envía resúmenes de texto de registros de auditoría a la utilidad `syslog`.

Los sistemas que instalan zonas no globales pueden auditar todas las zonas de forma idéntica desde la zona global. Estos sistemas también se pueden configurar para recopilar diferentes registros en las zonas no globales. Para obtener más información, consulte [“Auditoría y zonas de Oracle Solaris” en la página 645](#).

## Auditoría en un sistema con zonas de Oracle Solaris

Una zona es un entorno de sistema operativo virtualizado que se crea dentro de una única instancia del SO Oracle Solaris. El servicio de auditoría realiza la auditoría de la totalidad del sistema, incluidas las actividades en las zonas. Un sistema que ha instalado zonas no globales puede ejecutar un solo servicio de auditoría para auditar todas las zonas de manera idéntica o puede ejecutar un servicio de auditoría por zona, incluida la zona global.

Los sitios que cumplen con las siguientes condiciones pueden ejecutar un solo servicio de auditoría:

- El sitio requiere una pista de auditoría de única imagen.
- Las zonas no globales se utilizan como contenedores de aplicaciones. Las zonas forman parte de un dominio administrativo. Es decir, ninguna zona no global tiene archivos personalizados de servicio de nombres.

Si todas las zonas en un sistema están dentro de un dominio administrativo, la política de auditoría `zonename` se puede utilizar para distinguir eventos de auditoría configurados en zonas distintas.

- Los administradores desean una baja sobrecarga de auditoría. El administrador de la zona global audita todas las zonas de manera idéntica. Además, el daemon de auditoría de la zona global presta servicio a todas las zonas en el sistema.

Los sitios que cumplen con las siguientes condiciones pueden ejecutar un servicio de auditoría por zona:

- El sitio no requiere una pista de auditoría de única imagen.
- Las zonas no globales tienen archivos personalizados de servicio de nombres. Esos dominios administrativos separados, normalmente, funcionan como servidores.
- Los administradores de zonas individuales desean controlar la auditoría en las zonas que administran. En la auditoría por zona, los administradores de zonas pueden decidir activar o desactivar la auditoría para la zona que administran.

Las ventajas de la auditoría por zona son una pista de auditoría personalizada para cada zona y la capacidad de desactivar la auditoría en una zona por zona. Estas ventajas pueden ser

contrarrestadas por la sobrecarga administrativa. Cada administrador de zona debe administrar la auditoría. Cada zona ejecuta su propio daemon de auditoría y tiene su propia cola de auditoría y sus propios registros de auditoría. Estos registros de auditoría se deben gestionar.

## Acerca del servicio de auditoría en esta versión

En esta versión de Oracle Solaris, se han introducido las siguientes características para la auditoría.

- Se puede configurar un repositorio remoto que recibe los registros de auditoría. La conexión entre un sistema auditado y su repositorio remoto está protegida por el mecanismo GSS-API. Cualquier número de sistemas auditados se puede conectar al mismo repositorio remoto.
- Se definió una nueva clase de auditoría. La clase de auditoría `cusa` contiene eventos que afectan a los usuarios y roles.
- Los archivos de configuración de auditoría `audit_class`, `audit_event` y `audit_warn` tienen dos atributos de paquete definidos. El atributo `preserve=renamew` permite que los archivos se modifiquen, y las modificaciones se retienen en las actualizaciones de paquetes y en las correcciones de paquetes. El atributo `overlay=allow` permite que los archivos sean reemplazados por archivos en paquetes que crea un cliente.

# Planificación de la auditoría

En este capítulo, se describe cómo planificar la personalización del servicio de auditoría para su instalación de Oracle Solaris:

- “Planificación de la auditoría (tareas)” en la página 563
- “Comprensión de la política de auditoría” en la página 571
- “Control de costos de auditoría” en la página 573
- “Auditoría eficaz” en la página 575

Para obtener una descripción general de la auditoría, consulte el [Capítulo 26, “Auditoría \(descripción general\)”](#). Para obtener información sobre procedimientos para configurar la auditoría en su sitio, consulte el [Capítulo 28, “Gestión de auditoría \(tareas\)”](#). Para obtener información de referencia, consulte el [Capítulo 29, “Auditoría \(referencia\)”](#).

## Planificación de la auditoría (tareas)

Desea ser selectivo sobre los tipos de actividades que se auditan. Al mismo tiempo, desea recopilar información de auditoría útil. También debe planificar cuidadosamente a quién auditar y qué auditar. Si utiliza el complemento `audit_binfile` predeterminado, los archivos de auditoría pueden crecer rápidamente para llenar el espacio disponible, por lo tanto debe asignar suficiente espacio en disco.

El siguiente mapa de tareas hace referencia a las tareas principales necesarias para planificar el espacio en disco y los eventos que se deben registrar.

| Tarea                                                        | Para obtener instrucciones                                               |
|--------------------------------------------------------------|--------------------------------------------------------------------------|
| Determinar la estrategia de auditoría para zonas no globales | <a href="#">“Cómo planificar auditoría en zonas” en la página 564</a>    |
| Determinar a quién y qué auditar                             | <a href="#">“Cómo planificar a quién y qué auditar” en la página 565</a> |

| Tarea                                                                   | Para obtener instrucciones                                                                                             |
|-------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------|
| Planificar espacio de almacenamiento para la pista de auditoría         | <a href="#">“Cómo planificar espacio en el disco para los registros de auditoría” en la página 568</a>                 |
| Planificar la transmisión de la pista de auditoría a un servidor remoto | <a href="#">“Cómo prepararse para transmitir los registros de auditoría al almacenamiento remoto” en la página 569</a> |

## ▼ Cómo planificar auditoría en zonas

Si su sistema contiene zonas no globales, las zonas se pueden auditar cuando se audita la zona global, o el servicio de auditoría para cada zona no global se puede configurar, activar y desactivar por separado. Por ejemplo, puede auditar sólo las zonas no globales sin auditar la zona global.

Para ver una explicación de las compensaciones, consulte [“Auditoría en un sistema con zonas de Oracle Solaris” en la página 561](#).

- **Elija una de las siguientes opciones:**
  - **OPCIÓN 1: Configurar un único servicio de auditoría para todas las zonas.**

Auditar todas las zonas de manera idéntica puede crear una pista de auditoría de imagen única. Una pista de auditoría de imagen única se produce cuando utiliza `audit_binfile` o el complemento `audit_remote`, y todas las zonas en un sistema son parte de un solo dominio administrativo. Los registros de auditoría se pueden comparar fácilmente porque los registros en cada zona están preseleccionados con valores de configuración idénticos.

Esta configuración trata todas las zonas como parte de un sistema. La zona global ejecuta el único servicio de auditoría en un sistema y recopila registros de auditoría para cada zona. Se personalizan los archivos `audit_class` y `audit_event` sólo en la zona global y, a continuación, se copian estos archivos en cada zona no global.

**a. Utilice el mismo servicio de nombres para cada zona.**

---

**Nota** – Si los archivos de servicio de nombres están personalizados en zonas no globales y la política `perzone` no está establecida, se requiere el uso cuidadoso de herramientas de auditoría para seleccionar registros utilizables. Un ID de usuario en una zona puede hacer referencia a un usuario diferente del mismo ID en una zona diferente.

---

**b. Permita que los registros de auditoría incluyan el nombre de la zona.**

Para colocar el nombre de zona como parte del registro de auditoría, establezca la política `zonename` en la zona global. El comando `audit reduce` podrá seleccionar luego los eventos de auditoría por zona de la pista de auditoría. Si desea ver un ejemplo, consulte la página del comando `man auditreduce(1M)`.



Para planificar una pista de auditoría de imagen única, consulte [“Cómo planificar a quién y qué auditar” en la página 565](#). Comience con el primer paso. El administrador de la zona global también debe dejar a un lado el almacenamiento, como se describe en [“Cómo planificar espacio en el disco para los registros de auditoría” en la página 568](#).

#### ■ OPCIÓN 2: Configurar un servicio de auditoría por zona.

Opte por configurar la auditoría por zona si diferentes zonas usan diferentes bases de datos de servicio de nombres o si los administradores de zonas desean controlar la auditoría en sus zonas.

---

**Nota** – Para auditar zonas no globales, se debe establecer la política per zone, pero el servicio de auditoría no tiene que estar activado en la zona global. La auditoría de la zona no global se configura y el servicio de auditoría se activa y desactiva independientemente de la zona global.

---

- Cuando configura la auditoría por zona, establece la política de auditoría per zone en la zona global. Si la auditoría por zona se establece antes de que se inicie por primera vez la zona no global, la auditoría comienza en el primer inicio de la zona. Para establecer una política de auditoría, consulte [“Cómo configurar la auditoría por zona” en la página 610](#).
- Cada administrador de zona configura la auditoría para la zona.  
Un administrador de zona no global puede establecer todas las opciones de política excepto per zone y ahlt.
- Cada administrador de zona puede activar o desactivar la auditoría en la zona.
- Para generar registros que puedan rastrearse a sus respectivas zonas de origen durante la revisión, establezca la política de auditoría zonename.

Para planificar auditoría por zona, consulte [“Cómo planificar a quién y qué auditar” en la página 565](#). Puede saltar el primer paso. Si el complemento audit\_binfile está activo, cada administrador de zona debe dejar a un lado el almacenamiento para cada zona, como se describe en [“Cómo planificar espacio en el disco para los registros de auditoría” en la página 568](#).

## ▼ Cómo planificar a quién y qué auditar

### Antes de empezar

Si implementa zonas no globales, revise [“Cómo planificar auditoría en zonas” en la página 564](#) antes de utilizar este procedimiento.

#### 1 Determine si desea una pista de auditoría de imagen de sistema único.

---

**Nota** – Este paso se aplica sólo al complemento audit\_binfile.

---

Los sistemas dentro de un único dominio administrativo pueden crear una pista de auditoría de imagen de sistema único. Si los sistemas utilizan diferentes servicios de nombres, comience con el [Paso 2](#). Luego, complete el resto de los pasos de planificación para cada sistema.

Para crear una pista de auditoría de imagen de sistema único para un sitio, cada sistema en la instalación debe configurarse como se indica a continuación:

- Utilice el mismo servicio de nombres para todos los sistemas.  
Para una correcta interpretación de los registros de auditoría, los archivos `passwd`, `group` y `hosts` deben ser consistentes.
- Configure el servicio de auditoría de manera idéntica en todos los sistemas. Para obtener información sobre la visualización y modificación de la configuración de servicio, consulte la página del comando `man auditconfig(1M)`.
- Utilice los mismos archivos `audit_warn`, `audit_event` y `audit_class` para todos los sistemas.

## 2 Determine la política de auditoría.

De manera predeterminada, sólo la política `cnt` está activa.

Utilice el comando `auditconfig -lspolicy` para ver una descripción de opciones de políticas disponibles.

- Para ver los efectos de las opciones de política, consulte [“Comprensión de la política de auditoría” en la página 571](#).
- Para el efecto de la política `cnt`, consulte [“Políticas de auditoría para eventos síncronos y asíncronos” en la página 649](#).
- Para establecer una política de auditoría, consulte [“Cómo cambiar la política de auditoría” en la página 585](#).

## 3 Determine si desea modificar asignaciones evento-clase.

En la mayoría de las situaciones, la asignación predeterminada es suficiente. Sin embargo, si agrega nuevas clases, cambia las definiciones de clase o determina que un registro de una llamada del sistema específica no es útil, es posible que desee modificar asignaciones de evento-clase.

Para obtener un ejemplo, consulte [“Cómo cambiar una pertenencia a clase de un evento de auditoría” en la página 591](#).

## 4 Determine las clases de auditoría que se van preseleccionar.

La mejor hora para agregar clases de auditoría o cambiar las clases predeterminadas es antes de que los usuarios inicien sesión en el sistema.

Las clases de auditoría que preselecciona con las opciones `-setflags` y `-setnaflags` para el comando `auditconfig` se aplican a todos los usuarios y procesos. Puede preseleccionar una clase para comprobar si es correcta, si tiene fallos o ambas cosas.

Para la lista de clases de auditoría, lea el archivo `/etc/security/audit_class`.

## 5 Determine modificaciones de usuario para preselecciones en todo el sistema.

Si ha decidido que algunos usuarios se deben auditar de manera diferente en el sistema, puede modificar el atributo de seguridad `audit_flags` para usuarios individuales o para un perfil de derechos. La máscara de preselección de usuario se modifica para los usuarios cuyos indicadores de auditoría se definen explícitamente o a quienes se les asigna un perfil de derechos con indicadores de auditoría explícitos.

Para conocer el procedimiento, consulte [“Cómo configurar las características de auditoría de un usuario” en la página 581](#). Para conocer los valores de indicadores que están vigentes, consulte [“Orden de búsqueda para atributos de seguridad asignados” en la página 207](#).

## 6 Decida cómo gestionar el alias de correo electrónico `audit_warn`.

La secuencia de comandos `audit_warn` se ejecuta siempre que el sistema de auditoría detecta una situación que requiere atención administrativa. De manera predeterminada, la secuencia de comandos `audit_warn` envía un correo electrónico al alias `audit_warn` y envía un mensaje a la consola.

Para configurar el alias, consulte [“Cómo configurar el alias de correo electrónico `audit\_warn`” en la página 589](#).

## 7 Decida en qué formato y dónde recopilar registros de auditoría.

Dispone de tres opciones.

- De manera predeterminada, los registros de auditoría binarios se almacenan localmente. El directorio de almacenamiento predeterminado es `/var/audit`. Para más opciones de configuración del complemento `audit_binfile`, consulte [“Cómo crear sistemas de archivos ZFS para archivos de auditoría” en la página 593](#).
- Envíe registros de auditoría binarios a un repositorio protegido remoto mediante el complemento `audit_remote`. Debe tener un receptor para los registros. Para conocer los requisitos, consulte [“Gestión de un repositorio remoto” en la página 558](#). Para conocer el procedimiento, consulte [“Cómo enviar archivos de auditoría a un repositorio remoto” en la página 600](#).
- Envíe resúmenes de registros de auditoría a `syslog` utilizando el complemento `audit_syslog`. Para conocer el procedimiento, consulte [“Cómo configurar registros de auditoría `syslog`” en la página 605](#).

Para una comparación de formatos `syslog` y binarios, consulte [“Registros de auditoría” en la página 555](#).

## 8 Determine cuándo advertir al administrador sobre la reducción de espacio en disco.

---

**Nota** – Este paso se aplica sólo al complemento `audit_binfile`.

---

Cuando el espacio en disco en un sistema de archivos de auditoría está por debajo del porcentaje de espacio libre mínimo, o límite dinámico, el servicio de auditoría cambia al siguiente directorio de auditoría disponible. A continuación, el servicio envía una advertencia de que el límite dinámico se ha excedido.

Para establecer un porcentaje de espacio libre mínimo, consulte el [Ejemplo 28–17](#).

## 9 Decida la acción que se llevará a cabo cuando todos los directorios de auditoría estén completos.

---

**Nota** – Este paso se aplica sólo al complemento `audit_binfile`.

---

En la configuración predeterminada, el complemento `audit_binfile` está activo y la política `cnt` está establecida. En esta configuración, cuando la cola de auditoría de núcleo está completa, el sistema sigue funcionando. El sistema cuenta los registros de auditoría que se descartan, pero no registra los eventos. Para mayor seguridad, puede desactivar la política `cnt` y activar la política `ahlt`. La política `ahlt` detiene el sistema cuando un evento asíncrono no se puede ubicar en la cola de auditoría.

Para ver una explicación de estas opciones de política, consulte “[Políticas de auditoría para eventos síncronos y asíncronos](#)” en la [página 649](#). Para configurar estas opciones de política, consulte el [Ejemplo 28–6](#).

Sin embargo, si la cola `audit_binfile` está completa y la cola para otro complemento activo no está completa, entonces la cola del núcleo seguirá enviando registros al complemento que no está completo. Cuando la cola `audit_binfile` puede aceptar registros nuevamente, el servicio de auditoría volverá a enviarlos allí.

---

**Nota** – La política `cnt` o `ahlt` no se activa si la cola para al menos un complemento está aceptando registros de auditoría.

---

## ▼ Cómo planificar espacio en el disco para los registros de auditoría

El complemento `audit_binfile` crea una pista de auditoría. La pista de auditoría requiere espacio de archivo dedicado. Este espacio debe estar disponible y debe ser seguro. El sistema utiliza el sistema de archivos `/var/audit` para almacenamiento inicial. Puede configurar sistemas de archivos de auditoría adicionales para los archivos de auditoría. El siguiente procedimiento trata los problemas que debe resolver cuando planifica el almacenamiento de la pista de auditoría.

**Antes de empezar** Si implementa zonas no globales, complete “[Cómo planificar auditoría en zonas](#)” en la [página 564](#) antes de utilizar este procedimiento.

Utiliza el complemento `audit_binfile`.

### 1 Determine cuánta auditoría necesita el sitio.

Equilibre las necesidades de seguridad del sitio con la disponibilidad de espacio en disco para la pista de auditoría.

Para obtener indicaciones acerca de cómo reducir los requisitos de espacio manteniendo la seguridad del sitio y cómo diseñar el almacenamiento de auditoría, consulte “[Control de costos de auditoría](#)” en la [página 573](#) y “[Auditoría eficaz](#)” en la [página 575](#).

Para conocer los pasos prácticos, consulte “[Cómo reducir el volumen de los registros de auditoría que se producen](#)” en la [página 628](#), “[Cómo comprimir archivos de auditoría en un sistema de archivos dedicado](#)” en la [página 637](#) y el [Ejemplo 28–30](#).

### 2 Determine qué sistemas se van a auditar y configure sus sistemas de archivos de auditoría.

Cree una lista de todos los sistemas de archivos de auditoría que se van a utilizar. Para directrices de configuración, consulte “[Almacenamiento y gestión de la pista de auditoría](#)” en la [página 557](#) y la [página](#) del comando `man auditreduce(1M)`. Para especificar los sistemas de archivos de auditoría, consulte “[Cómo asignar espacio de auditoría para la pista de auditoría](#)” en la [página 597](#).

### 3 Sincronice los relojes en todos los sistemas.

Para obtener más información, consulte “[Indicaciones de hora confiables](#)” en la [página 558](#).

## ▼ Cómo prepararse para transmitir los registros de auditoría al almacenamiento remoto

---

**Nota** – Si dispone de un dominio Kerberos configurado con un servidor de auditoría remoto (ARS) identificado y todos los sistemas auditados dentro del dominio, puede omitir este procedimiento. Los pasos para configurar el ARS y los sistemas auditados se incluyen en “[Cómo configurar un repositorio remoto para los archivos de auditoría](#)” en la [página 601](#) y “[Cómo enviar archivos de auditoría a un repositorio remoto](#)” en la [página 600](#).

---

El complemento `audit_remote` envía la pista de auditoría binaria a un ARS en el mismo formato que el complemento `audit_binfile` escribe en los archivos de auditoría locales. El complemento `audit_remote` utiliza la biblioteca `libgss` para autenticar el ARS y un mecanismo GSS-API para proteger la transmisión con privacidad e integridad. Como referencia, consulte “[¿Qué es el servicio Kerberos?](#)” en la [página 347](#) y “[Componentes de Kerberos](#)” en la [página 356](#).

El único mecanismo GSS-API que se admite actualmente es `kerberosv5`. Para obtener más información, consulte la página del comando `man mech(4)`.

### Antes de empezar

Tiene planificado usar el complemento `audit_remote`.

## 1 Cree un dominio Kerberos para sus sistemas auditados.

### a. Instale el paquete KDC principal.

Puede utilizar el sistema que actuará como ARS o puede utilizar un sistema cercano. El ARS envía una cantidad considerable de tráfico de autenticación al KDC principal.

Si los paquetes Kerberos ya están en el sistema, la salida es similar a lo siguiente:

```
pkg search -l kerberos-5
INDEX ACTION VALUE PACKAGE
pkg.summary set Kerberos version 5 support pkg:/service/security/kerberos-5@vnn
pkg.summary set Kerberos V5 Master KDC pkg:/system/security/kerberos-5@vnn
```

El primer comando comprueba si paquete está instalado KDC principal de Kerberos V5 está instalado. El segundo comando instala el paquete.

```
pkg info system/security/kerberos-5
pkg: info: no packages matching these patterns are installed on the system.
pkg install pkg:/system/security/kerberos-5
```

En el KDC principal, usa los comandos `kdcmgr` y `kadmin` de Kerberos para gestionar el dominio. Para obtener más información, consulte las páginas del comando `man kdcmgr(1M)` y `kadmin(1M)`.

## 2 En cada sistema auditado que enviará registros de auditoría al ARS, instale el paquete KDC principal.

```
pkg install pkg:/system/security/kerberos-5
```

Este paquete incluye el comando `kclient`. En estos sistemas, ejecuta el comando `kclient` para conectarse con el KDC. Para obtener referencias, consulte la página del comando `man kclient(1M)`.

## 3 Sincronice los relojes en el dominio de KDC.

Si el sesgo de reloj es demasiado grande entre los sistemas auditados y el ARS, el intento de conexión fallará. Después de establecer una conexión, la hora local del ARS determina los nombres de los archivos de auditoría almacenados, como se describe en “[Convenciones de nombres de archivos de auditoría binarios](#)” en la página 651.

Para obtener más información sobre los relojes, consulte “[Indicaciones de hora confiables](#)” en la página 558.

## Comprensión de la política de auditoría

La política de auditoría determina las características de los registros de auditoría para el sistema local. Puede utilizar el comando `auditconfig` para establecer estas políticas. Para obtener más información, consulte la página del comando `man auditconfig(1M)`.

La mayoría de las opciones de política de auditoría están desactivadas de manera predeterminada para minimizar los requisitos de almacenamiento y las demandas de procesamiento del sistema. Estas opciones son propiedades del servicio de auditoría y determinan las políticas que están vigentes en el inicio del sistema. Para obtener más información, consulte la página del comando `man auditconfig(1M)`.

Utilice la siguiente tabla para determinar si las necesidades de su sitio justifican la sobrecarga adicional que se genera como resultado de la activación de una o más opciones de política de auditoría.

TABLA 27-1 Efectos de opciones de política de auditoría

| Nombre de política | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | Consideraciones de políticas                                                                                                                                                                                                                                                                                                                                                                                                 |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ahlt               | <p>Esta política se aplica sólo a eventos asíncronos. Cuando está desactivada, esta política permite que se complete el evento sin que se haya generado un registro de auditoría.</p> <p>Cuando está activada, esta política detiene el sistema cuando la cola de auditoría está completa. La intervención administrativa es necesaria para limpiar la cola de auditoría, liberar espacio para los registros de auditoría y reiniciar. Esta política sólo puede activarse en la zona global. La política afecta todas las zonas.</p> | <p>La opción desactivada tiene sentido cuando la disponibilidad del sistema es más importante que la seguridad.</p> <p>La opción activada tiene sentido en un entorno donde la seguridad es primordial. Para obtener más detalles, consulte “Políticas de auditoría para eventos síncronos y asíncronos” en la página 649.</p>                                                                                               |
| arge               | <p>Cuando está desactivada, esta política omite variables de entorno de un programa ejecutado del registro de auditoría <code>execve</code>.</p> <p>Cuando está activada, esta política agrega variables de entorno de un programa ejecutado al registro de auditoría <code>execve</code>. Los registros de auditoría resultantes contienen más detalles que cuando esta política está desactivada.</p>                                                                                                                              | <p>La opción desactivada recopila mucho menos información que la opción activada. Para una comparación, consulte “Cómo auditar todos los comandos por usuarios” en la página 630.</p> <p>La opción activada tiene sentido cuando audita a unos pocos usuarios. La opción también resulta útil cuando hay sospechas sobre las variables de entorno que se utilizan en programas en la clase de auditoría <code>ex</code>.</p> |

TABLA 27-1 Efectos de opciones de política de auditoría (Continuación)

| Nombre de política | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | Consideraciones de políticas                                                                                                                                                                                                                                                                                                                                                                                                       |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| argv               | <p>Cuando está desactivada, esta política omite argumentos de un programa ejecutado del registro de auditoría <code>execve</code>.</p> <p>Cuando está activada, esta política agrega argumentos de un programa ejecutado al registro de auditoría <code>execve</code>. Los registros de auditoría resultantes contienen más detalles que cuando esta política está desactivada.</p>                                                                                                                                                                                                                              | <p>La opción desactivada recopila mucho menos información que la opción activada. Para una comparación, consulte <a href="#">“Cómo auditar todos los comandos por usuarios” en la página 630</a>.</p> <p>La opción activada tiene sentido cuando audita a unos pocos usuarios. La opción también resulta útil cuando tiene motivos para creer que programas poco usuales se ejecutan en la clase de auditoría <code>ex</code>.</p> |
| cnt                | <p>Cuando está desactivada, esta política bloquea un usuario o una aplicación para que no se ejecute. El bloqueo ocurre cuando los registros de auditoría no se pueden agregar a la pista de auditoría porque la cola de auditoría está completa.</p> <p>Cuando está activada, esta política permite que se complete el evento sin que se haya generado un registro de auditoría. La política mantiene un recuento de registros de auditoría que se descartan.</p>                                                                                                                                               | <p>La opción desactivada tiene sentido en un entorno donde la seguridad es primordial.</p> <p>La opción activada tiene sentido cuando la disponibilidad del sistema es más importante que la seguridad. Para obtener más detalles, consulte <a href="#">“Políticas de auditoría para eventos síncronos y asíncronos” en la página 649</a>.</p>                                                                                     |
| group              | <p>Cuando está desactivada, esta política no agrega una lista de grupos a los registros de auditoría.</p> <p>Cuando está activada, esta política agrega una lista de grupos a cada registro de auditoría como un token especial.</p>                                                                                                                                                                                                                                                                                                                                                                             | <p>La opción desactivada normalmente satisface los requisitos de seguridad del sitio.</p> <p>La opción activada tiene sentido cuando necesita auditar los grupos suplementarios a los que pertenece el sujeto.</p>                                                                                                                                                                                                                 |
| path               | <p>Cuando está desactivada, esta política registra en un registro de auditoría una ruta como máximo que se utiliza durante una llamada del sistema.</p> <p>Cuando está activada, esta política registra cada ruta que se utiliza junto con un evento de auditoría para cada registro de auditoría.</p>                                                                                                                                                                                                                                                                                                           | <p>La opción desactivada ubica como máximo una ruta en un registro de auditoría.</p> <p>La opción activada introduce cada nombre de archivo o ruta que se utiliza durante una llamada del sistema en el registro de auditoría como un token <code>path</code>.</p>                                                                                                                                                                 |
| perzone            | <p>Cuando está desactivada, esta política mantiene una única configuración de auditoría para un sistema. Un servicio de auditoría se ejecuta en la zona global. Los eventos de auditoría en zonas específicas se pueden ubicar en el registro de auditoría si el token de auditoría <code>zonename</code> estaba preseleccionado.</p> <p>Cuando está activada, esta política mantiene una configuración de auditoría, una cola de auditoría y registros de auditoría independientes para cada zona. Un servicio de auditoría se ejecuta en cada zona. Esta política se puede activar sólo en la zona global.</p> | <p>La opción desactivada es útil cuando no tiene una razón en especial para mantener un registro de auditoría, una cola y un daemon independientes para cada zona.</p> <p>La opción activada es útil cuando no puede supervisar el sistema eficazmente mediante un examen simple de registros de auditoría con el token de auditoría <code>zonename</code>.</p>                                                                    |



TABLA 27-1 Efectos de opciones de política de auditoría (Continuación)

| Nombre de política    | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | Consideraciones de políticas                                                                                                                                                                                                                                                                                                                                            |
|-----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>public</code>   | <p>Cuando está desactivada, esta política no agrega eventos de sólo lectura de objetos públicos a la pista de auditoría cuando la lectura de archivos está preseleccionada. Las clases de auditoría que contienen eventos de sólo lectura incluyen <code>fr</code>, <code>fa</code> y <code>cl</code>.</p> <p>Cuando está activada, esta política registra todos los eventos de auditoría de sólo lectura de objetos públicos si una clase de auditoría apropiada está preseleccionada.</p> | <p>La opción desactivada normalmente satisface los requisitos de seguridad del sitio.</p> <p>La opción activada rara vez es útil.</p>                                                                                                                                                                                                                                   |
| <code>seq</code>      | <p>Cuando está desactivada, esta política no agrega un número de secuencia a cada registro de auditoría.</p> <p>Cuando está activada, esta política agrega un número de secuencia a cada registro de auditoría. El token <code>sequence</code> contiene el número de secuencia.</p>                                                                                                                                                                                                         | <p>La opción desactivada es suficiente si la auditoría se ejecuta sin problemas.</p> <p>La opción activada tiene sentido cuando la política <code>cnt</code> está activada. La política <code>seq</code> le permite determinar cuándo se descartan los datos. Como alternativa, puede utilizar el comando <code>auditstat</code> para ver registros descartados.</p>    |
| <code>trail</code>    | <p>Cuando está desactivada, esta política no agrega un token <code>trailer</code> a los registros de auditoría.</p> <p>Cuando está activada, esta política agrega un token <code>trailer</code> a cada registro de auditoría.</p>                                                                                                                                                                                                                                                           | <p>La opción desactivada crea un registro de auditoría más pequeño.</p> <p>La opción activada marca claramente el final de cada registro de auditoría con un token <code>trailer</code>. El token <code>trailer</code> se suele utilizar con el token <code>sequence</code>. El token <code>trailer</code> facilita la recuperación de pistas de auditoría dañadas.</p> |
| <code>zonename</code> | <p>Cuando está desactivada, esta política no incluye un token <code>zonename</code> en los registros de auditoría.</p> <p>Cuando está activada, esta política incluye un token <code>zonename</code> en cada registro de auditoría.</p>                                                                                                                                                                                                                                                     | <p>La opción desactivada es útil cuando no necesita hacer un seguimiento del comportamiento de auditoría por zonas.</p> <p>La opción activada es útil si desea aislar y comparar un comportamiento de auditoría entre zonas mediante la selección posterior de registros según la zona.</p>                                                                             |

## Control de costos de auditoría

Debido a que la auditoría consume recursos del sistema, debe controlar el grado de detalle que se registra. Cuando decide lo que se debe auditar, tenga en cuenta los siguientes costos de auditoría:

- Costo de mayor tiempo de procesamiento
- Costo de análisis de datos de auditoría

Si utiliza el complemento predeterminado, `audit_binfile`, también debe considerar el costo de almacenamiento de datos de auditoría.

## Costo de mayor tiempo de procesamiento de datos de auditoría

El costo de mayor tiempo de procesamiento es el menos significativo de los costos de auditoría. La primera razón es que la auditoría por lo general no se produce durante tareas de cálculos intensivos, como procesamiento de imágenes, cálculos complejos, etc. Si utiliza el complemento `audit_binfile`, otra razón es que los administradores de auditoría pueden mover las tareas de selección posterior del sistema auditado a sistemas que se dedican a analizar datos de auditoría. Finalmente, a menos que los sucesos del núcleo estén seleccionados previamente, el servicio de auditoría no tiene ningún impacto medible en el rendimiento del sistema.

## Costo de análisis de datos de auditoría

El costo de análisis es más o menos proporcional a la cantidad de datos de auditoría que se recopilan. El costo de análisis incluye el tiempo que se necesita para fusionar y revisar los registros de auditoría.

Para los registros recopilados por el complemento `audit_binfile`, el costo también incluye el tiempo que se necesita para archivar los registros y sus bases de datos de servicios de nombres admitidas, y mantener los registros en un lugar seguro. Las bases de datos admitidas incluyen `groups`, `hosts` y `passwd`.

Cuantos menos registros se generan, menor es el tiempo que se necesita para analizar la pista de auditoría. Las secciones, [“Costo de almacenamiento de datos de auditoría” en la página 574](#) y [“Auditoría eficaz” en la página 575](#) describen maneras de auditar de manera eficaz. La auditoría eficaz reduce la cantidad de datos de auditoría al tiempo que se sigue proporcionando suficiente cobertura para lograr los objetivos de seguridad del sitio.

## Costo de almacenamiento de datos de auditoría

Si utiliza el complemento `audit_binfile`, el costo de almacenamiento es el costo más significativo para la auditoría. La cantidad de datos de auditoría depende de lo siguiente:

- Número de usuarios
- Número de sistemas
- Cantidad de uso
- Grado de rastreabilidad y responsabilidad necesario

Debido a que estos factores varían de sitio en sitio, ninguna fórmula puede predeterminar la cantidad de espacio en disco que se debe destinar al almacenamiento de datos de auditoría. Utilice la siguiente información como guía:

- Comprenda las clases de auditoría.  
Antes de configurar la auditoría, debe comprender los tipos de eventos que las clases contienen. Puede cambiar las asignaciones de evento-clase de auditoría para optimizar la recopilación de registros de auditoría.
- Preseleccione las clases de auditoría con cuidado para reducir el volumen de registros que se generan.  
La auditoría completa, es decir, con la clase `all`, llena el espacio en disco rápidamente. Incluso una simple tarea, como compilar un programa podría generar un archivo de auditoría de gran tamaño. Un programa de tamaño moderado podría generar miles de registros de auditoría en menos de un minuto.  
Por ejemplo, si se omite la clase de auditoría `file_read`, `fr`, puede reducir significativamente el volumen de auditoría. Si selecciona auditar operaciones fallidas, sólo a veces puede reducir el volumen de auditoría. Por ejemplo, si realiza una auditoría de operaciones fallidas `file_read`, `-fr`, puede generar muchos menos registros que si realiza una auditoría de todos los eventos `file_read`.
- Si utiliza el complemento `audit_binfile`, la gestión eficiente de archivos de auditoría es también importante. Por ejemplo, puede comprimir un sistema de archivos ZFS dedicado a archivos de auditoría.
- Desarrolle una filosofía de auditoría para su sitio.  
Base la filosofía en medidas razonables. Tales medidas incluyen el importe de rastreabilidad que su sitio requiere y los tipos de usuarios que administra.

## Auditoría eficaz

Las siguientes técnicas lo pueden ayudar a lograr los objetivos de seguridad de su organización y al mismo tiempo auditar de manera más eficaz.

- Para la mayor cantidad de clases de auditoría posible, sólo preseleccione aquellas clases para usuarios y roles, y no para todo el sistema.
- Audite de manera aleatoria sólo un determinado porcentaje de usuarios a la vez.
- Si el complemento `audit_binfile` está activo, reduzca los requisitos de espacio en disco para archivos de auditoría filtrando, fusionando y comprimiendo los archivos. Desarrolle procedimientos para archivar los archivos, para transferir los archivos a soportes extraíbles y para almacenar los archivos fuera de línea.
- Supervise los datos de auditoría en tiempo real para comportamientos poco usuales.
  - Complemento `audit_syslog`: puede ampliar las herramientas de análisis y de gestión que ya haya desarrollado para gestionar los registros de auditoría en archivos `syslog`.

- Complemento `audit_binfile`: puede configurar procedimientos para supervisar la pista de auditoría para ciertas actividades. Puede escribir una secuencia de comandos para impulsar un aumento automático de la auditoría de determinados usuarios o determinados sistemas en respuesta a la detección de eventos poco usuales.

Por ejemplo, puede escribir una secuencia de comandos que haga lo siguiente:

1. Controla la creación de archivos de auditoría en los sistemas auditados.
2. Procesa los archivos de auditoría con el comando `tail`.

La conducción de la salida del comando `tail -0f` mediante el comando `praudit` pueden producir un flujo de registros de auditoría a medida que los registros se generan. Para obtener más información, consulte la página del comando `man tail(1)`.

3. Analice este flujo para tipos de mensajes poco usuales u otros indicadores y entregue el análisis al auditor.  
O bien, la secuencia de comandos se puede utilizar para desencadenar respuestas automáticas.
4. Supervise constantemente los sistemas de archivos de auditoría en busca de nuevos archivos de auditoría `not_terminated`.
5. Termine procesos `tail` pendientes cuando no se esté escribiendo en los archivos.

## Gestión de auditoría (tareas)

---

En este capítulo, se proporcionan procedimientos que lo ayudarán a configurar y gestionar la auditoría en un sistema Oracle Solaris. En este capítulo, también se incluyen instrucciones para administrar la pista de auditoría y solucionar problemas del servicio de auditoría. En este capítulo, se tratan las siguientes tareas:

- “Configuración del servicio de auditoría (tareas)” en la página 577
- “Configuración de registros de auditoría (tareas)” en la página 592
- “Configuración del servicio de auditoría en las zonas (tareas)” en la página 607
- “Activación y desactivación del servicio de auditoría (tareas)” en la página 611
- “Gestión de registros de auditoría en sistemas locales (tareas)” en la página 614
- “Solución de problemas del servicio de auditoría (tareas)” en la página 625

Para obtener una descripción general del servicio de auditoría, consulte el [Capítulo 26, “Auditoría \(descripción general\)”](#). Para obtener sugerencias de planificación, consulte el [Capítulo 27, “Planificación de la auditoría”](#). Para obtener información de referencia, consulte el [Capítulo 29, “Auditoría \(referencia\)”](#).

### Configuración del servicio de auditoría (tareas)

Antes de activar la auditoría en su red, puede modificar los valores predeterminados para satisfacer los requisitos de auditoría de su sitio. Lo mejor es personalizar la configuración de auditoría lo más posible antes de que los primeros usuarios inicien sesión.

Si ha implementado zonas, puede decidir auditar todas las zonas de la zona global o auditar las zonas no globales individualmente. Para obtener una descripción general, consulte [“Auditoría y zonas de Oracle Solaris” en la página 645](#). Para obtener información sobre planificación, consulte [“Cómo planificar auditoría en zonas” en la página 564](#). Para obtener información sobre los procedimientos, consulte [“Configuración del servicio de auditoría en las zonas \(tareas\)” en la página 607](#).

# Configuración del servicio de auditoría (mapa de tareas)

En el siguiente mapa de tareas, se hace referencia a los procedimientos para configurar la auditoría. Todas las tareas son opcionales.

| Tarea                                                                 | Descripción                                                                                                                                                                       | Para obtener instrucciones                                                                               |
|-----------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------|
| Mostrar valores predeterminados de auditoría.                         | Antes de configurar la auditoría, muestra la política predeterminada, los controles de colas, los indicadores y el uso de complementos.                                           | <a href="#">“Cómo visualizar los valores predeterminados del servicio de auditoría” en la página 578</a> |
| Seleccionar los eventos que se han auditado.                          | Selecciona previamente en todo el sistema clases de auditoría. Si un evento es atribuible, todos los usuarios se auditan para este evento.                                        | <a href="#">“Cómo preseleccionar clases de auditoría” en la página 580</a>                               |
| Seleccionar los eventos que se van a auditar para usuarios concretos. | Establece diferencias específicas de usuarios para las clases de auditoría en todo el sistema.                                                                                    | <a href="#">“Cómo configurar las características de auditoría de un usuario” en la página 581</a>        |
| Especificar la política de auditoría.                                 | Define datos adicionales de auditoría que el sitio necesita.                                                                                                                      | <a href="#">“Cómo cambiar la política de auditoría” en la página 585</a>                                 |
| Especificar controles de colas.                                       | Modifica el tamaño predeterminado de la memoria intermedia, los registros de auditoría en la cola y el intervalo de escritura de registros de auditoría en la memoria intermedia. | <a href="#">“Cómo cambiar controles de colas de auditoría” en la página 587</a>                          |
| Crear el alias de correo electrónico audit_warn.                      | Define quién recibe advertencias por correo electrónico cuando el servicio de auditoría necesita atención.                                                                        | <a href="#">“Cómo configurar el alias de correo electrónico audit_warn” en la página 589</a>             |
| Configurar registros de auditoría.                                    | Configura la ubicación de los registros de auditoría de cada complemento.                                                                                                         | <a href="#">“Configuración de registros de auditoría (tareas)” en la página 592</a>                      |
| Agregar clases de auditoría.                                          | Reduce el número de registros de auditoría mediante la creación de una nueva clase de auditoría para retener eventos críticos.                                                    | <a href="#">“Cómo agregar una clase de auditoría” en la página 590</a>                                   |
| Cambiar asignaciones de evento-clase.                                 | Reduce el número de registros de auditoría mediante el cambio de la asignación de evento-clase.                                                                                   | <a href="#">“Cómo cambiar una pertenencia a clase de un evento de auditoría” en la página 591</a>        |

## ▼ Cómo visualizar los valores predeterminados del servicio de auditoría

Los comandos en este procedimiento muestran la configuración de auditoría actual. La salida en este procedimiento se toma de un sistema no configurado.

**Antes de empezar** Debe convertirse en un administrador con el perfil de derechos de configuración de auditoría o control de auditoría asignado. Para obtener más información, consulte [“Cómo usar los derechos administrativos que tiene asignados” en la página 164.](#)

### 1 Visualice las clases preseleccionadas para eventos atribuibles.

```
auditconfig -getflags
active user default audit flags = lo(0x1000,0x1000)
configured user default audit flags = lo(0x1000,0x1000)
```

lo es el indicador para la clase de auditoría login/logout. El formato de la salida de la máscara es (*éxito, fallo*).

---

**Nota** – Para ver qué eventos están asignados a una clase y, por lo tanto, qué eventos se registran, ejecute el comando `auditrecord -c clase`.

---

### 2 Visualice las clases preseleccionadas para eventos no atribuibles.

```
auditconfig -getnaflags
active non-attributable audit flags = lo(0x1000,0x1000)
configured non-attributable audit flags = lo(0x1000,0x1000)
```

### 3 Visualice la política de auditoría.

```
$ auditconfig -getpolicy
configured audit policies = cnt
active audit policies = cnt
```

La política *activa* es la política actual, pero el valor de la política no es almacenado por el servicio de auditoría. La política *configurada* es almacenada por el servicio de auditoría, por lo que la política se restaura al reiniciar el servicio de auditoría.

### 4 Visualice información sobre los complementos de auditoría.

```
$ auditconfig -getplugin
Plugin: audit_binfile
 Attributes: p_dir=/var/audit;p_fsize=0;p_minfree=1;

Plugin: audit_syslog (inactive)
 Attributes: p_flags=;

Plugin: audit_remote (inactive)
 Attributes: p_hosts=;p_retries=3;p_timeout=5;
```

El complemento `audit_binfile` está activo de manera predeterminada.

### 5 Visualice los controles de colas de auditoría.

```
$ auditconfig -getqctrl
no configured audit queue hiwater mark
no configured audit queue lowater mark
no configured audit queue buffer size
no configured audit queue delay
active audit queue hiwater mark (records) = 100
active audit queue lowater mark (records) = 10
```

```
active audit queue buffer size (bytes) = 8192
active audit queue delay (ticks) = 20
```

El control de colas *activo* es el control de colas que está siendo utilizado actualmente por el núcleo. La cadena no configured indica que el sistema está utilizando los valores predeterminados.

## 6 Visualice las clases de auditoría que están preseleccionadas para usuarios existentes.

Busque los usuarios y, a continuación, visualice el valor de atributo `audit_flags` del usuario.

```
who
adoe pts/1 Oct 10 10:20 (:0.0)
adoe pts/2 Oct 10 10:20 (:0.0)
jdoe pts/5 Oct 12 12:20 (:0.0)
jdoe pts/6 Oct 12 12:20 (:0.0)
...
userattr audit_flags adoe
userattr audit_flags jdoe
```

De manera predeterminada, los usuarios sólo se auditan para la configuración en todo el sistema.

Para ver una descripción del comando `userattr`, consulte la página del comando [man userattr\(1\)](#). Para ver una descripción de la palabra clave `audit_flags`, consulte la página del comando [user\\_attr\(4\)](#).

## ▼ Cómo preseleccionar clases de auditoría

Preseccione clases de auditoría que contienen los eventos que desea supervisar. Los eventos que no están en clases preseleccionadas no se registran.

### Antes de empezar

Debe convertirse en un administrador con el perfil de derechos de configuración de auditoría asignado. Para obtener más información, consulte [“Cómo usar los derechos administrativos que tiene asignados” en la página 164](#).

## 1 Determine las clases preseleccionadas actuales.

```
auditconfig -getflags
...

auditconfig -getnaflags
...
```

Para obtener una explicación de la salida, consulte [“Cómo visualizar los valores predeterminados del servicio de auditoría” en la página 578](#).

## 2 Preseccione las clases atribuibles.

```
auditconfig -setflags lo,ps,fw
user default audit flags = ps,lo,fw(0x101002,0x101002)
```



Este comando audita los eventos en las clases login/logout, process start/stop y file write para determinar si se efectuaron con éxito o fallaron.

---

**Nota** – El comando `auditconfig -setflags` *sustituye* la preselección actual, por lo que usted debe especificar todas las clases que desea preseleccionar.

---

### 3 Preseleccione las clases no atribuibles.

La clase na contiene montajes no atribuibles, de inicio y de PROM, entre otros eventos.

```
auditconfig -setnaflags lo,na
non-attributable audit flags = lo,na(0x1400,0x1400)
```

Los argumentos lo y na son los únicos argumentos útiles de la opción -setnaflags.

---

**Nota** – El comando `auditconfig -setnaflags` *sustituye* la preselección actual, por lo que usted debe especificar todas las clases que desea preseleccionar.

---

## ▼ Cómo configurar las características de auditoría de un usuario

Mediante la preselección de clases por usuario en lugar de por sistema, a veces, puede reducir el impacto de la auditoría en el rendimiento del sistema. También puede que desee auditar a usuarios específicos de manera ligeramente diferente del sistema.

Las preselecciones de clase de auditoría para cada usuario son especificadas por el atributo de seguridad `audit_flags`. Estos valores específicos de usuario, además de las clases preseleccionadas para el sistema, determinan la máscara de auditoría del usuario, como se describe en “[Características del proceso de auditoría](#)” en la página 650.

#### Antes de empezar

Debe asumir el rol root. Para obtener más información, consulte “[Cómo usar los derechos administrativos que tiene asignados](#)” en la página 164.

- **Defina los indicadores de auditoría en la base de datos `user_attr` o `prof_attr`.**

Por ejemplo, puede crear un perfil de derechos que define los derechos de un subconjunto de sus usuarios. Los usuarios que tengan asignado ese perfil de derechos se auditan de forma idéntica.

- **Para definir indicadores de auditoría de un usuario, utilice el comando `usermod`.**

```
usermod -K audit_flags=fw:no jdoe
```

El formato de la palabra clave `audit_flags` es *siempre\_auditar:nunca\_auditar*.

|                     |                                                                                                                                                                                                                                                                                             |
|---------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>always-audit</i> | Muestra las clases de auditoría que se van a auditar para este usuario. Las modificaciones a las clases de todo el sistema están precedidas por un signo de intercalación (^). Las clases que se agregan a las clases de todo el sistema no están precedidas por un signo de intercalación. |
| <i>never-audit</i>  | Muestra las clases de auditoría que nunca se van a auditar para el usuario, incluso si estos eventos de auditoría se auditan en todo el sistema. Las modificaciones a las clases de todo el sistema están precedidas por un signo de intercalación (^).                                     |

Para especificar varias clases de auditoría, separe las clases con comas. Para obtener más información, consulte la página del comando `man audit_flags(5)`.

- **Para definir indicadores de auditoría para un perfil de derechos., utilice el comando `profiles`.**

```
profiles -p "System Administrator"
profiles:System Administrator> set name="Audited System Administrator"
profiles:Audited System Administrator> set always_audit=fw,as
profiles:Audited System Administrator> end
profiles:Audited System Administrator> exit
```

Cuando asigna el perfil de derechos de administrador del sistema auditado a un usuario o un rol, ese usuario o rol se audita en busca de esos indicadores, según el orden de búsqueda, como se describe en “Orden de búsqueda para atributos de seguridad asignados” en la página 207.

## Ejemplo 28–1 Cambio de eventos que se van a auditar para un usuario

En este ejemplo, la máscara de preselección de auditoría para todos los usuarios es la siguiente:

```
auditconfig -getflags
active user default audit flags = ss,lo(0x11000,0x11000)
configured user default audit flags = ss,lo(0x11000,0x11000)
```

Ningún usuario, excepto el administrador, inicia sesión.

Para reducir el impacto del evento de auditoría `AUE_PFEEXEC` en los recursos del sistema, el administrador no audita este evento en el nivel del sistema. En su lugar, el administrador selecciona previamente la clase `pf` para un usuario, `jdoe`. La clase `pf` se crea en el [Ejemplo 28–10](#).

```
usermod -K audit_flags=pf:no jdoe
```

El comando `userattr` muestra la agregación.

```
userattr audit_flags jdoe
pf:no
```

Cuando el usuario `jdoe` inicia sesión, la máscara de preselección de auditoría de `jdoe` es una combinación de los valores `audit_flags` con los valores predeterminados del sistema. 289 es el PID del shell de inicio de sesión de `jdoe`.

```
auditconfig -getpinfo 289
audit id = jdoe(1234)
process preselection mask = ss,pf,lo(0x0100000008011000,0x0100000008011000)
terminal id (maj,min,host) = 242,511,example1(192.168.160.171)
audit session id = 103203403
```

### Ejemplo 28-2 Modificación de excepción de preselección de auditoría para un usuario

En este ejemplo, la máscara de preselección de auditoría para todos los usuarios es la siguiente:

```
auditconfig -getflags
active user default audit flags = ss,lo(0x11000,0x11000)
configured user default audit flags = ss,lo(0x11000,0x11000)
```

Ningún usuario, excepto el administrador, inicia sesión.

El administrador decide no recopilar eventos `ss` fallidos para el usuario `jdoe`.

```
usermod -K audit_flags=~-ss:no jdoe
```

El comando `userattr` muestra la excepción.

```
userattr audit_flags jdoe
^-ss:no
```

Cuando el usuario `jdoe` inicia sesión, la máscara de preselección de auditoría de `jdoe` es una combinación de los valores `audit_flags` con los valores predeterminados del sistema. 289 es el PID del shell de inicio de sesión de `jdoe`.

```
auditconfig -getpinfo 289
audit id = jdoe(1234)
process preselection mask = +ss,lo(0x11000,0x1000)
terminal id (maj,min,host) = 242,511,example1(192.168.160.171)
audit session id = 103203403
```

### Ejemplo 28-3 Auditoría de usuarios seleccionados, sin auditoría en todo el sistema

En este ejemplo, se auditan el inicio de sesión y las actividades de rol de cuatro usuarios seleccionados en el sistema. No se preseleccionan clases de auditoría para el sistema.

En primer lugar, el administrador elimina todos los indicadores en todo el sistema.

```
auditconfig -setflags no
user default audit flags = no(0x0,0x0)
```

A continuación, el administrador selecciona previamente dos clases de auditoría para los cuatro usuarios. La clase pf se crea en el [Ejemplo 28–10](#).

```
usermod -K audit_flags=lo,pf:no jdoe
usermod -K audit_flags=lo,pf:no kdoe
usermod -K audit_flags=lo,pf:no pdoe
usermod -K audit_flags=lo,pf:no zdoe
```

A continuación, el administrador selecciona previamente la clase pf para el rol root.

```
userattr audit_flags root
rolemod -K audit_flags=lo,pf:no root
userattr audit_flags root
lo,pf:no
```

Para registrar intrusiones injustificadas, el administrador no cambia la auditoría de inicios de sesión no atribuibles.

```
auditconfig -getnaflags
active non-attributable audit flags = lo(0x1000,0x1000)
configured non-attributable audit flags = lo(0x1000,0x1000)
```

#### **Ejemplo 28–4** Eliminación de indicadores de auditoría de un usuario

En el siguiente ejemplo, el administrador elimina todos los indicadores de auditoría específicos de usuario. Los procesos existentes de usuarios que han iniciado sesión actualmente siguen siendo auditados.

El administrador ejecuta el comando usermod con la palabra clave audit\_flags establecida en ningún valor.

```
usermod -K audit_flags= jdoe
usermod -K audit_flags= kdoe
usermod -K audit_flags= ldoe
```

A continuación, el administrador verifica la eliminación.

```
userattr audit_flags jdoe
userattr audit_flags kdoe
userattr audit_flags ldoe
```

#### **Ejemplo 28–5** Creación de un perfil de derechos para un grupo de usuarios

El administrador desea que todos los perfiles de derechos administrativos del sitio auditen explícitamente la clase pf. Para cada perfil de derechos que se va a asignar, el administrador crea una versión específica de sitio en LDAP que incluye indicadores de auditoría.

En primer lugar, el administrador clona un perfil de derechos existente y, luego, cambia el nombre y agrega indicadores de auditoría.

```
profiles -p "Network Wifi Management" -S ldap
profiles: Network Wifi Management> set name="Wifi Management"
profiles: Wifi Management> set desc="Audited wifi management"
profiles: Wifi Management> set audit_always=pf
profiles: Wifi Management> exit
```

Después de repetir este procedimiento para cada perfil de derechos que se va a utilizar, el administrador enumera la información en el perfil de gestión de Wi-Fi.

```
profiles -p "Wifi Management" -S ldap info
name=Wifi Management
desc=Audited wifi management
auths=solaris.network.wifi.config
help=RtNetWifiMngmnt.html
always_audit=pf
```

## ▼ Cómo cambiar la política de auditoría

Puede cambiar la política de auditoría predeterminada para registrar información detallada sobre comandos auditados, para agregar un nombre de zona a cada registro o para satisfacer otros requisitos de seguridad del sitio.

### Antes de empezar

Debe convertirse en un administrador con el perfil de derechos de configuración de auditoría asignado. Para obtener más información, consulte [“Cómo usar los derechos administrativos que tiene asignados” en la página 164](#).

#### 1 Visualice la política de auditoría actual.

```
$ auditconfig -getpolicy
...
```

Para obtener una explicación de la salida, consulte [“Cómo visualizar los valores predeterminados del servicio de auditoría” en la página 578](#).

#### 2 Vea las opciones de política disponibles.

```
$ auditconfig -lspolicy
policy string description:
ahtl halt machine if it can not record an async event
all all policies for the zone
arge include exec environment args in audit recs
argv include exec command line args in audit recs
cnt when no more space, drop recs and keep a cnt
group include supplementary groups in audit recs
none no policies
path allow multiple paths per event
perzone use a separate queue and auditd per zone
public audit public files
seq include a sequence number in audit recs
trail include trailer token in audit recs
windata_down include downgraded window information in audit recs
```

---

```
windata_up include upgraded window information in audit recs
zonename include zonename token in audit recs
```

---

**Nota** – Las opciones de política `perzone` y `ahlt` solamente se pueden configurar en la zona global. Para que las compensaciones usen una opción de política particular, consulte [“Comprensión de la política de auditoría” en la página 571](#).

---

### 3 Active o desactive las opciones de política de auditoría seleccionadas.

```
auditconfig [-t] -setpolicy [prefix]policy[,policy...]
```

**-t**      Optativo. Crea una política *activa* o temporal. Puede definir una política temporal para depurar o para fines de prueba.

Una política temporal permanece vigente hasta que el servicio de auditoría se refresca o hasta que la política es modificada por el comando `auditconfig -setpolicy`.

**prefix**    Un valor de *prefix* de + agrega la lista de políticas a la política actual. Un valor de *prefix* de - elimina la lista de políticas de la política actual. Sin un prefijo, la política de auditoría se restablece. Esta opción le permite mantener las políticas de auditoría actuales.

**policy**    Selecciona la política que se activará o desactivará.

#### Ejemplo 28–6 Configuración de la opción de política de auditoría `ahlt`

En este ejemplo, la seguridad de sitio estricta requiere la política `ahlt`.

```
auditconfig -setpolicy -cnt
auditconfig -setpolicy +ahlt
```

El signo más (+) antes de la política `ahlt` agrega la política a la configuración de política actual. Sin el signo más, la política `ahlt` sustituye todas las políticas de auditoría actuales.

#### Ejemplo 28–7 Definición de una política de auditoría temporal

En este ejemplo, está configurada la política de auditoría `ahlt`. Para la depuración, el administrador agrega la política de auditoría `trail` a la política activa (`+trail`) temporalmente (`-t`). La política `trail` ayuda en la recuperación de pistas de auditoría dañadas.

```
$ auditconfig -setpolicy ahl t
$ auditconfig -getpolicy
configured audit policies = ahl t
active audit policies = ahl t
$ auditconfig -t -setpolicy +trail
configured audit policies = ahl t
active audit policies = ahl t, trail
```

El administrador desactiva la política `trail` cuando la depuración finaliza.

```
$ auditconfig -setpolicy -trail
$ auditconfig -getpolicy
 configured audit policies = ahlt
 active audit policies = ahlt
```

Refrescar el servicio de auditoría ejecutando el comando `audit -s` también elimina esta política temporal, además de otros valores temporales en el servicio de auditoría. Para ver ejemplos de otros valores temporales, consulte [“Cómo cambiar controles de colas de auditoría” en la página 587](#).

### Ejemplo 28–8 Configuración de la política de auditoría `perzone`

En este ejemplo, la política de auditoría `perzone` se agrega a la política existente en la zona global. La configuración de la política `perzone` se almacena como una propiedad permanente, por lo que la política `perzone` está en vigor durante la sesión y cuando el servicio de auditoría se reinicia. Para las zonas, la política está disponible en el siguiente inicio de zona.

```
$ auditconfig -getpolicy
 configured audit policies = cnt
 active audit policies = cnt
$ auditconfig -setpolicy +perzone
$ auditconfig -getpolicy
 configured audit policies = perzone,cnt
 active audit policies = perzone,cnt
```

## ▼ Cómo cambiar controles de colas de auditoría

El servicio de auditoría proporciona valores predeterminados para parámetros de cola de auditoría. Puede inspeccionar y cambiar permanente o temporalmente estos valores con el comando `auditconfig`.

**Antes de empezar** Debe convertirse en un administrador con el perfil de derechos de configuración de auditoría asignado. Para obtener más información, consulte [“Cómo usar los derechos administrativos que tiene asignados” en la página 164](#).

### 1 Visualice los valores actuales de los controles de colas de auditoría.

```
$ auditconfig -getqctrl
...
```

Para obtener una explicación de la salida, consulte [“Cómo visualizar los valores predeterminados del servicio de auditoría” en la página 578](#).

### 2 Modifique controles de colas de auditoría seleccionados.

Para ver ejemplos y una descripción de los controles de colas de auditoría, consulte la página del comando `man auditconfig(1M)`.

- Para modificar algunos o todos los controles de colas de auditoría, utilice la opción `-setqctrl`.

```
auditconfig [-t] -setqctrl hiwater lowater bufisz interval
```

Por ejemplo, establezca el valor *intervalo* en `10` sin establecer los otros controles.

```
auditconfig -setqctrl 0 0 0 10
```

- Para modificar un control de colas de auditoría específico, especifique su opción. La opción `-setqdelay` es el equivalente de `-setqctrl 0 0 0 intervalo`, como en `# auditconfig -setqdelay 10`.

```
auditconfig [-t] -setqhiwater value
```

```
auditconfig [-t] -setqlowater value
```

```
auditconfig [-t] -setqbufisz value
```

```
auditconfig [-t] -setqdelay value
```

### Ejemplo 28–9 Restablecimiento de un control de colas de auditoría al valor predeterminado

El administrador define todos los controles de colas de auditoría y luego regresa el valor *lowater* en el repositorio al valor predeterminado.

```
auditconfig -setqctrl 200 5 10216 10
auditconfig -setqctrl 200 0 10216 10
configured audit queue hiwater mark (records) = 200
no configured audit queue lowater mark
configured audit queue buffer size (bytes) = 10216
configured audit queue delay (ticks) = 10
active audit queue hiwater mark (records) = 200
active audit queue lowater mark (records) = 5
active audit queue buffer size (bytes) = 10216
active audit queue delay (ticks) = 10
```

A continuación, el administrador establece el valor *lowater* en el valor predeterminado para la sesión actual.

```
auditconfig -setqlowater 10
auditconfig -getqlowater
configured audit queue lowater mark (records) = 10
active audit queue lowater mark (records) = 10
```



## ▼ Cómo configurar el alias de correo electrónico `audit_warn`

La secuencia de comandos `/etc/security/audit_warn` genera correo que notifica al administrador sobre incidentes de auditoría que podrían requerir atención. Puede personalizar la secuencia de comandos y puede enviar el correo a una cuenta que no sea `root`.

Si la política `perzone` está establecida, el administrador de la zona no global debe configurar el alias de correo `audit_warn` en la zona no global.

### Antes de empezar

Debe convertirse en un administrador con la autorización `solaris.admin.edit/etc/security/audit_warn` asignada. De manera predeterminada, sólo el rol `root` tiene esta autorización. Para obtener más información, consulte [“Cómo usar los derechos administrativos que tiene asignados” en la página 164](#).

### ● Configure el alias de correo electrónico `audit_warn`.

Elija una de las siguientes opciones:

- **OPCIÓN 1:** reemplace el alias de correo electrónico `audit_warn` con otra cuenta de correo electrónico en la secuencia de comandos `audit_warn`.

Cambie el alias de correo electrónico `audit_warn` en la línea `ADDRESS` de la secuencia de comandos a otra dirección:

```
#ADDRESS=audit_warn # standard alias for audit alerts
ADDRESS=audadmin # role alias for audit alerts
```

---

**Nota** – Para obtener información sobre los efectos de modificar un archivo de configuración de auditoría, consulte [“Archivos de configuración de auditoría y empaquetado” en la página 645](#).

---

- **OPCIÓN 2:** redirija el correo electrónico `audit_warn` a otra cuenta de correo.

Agregue el alias de correo electrónico `audit_warn` al archivo de alias de correo apropiado. Puede agregar el alias al archivo local `/etc/mail/aliases` o a la base de datos `mail_aliases` en el nombre de espacio. La entrada `/etc/mail/aliases` se parecería a lo siguiente si las cuentas de correo electrónico `root` y `audadmin` se han agregado como miembros del alias de correo electrónico `audit_warn`:

```
audit_warn: root,audadmin
```

A continuación, ejecute el comando `newaliases` para reconstruir la base de datos de acceso aleatorio para el archivo `aliases`.

```
newaliases
/etc/mail/aliases: 14 aliases, longest 10 bytes, 156 bytes total
```

## ▼ Cómo agregar una clase de auditoría

Cuando crea su propia clase de auditoría, puede colocar en ella sólo los eventos de auditoría que desea auditar para su sitio. Esta estrategia puede reducir el número de registros que se recopilan y reducir el ruido en la pista de auditoría.

Al agregar la clase en un sistema, copie el cambio en todos los sistemas que se están auditando. La mejor práctica es crear clases de auditoría antes de que se conecten los primeros usuarios.

---

**Nota** – Para obtener información sobre los efectos de modificar un archivo de configuración de auditoría, consulte [“Archivos de configuración de auditoría y empaquetado” en la página 645](#).

---

### Antes de empezar

Seleccione bits libres para su entrada única. Verifique qué bits están disponibles para que usen los clientes en el archivo `/etc/security/audit_class`.

Debe convertirse en un administrador con la autorización `solaris.admin.edit/etc/security/audit_class` asignada. De manera predeterminada, sólo el rol `root` tiene esta autorización. Para obtener más información, consulte [“Cómo usar los derechos administrativos que tiene asignados” en la página 164](#).

#### 1 (Opcional) Guarde una copia de seguridad del archivo `audit_class`.

```
cp /etc/security/audit_class /etc/security/audit_class.orig
```

#### 2 Agregue las nuevas entradas al archivo `audit_class`.

Cada entrada tiene el siguiente formato:

*0x64bitnumber:flag:description*

Para obtener una descripción de los campos, consulte la página del comando `man audit_class(4)`. Para obtener una lista de clases existentes, lea el archivo `/etc/security/audit_class`.

---

**Consejo** – Los archivos de configuración de auditoría de Oracle Solaris le permiten crear su propio paquete que contenga estos archivos y reemplazar los paquetes de Oracle Solaris con archivos personalizados según el sitio. Cuando establece el atributo `preserve` en `true` en su paquete, los subcomandos `pkg`, como `verify`, `fix`, `revert`, etc, se ejecutarán en relación con sus paquetes. Para obtener más información, consulte las páginas del comando `man pkg(1)` y `pkg(5)`.

---

### Ejemplo 28–10 Creación de una clase de auditoría nueva

En este ejemplo, se crea una clase para mantener los comandos administrativos que se ejecutan en un rol. La entrada agregada al archivo `audit_class` se muestra a continuación:

```
0x0100000000000000:pf:profile command
```

La entrada crea la clase de auditoría nueva pf. En el [Ejemplo 28–11](#), se rellena la clase de auditoría nueva.

### Errores más frecuentes

Si ha personalizado el archivo `audit_class`, asegúrese de que los indicadores de auditoría asignados directamente a los usuarios o los perfiles de derechos sean coherentes con las clases de auditoría nuevas. Se producen errores cuando un valor `audit_flags` no es un subconjunto del archivo `audit_class`.

## ▼ Cómo cambiar una pertenencia a clase de un evento de auditoría

Puede que desee cambiar la pertenencia a clase de un evento de auditoría para reducir el tamaño de una clase de auditoría existente o para colocar el evento en una clase propia.



**Precaución** – Nunca quite el comentario de eventos en el archivo `audit_event`. Este archivo es utilizado por el comando `praudit` para leer archivos binarios de auditoría. Los archivos de auditoría almacenados pueden contener eventos que se muestran en el archivo.

Quando reconfigura asignaciones de evento-clase de auditoría en un sistema, copie el cambio en todos los sistemas que se auditan. Lo mejor es cambiar las asignaciones de evento-clase antes de que los primeros usuarios inicien sesión.

**Nota** – Para obtener información sobre los efectos de modificar un archivo de configuración de auditoría, consulte [“Archivos de configuración de auditoría y empaquetado” en la página 645](#).

### Antes de empezar

Debe convertirse en un administrador con la autorización `solaris.admin.edit/etc/security/audit_event` asignada. De manera predeterminada, sólo el rol `root` tiene esta autorización. Para obtener más información, consulte [“Cómo usar los derechos administrativos que tiene asignados” en la página 164](#).

#### 1 (Opcional) Guarde una copia de seguridad del archivo `audit_event`.

```
cp /etc/security/audit_event /etc/security/audit_event.orig
```

#### 2 Cambie la clase a la que pertenecen los eventos determinados; para esto, cambie la *class-list* de los eventos.

Cada entrada tiene el siguiente formato:

```
number:name:description:class-list
```

|                    |                                                                                                             |
|--------------------|-------------------------------------------------------------------------------------------------------------|
| <i>number</i>      | ID de evento de auditoría.                                                                                  |
| <i>name</i>        | Nombre del evento de auditoría.                                                                             |
| <i>description</i> | Normalmente, la llamada de sistema o el ejecutable que desencadena la creación de un registro de auditoría. |
| <i>class-list</i>  | Lista separada por comas de las clases de auditoría.                                                        |

---

**Consejo** – Los archivos de configuración de auditoría de Oracle Solaris le permiten crear su propio paquete que contenga estos archivos y reemplazar los paquetes de Oracle Solaris con archivos personalizados según el sitio. Cuando establece el atributo `preserve` en `true` en su paquete, los subcomandos `pkg`, como `verify`, `fix`, `revert`, etc, se ejecutarán en relación con sus paquetes. Para obtener más información, consulte las páginas del comando `man pkg(1)` y `pkg(5)`.

---

**Ejemplo 28–11** Asignación de eventos de auditoría existentes a una nueva clase

En este ejemplo, se asigna un evento de auditoría existente a la nueva clase creada en el [Ejemplo 28–10](#). De manera predeterminada, el evento de auditoría `AUE_PFEXEC` se asigna a varias clases de auditoría. Mediante la creación de la nueva clase, el administrador puede auditar eventos `AUE_PFEXEC` sin auditar los eventos en las otras clases.

```
grep pf /etc/security/audit_class
0x0100000000000000:pf:profile_command
grep AUE_PFEXEC /etc/security/audit_event
116:AUE_PFEXEC:execve(2) with pfexec enabled:ps,ex,ua,as,cusa
pfedit /etc/security/audit_event
#116:AUE_PFEXEC:execve(2) with pfexec enabled:ps,ex,ua,as,cusa
116:AUE_PFEXEC:execve(2) with pfexec enabled:pf
auditconfig -setflags lo,pf
user default audit flags = pf,lo(0x0100000000001000,0x010000000001000)
```

# Configuración de registros de auditoría (tareas)

Hay dos complementos de auditoría, `audit_binfile` y `audit_syslog`, que pueden crear registros de auditoría locales. Las siguientes tareas ayudan a configurar estos registros.

## Configuración de registros de auditoría (mapa de tareas)

En el siguiente mapa de tareas, se hace referencia a los procedimientos para configurar registros de auditoría para los distintos complementos. La configuración de los registros para el complemento `audit_binfile` es opcional. Los registros para otros complementos deben ser configurados por un administrador.

| Tarea                                                                                | Descripción                                                                                               | Para obtener instrucciones                                                                              |
|--------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------|
| Agregar almacenamiento local para el complemento <code>audit_binfile</code> .        | Crea espacio en disco adicional para los archivos de auditoría y los protege con los permisos de archivo. | <a href="#">“Cómo crear sistemas de archivos ZFS para archivos de auditoría” en la página 593</a>       |
| Asignar almacenamiento para el complemento <code>audit_binfile</code> .              | Identifica directorios para registros de auditoría binarios.                                              | <a href="#">“Cómo asignar espacio de auditoría para la pista de auditoría” en la página 597</a>         |
| Configurar transmisión por secuencias de registros de auditoría a un sistema remoto. | Permite enviar registros de auditoría a un repositorio remoto por medio de un mecanismo protegido.        | <a href="#">“Cómo enviar archivos de auditoría a un repositorio remoto” en la página 600</a>            |
| Configurar almacenamiento remoto para los archivos de auditoría.                     | Le permite recibir los registros de auditoría en un sistema remoto.                                       | <a href="#">“Cómo configurar un repositorio remoto para los archivos de auditoría” en la página 601</a> |
| Configurar el almacenamiento para el complemento <code>audit_syslog</code> .         | Permite transmitir eventos de auditoría en formato de texto a <code>syslog</code> .                       | <a href="#">“Cómo configurar registros de auditoría <code>syslog</code>” en la página 605</a>           |

### ▼ Cómo crear sistemas de archivos ZFS para archivos de auditoría

El procedimiento siguiente muestra cómo crear una agrupación ZFS para los archivos de auditoría, así como los sistemas de archivos y los puntos de montaje correspondientes. De manera predeterminada, el sistema de archivos `/var/audit` contiene archivos de auditoría para el complemento `audit_binfile`.

#### Antes de empezar

Debe convertirse en un administrador al que se le ha asignado perfiles de derechos de gestión de sistemas de archivos ZFS y gestión de almacenamiento ZFS. El último perfil permite crear agrupaciones de almacenamiento. Para obtener más información, consulte [“Cómo usar los derechos administrativos que tiene asignados” en la página 164](#).

**1 Determine la cantidad de espacio en disco que sea necesaria.**

Asigne, por lo menos, 200 MB de espacio en disco por host. Sin embargo, la cantidad de auditoría que necesita es la que dicta los requisitos de espacio en disco. Por lo tanto, los requisitos de espacio en disco pueden ser mucho mayores que los que indica esta figura.

---

**Nota** – La preselección de clases predeterminada crea archivos en `/var/audit` que aumentan en 80 bytes aproximadamente por cada instancia registrada de un evento en la clase `lo`, como un inicio de sesión, un cierre de sesión o una asunción de rol.

---

**2 Cree una agrupación de almacenamiento ZFS duplicada.**

El comando `zpool create` crea una agrupación de almacenamiento, es decir, un contenedor para los sistemas de archivos ZFS. Para obtener más información, consulte el [Capítulo 1, “Sistema de archivos ZFS de Oracle Solaris \(introducción\)”](#) de *Administración de Oracle Solaris 11.1: sistemas de archivos ZFS*.

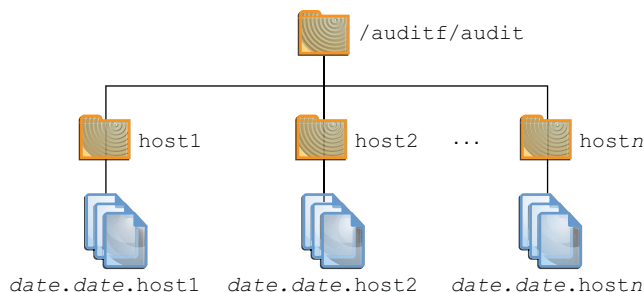
```
zpool create audit-pool mirror disk1 disk2
```

Por ejemplo, cree la agrupación `auditp` de dos discos, `c3t1d0` y `c3t2d0`, y duplíquelos.

```
zpool create auditp mirror c3t1d0 c3t2d0
```

**3 Cree un sistema de archivos ZFS y un punto de montaje para los archivos de auditoría.**

Cree el sistema de archivos y el punto de montaje con un comando. En el momento de la creación, se monta el sistema de archivos. Por ejemplo, la siguiente ilustración muestra el almacenamiento de pista de auditoría almacenado por nombre de host.




---

**Nota** – Si tiene previsto cifrar el sistema de archivos, debe cifrar el sistema de archivos en el momento de la creación. Si desea ver un ejemplo, consulte el [Ejemplo 28–12](#).

El cifrado requiere gestión. Por ejemplo, una frase de contraseña se requiere en el momento del montaje. Para obtener más información, consulte “[Cifrado de sistemas de archivos ZFS](#)” de *Administración de Oracle Solaris 11.1: sistemas de archivos ZFS*.

---

```
zfs create -o mountpoint=/mountpoint audit-pool/mountpoint
```

Por ejemplo, cree el punto de montaje `/audit` para el sistema de archivos `auditf`.

```
zfs create -o mountpoint=/audit auditp/auditf
```

#### 4 Cree un sistema de archivos ZFS para los archivos de auditoría.

```
zfs create -p auditp/auditf/system
```

Por ejemplo, cree un sistema de archivos ZFS sin cifrar para el sistema `sys1`.

```
zfs create -p auditp/auditf/sys1
```

#### 5 (Opcional) Cree sistemas de archivos adicionales para archivos de auditoría.

Un motivo para crear sistemas de archivos adicionales es evitar el desbordamiento de la auditoría. Puede establecer una cuota ZFS por sistema de archivos, como se muestra en el [Paso 8](#). El alias de correo electrónico `audit_warn` le notifica cuando se alcanza cada cuota. Para liberar espacio, puede mover los archivos de auditoría cerrados a un servidor remoto.

```
zfs create -p auditp/auditf/sys1.1
```

```
zfs create -p auditp/auditf/sys1.2
```

#### 6 Proteja el sistema de archivos de auditoría principal.

Las siguientes propiedades ZFS se establecen en `off` para todos los sistemas de archivos en la agrupación:

```
zfs set devices=off auditp/auditf
```

```
zfs set exec=off auditp/auditf
```

```
zfs set setuid=off auditp/auditf
```

#### 7 Comprima los archivos de auditoría en la agrupación.

Normalmente, la compresión está definida en ZFS, en el nivel del sistema de archivos. Sin embargo, debido a que todos los sistemas de archivos de esta agrupación contienen archivos de auditoría, la compresión se establece en el conjunto de datos de nivel superior para la agrupación.

```
zfs set compression=on auditp
```

Consulte también [“Interacciones entre propiedades de compresión, eliminación de datos duplicados y cifrado de ZFS”](#) de *Administración de Oracle Solaris 11.1: sistemas de archivos ZFS*.

**8 Defina las cuotas.**

Puede definir cuotas en el sistema de archivos principal, los sistemas de archivos descendientes o en ambos. Si define una cuota en el sistema de archivos de auditoría principal, las cuotas en los sistemas de archivos descendientes imponen un límite adicional.

**a. Defina una cuota en el sistema de archivos de auditoría principal.**

En el siguiente ejemplo, cuando ambos discos en la agrupación `auditp` alcanzan la cuota, la secuencia de comandos `audit_warn` notifica al administrador de la auditoría.

```
zfs set quota=510G auditp/auditf
```

**b. Defina una cuota en los sistemas de archivos de auditoría descendientes.**

En el siguiente ejemplo, cuando se alcanza la cuota para el sistema de archivos `auditp/auditf/sistema`, la secuencia de comandos `audit_warn` notifica al administrador de la auditoría.

```
zfs set quota=170G auditp/auditf/sys1
zfs set quota=170G auditp/auditf/sys1.1
zfs set quota=165G auditp/auditf/sys1.2
```

**9 Para una agrupación grande, limite el tamaño de los archivos de auditoría.**

De manera predeterminada, un archivo de auditoría puede crecer hasta alcanzar el tamaño de la agrupación. Para facilitar la gestión, limite el tamaño de los archivos de auditoría. Consulte el [Ejemplo 28–14](#).

**Ejemplo 28–12 Creación de un sistema de archivos cifrado para archivos de auditoría**

Para cumplir con los requisitos de seguridad del sitio, el administrador crea el sistema de archivos de auditoría con el cifrado activado. A continuación, el administrador define el punto de montaje.

```
zfs create -o encryption=on auditp/auditf
Enter passphrase for auditp/auditf': /** Type 8-character minimum passphrase**/
Enter again: /** Confirm passphrase **/
zfs set -o mountpoint=/audit auditp/auditf
```

No puede accederse al sistema de archivos sin la frase de contraseña, de modo que el administrador la guarda en una ubicación segura.

Cuando el administrador crea sistemas de archivos adicionales en el sistema de archivos `auditf`, estos sistemas de archivos descendientes también se cifran.

**Ejemplo 28–13 Configuración de una cuota en el directorio `/var/audit`**

En este ejemplo, el administrador define una cuota en el sistema de archivos de auditoría predeterminado. Cuando se alcanza esta cuota, la secuencia de comandos `audit_warn` advierte al administrador de la auditoría.



```
zfs set quota=252G rpool/var/audit
```

## ▼ Cómo asignar espacio de auditoría para la pista de auditoría

En este procedimiento, utilice atributos para el complemento `audit_binfile` con el fin de asignar espacio en disco adicional a la pista de auditoría.

### Antes de empezar

Debe convertirse en un administrador con el perfil de derechos de configuración de auditoría asignado. Para obtener más información, consulte [“Cómo usar los derechos administrativos que tiene asignados” en la página 164](#).

#### 1 Determine los atributos para el complemento `audit_binfile`.

Lea la sección OBJECT ATTRIBUTES de la página del comando `man audit_binfile(5)`.

```
man audit_binfile
```

```
...
```

```
OBJECT ATTRIBUTES
```

```
The p_dir attribute specifies where the audit files will be created.
The directories are listed in the order in which they are to be used.
```

```
The p_minfree attribute defines the percentage of free space that the
audit system requires before the audit daemon invokes the audit_warn
script.
```

```
The p_fsize attribute defines the maximum size that an audit
file can become before it is automatically closed and a new
audit file is opened. ... The format of the p_fsize value can
be specified as an exact value in bytes or in a human-readable
form with a suffix of B, K, M, G, T, P, E, Z (for bytes,
kilobytes, megabytes, gigabytes, terabytes, petabytes, exabytes,
or zettabytes, respectively). Suffixes of KB, MB, GB, TB, PB, EB,
and ZB are also accepted.
```

#### 2 Para agregar directorios a la pista de auditoría, especifique el atributo `p_dir`.

El sistema de archivos predeterminado es `/var/audit`.

```
auditconfig -setplugin audit_binfile p_dir=/audit/sys1.1,/var/audit
```

El comando anterior establece el sistema de archivos `/audit/sys1.1` como el directorio principal para archivos de auditoría y el sistema de archivos `/var/audit` como el directorio secundario. En este escenario, `/var/audit` es el directorio de último recurso. Para que esta configuración se realice correctamente, el sistema de archivos `/audit/sys1.1` debe existir.

Ha creado un sistema de archivos similar en [“Cómo crear sistemas de archivos ZFS para archivos de auditoría” en la página 593](#).

### 3 Refresque el servicio de auditoría.

El comando `auditconfig -setplugin` define el valor *configurado*. Este valor es una propiedad del servicio de auditoría, por lo que se restaura cuando el servicio se refresca o se actualiza. El valor configurado se convierte en *activo* cuando el servicio de auditoría se refresca o se actualiza. Para obtener información sobre valores activos y configurados, consulte la página del comando `man auditconfig(1M)`.

```
audit -s
```

#### Ejemplo 28-14 Limitación de tamaño de archivo para el complemento `audit_binfile`

En el siguiente ejemplo, el tamaño de un archivo de auditoría binario está establecido en un tamaño específico. El tamaño está especificado en megabytes.

```
auditconfig -setplugin audit_binfile p_fsize=4M
auditconfig -getplugin audit_binfile
Plugin: audit_binfile
Attributes: p_dir=/var/audit;p_fsize=4M;p_minfree=1;
```

De manera predeterminada, un archivo de auditoría puede crecer sin límite. Para crear archivos de auditoría más pequeños, el administrador especifica un límite de tamaño de archivo de 4 MB. El servicio de auditoría crea un nuevo archivo cuando se alcanza el límite de tamaño. El límite de tamaño de archivo entra en vigor después de que el administrador refresca el servicio de auditoría.

```
audit -s
```

#### Ejemplo 28-15 Especificación de varios cambios para un complemento de auditoría

En el siguiente ejemplo, el administrador en un sistema con un alto rendimiento y una agrupación ZFS grande cambia el tamaño de la cola, el tamaño del archivo binario y la advertencia del límite dinámico para el complemento `audit_binfile`. El administrador permite que los archivos de auditoría crezcan a 4 GB, es advertido cuando queda un 2% de la agrupación ZFS y duplica el tamaño de la cola permitido. El tamaño predeterminado de la cola es la marca de agua superior para la cola de la auditoría del núcleo, 100, como en `active audit queue hiwater mark (records) = 100`.

```
auditconfig -getplugin audit_binfile
Plugin: audit_binfile
Attributes: p_dir=/var/audit;p_fsize=2G;p_minfree=1;
auditconfig -setplugin audit_binfile "p_minfree=2;p_fsize=4G" 200
auditconfig -getplugin audit_binfile
Plugin: audit_binfile
Attributes: p_dir=/var/audit;p_fsize=4G;p_minfree=2;
Queue size: 200
```

Las especificaciones cambiadas entran en vigor después de que el administrador refresca el servicio de auditoría.

```
audit -s
```

**Ejemplo 28-16** Eliminación del tamaño de la cola de un complemento de auditoría

En el siguiente ejemplo, se elimina el tamaño de la cola para el complemento `audit_binfile`.

```
auditconfig -getplugin audit_binfile
Plugin: audit_binfile
 Attributes: p_dir=/var/audit;p_fsize=4G;p_minfree=2;
 Queue size: 200
auditconfig -setplugin audit_binfile "" 0
auditconfig -getplugin audit_binfile
Plugin: audit_binfile
 Attributes: p_dir=/var/audit;p_fsize=4G;p_minfree=2;
```

Las comillas vacías ("" ) conservan los valores de atributo actuales. Un `0` al final, establece el tamaño de la cola para el complemento en el valor predeterminado.

El cambio en la especificación `qsize` para el complemento entra en vigor después de que el administrador refresca el servicio de auditoría.

```
audit -s
```

**Ejemplo 28-17** Definición de un límite dinámico para advertencias

En este ejemplo, está configurado el nivel mínimo de espacio libre para todos los sistemas de archivos de auditoría, de modo que se emite una advertencia cuando aún queda disponible el 2 % del sistema de archivos.

```
auditconfig -setplugin audit_binfile p_minfree=2
```

El porcentaje predeterminado es uno (1). Para una agrupación ZFS grande, seleccione un porcentaje razonablemente bajo. Por ejemplo, el 10 % de 16 TB es aproximadamente 16 GB, lo que advertiría al administrador de la auditoría cuando queda bastante espacio en disco. Un valor de 2 envía el mensaje `audit_warn` cuando quedan aproximadamente 2 GB de espacio en disco.

El alias de correo electrónico `audit_warn` recibe la advertencia. Para configurar el alias, consulte [“Cómo configurar el alias de correo electrónico `audit\_warn`” en la página 589](#).

Para una agrupación grande, el administrador también limita el tamaño del archivo a 3 GB.

```
auditconfig -setplugin audit_binfile p_fsize=3G
```

Las especificaciones `p_minfree` y `p_fsize` para el complemento entran en vigor después de que el administrador refresca el servicio de auditoría.

```
audit -s
```

## ▼ Cómo enviar archivos de auditoría a un repositorio remoto

En este procedimiento, se utilizan atributos para el complemento `audit_remote` para enviar la pista de auditoría a un repositorio de auditoría remoto. Para configurar un repositorio remoto en un sistema Oracle Solaris, consulte [“Cómo configurar un repositorio remoto para los archivos de auditoría” en la página 601](#).

### Antes de empezar

Debe tener un receptor de archivos de auditoría en el repositorio remoto. Debe convertirse en un administrador con el perfil de derechos de configuración de auditoría asignado. Para obtener más información, consulte [“Cómo usar los derechos administrativos que tiene asignados” en la página 164](#).

#### 1 Determine los atributos para el complemento `audit_remote`.

Lea la sección OBJECT ATTRIBUTES de la página del comando `man audit_remote(5)`.

```
man audit_remote
...
OBJECT ATTRIBUTES
 The p_hosts attribute specifies the remote servers.
 You can also specify the port number and the GSS-API
 mechanism.

 The p_retries attribute specifies the number of retries for
 connecting and sending data. The default is 3.

 The p_timeout attribute specifies the number of seconds
 in which a connection times out.
```

El puerto predeterminado es el puerto asignado por IANA `solaris_audit`, 16162/tcp. El mecanismo predeterminado es `kerberos_v5`. El tiempo de espera predeterminado es de 5 s. También puede especificar un tamaño de cola para el complemento.

#### 2 Para especificar el sistema receptor remoto, utilice el atributo `p_hosts`.

En este ejemplo, el sistema receptor utiliza un puerto diferente.

```
auditconfig -setplugin audit_remote p_hosts=ars.example.com:16088:kerberos_v5
```

#### 3 Para cambiar otros atributos del complemento, especifíquelos.

Por ejemplo, el siguiente comando especifica valores para todos los atributos opcionales:

```
auditconfig -setplugin audit_remote "p_retries=;p_timeout=3" 300
```

#### 4 Verifique los valores y, a continuación, active el complemento.

Por ejemplo, los siguientes comandos especifican y verifican los valores del complemento:

```
auditconfig -getplugin audit_remote
Plugin: audit_remote (inactive)
 Attributes: p_hosts=ars.example.com:16088:kerberos_v5;p_retries=5;p_timeout=3;
 Queue size: 300
auditconfig -setplugin audit_remote active
```

## 5 Refresque el servicio de auditoría.

El servicio de auditoría lee el cambio de complemento de auditoría después del refrescamiento.

```
audit -s
```

### Ejemplo 28–18 Ajuste del tamaño de búfer de cola de auditoría

En este ejemplo, la cola de auditoría está llena detrás del complemento `audit_remote`. Este sistema auditado está configurado para auditar muchas clases y transmite a través de una red lenta, con mucho tráfico. El administrador aumenta el tamaño del búfer del complemento para permitir que la cola de auditoría crezca y no exceda el límite del búfer antes que los registros se eliminen de la cola.

```
audsys1 # auditconfig -setplugin audit_remote "" 1000
audsys1 # audit -s
```

## ▼ Cómo configurar un repositorio remoto para los archivos de auditoría

En este proceso, puede configurar un sistema remoto, el servidor de auditoría remoto (ARS), para recibir y almacenar los registros de auditoría de uno o más sistemas auditados. A continuación, debe activar el daemon de auditoría en el servidor remoto.

La configuración es doble. En primer lugar, configure los mecanismos de seguridad subyacentes para transportar de modo seguro los datos de auditoría, es decir, configure el KDC. En segundo lugar, se debe configurar el servicio de auditoría en el sistema auditado y el ARS. En este procedimiento, se ilustra un caso con un cliente auditado y un ARS, en el que el ARS y el KDC están en el mismo servidor. Del mismo modo, se pueden configurar escenarios más complejos.

### Antes de empezar

Debe asumir el rol `root`. Ha instalado los paquetes Kerberos, como se describe en [“Cómo prepararse para transmitir los registros de auditoría al almacenamiento remoto” en la página 569](#). Trabaja con un administrador que tiene configurado el sistema auditado, como se describe en [“Cómo enviar archivos de auditoría a un repositorio remoto” en la página 600](#).

## 1 Configure el mecanismo de transporte de seguridad subyacente.

Necesita un KDC en un sistema que tanto el sistema auditado y el ARS pueden utilizar, un principal de host para cada sistema y un principal de servicio `audit`.

### a. Configure el KDC.

Si su sitio tiene configurado un KDC, utilícelo y continúe con el [Paso c](#). La siguiente serie de comandos ilustra una estrategia de configuración de KDC:

```
arstore # kdcmgr -a audr/admin -r EXAMPLE.COM create master
```

Este comando usa el principal administrativo `audr/admin` para crear un KDC maestro en el dominio `EXAMPLE.COM`, activa el KDC maestro e inicia el servicio Kerberos.

#### b. Verifique que el KDC esté disponible.

Para obtener más información, consulte la página del comando `man kdcmgr(1M)`.

```
kdcmgr status
KDC Status Information

svc:/network/security/krb5kdc:default (Kerberos key distribution center)
 State: online since Wed Feb 29 01:59:27 2012
 See: man -M /usr/share/man -s 1M krb5kdc
 See: /var/svc/log/network-security-krb5kdc:default.log
 Impact: None.

KDC Master Status Information

svc:/network/security/kadmin:default (Kerberos administration daemon)
 State: online since Wed Feb 29 01:59:28 2012
 See: man -M /usr/share/man -s 1M kadmind
 See: /var/svc/log/network-security-kadmin:default.log
 Impact: None.

Transaction Log Information

Kerberos update log (/var/krb5/principal.ulong)
Update log dump :
 Log version # : 1
 Log state : Stable
 Entry block size : 2048
 Number of entries : 13
 First serial # : 1
 Last serial # : 13
 First time stamp : Wed Feb 29 01:59:27 2012
 Last time stamp : Mon Mar 5 19:29:28 2012

Kerberos Related File Information

(Displays any missing files)
```

#### c. Agregue el principal del servicio `audit` al archivo `keytab` de KDC.

Puede agregar el principal escribiendo el comando `kadmin.local` en el sistema KDC. O bien, puede agregar de forma remota el principal mediante el comando `kadmin` y una contraseña. En este ejemplo, el sistema `arstore` está ejecutando el KDC.

```
kadmin -p audr/admin
kadmin: addprinc -randkey audit/arstore.example.com@EXAMPLE.COM
kadmin: ktadd audit/arstore.example.com@EXAMPLE.COM
```

#### d. En cada sistema auditado, agregue claves.

El destinatario y el remitente deben tener claves.

```
enigma # kclient
.. Enter the Kerberos realm: EXAMPLE.COM
```

```
.. KDC hostname for the above realm: arstore.example.com
.. Will this client need service keys ? [y/n]: y
```

## 2 Configure el servicio de auditoría en el ARS.

- Para crear un grupo que acepta los registros de auditoría de cualquier sistema auditado en el dominio Kerberos, asigne un nombre a un grupo de conexión.

```
auditconfig -setremote group create Bank_A
```

Bank\_A es un grupo de conexión. Como el atributo `hosts` no está definido, este grupo acepta todas las conexiones, lo que significa que es un grupo *wildcard*. Cualquier sistema auditado en este dominio Kerberos cuyo complemento `audit_remote` esté correctamente configurado puede alcanzar este ARS.

- Para limitar las conexiones a este grupo, especifique los sistemas auditados que pueden utilizar este repositorio.

```
auditconfig -setremote group Bank_A "hosts=enigma.example.com"
```

El grupo de conexión Bank\_A ahora sólo acepta conexiones del sistema enigma. Una conexión de cualquier otro host se rechaza.

- Para evitar que un archivo de auditoría en este grupo sea demasiado grande, establezca un tamaño máximo.

```
auditconfig -setremote group Bank_A "binfile_size=4GB"
auditconfig -getremote
Audit Remote Server
Attributes: listen_address=;login_grace_time=30;max_startups=10;listen_port=0;
Connection group: Bank_A (inactive)
Attributes: binfile_dir=/var/audit;binfile_fsize=4GB;binfile_minfree=1;
hosts=enigma.example.com;
```

## 3 Configure el servicio de auditoría en el sistema auditado.

Para especificar el ARS, utilice el atributo `p_hosts`.

```
enigma # auditconfig -setplugin audit_remote active p_hosts=arstore.example.com
enigma # auditconfig -getplugin audit_remote
Plugin: audit_remote
Attributes: p_retries=3;p_timeout=5;p_hosts=arstore.example.com;
```

## 4 Refresque el servicio de auditoría.

El servicio de auditoría lee el cambio de complemento de auditoría después del refrescamiento.

```
audit -s
```

El KDC ahora gestiona la conexión entre el sistema auditado enigma y el ARS.

**Ejemplo 28–19** Transmisión por secuencias de registros de auditoría a diferentes ubicaciones de archivos en el mismo ARS

En este ejemplo, se amplía el ejemplo en el procedimiento. El administrador separa los registros de auditoría por host en el ARS mediante la creación de dos grupos de conexión.

Los archivos de auditoría de la transmisión audsys1 al grupo de conexiones Bank\_A en este ARS.

```
arstore # auditconfig -setremote group create Bank_A
arstore # auditconfig -setremote group active Bank_A "hosts=audsys1"
 "hosts=audsys1;binfile_dir=/var/audit/audsys1;binfile_fsize=4M;"
```

Los archivos de auditoría de audsys2 se transmiten al grupo de conexión Bank\_B.

```
arstore # auditconfig -setremote group create Bank_B
arstore # auditconfig -setremote group active Bank_B \
 "hosts=audsys2;binfile_dir=/var/audit/audsys2;binfile_fsize=4M;"
```

Para facilitar las tareas de mantenimiento, el administrador establece otros valores de atributo de la misma forma.

```
arstore # auditconfig -getremote
Audit Remote Server
 Attributes: listen_address=;login_grace_time=30;max_startups=10;listen_port=0;

Connection group: Bank_A
 Attributes: binfile_dir=/var/audit/audsys1;binfile_fsize=4M;binfile_minfree=1;
 hosts=audsys1

Connection group: Bank_B
 Attributes: binfile_dir=/var/audit/audsys2;binfile_fsize=4M;binfile_minfree=1;
 hosts=audsys2
```

**Ejemplo 28–20** Colocación del ARS en un sistema diferente de KDC

En este ejemplo, el administrador coloca el ARS en un sistema diferente del KDC. En primer lugar, el administrador crea y configura el KDC maestro.

```
kserve # kdcmgr -a audr/admin -r EXAMPLE.COM create master
kserve # kadmin.local -p audr/admin
kadmin: addprinc -randkey audit/arstore.example.com@EXAMPLE.COM
kadmin: ktadd -t /tmp/krb5.keytab.audit audit/arstore.example.com@EXAMPLE.COM
```

Después de transmitir de manera segura el archivo /tmp/krb5.keytab.audit al ARS, arstore, el administrador mueve el archivo a la ubicación correcta.

```
arstore # chown root:root krb5.keytab.audit
arstore # chmod 600 krb5.keytab.audit
arstore # mv krb5.keytab.audit /etc/krb5/krb5.keytab
```



En lugar de volver a escribir el archivo, el administrador también tiene la opción de utilizar el comando `ktutil` en el ARS para fusionar el archivo `krb5.keytab.audit` del KDC con las claves existentes en el archivo `/etc/krb5/krb5.keytab` de `arstore`.

Por último, el administrador genera claves en el sistema auditado.

```
enigma # kclient
.. Enter the Kerberos realm: EXAMPLE.COM
.. KDC hostname for the above realm: kserv.example.com
.. Will this client need service keys ? [y/n]: y
```

## ▼ Cómo configurar registros de auditoría `syslog`

Puede indicar al servicio de auditoría que copie algunos o todos los registros de auditoría de la cola de auditoría en la utilidad `syslog`. Si registra datos de auditoría binarios y resúmenes de textos, los datos binarios proporcionan un registro completo de auditoría, mientras que los resúmenes filtran los datos para la revisión en tiempo real.

### Antes de empezar

Para configurar el complemento `audit_syslog`, debe convertirse en un administrador con el perfil de derechos de configuración de auditoría asignado. Para configurar la utilidad `syslog` y crear el archivo `auditlog`, debe asumir el rol `root`.

- 1 **Seleccione las clases de auditoría que se enviarán al complemento `audit_syslog` y active el complemento.**

---

**Nota** – Las clases de auditoría `p_flags` deben ser preseleccionadas como valores predeterminados del sistema o en los indicadores de auditoría de un usuario o de un perfil de derechos. Los registros no se recopilan para una clase que no está preseleccionada.

---

```
auditconfig -setplugin audit_syslog active p_flags=lo,+as,-ss
```

- 2 **Determine qué instancia del servicio `system-log` está en línea.**

```
svcs system-log
STATE STIME FMRI
disabled 13:11:55 svc:/system/system-log:rsyslog
online 13:13:27 svc:/system/system-log:default
```

---

**Nota** – Si la instancia de servicio `rsyslog` está en línea, modifique el archivo `rsyslog.conf`.

---

**3 Configure la utilidad syslog.****a. Agregue una entrada audit.notice al archivo syslog.conf.**

La entrada incluye la ubicación del archivo de registro.

```
cat /etc/syslog.conf
...
audit.notice /var/adm/auditlog
```

**b. Cree el archivo de registro.**

```
touch /var/adm/auditlog
```

**c. Refresque la información de configuración del servicio system-log.**

```
svcadm refresh system-log:default
```

---

**Nota** – Refresque la instancia de servicio system-log:rsyslog si el servicio rsyslog está en línea.

---

**4 Refresque el servicio de auditoría.**

El servicio de auditoría lee los cambios en el complemento de auditoría tras el refrescamiento.

```
audit -s
```

**5 Archive con regularidad los archivos de registro syslog.**

El servicio de auditoría puede generar muchas salidas. Para gestionar los registros, consulte la página del comando man [logadm\(1M\)](#).

**Ejemplo 28–21 Especificación de clases de auditoría para salida de syslog**

En el siguiente ejemplo, la utilidad syslog recopila un subconjunto de clases de auditoría preseleccionadas. La clase pf se crea en el [Ejemplo 28–10](#).

```
auditconfig -setnaflags lo,na
auditconfig -setflags lo,ss
usermod -K audit_flags=pf:no jdoe
auditconfig -setplugin audit_syslog active p_flags=lo,+na,-ss,+pf
```

Los argumentos del comando auditconfig indican al sistema que recopile todos los registros de auditoría de inicio y cierre de sesión, no atribuibles y de cambio de estado del sistema. La entrada del complemento audit\_syslog indica a la utilidad syslog que recopile todos los inicios de sesión, los eventos no atribuibles con éxito y los cambios de estado del sistema con fallos.

Para el usuario jdoe, la utilidad binaria recopila llamadas correctas e incorrectas para el comando pfexec. La utilidad syslog recopila llamadas correctas para el comando pfexec.

**Ejemplo 28–22 Colocación de registros de auditoría `syslog` en un sistema remoto**

Puede cambiar la entrada `audit.notice` en el archivo `syslog.conf` para que haga referencia a un sistema remoto. En este ejemplo, el nombre del sistema local es `sys1.1`. El sistema remoto es `remote1`.

```
sys1.1 # cat /etc/syslog.conf
...
audit.notice @remote1
```

La entrada `audit.notice` en el archivo `syslog.conf` del sistema `remote1` hace referencia al archivo de registro.

```
remote1 # cat /etc/syslog.conf
...
audit.notice /var/adm/auditlog
```

## Configuración del servicio de auditoría en las zonas (tareas)

El servicio de auditoría audita todo el sistema, incluidos los eventos de auditoría en las zonas. Un sistema que tenga zonas no globales instaladas puede auditar todas las zonas de forma idéntica o puede configurar la auditoría por zona. Para obtener más información, consulte [“Cómo planificar auditoría en zonas” en la página 564](#).

Quando se auditan las zonas no globales exactamente como se audita la zona global, los administradores de la zona no global pueden no tener acceso a los registros de auditoría. Además, el administrador de la zona global puede modificar las máscaras de preselección de auditoría de los usuarios en las zonas no globales.

Quando se auditan las zonas no globales de forma individual, los registros de auditoría están visibles para la zona no global y para la zona global desde el directorio raíz de zonas no globales.

### ▼ **Cómo configurar todas las zonas de forma idéntica para la auditoría**

Este procedimiento activa las auditorías de cada zona de forma idéntica. Este método requiere la menor sobrecarga del equipo y la menor cantidad de recursos administrativos.

**Antes de empezar**

Debe asumir el rol `root`. Para obtener más información, consulte [“Cómo usar los derechos administrativos que tiene asignados” en la página 164](#).

- 1 **Configure la zona global para la auditoría.**

Complete las tareas en “[Configuración del servicio de auditoría \(mapa de tareas\)](#)” en la [página 578](#), con las siguientes excepciones:

- No active la política de auditoría perzone.
- Establezca la política zonename. Esta política agrega el nombre de la zona a cada registro de auditoría.

```
auditconfig -setpolicy +zonename
```

## 2 Si modifica archivos de configuración de auditoría, cópielos de la zona global a cada zona no global.

Si modifica el archivo `audit_class` o `audit_event`, cópielo de una de estas dos formas:

- Puede montar en bucle de retorno los archivos.
- Puede copiar los archivos.

La zona no global debe estar en ejecución.

- Monte los archivos `audit_class` y `audit_event` cambiados como un sistema de archivos de bucle de retorno (`lofs`).

### a. Desde la zona global, detenga la zona no global.

```
zoneadm -z non-global-zone halt
```

### b. Cree un montaje en bucle de retorno de sólo lectura para cada archivo de configuración de auditoría que haya modificado en la zona global.

```
zonecfg -z non-global-zone
add fs
 set special=/etc/security/audit-file
 set dir=/etc/security/audit-file
 set type=lofs
 add options [ro,nodevices,nosetuid]
 commit
end
exit
```

### c. Para que los cambios entren en vigencia, inicie la zona no global.

```
zoneadm -z non-global-zone boot
```

Más adelante, si modifica un archivo de configuración de auditoría en la zona global, debe reiniciar cada zona para refrescar los archivos montados en bucle de retorno en las zonas no globales.

- Copie los archivos.

### a. Desde la zona global, muestre el directorio `/etc/security` en cada zona no global.

```
ls /zone/zonename/root/etc/security/
```

**b. Copie los archivos `audit_class` y `audit_event` cambiados en el directorio `/etc/security` de cada zona.**

```
cp /etc/security/audit-file /zone/zonename/root/etc/security/audit-file
```

Más adelante, si cambia uno de estos archivos en la zona global, debe copiar el archivo cambiado a las zonas no globales.

Las zonas no globales se auditan cuando se reinicia el servicio de auditoría en la zona global o cuando las zonas se reinician.

### **Ejemplo 28–23 Montaje de archivos de configuración de auditoría como montajes de bucle de retorno en una zona**

En este ejemplo, el administrador del sistema ha modificado los archivos `audit_class`, `audit_event` y `audit_warn`.

El archivo `audit_warn` solamente se lee en la zona global, por lo que no se tiene que montar en las zonas no globales.

En este sistema, `machine1`, el administrador ha creado dos zonas no globales, `machine1-webserver` y `machine1-appserver`. El administrador ha terminado de modificar los archivos de configuración de auditoría. Si el administrador más tarde modifica los archivos, la zona se debe reiniciar para volver a leer los montajes de bucle de retorno.

```
zoneadm -z machine1-webserver halt
zoneadm -z machine1-appserver halt
zonecfg -z machine1-webserver
add fs
 set special=/etc/security/audit_class
 set dir=/etc/security/audit_class
 set type=lofs
 add options [ro,nodevices,nosetuid]
 commit
end
add fs
 set special=/etc/security/audit_event
 set dir=/etc/security/audit_event
 set type=lofs
 add options [ro,nodevices,nosetuid]
 commit
end
exit
zonecfg -z machine1-appserver
add fs
 set special=/etc/security/audit_class
 set dir=/etc/security/audit_class
 set type=lofs
 add options [ro,nodevices,nosetuid]
 commit
end
...
exit
```

Cuando las zonas no globales se reinician, los archivos `audit_class` y `audit_event` son de sólo lectura en las zonas.

## ▼ Cómo configurar la auditoría por zona

Este procedimiento permite que distintos administradores de zonas controlen el servicio de auditoría en sus zonas. Para obtener una lista completa de las opciones de política, consulte la página del comando `man auditconfig(1M)`.

### Antes de empezar

Para configurar la auditoría, debe convertirse en administrador con el perfil de derechos de configuración de auditoría asignado. Para activar el servicio de auditoría, debe convertirse en un administrador con el perfil de derechos de control de auditoría asignado. Para obtener más información, consulte “Cómo usar los derechos administrativos que tiene asignados” en la página 164.

- 1 En la zona global, configure la auditoría.
  - a. Complete las tareas en “Configuración del servicio de auditoría (mapa de tareas)” en la página 578.
  - b. Agregue la política de auditoría `perzone`. Para el comando, consulte el Ejemplo 28–8.

---

**Nota** – No es necesario activar el servicio de auditoría en la zona global.

---

- 2 En cada zona no global que planea auditar, configure los archivos de auditoría.
  - a. Complete las tareas en “Configuración del servicio de auditoría (mapa de tareas)” en la página 578.
  - b. No configure los valores de auditoría en todo el sistema.  
Específicamente, no agregue la política `perzone` o añada al archivo a la zona no global.

- 3 Active la auditoría en su zona.

```
myzone# audit -s
```

### Ejemplo 28–24 Desactivación de la auditoría en una zona no global

Este ejemplo funciona si está establecida la política de auditoría `perzone`. El administrador de zonas de la zona `noaudit` desactiva la auditoría para dicha zona.

```
noauditzone # auditconfig -getcond
audit condition = auditing
```

```
noauditzone # audit -t
noauditzone # auditconfig -getcond
audit condition = noaudit
```

## Activación y desactivación del servicio de auditoría (tareas)

El servicio de auditoría está activado de manera predeterminada. Si la política de auditoría perzone se configura en la zona global, los administradores de zonas pueden activar, refrescar y desactivar el servicio de auditoría en sus zonas no globales.

### ▼ Cómo refrescar el servicio de auditoría

Este procedimiento actualiza el servicio de auditoría cuando se haya cambiado la configuración de un complemento de auditoría después de activar el servicio de auditoría.

#### Antes de empezar

Debe convertirse en un administrador con el perfil de derechos de control de auditoría asignado. Para obtener más información, consulte [“Cómo usar los derechos administrativos que tiene asignados” en la página 164](#).

#### 1 Refresque el servicio de auditoría.

```
audit -s
```

---

**Nota** – Al refrescar el servicio de auditoría, toda la configuración temporal se pierde. La política de auditoría y los controles de colas permiten valores temporales. Para obtener más información, consulte la página del comando `man auditconfig(1M)`.

---

#### 2 Actualice las máscaras de preselección de los usuarios que se están auditando en ese momento.

Refrescar el servicio de auditoría *no* cambia las máscaras de procesos existentes. Para restablecer explícitamente la máscara de preselección de un proceso existente, consulte [“Cómo actualizar la máscara de preselección de usuarios con sesión iniciada” en la página 634](#).

### Ejemplo 28–25 Refrescamiento de un servicio de auditoría activado

En este ejemplo, el administrador reconfigura la auditoría, verifica los cambios y luego refresca el servicio de auditoría.

- En primer lugar, el administrador agrega una política temporal.

```
auditconfig -t -setpolicy +zonename
auditconfig -getpolicy
configured audit policies = ahlt,arge,argv,perzone
active audit policies = ahlt,arge,argv,perzone,zonename
```

- A continuación, el administrador especifica controles de colas.

```
auditconfig -setqctrl 200 20 0 0
auditconfig -getqctrl
configured audit queue hiwater mark (records) = 200
configured audit queue lowater mark (records) = 20
configured audit queue buffer size (bytes) = 8192
configured audit queue delay (ticks) = 20
active audit queue hiwater mark (records) = 200
active audit queue lowater mark (records) = 20
active audit queue buffer size (bytes) = 8192
active audit queue delay (ticks) = 20
```

- A continuación, el administrador especifica atributos de complementos.
  - Para el complemento `audit_binfile`, el administrador elimina el valor `qsize`.

```
auditconfig -getplugin audit_binfile
Plugin: audit_binfile
 Attributes: p_dir=/audit/sys1.1,/var/audit;
 p_minfree=2;p_fsize=4G;
Queue size: 200
auditconfig -setplugin audit_binfile "" 0
auditconfig -getplugin audit_binfile
Plugin: audit_binfile
 Attributes: p_dir=/audit/sys1.1,/var/audit
 p_minfree=2;p_fsize=4G;
```

- Para el complemento `audit_syslog`, el administrador especifica que los eventos de inicio y cierre de sesión con éxito y los archivos ejecutables con fallos se envíen a `syslog`. `qsize` para este complemento se define en 150.

```
auditconfig -setplugin audit_syslog active p_flags=+lo,-ex 150
auditconfig -getplugin audit_syslog
auditconfig -getplugin audit_syslog
Plugin: audit_syslog
 Attributes: p_flags=+lo,-ex;
Queue size: 150
```

- El administrador no configura ni usa el complemento `audit_remote`.
- Luego, el administrador refresca el servicio de auditoría y verifica la configuración.
  - La política `zonename` temporal ya no está definida.

```
audit -s
auditconfig -getpolicy
configured audit policies = ahlt,arge,argv,perzone
active audit policies = ahlt,arge,argv,perzone
```

- Los controles de colas permanecen igual.

```
auditconfig -getqctrl
configured audit queue hiwater mark (records) = 200
configured audit queue lowater mark (records) = 20
configured audit queue buffer size (bytes) = 8192
configured audit queue delay (ticks) = 20
active audit queue hiwater mark (records) = 200
active audit queue lowater mark (records) = 20
active audit queue buffer size (bytes) = 8192
active audit queue delay (ticks) = 20
```

- El complemento `audit_binfile` no tiene un tamaño de cola especificado. El complemento `audit_syslog` tiene un tamaño de cola especificado.



```
auditconfig -getplugin
Plugin: audit_binfile
 Attributes: p_dir=/var/audit;p_fsize=4G;p_minfree=2;

Plugin: audit_syslog
 Attributes: p_flags=+lo,-ex;
 Queue size: 50
...
```

## ▼ Cómo desactivar el servicio de auditoría

Este procedimiento muestra cómo desactivar la auditoría en la zona global y en una zona no global cuando se configura la política de auditoría perzone. Después de que la política perzone esté definida en la zona global, una zona no global que haya activado la auditoría sigue recopilando registros de auditoría en los reinicios de la zona global y de la zona no global.

### Antes de empezar

Para activar o desactivar el servicio de auditoría, debe convertirse en administrador con el perfil de derechos de control de auditoría asignado. Para obtener más información, consulte [“Cómo usar los derechos administrativos que tiene asignados”](#) en la página 164.

### ● Ejecute el comando `audit -t` para desactivar el servicio de auditoría.

Para obtener más información, consulte las páginas del comando `man audit(1M)` y `auditd(1M)`.

#### ■ En la zona global, desactive el servicio de auditoría.

```
audit -t
```

Si la política de auditoría perzone no está definida, este comando desactiva la auditoría en todas las zonas. Si está establecida la política de auditoría perzone, las zonas no globales no se ven afectadas.

#### ■ En una zona no global, desactive el servicio de auditoría.

Si la política de auditoría perzone está definida, el administrador de zonas no globales debe desactivar el servicio en la zona no global.

```
zone1 # audit -t
```

## ▼ Cómo activar el servicio de auditoría

Este procedimiento activa el servicio de auditoría para todas las zonas después de que un administrador desactiva el servicio. Para iniciar el servicio de auditoría en una zona no global, consulte el [Ejemplo 28–26](#).

### Antes de empezar

Para activar o desactivar el servicio de auditoría, debe convertirse en administrador con el perfil de derechos de control de auditoría asignado. Para obtener más información, consulte [“Cómo usar los derechos administrativos que tiene asignados”](#) en la página 164.

1 Use el comando `audit -s` para activar el servicio de auditoría.

```
audit -s
```

Para obtener más información, consulte la página del comando `man audit(1M)`.

2 Verifique que la auditoría esté activada.

```
auditconfig -getcond
audit condition = auditing
```

**Ejemplo 28–26** Activación de la auditoría en una zona no global

En este ejemplo, el administrador de zonas activa el servicio de auditoría para `zone1` después de realizar las siguientes acciones:

- El administrador de zonas globales establece la política `perzone` en la zona global.
- El administrador de zonas de la zona no global configura el servicio de auditoría y las personalizaciones por usuario.

A continuación, el administrador de zonas activa el servicio de auditoría para la zona.

```
zone1# audit -s
```

# Gestión de registros de auditoría en sistemas locales (tareas)

El complemento predeterminado, `audit_binfile`, crea una pista de auditoría. La pista puede contener grandes cantidades de datos. Las siguientes tareas muestran cómo trabajar con todos estos datos.

## Gestión de registros de auditoría en sistemas locales (mapa de tareas)

El siguiente mapa de tareas hace referencia a los procedimientos para seleccionar, analizar y gestionar los registros de auditoría.

| Tarea                                               | Descripción                                                                                                              | Para obtener instrucciones                                                        |
|-----------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------|
| Mostrar los formatos de los registros de auditoría. | Muestra el tipo de información que se recopila para un evento de auditoría y el orden en que se presenta la información. | “Cómo visualizar definiciones de registros de auditoría” en la página 615         |
| Fusionar registros de auditoría.                    | Combina los archivos de auditoría de varias máquinas en una pista de auditoría.                                          | “Cómo fusionar archivos de auditoría de la pista de auditoría” en la página 616   |
| Seleccionar los registros para examinar.            | Selecciona eventos determinados de estudio.                                                                              | “Cómo seleccionar eventos de auditoría de la pista de auditoría” en la página 618 |

| Tarea                                                      | Descripción                                                                                                                                     | Para obtener instrucciones                                                                            |
|------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------|
| Mostrar registros de auditoría.                            | Permite la visualización de registros de auditoría binarios.                                                                                    | <a href="#">“Cómo visualizar el contenido de los archivos de auditoría binarios” en la página 620</a> |
| Depurar archivos de auditoría denominados incorrectamente. | Proporciona una indicación de hora final para auditar archivos de auditoría que quedaron abiertos inadvertidamente en el servicio de auditoría. | <a href="#">“Cómo depurar un archivo de auditoría not_terminated” en la página 622</a>                |
| Evitar el desbordamiento de la pista de auditoría.         | Impide que los sistemas de archivos de auditoría se llenen.                                                                                     | <a href="#">“Cómo evitar el desbordamiento de la pista de auditoría” en la página 623</a>             |

## ▼ Cómo visualizar definiciones de registros de auditoría

El comando `audit record` muestra definiciones de registros de auditoría. Las definiciones indican el número de evento de auditoría, la clase de auditoría, la máscara de selección y el formato de registro de un evento de auditoría.

- **Coloque las definiciones de todos los registros de eventos de auditoría en un archivo HTML.**

La opción `-a` muestra una lista de todas las definiciones de eventos de auditoría. La opción `-h` coloca la lista en formato HTML.

```
% auditrecord -ah > audit.events.html
```

---

**Consejo** – Cuando visualiza el archivo HTML en un explorador, use la herramienta de búsqueda del explorador para buscar definiciones de registros de auditoría específicas.

---

Para obtener más información, consulte la página del comando `man auditrecord(1M)`.

### Ejemplo 28–27 Visualización de las definiciones de registros de auditoría de un programa

En este ejemplo, se muestra la definición de todos los registros de auditoría que se generan mediante el programa `login`. Los programas de inicio de sesión incluyen `rlogin`, `telnet`, `newgrp` y la función de Secure Shell de Oracle Solaris.

```
% auditrecord -p login
...
login: logout
 program various See login(1)
 event ID 6153 AUE_logout
 class lo (0x0000000000001000)
...
newgrp
 program newgrp See newgrp login
 event ID 6212 AUE_newgrp_login
 class lo (0x0000000000001000)
...
```

```
rlogin
 program /usr/sbin/login See login(1) - rlogin
 event ID 6155 AUE_rlogin
 class lo (0x0000000000001000)
...
/usr/lib/ssh/sshd
 program /usr/lib/ssh/sshd See login - ssh
 event ID 6172 AUE_ssh
 class lo (0x0000000000001000)
...
telnet login
 program /usr/sbin/login See login(1) - telnet
 event ID 6154 AUE_telnet
 class lo (0x0000000000001000)
...
```

**Ejemplo 28–28** Visualización de definiciones de registros de auditoría de una clase de auditoría

En este ejemplo, se muestran las definiciones de todos los registros de auditoría en la clase pf que fue creada en el [Ejemplo 28–10](#).

```
% auditrecord -c pf

pfexec
 system call pfexec See execve(2) with pfexec enabled
 event ID 116 AUE_PFEXEC
 class pf (0x0100000000000000)
 header
 path pathname of the executable
 path pathname of working directory
 [privileges] privileges if the limit or inheritable set are changed
 [privileges] privileges if the limit or inheritable set are changed
 [process] process if ruid, euid, rgid or egid is changed
 exec_arguments
 [exec_environment] output if arge policy is set
 subject
 [use_of_privilege]
 return
```

El token use\_of\_privilege se registra siempre que se utiliza un privilegio. Los tokens privileges se registran si el conjunto heredable o límite se cambia. El token process se registra si un ID se cambia. Ninguna opción de política es necesaria para que estos tokens se incluyan en el registro.

▼ **Cómo fusionar archivos de auditoría de la pista de auditoría**

Mediante la fusión de los archivos de auditoría de todos los directorios de auditoría, puede analizar el contenido de toda la pista de auditoría.

---

**Nota** – Debido a que las indicaciones de hora en la pista de auditoría están en la hora universal coordinada (UTC), la fecha y la hora se deben traducir a la zona horaria actual para que tengan sentido. Tenga en cuenta este punto siempre que manipule estos archivos con los comandos de archivo estándar en lugar de utilizar el comando `auditreduce`.

---

**Antes de empezar**

Debe convertirse en un administrador con el perfil de derechos de revisión de auditoría asignado. Para obtener más información, consulte [“Cómo usar los derechos administrativos que tiene asignados” en la página 164](#).

**1 Cree un sistema de archivos para almacenar los archivos de auditoría fusionados.**

Para reducir la posibilidad de que se alcance el límite de espacio en disco, este sistema de archivos debe estar en *otra zpool* de los sistemas de archivos que creó en [“Cómo crear sistemas de archivos ZFS para archivos de auditoría” en la página 593](#) para almacenar los archivos originales.

**2 Fusione los registros de auditoría en la pista de auditoría.**

Vaya al directorio para almacenar archivos de auditoría fusionados. Desde este directorio, fusione los registros de auditoría en un archivo con un sufijo con nombre. Todos los directorios de la pista de auditoría en el sistema local se fusionan y se almacenan en este directorio.

```
cd audit-storage-directory
auditreduce -Uppercase-option -O suffix
```

Las opciones en mayúscula del comando `auditreduce` manipulan los archivos en la pista de auditoría. Las opciones en mayúscula incluyen las siguientes:

- A                   Selecciona todos los archivos en la pista de auditoría.
- C                   Selecciona únicamente archivos completos.
- M                   Selecciona los archivos con un sufijo determinado. El sufijo puede ser un nombre de máquina o puede ser un sufijo que haya especificado para un archivo de resumen.
- O                   Crea un archivo de auditoría con indicaciones de hora de 14 caracteres para la hora de inicio y la hora de finalización, con el sufijo *suffix* en el directorio actual.
- R *pathname*       Especifica la lectura de archivos de auditoría en *pathname*, un directorio raíz de auditoría alternativo.
- S *server*           Especifica la lectura de archivos de auditoría del servidor especificado.

Para obtener la lista completa de opciones, consulte la página del comando [man auditreduce\(1M\)](#).

**Ejemplo 28–29** Copia de archivos de auditoría a un archivo de resumen

En el ejemplo siguiente, un administrador que tiene asignado el perfil de derechos de administrador del sistema copia todos los archivos de la pista de auditoría en un archivo fusionado, en un sistema de archivos diferente. El sistema de archivos `/var/audit/storage` está en un disco separado del sistema de archivos `/var/audit`, el sistema de archivos raíz de auditoría.

```
$ cd /var/audit/storage
$ auditreduce -A -O All
$ ls /var/audit/storage/*All
20100827183214.20100827215318.All
```

En el siguiente ejemplo, sólo los archivos completos se copian de la pista de auditoría a un archivo fusionado. La ruta completa se especifica como el valor de la opción `-O`. El último elemento de la ruta, `Complete`, se utiliza como el sufijo.

```
$ auditreduce -C -O /var/audit/storage/Complete
$ ls /var/audit/storage/*Complete
20100827183214.20100827214217.Complete
```

En el siguiente ejemplo, si agrega la opción `-D`, se suprimen los archivos de auditoría originales.

```
$ auditreduce -C -O daily_sys1.1 -D sys1.1
$ ls *sys1.1
20100827183214.20100827214217.daily_sys1.1
```

## ▼ Cómo seleccionar eventos de auditoría de la pista de auditoría

Puede filtrar registros de auditoría para examinarlos. Para obtener una lista completa de las opciones de filtrado, consulte la página del comando `man auditreduce(1M)`.

### Antes de empezar

Debe convertirse en un administrador con el perfil de derechos de revisión de auditoría asignado. Para obtener más información, consulte [“Cómo usar los derechos administrativos que tiene asignados” en la página 164](#).

- **Seleccione los tipos de registros que desee de la pista de auditoría o de un archivo de auditoría especificado.**

```
auditreduce -lowercase-option argument [optional-file]
```

*argument* Argumento específico que requiere una opción en minúscula. Por ejemplo, la opción `-c` requiere un *argument* de una clase de auditoría, como `ua`.

- d Selecciona todos los eventos en una fecha determinada. El formato de fecha de *argument* es *aaammdd*. Otras opciones de fecha, -b y -a, seleccionan los eventos antes y después de una fecha determinada.
  - u Selecciona todos los eventos atribuibles a un usuario determinado. *argument* es un nombre de usuario. Otra opción de usuario, -e, selecciona todos los eventos atribuibles a un ID de usuario vigente.
  - c Selecciona todos los eventos de una clase de auditoría preseleccionada. *argument* es un nombre de clase de auditoría
  - m Selecciona todas las instancias de un evento de auditoría determinado. *argument* es un evento de auditoría.
  - o Selecciona por tipo de objeto. Utilice esta opción para seleccionar por archivo, grupo, responsable de archivo, FMRI, pid y otros tipos de objetos.
- optional-file* Nombre de un archivo de auditoría.

Para obtener la lista completa de opciones, consulte la página del comando [man auditreduce\(1M\)](#).

### Ejemplo 28–30 Combinación y reducción de archivos de auditoría

El comando `audit reduce` puede eliminar los registros menos interesantes a medida que combina los archivos de entrada. Por ejemplo, puede utilizar el comando `audit reduce` para retener únicamente los registros de inicio y cierre de sesión en los archivos de auditoría de más de un mes. Si necesita recuperar la pista de auditoría completa, puede recuperar la pista del medio de copia de seguridad.

```
cd /var/audit/audit_summary
auditreduce -O lo.summary -b 20100827 -c lo; compress *lo.summary
```

### Ejemplo 28–31 Copia de los registros de auditoría de un usuario en un archivo de resumen

En este ejemplo, se fusionan los registros en la pista de auditoría que contienen el nombre de un usuario determinado. La opción -e busca el usuario vigente. La opción -u busca el usuario de inicio de sesión.

```
$ cd /var/audit/audit_summary
$ auditreduce -e tamiko -O tamiko
```

Puede buscar eventos específicos en este archivo. En el siguiente ejemplo, se verifica la hora en que el usuario inició y cerró sesión el 7 de septiembre de 2010, hora local. Sólo se verifican los archivos con el nombre del usuario como sufijo de archivo. La abreviatura de la fecha es *aaaammdd*.

```
auditreduce -M tamiko -O tamikolo -d 20100907 -u tamiko -c lo
```

## Ejemplo 28–32 Copia de registros seleccionados en un archivo único

En este ejemplo, los registros de inicio y cierre de sesión de un día determinado se seleccionan de la pista de auditoría. Los registros se fusionan en un archivo de destino. El archivo de destino se escribe en un sistema de archivos que no sea el sistema de archivos que contiene el directorio raíz de auditoría.

```
auditreduce -c lo -d 20100827 -O /var/audit/audit_summary/logins
ls /var/audit/audit_summary/*logins
/var/audit/audit_summary/20100827183936.20100827232326.logins
```

## ▼ Cómo visualizar el contenido de los archivos de auditoría binarios

El comando `praudit` permite ver los contenidos de los archivos de auditoría binarios. Puede redireccionar la salida del comando `audit reduce` o puede leer un archivo de auditoría determinado. La opción `-x` es útil para el procesamiento posterior.

### Antes de empezar

Debe convertirse en un administrador con el perfil de derechos de revisión de auditoría asignado. Para obtener más información, consulte [“Cómo usar los derechos administrativos que tiene asignados” en la página 164](#).

### ● Utilice uno de los siguientes comandos `praudit` para producir la mejor salida según su propósito.

Los siguientes ejemplos muestran la salida de `praudit` para el mismo evento de auditoría. Las políticas de auditoría se configuraron para incluir el token `sequence`.

- El comando `praudit -s` muestra los registros de auditoría en formato corto, un token por línea. Utilice la opción `-l` para colocar cada registro en una línea.

```
$ auditreduce -c lo | praudit -s
header,69,2,AUE_screenlock,,mach1,2010-10-14 08:02:56.348 -07:00
subject,jdoe,root,staff,jdoe,staff,856,50036632,82 0 mach1
return,success,0
sequence,1298
```

- El comando `praudit -r` muestra los registros de auditoría en su formato básico, un token por línea. Utilice la opción `-l` para colocar cada registro en una línea.

```
$ auditreduce -c lo | praudit -r
21,69,2,6222,0x0000,10.132.136.45,1287070091,698391050
36,26700,0,10,26700,10,856,50036632,82 0 10.132.136.45
39,0,0
47,1298
```



- El comando `praudit -x` muestra los registros de auditoría en formato XML, un token por línea. Utilice la opción `-l` para colocar la salida XML para un registro en una línea. La siguiente lista se divide en dos líneas de salida para entrar en esta página impresa:

```
$ auditreduce -c lo | praudit -x
<record version="2" event="screenlock - unlock" host="mach1"
 iso8601="2010-10-14 08:28:11.698 -07:00">
 <subject audit-uid="jdoe" uid="root" gid="staff" ruid="jdoe
 rgid="staff" pid="856" sid="50036632" tid="82 0 mach1"/>
 <return errval="success" retval="0"/>
 <sequence seq-num="1298"/>
</record>
```

### Ejemplo 28–33 Impresión de toda la pista de auditoría

Con una conducción al comando de impresión, la salida de toda la pista de auditoría pasa a la impresora. Por motivos de seguridad, la impresora tiene acceso limitado.

```
auditreduce | praudit | lp -d example.protected.printer
```

### Ejemplo 28–34 Visualización de un archivo de auditoría específico

En este ejemplo, se examina un archivo de inicio de sesión de resumen en la ventana de terminal.

```
cd /var/audit/audit_summary/logins
praudit 20100827183936.20100827232326.logins | more
```

### Ejemplo 28–35 Paso de registros de auditoría a formato XML

En este ejemplo, los registros de auditoría se convierten a formato XML.

```
praudit -x 20100827183214.20100827215318.logins > 20100827.logins.xml
```

El archivo XML se puede visualizar en un explorador. El contenido del archivo sólo puede ser operado por una secuencia de comandos para extraer la información relevante.

### Ejemplo 28–36 Procesamiento de la salida de `praudit` con una secuencia de comandos

Es posible que quiera procesar la salida del comando `praudit` como líneas de texto. Por ejemplo, es posible que quiera seleccionar registros que el comando `auditreduce` no puede seleccionar. Puede utilizar una secuencia de comandos de shell sencilla para procesar la salida del comando `praudit`. La siguiente secuencia de comandos de ejemplo coloca un registro de auditoría en una línea, busca una cadena especificada por el usuario y devuelve el archivo de auditoría a su forma original.

```
#!/bin/sh
#
This script takes an argument of a user-specified string.
The sed command prefixes the header tokens with Control-A
The first tr command puts the audit tokens for one record
onto one line while preserving the line breaks as Control-A
#
praudit | sed -e '1,2d' -e '$s/^file.*$//' -e 's/^header/^aheader/' \
| tr '\012\001' '\002\012' \
| grep "$1" \
| tr '\002' '\012'
```

*Finds the user-specified string*  
*Restores the original newline breaks*

Tenga en cuenta que ^a en la secuencia de comandos equivale a Control-A, no los dos caracteres ^ y a. El prefijo distingue el token header de la cadena header que podría aparecer como texto.

### Errores más frecuentes

Un mensaje similar al siguiente indica que no tiene privilegios suficientes para usar el comando praudit:

```
praudit: Can't assign 20090408164827.20090408171614.sys1.1 to stdin.
```

Ejecute el comando praudit un shell de perfil. Debe convertirse en un administrador con el perfil de derechos de revisión de auditoría asignado. Para obtener más información, consulte [“Cómo usar los derechos administrativos que tiene asignados” en la página 164.](#)

## ▼ Cómo depurar un archivo de auditoría not\_terminated

Quando se producen interrupciones anómalas del sistema, el servicio de auditoría se cierra mientras su archivo de auditoría aún está abierto. O bien un sistema de archivos se vuelve inaccesible y hace que el sistema cambie a un nuevo sistema de archivos. En esos casos, un archivo de auditoría permanece con la cadena not\_terminated como indicación de hora final, aunque el archivo ya no se utilice para los registros de auditoría. Utilice el comando auditreduce -0 para otorgar al archivo la indicación de hora correcta.

### Antes de empezar

Debe convertirse en un administrador con el perfil de derechos de revisión de auditoría asignado. Para obtener más información, consulte [“Cómo usar los derechos administrativos que tiene asignados” en la página 164.](#)

- 1 Enumere los archivos con la cadena not\_terminated en el sistema de archivos de auditoría según el orden de creación.

```
ls -Rlt audit-directory*/ * | grep not_terminated
```

-R Muestra los archivos en los subdirectorios.

- t Muestra la lista de archivos desde el más reciente hasta el más antiguo.
- 1 Muestra los archivos en una columna.

## 2 Depure el archivo `not_terminated` anterior.

Especifique el nombre del archivo anterior en el comando `auditreduce -O`.

```
auditreduce -O system-name old-not-terminated-file
```

## 3 Elimine el archivo `not_terminated` anterior.

```
rm system-name old-not-terminated-file
```

### Ejemplo 28–37 Depuración de archivos de auditoría `not_terminated` cerrados

En el siguiente ejemplo, se encontraron archivos `not_terminated`, se renombraron y se eliminaron los originales.

```
ls -Rlt */* | grep not_terminated
.../egret.1/20100908162220.not_terminated.egret
.../egret.1/20100827215359.not_terminated.egret
cd */egret.1
auditreduce -O egret 20100908162220.not_terminated.egret
ls -lt
20100908162220.not_terminated.egret Current audit file
20100827230920.20100830000909.egret Cleaned up audit file
20100827215359.not_terminated.egret Input (old) audit file
rm 20100827215359.not_terminated.egret
ls -lt
20100908162220.not_terminated.egret Current audit file
20100827230920.20100830000909.egret Cleaned up audit file
```

La indicación de hora de inicio en el nuevo archivo refleja la hora del primer evento de auditoría en el archivo `not_terminated`. La indicación de hora final refleja la hora del último evento de auditoría en el archivo.

## ▼ Cómo evitar el desbordamiento de la pista de auditoría

Si la política de seguridad requiere que todos los datos de auditoría se guarden, evite la pérdida de registros de auditoría.

### Antes de empezar

Debe asumir el rol `root`. Para obtener más información, consulte [“Cómo usar los derechos administrativos que tiene asignados” en la página 164](#).

**1 Establezca un tamaño libre mínimo en el complemento audit\_binfile.**

Utilice el atributo `p_minfree`.

El alias de correo electrónico `audit_warn` envía una advertencia cuando el espacio en disco llega al tamaño libre mínimo. Consulte el [Ejemplo 28–17](#).

**2 Configure un programa para archivar con regularidad los archivos de auditoría.**

Almacene los archivos de auditoría mediante una copia de los archivos en los medios sin conexión. También puede mover los archivos a un sistema de archivos de almacenamiento.

Si recopila registros de auditoría de texto con la utilidad `syslog`, archive los registros de texto. Para más información, consulte la página del comando `man logadm(1M)`.

**3 Establezca un programa para suprimir los archivos de auditoría almacenados del sistema de archivos de auditoría.**

**4 Guarde y almacene información auxiliar.**

Archive la información que sea necesaria para interpretar los registros de auditoría junto con la pista de auditoría. Como mínimo, guarde los archivos `passwd`, `group`, y `hosts`. También podría archivar los archivos `audit_event` y `audit_class`.

**5 Mantenga registros de qué archivos de auditoría se han archivado.**

**6 Almacene los medios archivados adecuadamente.**

**7 Reduzca la cantidad de capacidad del sistema de archivos que se necesita activando la compresión ZFS.**

En un sistema de archivos ZFS que está dedicado a archivos de auditoría, la compresión reduce los archivos considerablemente. Para ver un ejemplo, consulte “[Cómo comprimir archivos de auditoría en un sistema de archivos dedicado](#)” en la página 637.

Consulte también “[Interacciones entre propiedades de compresión, eliminación de datos duplicados y cifrado de ZFS](#)” de *Administración de Oracle Solaris 11.1: sistemas de archivos ZFS*.

**8 Reduzca el volumen de los datos de auditoría que almacene mediante la creación de archivos de resumen.**

Puede extraer archivos de resumen de la pista de auditoría mediante las opciones en el comando `audit reduce`. Los archivos de resumen contienen únicamente registros para tipos especificados de eventos de auditoría. Para extraer archivos de resumen, consulte el [Ejemplo 28–30](#) y el [Ejemplo 28–32](#).

## Solución de problemas del servicio de auditoría (tareas)

En esta sección, se tratan distintos mensajes de error de auditoría, las preferencias y la auditoría proporcionada por otras herramientas. Estos procedimientos pueden ayudar a registrar eventos de auditoría necesarios y a depurar problemas de auditoría.

## Solución de problemas del servicio de auditoría (mapa de tareas)

El siguiente mapa de tareas hace referencia a los procedimientos para la resolución de problemas de auditoría.

| Problema                                                                                                         | Solución                                                                                                                           | Para obtener instrucciones                                                                                              |
|------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------|
| ¿Por qué los registros de auditoría no se registran cuando tengo configurada la auditoría?                       | Solucione problemas del servicio de auditoría.                                                                                     | <a href="#">“Cómo determinar que la auditoría se está ejecutando”</a> en la página 626                                  |
| ¿Cómo puedo reducir la cantidad de información sobre auditoría que se está recopilando?                          | Audite sólo los eventos que desea auditar.                                                                                         | <a href="#">“Cómo reducir el volumen de los registros de auditoría que se producen”</a> en la página 628                |
| ¿Cómo puedo auditar todo lo que un usuario hace en el sistema?                                                   | Audite uno o más usuarios para cada comando.                                                                                       | <a href="#">“Cómo auditar todos los comandos por usuarios”</a> en la página 630                                         |
| ¿Cómo puedo cambiar los eventos de auditoría que se graban y hacer que el cambio afecte las sesiones existentes? | Actualice la máscara de preselección de un usuario.                                                                                | <a href="#">“Cómo actualizar la máscara de preselección de usuarios con sesión iniciada”</a> en la página 634           |
| ¿Cómo puedo localizar modificaciones en archivos determinados?                                                   | Audite las modificaciones en los archivos y, luego, use el comando <code>audit reduce</code> para encontrar archivos determinados. | <a href="#">“Cómo buscar registros de auditoría de los cambios realizados en archivos específicos”</a> en la página 632 |
| ¿Cómo puedo reducir el tamaño de mis archivos de auditoría?                                                      | Limite el tamaño del archivo de auditoría binario.                                                                                 | <a href="#">“Cómo limitar el tamaño de los archivos de auditoría binarios”</a> en la página 636                         |
| ¿Cómo puedo utilizar menos espacio en el sistema de archivos para los archivos de auditoría?                     | Utilice las cuotas y la compresión ZFS.                                                                                            | <a href="#">“Cómo comprimir archivos de auditoría en un sistema de archivos dedicado”</a> en la página 637              |
| ¿Cómo puedo eliminar eventos de auditoría del archivo <code>audit_event</code> ?                                 | Actualice correctamente el archivo <code>audit_event</code> .                                                                      | <a href="#">“Cómo evitar la auditoría de eventos específicos”</a> en la página 635                                      |
| ¿Cómo puedo auditar todos los inicios de sesión a un sistema Oracle Solaris?                                     | Audite los inicios de sesión de cualquier sistema.                                                                                 | <a href="#">“Cómo auditar inicios de sesión de otros sistemas operativos”</a> en la página 638                          |

| Problema                                                                          | Solución                                                                                            | Para obtener instrucciones                                                            |
|-----------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| ¿Por qué no se mantienen los registros de auditoría de mis transferencias de FTP? | Utilice la herramienta de auditoría adecuada para las utilidades que generan sus propios registros. | <a href="#">“Cómo auditar transferencias de archivos FTP y SFTP” en la página 639</a> |

## ▼ Cómo determinar que la auditoría se está ejecutando

La auditoría está activada de manera predeterminada. Si cree que la auditoría no se ha desactivado, pero los registros de auditoría no se están enviando al complemento activo, utilice el siguiente procedimiento para aislar el problema.

**Antes de empezar** Para modificar un sistema de archivos, debe tener asignada la autorización `solaris.admin.edit/ path-to-system-file`. De manera predeterminada, el rol `root` tiene esta autorización. Para configurar la auditoría, debe convertirse en administrador con el perfil de derechos de configuración de auditoría asignado.

### 1 Determine que la auditoría se esté ejecutando.

Utilice cualquiera de los métodos siguientes:

- Compruebe la condición actual de la auditoría.

La siguiente lista indica que la auditoría no se está ejecutando:

```
auditconfig -getcond
audit condition = noaudit
```

La siguiente lista indica que la auditoría se está ejecutando:

```
auditconfig -getcond
audit condition = auditing
```

- Compruebe que el servicio de auditoría se esté ejecutando.

La siguiente lista indica que la auditoría no se está ejecutando:

```
svcs -x auditd
svc:/system/auditd:default (Solaris audit daemon)
State: disabled since Sun Oct 10 10:10:10 2010
Reason: Disabled by an administrator.
 See: http://support.oracle.com/msg/SMF-8000-05
 See: auditd(1M)
 See: audit(1M)
 See: auditconfig(1M)
 See: audit_flags(5)
 See: audit_binfile(5)
 See: audit_syslog(5)
 See: audit_remote(5)
 See: /var/svc/log/system-auditd:default.log
Impact: This service is not running.
```

La siguiente lista indica que el servicio de auditoría se está ejecutando:

```
svcs auditd
STATE STIME FMRI
online 10:10:10 svc:/system/auditd:default
```

Si el servicio de auditoría no se está ejecutando, actívelo. Para conocer el procedimiento, consulte [“Cómo activar el servicio de auditoría” en la página 613](#).

## 2 Verifique que, al menos, un complemento esté activo.

```
audit -v
audit: no active plugin found
```

Si no hay ningún complemento activo, active uno.

```
auditconfig -setplugin audit_binfile active
audit -v
configuration ok
```

## 3 Si crea una clase de auditoría personalizada, compruebe que haya asignado eventos a la clase.

Por ejemplo, la siguiente lista de indicadores contiene la clase pf, que el software Oracle Solaris no entregó:

```
auditconfig -getflags
active user default audit flags = pf,lo(0x0100000000000000,00x0100000000001000)
configured user default audit flags = pf,lo(0x0100000000000000,00x0100000000001000)
```

Para obtener una descripción de la creación de la clase pf, consulte [“Cómo agregar una clase de auditoría” en la página 590](#).

### a. Compruebe que la clase esté definida en el archivo audit\_class.

La clase de auditoría debe estar definida, y su máscara debe ser única.

```
grep pf /etc/security/audit_class Verify class exists
0x0100000000000000:pf:profile
grep 0x0100000000000000 /etc/security/audit_class Ensure mask is unique
0x0100000000000000:pf:profile
```

Reemplace una máscara que no sea única. Si la clase no está definida, defínala. De lo contrario, ejecute el comando `auditconfig -setflags` con los valores válidos para restablecer los indicadores actuales.

### b. Compruebe que los eventos se hayan asignado a la clase.

Utilice uno de los métodos siguientes:

```
auditconfig -lsevent | egrep " pf|,pf|pf,"
AUE_PFEEXEC 116 pf execve(2) with pfexec enabled
```

```
auditrecord -c pf
List of audit events assigned to pf class
```

Si los eventos no están asignados a la clase, asigne los eventos adecuados a esta clase.

**4 Si los pasos anteriores no indicaban un problema, revise su correo electrónico y los archivos de registro.**

**a. Lea el correo electrónico enviado al alias `audit_warn`.**

La secuencia de comandos `audit_warn` envía mensajes de alerta al alias de correo electrónico `audit_warn`. Ante la ausencia de un alias configurado correctamente, los mensajes se envían a la cuenta `root`.

**b. Revise los archivos de registro para el servicio de auditoría.**

La salida del comando `svcs -s auditd` muestra la ruta completa a los registros de auditoría que el servicio de auditoría produce. Para ver un ejemplo, consulte la lista en el [Paso 1](#).

**c. Revise los archivos de registro del sistema.**

La secuencia de comandos `audit_warn` escribe mensajes `daemon.alert` en el archivo `/var/log/syslog`.

El archivo `/var/adm/messages` podría contener información.

**5 Después de encontrar y corregir los problemas, active o reinicie el servicio de auditoría.**

```
audit -s
```

## ▼ **Cómo reducir el volumen de los registros de auditoría que se producen**

Después de determinar qué eventos deben auditarse en su sitio, utilice las siguientes sugerencias para crear los archivos de auditoría sólo con la información necesaria.

**Antes de empezar**

Para preseleccionar clases de auditoría y definir la política de auditoría, debe tener asignado el perfil de derechos de configuración de auditoría. Para modificar un sistema de archivos, debe tener asignada la autorización `solaris.admin.edit/path-to-system-file`. De manera predeterminada, el rol `root` tiene esta autorización. Para asignar indicadores de auditoría a usuarios, roles y perfiles de derechos, debe asumir el rol `root`.

**1 Utilice la política de auditoría predeterminada.**

En concreto, evite agregar eventos y tokens de auditoría a la pista de auditoría. Las siguientes políticas aumentan el tamaño de la pista de auditoría.

- Política `arge`: agrega variables de entorno a los eventos de auditoría `execv`. Si bien, auditar eventos `execv` puede ser muy costoso, agregar variables al registro de auditoría no es costoso.



- Política `argv`: agrega parámetros de comandos a los eventos de auditoría `execv`. Si bien, auditar eventos `execv` puede ser muy costoso, agregar parámetros de comandos al registro de auditoría no es costoso.
- Política `public`: si va a auditar eventos de archivos, agregue un evento a la pista de auditoría cada vez que ocurra un evento auditable en un [objeto público](#). Las clases de archivos incluyen `fa`, `fc`, `fd`, `fm`, `fr`, `fw` y `cl`. Para la definición de un archivo público, consulte “[Conceptos y terminología de auditoría](#)” en la [página 548](#).
- Política `path`: agrega un token `path` a los eventos de auditoría que incluyen un token `path` opcional.
- Política `group`: agrega un token de grupo a los eventos de auditoría que incluyen un token `newgroups` opcional.
- Política `seq`: agrega un token de secuencia a cada evento de auditoría.
- Política `trail`: agrega un token de ubicador a cada evento de auditoría.
- Política `windata_down`: en un sistema configurado con Trusted Extensions, agrega eventos cuando se disminuye el nivel de la información en una ventana con etiqueta.
- Política `windata_up`: en un sistema configurado con Trusted Extensions, agrega eventos cuando se aumenta el nivel de la información en una ventana con etiqueta.
- Política `zonename`: agrega el nombre de zona a cada evento de auditoría. Si la zona global es la única zona configurada, agrega la cadena `zone_global` a cada evento de auditoría.

El siguiente registro de auditoría muestra el uso del comando `ls`. La clase `ex` se está auditando y la política predeterminada está en uso:

```
header,129,2,AUE_EXECVE,,mach1,2010-10-14 11:39:22.480 -07:00
path,/usr/bin/ls
attribute,100555,root,bin,21,320271,18446744073709551615
subject,jdoe,root,root,root,root,2404,50036632,82 0 mach1
return,success,0
```

A continuación, se muestra el mismo registro cuando se activan todas las políticas:

```
header,1578,2,AUE_EXECVE,,mach1,2010-10-14 11:45:46.658 -07:00
path,/usr/bin/ls
attribute,100555,root,bin,21,320271,18446744073709551615
exec_args,2,ls,/etc/security
exec_env,49,MANPATH=/usr/share/man,USER=jdoe,GDM_KEYBOARD_LAYOUT=us,EDITOR=gedit,
LANG=en_US.UTF-8,GDM_LANG=en_US.UTF-8,PS1=#,GDMSESSION=gnome,SESSIONTYPE=1,SHLVL=2,
HOME=/home/jdoe,LOGNAME=jdoe,G_FILENAME_ENCODING=@locale,UTF-8, PRINTER=example-dbl,
...
path,/lib/ld.so.1
attribute,100755,root,bin,21,393073,18446744073709551615
subject,jdoe,root,root,root,root,2424,50036632,82 0 mach1
group,root,other,bin,sys,adm,uucp,mail,tty,lp,nuucp,daemon
return,success,0
zone,global
sequence,197
trailer,1578
```

**2 Utilice el complemento `audit_syslog` para enviar algunos eventos de auditoría a `syslog`.**

Y no envíe dichos eventos de auditoría al complemento `audit_binfile` o `audit_remote`. Esta estrategia funciona sólo si no es necesario mantener registros binarios de los eventos de auditoría que envía a los registros `syslog`.

**3 Defina menos indicadores de auditoría en todo el sistema y audite usuarios individuales.**

Reduzca la cantidad de auditoría para todos los usuarios mediante la reducción del número de clases de auditoría que se auditan en todo el sistema.

Utilice la palabra clave `audit_flags` para los comandos `roleadd`, `rolemod`, `useradd` y `usermod` con el fin de auditar eventos de usuarios y roles específicos. Para ver ejemplos consulte el [Ejemplo 28–21](#) y la página del comando `man usermod(1M)`.

Utilice las propiedades `always_audit` y `never_audit` del comando `profiles` para auditar eventos de perfiles de derechos específicos. Para obtener información, consulte la página del comando `man profiles(1)`.

---

**Nota** – Al igual que otros atributos de seguridad, los indicadores de auditoría son afectados por orden de búsqueda. Para obtener más información, consulte [“Orden de búsqueda para atributos de seguridad asignados” en la página 207](#).

---

**4 Cree sus propias clases de auditoría personalizadas.**

Puede crear clases de auditoría en el sitio. En estas clases, coloque sólo los eventos de auditoría que necesita supervisar. Para conocer el procedimiento, consulte [“Cómo agregar una clase de auditoría” en la página 590](#).

---

**Nota** – Para obtener información sobre los efectos de modificar un archivo de configuración de auditoría, consulte [“Archivos de configuración de auditoría y empaquetado” en la página 645](#).

---

## ▼ **Cómo auditar todos los comandos por usuarios**

Como parte de la política de seguridad del sitio, algunos sitios requieren registros de auditoría de todos los comandos ejecutados por la cuenta `root` y los roles administrativos. Algunos sitios pueden requerir registros de auditoría de todos los comandos por todos los usuarios. Además, los sitios pueden requerir que los argumentos de los comandos y el entorno se registren.

**Antes de empezar**

Para preseleccionar clases de auditoría y definir la política de auditoría, debe tenerse en cuenta el perfil de derechos de configuración de auditoría asignado. Para asignar indicadores de auditoría a usuarios, roles y perfiles de derechos, debe asumir el rol `root`.

**1 Audite las clases `to` y `ex`.**

La clase `ex` audita todas las llamadas a las funciones `exec()` y `execve()`.

La clase `lo` audita los inicios de sesión, los cierres de sesión y los bloqueos de pantalla. La siguiente salida muestra todos los eventos de las clases `ex` y `lo`.

```
% auditconfig -lsevent | grep " lo "
AUE_login 6152 lo login - local
AUE_logout 6153 lo logout
AUE_telnet 6154 lo login - telnet
AUE_rlogin 6155 lo login - rlogin
AUE_rshd 6158 lo rsh access
AUE_su 6159 lo su
AUE_rexecd 6162 lo rexecd
AUE_passwd 6163 lo passwd
AUE_rexd 6164 lo rexd
AUE_ftpd 6165 lo ftp access
AUE_ftpd_logout 6171 lo ftp logout
AUE_ssh 6172 lo login - ssh
AUE_role_login 6173 lo role login
AUE_newgrp_login 6212 lo newgrp login
AUE_admin_authenticate 6213 lo admin login
AUE_screenlock 6221 lo screenlock - lock
AUE_screenunlock 6222 lo screenlock - unlock
AUE_zlogin 6227 lo login - zlogin
AUE_su_logout 6228 lo su logout
AUE_role_logout 6229 lo role logout
AUE_smbd_session 6244 lo smbd(1m) session setup
AUE_smbd_logoff 6245 lo smbd(1m) session logoff
AUE_ClientConnect 9101 lo client connection to x server
AUE_ClientDisconnect 9102 lo client disconn. from x server
% auditconfig -lsevent | egrep " ex |ex |ex,"
AUE_EXECVE 23 ex,ps execve(2)
```

- **Para auditar los roles administrativos de estas clases, modifique los atributos de seguridad de los roles.**

En el siguiente ejemplo, `root` es un rol. El sitio ha creado tres roles: `sysadm`, `auditadm` y `netadm`. Todos los roles se auditan para determinar el éxito y el fallo de eventos en las clases `ex` y `lo`.

```
rolemod -K audit_flags=lo,ex:no root
rolemod -K audit_flags=lo,ex:no sysadm
rolemod -K audit_flags=lo,ex:no auditadm
rolemod -K audit_flags=lo,ex:no netadm
```

- **Para auditar todos los usuarios de estas clases, establezca los indicadores de todo el sistema.**

```
auditconfig -setflags lo,ex
```

El resultado es similar al siguiente:

```
header,129,2,AUE_EXECVE,,mach1,2010-10-14 12:17:12.616 -07:00
path,/usr/bin/ls
attribute,100555,root,bin,21,320271,18446744073709551615
subject,jdoe,root,root,root,root,2486,50036632,82 0 mach1
return,success,0
```

- 2 Para registrar los argumentos de los comandos, agregue la política `argv`.**

```
auditconfig -setpolicy +argv
```

El token `exec_args` registra los argumentos de los comandos:

```
header,151,2,AUE_EXECVE,,mach1,2010-10-14 12:26:17.373 -07:00
path,/usr/bin/ls
attribute,100555,root,bin,21,320271,18446744073709551615
exec_args,2,ls,/etc/security
subject,jdoe,root,root,root,root,2494,50036632,82 0 mach1
return,success,0
```

### 3 Para registrar el entorno en el que se ejecuta el comando, agregue la política `arge`.

```
auditconfig -setpolicy +arge
```

El token `exec_env` registra el entorno de los comandos:

```
header,1460,2,AUE_EXECVE,,mach1,2010-10-14 12:29:39.679 -07:00
path,/usr/bin/ls
attribute,100555,root,bin,21,320271,18446744073709551615
exec_args,2,ls,/etc/security
exec_env,49,MANPATH=/usr/share/man,USER=jdoe,GDM_KEYBOARD_LAYOUT=us,EDITOR=gedit,
LANG=en_US.UTF-8,GDM_LANG=en_US.UTF-8,PS1=#,GDMSESSION=gnome,SESSIONTYPE=1,SHLV=2,
HOME=/home/jdoe,LOGNAME=jdoe,G_FILENAME_ENCODING=@locale,UTF-8,
PRINTER=example-dbl,...,=/usr/bin/ls
subject,jdoe,root,root,root,root,2502,50036632,82 0 mach1
return,success,0
```

## ▼ Cómo buscar registros de auditoría de los cambios realizados en archivos específicos

Si tiene como objetivo registrar las escrituras de los archivos en comparación con un número limitado de archivos, como `/etc/passwd` y los archivos en el directorio `/etc/default`, puede utilizar el comando `auditreduce` para ubicar los archivos.

#### Antes de empezar

El rol `root` puede realizar todas las tareas en este procedimiento.

Si tienen derechos administrativos distribuidos en su organización, tenga en cuenta lo siguiente:

- Un administrador con el perfil de derechos de configuración de auditoría puede ejecutar el comando `auditconfig`.
- Un administrador con el perfil de derechos de revisión de auditoría puede ejecutar el comando `auditreduce`.
- Sólo el rol `root` puede asignar indicadores de auditoría.

Para obtener más información, consulte [“Cómo usar los derechos administrativos que tiene asignados” en la página 164](#).

## 1 Auditoría de la clase fw.

Agregar la clase a los indicadores de auditoría de un usuario o rol genera menos registros que agregar la clase a la máscara de preselección de auditoría en todo el sistema. Lleve a cabo uno de los pasos siguientes:

- **Agregue la clase fw a roles concretos.**

```
rolemod -K audit_flags=fw:no root
rolemod -K audit_flags=fw:no sysadm
rolemod -K audit_flags=fw:no auditadm
rolemod -K audit_flags=fw:no netadm
```

- **Agregue la clase fw a los indicadores de todo el sistema.**

```
auditconfig -getflags
active user default audit flags = lo(0x1000,0x1000)
configured user default audit flags = lo(0x1000,0x1000)
auditconfig -setflags lo,fw
user default audit flags = lo,fw(0x1002,0x1002)
```

## 2 O audite escrituras con éxito de archivos.

Auditar éxitos genera menos registros que auditar fallos y éxitos. Lleve a cabo uno de los pasos siguientes:

- **Agregue la clase +fw a roles concretos.**

```
rolemod -K audit_flags=+fw:no root
rolemod -K audit_flags=+fw:no sysadm
rolemod -K audit_flags=+fw:no auditadm
rolemod -K audit_flags=+fw:no netadm
```

- **Agregue la clase +fw a los indicadores de todo el sistema.**

```
auditconfig -getflags
active user default audit flags = lo(0x1000,0x1000)
configured user default audit flags = lo(0x1000,0x1000)
auditconfig -setflags lo,+fw
user default audit flags = lo,+fw(0x1002,0x1000)
```

- **Si los indicadores de todo el sistema se auditan para determinar el éxito y el fracaso, audite los éxitos sólo para usuarios y roles específicos.**

```
auditconfig -getflags
active user default audit flags = lo,fw(0x1002,0x1002)
configured user default audit flags = lo,fw(0x1002,0x1002)
rolemod -K audit_flags=~fw:no root
rolemod -K audit_flags=~fw:no sysadm
rolemod -K audit_flags=~fw:no auditadm
rolemod -K audit_flags=~fw:no netadm
```

Los indicadores de todo el sistema aún no tienen cambios, pero la máscara de preselección para estos cuatro roles ha cambiado.

```
auditconfig -getflags
active user default audit flags = lo,fw(0x1002,0x1000)
```

```
configured user default audit flags = lo,fw(0x1002,0x1000)
```

### 3 Para buscar los registros de auditoría para archivos específicos, utilice el comando `auditreduce`.

```
auditreduce -o file=/etc/passwd,/etc/default -O filechg
```

El comando `auditreduce` busca en la pista de auditoría todas las instancias del argumento `file`. El comando crea un archivo binario con el sufijo `filechg` que contiene todos los registros que incluyen los nombres de ruta de los archivos de interés. Consulte la página del comando [man auditreduce\(1M\)](#) para conocer la sintaxis de la opción `-o file=nombre_ruta`.

### 4 Para leer el archivo `filechg`, utilice el comando `praudit`.

```
praudit *filechg
```

## ▼ Cómo actualizar la máscara de preselección de usuarios con sesión iniciada

Desea que los usuarios que ya han iniciado sesión sean auditados para detectar si hubo cambios en la máscara de preselección de auditoría de todo el sistema.

#### Antes de empezar

Debe convertirse en un administrador con el perfil de derechos de configuración de auditoría asignado. Para finalizar las sesiones de usuario, es necesario que se convierta en administrador con el perfil de derechos de administración de procesos asignado. Para obtener más información, consulte “[Cómo usar los derechos administrativos que tiene asignados](#)” en la página 164.

### ● Actualice la máscara de preselección de los usuarios que ya iniciaron sesión.

Dispone de dos opciones. Puede terminar las sesiones existentes o utilizar el comando `auditconfig` para actualizar las máscaras de preselección.

#### ■ Termine las sesiones existentes de los usuarios.

Los usuarios pueden cerrar la sesión y volver a iniciarla. Asimismo, usted, en un rol que tiene asignado el perfil de derechos de gestión de procesos puede terminar (eliminar) manualmente sesiones activas. Las nuevas sesiones heredan la nueva máscara de preselección. Sin embargo, cerrar la sesión de los usuarios puede ser poco práctico.

- **Cambie de forma dinámica la máscara de preselección de cada usuario con sesión iniciada.**

En este ejemplo, se presupone que ha cambiado la máscara de preselección de auditoría de todo el sistema de `lo` a `lo,ex`.

```
auditconfig -setflags lo,ex
```

- Enumere los usuarios regulares que han iniciado sesión y sus ID de proceso.**

```
who -a
jdoe - vt/2 Jan 25 07:56 4:10 1597 (:0)
jdoe + pts/1 Jan 25 10:10 . 1706 (:0.0)
...
jdoe + pts/2 Jan 25 11:36 3:41 1706 (:0.0)
```

- Para realizar una comparación con posterioridad, visualice la máscara de preselección de cada usuario.**

```
auditconfig -getpinfo 1706
audit id = jdoe(1234)
process preselection mask = lo(0x1000,0x1000)
terminal id (maj,min,host) = 9426,65559,mach1(192.168.123.234)
audit session id = 103203403
```

- Modifique la máscara de preselección apropiada mediante la ejecución de uno o más de los siguientes comandos:**

```
auditconfig -setpmask 1706 lo,ex /* for this process */
auditconfig -setumask jdoe lo,ex /* for this user */
auditconfig -setsmask 103203403 lo,ex /* for this session */
```

- Verifique que la máscara de preselección para el usuario haya cambiado.**

Por ejemplo, compruebe un proceso que existía antes de haber cambiado la máscara.

```
auditconfig -getpinfo 1706
audit id = jdoe(1234)
process preselection mask = ex,lo(0x40001000,0x40001000)
terminal id (maj,min,host) = 9426,65559,mach1(192.168.123.234)
audit session id = 103203403
```

## ▼ Cómo evitar la auditoría de eventos específicos

Con fines de mantenimiento, a veces, un sitio quiere evitar que se auditen eventos.

### Antes de empezar

Debe asumir el rol `root`. Para obtener más información, consulte [“Cómo usar los derechos administrativos que tiene asignados” en la página 164](#).

- Cambie la clase del evento a la clase `no`.**

---

**Nota** – Para obtener información sobre los efectos de modificar un archivo de configuración de auditoría, consulte [“Archivos de configuración de auditoría y empaquetado” en la página 645.](#)

---

Por ejemplo, los eventos 26 y 27 pertenecen a la clase pm.

```
audit_event file
...
25:AUE_VFORK:vfork(2):ps
26:AUE_SETGROUPS:setgroups(2):pm
27:AUE_SETPGRP:setpgrp(2):pm
28:AUE_SWAPON:swapon(2):no
...
```

Cambie estos eventos a la clase no.

```
audit_event file
...
25:AUE_VFORK:vfork(2):ps
26:AUE_SETGROUPS:setgroups(2):no
27:AUE_SETPGRP:setpgrp(2):no
28:AUE_SWAPON:swapon(2):no
...
```

Si la clase pm está siendo auditada actualmente, las sesiones existentes aún auditarán los eventos 26 y 27. Para detener la auditoría de estos eventos, debe actualizar las máscaras de preselección de los usuarios siguiendo las instrucciones de [“Cómo actualizar la máscara de preselección de usuarios con sesión iniciada” en la página 634.](#)




---

**Precaución** – Nunca quite el comentario de eventos en el archivo `audit_event`. Este archivo es utilizado por el comando `praudit` para leer archivos binarios de auditoría. Los archivos de auditoría almacenados pueden contener eventos que se muestran en el archivo.

---

## 2 Refresque los eventos del núcleo.

```
auditconfig -conf
Configured 283 kernel events.
```

## ▼ Cómo limitar el tamaño de los archivos de auditoría binarios

Los archivos de auditoría binarios crecen sin límite. Para facilitar el archivado y la búsqueda, puede que desee limitar el tamaño. También puede crear archivos binarios más pequeños a partir del archivo original.

### Antes de empezar

Debe convertirse en un administrador que tiene asignado el perfil de derechos de configuración de auditoría para definir el atributo `p_size`. Debe convertirse en un administrador que tiene



asignado el perfil de derechos de revisión de auditoría para utilizar el comando `audit reduce`. Para obtener más información, consulte [“Cómo usar los derechos administrativos que tiene asignados” en la página 164](#).

**1 Utilice el atributo `p_fsize` para limitar el tamaño de archivos de auditoría binarios individuales.**

Para obtener una descripción del atributo `p_fsize`, consulte la sección ATRIBUTOS DE OBJETO de la página del comando `man audit_binfile(5)`.

Si desea ver un ejemplo, consulte el [Ejemplo 28–14](#).

**2 Utilice el comando `audit reduce` para seleccionar registros y escribir esos registros en un archivo más pequeño para un mayor análisis.**

Las opciones `audit reduce -minúscula` buscan registros específicos.

Las opciones `audit reduce -mayúscula` escriben las selecciones en un archivo. Para obtener más información, consulte la página del comando `man audit reduce(1M)`. Consulte también [“Gestión de registros de auditoría en sistemas locales \(tareas\)” en la página 614](#).

## ▼ **Cómo comprimir archivos de auditoría en un sistema de archivos dedicado**

Los archivos de auditoría pueden crecer mucho. Puede establecer un límite superior para el tamaño de un archivo, como se muestra en el [Ejemplo 28–14](#). En este procedimiento, se utiliza la compresión para reducir el tamaño.

**Antes de empezar**

Debe convertirse en un administrador al que se le ha asignado perfiles de derechos de gestión de sistemas de archivos ZFS y gestión de almacenamiento ZFS. El último perfil permite crear agrupaciones de almacenamiento. Para obtener más información, consulte [“Cómo usar los derechos administrativos que tiene asignados” en la página 164](#).

**1 Dedique un sistema de archivos ZFS para archivos de auditoría.**

Para conocer el procedimiento, consulte [“Cómo crear sistemas de archivos ZFS para archivos de auditoría” en la página 593](#).

**2 Comprima la agrupación de almacenamiento ZFS mediante una de las siguientes opciones.**

Con ambas opciones, se comprime el sistema de archivos de auditoría. Después de que el servicio de auditoría se refresca, la razón de compresión se muestra.

Para establecer la compresión, utilice el comando `zfs set compression=onconjunto_datos`. En los siguientes ejemplos, la agrupación `ZFS auditp/auditf` es el conjunto de datos.

- **Utilice el algoritmo de compresión predeterminado.**

```
zfs set compression=on auditp/auditf
audit -s
zfs get compressratio auditp/auditf
NAME PROPERTY VALUE SOURCE
auditp/auditf compressratio 4.54x -
```

- **Utilice un algoritmo de compresión superior.**

```
zfs set compression=zip-9 auditp/auditf
zfs get compression auditp/auditf
NAME PROPERTY VALUE SOURCE
auditp/auditf compression zip-9 local
audit -s
zfs get compressratio auditp/auditf
NAME PROPERTY VALUE SOURCE
auditp/auditf compressratio 16.89x -
```

El algoritmo de compresión `zip-9` genera archivos que ocupan un tercio menos de espacio que el algoritmo de compresión predeterminado, `lzjb`. Para obtener más información, consulte el [Capítulo 5, “Administración de sistemas de archivos ZFS de Oracle Solaris”](#) de *Administración de Oracle Solaris 11.1: sistemas de archivos ZFS*.

## ▼ Cómo auditar inicios de sesión de otros sistemas operativos

El sistema operativo Oracle Solaris puede auditar todos los inicios de sesión, independientemente del origen.

**Antes de empezar** Debe convertirse en un administrador con el perfil de derechos de configuración de auditoría asignado. Para obtener más información, consulte [“Cómo usar los derechos administrativos que tiene asignados” en la página 164](#).

### 1 Audite la clase `lo` para los eventos atribuibles y no atribuibles.

Esta clase audita los inicios de sesión, los cierres de sesión y los bloqueos de pantalla. Estas clases se auditan de manera predeterminada.

```
auditconfig -getflags
active user default audit flags = lo(0x1000,0x1000)
configured user default audit flags = lo(0x1000,0x1000)
auditconfig -getnaflags
active non-attributable audit flags = lo(0x1000,0x1000)
configured non-attributable audit flags = lo(0x1000,0x1000)
```

## 2 Si los valores se han modificado, agregue el indicador `lo`.

```
auditconfig -getflags
active user default audit flags = as,st(0x20800,0x20800)
configured user default audit flags = as,st(0x20800,0x20800)
auditconfig -setflags lo,as,st
user default audit flags = as,lo,st(0x21800,0x21800)
auditconfig -getnaflags
active non-attributable audit flags = na(0x400,0x400)
configured non-attributable audit flags = na(0x400,0x400)
auditconfig -setnaflags lo,na
non-attributable audit flags = lo,na(0x1400,0x1400)
```

---

**Nota** – Para auditar inicios de sesión `ssh`, su sistema debe ejecutar el daemon `ssh` de Oracle Solaris. Este daemon se modifica para el servicio de auditoría en un sistema Oracle Solaris. Para obtener más información, consulte [“Secure Shell y el proyecto OpenSSH” en la página 296](#).

---

## ▼ Cómo auditar transferencias de archivos FTP y SFTP

El servicio FTP crea registros de sus transferencias de archivos. El servicio SFTP, que se ejecuta bajo el protocolo `ssh`, puede ser auditado mediante la preselección de la clase de auditoría `ft`. Se pueden auditar los inicios de sesión en ambos servicios.

### Antes de empezar

Debe convertirse en un administrador con el perfil de derechos de configuración de auditoría asignado. Para obtener más información, consulte [“Cómo usar los derechos administrativos que tiene asignados” en la página 164](#).

### 1 Para registrar comandos y transferencias de archivos del servicio FTP, consulte la página del comando `man proftpd(8)`.

Para conocer las opciones de registro disponibles, lea [ProFTPD Logging \(http://www.proftpd.org/docs/howto/Logging.html\)](http://www.proftpd.org/docs/howto/Logging.html).

### 2 Para registrar el acceso a `sftp` y las transferencias de archivos, audite la clase `ft`.

La clase `ft` incluye las siguientes transacciones SFTP:

```
% auditrecord -c ft
file transfer: chmod ...
file transfer: chown ...
file transfer: get ...
file transfer: mkdir ...
file transfer: put ...
file transfer: remove ...
file transfer: rename ...
file transfer: rmdir ...
file transfer: session start ...
file transfer: session end ...
file transfer: symlink ...
file transfer: utimes
```

**3 Para registrar el acceso al servidor FTP, audite la clase lo.**

Como indica la siguiente salida, el inicio y cierre de sesión del daemon proftpd generan registros de auditoría.

```
% auditrecord -c lo | more
...
FTP server login
 program proftpd See in.ftpd(1M)
 event ID 6165 AUE_ftpd
 class lo (0x0000000000001000)
 header
 subject
 [text]
 return error message

FTP server logout
 program proftpd See in.ftpd(1M)
 event ID 6171 AUE_ftpd_logout
 class lo (0x0000000000001000)
 header
 subject
 return
...
```

## Auditoría (referencia)

---

En este capítulo, se describen los componentes importantes de la auditoría y se tratan los siguientes temas:

- “Servicio de auditoría” en la página 641
- “Páginas del comando man del servicio de auditoría” en la página 643
- “Perfiles de derechos para administración de auditoría” en la página 644
- “Auditoría y zonas de Oracle Solaris” en la página 645
- “Archivos de configuración de auditoría y empaquetado” en la página 645
- “Clases de auditoría” en la página 646
- “Complementos de auditoría” en la página 647
- “Servidor de auditoría remoto” en la página 648
- “Política de auditoría” en la página 648
- “Características del proceso de auditoría” en la página 650
- “Pista de auditoría” en la página 651
- “Convenciones de nombres de archivos de auditoría binarios” en la página 651
- “Estructura de registro de auditoría” en la página 651
- “Formatos de token de auditoría” en la página 653

Para obtener una descripción general de la auditoría, consulte el [Capítulo 26, “Auditoría \(descripción general\)”](#). Para obtener sugerencias de planificación, consulte el [Capítulo 27, “Planificación de la auditoría”](#). Para obtener información sobre procedimientos para configurar la auditoría en su sitio, consulte el [Capítulo 28, “Gestión de auditoría \(tareas\)”](#).

## Servicio de auditoría

El servicio de auditoría, `auditd`, está activado de manera predeterminada. Para activar, refrescar o desactivar el servicio, consulte [“Activación y desactivación del servicio de auditoría \(tareas\)” en la página 611](#).

Sin configuración de cliente, los siguientes valores predeterminados están establecidos:

- Se auditan todos los eventos de inicio de sesión.  
Se auditan los intentos de inicio de sesión correctos y con errores.
- Todos los usuarios se auditan para eventos de inicio y cierre de sesión, incluidos la asunción de roles y el bloqueo de pantalla.
- El complemento `audit_binfile` está activo. El directorio `/var/audit` almacena los registros de auditoría, el tamaño de un archivo de auditoría no está limitado y el tamaño de la cola es de 100 registros.
- La política `cnt` está establecida.  
Cuando los registros de auditoría llenan el espacio en disco disponible, el sistema realiza un seguimiento de la cantidad de registros de auditoría descartados. Una advertencia se emite cuando resta un uno por ciento de espacio en disco disponible.
- Los siguientes controles de cola de auditoría están establecidos.
  - Número máximo de registros en la cola de auditoría antes de generar los bloqueos de registros: 100
  - Número mínimo de registros en la cola de auditoría ante de que los procesos de auditoría bloqueados se desbloqueen: 10
  - Tamaño de memoria intermedia para la cola de auditoría: 8.192 bytes
  - Intervalo de escritura de registros de auditoría en la pista de auditoría: 20 segundos

Para mostrar los valores predeterminados, consulte [“Cómo visualizar los valores predeterminados del servicio de auditoría” en la página 578.](#)

El servicio de auditoría permite definir valores temporales o activos. Estos valores pueden diferir de los valores configurados o de los valores de propiedades.

- Los valores temporales no se restauran al refrescar o reiniciar el servicio de auditoría.  
La política de auditoría y los controles de cola de auditoría aceptan valores temporales. Los indicadores de auditoría no tienen un valor temporal.
- Los valores configurados se almacenan como valores de propiedades del servicio, por lo tanto, se restablecen al refrescar o reiniciar el servicio de auditoría.

Los perfiles de derechos controlan quién puede administrar el servicio de auditoría. Para obtener más información, consulte [“Perfiles de derechos para administración de auditoría” en la página 644.](#)

De manera predeterminada, todas las zonas se auditan de la misma manera. Consulte [“Auditoría y zonas de Oracle Solaris” en la página 645.](#)

# Páginas del comando man del servicio de auditoría

En la siguiente tabla se resumen las principales páginas del comando man administrativas para el servicio de auditoría.

| Página de comando man            | Resumen                                                                                                                                                                                                                                                                                                                                                                                                           |
|----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">audit(1M)</a>        | Comandos que controlan las acciones del servicio de auditoría<br><br>audit -n inicia un nuevo archivo de auditoría para el complemento audit_binfile.<br><br>audit -s activa y refresca la auditoría.<br><br>audit -t desactiva la auditoría.<br><br>audit -v verifica que al menos un complemento esté activo.                                                                                                   |
| <a href="#">audit_binfile(5)</a> | Complemento de auditoría predeterminado que envía registros de auditoría a un archivo binario. Consulte también <a href="#">“Complementos de auditoría” en la página 647</a> .                                                                                                                                                                                                                                    |
| <a href="#">audit_remote(5)</a>  | Complemento de auditoría que envía registros de auditoría a un receptor remoto.                                                                                                                                                                                                                                                                                                                                   |
| <a href="#">audit_syslog(5)</a>  | Complemento de auditoría que envía resúmenes de texto a la utilidad syslog.                                                                                                                                                                                                                                                                                                                                       |
| <a href="#">audit_class(4)</a>   | Archivo que contiene las definiciones de clases de auditoría. Los ocho bits de orden superior están disponibles para que los clientes creen nuevas clases de auditoría. Para modificar este archivo en la actualización del sistema, consulte <a href="#">“Cómo agregar una clase de auditoría” en la página 590</a> .                                                                                            |
| <a href="#">audit_event(4)</a>   | Archivo que contiene las definiciones de eventos de auditoría y asigna los eventos a clases de auditoría. La asignación se puede modificar. Para modificar este archivo en la actualización del sistema, consulte <a href="#">“Cómo cambiar una pertenencia a clase de un evento de auditoría” en la página 591</a> .                                                                                             |
| <a href="#">audit_flags(5)</a>   | Describe la sintaxis de la preselección de clases de auditoría, los prefijos para seleccionar sólo los eventos con fallos o sólo los eventos correctos, y los prefijos que modifican una preselección existente.                                                                                                                                                                                                  |
| <a href="#">audit.log(4)</a>     | Describe los nombres de archivos de auditoría binarios, la estructura interna de un archivo y la estructura de cada token de auditoría.                                                                                                                                                                                                                                                                           |
| <a href="#">audit_warn(1M)</a>   | Secuencia de comandos que notifica a un alias de correo electrónico cuando el servicio de auditoría encuentra una condición poco habitual al escribir los registros de auditoría. Puede personalizar esta secuencia de comandos para su ubicación a fin de advertir acerca de las condiciones que puedan requerir intervención manual. O bien, puede especificar cómo manejar dichas condiciones automáticamente. |
| <a href="#">auditconfig(1M)</a>  | Comando que recupera y establece parámetros de configuración de auditoría.<br><br>Escriba auditconfig sin opciones para obtener una lista de parámetros que se pueden recuperar y establecer.                                                                                                                                                                                                                     |

| Página de comando man           | Resumen                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">auditrecord(1M)</a> | Comando que muestra la definición de eventos de auditoría en el archivo <code>/etc/security/audit_event</code> . Para una salida de ejemplo, consulte <a href="#">“Cómo visualizar definiciones de registros de auditoría” en la página 615</a> .                                                                                                                                                                                                                                                                                                                          |
| <a href="#">auditreduce(1M)</a> | <p>Comando que selecciona posteriormente y fusiona registros de auditoría que se almacenan en formato binario. El comando puede fusionar los registros de auditoría de uno o más archivos de auditoría de entrada. Los registros permanecen en formato binario.</p> <p>Las opciones de mayúscula afectan la selección de archivos. Las opciones de minúscula afectan la selección de registros.</p>                                                                                                                                                                        |
| <a href="#">auditstat(1M)</a>   | Comando que muestra estadísticas de auditoría de núcleo. Por ejemplo, el comando puede mostrar el número de registros en la cola de auditoría de núcleo, el número de registros descartados y el número de registros de auditoría que los procesos de usuario generaron en el núcleo como resultado de llamadas del sistema.                                                                                                                                                                                                                                               |
| <a href="#">praudit(1M)</a>     | <p>Comando que lee los registros de auditoría en formato binario a partir de la entrada estándar y muestra los registros en un formato presentable. La entrada puede conducirse desde el comando <code>auditreduce</code> o desde un único archivo de auditoría o una lista de archivos de auditoría. La entrada también se puede generar con el comando <code>tail -0f</code> para un archivo de auditoría actual.</p> <p>Para una salida de ejemplo, consulte <a href="#">“Cómo visualizar el contenido de los archivos de auditoría binarios” en la página 620</a>.</p> |
| <a href="#">syslog.conf(4)</a>  | Archivo configurado para enviar resúmenes de texto de registros de auditoría para la utilidad <code>syslog</code> para el complemento <code>audit_syslog</code> .                                                                                                                                                                                                                                                                                                                                                                                                          |

## Perfiles de derechos para administración de auditoría

- Oracle Solaris proporciona perfiles de derechos para configurar el servicio de auditoría, para activar y desactivar el servicio, y para analizar la pista de auditoría. Para editar un archivo de configuración de auditoría se requieren privilegios de root.
- **Configuración de auditoría:** permite que un administrador configure los parámetros del servicio de auditoría y ejecute el comando `auditconfig`.
  - **Control de auditoría:** permite que un administrador inicie, refresque y desactive el servicio de auditoría y ejecute el comando `audit` para iniciar, refrescar o detener el servicio.
  - **Revisión de auditoría:** permite que un administrador analice registros de auditoría. Este perfil de derechos concede autorización para leer registros de auditoría con los comandos `praudit` y `auditreduce`. Este administrador también puede ejecutar el comando `auditstat`.
  - **Administrador del sistema:** incluye el perfil de derechos de revisión de auditoría. Un administrador con el perfil de derechos de administrador del sistema puede analizar los registros de auditoría.



Para configurar roles para manejar el servicio de auditoría, consulte [“Configuración inicial de RBAC \(mapa de tareas\)” en la página 168.](#)

## Auditoría y zonas de Oracle Solaris

Las zonas no globales se pueden auditar exactamente como se audita la zona global, o las zonas no globales pueden establecer sus propios indicadores, almacenamiento y políticas de auditoría.

Cuando todas las zonas se auditan de manera idéntica, los archivos `audit_class` y `audit_event` en la zona global proporcionan las asignaciones de clase-evento para auditoría en cada zona. La opción de política `+zonename` es útil para la selección posterior de registros por nombre de zona.

Las zonas se pueden auditar individualmente. Cuando la opción de política, `perzone`, se establece en la zona global, cada zona no global ejecuta su propio servicio de auditoría, gestiona su propia cola de auditoría y especifica el contenido y la ubicación de los registros de auditoría. Una zona no global también puede definir la mayoría de las opciones de la política de auditoría. No puede definir una política que afecte a todo el sistema, por lo que una zona no global no puede definir las políticas `ahlt` o `perzone`. Para más información, consulte [“Auditoría en un sistema con zonas de Oracle Solaris” en la página 561](#) y [“Cómo planificar auditoría en zonas” en la página 564.](#)

Para obtener más información sobre las zonas, consulte la [Parte II, “Zonas de Oracle Solaris” de Administración de Oracle Solaris 11.1: zonas de Oracle Solaris, zonas de Oracle Solaris 10 y gestión de recursos.](#)

## Archivos de configuración de auditoría y empaquetado

Los archivos de configuración de auditoría en Oracle Solaris se marcan en el paquete con el atributo de paquete `preserve=renamenew`. Este atributo mantiene cualquier modificación que realice en los archivos entre las actualizaciones. Para obtener información sobre los efectos de los valores `preserve`, consulte la página del comando `man pkg(5)`.

Estos archivos de configuración también se marcan con el atributo de paquete `overlay=allow`. Este atributo le permite crear su propio paquete que contiene estos archivos y reemplazar los archivos de Oracle Solaris con archivos de su paquete. Cuando se establece el atributo `overlay` en `true` en su paquete, los subcomandos `pkg`, como `verify`, `fix`, `revert`, etc., devolverán resultados en sus paquetes. Para obtener más información, consulte las páginas del comando `man pkg(1)` y `pkg(5)`.

## Clases de auditoría

Oracle Solaris define clases de auditoría como contenedores prácticos para un gran número de eventos de auditoría.

Puede reconfigurar clases de auditoría y realizar nuevas clases de auditoría. Los nombres de clase de auditoría puede tener un máximo de 8 caracteres de longitud. La descripción de clase está limitada a 72 caracteres. Se permite el uso de caracteres numéricos y no alfanuméricos. Para obtener más información, consulte la página del comando `man audit_class(4)` y “Cómo agregar una clase de auditoría” en la página 590.



---

**Precaución** – La clase `all` puede generar grandes cantidades de datos y llenar rápidamente los discos. Utilice la clase `all` sólo si se tienen motivos extraordinarios para auditar todas las actividades.

---

## Sintaxis de la clase de auditoría

Los eventos en una clase de auditoría se pueden auditar para determinar si la clase es correcta, si tiene fallos o ambas cosas.

- Sin un prefijo, una clase de eventos se audita para determinar si es correcta o si falló.
- Con un prefijo de signo más (+), se audita una clase de eventos únicamente para determinar si son correctos.
- Con un prefijo de signo menos (-), se audita una clase de los eventos únicamente para determinar si tienen fallos.
- Con un signo de intercalación (^) anterior a un prefijo o a un indicador de auditoría, se modifica una preselección actual. Por ejemplo,
  - Si `ot` está preseleccionado para el sistema, y la preselección de un usuario es `^ot`, dicho usuario no se audita para eventos en la clase `other`.
  - Si `+ot` está preseleccionado para el sistema, y la preselección de un usuario es `^+ot`, dicho usuario no se audita para eventos correctos en la clase `other`.
  - Si `-ot` está preseleccionado para el sistema, y la preselección de un usuario es `^-ot`, dicho usuario no se audita para eventos con fallos en la clase `other`.

Para revisar la sintaxis de la preselección de clases de auditoría, consulte la página del comando `man audit_flags(5)`.

Las clases de auditoría y sus prefijos se pueden especificar en los siguientes comandos:

- Como argumentos para las opciones del comando `auditconfig -setflags` y `-setnaflags`.
- Como valores del atributo `p_flags` para el complemento `audit_syslog`. Especifica el atributo como una opción para el comando `auditconfig -setplugin audit_syslog active`.
- Como valores para la opción `-K audit_flags=always-audit-flags:never-audit-flags` para los comandos `useradd`, `usermod`, `roleadd` y `rolemod`.
- Como valores para las propiedades `-always_audit` y `-never_audit` del comando `profiles`.

## Complementos de auditoría

Los complementos de auditoría especifican cómo manejar los registros de auditoría en la cola de auditoría. Los complementos de auditoría se especifican por nombre: `audit_binfile`, `audit_remote` y `audit_syslog` como argumentos para el comando `auditconfig -setplugin`. Los complementos se pueden especificar en detalle mediante los siguientes atributos:

- Complemento `audit_binfile`
  - Dónde enviar datos binarios (atributo - `p_dir`)
  - El espacio mínimo restante en un disco antes de que el administrador reciba una advertencia (atributo - `p_minfree`)
  - El tamaño máximo de un archivo de auditoría (atributo - `p_fsize`)
- Complemento `audit_remote`
  - Un servidor de auditoría autenticado remoto al que enviar datos de auditoría binarios (atributo - `p_hosts`)
  - El número de intentos para alcanzar un servidor de auditoría autenticado remoto (atributo - `p_retries`)
  - La cantidad de segundos entre intentos para alcanzar un servidor de auditoría autenticado remoto (atributo - `p_timeout`)
- Complemento `audit_syslog`
  - Una selección de resúmenes de textos de registros de auditoría que se deben enviar (atributo `syslog - p_flags`)
- Para todos los complementos, el número máximo de registros de auditoría que están en cola para el complemento (atributo - `qsize`)

Consulte las páginas del comando `man audit_binfile(5)`, `audit_remote(5)`, `audit_syslog(5)` y `auditconfig(1M)`.

## Servidor de auditoría remoto

El servidor de auditoría remoto (ARS) recibe los registros de auditoría por un enlace seguro desde los sistemas auditados y almacena los registros.

La recepción se basa en que se configure lo siguiente:

- Un dominio Kerberos con principios de auditoría específicos y un mecanismo GSS-API.
- El ARS con al menos un *grupo de conexión* configurado y activo.
- Al menos un sistema auditado en el grupo de conexión y un complemento `audit_remote` configurado y activo.

En la propiedad `group` del ARS, se especifica un grupo de conexión. Para la gestión de archivos, `group` puede limitar el tamaño del archivo de auditoría y especificar el espacio libre mínimo. El motivo principal para especificar diferentes grupos de conexiones es especificar diferentes ubicaciones de almacenamiento en el ARS, como se muestra en el [Ejemplo 28–19](#).

Para obtener más información sobre el ARS, consulte la página del comando `man arsd(5)`. Para obtener información de configuración del ARS, consulte las opciones `-setremote` en la página del comando `man auditconfig(1M)`.

Para configurar los sistemas auditados, consulte la página del comando `man audit_remote(5)` y la opción `-setplugin` en la página del comando `man auditconfig(1M)`.

## Política de auditoría

La política de auditoría determina si se agrega información adicional a la pista de auditoría.

Las siguientes políticas agregan tokens a los registros de auditoría: `arge`, `argv`, `group`, `path`, `seq`, `trail`, `windata_down`, `windata_up` y `zonename`. Las políticas `windata_down` y `windata_up` son utilizadas por la función Trusted Extensions de Oracle Solaris. Para obtener más información, consulte el [Capítulo 22, “Auditoría de Trusted Extensions \(descripción general\)” de Configuración y administración de Trusted Extensions](#).

Las políticas restantes no agregan tokens. La política `public` limita la auditoría de archivos públicos. La política `perzone` establece colas de auditoría independientes para zonas no globales. Las políticas `ahlt` y `cnt` determinan qué sucede cuando no se pueden enviar registros de auditoría. Para obtener más detalles, consulte “[Políticas de auditoría para eventos síncronos y asíncronos](#)” en la página 649.

Los efectos de las diferentes opciones de políticas de auditoría se describen en “[Comprensión de la política de auditoría](#)” en la página 571. Para obtener una descripción de las opciones de política de auditoría, consulte la opción `-setpolicy` en la página del comando `man auditconfig(1M)`. Para obtener una lista de las opciones de política disponibles, ejecute el comando `auditconfig -lspolicy`. Para la política actual, ejecute el comando `auditconfig -getpolicy`.

## Políticas de auditoría para eventos síncronos y asíncronos

Juntas, la política `ahlt` y la política `cnt` rigen lo que ocurre cuando la cola de auditoría está completa y no puede aceptar más eventos.

---

**Nota** – La política `cnt` o `ahlt` no se activa si la cola para al menos un complemento puede aceptar registros de auditoría.

---

Las políticas `cnt` y `ahlt` son independientes y están relacionadas. Las combinaciones de las políticas tienen los siguientes efectos:

- `-ahlt +cnt` es la política predeterminada que se envía. Este valor predeterminado le permite a un evento auditado ser procesado incluso si el evento no se puede registrar.  
 La política `-ahlt` indica que si un registro de auditoría de un evento asíncrono no se puede ubicar en la cola de auditoría de núcleo, el sistema contará los eventos y continuará el procesamiento. En la zona global, el contador `as_dropped` registra el recuento.  
 La política `+cnt` indica que si llega un evento síncrono y el evento no se puede ubicar en la cola de auditoría de núcleo, el sistema contará el evento y continuará el procesamiento. El contador `as_dropped` de la zona registra el recuento.  
 La configuración `-ahlt +cnt` se usa generalmente en sitios donde el procesamiento debe continuar, incluso si continuar con el procesamiento puede producir una pérdida de registros de auditoría. El campo `auditstat drop` muestra el número de registros de auditoría que se descartan en una zona.
- La política `+ahlt -cnt` indica que el procesamiento se detiene cuando un evento asíncrono no se puede agregar a la cola de auditoría de núcleo.  
 La política `+ahlt` indica que si un registro de auditoría de un evento asíncrono no se puede ubicar en la cola de auditoría de núcleo, todo el procesamiento se detiene. El sistema entrará en estado de alerta. El evento asíncrono no estará en la cola de auditoría y se debe recuperar de punteros en la pila de llamadas.  
 La política `-cnt` indica que si un evento síncrono no se puede ubicar en la cola de auditoría de núcleo, el subproceso que intenta entregar el evento se bloqueará. El subproceso se coloca en una cola inactiva hasta que el espacio de auditoría pase a estar disponible. Ningún recuento se mantiene. Los programas podrían parecer bloquearse hasta que el espacio de auditoría pase a estar disponible.  
 La configuración `+ahlt -cnt` se usa generalmente en sitios donde un registro de cada evento de auditoría tiene prioridad sobre disponibilidad del sistema. Los programas parecerán bloquearse hasta que el espacio de auditoría pase a estar disponible. El campo `auditstat wblk` muestra el número de veces que los subprocesos se bloquearon.

Sin embargo, si un evento asíncrono se produce, el sistema entrará en estado de alerta, lo que lleva a una interrupción. La cola de núcleo de eventos de auditoría se puede recuperar manualmente de un volcado de bloqueo guardado. El evento asíncrono no estará en la cola de auditoría y se debe recuperar de punteros en la pila de llamadas.

- La política `-ahlt -cnt` indica que si un evento asíncrono no se puede ubicar en la cola de auditoría de núcleo, el evento se contará y continuará el procesamiento. Cuando un evento síncrono no se puede ubicar en la cola de auditoría de núcleo, el subproceso que intenta entregar el evento se bloqueará. El subproceso se coloca en una cola inactiva hasta que el espacio de auditoría pase a estar disponible. Ningún recuento se mantiene. Los programas podrían parecer bloquearse hasta que el espacio de auditoría pase a estar disponible.

La configuración `-ahlt -cnt` se usa generalmente en los sitios donde el registro de todos los eventos de auditoría síncronos tiene prioridad sobre alguna posible pérdida de registros de auditoría asíncronos. El campo `auditstat wblk` muestra el número de veces que los subprocesos se bloquearon.

- La política `+ahlt +cnt` indica que si un evento asíncrono no se puede ubicar en la cola de auditoría de núcleo, el sistema entrará en estado de alerta. Si un evento síncrono no se puede ubicar en la cola de auditoría de núcleo, el sistema contará el evento y continuará el procesamiento.

## Características del proceso de auditoría

Las siguientes características de auditoría se definen en el primer inicio de sesión:

- **Máscara de preselección de procesos:** una combinación de la máscara de auditoría en todo el sistema y la máscara de auditoría específica de usuario, si una máscara de auditoría de usuario se ha especificado. Cuando un usuario inicia sesión, el proceso de inicio de sesión combina las clases preseleccionadas para establecer la *máscara de preselección de proceso* para los procesos del usuario. La máscara de preselección de proceso especifica los sucesos que generan registros de auditoría.

El siguiente algoritmo describe el modo en que el sistema obtiene la máscara de preselección de proceso del usuario:

```
(system-wide default flags + always-audit-classes) - never-audit-classes
```

Agregue clases de auditoría en todo el sistema de los resultados del comando `auditconfig -getflags` a las clases del valor *always-audit-classes* para la palabra clave `always_audit` del usuario. Luego, reste del total las clases del campo *nunca\_auditar\_clases* del usuario. Consulte también la página del comando `man audit_flags(5)`.

- **ID de usuario de auditoría:** un proceso adquiere un ID de usuario de auditoría inmutable cuando el usuario inicia sesión. Este ID es heredado por todos los procesos secundarios comenzados por el proceso inicial del usuario. El ID de usuario de auditoría ayuda a aplicar responsabilidad. Incluso después de que un usuario asume un rol, el ID del usuario de

auditoría sigue siendo el mismo. El ID del usuario de auditoría que se guarda en cada registro de auditoría le permite siempre rastrear las acciones hasta el usuario de inicio de sesión.

- **ID de sesión de auditoría:** el ID de sesión de auditoría se asigna cuando se inicia sesión. Este ID de sesión es heredado por todos los procesos secundarios.
- **ID de terminal:** para un inicio de sesión local, el ID de terminal está formado por la dirección IP del sistema local seguido por un número único que identifica el dispositivo físico en el que inició sesión el usuario. La mayoría de las veces, el inicio de sesión es a través de la consola. El número que corresponde al dispositivo de la consola es 0, 0. Para un inicio de sesión remoto, el ID de terminal consta de una dirección IP del host remoto seguido del número de puerto remoto y el número de puerto local.

## Pista de auditoría

La *pista de auditoría* contiene archivos de auditoría binarios. La pista se crea mediante el complemento `audit_binfile`. El servicio de auditoría recopila los registros en la cola de auditoría y los envía al complemento, que los escribe en el disco.

## Convenciones de nombres de archivos de auditoría binarios

El complemento `audit_binfile` crea archivos de auditoría binarios. Cada archivo de auditoría binario es una recopilación de registros autocontenidos. El nombre del archivo identifica el período durante el cual los registros se generaron y el sistema que los generó. Las indicaciones de hora que indican el período de tiempo se especifican en formato de hora universal coordinada (UTC) para asegurarse de que se muestren en orden correcto, incluso entre zonas horarias.

Para obtener más información, consulte la página del comando `man audit.log(4)`. Para obtener ejemplos de nombres de archivos de auditoría abiertos y cerrados, consulte “[Cómo depurar un archivo de auditoría not\\_terminated](#)” en la [página 622](#).

## Estructura de registro de auditoría

Un registro de auditoría es una secuencia de tokens de auditoría. Cada token de auditoría contiene información del evento, como ID de usuario, hora y fecha. Un token header comienza un registro de auditoría, y un token opcional trailer, lo concluye. Otras tokens de auditoría contienen información relevante para el evento de auditoría. En la siguiente figura se muestra un registro de auditoría de núcleo típico y un registro de auditoría de nivel de usuario típico.

FIGURA 29-1 Estructuras de registros de auditoría típicas

|                 |                |
|-----------------|----------------|
| token header    | token header   |
| token arg       | token subject  |
| tokens de datos | [otros tokens] |
| token subject   | token return   |
| token return    |                |

## Análisis de registro de auditoría

El análisis de registro de auditoría incluye la selección posterior de los registros de la pista de auditoría. Puede utilizar uno de estos dos métodos para analizar los datos binarios recopilados.

- Puede utilizar para ello el comando `praudit`. Las opciones para el comando proporcionan diferentes salidas de texto. Por ejemplo, el comando `praudit -x` proporciona XML para introducir en secuencias de comandos y exploradores. La salida de `praudit` no incluye campos cuyo único propósito es ayudar a analizar los datos binarios. Tenga en cuenta que el orden y el formato de la salida de `praudit` no están garantizados entre las versiones de Oracle Solaris.

Para ver ejemplos de una salida `praudit`, consulte [“Cómo visualizar el contenido de los archivos de auditoría binarios” en la página 620](#).

Para obtener ejemplos de una salida `praudit` para cada token de auditoría, consulte los tokens individuales en [“Formatos de token de auditoría” en la página 653](#).

- Puede escribir un programa para analizar el flujo de datos binarios. El programa deben tener en cuenta las variantes de un registro de auditoría. Por ejemplo, la llamada del sistema `ioctl()` crea un registro de auditoría para "nombre de archivo incorrecto". Este registro contiene diferentes tokens del registro de auditoría `ioctl()` para "descriptor de archivo no válido".
  - Para obtener una descripción del orden de los datos binarios en cada token de auditoría, consulte la página del comando `man audit.log(4)`.
  - Para valores del manifiesto, consulte el archivo `/usr/include/bsm/audit.h`.
  - Para ver el orden de los tokens en un registro de auditoría, use el comando `auditrecord`. La salida del comando `auditrecord` incluye los diferentes tokens para los diferentes valores de manifiesto. Los corchetes (`[]`) indican que un token de auditoría es opcional. Para obtener más información, consulte la página del comando `man auditrecord(1M)`.



# Formatos de token de auditoría

Cada token de auditoría tienen un identificador de tipo de token, que está seguido por los datos específicos para el token. La siguiente tabla muestra los nombres de token con una breve descripción de cada uno. Los tokens obsoletos se mantienen por motivos de compatibilidad con las versiones anteriores de Solaris.

TABLA 29-1 Tokens de auditoría para auditoría

| Nombre de token         | Descripción                                                                          | Para obtener más información                                     |
|-------------------------|--------------------------------------------------------------------------------------|------------------------------------------------------------------|
| <code>acl</code>        | Información de entrada de control de acceso (ACE) y lista de control de acceso (ACL) | <a href="#">“Token <code>acl</code>” en la página 654</a>        |
| <code>arbitrary</code>  | Datos con información de formato y de tipo                                           | Consulte la página del comando <code>man audit.log(4)</code> .   |
| <code>argument</code>   | Valor de argumento de llamada de sistema                                             | <a href="#">“Token <code>argument</code>” en la página 655</a>   |
| <code>attribute</code>  | Información de vnode de archivo                                                      | <a href="#">“Token <code>attribute</code>” en la página 655</a>  |
| <code>cmd</code>        | Argumentos de comandos y variables de entornos                                       | <a href="#">“Token <code>cmd</code>” en la página 655</a>        |
| <code>exec_args</code>  | Argumentos de llamada de sistema <code>exec</code>                                   | <a href="#">“Token <code>exec_args</code>” en la página 656</a>  |
| <code>exec_env</code>   | Variables de entorno de llamada de sistema <code>exec</code>                         | <a href="#">“Token <code>exec_env</code>” en la página 656</a>   |
| <code>exit</code>       | Información de salida de programa                                                    | Consulte la página del comando <code>man audit.log(4)</code> .   |
| <code>file</code>       | Información de archivo de auditoría                                                  | <a href="#">“Token <code>file</code>” en la página 656</a>       |
| <code>fmri</code>       | Indicador de recursos de gestión de estructura                                       | <a href="#">“Token <code>fmri</code>” en la página 657</a>       |
| <code>group</code>      | Información de grupos de procesos                                                    | <a href="#">“Token <code>group</code>” en la página 657</a>      |
| <code>header</code>     | Indica el comienzo del registro de auditoría                                         | <a href="#">“Token <code>header</code>” en la página 657</a>     |
| <code>ip</code>         | Información de encabezado IP                                                         | Consulte la página del comando <code>man audit.log(4)</code> .   |
| <code>ip_address</code> | Dirección de Internet                                                                | <a href="#">“Token <code>ip_address</code>” en la página 658</a> |
| <code>ip_port</code>    | Dirección de puerto de Internet                                                      | <a href="#">“Token <code>ip_port</code>” en la página 658</a>    |
| <code>ipc</code>        | Información de System V IPC                                                          | <a href="#">“Token <code>ipc</code>” en la página 658</a>        |
| <code>IPC_perm</code>   | Información de acceso de objetos de System V IPC                                     | <a href="#">“Token <code>IPC_perm</code>” en la página 659</a>   |
| <code>opaque</code>     | Datos no estructurados (sin especificar formato)                                     | Consulte la página del comando <code>man audit.log(4)</code> .   |
| <code>path</code>       | Información de ruta                                                                  | <a href="#">“Token <code>path</code>” en la página 659</a>       |
| <code>path_attr</code>  | Información de ruta de acceso                                                        | <a href="#">“Token <code>path_attr</code>” en la página 659</a>  |
| <code>privilege</code>  | Información de conjunto de privilegios                                               | <a href="#">“Token <code>privilege</code>” en la página 660</a>  |
| <code>process</code>    | Información de proceso                                                               | <a href="#">“Token <code>process</code>” en la página 660</a>    |

TABLA 29-1 Tokens de auditoría para auditoría (Continuación)

| Nombre de token              | Descripción                                                   | Para obtener más información                                                                                              |
|------------------------------|---------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------|
| return                       | Estado de llamada de sistema                                  | “Token return” en la página 660                                                                                           |
| sequence                     | Número de secuencia                                           | “Token sequence” en la página 661                                                                                         |
| socket                       | Direcciones y tipo de socket                                  | “Token socket” en la página 661                                                                                           |
| subject                      | Información de "subject" (tiene el mismo formato que process) | “Token subject” en la página 661                                                                                          |
| text                         | Cadena ASCII                                                  | “Token text” en la página 662                                                                                             |
| trailer                      | Indica el final del registro de auditoría                     | “Token trailer” en la página 662                                                                                          |
| use of authorization         | Uso de autorización                                           | “Token use of authorization” en la página 662                                                                             |
| use of privilege             | Uso de privilegio                                             | “Token use of privilege” en la página 662                                                                                 |
| user                         | ID de usuario y nombre de usuario                             | “Token user” en la página 663                                                                                             |
| xclient                      | Identificación de los clientes X                              | “Token xclient” en la página 663                                                                                          |
| zonename                     | Nombre de la zona                                             | “Token zonename” en la página 663                                                                                         |
| Tokens de Trusted Extensions | Label e información de sistema de ventanas X                  | Consulte “Referencia de auditoría de Trusted Extensions” de <i>Configuración y administración de Trusted Extensions</i> . |

Los siguientes tokens son obsoletos:

- liaison
- host
- tid

Para obtener más información sobre tokens obsoletos, consulte el material de referencia para la versión que incluye el token.

Un registro de auditoría comienza siempre con un token header. El token header indica dónde comienza el registro de auditoría en la pista de auditoría. En el caso de eventos atribuibles, los tokens subject y process hacen referencia a los valores del proceso que causaron el evento. En el caso de eventos no atribuibles, el token process hace referencia al sistema.

## Token acl

El token acl tiene dos maneras de registrar información sobre entradas de control de acceso (ACEs) para un sistema de archivos ZFS y listas de control de acceso (ACLs) para un sistema de archivos UFS.

Cuando el token `acl` está registrado para un sistema de archivos UFS, el comando `praudit -x` muestra los campos de la siguiente manera:

```
<acl type="1" value="root" mode="6"/>
```

Cuando el token `acl` está registrado para un conjunto de datos ZFS, el comando `praudit -x` muestra los campos de la siguiente manera:

```
<acl who="root" access_mask="default" flags="-i,-R" type="2"/>
```

## Token argument

El token `argument` contiene información sobre los argumentos de una llamada del sistema: el número de argumentos de la llamada del sistema, el valor de los argumento y una descripción opcional. Este token permite un argumento de llamada de sistema de número entero de 32 bits en un registro de auditoría.

El comando `praudit -x` muestra los campos del token `argument` de la siguiente manera:

```
<argument arg-num="2" value="0x5401" desc="cmd"/>
```

## Token attribute

El token `attribute` contiene información del `vnode` del archivo.

El token `attribute` por lo general acompaña un token `path`. El token `attribute` se produce durante búsquedas de ruta. Si ocurre un error de búsqueda de ruta, no hay un `vnode` disponible para obtener la información de archivo necesaria. Por lo tanto, el token `attribute` no se encuentra incluido como parte del registro de auditoría. El comando `praudit -x` muestra los campos del token `attribute` de la siguiente manera:

```
<attribute mode="20620" uid="root" gid="tty" fsid="0" nodeid="9267" device="108233"/>
```

## Token cmd

El token `cmd` registra la lista de argumentos y la lista de variables del entorno asociadas con un comando.

El comando `praudit -x` muestra los campos del token `cmd`. El siguiente es un token `cmd` truncado. La línea se ajusta con fines de visualización.

```
<cmd><arg>WINDOWID=6823679</arg>
<arg>COLORTERM=gnome-terminal</arg>
<arg>...LANG=C</arg>...<arg>HOST=machine1</arg>
<arg>LPDEST=printer1</arg>...</cmd>
```

## Token `exec_args`

El token `exec_args` registra los argumentos en una llamada de sistema `exec()`.

El comando `praudit -x` muestra los campos del token `exec_args` de la siguiente manera:

```
<exec_args><arg>/usr/bin/sh</arg><arg>/usr/bin/hostname</arg></exec_args>
```

---

**Nota** – El token `exec_args` sólo se muestra cuando está activada la opción de política de auditoría `argv`.

---

## Token `exec_env`

El token `exec_env` registra las variables de entorno actuales en una llamada de sistema `exec()`.

El comando `praudit -x` muestra los campos del token `exec_env`. La línea se ajusta con fines de visualización.

```
<exec_env><env>_=/usr/bin/hostname</env>
<env>LANG=C</env><env>PATH=/usr/bin:/usr/ucb</env>
<env><env>LOGNAME=jdoe</env><env>USER=jdoe</env>
<env>DISPLAY=:0</env><env>SHELL=/bin/csh</env>
<env>HOME=/home/jdoe</env><env>PWD=/home/jdoe</env><env>TZ=US/Pacific</env>
</exec_env>
```

---

**Nota** – El token `exec_env` sólo se muestra cuando está activada la opción de política de auditoría `arge`.

---

## Token `file`

El token `file` es un token especial que marca el inicio de un nuevo archivo de auditoría y el fin de un antiguo archivo de auditoría cuando se desactiva el archivo antiguo. El token `file` inicial identifica el archivo anterior en la pista de auditoría. El token `file` final identifica el archivo siguiente en la pista de auditoría. Estos tokens “unen” archivos de auditoría sucesivos en una pista de auditoría.

El comando `praudit -x` muestra los campos del token `file`. La línea se ajusta con fines de visualización.

```
<file iso8601="2009-04-08 14:18:26.200 -07:00">
/var/audit/machine1/files/20090408211826.not_terminated.machine1</file>
```

## Token fmri

El token `fmri` registra el uso de un indicador de recursos de gestión de fallos (FMRI). Para obtener más información, consulte la página de comando `man smf(5)`

El comando `praudit -x` muestra el contenido del token `fmri`:

```
<fmri service_instance="svc:/system/cryptosvc">/fmri>
```

## Token group

El token `group` registra las entradas del grupo de la credencial del proceso.

El comando `praudit -x` muestra los campos del token `groups` de la siguiente manera:

```
<group><gid>staff</gid><gid>other</gid></group>
```

---

**Nota** – El token `group` es una salida sólo cuando la opción de política de auditoría `group` está activa.

---

## Token header

El token `header` es especial en cuanto marca el inicio de un registro de auditoría. El token `header` se combina con el token `trailer` para encerrar todos los tokens en el registro.

De manera poco frecuente, un token `header` puede incluir uno o más modificadores de eventos:

- `fe` indica un evento de auditoría con errores
- `fp` indica el uso con errores de privilegios
- `na` indica un evento no atribuible
 

```
header,52,2,system booted,na,mach1,2011-10-10 10:10:20.564 -07:00
```
- `rd` indica que los datos se leen del objeto
- `sp` indica el uso correcto del privilegio
 

```
header,120,2,exit(2),sp,mach1,2011-10-10 10:10:10.853 -07:00
```
- `wr` indica que los datos se escriben en el objeto

El comando `praudit` muestra el token `header` de la siguiente manera:

```
header,756,2,execve(2),,machine1,2010-10-10 12:11:10.209 -07:00
```

El comando `praudit -x` muestra los campos del token `header` al comienzo del registro de auditoría. La línea se ajusta con fines de visualización.

```
<record version="2" event="execve(2)" host="machine1"
iso8601="2010-10-10 12:11:10.209 -07:00">
```

## Token ip address

El token ip address contiene una dirección de protocolo de Internet (dirección IP). La dirección IP se pueden mostrar en formato IPv4 o IPv6. La dirección IPv4 utiliza 4 bytes. La dirección IPv6 utiliza 1 byte para describir el tipo de dirección y 16 bytes para describir la dirección.

El comando `praudit -x` muestra el contenido del token ip address de la siguiente manera:

```
<ip_address>machine1</ip_address>
```

## Token ip port

El token ip port contiene las direcciones de los puertos TCP o UDP.

El comando `praudit` muestra el token ip port de la siguiente manera:

```
ip port,0xf6d6
```

## Token ipc

El token ipc contiene el identificador de mensaje de System V IPCe, los indicadores de semáforo o el identificador de memoria compartida usado por el emisor de llamada para identificar un objeto IPC determinado.

---

**Nota** – Los identificadores del objeto IPC infringen la naturaleza sin contexto de los tokens de auditoría. Ningún “nombre” global identifica de forma exclusiva objetos IPC. En su lugar, los objetos IPC se identifican por sus identificadores. Los identificadores sólo son válidos durante el tiempo que los objetos IPC están activos. Sin embargo, la identificación de los objetos IPC no debería suponer ningún problema. Los mecanismos de System V IPC rara vez se utilizan, y todos los mecanismos comparten la misma clase de auditoría.

---

La siguiente tabla muestra los posibles valores del campo de tipo de objeto IPC. Los valores se definen en el archivo `/usr/include/bsm/audit.h`.

TABLA 29-2 Valores para el campo de tipo de objeto IPC

| Nombre     | Valor | Descripción                      |
|------------|-------|----------------------------------|
| AU_IPC_MSG | 1     | Objeto de mensaje IPC            |
| AU_IPC_SEM | 2     | Objeto de semáforo IPC           |
| AU_IPC_SHM | 3     | Objeto de memoria compartida IPC |

El comando `praudit -x` muestra los campos del token `ipc` de la siguiente manera:

```
<IPC ipc-type="shm" ipc-id="15"/>
```

## Token IPC\_perm

El token `IPC_perm` contiene una copia de los permisos de acceso de System V IPC. Este token se agrega a los registros de auditoría generados por los eventos de memoria compartida IPC, los eventos de semáforo IPC y los eventos de mensajes IPC.

El comando `praudit -x` muestra los campos del token `IPC_perm`. La línea se ajusta con fines de visualización.

```
<IPC_perm uid="jdoe" gid="staff" creator-uid="jdoe"
creator-gid="staff" mode="100600" seq="0" key="0x0"/>
```

Los valores se toman de la estructura de `IPC_perm` asociada con el objeto IPC.

## Token path

El token de auditoría `path` contiene información sobre la ruta de acceso para un objeto.

El comando `praudit -x` muestra el contenido del token `path`:

```
<path>/export/home/srv/.xsession-errors</path>
```

## Token path\_attr

El token de auditoría `path_attr` contiene información sobre la ruta de acceso para un objeto. La ruta de acceso especifica la secuencia de los objetos de archivo de atributos en el objeto de token `path`. Las llamadas de sistema, como `openat()`, permiten acceder a los archivos de atributos. Para obtener más información acerca de los objetos de archivos de atributos, consulte la página del comando `man fsattr(5)`.

El comando `praudit` muestra el token `path_attr` de la siguiente manera:

```
path_attr,1,attr_file_name
```

## Token privilege

El token `privilege` registra el uso de privilegios en un proceso. El token `privilege` no registra privilegios en la configuración básica. Si un privilegio se ha eliminado del conjunto básico por una acción administrativa, entonces la utilización de ese privilegio se registra. Para obtener más información sobre los privilegios, consulte [“Privilegios \(descripción general\)” en la página 144](#)

El comando `praudit -x` muestra los campos del token `privilege`.

```
<privilege set-type="Inheritable">ALL</privilege>
```

## Token process

El token `process` contiene información acerca del usuario asociado con un proceso, como el destinatario de una señal.

El comando `praudit -x` muestra los campos del token `process`. La línea se ajusta con fines de visualización.

```
<process audit-uid="-2" uid="root" gid="root" ruid="root"
rgid="root" pid="567" sid="0" tid="0 0 0.0.0.0"/>
```

## Token return

El token `return` contiene el estado de devolución de la llamada de sistema (`u_error`) y el valor de devolución de proceso (`u_rval1`).

El token `return` siempre se devuelve como parte de los registros de auditoría generadas por el núcleo para las llamadas de sistema. En la auditoría de la aplicación, este token indica el estado de salida y otros valores de devolución.

El comando `praudit` muestra el token `return` para una llamada de sistema de la siguiente manera:

```
return,failure: Operation now in progress,-1
```

El comando `praudit -x` muestra los campos del token `return` de la siguiente manera:

```
<return errval="failure: Operation now in progress" retval="-1/">
```



## Token sequence

El token sequence contiene un número de secuencia. El número de secuencia se incrementa cada vez que un registro de auditoría se agregue a la pista de auditoría. Este token es útil para la depuración.

El comando `praudit -x` muestra el contenido del token sequence:

```
<sequence seq-num="1292"/>
```

---

**Nota** – El token sequence sólo se muestra cuando está activada la opción de política de auditoría seq.

---

## Token socket

El token socket contiene información que describe un socket de Internet. En algunos casos, el token incluye solamente el puerto remoto y la dirección IP remota.

El comando `praudit` muestra esta instancia del token socket de la siguiente manera:

```
socket,0x0002,0x83b1,localhost
```

El token ampliado agrega información, incluidos el tipo de socket e información sobre el puerto local.

El comando `praudit -x` muestra esta instancia del token socket de la siguiente manera. La línea se ajusta con fines de visualización.

```
<socket sock_domain="0x0002" sock_type="0x0002" lport="0x83cf"
laddr="example1" fport="0x2383" faddr="server1.Subdomain.Domain.COM"/>
```

## Token subject

El token subject describe un usuario que lleva a cabo o intenta llevar a cabo una operación. El formato es el mismo que el del token process.

El token subject siempre se devuelve como parte de los registros de auditoría generados por el núcleo para las llamadas de sistema. El comando `praudit` muestra el token subject de la siguiente manera:

```
subject,jdoe,root,root,root,root,1631,1421584480,8243 65558 machine1
```

El comando `praudit -x` muestra los campos del token subject. La línea se ajusta con fines de visualización.

```
<subject audit-uid="jdoe" uid="root" gid="root" ruid="root"
rgid="root" pid="1631" sid="1421584480" tid="8243 65558 machine1"/>
```

## Token text

El token text contiene una cadena de texto.

El comando `praudit -x` muestra el contenido del token text:

```
<text>booting kernel</text>
```

## Token trailer

Los dos tokens, header y trailer, son especiales en cuanto distinguen los puntos finales de un registro de auditoría y encierran todos los demás tokens. Un token header comienza un registro de auditoría. Un token trailer finaliza un registro de auditoría. El token trailer es un token opcional. El token trailer se agrega como el último token de cada registro sólo cuando la opción de política de auditoría `trail` está configurada.

Cuando un registro de auditoría se genera cuando los ubicadores están desactivados, el comando `auditreduce` puede verificar que el ubicador haga referencia correctamente al encabezado del registro. El token trailer admite búsquedas hacia atrás en la pista de auditoría.

El comando `praudit` muestra el token trailer de la siguiente manera:

```
trailer,136
```

## Token use of authorization

El token use of authorization registra el uso de autorización.

El comando `praudit` muestra el token use of authorization de la siguiente manera:

```
use of authorization,solaris.role.delegate
```

## Token use of privilege

El token use of privilege registra el uso de privilegio.

El comando `praudit -x` muestra los campos del token use of privilege de la siguiente manera:

```
<use_of_privilege result="successful use of priv">proc_setid</use_of_privilege>
```

## Token user

El token user registra el nombre de usuario y el ID de usuario. Este token está presente si el nombre de usuario es diferente del emisor de la llamada.

El comando `praudit -x` muestra los campos del token user de la siguiente manera:

```
<user uid="123456" username="tester1"/>
```

## Token xclient

El token xclient contiene el número de conexiones de cliente al servidor X.

El comando `praudit -x` muestra el contenido del token xclient de la siguiente manera:

```
<X_client>15</X_client>
```

## Token zonename

El token zonename registra la zona en la que ocurrió el evento de auditoría. La cadena “global” indica los eventos de auditoría que se producen en la zona global.

El comando `praudit -x` muestra el contenido del token zonename:

```
<zone name="graphzone"/>
```



# Glosario

---

|                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>AES</b>                        | Advanced Encryption Standard. Una técnica de cifrado de datos en bloques de 128 bits simétricos. En octubre de 2000, el gobierno de los Estados Unidos adoptó la variante Rijndael del algoritmo como estándar de cifrado. AES sustituye el cifrado <a href="#">principal de usuario</a> como estándar gubernamental.                                                                                                                                                                     |
| <b>algoritmo</b>                  | Un algoritmo criptográfico. Se trata de un procedimiento informático establecido que realiza el cifrado o el hashing de una entrada.                                                                                                                                                                                                                                                                                                                                                      |
| <b>algoritmo criptográfico</b>    | Consulte <a href="#">algoritmo</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>almacén de claves</b>          | Un almacén de claves contiene contraseñas, frases de contraseña, certificados y otros objetos de autenticación para que recuperen las aplicaciones. Un almacén de claves puede ser específico para una tecnología o puede ser una ubicación que utilizan varias aplicaciones.                                                                                                                                                                                                             |
| <b>aplicación con privilegios</b> | Una aplicación que puede sustituir los controles del sistema. La aplicación comprueba los atributos de seguridad, como UID, GID, autorizaciones o privilegios específicos.                                                                                                                                                                                                                                                                                                                |
| <b>archivo de ticket</b>          | Consulte <a href="#">caché de credenciales</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>archivo intermedio</b>         | Un archivo intermedio contiene una copia cifrada de la clave maestra para el KDC. Esta clave maestra se utiliza cuando un servidor se reinicia para autenticar automáticamente el KDC antes de que inicie los procesos kadmind y krb5kdc. Dado que el archivo intermedio incluye la clave maestra, el archivo y sus copias de seguridad deben mantenerse en un lugar seguro. Si el cifrado está en peligro, la clave podría utilizarse para acceder o modificar la base de datos del KDC. |
| <b>archivo keytab</b>             | Un archivo de tabla de claves que contiene una o varias claves (principales). Un host o servicio utiliza un archivo keytab de la misma manera que un usuario utiliza una contraseña.                                                                                                                                                                                                                                                                                                      |
| <b>archivos de auditoría</b>      | Registros de auditoría binarios. Los archivos de auditoría se almacenan de manera independiente en un sistema de archivos de auditoría.                                                                                                                                                                                                                                                                                                                                                   |
| <b>asignación de dispositivos</b> | Protección de dispositivos en el nivel de usuario. La asignación de dispositivos restringe el uso exclusivo de un dispositivo a un usuario a la vez. Los datos del dispositivo se depuran antes de volver a utilizar el dispositivo. Las autorizaciones se pueden utilizar para limitar quién tiene permiso para asignar un dispositivo.                                                                                                                                                  |

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>atributos de seguridad</b>   | En RBAC, sustituciones a la política de seguridad que permiten que un comando administrativo se ejecute correctamente al ser ejecutado por un usuario y no por un superusuario. En el modelo de superusuario, los programas <code>setuid</code> y <code>setgid</code> son atributos de seguridad. Cuando estos atributos se aplican a un comando, el comando se ejecuta correctamente sin importar quién lo ejecuta. En el modelo de privilegios, los atributos de seguridad son privilegios. Cuando un privilegio se otorga a un comando, el comando se ejecuta correctamente. El modelo de privilegios es compatible con el modelo de superusuario, ya que el modelo de privilegios reconoce también los programas <code>setuid</code> y <code>setgid</code> como atributos de seguridad. |
| <b>autenticación</b>            | Proceso de verificación de la identidad reclamada de un principal.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>autenticador</b>             | Los clientes transfieren autenticadores al solicitar tickets (desde un KDC) y servicios (desde un servidor). Contienen información que se genera mediante una clave de sesión conocida sólo por el cliente y el servidor y que se puede verificar como de origen reciente, lo cual indica que la transacción es segura. Cuando se utiliza con un ticket, un autenticador sirve para autenticar un principal de usuario. Un autenticador incluye el nombre de principal del usuario, la dirección IP del host del usuario y una indicación de hora. A diferencia de un ticket, un autenticador se puede utilizar sólo una vez, generalmente, cuando se solicita acceso a un servicio. Un autenticador se cifra mediante la clave de sesión para ese cliente y ese servidor.                  |
| <b>autorización</b>             | <ol style="list-style-type: none"> <li>1. En Kerberos, el proceso para determinar si un principal puede utilizar un servicio, a qué objetos puede acceder el principal y el tipo de acceso permitido para cada objeto.</li> <li>2. En el control de acceso basado en roles (RBAC), un permiso que se puede asignar a un rol o a un usuario (o que está incrustado en un perfil de derechos) para realizar una clase de acciones que, de lo contrario, están prohibidas por la política de seguridad.</li> </ol>                                                                                                                                                                                                                                                                             |
| <b>Blowfish</b>                 | Algoritmo cifrado de bloques simétricos con una clave de tamaño variable que va de 32 a 448 bits. Bruce Schneier, su creador, afirma que Blowfish se optimiza en el caso de aplicaciones en que la clave se modifica con poca frecuencia.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>caché de credenciales</b>    | Un espacio de almacenamiento (generalmente, un archivo) que contiene credenciales recibidas del KDC.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>cifrado de clave privada</b> | En el cifrado de clave privada, el remitente y el receptor utilizan la misma clave para el cifrado. Consulte también <a href="#">cifrado de clave pública</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>cifrado de clave pública</b> | Un esquema de cifrado en el que cada usuario tiene dos claves, una clave pública y una clave privada. En el cifrado de clave pública, el remitente utiliza la clave pública del receptor para cifrar el mensaje y el receptor utiliza una clave privada para descifrarlo. El servicio Kerberos es un sistema de clave privada. Consulte también <a href="#">cifrado de clave privada</a> .                                                                                                                                                                                                                                                                                                                                                                                                  |

|                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|--------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>clave</b>                   | <p>1. Generalmente, uno de los dos tipos principales de claves:</p> <ul style="list-style-type: none"> <li>■ <i>Clave simétrica</i>: una clave de cifrado que es idéntica a la clave de descifrado. Las claves simétricas se utilizan para cifrar archivos.</li> <li>■ <i>Claves asimétrica o clave pública</i>: una clave que se utiliza en algoritmos de clave pública, como Diffie-Hellman o RSA. Las claves públicas incluyen una clave privada que sólo conoce un usuario, una clave pública utilizada por el servidor o recurso general y un par de claves privada-pública que combina ambas. La clave privada también se denomina clave <i>secreta</i>. La clave pública también se denomina clave <i>compartida</i> o clave <i>común</i>.</li> <li>■ 2. Una entrada (nombre de principal) en un archivo keytab. Consulte también <a href="#">archivo keytab</a>.</li> </ul> <p>3. En Kerberos, una clave de cifrado, que puede ser de tres tipos:</p> <ul style="list-style-type: none"> <li>■ <i>Clave privada</i>: una clave de cifrado que comparten un principal y el KDC, y que se distribuye fuera de los límites del sistema. Consulte también <a href="#">clave privada</a>.</li> <li>■ <i>Clave de servicio</i>: esta clave tiene el mismo propósito que la clave privada, pero la utilizan servidores y servicios. Consulte también <a href="#">clave de servicio</a>.</li> <li>■ <i>Clave de sesión</i>: una clave de cifrado temporal que se utiliza entre dos principales y cuya duración se limita a la duración de una única sesión de inicio. Consulte también <a href="#">clave de sesión</a>.</li> </ul> |
| <b>clave de servicio</b>       | Una clave de cifrado que se comparte entre un principal de servicio y el KDC, y se distribuye fuera de los límites del sistema. Consulte también <a href="#">clave</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>clave de sesión</b>         | Una clave generada por el servicio de autenticación o el servicio de otorgamiento de tickets. Una clave de sesión se genera para proporcionar transacciones seguras entre un cliente y un servicio. La duración de una clave de sesión está limitada a una única sesión de inicio. Consulte también <a href="#">clave</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>clave privada</b>           | Una clave que se asigna a cada principal de usuario y que sólo conocen el usuario del principal y el KDC. Para los principales de usuario, la clave se basa en la contraseña del usuario. Consulte también <a href="#">clave</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>clave secreta</b>           | Consulte <a href="#">clave privada</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>cliente</b>                 | <p>De manera restringida, un proceso que utiliza un servicio de red en nombre de un usuario; por ejemplo, una aplicación que utiliza rlogin. En algunos casos, un servidor puede ser el cliente de algún otro servidor o servicio.</p> <p>De manera más amplia, un host que: a) recibe una credencial de Kerberos y b) utiliza un servicio proporcionado por un servidor.</p> <p>Informalmente, un principal que utiliza un servicio.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>confidencialidad</b>        | Consulte <a href="#">privacidad</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>conjunto básico</b>         | El conjunto de privilegios asignados al proceso de un usuario en el momento de inicio de sesión. En un sistema sin modificaciones, cada conjunto heredable inicial del usuario es equivalente al conjunto básico en el inicio de sesión.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>conjunto de privilegios</b> | Una recopilación de privilegios. Cada proceso tiene cuatro conjuntos de privilegios que determinan si un proceso puede utilizar un privilegio determinado. Consulte <a href="#">límite definido</a> , <a href="#">conjunto vigente</a> , <a href="#">conjunto permitido</a> y <a href="#">conjunto heredable</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |

Además, el [conjunto básico](#) de privilegios es la recopilación de privilegios asignados al proceso de un usuario en el momento de inicio de sesión.

**conjunto heredable**

El conjunto de privilegios que un proceso puede heredar a través de una llamada a `exec`.

**conjunto permitido**

El conjunto de privilegios que están disponibles para que utilice un proceso.

**conjunto vigente**

El conjunto de privilegios que actualmente están vigentes en un proceso.

**consumidor**

En la función de estructura criptográfica de Oracle Solaris, un consumidor es un usuario de los servicios criptográficos prestados por los proveedores. Los consumidores pueden ser aplicaciones, usuarios finales u operaciones de núcleo. Kerberos, IKE e IPsec son ejemplos de consumidores. Para ver ejemplos de proveedores, consulte [proveedor](#).

**credencial**

Un paquete de información que incluye un ticket y una clave de sesión coincidente. Se utiliza para autenticar la identidad de un principal. Consulte también [ticket](#), [clave de sesión](#).

**código de autenticación de mensajes (MAC)**

MAC proporciona seguridad en la integridad de los datos y autentica el origen de los datos. MAC no proporciona protección contra intromisiones externas.

**DES**

Siglas en inglés de Data Encryption Standard, estándar de cifrado de datos. Método de cifrado de clave simétrica que se desarrolló en 1975 y que ANSI estandarizó en 1981 como ANSI X.3.92. DES utiliza una clave de 56 bits.

**desfase de reloj**

La cantidad máxima de tiempo que pueden diferir los relojes del sistema interno de todos los hosts que participan en el sistema de autenticación Kerberos. Si el sesgo de reloj se excede entre cualquiera de los hosts participantes, las solicitudes se rechazan. El desfase de reloj se puede especificar en el archivo `krb5.conf`.

**dominio**

1. La red lógica gestionada por una única base de datos de Kerberos y un juego de centros de distribución de claves (KDC).

2. La tercera parte de un nombre de principal. Para el nombre de principal `jdoe/admin@ENG.EXAMPLE.COM`, el dominio es `ENG.EXAMPLE.COM`. Consulte también [nombre de principal](#).

**DSA**

Siglas en inglés de Digital Signature Algorithm, algoritmo de firma digital. Algoritmo de clave pública con un tamaño de clave variable que va de 512 a 4096 bits. DSS, el estándar del gobierno de los Estados Unidos, llega hasta los 1024 bits. DSA se basa en el algoritmo [SHA1](#) para las entradas.

**elemento inicial**

Un iniciador numérico para generar números aleatorios. Cuando el iniciador comienza desde un origen aleatorio, el elemento inicial se denomina *elemento inicial aleatorio*.

**escalada de privilegios**

Obtención de acceso a recursos que se encuentran fuera del rango de recursos permitidos por los atributos de seguridad asignados, incluidas las sustituciones. Como resultado, un proceso puede realizar acciones no autorizadas.



|                                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>evento asíncrono de auditoría</b>     | Los eventos asíncronos constituyen la minoría de los eventos del sistema. Estos eventos no están asociados con ningún proceso; por lo tanto, no hay procesos disponibles para bloquear y reactivar más adelante. Los eventos de inicio del sistema y entrada y salida de la PROM son ejemplos de eventos asíncronos.                                                                                                                                                                                                                                                                                                         |
| <b>evento de auditoría no atribuible</b> | Un evento de auditoría cuyo iniciador no se puede determinar, como el evento AUE_BOOT.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>evento síncrono de auditoría</b>      | La mayoría de los eventos de auditoría. Estos eventos están asociados con un proceso en el sistema. Un evento no atribuible que está asociado con un proceso es un evento síncrono, como un error de inicio de sesión.                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>FQDN</b>                              | Siglas en inglés de Fully Qualified Domain Name, nombre de dominio completo. Por ejemplo, <code>central.example.com</code> (en lugar de simplemente <code>denver</code> ).                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>frase de contraseña</b>               | Una frase que se utiliza para verificar que una clave privada haya sido creada por el usuario de la frase de contraseña. Una buena frase de contraseña tiene una longitud de 10 a 30 caracteres, combina caracteres alfabéticos y numéricos, y evita el texto y los nombres simples. Se le pedirá la frase de contraseña para autenticar el uso de la clave privada para cifrar y descifrar comunicaciones.                                                                                                                                                                                                                  |
| <b>GSS-API</b>                           | Generic Security Service Application Programming Interface. Una capa de red que proporciona apoyo para diversos servicios de seguridad modulares, incluido el servicio Kerberos. GSS-API proporciona servicios de privacidad, integridad y autenticación de seguridad. Consulte también <a href="#">autenticación</a> , <a href="#">integridad</a> y <a href="#">privacidad</a> .                                                                                                                                                                                                                                            |
| <b>host</b>                              | Un sistema al que se puede acceder a través de una red.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>imagen de único sistema</b>           | Una imagen de único sistema se utiliza en la auditoría Oracle Solaris para describir un grupo de sistemas auditados que utilizan el mismo servicio de nombres. Estos sistemas envían sus registros de auditoría a un servidor de auditoría central, donde los registros se pueden comparar como si procedieran de un sistema.                                                                                                                                                                                                                                                                                                |
| <b>instancia</b>                         | La segunda parte de un nombre de principal; una instancia cualifica la primera parte del nombre de principal. En el caso de un principal de servicio, la instancia es obligatoria. La instancia es el nombre de dominio completo del host, como en <code>host/central.example.com</code> . Para los principales de usuario, una instancia es opcional. Sin embargo, tenga en cuenta que <code>jdoe</code> y <code>jdoe/admin</code> son principales únicos. Consulte también <a href="#">primaria</a> , <a href="#">nombre de principal</a> , <a href="#">principal de servidor</a> , <a href="#">principal de usuario</a> . |
| <b>integridad</b>                        | Un servicio de seguridad que, además de la autenticación del usuario, permite validar los datos transmitidos mediante una suma de comprobación criptográfica. Consulte también <a href="#">autenticación</a> y <a href="#">privacidad</a> .                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>KDC</b>                               | <p>Siglas en inglés de Key Distribution Center, centro de distribución de claves. Un equipo que tiene tres componentes Kerberos V5:</p> <ul style="list-style-type: none"> <li>■ Base de datos de claves y principal</li> <li>■ Servicio de autenticación</li> <li>■ Servicio de otorgamiento de tickets</li> </ul> <p>Cada dominio tiene un KDC maestro y debe tener uno o varios KDC esclavos.</p>                                                                                                                                                                                                                         |
| <b>KDC esclavo</b>                       | Una copia de un KDC maestro, que es capaz de realizar la mayoría de las funciones del maestro. Cada dominio, generalmente, tiene varios KDC esclavos (y un solo KDC maestro). Consulte también <a href="#">KDC</a> , <a href="#">KDC maestro</a> .                                                                                                                                                                                                                                                                                                                                                                           |

|                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-----------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>KDC maestro</b>                | El KDC maestro en cada dominio, que incluye un servidor de administración Kerberos, kadmind, y un daemon de otorgamiento de tickets y autenticación, krb5kdc. Cada dominio debe tener al menos un KDC maestro y puede tener varios KDC duplicados, o esclavos, que proporcionan servicios de autenticación a los clientes.                                                                                                                                                                                                                                                                                                                                                     |
| <b>Kerberos</b>                   | <p>Un servicio de autenticación, el protocolo utilizado por ese servicio o el código utilizado para implementar ese servicio.</p> <p>La implementación de Oracle Solaris Kerberos que está estrechamente basada en la implementación de Kerberos V5.</p> <p>Aunque son técnicamente diferentes, "Kerberos" y "Kerberos V5" suelen utilizarse de forma indistinta en la documentación de Kerberos.</p> <p>En la mitología griega, Kerberos (también escrito Cerberus) era un mastín feroz de tres cabezas que protegía las puertas de Hades.</p>                                                                                                                                |
| <b>kvno</b>                       | Siglas en inglés de Key Version Number, número de versión de clave. Un número de secuencia que realiza un seguimiento de una clave determinada en orden de generación. El kvno más alto corresponde a la clave más reciente y actual.                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Lista de control de acceso</b> | Una lista de control de acceso (ACL) proporciona un nivel de seguridad de archivos más específico que la protección de archivos UNIX tradicionales. Por ejemplo, una ACL permite autorizar el acceso de lectura de grupo a un archivo, pero permitir que un solo miembro de ese grupo escriba en el archivo.                                                                                                                                                                                                                                                                                                                                                                   |
| <b>límite definido</b>            | El límite exterior que indica qué privilegios están disponibles para un proceso y sus procesos secundarios.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>MAC</b>                        | <ol style="list-style-type: none"><li>1. Consulte <a href="#">código de autenticación de mensajes (MAC)</a>.</li><li>2. También se denomina etiquetado. En la terminología de seguridad gubernamental, MAC significa control de acceso obligatorio (del inglés Mandatory Access Control). Etiquetas como Top Secret y Confidential son ejemplos de MAC. MAC se diferencia de DAC, que significa control de acceso discrecional (del inglés Discretionary Access Control). Los permisos UNIX son un ejemplo de DAC.</li><li>3. En hardware, la dirección única del sistema en una LAN. Si el sistema está en una Ethernet, la dirección MAC es la dirección Ethernet.</li></ol> |
| <b>MD5</b>                        | Una función de hash criptográfica iterativa utilizada para autenticar mensajes, incluso las firmas digitales. Rivest desarrolló esta función en 1991. Su uso está descartado.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>mecanismo</b>                  | <ol style="list-style-type: none"><li>1. Un paquete de software que especifica técnicas criptográficas para lograr la autenticación o confidencialidad de los datos. Ejemplos: clave pública Diffie-Hellman, Kerberos V5.</li><li>2. En la función de estructura criptográfica de Oracle Solaris, la implementación de un algoritmo para un propósito determinado. Por ejemplo, un mecanismo DES que se aplica a la autenticación, como CKM_DES_MAC, es un mecanismo distinto de un mecanismo DES que se aplica al cifrado, CKM_DES_CBC_PAD.</li></ol>                                                                                                                         |
| <b>mecanismo de seguridad</b>     | Consulte <a href="#">mecanismo</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

|                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>minimización</b>           | La instalación del sistema operativo mínimo necesario para ejecutar el servidor. Cualquier software que no se relacione directamente con el funcionamiento del servidor no se instala o se suprime después de la instalación.                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>modelo de privilegios</b>  | Un modelo de seguridad más estricto en un sistema informático que el modelo de superusuario. En el modelo de privilegios, los procesos requieren un privilegio para ejecutarse. La administración del sistema se puede dividir en partes discretas que se basan en los privilegios que los administradores tienen en sus procesos. Los privilegios se pueden asignar al proceso de inicio de sesión de un administrador. O bien, los privilegios se pueden asignar para que estén vigentes para determinados comandos solamente.                                                                                          |
| <b>modelo de superusuario</b> | El modelo de seguridad UNIX típico en un sistema informático. En el modelo de superusuario, un administrador tiene todo el control del sistema o ningún control (todo o nada). Generalmente, para administrar el equipo, un usuario se convierte en superusuario (root) y puede llevar a cabo todas las actividades administrativas.                                                                                                                                                                                                                                                                                      |
| <b>motor de exploración</b>   | Una aplicación de terceros, que reside en un host externo, que examina un archivo para ver si contiene virus conocidos.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>nombre de principal</b>    | <ol style="list-style-type: none"><li>1. El nombre de un principal, con el formato <i>primary/instance@REALM</i>. Consulte también, <a href="#">instancia</a>, <a href="#">primaria</a>, <a href="#">dominio</a>.</li><li>2. (RPCSEC_GSS API) Consulte <a href="#">principal de cliente</a>, <a href="#">principal de servidor</a>.</li></ol>                                                                                                                                                                                                                                                                             |
| <b>NTP</b>                    | Siglas en inglés de Network Time Protocol, protocolo de hora de red. Software de la Universidad de Delaware que permite gestionar la sincronización precisa del tiempo o del reloj de la red, o de ambos, en un entorno de red. Puede usar NTP para mantener el desfase de reloj en un entorno de Kerberos. Consulte también <a href="#">desfase de reloj</a> .                                                                                                                                                                                                                                                           |
| <b>objeto público</b>         | Un archivo que es propiedad del usuario root y que todos pueden leer, como cualquier archivo en el directorio /etc.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>PAM</b>                    | Siglas en inglés de Pluggable Authentication Module, módulo de autenticación conectable. Una estructura que permite que se utilicen varios mecanismos de autenticación sin que sea necesario recompilar los servicios que los utilizan. PAM permite inicializar la sesión de Kerberos en el momento del inicio de sesión.                                                                                                                                                                                                                                                                                                 |
| <b>perfil de derechos</b>     | También se denomina derecho o perfil. Una recopilación de sustituciones utilizada en RBAC que se puede asignar a un rol o a un usuario. Un perfil de derechos puede constar de autorizaciones, privilegios, comandos con atributos de seguridad y otros perfiles de derechos.                                                                                                                                                                                                                                                                                                                                             |
| <b>pista de auditoría</b>     | La recopilación de todos los archivos de auditoría de todos los hosts.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>política</b>               | Generalmente, un plan o curso de acción que influye sobre decisiones y acciones, o las determina. Para los sistemas informáticos, la política suele hacer referencia a la política de seguridad. La política de seguridad de su sitio es el conjunto de reglas que definen la confidencialidad de la información que se está procesando y las medidas que se utilizan para proteger la información contra el acceso no autorizado. Por ejemplo, la política de seguridad puede requerir que se auditen los sistemas, que los dispositivos se protejan con privilegios y que las contraseñas se cambien cada seis semanas. |

Para la implementación de la política en áreas específicas del SO Oracle Solaris, consulte [política de auditoría](#), [política en la estructura criptográfica](#), [política de dispositivos](#), [política Kerberos](#), [política de contraseñas](#) y [política RBAC](#).

**política de auditoría**

La configuración global y por usuario que determina qué eventos de auditoría se registran. La configuración global que se aplica al servicio de auditoría, generalmente, afecta qué información opcional se incluye en la pista de auditoría. Dos valores, `cnt` y `ahlt`, afectan al funcionamiento del sistema cuando se completa la cola de auditoría. Por ejemplo, es posible que la política de auditoría requiera que un número de secuencia forme parte de cada registro de auditoría.

**política de contraseñas**

Los algoritmos de cifrado que se pueden utilizar para generar contraseñas. También puede referirse a cuestiones más generales sobre las contraseñas, como la frecuencia con la que deben cambiarse las contraseñas, cuántos intentos de escribir la contraseña se permiten y otras consideraciones de seguridad. La política de seguridad requiere contraseñas. La política de contraseñas requiere que las contraseñas se cifren con el algoritmo AES y puede exigir requisitos adicionales relacionados con la seguridad de las contraseñas.

**política de dispositivos**

Protección de dispositivos en el nivel de núcleo. La política de dispositivos se implementa como dos conjuntos de privilegios en un dispositivo. Un conjunto de privilegios controla el acceso de lectura al dispositivo. El segundo conjunto de privilegios controla el acceso de escritura al dispositivo. Consulte también [política](#).

**política de seguridad**

Consulte [política](#).

**política en la estructura criptográfica**

En la función de estructura criptográfica de Oracle Solaris, la política es la desactivación de mecanismos criptográficos existentes. Después de esto, los mecanismos no se pueden utilizar. La política en la estructura criptográfica puede impedir el uso de un mecanismo determinado, como `CKM_DES_CBC`, de un proveedor, como DES.

**política Kerberos**

Un conjunto de reglas que rige el uso de contraseñas en el servicio Kerberos. Las políticas pueden regular los accesos de los principales, o los parámetros de tickets, como la duración.

**política para tecnologías de clave pública**

En la estructura de gestión de claves (KMF), la política es la gestión del uso de certificados. La base de datos de políticas KMF puede limitar el uso de las claves y los certificados administrados por la biblioteca KMF.

**política RBAC**

La política de seguridad que está asociada a un comando. En la actualidad, `solaris` es la política válida. La política `solaris` reconoce privilegios, autorizaciones y atributos de `securityd`.

**primaria**

La primera parte de un nombre de principal. Consulte también [instancia](#), [nombre de principal](#), [dominio](#).

**principal**

1. Un cliente o usuario con un nombre único o una instancia de servidor o servicio que participa en una comunicación de red. Las transacciones de Kerberos implican interacciones entre principales (principales de servicio y principales de usuario) o entre principales y KDC. En otras palabras, un principal es una entidad única a la que Kerberos puede asignar tickets. Consulte también [nombre de principal](#), [principal de servidor](#), [principal de usuario](#).

2. (RPCSEC\_GSS API) Consulte [principal de cliente](#), [principal de servidor](#).

|                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>principal admin</b>             | Un principal de usuario con un nombre del tipo <i>nombre de usuario/admin</i> (como en <code>jdoe/admin</code> ). Un principal admin puede tener más privilegios (por ejemplo, para modificar las políticas) que un principal de usuario común. Consulte también <a href="#">nombre de principal</a> , <a href="#">principal de usuario</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>principal de cliente</b>        | (RPCSEC_GSS API) Un cliente (un usuario o una aplicación) que utiliza los servicios de red RPCSEC_GSS seguros. Los nombres de principales de cliente se almacenan con el formato <code>rpc_gss_principal_t</code> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>principal de host</b>           | Una instancia determinada de un principal de servicio en la que el principal (indicado por el nombre principal host) está configurado para proporcionar un rango de servicios de red, como <code>ftp</code> , <code>rcp</code> o <code>rlogin</code> . Un ejemplo de un principal de host principal es <code>host/central.example.com@EXAMPLE.COM</code> . Consulte también <a href="#">principal de servidor</a> .                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>principal de servidor</b>       | (RPCSEC_GSS API) Un principal que proporciona un servicio. El principal de servidor se almacena como una cadena ASCII con el formato <i>servicio@host</i> . Consulte también <a href="#">principal de cliente</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>principal de servidor</b>       | Un principal que proporciona autenticación Kerberos para un servicio o servicios. Para los principales de servicio, el nombre de principal es el nombre de un servicio, como <code>ftp</code> y su instancia es el nombre de host completo del sistema que proporciona el servicio. Consulte también <a href="#">principal de host</a> , <a href="#">principal de usuario</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>principal de usuario</b>        | Un principal atribuido a un usuario determinado. El nombre primario de un principal de usuario es un nombre de usuario y su instancia opcional es un nombre que se utiliza para describir el uso que se pretende hacer de las credenciales correspondientes (por ejemplo, <code>jdoe</code> o <code>jdoe/admin</code> ). También se conoce como instancia de usuario. Consulte también <a href="#">principal de servidor</a> .                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>privacidad</b>                  | Un servicio de seguridad en el que los datos transmitidos se cifran antes de enviarse. La privacidad también incluye la integridad de los datos y la autenticación de usuario. Consulte también <a href="#">autenticación</a> , <a href="#">integridad</a> y <a href="#">servicio</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>privilegio</b>                  | Un derecho discreto en un proceso de un sistema Oracle Solaris. Los privilegios ofrecen un control más específico de los procesos que <code>root</code> . Los privilegios se definen y se aplican en el núcleo. Para obtener una descripción completa de los privilegios, consulte la página del comando <code>man privileges(5)</code> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>privilegio mínimo</b>           | Un modelo de seguridad que ofrece a un proceso especificado sólo un subconjunto de poderes de superusuario. El modelo de privilegios básico asigna suficientes privilegios a los usuarios comunes para que puedan realizar tareas administrativas personales, como montar sistemas de archivos o cambiar la propiedad de los archivos. Por otro lado, los procesos se ejecutan sólo con esos privilegios, que son necesarios para completar la tarea, en lugar de con toda la capacidad de superusuario, es decir, todos los privilegios. Los daños debidos a errores de programación como desbordamiento de la memoria intermedia se pueden contener para un usuario que no es <code>root</code> , que no tiene acceso a capacidades críticas como la lectura o escritura en archivos de sistema protegidos o la detención del equipo. |
| <b>protección</b>                  | La modificación de la configuración predeterminada del sistema operativo para eliminar las vulnerabilidades de seguridad inherentes al host.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>protocolo de Diffie-Hellman</b> | También se lo denomina "criptografía de claves públicas". Se trata de un protocolo de claves criptográficas asimétricas que desarrollaron Diffie y Hellman en 1976. Este protocolo permite a dos usuarios intercambiar una clave secreta mediante un medio no seguro, sin ningún otro secreto. <a href="#">Kerberos</a> utiliza el protocolo Diffie-Hellman.                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

|                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|--------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>proveedor</b>                     | En la función de estructura criptográfica de Oracle Solaris, un servicio criptográfico proporcionado a los consumidores. Las bibliotecas PKCS #11, los módulos criptográficos y los aceleradores de hardware son ejemplos de proveedores. Los proveedores se conectan a la estructura criptográfica y también se conocen como <i>complementos</i> . Para ver ejemplos de consumidores, consulte <a href="#">consumidor</a> .                                          |
| <b>proveedor de hardware</b>         | En la función de estructura criptográfica de Oracle Solaris, un controlador del dispositivo y su acelerador de hardware. Los proveedores de hardware descargan operaciones criptográficas costosas del sistema informático y, de esa manera, liberan los recursos de la CPU para otros usos. Consulte también <a href="#">proveedor</a> .                                                                                                                             |
| <b>proveedor de software</b>         | En la función de estructura criptográfica de Oracle Solaris, un módulo de software de núcleo o una biblioteca PKCS #11 que proporciona servicios criptográficos. Consulte también <a href="#">proveedor</a> .                                                                                                                                                                                                                                                         |
| <b>QOP</b>                           | Siglas en inglés de Quality of Protection, calidad de protección. Un parámetro que se utiliza para seleccionar los algoritmos criptográficos que se utilizan junto con el servicio de integridad o de privacidad.                                                                                                                                                                                                                                                     |
| <b>RBAC</b>                          | Control de acceso basado en roles, una función de Oracle Solaris. Una alternativa al modelo de superusuario de todo o nada. El RBAC permite que una organización separe las capacidades de superusuario y las asigne a cuentas de usuario especiales denominadas roles. Los roles se pueden asignar a individuos específicos según sus responsabilidades.                                                                                                             |
| <b>reconocimiento de privilegios</b> | Programas, secuencias de comandos y comandos que activan y desactivan el uso de privilegios en su código. En un entorno de producción, los privilegios que estén activados deben proporcionarse al proceso, por ejemplo, solicitando a los usuarios del programa que utilicen un perfil de derechos que agrega los privilegios al programa. Para obtener una descripción completa de los privilegios, consulte la página del comando <code>man privileges(5)</code> . |
| <b>red privada virtual (VPN)</b>     | Una red que proporciona comunicaciones seguras al utilizar el cifrado y el establecimiento de túneles para conectar usuarios a través de una red pública.                                                                                                                                                                                                                                                                                                             |
| <b>relación</b>                      | Una variable de configuración o un vínculo definidos en los archivos <code>kdc.conf</code> o <code>krb5.conf</code> .                                                                                                                                                                                                                                                                                                                                                 |
| <b>resumen</b>                       | Consulte <a href="#">resumen de mensaje</a> .                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>resumen de mensaje</b>            | Un resumen de mensaje es un valor hash que se calcula a partir de un mensaje. El valor hash identifica el mensaje casi de manera exclusiva. Un resumen es útil para verificar la integridad de un archivo.                                                                                                                                                                                                                                                            |
| <b>rol</b>                           | Una identidad especial para ejecutar aplicaciones con privilegios que sólo los usuarios asignados pueden asumir.                                                                                                                                                                                                                                                                                                                                                      |
| <b>RSA</b>                           | Método para la obtención de firmas digitales y criptosistemas de claves públicas. Dicho método lo describieron sus creadores, Rivest, Shamir y Adleman, en 1978.                                                                                                                                                                                                                                                                                                      |
| <b>SEAM</b>                          | Sun Enterprise Authentication Mechanism. El nombre del producto para las versiones iniciales de un sistema para autenticar usuarios de una red, basado en la tecnología Kerberos V5 desarrollada en el Massachusetts Institute of Technology. El producto ahora se denomina servicio Kerberos. SEAM se refiere a las partes del servicio Kerberos que no se incluyeron en las diferentes versiones de Solaris.                                                        |
| <b>Secure Shell</b>                  | Un protocolo especial para el inicio de sesión remoto seguro y otros servicios de red seguros a través de una red no segura.                                                                                                                                                                                                                                                                                                                                          |

|                                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|----------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>separación de tareas</b>            | Parte de la noción de <a href="#">privilegio mínimo</a> . La separación de tareas impide que un usuario realice o apruebe todas las acciones que permiten completar una transacción. Por ejemplo, en <a href="#">RBAC</a> , puede separar la creación de un usuario de inicio de sesión de la asignación de sustituciones de seguridad. Un rol crea el usuario. Un rol individual puede asignar atributos de seguridad, como perfiles de derechos, roles y privilegios a los usuarios existentes.                                                                                                                                                                                                                                                                                                                                                                          |
| <b>servicio</b>                        | <p>1. Un recurso proporcionado a clientes de la red, a menudo, por más de un servidor. Por ejemplo, si ejecuta <code>rlogin</code> en el equipo <code>central.example.com</code>, ese equipo es el servidor que proporciona el servicio <code>rlogin</code>.</p> <p>2. Un servicio de seguridad (ya sea de integridad o privacidad) que proporciona un nivel de protección más allá de la autenticación. Consulte también <a href="#">integridad</a> y <a href="#">privacidad</a>.</p>                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>servicio de seguridad</b>           | Consulte <a href="#">servicio</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>servidor</b>                        | Un principal que proporciona un recurso a los clientes de la red. Por ejemplo, si ejecuta <code>ssh</code> en el sistema <code>central.example.com</code> , ese sistema es el servidor que proporciona el servicio <code>ssh</code> . Consulte también <a href="#">principal de servidor</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>servidor de aplicaciones</b>        | Consulte <a href="#">servidor de aplicaciones de red</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>servidor de aplicaciones de red</b> | Un servidor que proporciona aplicaciones de red, como <code>ftp</code> . Un dominio puede contener varios servidores de aplicaciones de red.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>SHA1</b>                            | Siglas en inglés de Secure Hashing Algorithm, algoritmo de hash seguro. El algoritmo funciona en cualquier tamaño de entrada que sea inferior a $2^{64}$ para generar un resumen del mensaje. El algoritmo SHA-1 es la entrada de <a href="#">DSA</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>shell de perfil</b>                 | En RBAC, un shell que permite que un rol (o un usuario) ejecute desde la línea de comandos cualquier aplicación con privilegios asignada a los perfiles de derechos del rol. Los shells de perfiles son <code>pfsh</code> , <code>pfcsch</code> y <code>pfksh</code> . Corresponden al shell Bourne ( <code>sh</code> ), shell C ( <code>csh</code> ) y shell Korn ( <code>ksh</code> ), respectivamente.                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>TGS</b>                             | Siglas en inglés de Ticket-Granting Service, servicio de otorgamiento de tickets. La parte del KDC que es responsable de emitir tickets.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>TGT</b>                             | Siglas en inglés de Ticket-Granting Ticket, Ticket de otorgamiento de tickets. Un ticket emitido por el KDC que permite que un cliente solicite tickets para otros servicios.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>ticket</b>                          | Un paquete de información que se utiliza para transmitir de manera segura la identidad de un usuario a un servidor o servicio. Un ticket es válido únicamente para un solo cliente y un servicio determinado en un servidor específico. Un ticket contiene el nombre de principal del servicio, el nombre de principal del usuario, la dirección IP del host del usuario, una indicación de hora y un valor que define la duración del ticket. Un ticket se crea con una clave de sesión aleatoria que utilizará el cliente y el servicio. Una vez que se ha creado un ticket, se puede volver a utilizar hasta que caduque. Un ticket sólo sirve para autenticar un cliente cuando se presenta junto con un autenticador nuevo. Consulte también <a href="#">autenticador</a> , <a href="#">credencial</a> , <a href="#">servicio</a> y <a href="#">clave de sesión</a> . |

|                                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|---------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ticket de sustituto</b>            | Un ticket que puede utilizar un servicio en nombre de un cliente para realizar una operación para el cliente. Por lo tanto, se dice que el servicio actúa como sustituto del cliente. Con el ticket, el servicio puede asumir la identidad del cliente. El servicio puede utilizar un ticket de sustituto para obtener un ticket de servicio para otro servicio, pero no puede obtener un ticket de otorgamiento de tickets. La diferencia entre un ticket de sustituto y un ticket reenviable es que un ticket de sustituto únicamente es válido para una sola operación. Consulte también <a href="#">ticket reenviable</a> .                                                                                                                                                                                                                                                                         |
| <b>ticket inicial</b>                 | Un ticket que se emite directamente (es decir, que no se basa en un ticket de otorgamiento de tickets existente). Algunos servicios, como las aplicaciones que cambian las contraseñas, posiblemente requieran que los tickets se marquen como <i>iniciales</i> para garantizar que el cliente pueda demostrar que conoce su clave secreta. Esta garantía es importante porque un ticket inicial indica que el cliente se ha autenticado recientemente (en lugar de basarse en un ticket de otorgamiento de tickets, que posiblemente haya existido durante mucho tiempo).                                                                                                                                                                                                                                                                                                                              |
| <b>ticket no válido</b>               | Un ticket posfechado que todavía no puede utilizarse. Un servidor de aplicaciones rechaza un ticket no válido hasta que se valide. Para validar un ticket no válido, el cliente debe presentarlo al KDC en una solicitud TGS, con el indicador VALIDATE definido, después de que haya pasado la hora de inicio. Consulte también <a href="#">ticket posfechado</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>ticket posfechado</b>              | Un ticket posfechado no es válido hasta que transcurra un tiempo especificado tras su creación. Un ticket de este tipo es útil, por ejemplo, para los trabajos por lotes que deben ejecutarse tarde por la noche, ya que si el ticket es robado, no se puede utilizar hasta que se ejecute el trabajo por lotes. Los tickets posfechados se emiten como <i>no válidos</i> y siguen teniendo ese estado hasta que: a) haya pasado su hora de inicio, y b) el cliente solicite la validación por parte del KDC. Generalmente, un ticket posfechado es válido hasta la hora de vencimiento del ticket de otorgamiento de tickets. Sin embargo, si el ticket posfechado se marca como <i>renovable</i> , su duración suele definirse para que coincida con la duración total del ticket de otorgamiento de tickets. Consulte también, <a href="#">ticket no válido</a> , <a href="#">ticket renovable</a> . |
| <b>ticket reenviable</b>              | Un ticket que un cliente puede utilizar para solicitar un ticket en un host remoto sin que sea necesario que el cliente complete todo el proceso de autenticación en ese host. Por ejemplo, si el usuario david obtiene un ticket reenviable mientras está en el equipo de jennifer, puede iniciar sesión en su propio equipo sin tener que obtener un ticket nuevo (y, por lo tanto, autenticarse nuevamente). Consulte también <a href="#">ticket de sustituto</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>ticket renovable</b>               | Debido a que los tickets con duraciones muy largas constituyen un riesgo de seguridad, los tickets se pueden designar como <i>renovables</i> . Un ticket renovable tiene dos horas de vencimiento: a) la hora de vencimiento de la instancia actual del ticket, y b) la duración máxima de cualquier ticket. Si un cliente desea seguir utilizando un ticket, debe renovarlo antes del primer vencimiento. Por ejemplo, un ticket puede ser válido por una hora, pero todos los tickets tienen una duración máxima de 10 h. Si el cliente que tiene el ticket desea conservarlo durante más de una hora, debe renovarlo. Cuando un ticket alcanza la duración máxima, vence automáticamente y no se puede renovar.                                                                                                                                                                                      |
| <b>tipo</b>                           | Históricamente, <i>tipo de seguridad</i> y <i>tipo de autenticación</i> tenían el mismo significado; ambos indicaban el tipo de autenticación (AUTH_UNIX, AUTH_DES, AUTH_KERB). RPCSEC_GSS también es un tipo de seguridad, aunque proporciona servicios de privacidad e integridad, además de autenticación.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>tipo de seguridad</b>              | Consulte <a href="#">tipo</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>ámbito del servicio de nombres</b> | El ámbito en el que un rol puede operar, es decir, un host individual o todos los hosts gestionados por un servicio de nombres especificado, como NIS o LDAP.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |



# Índice

---

## Números y símbolos

[ ] (corchetes), salida `auditrecord`, 652  
\$\$ (signo de dólar doble), número de proceso de shell principal, 199  
@ (arroba), archivo `device_allocate`, 90  
\* (asterisco)  
    archivo `device_allocate`, 89, 90  
    carácter comodín  
        en autorizaciones RBAC, 209  
    comprobación en autorizaciones RBAC, 182  
\  
    archivo `device_allocate`, 90  
    archivo `device_maps`, 89  
.(punto)  
    separador de nombre de autorización, 209  
    visualización de archivos ocultos, 120  
;(punto y coma), archivo `device_allocate`, 89  
# (signo de almohadilla)  
    archivo `device_allocate`, 90  
    archivo `device_maps`, 89  
^ (signo de intercalación)  
    en prefijos de clase de auditoría, 581–585, 633  
    modificador de prefijo de clase de auditoría, 646–647  
= (signo igual), símbolo de permisos de archivo, 117  
- (signo menos)  
    archivo `su_log`, 63  
    prefijo de clase de auditoría, 646–647  
    símbolo de permisos de archivo, 117  
- (signo menos), símbolo de tipo de archivo, 112  
+ (signo más)  
    archivo `su_log`, 63

+ (signo más) (*Continuación*)  
    prefijo de clase de auditoría, 646–647  
    símbolo de permisos de archivo, 117  
+ (signo-más), en prefijos de clase de auditoría, 605  
> (redirigir salida), prevención, 45  
>> (agregar salida), prevención, 45

## A

opción `-A`, comando `auditreduce`, 618  
acces  
    seguridad  
        dispositivos periféricos, 41  
acceso  
    acceso al servidor  
        con Kerberos, 537–540  
    acceso root  
        mostrar intentos en la consola, 63–65  
        restricción, 49, 63–65  
        supervisión de intentos de comando `su`, 62–63  
        supervisión de intentos del comando `su`, 43–44  
autenticación de inicio de sesión con Secure Shell, 309–310  
autenticación RPC segura, 335  
espacio de direcciones, 43  
listas de control  
    *Ver* ACL  
obtención de acceso a un servicio específico, 540  
otorgamiento de acceso a su cuenta, 518–520  
restricción para  
    dispositivos, 41–42, 73

acceso, restricción para (*Continuación*)

hardware del sistema, 65–66

restricción para servidores KDC, 449

## seguridad

ACL, 48–49

ACL de UFS, 118

autenticación de inicio de sesión, 309–310

cliente-servidor NFS, 337–340

comunicación de problemas, 54

configuración de cortafuegos, 53

configuración de variable PATH, 45

configuración del cortafuegos, 53

control de inicio de sesión, 36

control de red, 50–54

control del uso del sistema, 43–47

dispositivos, 73

hardware del sistema, 65–66

programas `setuid`, 46

restricciones de acceso de inicio de sesión, 36

restricción de acceso a archivos, 45

seguimiento de inicio de sesión `root`, 43–44

seguridad física, 35–36

sistemas remotos, 293

supervisión del uso del sistema, 47

uso compartido de archivos, 49

acceso `root`

intentos de supervisión, 63–65

resolución de problemas remota, 64

supervisión y restricción, 62–65

## ACL

archivo `kadm5.acl`, 483, 485, 489

descripción, 48–49, 118

formato de entradas, 118

## activación

asignación de dispositivos, 76–77

auditoría, 613–614

interrupción del teclado, 66

mecanismos criptográficos, 250

mecanismos y funciones en el proveedor de

hardware, 256

servicio de auditoría, 613–614

uso de un proveedor de software de núcleo, 252

## adición

principal de servicio a archivo `keytab`

(Kerberos), 505–506

principales de administración (Kerberos), 384

## administración

algoritmos de contraseñas, 59–62

asignación de dispositivos, 75–76

## auditoría

activación, 613–614

archivos de auditoría, 620–622

clases de auditoría, 552–553

comando `audit -s`, 611–613, 613–614comando `audit -t`, 613comando `auditconfig`, 578, 580–581comando `auditreduce`, 616–618comando `praudit`, 620–622complemento `audit_remote`, 600–601, 601–605complemento `audit_syslog`, 605–607

complementos, 600–601, 601–605

configuración, 578

control de costos, 573

controles de colas, 587–588

desactivación, 613

descripción, 560

eficacia, 575

eventos de auditoría, 551

perfiles de derechos necesarios, 644–645

política, 585–587

reducción de requisitos de espacio, 574–575

refrescamiento, 611–613

registros de auditoría, 553

zonas, 607–611

en zonas, 561–562, 645

autorizaciones, 180–181

comandos de la estructura criptográfica, 226

contraseña de rol, 187–188

contraseña de usuario para asumir rol, 189–190,  
191–192

estructura criptográfica y FIPS-140, 228

estructura criptográfica y zonas, 227

inicios de sesión remotos con Secure Shell, 305–307

## Kerberos

políticas, 490–499

principales, 476–490

administración, Kerberos (*Continuación*)

- tablas de claves, 504–510
- mapa de tareas de la estructura criptográfica, 241
- mapa de tareas de RPC segura, 340
- metarranura, 226
- perfiles de derechos, 175–177
  - de un usuario, 189–190, 192
- permisos de archivo, 119–128
- política de dispositivos, 73–74
- privilegios, 194
- propiedades de seguridad
  - autorizaciones, 180–181
  - de un perfil de derechos, 175–177, 177–179
  - de un rol, 187–188, 188–189, 189–190, 191–192
  - de un usuario, 162–164
  - de una aplicación antigua, 181–182
- propiedades RBAC, 175–177, 180–181
- roles para reemplazar al superusuario, 169–171
- Secure Shell
  - clientes, 320
  - descripción general, 317–319
  - mapa de tareas, 298
  - servidores, 320
- seguridad de archivos de cliente-servidor
  - NFS, 337–340
  - ZFS de forma remota con Secure Shell, 310–311
- administrador del sistema (RBAC)
  - perfil de derechos, 206
  - protección de hardware, 65
  - rol recomendado, 133
- administradores, restricción de derechos, 190–191
- administrar, sin privilegios, 146
- advertencia sobre caducidad de ticket, 416

## agregación

- atributos de seguridad
  - a aplicaciones antiguas, 181–182
  - a roles, 188–189
  - para usuarios, 162–164
- auditoría
  - de roles, 174–175
  - de usuarios individuales, 581–585, 630
  - de zonas, 563–570
- autenticación DH para sistemas de archivos
  - montados, 340

agregación (*Continuación*)

- autorizaciones
  - a comando, 180–181
- clases de auditoría, 590–591
- complemento de biblioteca, 247
- complementos
  - auditoría, 600–601, 601–605, 605–607
  - estructura criptográfica, 246–247
  - KMF, 273–274
- dispositivo asignable, 76–77
- mecanismos y funciones de proveedor de hardware, 256
- nueva autorización, 180–181
- nuevo perfil de derechos, 175–177
- nuevo perfil de derechos de uno existente, 177–179
- política de auditoría, 585–587
- política de auditoría temporal, 586–587
- privilegios
  - a comando en perfil de derechos, 177
  - directamente a usuario, 164
  - directamente al rol, 189
- propiedades RBAC
  - a aplicaciones antiguas, 181–182
- proveedor de software, 246–247
- proveedor de software de nivel de usuario, 247
- rol cryptomgt, 174
- rol relacionado con seguridad, 174
- roles, 171–173
- seguridad para dispositivos, 75–81
- seguridad para hardware del sistema, 65–66
- sistemas de archivos de auditoría, 593–597
- usuarios con privilegios, 163–164
- agregar, módulos PAM, 281–282
- algoritmo de cifrado 3des, archivo `ssh_config`, 321
- algoritmo de cifrado 3des-cbc, archivo `ssh_config`, 321
- algoritmo de cifrado aes128-cbc, archivo `ssh_config`, 321
- algoritmo de cifrado aes128-ctr, archivo `ssh_config`, 321
- algoritmo de cifrado arc four, archivo `ssh_config`, 321
- algoritmo de cifrado Blowfish
  - archivo `policy.conf`, 60

- algoritmo de cifrado Blowfish (*Continuación*)
  - archivo `ssh_config`, 321
  - permiso en entornos heterogéneos, 60
- algoritmo de cifrado Blowfish, proveedor de núcleo, 242
- algoritmo de cifrado blowfish-cbc, archivo `ssh_config`, 321
- algoritmo de cifrado hmac-sha1, archivo `ssh_config`, 323
- algoritmo de cifrado MD4, proveedor de núcleo, 242
- algoritmo de cifrado MD5
  - archivo `policy.conf`, 59–60, 60
  - permiso en entornos heterogéneos, 60
- algoritmo de cifrado MD5, proveedor de núcleo, 242
- algoritmo de contraseña `crypt_bsdbf`, 38
- algoritmo de contraseña `crypt_bsdbf`, 38
- algoritmo de contraseña `crypt_sha256`, 38, 59–62
- algoritmo de contraseña `crypt_sunmd5`, 38
- algoritmo de contraseña `crypt_unix`, 38
- algoritmo `hmac-md5`, archivo `ssh_config`, 323
- algoritmos
  - cifrado de archivo, 238–241
  - cifrado de contraseña, 38, 59–62
  - contraseña
    - configuración, 59–60
  - definición en la estructura criptográfica, 223
  - lista de la estructura criptográfica, 242–246
  - protección de frase de contraseña en `ssh-keygen`, 296
- almacenamiento
  - archivos de auditoría, 568–569, 593–597
  - auditoría remota de archivos, 569–570
  - contraseña, 239
- almacenes de claves
  - administrados por KMF, 260
  - admitidos por KMF, 260, 261
  - definición en la estructura criptográfica, 224
  - enumeración de contenido, 263
  - exportación de certificados, 266–267
  - importación de certificados, 264–265
  - protección con contraseña en KMF, 267–268
- ALTSHELL en Secure Shell, 325
- antememoria, credenciales, 537
- antivirus, *Ver* análisis de virus
- análisis de virus
  - archivos, 67–68
  - configuración, 69–72
  - descripción, 68
  - motores, 67–68
- aplicación con privilegios
  - comprobación de autorizaciones, 140
  - comprobación de ID, 139
  - comprobación de privilegios, 140
  - descripción, 135
- archivo, archivos de auditoría, 623–624
- archivo `~/gkadmin`, descripción, 527
- archivo `~/k5login`, descripción, 527
- archivo `~/rhosts`, descripción, 327
- archivo `~/shosts`, descripción, 327
- archivo `~/ssh/authorized_keys`
  - descripción, 327
  - valor de sustitución, 328
- archivo `~/ssh/config`
  - descripción, 328
  - valor de sustitución, 328
- archivo `~/ssh/environment`, descripción, 327
- archivo `~/ssh/id_dsa`, valor de sustitución, 328
- archivo `~/ssh/id_rsa`, valor de sustitución, 328
- archivo `~/ssh/identity`, valor de sustitución, 328
- archivo `~/ssh/known_hosts`
  - descripción, 327
  - valor de sustitución, 328
- archivo `~/ssh/rc`, descripción, 327
- archivo `/etc/default/kbd`, 66
- archivo `/etc/default/login`
  - descripción, 327
  - restricción de acceso root remoto, 63–65
  - Secure Shell y, 325–326
- archivo `/etc/default/su`
  - mostrar intentos del comando `su`, 63–65
  - supervisión de comando `su`, 62–63
  - supervisión de intentos de acceso, 63–65
- archivo `/etc/hosts.equiv`, descripción, 327
- archivo `/etc/krb5/kadm5.acl`, descripción, 528
- archivo `/etc/krb5/kadm5.keytab`, descripción, 528
- archivo `/etc/krb5/kdc.conf`, descripción, 528
- archivo `/etc/krb5/kpropd.acl`, descripción, 528
- archivo `/etc/krb5/krb5.conf`, descripción, 528

- archivo /etc/krb5/krb5.keytab, descripción, 528
- archivo /etc/krb5/warn.conf, descripción, 528
- archivo /etc/logind/perm, 41
- archivo /etc/nologin
  - desactivación temporal de inicios de sesión de usuario, 58–59
  - descripción, 327
- archivo /etc/pam.conf, Kerberos y, 528
- archivo /etc/publickey, autenticación DH y, 337
- archivo /etc/rsyslog.conf, PAM y, 283
- archivo /etc/security/audit\_event, eventos de auditoría y, 551
- archivo /etc/security/device\_allocate, 89
- archivo /etc/security/device\_maps, 88
- archivo /etc/security/policy.conf, configuración de algoritmos, 59–60
- archivo /etc/ssh\_host\_dsa\_key.pub,
  - descripción, 326
- archivo /etc/ssh\_host\_key.pub, descripción, 326
- archivo /etc/ssh\_host\_rsa\_key.pub,
  - descripción, 326
- archivo /etc/ssh/shosts.equiv, descripción, 327
- archivo /etc/ssh/ssh\_config
  - configuración de Secure Shell, 320
  - descripción, 328
  - palabras clave, 320–326
  - parámetros específicos de host, 325
  - valor de sustitución, 328
- archivo /etc/ssh/ssh\_host\_dsa\_key,
  - descripción, 326
- archivo /etc/ssh/ssh\_host\_key, valor de sustitución, 328
- archivo /etc/ssh/ssh\_host\_rsa\_key,
  - descripción, 326
- archivo /etc/ssh/ssh\_known\_hosts
  - control de distribución, 326
  - descripción, 327
  - distribución segura, 326
  - valor de sustitución, 328
- archivo /etc/ssh/sshd\_config
  - descripción, 326
  - palabras clave, 320–326
- archivo /etc/ssh/sshr, descripción, 328
- archivo /etc/syslog.conf
  - auditoría y, 606, 644
  - mensajes de pilas ejecutables y, 119
  - PAM y, 283
- archivo .gkadmin
  - descripción, 527
  - herramienta SEAM y, 474
- archivo .k5.REALM, descripción, 528
- archivo .k5login
  - descripción, 518–520, 527
  - en lugar de revelar la contraseña, 519
- archivo .rhosts, descripción, 327
- archivo .shosts, descripción, 327
- archivo /system/volatile/sshd.pid,
  - descripción, 327
- archivo /tmp/krb5cc\_uid, descripción, 528
- archivo /tmp/ovsec\_admin.xxxxx, descripción, 528
- archivo /var/adm/auditlog, registros de auditoría de texto, 606
- archivo /var/adm/messages
  - mensajes de pilas ejecutables, 119
  - resolución de problemas de auditoría, 628
- archivo /var/adm/sulog, supervisión de contenido de, 62
- archivo /var/krb5/.k5.REALM, descripción, 528
- archivo /var/krb5/kadmin.log, descripción, 528
- archivo /var/krb5/kdc.log, descripción, 528
- archivo /var/krb5/principal, descripción, 528
- archivo /var/krb5/principal.kadm5,
  - descripción, 528
- archivo /var/krb5/principal.kadm5.lock,
  - descripción, 528
- archivo /var/krb5/principal.ok, descripción, 528
- archivo /var/krb5/principal.ulong, descripción, 528
- archivo /var/krb5/slave\_datatrans,
  - descripción, 528
- archivo /var/krb5/slave\_datatrans\_slave,
  - descripción, 529
- archivo /var/log/syslog, resolución de problemas de auditoría, 628
- archivo audit\_class
  - agregación de una clase, 590–591
  - resolución de problemas, 591

- archivo `audit_event`
  - cambio de pertenencia a clase, 591–592
  - descripción, 551
  - eliminación de eventos de manera segura, 635–636
- archivo `auditlog`, registros de auditoría de texto, 606
- archivo `authorized_keys`, descripción, 327
- archivo de configuración PAM, agregación de pila `su`, 166
- archivo de reglas (BART), 95
- archivo de ticket, *Ver* antememoria de credenciales
- archivo `default/login`, descripción, 327
- archivo `device_allocate`
  - descripción, 89–91
  - ejemplo, 79, 89
  - formato, 89
- archivo `device_maps`
  - descripción, 88
  - entradas de ejemplo, 88
  - formato, 88
- archivo `hosts.equiv`, descripción, 327
- archivo intermedio
  - creación, 391, 440
  - definición, 531
- archivo `kadm5.acl`
  - descripción, 528
  - entrada de KDC maestro, 378, 384, 428
  - formato de las entradas, 489
  - nuevos principales y, 483, 485
- archivo `kadm5.keytab`, descripción, 528
- archivo `kadmin.log`, descripción, 528
- archivo `kbd`, 66
- archivo `kdc.conf`
  - descripción, 528
  - duración de tickets y, 534
- archivo `kdc.log`, descripción, 528
- archivo `keytab`
  - adición de principal de servicio a, 504, 505–506
  - adición del principal host del KDC maestro al, 379, 386
  - administración, 504–510
  - administración mediante el comando `ktutil`, 504
  - desactivación de un servicio de host con el comando `delete_entry`, 509
- archivo `keytab` (*Continuación*)
  - eliminación de principales con el comando `ktremove`, 507
  - eliminación de un principal de servicio del, 506–507
  - lectura en memoria intermedia de `keytab` con el comando `read_kt`, 508, 509
  - visualización de contenidos con el comando `ktutil`, 507
  - visualización de memoria intermedia de lista de claves con el comando `list`, 508, 509
- archivo `known_hosts`
  - control de distribución, 326
  - descripción, 327
- archivo `kpropd.acl`, descripción, 528
- archivo `krb-warn.conf`, descripción, 529
- archivo `krb5.conf`
  - definición de puertos, 365
  - descripción, 528
  - edición, 376, 382
  - sección `domain_realm`, 363
- archivo `krb5.keytab`, descripción, 528
- archivo `krb5cc_uid`, descripción, 528
- archivo `login`, restricción del acceso root remoto, 63–65
- archivo `messages`, mensajes de pilas ejecutables, 119
- archivo `nologin`, descripción, 327
- archivo `ovsec_adm.xxxxxx`, descripción, 528
- archivo `pam.conf`, *Ver* archivos de configuración PAM
- archivo `policy.conf`
  - descripción, 212, 213
  - especificación de algoritmo de contraseña en servicios de nombres, 61
  - especificación de algoritmos de cifrado en, 59–60
  - especificación de algoritmos de contraseña, 59–60
  - palabras clave
    - para algoritmos de contraseña, 39
    - para autorizaciones RBAC, 212
    - para perfiles de derechos, 212
    - para privilegios, 212, 216
    - para propietario de estación de trabajo, 212
- archivo `principal`, descripción, 528
- archivo `principal.kadm5`, descripción, 528
- archivo `principal.kadm5.lock`, descripción, 528
- archivo `principal.ok`, descripción, 528

- archivo principal.ulong, descripción, 528
- archivo shosts.equiv, descripción, 327
- archivo slave\_datatrans
  - descripción, 528
  - propagación de KDC y, 430–431
- archivo slave\_datatrans\_slave, descripción, 529
- archivo ssh\_config
  - configuración de Secure Shell, 320
  - palabras clave, 320–326
    - Ver palabra clave específica
  - parámetros específicos de host, 325
  - valor de sustitución, 328
- archivo ssh\_host\_dsa\_key, descripción, 326
- archivo ssh\_host\_dsa\_key.pub, descripción, 326
- archivo ssh\_host\_key, valor de sustitución, 328
- archivo ssh\_host\_key.pub, descripción, 326
- archivo ssh\_host\_rsa\_key, descripción, 326
- archivo ssh\_host\_rsa\_key.pub, descripción, 326
- archivo ssh\_known\_hosts, 327
- archivo sshd\_config
  - descripción, 326
  - palabras clave, 320–326
    - Ver palabra clave específica
  - valores de sustitución de entradas
    - /etc/default/login, 325–326
- archivo sshd.pid, descripción, 327
- archivo sshrc, descripción, 328
- archivo su, supervisión de comando su, 62–63
- archivo sulog, 62–63
  - supervisión de contenido de, 62
- archivo syslog.conf
  - depuración de privilegios, 216
  - entrada priv.debug, 216
  - mensajes de pilas ejecutables, 119
  - nivel audit.notice, 606
  - nivel kern.notice, 119
  - y auditoría, 644
- archivo user\_attr, excepciones para clases de auditoría
  - en todo el sistema, 553
- archivo/var/user/\$USER/krb-warn.conf,
  - descripción, 529
- archivo warn.conf, descripción, 528
- archivos
  - análisis de integridad, 93–109
- archivos (*Continuación*)
  - archivos especiales, 113–115
  - audit\_class, 643
  - audit\_event, 643
  - auditoría de modificaciones de, 632–634
  - búsqueda de archivos con permisos setuid, 126
  - cambio de permisos de archivo especiales, 125–126
  - cambio de propiedad, 112, 121–122
  - cambio de propiedad de grupo, 122
  - cifrado, 229–230, 238–241
  - con información de privilegios, 216–217
  - copia con Secure Shell, 313–314
  - cálculo de MAC de, 236–238
  - cálculo de resúmenes de, 234–235, 235
  - cálculo de un resumen, 234–235
  - descifrado, 239
  - hashing, 229–230
  - kdc.conf, 534
  - Kerberos, 527–529
  - manifiestos (BART), 106–107
  - manifiestos de BART, 106–107
  - montaje con autenticación DH, 344
  - objetos públicos, 550
  - para administrar Secure Shell, 326
  - permisos
    - bit de permanencia, 115
    - cambio, 112, 116–118, 123
    - descripción, 113
    - modo absoluto, 116, 124–125
    - modo simbólico, 116, 117, 123
    - setgid, 114–115
    - setuid, 114
    - valor umask, 115–116
    - valores predeterminados, 115–116
  - PKCS #12, 266
  - privilegios relacionados con, 145
  - propiedad
    - y permiso setgid, 114–115
    - y permiso setuid, 114
  - protección con permisos UNIX, 119–120
  - resumen de, 234–235
  - rsyslog.conf, 282–283, 605–607
  - seguimiento de integridad, 93–109



archivos (*Continuación*)

- seguridad
  - ACL, 48–49
  - cambio de permisos, 116–118, 123
  - cambio de propiedad, 121–122
  - cifrado, 48, 229–230
  - clases de usuario, 112
  - permisos de archivo, 113
  - permisos de archivo especiales, 117
  - permisos de directorio, 113
  - permisos UNIX, 111–118
  - restricción de acceso, 45
  - tipos de archivo, 112
  - umask predeterminado, 115–116
  - visualización de información de archivos, 112, 120–121
- syslog.conf, 282–283, 605–607
- syslog.conf, 644
- símbolos de tipo de archivo, 112
- tipos de archivo, 112
- uso compartido con autenticación DH, 343–344
- verificación de la integridad mediante
  - digest, 234–235
- visualización de archivos ocultos, 120
- visualización de información de archivos, 120–121
- visualización de información sobre, 112

archivos crontab, autorizaciones requeridas, 214

archivos de auditoría

- combinación, 616–618
- compresión en disco, 637–638
- copia de mensajes a un único archivo, 620
- creación de archivos de resumen, 619, 620
- efectos de hora universal coordinada (UTC), 617
- gestión, 623–624
- impresión, 621
- indicaciones de hora, 651
- lectura con `praudit`, 620–622
- limitación del tamaño de, 636–637
- reducción, 616–618
- reducción de requisitos de espacio, 574–575
- reducción de requisitos de espacio de
  - almacenamiento, 575
- reserva de espacio en disco para, 593–597
- sistemas de archivos ZFS, 593–597, 637–638

## archivos de configuración

- archivo `device_maps`, 88
- archivo `policy.conf`, 38, 59–60, 213
- archivo `syslog.conf`, 216
- auditoría, 643–644
- con información de privilegios, 216–217
- PAM
  - sintaxis, 285
- para algoritmos de contraseña, 38
- Secure Shell, 318

archivos de identidad (Secure Shell), convenciones de denominación, 326

## archivos de registro

- BART
  - salida detallada, 108–109
  - salida programática, 108–109
- configuración para servicio de auditoría, 605–607
- registros de auditoría, 555, 621
- registros de auditoría `syslog`, 644
- supervisión de comando `su`, 62–63
- `/var/adm/messages`, 628
- `/var/log/syslog`, 628

archivos ejecutables de 32 bits, evitar que se ponga en riesgo la seguridad, 118–119

archivos log, intentos de conexión fallidos, 59

archivos PKCS #12, protección, 266

arroba (@), archivo `device_allocate`, 90

asignaciones, eventos a clases (auditoría), 553

asignaciones de evento-clase de auditoría,

- cambio, 591–592

## asignación

- autorizaciones en un perfil de derechos, 180–181
- nombres de host en dominios (Kerberos), 363
- perfil de derechos
  - a un rol, 188–189
- privilegios a comandos en un perfil de derechos, 177
- privilegios a comandos en una secuencia de comandos, 203–204
- privilegios a usuario, 164
- privilegios al rol, 189
- rol para un usuario localmente, 173–174
- UID a principales de Kerberos, 543

asignación de credenciales GSS, 366



- asignación de dispositivo
  - comandos, 87
  - ejemplos, 82
- asignación de dispositivos
  - activación, 76–77
  - activación de asignación de dispositivos, 76–77
  - agregar dispositivos, 75–76
  - archivo de configuración, 88
  - archivo device\_allocate, 89–91
  - archivo device\_maps, 88–89
  - asignación forzada de dispositivos, 78–79
  - asignar dispositivos, 81–82
  - auditoría, 80–81
  - autorizaciones, 86–87
  - autorizaciones para comandos, 87–88
  - autorización de usuarios para asignar, 77
  - cambio de dispositivos asignables, 79–80
  - comando deallocate
    - secuencias de comandos device-clean y, 92
    - uso, 84
  - componentes del mecanismo, 86
  - desactivación, 77
  - desasignación de dispositivos, 84
  - desasignación forzada de dispositivos, 79
  - desmontaje de un dispositivo asignado, 84
  - dispositivos asignables, 90, 91
  - estado de error de asignación, 88
  - forzada, 78–79
  - gestión de dispositivos, 75–76
  - mapa de tareas, 75–76
  - montaje de dispositivos, 82–83
  - no requieren autorización, 80
  - perfiles de derechos, 86–87
  - permisos de resolución de problemas, 78
  - por usuarios, 81–82
  - prevención, 80
  - procedimientos de usuario, 75–81
  - requiere autorización, 79–80
  - resolución de problemas, 82, 83
  - secuencias de comandos device-clean
    - descripción, 91–92
    - opciones, 92
    - redacción de secuencias de comandos nuevas, 92
  - servicio SMF, 86
- asignación de dispositivos (*Continuación*)
  - uso, 75–81
  - uso del comando allocate, 81–82
  - visualización de información, 78
- asterisco (\*)
  - archivo device\_allocate, 89, 90
  - carácter comodín
    - en autorizaciones RBAC, 209
  - comprobación en autorizaciones RBAC, 182
- asunción de rol, cómo, 168–186
- asunción de un rol, en una ventana de terminal, 161–162
- asunción del rol, root, 161–162
- atributo qsize, complementos de auditoría, 587–588
- atributos, palabra clave en BART, 98
- atributos de archivo de reglas, *Ver* palabras clave
- atributos de seguridad
  - comprobar, 139
  - consideraciones al asignar directamente, 143
  - consideraciones de uso al asignar directamente, 143
  - descripción, 135
  - ID especial en comandos, 140
  - lista de todos los RBAC, 157–158
  - orden de búsqueda, 207
  - perfil de derechos de seguridad de la red, 137
  - privilegios en comandos, 140
  - uso para montar dispositivo asignado, 77
- auditoría
  - activación, 613–614
  - actualización de información, 611–613
  - agregación de indicadores de auditoría a un grupo de usuarios, 584–585
  - asignación de dispositivos, 80–81
  - búsqueda de cambios en archivos
    - específicos, 632–634
  - cambios en la versión actual, 562
  - cambios en política de dispositivos, 74
  - configuración
    - idéntica para todas las zonas, 607–610
    - por zona, 610–611
    - todas las zonas, 577–592
    - zona global, 586
  - configuración en la zona global, 564
  - definición de preselección, 550

auditoría (*Continuación*)

- definición de selección posterior, 550
- definición local, 550
- definición remota, 551
- desactivación, 613
- determinación de ejecución, 626–628
- eliminación de indicadores de auditoría específicos de usuario, 584
- establecimiento de controles de colas, 587–588
- inicios de sesión, 638–639
- módulos de complemento, 554
- obtención de controles de colas, 587–588
- perfiles de derechos para, 644–645
- planificación, 563–570
- planificación en zonas, 564–565
- privilegios y, 217
- resolución de problemas, 625–626
- resolución de problemas de comando praudit, 622
- resúmenes de páginas del comando man, 643–644
- roles, 174–175
- servidor de auditoría remota (ARS), 558
- sólo usuarios, 583–584
- todos los comandos por usuarios, 630–632
- transferencias de archivos de sftp, 639–640
- valores predeterminados, 641–642
- zonas y, 561–562, 645

## auditoría local, 550

## auditoría remota, 551

## autenticación

- archivos montados en NFS, 343, 344
- autenticación DH, 336–340
- configuración entre dominios, 393–395
- desactivación con la opción -X, 522
- descripción, 51–52
- descripción general de Kerberos, 537
- Kerberos y, 347
- RPC segura, 335
- Secure Shell
  - métodos, 294–295
  - proceso, 318–319
- seguridad de red, 51–52
- servicios de nombres, 335
- sesión cliente-servidor AUTH\_DH, 337–340
- terminología, 531–532

autenticación (*Continuación*)

- tipos, 51–52
- uso con NFS, 335
- autenticación AUTH\_DES, *Ver* autenticación AUTH\_DH
- autenticación AUTH\_DH, y NFS, 335
- autenticación basada en host
  - configuración en Secure Shell, 298–301
  - descripción, 294
- autenticación de clave pública, Secure Shell, 294
- autenticación de contraseña, Secure Shell, 294
- autenticación DH
  - configuración en NIS, 341–342
  - descripción, 336–340
  - montaje de archivos con, 344
  - para cliente NIS, 341–342
  - uso compartido de archivos con, 343–344
- autenticación Diffie-Hellman, *Ver* autenticación DH
- autenticación entre dominios, configuración, 393–395
- autenticación Kerberos, y RPC segura, 336
- autenticador
  - en Kerberos, 532, 539
- automatización de la creación de principales, 477–478
- autorizaciones
  - agregación a perfil de derechos, 180–181
  - asignación de dispositivos, 86–87
  - eliminación desde perfil de derechos, 179
  - Kerberos y, 347
  - solución de problemas, 182–186
  - tipos, 51–52
- autorizaciones (RBAC)
  - base de datos, 209–212
  - comandos que requieren autorizaciones, 214–215
  - comprobación de caracteres comodín, 182
  - comprobar en aplicación con privilegios, 140
  - convención de denominación, 209
  - definición, 138–139
  - delegar, 209
  - descripción, 135, 208–209
  - granularidad, 209
  - no requieren asignación de dispositivos, 80
  - para asignación de dispositivos, 87–88
  - para asignar dispositivos, 77
  - solaris.device.allocate, 77, 87
  - solaris.device.revoke, 88

autorización `solaris.admin.edit`, agregación a perfil de derechos, 178

autorización `solaris.device.revoke`, 88

autorización `solaris.smf.value`, eliminación desde perfil de derechos, 179

ayuda

- herramienta SEAM, 474
- URL en línea, 370

ayuda contextual, herramienta SEAM, 474

ayuda en pantalla

- herramienta SEAM, 474
- URL para, 370

## B

barra diagonal inversa (\)

- archivo `device_allocate`, 89, 90

BART

- componentes, 94–95
- consideraciones de seguridad, 96
- descripción general, 93–95
- mapa de tareas, 96
- salida detallada, 109
- salida programática, 109

base de datos `auth_attr`

- descripción, 211
- resumen, 209

base de datos `cred`, autenticación DH, 336–340

base de datos de usuario (RBAC), *Ver* base de datos `user_attr`

base de datos `exec_attr`

- descripción, 212
- resumen, 209

base de datos `prof_attr`

- descripción, 211
- resumen, 209

base de datos `user_attr`

- descripción, 209, 210–211
- enumeración de excepciones de usuario para preselección de auditoría, 581–585

bases de datos

- `auth_attr`, 211
- claves secretas NFS, 337
- copia de seguridad y propagación de KDC, 430–431

bases de datos (*Continuación*)

- creación de KDC, 377
- `cred` para RPC segura, 337
- `exec_attr`, 212
- `prof_attr`, 211
- propagación de KDC, 367
- `publickey` para RPC segura, 337
- RBAC, 209–212
- `user_attr`, 210–211

biblioteca `/usr/lib/libsasl.so`, descripción general, 331

biblioteca PKCS #11

- agregación de biblioteca de proveedor, 247
- en la estructura criptográfica, 223

bibliotecas, proveedores de nivel de usuario, 242

bloques Match

- directorio `chroot` y, 303–304
- excepciones para valores predeterminados del sistema Secure Shell, 302–303

## C

opción `-C`, comando `auditreduce`, 618

shell C, versión con privilegios, 142

caballo de Troya, 44

cambio

- algoritmo de contraseña para un dominio, 61
- algoritmo de contraseña predeterminado, 59–62
- archivo `audit_class`, 590–591
- archivo `audit_event`, 591–592
- contenido de perfil de derechos, 175–177
- contraseña de rol, 187–188
- contraseña root, 56
- dispositivos asignables, 79–80
- la frase de contraseña para Secure Shell, 307
- mapa de tareas de algoritmo de contraseña, 59–62
- permisos de archivo
  - especiales, 125–126
  - modo absoluto, 124–125
  - modo simbólico, 123
- permisos de archivo especiales, 125–126
- propiedad de archivo, 121–122
- propiedad de grupo de archivo, 122
- propiedades de rol, 188–189

cambio (*Continuación*)

- rol root a usuario, 192–194
- su contraseña con `kpasswd`, 516
- su contraseña con `passwd`, 516
- valores predeterminados de auditoría, 580–581

## caracteres comodín

- en autorizaciones RBAC, 209
- para hosts en Secure Shell, 314

## características de auditoría

- ID de sesión, 651
- ID de terminal, 651
- ID de usuario de auditoría, 650
- máscara de preselección de procesos de usuario, 650
- procesos, 650–651

## características de auditoría de proceso

- ID de sesión de auditoría, 651
- ID de terminal, 651
- ID de usuario de auditoría, 650
- máscara de preselección de procesos, 650

Centro de distribución de claves, *Ver* KDC

## certificado X.509 v3, generación, 272–273

## certificados

- exportación para uso por parte de otro sistema, 266–267
- firma de CSR PKCS #10
  - uso del comando `pktool`, 272–273
- generación con comando `pktool`
  - `gencert`, 263–264
- importación en almacén de claves, 264–265

## cifrado

- algoritmo de contraseña, 38
- algoritmo DES, 336
- algoritmos
  - Kerberos y, 369–370
- archivos, 48, 229–230, 238–241
- clave privada del usuario NIS, 342
- comando `encrypt`, 238–241
- con la opción `-x`, 522
- contraseñas, 59–62
- especificación de algoritmo de contraseña
  - localmente, 59–62
- especificación de algoritmos de contraseña en el archivo `policy.conf`, 38

cifrado (*Continuación*)

- especificación de algoritmos en archivo `ssh_config`, 321
  - generación de clave simétrica
    - uso del comando `pktool`, 230–234
  - las comunicaciones entre hosts, 308
  - lista de algoritmos de contraseña, 38
  - modos
    - Kerberos y, 369–370
  - NFS seguro, 336
  - servicio de privacidad, 347
  - tipos
    - Kerberos y, 369–370, 541–543
  - tráfico de red entre hosts, 293–295
  - uso de comandos de nivel de usuario, 226–227
- cifrado DES, NFS seguro, 336
- cifrado DES, proveedor de núcleo, 242
- clase de auditoría `all`, precaución de uso, 646
- clases, *Ver* clases de auditoría
- clases *auditar\_nunca*, máscara de preselección de procesos, 650
- clases *auditar\_siempre*, máscara de preselección de procesos, 650
- clases de auditoría
- agregación, 590–591
  - asignación de eventos, 553
  - configuración, 646–647
  - descripción, 548, 551
  - descripción general, 552–553
  - excepciones de usuarios, 581–585
  - excepciones para configuraciones en todo el sistema, 553
  - modificación de valor predeterminado, 590–591
  - máscara de preselección de procesos, 650
  - prefijos, 646–647
  - preselección, 550
    - efecto en objetos públicos, 550
    - para fallo, 583, 605, 606
    - para éxito, 583, 605
    - para éxito y fallo, 580–581
  - reemplazo, 580–581
  - selección posterior, 550
  - sintaxis, 646
  - visualización de valores predeterminados, 578–580

- clases de usuario de archivos, 112
- claves
  - clave de servicio, 504–510
  - claves de sesión
    - autenticación de Kerberos y, 537
  - creación de clave DH para usuario NIS, 342–343
  - creación para Secure Shell, 305–307
  - definición en Kerberos, 531
  - generación de clave simétrica
    - uso del comando `pktool`, 230–234
  - generación de par de claves
    - uso del comando `pktool`, 268–272
  - generación para Secure Shell, 305–307
  - uso para MAC, 237
- claves comunes
  - autenticación DH y, 336–340
  - cálculo, 339
- claves de conversación
  - descifrado en RPC segura, 339
  - generación en RPC segura, 338
- claves de servicio
  - archivos `keytab` y, 504–510
  - definición en Kerberos, 531
- claves de sesión
  - autenticación de Kerberos y, 537
  - definición en Kerberos, 531
- claves privadas
  - Ver también* claves secretas
  - archivos de identidad de Secure Shell, 326
  - definición en Kerberos, 531
- claves públicas
  - archivos de identidad de Secure Shell, 326
  - autenticación DH y, 336–340
  - cambio de frase de contraseña, 307
  - generación de par de clave pública y clave privada, 305–307
- claves secretas
  - creación, 230–234
  - generación
    - uso del comando `pktool`, 230–234
  - generación para RPC segura, 337
- clientes
  - configuración de Kerberos, 405–423
  - configuración para Secure Shell, 318, 320
  - clientes (*Continuación*)
    - definición en Kerberos, 531
    - sesión cliente-servidor `AUTH_DH`, 337–340
  - clonación, contenido de perfil de derechos, 177–179
  - cola de auditoría, eventos incluidos, 553
  - comando `/usr/bin/ftp`, Kerberos y, 529
  - comando `/usr/bin/kdestroy`, Kerberos y, 529
  - comando `/usr/bin/kinit`, Kerberos y, 529
  - comando `/usr/bin/klist`, Kerberos y, 529
  - comando `/usr/bin/kpasswd`, Kerberos y, 529
  - comando `/usr/bin/ktutil`, Kerberos y, 529
  - comando `/usr/bin/kvno`, Kerberos y, 529
  - comando `/usr/bin/rcp`, Kerberos y, 529
  - comando `/usr/bin/rlogin`, Kerberos y, 529
  - comando `/usr/bin/rsh`, Kerberos y, 529
  - comando `/usr/bin/scp`, Kerberos y, 529
  - comando `/usr/bin/sftp`, Kerberos y, 529
  - comando `/usr/bin/ssh`, Kerberos y, 529
  - comando `/usr/bin/telnet`, Kerberos y, 529
  - comando `/usr/lib/kprop`, descripción, 529
  - comando `/usr/sbin/gkadmin`, descripción, 529
  - comando `/usr/sbin/gsscred`, descripción, 530
  - comando `/usr/sbin/kadmin`, descripción, 530
  - comando `/usr/sbin/kadmin.local`, descripción, 530
  - comando `/usr/sbin/kclient`, descripción, 530
  - comando `/usr/sbin/kdb5_ldap_util`, descripción, 530
  - comando `/usr/sbin/kdb5_util`, descripción, 530
  - comando `/usr/sbin/kgcmgr`, descripción, 530
  - comando `/usr/sbin/kproplog`, descripción, 530
  - comando `add_drv`, descripción, 85
  - comando `allocate`
    - autorizaciones requeridas, 88, 214
    - autorización de usuario, 77
    - estado de error de asignación, 88
    - medio extraíble, 82
    - uso, 81–82
  - comando `at`, autorizaciones requeridas, 214
  - comando `atq`, autorizaciones requeridas, 214
  - comando `audit`
    - desactivación de servicio de auditoría, 613
    - opciones, 643
    - refrescamiento de servicio de auditoría, 611–613
  - comando `audit -s`, 611–613, 613–614

- comando `audit -t`, 613
- comando `auditconfig`
  - agregación de sistemas de archivos de auditoría, 597–599
  - clases de auditoría como argumentos, 552
  - configuración de atributos
    - `audit_binfile`, 597–599
  - configuración de atributos `audit_remote`, 600–601
  - configuración de controles de colas, 587–588
  - configuración de parámetros de auditoría en todo el sistema, 552
  - configuración de política, 585–587
  - configuración de política de auditoría, 631
  - descripción, 643
  - envío de archivos a repositorio remoto, 600–601, 601–605
  - establecimiento de atributos
    - `audit_remote`, 601–605
  - establecimiento de política de auditoría
    - activa, 586–587
  - establecimiento de política de auditoría
    - temporal, 586–587
  - opciones de control de colas, 587–588
  - opciones de política, 585–587
  - opción `-getplugin`, 600–601, 601–605, 605–607
  - opción `-setflags`, 580–581
  - opción `-setnaflags`, 580–581
  - opción `-setplugin`, 600–601, 601–605, 605–607
  - preselección de clases de auditoría, 580–581
  - visualización de preselección de auditoría
    - predeterminada, 580–581
  - visualización de valores predeterminados de auditoría, 578–580
- comando `auditrecord`
  - [ ] (corchetes) en salida, 652
  - descripción, 644
  - ejemplo, 615
  - lista de formatos de clase, 616
  - lista de formatos de programa, 615–616
  - lista de todos los formatos, 615
  - tokens opcionales ([ ]), 652
  - visualización de definiciones de registros de auditoría, 615–616
- comando `auditreduce`
  - depuración de archivos de auditoría, 622–623
  - descripción, 644
  - ejemplos, 616–618
  - filtrado de opciones, 618
  - fusión de registros de auditoría, 616–618
  - opción `-A`, 618
  - opción `-b`, 619
  - opción `-C`, 618
  - opción `-c`, 620
  - opción `-d`, 620
  - opción `-e`, 619–620
  - opción `-M`, 618
  - opción `-O`, 616–618, 618, 619–620
  - selección de registros de auditoría, 618–620
  - tokens trailer y, 662
  - uso de indicación de hora, 617
  - uso de opciones en mayúscula, 617
  - uso de opciones en minúscula, 618
- comando `auditstat`, descripción, 644
- comando `auths`, descripción, 213
- comando `bart create`, 94, 96–98
- comando `cd rw`, autorizaciones requeridas, 214
- comando `chgrp`
  - descripción, 112
  - sintaxis, 122
- comando `chkey`, 337, 342
- comando `chmod`
  - cambio de permisos especiales, 125–126, 126
  - descripción, 112
  - sintaxis, 125
- comando `chown`, descripción, 112
- comando `crypt`, seguridad de archivos, 48
- comando `cryptoadm`
  - desactivación de mecanismos criptográficos, 249, 251
  - desactivación de mecanismos de
    - hardware, 255–256
  - descripción, 225
  - instalación de una biblioteca PKCS #11, 247
  - lista de proveedores, 242
  - opción `-m`, 250, 251
  - opción `-p`, 250, 251

- comando `cryptoadm` (*Continuación*)
  - restauración de un proveedor de software de núcleo, 252
- comando `cryptoadm install`, instalación de una biblioteca PKCS #11, 247
- comando `csch`, versión con privilegios, 142
- comando `dealloc`
  - autorizaciones requeridas, 88, 214
  - estado de error de asignación, 88
  - secuencias de comandos `device-clean` y, 92
  - uso, 84
- comando `decrypt`
  - descripción, 226
  - sintaxis, 239
- comando `delete_entry`, comando `ktutil`, 509
- comando `devfsadm`, descripción, 85
- comando `digest`
  - descripción, 226
  - ejemplo, 235
  - sintaxis, 234
- comando `dminfo`, 88
- comando `eeeprom`, 36, 65–66
- comando `eject`, limpieza de dispositivos y, 92
- comando `elfsign`, descripción, 227
- comando `encrypt`
  - descripción, 226
  - mensajes de error, 240
  - resolución de problemas, 240
- comando `find`, búsqueda de archivos con permisos `setuid`, 126
- comando `ftp`
  - definición de nivel de protección en, 523
  - Kerberos y, 520–523, 529
  - registro de transferencias de archivos, 639–640
- comando `getdevpolicy`, descripción, 85
- comando `getent`, descripción, 213
- comando `gkadmin`
  - Ver también herramienta SEAM
  - descripción, 529
- comando `gsscred`, descripción, 530
- comando `kadmin`
  - comando `ktadd`, 505–506
  - comando `ktremove`, 507
  - creación de principal `host`, 378, 385
- comando `kadmin` (*Continuación*)
  - descripción, 530
  - eliminación de principales de `keytab` con, 506–507
  - herramienta SEAM y, 472
- comando `kadmin.local`
  - adición de principales de administración, 384
  - automatización de la creación de principales, 477
  - descripción, 530
- comando `kclient`, descripción, 530
- comando `kdb5_ldap_util`, descripción, 530
- comando `kdb5_util`
  - creación de archivo intermedio, 391, 440
  - creación de base de datos KDC, 377
  - descripción, 530
- comando `kdcmgr`
  - configuración de esclavo
    - automática, 387
    - interactiva, 387
  - configuración de maestro
    - automática, 374
    - interactiva, 375
  - estado de servidor, 375
- comando `kdestroy`
  - ejemplo, 514–515
  - Kerberos y, 529
- comando `keylogin`, uso para RPC segura, 337
- comando `kgcmgr`, descripción, 530
- comando `kinit`
  - duración de `ticket`, 534
  - ejemplo, 512–513
  - Kerberos y, 529
  - opción `-F`, 512
- comando `klist`
  - ejemplo, 513–514
  - Kerberos y, 529
  - opción `-f`, 513–514
- comando `kmfcfg`
  - subcomando `list plugin`, 273–274
  - subcomandos de complemento, 260
  - subcomandos de complementos, 261
- comando `kpasswd`
  - comando `passwd` y, 516
  - ejemplo, 518
  - Kerberos y, 529



- comando `kpasswd` (*Continuación*)
  - mensaje de error, 517
- comando `kprop`, descripción, 529
- comando `kproplog`, descripción, 530
- comando `ksh`, versión con privilegios, 142
- comando `ktadd`
  - adición de principal de servicio, 504, 505–506
  - sintaxis, 505
- comando `ktremove`, 507
- comando `ktutil`
  - administración del archivo `keytab`, 504
  - comando `delete_entry`, 509
  - comando `list`, 508, 509
  - comando `read_kt`, 508, 509
  - Kerberos y, 529
  - visualización de la lista de principales, 507–508
  - visualización de lista de principales, 507
- comando `kvno`, Kerberos y, 529
- comando `list`, 508, 509
- comando `list_devices`
  - autorizaciones requeridas, 88, 214
- comando `logadm`, archivo de archivos de auditoría de resumen de texto, 624
- comando `logins`
  - sintaxis, 57
  - visualización de estado de inicio de sesión de usuario, 57–58
  - visualización de usuarios sin contraseñas, 58
- comando `mac`
  - descripción, 226
  - sintaxis, 236
- comando `mount`, con atributos de seguridad, 77
- comando `mt`, 91
- comando `newkey`
  - creación de clave para usuario NIS, 342–343
  - generación de claves, 337
- comando `nisaddcred`, generación de claves, 337
- comando `pam_roles`, descripción, 213
- comando `passwd`
  - cambio de contraseña de rol, 187–188
  - sintaxis, 56
  - y comando `kpasswd`, 516
  - y servicios de nombres, 37
- comando `perfiles`, descripción, 213
- comando `pfcsch`, descripción, 142
- comando `pfedit`, descripción, 213
- comando `pfexec`, descripción, 213
- comando `pfksh`, descripción, 142
- comando `pfsh`, descripción, 142
- comando `pktool`
  - administración de objetos PKI, 260
  - creación de un certificado autofirmado, 263–264
  - firma de CSR PKCS #10, 272–273
  - generación de claves secretas, 230–234
  - generación de pares de claves, 268–272
  - subcomando `export`, 266–267
  - subcomando `gencert`, 263–264
  - subcomando `import`, 264–265
  - subcomando `list`, 263
  - subcomando `setpin`, 267–268
- comando `ppriv`, enumeración de privilegios, 199
- comando `praudit`
  - conducción de salida de `audit reduce a`, 621
  - conversión de registros de auditoría a formato legible, 621
  - descripción, 644
  - formato XML, 621
  - uso en una secuencia de comandos, 621–622
  - visualización de registros de auditoría, 620–622
- comando `profile`, modificación de perfil de derechos, 177
- comando `profiles`
  - creación de perfiles de derechos, 175–177
  - enumeración de perfiles de derechos de usuario, 160
- comando `rcp`
  - Kerberos y, 520–523, 529
- comando `read_kt`, 508, 509
- comando `rem_drv`, descripción, 85
- comando `rlogin`
  - Kerberos y, 520–523, 529
- comando `roleadd`
  - descripción, 213
  - uso, 171
- comando `rolemod`
  - cambio de propiedades de rol, 188, 191
  - contraseñas para roles, 189–190, 191–192
  - descripción, 213



- comando roles
  - descripción, 213
  - uso, 161
- comando rsh
  - Kerberos y, 520–523, 529
- comando rsh (shell restringido), 45
- comando scp
  - copia de archivos con, 313–314
  - descripción, 329
  - Kerberos y, 529
- comando sendmail, autorizaciones requeridas, 215
- comando sftp
  - auditoría de transferencias de archivos, 639–640
  - copia de archivos con, 314
  - descripción, 329
  - directorio chroot y, 303–304
  - Kerberos y, 529
- comando sh, versión con privilegios, 142
- comando ssh
  - administración remota de ZFS, 310–311
  - descripción, 329
  - Kerberos y, 529
  - opciones de reenvío del puerto, 312–313
  - uso, 307–308
  - uso de un comando de proxy, 315
  - valores de sustitución de palabras clave, 329
- comando ssh-add
  - almacenamiento de claves privadas, 309–310
  - descripción, 329
  - ejemplo, 309–310
- comando ssh-agent
  - descripción, 329
  - desde la línea de comandos, 309–310
- comando ssh-keygen
  - descripción, 329
  - protección de frase de contraseña, 296
  - uso, 305–307
- comando ssh-keyscan, descripción, 329
- comando ssh-keysign, descripción, 329
- comando sshd, descripción, 329
- comando su
  - en asunción de rol, 161–162
  - mostrar intentos de acceso en la consola, 63–65
  - supervisión de uso, 62–63
- comando svcadm
  - activación de daemon de servidor de claves, 341
  - activación de la estructura criptográfica, 256–257
  - administración de la estructura criptográfica, 225, 226
  - refrescar la estructura criptográfica, 246–247
  - reinicio
    - daemon syslog, 606
    - Secure Shell, 301
- comando svcs
  - lista de servicios criptográficos, 256–257
  - listado de servicio de servidor de claves, 341
- comando tail, ejemplo de uso, 576
- comando telnet
  - Kerberos y, 520–523, 529
- comando truss, para depuración de privilegios, 201
- comando umount, con atributos de seguridad, 77
- comando update\_drv, descripción, 85
- comando useradd, descripción, 213
- comando userattr
  - descripción, 213
  - visualización de excepciones a auditoría en todo el sistema, 578–580
- comando userdel, descripción, 213
- comando usermod
  - cambio de propiedades RBAC de usuario, 162
  - descripción, 214
- comando usermod
  - especificación de excepciones de usuario para preselección de auditoría, 581–585
- comando usermod
  - excepciones para auditoría en todo el sistema, 553
- comando usermod
  - palabra clave audit\_flags, 581–585
  - uso de prefijo (^) de signo de intercalación para excepción audit\_flags, 583
- comando usermod
  - uso para asignar rol, 173–174
- comando xauth, reenvío de X11, 324
- comandos
  - Ver también* comandos individuales
  - comandos criptográficos de nivel de usuario, 226–227
  - comandos de administración RBAC, 213–214

comandos (*Continuación*)

- comandos de asignación de dispositivos, 87
- comandos de la estructura criptográfica, 226
- comandos de política de dispositivos, 85
- comandos de protección de archivos, 111
- comandos de RPC segura, 337
- comandos Secure Shell, 329–330
- determinación de comandos con privilegios de usuario, 198–199
- Kerberos, 529–530
  - para administrar privilegios, 215
  - que asignan privilegios, 150
  - que comprueban privilegios, 140
- comandos de Kerberos, 520–526
- comandos de shell, transferencia de número de proceso de shell principal, 199
- comandos Kerberizados, ejemplos, 525–526
- combinación de archivos de auditoría, desde distintas zonas, 645
- combinación de archivos de auditoría, comando `auditreduce`, 616–618
- compatibilidad con FIPS-140
  - acceso remoto de Secure Shell, 297–298
  - Secure Shell mediante una tarjeta Sun Crypto Accelerator 6000, 297–298
- complemento `audit_binfile`, 554
  - configuración de advertencia de espacio libre, 599
  - configuración de atributos, 597–599
  - eliminación de tamaño de cola, 599
  - limitación de tamaño de archivo de auditoría, 598
  - obtención de atributos, 598, 599
- complemento `audit_remote`, 554
  - configuración, 601–605
  - configuración de atributos, 600–601
  - establecimiento de atributos, 601–605
  - obtención de atributos, 600–601, 601–605
  - resolución de problemas de cola de auditoría llena, 601
- complemento `audit_syslog`, 554
  - configuración de atributos, 605–607
- complemento `crammd5.so.1`, SASL y, 332
- complemento de mecanismo de seguridad EXTERNAL, SASL y, 332
- complemento `digestmd5.so.1`, SASL y, 332

- complemento `gssapi.so.1`, SASL y, 332
- complemento INTERNAL, SASL y, 332
- complemento `plain.so.1`, SASL y, 332
- complementos
  - agregación a KMF, 273–274
  - auditoría, 554
  - eliminación de KMF, 273–274
  - estructura criptográfica, 223
  - gestionados en KMF, 261
  - SASL y, 332
- complementos de auditoría
  - atributo `qsize`, 587–588
  - complemento `audit_binfile`, 587–588, 597–599
  - complemento `audit_remote`, 600–601, 601–605
  - complemento `audit_syslog`, 605–607
  - descripción, 549
  - resumen, 643–644, 647, 648
- componentes
  - BART, 94–95
  - mecanismo de asignación de dispositivos, 86
  - RBAC, 135–137
  - sesión de usuario de Secure Shell, 319
- compresión, archivos de auditoría en disco, 637–638
- comprobación de privilegios, en aplicaciones, 140
- conexión, log de conexiones fallidas, 59
- conexión segura, por medio de un cortafuegos, 314
- configuración
  - archivo `audit_class`, 590–591
  - archivo `audit_event`, 591–592
  - asignación de dispositivos, 75–76
  - auditoría, 577–592
  - auditoría en zonas, 561–562, 645
  - auditoría idéntica para zonas no globales, 607–610
  - auditoría por zona, 610–611
  - autenticación basada en host para Secure Shell, 298–301
  - autorizaciones, 180–181
  - clases de auditoría, 580–581
  - clave DH en NIS, 341–342
  - clave DH para usuario NIS, 342–343
  - contraseña para acceso al hardware, 65–66
  - controles de colas de auditoría, 587–588
  - directorio `chroot` para `sftp`, 303–304
  - espacio para pista de auditoría, 597–599

configuración (*Continuación*)

- excepciones para valores predeterminados del sistema Secure Shell, 302–303
- Kerberos
  - adición de principales de administración, 384
  - autenticación entre dominios, 393–395
  - clientes, 405–423
  - descripción general, 371–450
  - mapa de tareas, 371–372
  - servidor KDC esclavo, 386–387, 387–388, 388–392
  - servidor KDC maestro, 374, 375, 376–379
  - servidor KDC maestro con LDAP, 380–386
  - servidores NFS, 399–401
- mapa de tareas de auditoría, 578
- mapa de tareas de RBAC, 168–169
- mapa de tareas de registros de auditoría, 593
- mapa de tareas de Secure Shell, 298
- perfiles de derechos, 175–177
- política arge, 632
- política argv, 631
- política de auditoría, 585–587
- política de auditoría activa, 586–587
- política de auditoría ahlt, 586
- política de auditoría permanente, 585–587
- política de auditoría perzone, 587
- política de auditoría temporal, 585–587
- política de dispositivos, 73–74
- política de servicio de auditoría, 585–587
- prevención de desbordamiento de pista de auditoría, 623–624
- RBAC, 168–186
- reenvío del puerto en Secure Shell, 301
- resúmenes de texto de registros de auditoría, 605–607
- rol root a usuario, 192–194
- roles, 171–173, 188–189
- secuencia de comandos audit\_warn, 589
- Secure Shell
  - clientes, 320
  - servidores, 320
- seguridad del hardware, 65–66
- usuarios con privilegios, 163–164

configuración (*Continuación*)

- valores predeterminados de principal (Kerberos), 487–488
- configuración automática
  - Kerberos
    - servidor KDC esclavo, 386–387
    - servidor KDC maestro, 374
- configuración de servicio de nombres, restricciones de acceso de inicio de sesión, 36
- configuración de servidores de aplicaciones, 395–398
- configuración del cortafuegos de Internet, 53
- configuración interactiva
  - Kerberos
    - servidor KDC esclavo, 387–388
    - servidor KDC maestro, 375
- configuración manual
  - Kerberos
    - servidor KDC esclavo, 388–392
    - servidor KDC maestro, 376–379
    - servidor KDC maestro con LDAP, 380–386
- conjunto básico de privilegios, 149
- conjunto heredable de privilegios, 148
- conjunto límite de privilegios, 148
- conjunto permitido de privilegios, 148
- conjunto vigente de privilegios, 148
- conjuntos de privilegios
  - agregar privilegios a, 151
  - básicos, 149
  - eliminar privilegios de, 151
  - enumerar, 149
  - heredables, 148
  - límite, 148
  - permitidos, 148
  - vigentes, 148
- consola, mostrar intentos del comando su, 63–65
- CONSOLE en Secure Shell, 325
- consumidores, definición en la estructura criptográfica, 224
- contraseñas
  - acceso al hardware y, 65–66
  - algoritmos de cifrado, 38
  - autenticación en Secure Shell, 294
  - búsqueda de usuarios sin contraseñas, 58
  - cambio con el comando kpasswd, 516

contraseñas (*Continuación*)

- cambio con el comando `passwd`, 516
- cambio con el comando `passwd -r`, 37
- cambio de contraseña de rol, 187–188
- descifrado de clave secreta para RPC segura, 337
- eliminación en Secure Shell, 309–310
- especificación de algoritmo, 59–60
  - en servicios de nombres, 61
  - localmente, 59–62
- gestión, 515–520
- inicios de sesión en el sistema, 37
- LDAP, 37
  - especificación de nuevo algoritmo de contraseña, 61–62
- locales, 37
- mapa de tareas, 55–56
- modificación de la contraseña de un principal, 486
- modo de seguridad de PROM, 36, 65–66
- NIS, 37
  - especificación de nuevo algoritmo de contraseña, 61
- otorgamiento de acceso sin revelar, 518–520
- políticas y, 516
- protección
  - almacén de claves, 266
  - archivo PKCS #12, 266
- requerir para acceso al hardware, 65–66
- restricción de algoritmos de cifrado en un entorno heterogéneo, 60
- seguridad de inicio de sesión, 36, 37
- sugerencias para la elección, 515–516
- UNIX y Kerberos, 515–520
- uso de algoritmo de cifrado MD5 para, 59–60
- uso de Blowfish en un entorno heterogéneo, 60
- uso de nuevo algoritmo, 60
- uso de usuario para asumir rol, 189–190, 191–192
- visualización de usuarios sin contraseñas, 58

control, uso del sistema, 43–47

control de acceso basado en roles, *Ver* RBAC

control de costos, y auditoría, 573

control de recursos `project.max-locked-memory`, 147

control de recursos `zone.max-locked-memory`, 147

controlador `n2cp`

- complemento de hardware para estructura criptográfica, 223
- lista de mecanismos, 254

controlador `ncp`

- complemento de hardware para estructura criptográfica, 223
- lista de mecanismos, 254

controles de cola de auditoría, obtención, 587–588

controles de colas de auditoría, visualización de valores predeterminados, 578–580

controles de recursos

- privilegios y, 147
- `project.max-locked-memory`, 147
- `zone.max-locked-memory`, 147

convenciones de denominación

- archivos de auditoría, 651
- archivos de identidad de Secure Shell, 326
- autorizaciones RBAC, 209
- devices, 78

conversión, registros de auditoría en formato legible, 621

copia, archivos con Secure Shell, 313–314

copia de registros de auditoría a un único archivo, 620

copia de seguridad

- base de datos de Kerberos, 430–431
- KDC esclavos, 365

corchetes ([ ]), salida `audit record`, 652

correcto, prefijo de clase de auditoría, 646–647

correo, uso con Secure Shell, 312

costos de almacenamiento, y auditoría, 574–575

costos de tiempo de procesamiento, de servicio de auditoría, 574

creación

- almacenamiento para archivos de auditoría binarios, 593–597
- archivo intermedio, 391, 440
- autorización, 180–181
- claves de Secure Shell, 305–307
- claves secretas
  - para cifrado, 230–234
- nueva política (Kerberos), 482, 495–496
- nuevo principal (Kerberos), 482–484
- par de claves, 268–272

creación (*Continuación*)  
 perfil de derechos para un grupo de usuarios, 584–585  
 perfiles de derechos, 175–177  
 pista de auditoría, 651  
 resúmenes de archivos, 234–235  
 roles, 171–173  
 secuencias de comandos device-clean nuevas, 92  
 tabla de credenciales, 401  
 tickets con kinit, 512–513  
 usuario root, 192–194  
 usuarios con privilegios, 163–164

credencial  
 asignación, 366  
 descripción, 338, 532  
 o tickets, 349  
 obtención para un servidor, 539  
 obtención para un TGS, 537–538

credenciales, antememoria, 537

criptografía de clave pública  
 base de datos de claves públicas para RPC  
 segura, 337  
 claves comunes  
 cálculo, 339  
 claves secretas NFS, 337  
 generación de claves  
 claves de conversación para NFS seguro, 338  
 uso de Diffie-Hellman, 337  
 modificación de claves públicas y claves secretas NFS, 337  
 sesión cliente-servidor AUTH\_DH, 337–340

Cryptoki, *Ver* Biblioteca PKCS #11

CSR PKCS #10, uso, 272–273

cuenta root, descripción, 40

cuentas de usuario  
 cambio de contraseña root, 56  
 visualización de estado de inicio de sesión, 57–58

cuentas de usuarios  
*Ver también* usuarios

cálculo  
 clave secreta, 230–234  
 MAC de un archivo, 236–238  
 resumen de un archivo, 234–235

código de autenticación de mensajes (MAC), cálculo para archivo, 236–238

## D

opción -D, comando ppriv, 201

daemon /usr/lib/inet/proftpd, Kerberos y, 530

daemon /usr/lib/krb5/kadmind, Kerberos y, 530

daemon /usr/lib/krb5/kpropd, Kerberos y, 530

daemon /usr/lib/krb5/krb5kdc, Kerberos y, 530

daemon /usr/lib/krb5/ktkt\_warnd, Kerberos y, 530

daemon /usr/sbin/in.rlogind, Kerberos y, 530

daemon /usr/sbin/in.rshd, Kerberos y, 530

daemon /usr/sbin/in.telnetd, Kerberos y, 530

daemon auditd  
 refrescamiento de servicio de auditoría, 611, 612

daemon de agente, Secure Shell, 309–310

daemon gssd, Kerberos y, 530–531

daemon in.rlogind, Kerberos y, 530

daemon in.rshd, Kerberos y, 530

daemon in.telnetd, Kerberos y, 530

daemon kadmind  
 KDC maestro y, 531  
 Kerberos y, 530

daemon kcfd, 226, 256–257

daemon keyserv, 340–341

daemon kpropd, Kerberos y, 530

daemon krb5kdc  
 inicio, 392, 440  
 KDC maestro y, 531  
 Kerberos y, 530

daemon ktkt\_warnd, Kerberos y, 530

daemon proftpd, Kerberos y, 530

daemon rlogind, Kerberos y, 530

daemon rshd, Kerberos y, 530

daemon sshd, Kerberos y, 530

daemon telnetd, Kerberos y, 530

daemon/usr/lib/ssh/sshd, Kerberos y, 530

daemons  
 ejecutar con privilegios, 146

kcfd, 226

keyserv, 340–341

nscd (daemon de caché de servicio de nombres), 213

daemons (*Continuación*)

ssh-agent, 309–310

sshd, 317–319

tabla de Kerberos, 530–531

## decisiones de configuración

algoritmo de contraseña, 38

## auditoría

a quién y qué auditar, 565–568

almacenamiento de archivos, 568–569

almacenamiento remoto de archivos, 569–570

política, 571–573

zonas, 564–565

## Kerberos

asignación de nombres de host en dominios, 363

clientes, 367–368

dominios, 362–363

jerarquía de dominios, 363

KDC esclavos, 365

nombres de dominio, 362

nombres de principal de servicio y cliente, 364

número de dominios, 362–363

propagación de base de datos, 367

puertos, 365

servidor KDC, 368–369

sincronización de reloj, 367

tipos de cifrado, 369–370

delegar, autorizaciones RBAC, 209

depuración, archivos de auditoría binarios, 622–623

derecho, *Ver* perfiles de derechosderechos, restricción de administrador a asignado de  
forma explícita, 190–191

## desactivación

acceso root remoto, 63–65

archivos ejecutables de 32 bits que ponen en riesgo la  
seguridad, 118–119

asignación de dispositivos, 77

cierre del teclado, 66

inicios de sesión de usuario, 58–59

inicios de sesión temporalmente, 58–59

interrupción del teclado, 66

mecanismos criptográficos, 249

mecanismos de hardware, 255–256

pilas ejecutables, 127–128

política de auditoría, 585–587

desactivación (*Continuación*)

programas que utilicen pilas ejecutables, 127–128

registro de mensajes de pilas ejecutables, 128

secuencia de interrupción, 66

secuencia de interrupción del sistema, 66

servicio de auditoría, 613

servicio en un host (Kerberos), 508–510

## desasignación

dispositivos, 84

forzada, 79

micrófono, 84

## descifrado

archivos, 239

claves de conversación para RPC segura, 339

claves secretas, 337

claves secretas NFS, 337

desfase de reloj, Kerberos y, 424–425

desinstalación, proveedores criptográficos, 251

desmontaje, dispositivos asignados, 84

destrucción, tickets con kdest roy, 514–515

detención (RBAC), perfil de derechos, 206

## determinación

archivos con permisos setuid, 126

auditoría en ejecución, 626–628

ID de auditoría de un usuario, 635

mapa de tareas de privilegios, 194

privilegios en un proceso, 199–200

## direcciones IP

comprobación de Secure Shell, 321

excepciones para valores predeterminados de Secure  
Shell, 302–303

directorio chroot, sftp y, 303–304

directorio de auditoría, creación de sistemas de archivos  
para, 593–597

## directorios

*Ver también* archivos

directorios públicos, 115

## permisos

descripción, 113

valores predeterminados, 115–116

visualización de archivos e información  
relacionada, 112, 120–121

## directorios públicos

auditoría, 550

directorios públicos (*Continuación*)  
 bit de permanencia y, 115  
 disco duro, requisitos de espacio para  
 auditoría, 574–575  
 disposición de espacio de direcciones, ejecución  
 aleatoria de tiempo de carga, 43  
 dispositivo /dev/arp, obtención de información  
 MIB-II IP, 75  
 dispositivos  
 activación de asignación, 76–77  
 asignación de dispositivos  
*Ver* asignación de dispositivos  
 asignación forzada, 78–79  
 asignación para uso, 75–81  
 auditoría de asignación, 80–81  
 auditoría de cambios en política, 74  
 autorización de usuarios para asignar, 77  
 cambio de los que se pueden asignar, 79–80  
 comandos de política, 85  
 control de acceso de inicio de sesión, 41  
 desasignación de un dispositivo, 84  
 desasignación forzada, 79  
 desmontaje de un dispositivo asignado, 84  
 enumeración, 74  
 enumeración de nombres de dispositivos, 78  
 gestión, 73–74  
 gestión de asignación de, 75–76  
 modelo de privilegios y, 152  
 modelo de superusuario y, 152  
 montaje de dispositivos asignados, 82–83  
 no requieren autorización para uso, 80  
 obtención de información MIB-II IP, 75  
 prevención de uso de algunos, 80  
 prevención de uso de todos, 80  
 protección en el núcleo, 41  
 protección por asignación de dispositivos, 41  
 seguridad, 41–42  
 visualización de información de asignación, 78  
 visualización de política de dispositivos, 74  
 zonas y, 41  
 dispositivos de audio, seguridad, 92  
 dispositivos SCSI, secuencia de comandos  
 st\_clean, 91  
 DNS, Kerberos y, 364

dominios (Kerberos)  
 asignación de nombres de host en, 363  
 configuración de autenticación entre  
 dominios, 393–395  
 contenidos de, 354  
 decisiones de configuración, 362–363  
 directos, 394–395  
 en nombres de principales, 352–353  
 jerarquía, 363  
 jerárquicos, 393–394  
 jerárquicos o no jerárquicos, 353  
 nombres, 362  
 número de, 362–363  
 servidores y, 354  
 solicitud de tickets para dominios específicos, 522  
 dominios directos, 394–395  
 dominios jerárquicos  
 configuración, 393–394  
 en Kerberos, 353, 363  
 dominios no jerárquicos, en Kerberos, 353  
 duplicación, principales (Kerberos), 485  
 duración de tickets, en Kerberos, 534–535

## E

eficacia, auditoría y, 575  
 ejecución aleatoria de tiempo de carga, disposición de  
 espacio de direcciones, 43  
 ejecución de comandos, Secure Shell, 319  
 elección, su contraseña, 515–516  
 eliminación  
 auditoría específica de usuario, 584  
 complementos de KMF, 273–274  
 eventos de auditoría del archivo  
 audit\_event, 635–636  
 principal de servicio del archivo keytab, 506–507  
 principales con el comando kt remove, 507  
 privilegios de conjunto básico, 176  
 privilegios de conjunto límite, 164  
 privilegios de conjunto límite en perfil de  
 derechos, 177  
 proveedores criptográficos, 251  
 proveedores de software  
 permanente, 253



- eliminación, proveedores de software (*Continuación*)
    - temporal, 252
  - enlaces simbólicos, permisos de archivo, 113
  - entrada `audit.notice`, archivo `syslog.conf`, 606
  - entrada `kern.notice`, archivo `syslog.conf`, 119
  - entrada `priv.debug`, archivo `syslog.conf`, 216
  - entrada `rsyslog.conf`
    - creación para PAM, 282–283
    - creación para registros de auditoría de tiempo real, 605–607
  - entrada `syslog.conf`
    - creación para PAM, 282–283
    - creación para registros de auditoría de tiempo real, 605–607
  - enumeración
    - contenido de almacenes de claves, 263
    - derechos de usuario inicial, 158–160
    - política de dispositivos, 74
    - roles que puede asumir, 161
    - sus derechos RBAC, 158–160
  - enumerar, roles que puede asumir, 213
  - Equipo de Respuesta ante Emergencias Informáticas/Centro de Coordinación (CERT/CC), 54
  - equivalentes de línea de comandos de la herramienta SEAM, 473–474
  - errores, estado de error de asignación, 88
  - espacio de direcciones, disposición aleatoria, 43
  - espacio en disco, para archivos de auditoría binarios, 593–597
  - establecimiento
    - controles de colas de auditoría, 587–588
    - política de auditoría, 585–587
  - estado de error de asignación, 88
  - estructura criptográfica
    - administración con rol, 174
    - biblioteca PKCS #11, 223
    - comando `cryptoadm`, 225, 226
    - comando `elfsign`, 227
    - comandos de nivel de usuario, 226–227
    - complementos de hardware, 223
    - conexión de proveedores, 227
    - consumidores, 223
    - definición de términos, 223
    - estructura criptográfica (*Continuación*)
      - descripción, 221–223
      - FIPS-140 y, 228
      - firma de proveedores, 227
      - interacción con, 225–227
      - lista de proveedores, 242–246
      - mensajes de error, 240
      - optimizaciones de SPARC T4 series, 228
      - proveedores, 223
      - refrescar, 256–257
      - registro de proveedores, 227
      - reinicio, 256–257
      - zonas y, 227, 256–257
  - estructura de gestión de claves (KMF), *Ver* KMF
  - estándar de cifrado de datos, *Ver* cifrado DES
  - evento, descripción, 551
  - eventos de auditoría
    - archivo `audit_event`, 551
    - asignación a clases, 553
    - asíncronos, 649–650
    - cambio de pertenencia a clase, 591–592
    - descripción, 551
    - eliminación del archivo `audit_event`, 635–636
    - resumen, 548
    - selección de pista de auditoría, 618–620
    - selección desde pista de auditoría en zonas, 645
    - síncronos, 649–650
    - visualización desde archivos binarios, 620–622
  - eventos de auditoría asíncronos, 649–650
- F**
- opción `-f`
    - comandos Kerberizados, 521, 523–524
    - secuencia de comandos `st_clean`, 92
  - opción `-F`
    - comando `deallocate`, 88
    - comandos Kerberizados, 522, 523–524
  - fallo, prefijo de clase de auditoría, 646–647
  - FIPS-140, estructura criptográfica y, 228
  - firma
    - CSR PKCS #10, 272–273
    - uso del comando `pktool`, 272–273
  - firma de proveedores, estructura criptográfica, 227



flecha de agregación (>>), prevención de agregación, 45  
 flecha de redirección (>), prevención de redirección, 45  
 formato de archivo de reglas (BART), 107–108  
 formato de registro de auditoría legible, conversión de registros de auditoría en, 621  
 formato de registros de auditoría, comando `auditrecord`, 615  
 formato XML, registros de auditorías, 621  
 FQDN (nombre de dominio completo), en Kerberos, 364  
 frases de contraseña  
   almacenamiento seguro, 239  
   comando `encrypt`, 238  
   comando `mac`, 236  
   generación en KMF, 267–268  
   uso para MAC, 237  
 frases de contraseñas  
   cambio para Secure Shell, 307  
   ejemplo, 308  
   uso en Secure Shell, 309–310  
 fusión, registros de auditoría binarios, 616–618

## G

generación  
   certificado X.509 v3, 272–273  
   certificados con comando `pktool`, 263–264  
   clave simétrica  
     uso del comando `pktool`, 230–234  
   claves de Secure Shell, 305–307  
   claves para Secure Shell, 305–307  
   claves secretas NFS, 337  
   frases de contraseña con el comando `pktool`, 267–268  
   número aleatorio  
     uso del comando `pktool`, 230–234  
   par de claves  
     uso del comando `pktool`, 268–272  
 gestión  
   *Ver también* administración  
   almacenes de claves con KMF, 261  
   archivos de auditoría, 616–618, 623–624

gestión (*Continuación*)  
   auditoría  
     prevención de desbordamiento de pista de auditoría, 623–624  
     auditoría en zonas, 561–562, 564–565, 645  
     contraseñas con Kerberos, 515–520  
     desbordamiento de pista de auditoría, 623–624  
     dispositivos, 75–76  
     mapa de tareas de asignación de dispositivos, 75–76  
     mapa de tareas de privilegios, 194  
     mapa de tareas de RBAC, 186–187  
     mapa de tareas de registros de auditoría, 614–615  
     permisos de archivo, 119–128  
   gestión de criptografía (RBAC), creación de rol, 174  
   gestión de derechos de procesos, *Ver* privilegios  
   gestión de derechos de usuarios, *Ver* privilegios  
   gestión de dispositivos, *Ver* política de dispositivos  
   gestión de impresoras (RBAC), perfil de derechos, 206  
 grupos  
   cambio de propiedad de archivo, 122  
   excepciones para valores predeterminados de Secure Shell, 302–303  
 GSS-API  
   autenticación en Secure Shell, 294  
   credenciales en Secure Shell, 318  
   Kerberos y, 348

## H

hardware  
   estructura criptográfica y, 228  
   lista de aceleradores de hardware conectados, 254  
   protección, 35–36, 65–66  
   requerir contraseña para acceso, 65–66  
   SPARC T4 series, 228  
 hardware del sistema, control de acceso a, 65–66  
 hash  
   algoritmos  
     Kerberos y, 369–370  
   hashing, archivos, 229–230  
   Help Contents, herramienta SEAM, 474  
   herramienta básica de creación de informes de auditoría, *Ver* BART

- herramienta de generación de informes, *Ver*
  - comparación `bart`
- herramienta SEAM
  - archivo `.gkadmin`, 474
  - archivos modificados por, 474
  - ayuda, 474
  - ayuda contextual, 474
  - ayuda en pantalla, 474
  - campo Filter Pattern, 479
  - comando `gkadmin`, 471
  - comando `kadmin`, 471
  - configuración de valores predeterminados de principal, 487–488
  - creación de un nuevo principal, 482–484
  - creación de una nueva política, 482, 495–496
  - descripción de paneles, 499–502
  - descripción general, 472–476
  - duplicación de un principal, 485
  - efecto de los privilegios, 503
  - equivalentes de línea de comandos, 473–474
  - Help Contents, 474
  - inicio, 475–476
  - modificación de un principal, 485–486
  - modificación de una política, 497–498
  - o comando `kadmin`, 472
  - privilegios, 502
  - supresión de políticas, 498–499
  - supresión de un principal, 487
  - tabla de paneles, 499–502
  - valores predeterminados, 475
  - ventana de inicio de sesión, 475
  - visualización de atributos de política, 493–495
  - visualización de la lista de políticas, 491–493
  - visualización de la lista de principales, 478–480
  - visualización de los atributos de un principal, 480–482
  - visualización de sublista de principales, 479
  - y privilegios de administración limitados, 502–503
  - y privilegios de lista, 502
  - y sistema de ventanas X, 473–474
- hora universal coordinada (UTC)
  - uso de indicaciones de hora en auditoría, 651
  - uso de indicación de hora en auditoría, 617

- hosts
  - desactivación de servicio de Kerberos en, 508–510
  - excepciones para valores predeterminados de Secure Shell, 302–303
  - hosts de confianza, 53
  - hosts de Secure Shell, 294
- hosts de confianza, 53

## I

- opción `-I`
  - comando `bart create`, 97
  - secuencia de comandos `st_clean`, 92
- ID, asignación de UNIX a principales de Kerberos, 543
- ID de sesión, auditoría, 651
- ID de sesión de auditoría, 651
  - descripción general, 547–548
- ID de terminal, auditoría, 651
- ID de usuario
  - en servicios NFS, 401
  - ID de auditoría y, 547–548, 650
- ID de usuario de auditoría
  - descripción general, 547–548
  - mecanismo, 650
- identificadores
  - auditoría
    - mecanismo, 650
    - sesión de auditoría, 651
- idioma de especificación de archivo de reglas, *Ver* *sintaxis de comillas*
- IDs
  - auditoría
    - descripción general, 547–548
- impedir
  - uso de mecanismo de hardware, 255–256
  - uso de un proveedor de software de núcleo, 251–254
- impresión, registro de auditoría, 621
- indicaciones de hora, archivos de auditoría, 651
- indicador de control "binding", PAM, 288
- indicador de control "definitive", PAM, 288
- indicador de control "include", PAM, 288
- indicador de control "optional", PAM, 289
- indicador de control "required", PAM, 289

- indicador de control "requisite", PAM, 289
- indicador de control "sufficient", PAM, 289
- indicadores de auditoría, resumen, 548
- indicadores de control, PAM, 288
- informes, BART, 93
- informática, clave DH, 342
- iniciar sesión, conjunto básico de privilegios del usuario, 149
- inicio
  - asignación de dispositivos, 76–77
  - auditoría, 613–614
  - daemon del KDC, 392, 440
  - servidor de claves RPC segura, 340–341
- inicio de sesión
  - auditoría de inicios de sesión, 638–639
  - con Secure Shell, 307–308
  - con Secure Shell para mostrar una GUI, 308
  - desactivación temporal, 58–59
- inicio de sesión root
  - restricción de la consola, 63–65
  - seguimiento, 43–44
- mapa de tareas, 55–56
- seguridad
  - control de acceso al sistema, 36
  - control de acceso en dispositivos, 41
  - restricciones de acceso, 36
  - seguimiento de inicio de sesión root, 43–44
- visualización de estado de inicio de sesión de usuario, 57–58
- y AUTH\_DH, 337

inicio de sesión automático

- activación, 521
- desactivación, 522

inicios de sesión remotos

- autenticación, 51–52
- autorización, 51–52
- impedir el acceso root, 63–65
- seguridad y, 339

instalación, seguridad predeterminada, 46

instancias, en nombres de principales, 352–353

integridad

- Kerberos y, 347
- servicio de seguridad, 355

intercambio de KDC maestros y esclavos, 425–430

## K

opción -k

- comando encrypt, 238
- comando mac, 236
- comandos Kerberizados, 522

opción -K

- comando rolemod, 189
- comando usermod, 164
- comandos Kerberizados, 522

KDC

- configuración de esclavo
  - automática, 386–387
  - interactiva, 387–388
  - manual, 388–392
- configuración de maestro
  - automática, 374
  - interactiva, 375
  - manual, 376–379
- configuración de servidor maestro
  - con LDAP, 380–386
- copia de archivos de administración del esclavo al maestro, 390, 438
- copia de seguridad y propagación, 430–431
- creación de base de datos, 377
- creación de principal host, 378, 385
- esclavo, 365
  - definición, 531
- esclavo o maestro, 354, 373
- inicio de daemon, 392, 440
- intercambio de maestro y esclavo, 425–430
- maestro
  - definición, 531
- planificación, 365
- propagación de base de datos, 367
- puertos, 365
- restricción de acceso a servidores, 449
- sincronización de relojes
  - KDC esclavo, 392, 440
  - KDC maestro, 379, 386

KDC esclavos

- configuración, 388–392
- configuración automática, 386–387
- configuración interactiva, 387–388
- intercambio con KDC maestro, 425–430

**KDC esclavos** (*Continuación*)

- KDC maestro y, 354
- o maestro, 373
- planificación para, 365

**KDC maestro**

- configuración automática, 374
- configuración con LDAP, 380–386
- configuración interactiva, 375
- configuración manual, 376–379
- definición, 531
- intercambio con KDC esclavo, 425–430
- KDC esclavos y, 354, 373

**KDC maestros, definición,** 531**Kerberos**

- administración, 471–510
- aplicaciones remotas, 352
- archivos, 527–529
- ayuda pantalla, 370
- comandos, 520–526, 529–530
- componentes de, 356–357
- configuración de servidores KDC, 373–392
- daemons, 530–531
- decisiones de configuración, 361–370
- descripción general
  - comandos Kerberizados, 520–523
  - sistema de autenticación, 348–354, 537
- dominios
  - Ver* dominios (Kerberos)
- ejemplos de uso de comandos
  - Kerberizados, 525–526
- gestión de contraseñas, 515–520
- herramientas de administración
  - Ver* herramienta SEAM
- mensajes de error, 451–466
- obtención de acceso al servidor, 537–540
- opciones para comandos Kerberizados, 521
- otorgamiento de acceso a su cuenta, 518–520
- planificación de, 361–370
- protocolo Kerberos V5, 347
- referencia, 527–543
- resolución de problemas, 466
- tabla de opciones de comandos de red, 522
- terminología, 531–536

**Kerberos** (*Continuación*)

- tipos de cifrado
    - descripción general, 369–370
    - uso, 541–543
  - uso, 511–526
- KMF**
- administración
    - política PKI, 261
    - tecnologías de clave pública (PKI), 259
  - agregación de complemento, 273–274
  - almacenes de claves, 260, 261
  - biblioteca, 260
  - creación
    - certificado autofirmado, 263–264
    - contraseña para almacén de claves, 267–268
    - frases de contraseña para almacenes de claves, 262
  - eliminación de complemento, 273–274
  - enumeración de complementos, 273–274
  - exportación de certificados, 266–267
  - gestión
    - almacenes de claves, 261
    - complementos, 261
  - importación de certificados en almacén de claves, 264–265
  - utilidades, 260

**L**

- opción -L, comando ssh, 312–313
- LDAP, configuración de KDC maestro con, 380–386
- limitación
  - tamaño de archivo de auditoría, 636–637
  - uso de privilegios en un perfil de derechos, 176
- limpieza estándar, secuencia de comandos
  - st\_clean, 92
- limpieza forzada, secuencia de comandos st\_clean, 92
- lista
  - proveedores de estructura criptográfica, 254
  - proveedores de hardware, 254
  - proveedores de la estructura criptográfica, 242–246
  - proveedores disponibles de la estructura criptográfica, 242–246
  - todos los atributos de seguridad de RBAC, 157–158

lista (*Continuación*)

- usuarios sin contraseñas, 58

## lista de control de acceso

- Ver ACL

## listas de control de acceso (ACL), Ver ACL

## llamadas de sistema

- ioctl para limpiar dispositivo de audio, 92

- token de auditoría `exec_args`, 656

- token de auditoría `exec_env`, 656

- token de auditoría `return`, 660

llamadas del sistema, token de auditoría `argument`, 655llamadas del sistema `ioctl()`, `AUDIO_SETINFO()`, 92línea `flags`, máscara de preselección de procesos, 650**M**opción `-M`, comando `auditreduce`, 618

## manifiestos

- Ver también `bart create`

- control, 93

- formato de archivo, 106–107

- personalización, 99–100

- prueba en BART, 95

## manifiestos de control (BART), 93

## manifiestos de prueba, BART, 95

mapa `publickey`, autenticación DH, 336–340

## mapas de tarea

- gestión de registros de auditoría, 614–615

- resolución de problemas de auditoría, 625–626

## mapas de tareas

- administración de la estructura

- criptográfica, 241–242

- administración de políticas (Kerberos), 490–491

- administración de principales (Kerberos), 476–477

- administración de RPC segura, 340

- asignación de dispositivos, 75–76

- configuración de auditoría, 578

- configuración de Kerberos, 371–372

- configuración de política de dispositivos, 73–74

- configuración de RBAC, 168–169

- configuración de registros de auditoría, 593

- configuración de Secure Shell, 298

- configuración de servidores NFS con Kerberos, 398

- gestión de asignación de dispositivos, 75–76

mapas de tareas (*Continuación*)

- gestión de política de dispositivos, 73–74

- gestión de RBAC, 186–187

- mantenimiento de Kerberos, 372

- PAM, 279

- planificación de auditoría, 563–570

- política de dispositivos, 73–74

- privilegios, enumeración, gestión y uso, 194

- protección contra programas con riesgo de seguridad, 126

- protección de archivos con mecanismos

- criptográficos, 229–230

- protección de archivos con permisos UNIX, 119

- protección de inicios de sesión y contraseñas, 55–56

- uso de la configuración predeterminada de

- RBAC, 156–157

- uso de la estructura de gestión de claves (mapa de tareas), 262–263

- uso de RBAC, 155–156

- uso de Secure Shell, 304–305

- uso del mapa de tareas de BART, 96

## mecanismo, definición en la estructura

- criptográfica, 224

## mecanismo de seguridad, especificación con la opción

- `-m`, 522

mecanismo `mech_dh`, credenciales GSS-API, 318mecanismo `mech_krb`, credenciales GSS-API, 318

## mecanismos

- activación de algunos en el proveedor de

- hardware, 256

- desactivación de todo en el proveedor de

- hardware, 255–256

## mecanismos criptográficos, optimizado para SPARC T4

- series, 228

## mediante, permisos de archivo, 119–128

## medio extraíble, asignación, 82

medios, secuencias de comandos `device-clean`, 91–92

## mensajes de error

- comando `encrypt`, 240

- con `kpasswd`, 517

- Kerberos, 451–466

## metarranura

- administración, 226

- definición en la estructura criptográfica, 224

- MIB-II IP, obtención de información de /dev/arp no de /dev/Ip, 75
  - micrófono
    - asignación, 81
    - desasignación, 84
  - modificación
    - atributos de seguridad del usuario, 581–585
    - claves secretas NFS, 337
    - contraseña de principal (Kerberos), 486
    - políticas (Kerberos), 497–498
    - principales (Kerberos), 485–486
    - roles (RBAC), 188–189
    - usuarios (RBAC), 162–164
  - modificador de eventos de auditoría fe, 657
  - modificador de eventos de auditoría fp, 657
  - modificador de eventos de auditoría na, 657
  - modificador de eventos de auditoría rd, 657
  - modificador de eventos de auditoría sp, 657
  - modificador de eventos de auditoría wr, 657
  - modificadores de eventos, registros de auditoría, 657
  - modo, definición en la estructura criptográfica, 224
  - modo absoluto
    - cambio de permisos de archivo, 116, 124–125
    - cambio de permisos de archivo especiales, 125–126
    - configuración de permisos especiales, 117
    - descripción, 116
  - modo de seguridad de PROM, 65–66
  - modo simbólico
    - cambio de permisos de archivo, 117, 123
    - descripción, 116
  - modos de permiso de archivo
    - modo absoluto, 116
    - modo simbólico, 117
  - modos de seguridad, configuración de entorno con varios, 403–405
  - montaje
    - archivos con autenticación DH, 344
    - CD-ROM asignado, 83
    - dispositivos asignados, 82–83
  - mostrar
    - intentos de acceso root, 63–65
    - intentos del comando su, 63–65
    - roles que puede asumir, 213
  - máscara (auditoría), descripción de preselección de procesos, 650
  - máscara de preselección (auditoría), descripción, 650
  - máscara de preselección de auditoría
    - modificación para usuarios existentes, 634–635
    - modificación para usuarios individuales, 581–585
  - máscara de preselección de procesos, descripción, 650
  - métodos de autenticación
    - basada en host en Secure Shell, 298–301
    - basado en host en Secure Shell, 295
    - claves públicas en Secure Shell, 295
    - contraseña en Secure Shell, 295
    - credenciales GSS-API en Secure Shell, 295
    - Secure Shell, 294–295
  - módulo de autenticación conectable, Ver PAM
  - módulo pam\_tty\_tickets.so.1, PAM, 166
  - módulos, cifrado de contraseña, 38
  - módulos PAM, 166
- ## N
- NFS seguro, 336
  - nivel de protección
    - definición en ftp, 523
    - privado, 523
    - seguro, 523
    - sin cifrar, 523
  - nivel de protección privado, 523
  - nivel de protección seguro, 523
  - nivel de protección sin cifrar, 523
  - nombres
    - nombres de dispositivos
      - archivo device\_maps, 89, 90
    - nombres de cliente, planificación en Kerberos, 364
    - nombres de host, asignación en dominios, 363
    - ns cd (daemon de caché de servicio de nombres),
      - usar, 213
  - NSS, gestión de almacén de claves, 261
  - NTP
    - esclavo KDC y, 440
    - KDC esclavo y, 392
    - KDC maestro y, 379, 386
    - planificación de Kerberos y, 367

## nuevas funciones

- mejoras de la auditoría, 562
- mejoras de Secure Shell, 296–297
- SASL, 331
- Secure Shell y FIPS-140, 297–298

número de secuencia de depuración, 661

números aleatorios, comando `pktool`, 230–234

números de ID de usuario (UID), cuentas especiales y, 40

**O**

## opción -O

- comando `auditreduce`, 616–618, 618, 619–620

objetos públicos, auditoría, 550

## obtención

- acceso a un servicio específico, 540
- comandos con privilegios, 188–189
- credencial para un servidor, 539
- credencial para un TGS, 537–538
- privilegios, 150, 164, 189
- privilegios en un proceso, 199–200
- tickets con `kinit`, 512–513
- tickets reenviables, 512

obtener, privilegios, 149

opciones para comandos Kerberizados, 521

## opción -a

- comando `auditrecord`, 615
- comando `digest`, 235
- comando `encrypt`, 238
- comando `mac`, 236
- comandos Kerberizados, 521

opción -b, comando `auditreduce`, 619

## opción -c

- comando `auditrecord`, 616
- comando `auditreduce`, 620

## opción -d

- comando `auditreduce`, 619, 620

## opción -e

- comando `auditreduce`, 619–620
- comando `ppriv`, 201

opción -h, comando `auditrecord`, 615

## opción -i

- comando `bart create`, 97, 100

opción -i (*Continuación*)

- comando `encrypt`, 238
- secuencia de comandos `st_clean`, 92

## opción -K

- comando `encrypt`, 238
- comando `mac`, 236

## opción -l

- comando `digest`, 234
- comando `mac`, 236
- comando `ssh`, 307–308

## opción -m

- comando `cryptoadm`, 250, 251
- comandos Kerberizados, 522

opción -n, comando `bart create`, 97

opción -o, comando `encrypt`, 238

## opción -p

- `bart create`, 100
- comando `auditrecord`, 615–616
- comando `cryptoadm`, 250, 251
- comando `logins`, 58

## opción -r

- `bart create`, 100
- comando `passwd`, 37

## opción -s

- comando `audit`, 611–613, 613–614

## opción -T

- comando `encrypt`, 238
- comando `mac`, 236

opción -t, comando `audit`, 613

## opción -v

- comando `digest`, 235
- comando `mac`, 236
- comando `ppriv`, 199

## opción -X

- comando `ssh`, 308

opción -x, comandos Kerberizados, 522

opción `auto_transition`, SASL y, 333

opción `auxprop_login`, SASL y, 333

opción `canon_user_plugin`, SASL y, 333

opción de instalación con seguridad predeterminada, 46

opción de instalación `netservices limited`, 46

opción `-getflags`

- comando `auditconfig`, 578–580, 580–581



- opción -getnaflags
  - comando auditconfig, 578–580, 580–581
- opción -getplugin
  - comando auditconfig, 578–580, 600–601, 601–605, 605–607
- opción -getpolicy
  - comando auditconfig, 578–580, 585–587
- opción -getqctrl, comando auditconfig, 578–580
- opción keytab, SASL y, 333
- opción log\_level, SASL y, 333
- opción -lspolicy, comando auditconfig, 585–587
- opción mech\_list, SASL y, 333
- opción plugin\_list, SASL y, 333
- opción pwcheck\_method, SASL y, 333
- opción reauth\_timeout, SASL y, 333
- opción rewoffl, comando mt, 91
- opción saslauthd\_path, SASL y, 333
- opción -setflags, comando auditconfig, 580–581
- opción -setnaflags, comando auditconfig, 580–581
- opción -setplugin
  - comando auditconfig, 600–601, 601–605, 605–607
- opción -setpolicy, comando auditconfig, 585–587
- opción use\_authid, SASL y, 333
- OpenSSH, *Ver* Secure Shell
- OpenSSL
  - gestión de almacén de claves, 261
  - versión, 260
- operador (RBAC)
  - perfil de derechos, 206
  - rol recomendado, 133
- orden de búsqueda
  - atributos de seguridad, 207
  - atributos de seguridad de usuarios, 208
- otorgamiento de acceso a su cuenta, 518–520

## P

- palabra clave AllowGroups, archivo sshd\_config, 321
- palabra clave AllowTcpForwarding
  - archivo sshd\_config, 321
  - cambio, 301
- palabra clave AllowUsers, archivo sshd\_config, 321
- palabra clave audit\_flags, 580

- palabra clave audit\_flags (*Continuación*)
  - especificación de excepciones de usuario para preselección de auditoría, 581–585
  - uso, 647
  - uso de prefijo (^) de signo de intercalación, 583
- palabra clave AuthorizedKeysFile, archivo sshd\_config, 321
- palabra clave AUTHS\_GRANTED, archivo policy.conf, 212
- palabra clave Banner, archivo sshd\_config, 321
- palabra clave Batchmode, archivo ssh\_config, 321
- palabra clave BindAddress, archivo ssh\_config, 321
- palabra clave ChallengeResponseAuthentication, *Ver* palabra clave KbdInteractiveAuthentication
- palabra clave CheckHostIP, archivo ssh\_config, 321
- palabra clave ChrootDirectory, archivo ssh\_config, 321
- palabra clave Cipher, archivo ssh\_config, 321
- palabra clave Ciphers, Secure Shell, 321
- palabra clave ClearAllForwardings, reenvío del puerto de Secure Shell, 321
- palabra clave ClientAliveCountMax, archivo ssh\_config, 321
- palabra clave ClientAliveInterval, archivo ssh\_config, 321
- palabra clave Compression, Secure Shell, 321
- palabra clave CompressionLevel, archivo ssh\_config, 321
- palabra clave ConnectionAttempts, archivo ssh\_config, 321
- palabra clave ConnectTimeout, archivo ssh\_config, 321
- palabra clave CONSOLE\_USER, archivo policy.conf, 212
- palabra clave CRYPT\_ALGORITHMS\_ALLOW, archivo policy.conf, 39
- palabra clave CRYPT\_ALGORITHMS\_DEPRECATE, archivopolicy.conf, 39
- palabra clave CRYPT\_DEFAULT, archivo policy.conf, 39
- palabra clave DenyGroups, archivo sshd\_config, 321
- palabra clave DenyUsers, archivo sshd\_config, 321
- palabra clave DisableBanner, archivo ssh\_config, 321



- palabra clave DSAAuthentication, *Ver* palabra clave PubkeyAuthentication
- palabra clave DynamicForward, archivo `ssh_config`, 321
- palabra clave EscapeChar, archivo `ssh_config`, 321
- palabra clave FallBackToRsh, archivo `ssh_config`, 321
- palabra clave ForwardAgent, autenticación de reenvío de Secure Shell, 322
- palabra clave ForwardX11, reenvío del puerto de Secure Shell, 322
- palabra clave ForwardX11Trusted, reenvío del puerto de Secure Shell, 322
- palabra clave GatewayPorts, Secure Shell, 322
- palabra clave GlobalKnownHostsFile  
*Ver* palabra clave GlobalKnownHostsFile  
archivo `ssh_config`, 322
- palabra clave GSSAPIAuthentication, Secure Shell, 322
- palabra clave GSSAPIDelegateCredentials, archivo `ssh_config`, 322
- palabra clave GSSAPIKeyExchange, Secure Shell, 322
- palabra clave GSSAPIStoreDelegatedCredentials, archivo `sshd_config`, 322
- palabra clave HashKnownHosts, archivo `ssh_config`, 322
- palabra clave Host  
archivo `ssh_config`, 322, 325
- palabra clave HostbasedAuthentication, Secure Shell, 322
- palabra clave HostbasedUsesNameFromPacketOnly, archivo `sshd_config`, 322
- palabra clave HostKey, archivo `sshd_config`, 322
- palabra clave HostKeyAlgorithms, archivo `ssh_config`, 322
- palabra clave HostKeyAlias, archivo `ssh_config`, 322
- palabra clave HostName, archivo `ssh_config`, 322
- palabra clave IgnoreIfUnknown, archivo `ssh_config`, 322
- palabra clave IgnoreRhosts, archivo `sshd_config`, 322
- palabra clave IgnoreUserKnownHosts, archivo `sshd_config`, 322
- palabra clave KbdInteractiveAuthentication, Secure Shell, 322
- palabra clave KeepAlive, Secure Shell, 322
- palabra clave KeyRegenerationInterval, archivo `sshd_config`, 322
- palabra clave ListenAddress, archivo `sshd_config`, 323
- palabra clave LocalForward, archivo `ssh_config`, 323
- palabra clave LoginGraceTime, archivo `sshd_config`, 323
- palabra clave LogLevel, Secure Shell, 323
- palabra clave LookupClientHostnames, archivo `sshd_config`, 323
- palabra clave MACS, Secure Shell, 323
- palabra clave Match, archivo `sshd_config`, 323
- palabra clave MaxStartups, archivo `sshd_config`, 323
- palabra clave NoHostAuthenticationForLocalHost, archivo `ssh_config`, 323
- palabra clave NumberOfPasswordPrompts, archivo `ssh_config`, 323
- palabra clave PAMServiceName, archivo `sshd_config`, 323
- palabra clave PAMServicePrefix, archivo `sshd_config`, 323
- palabra clave PasswordAuthentication, Secure Shell, 323
- palabra clave PermitEmptyPasswords, archivo `sshd_config`, 323
- palabra clave PermitRootLogin, archivo `sshd_config`, 323
- palabra clave PermitUserEnvironment, archivo `sshd_config`, 323
- palabra clave PidFile, Secure Shell, 323
- palabra clave Port, Secure Shell, 323
- palabra clave PreferredAuthentications, archivo `ssh_config`, 323
- palabra clave PreUserauthHook, archivo `ssh_config`, 323
- palabra clave PrintLastLog, archivo `ssh_config`, 323
- palabra clave PrintMotd, archivo `sshd_config`, 323
- palabra clave PRIV\_DEFAULT  
archivo `policy.conf`, 212, 216
- palabra clave PRIV\_LIMIT  
archivo `policy.conf`, 212, 216

- palabra clave PROFS\_GRANTED, archivo
  - policy.conf, 212
- palabra clave Protocol, Secure Shell, 323
- palabra clave ProxyCommand, archivo ssh\_config, 323
- palabra clave PubkeyAuthentication, Secure Shell, 324
- palabra clave RekeyLimit, archivo ssh\_config, 324
- palabra clave RemoteForward, archivo
  - ssh\_config, 324
- palabra clave RhostsAuthentication, Secure Shell, 324
- palabra clave RhostsRSAAuthentication, Secure Shell, 324
- palabra clave roleauth
  - contraseñas para roles, 189–190, 191–192
- palabra clave RSAAuthentication, Secure Shell, 324
- palabra clave ServerAliveCountMax, archivo
  - ssh\_config, 324
- palabra clave ServerAliveInterval, archivo
  - ssh\_config, 324
- palabra clave ServerKeyBits, archivo
  - sshd\_config, 324
- palabra clave StrictHostKeyChecking, archivo
  - ssh\_config, 324
- palabra clave StrictModes, archivo sshd\_config, 324
- palabra clave Subsystem, archivo sshd\_config, 324
- palabra clave SyslogFacility, archivo
  - sshd\_config, 324
- palabra clave UseOpenSSLEngine
  - Secure Shell, 324
- palabra clave UsePrivilegedPort, Secure Shell, 324
- palabra clave User, archivo ssh\_config, 324
- palabra clave UserKnownHostsFile, archivo
  - ssh\_config, 324
- palabra clave UserKnownHostsFile2, *Ver* palabra clave UserKnownHostsFile
- palabra clave UseRsh, archivo ssh\_config, 324
- palabra clave VerifyReverseMapping, archivo
  - ssh\_config, 324
- palabra clave X11DisplayOffset, archivo
  - sshd\_config, 324
- palabra clave X11Forwarding, archivo
  - sshd\_config, 324
- palabra clave X11UseLocalHost, archivo
  - sshd\_config, 324
- palabra clave XAuthLocation, reenvío del puerto de Secure Shell, 324
- palabras clave
  - Ver también* palabra clave específica
  - atributo en BART, 98
  - Secure Shell, 320–326
  - valores de sustitución de línea de comandos en Secure Shell, 329
- PAM
  - agregar un módulo, 281–282
  - apilamiento
    - diagramas, 289
    - ejemplo, 291–292
    - explicado, 287
  - archivo /etc/rsyslog.conf, 283
  - archivo /etc/syslog.conf, 283
  - archivo de configuración
    - Kerberos y, 528
  - archivos de configuración
    - apilamiento, 287–290
    - indicadores de control, 288
    - introducción, 285
    - sintaxis, 286
  - descripción general, 277
  - estructura, 278
  - Kerberos y, 357
  - mapa de tareas, 279
  - pila para almacenar en caché la autenticación, 166
  - planificación, 280
- paneles, tabla de la herramienta SEAM, 499–502
- pares de claves
  - creación, 268–272
  - generación
    - uso del comando pktool, 268–272
- PASSREQ en Secure Shell, 325
- PATH en Secure Shell, 325
- perfil de derechos de configuración de auditoría, 644
  - auditoría de un rol, 174–175
  - configuración de política de auditoría, 585–587
  - preselección de clases de auditoría, 580–581
  - visualización de valores predeterminados de auditoría, 578–580

- perfil de derechos de control de auditoría, 644
  - activación de servicio de auditoría, 613–614
  - desactivación de servicio de auditoría, 613
  - refrescamiento de servicio de auditoría, 611–613
- perfil de derechos de copia de seguridad de medios
  - asignación a usuarios de confianza, 134, 171
- perfil de derechos de gestión de almacenamiento de ZFS, creación de agrupaciones para archivos de auditoría, 593–597
- perfil de derechos de gestión de dispositivos, 86–87
- perfil de derechos de gestión de IPsec de red, agregación de autorización `solaris.admin.edit`, 178
- perfil de derechos de gestión de sistemas de archivos ZFS, creación de sistemas de archivos de auditoría, 593–597
- perfil de derechos de gestión VSCAN, eliminación de autorizaciones, 179
- perfil de derechos de restauración de medios,
  - asignación a usuarios de confianza, 171
- perfil de derechos de revisión de auditoría, 644
- perfil de derechos de seguridad de dispositivos, 76–77, 86–87
- perfil de derechos de seguridad de usuarios,
  - modificación de preselección de auditoría para usuarios, 581–585
- perfiles, *Ver* perfiles de derechos
- perfiles de derechos
  - administrador del sistema, 206
  - agregación de autorización
    - `solaris.admin.edit`, 178
  - agregación de privilegios a comando, 177
  - asignación a usuarios de confianza, 134, 171
  - para servicio de auditoría, 644–645
  - autenticación con contraseña de usuario, 189–190, 192
  - bases de datos
    - Ver* base de datos `prof_attr` y base de datos `exec_attr`
  - cambio de contenido de, 175–177
  - clonación de contenido de, 177–179
  - contenido de perfiles típicos, 205
  - creación para usuarios Sun Ray, 176
  - descripciones de principales perfiles de derechos, 205
- perfiles de derechos (*Continuación*)
  - descripción, 135, 141
  - detención, 206, 208
  - eliminación de autorizaciones, 179
  - eliminación de privilegios de conjunto límite, 177
  - gestión de dispositivos, 86–87
  - gestión de impresoras, 206
  - gestión de IPsec de red, 178
  - gestión VSCAN, 179
  - modificación, 175–177, 177–179
  - operador, 206
  - orden de búsqueda, 207
  - prevención de escalada de privilegios, 134, 171
  - restricción de privilegios básicos, 176
  - seguridad de dispositivos, 76–77, 86–87
  - solución de problemas, 182–186
  - todos, 206
  - uso de perfil de administrador del sistema, 65
  - usuario de la consola, 206, 208
  - usuario de Solaris básico, 206
  - ver contenido, 207
- permisos
  - ACL de UFS y, 118
  - ACL y, 48–49
  - bit de permanencia, 115
  - búsqueda de archivos con permisos `setuid`, 126
  - cambio de permisos de archivo
    - comando `chmod`, 112
    - modo absoluto, 116, 124–125
    - modo simbólico, 116, 117, 123
  - clases de usuario y, 112
  - los permisos de archivo
    - modo absoluto, 116
  - permisos de archivo
    - cambio, 116–118, 123
    - descripción, 113
    - modo absoluto, 124–125
    - modo simbólico, 116, 117, 123
    - permisos especiales, 115, 117
  - permisos de archivo especiales, 113–115, 115, 117
  - permisos de directorio, 113
  - permisos `setgid`
    - descripción, 114–115
    - modo absoluto, 117, 126

- permisos, permisos setgid (*Continuación*)
  - modo simbólico, 117
- permisos setuid
  - descripción, 114
  - modo absoluto, 117, 126
  - modo simbólico, 117
  - riesgos de seguridad, 114
  - valor umask, 115–116
  - valores predeterminados, 115–116
- permisos de archivo UNIX, *Ver* archivos, permisos
- permisos de bit de permanencia
  - descripción, 115
  - modo absoluto, 117, 126
  - modo simbólico, 117
- permisos de ejecución, modo simbólico, 117
- permisos de escritura, modo simbólico, 117
- permisos de lectura, modo simbólico, 117
- permisos especiales
  - bit de permanencia, 115
  - permisos setgid, 114–115
  - permisos setuid, 114
- permisos setgid
  - descripción, 114–115
  - modo absoluto, 117, 126
  - modo simbólico, 117
  - riesgos de seguridad, 115
- permisos setuid
  - búsqueda de archivos con permisos establecidos, 126
  - descripción, 114
  - modo absoluto, 117, 126
  - modo simbólico, 117
  - riesgos de seguridad, 46, 114
- personalización, manifiestos, 99–100
- personalización de un informe (BART), 104–106
- pilas ejecutables
  - desactivación de registro de mensajes, 128
  - protección contra, 127–128
  - protección contra procesos de 32 bits, 118
  - registro de mensajes, 119
- pista de auditoría
  - agregación de espacio en disco, 597–599
  - costos de análisis, 574
- pista de auditoría (*Continuación*)
  - creación
    - archivos de resumen, 619
  - depuración de archivos no terminados, 622–623
  - descripción, 550
  - descripción general, 560
  - efecto de política de auditoría, 571
  - envío de archivos a repositorio remoto, 600–601, 601–605
  - prevención de desbordamiento, 623–624
  - reducción de tamaño de, 628–630, 637–638
  - selección de eventos de, 618–620
  - sin objetos públicos, 550
  - supervisión en tiempo real, 575
  - vista de eventos desde distintas zonas, 645
  - visualización de eventos desde, 620–622
- PKCS #11 tokens de software, gestión de almacén de claves, 261
- PKI
  - administración por KMF, 259
  - política administrada por KMF, 261
- placa Crypto Accelerator 1000 de Sun, lista de mecanismos, 255–256
- placa Sun Crypto Accelerator 6000
  - complemento de hardware para estructura criptográfica, 223
  - lista de mecanismos, 254
  - Secure Shell y FIPS-140, 297–298
- planificación
  - auditoría, 563–570
  - auditoría en zonas, 564–565
- Kerberos
  - decisiones de configuración, 361–370
  - dominios, 362–363
  - jerarquía de dominios, 363
  - KDC esclavos, 365
  - nombres de dominio, 362
  - nombres de principal de servicio y cliente, 364
  - número de dominios, 362–363
  - propagación de base de datos, 367
  - puertos, 365
  - sincronización de reloj, 367
- PAM, 280
- RBAC, 169–171

- política
  - definición en la estructura criptográfica, 224
  - definición en Oracle Solaris, 31–32
- política de auditoría
  - configuración de `arge`, 632
  - configuración de `argv`, 631
  - configuración en zona global, 561–562, 645
  - configuración `perzone`, 587
  - descripción, 549
  - efectos de, 571–573
  - establecimiento, 585–587
  - establecimiento de `ahlt`, 586
  - `public`, 573
  - que no afecta `tokens`, 648
  - `tokens` agregados por, 648
  - `tokens` de auditoría de, 648
  - valores predeterminados, 571–573
  - visualización de valores predeterminados, 578–580
- política de auditoría activa, política de auditoría temporal, 585–587
- política de auditoría `ahlt`
  - con política `cnt`, 649–650
  - descripción, 571
  - establecimiento, 586
- política de auditoría `arge`
  - configuración, 632
  - descripción, 571
  - y `token exec_env`, 656
- política de auditoría `argv`
  - configuración, 631
  - descripción, 572
  - y `token exec_args`, 656
- política de auditoría `cnt`
  - con política `ahlt`, 649–650
  - descripción, 572
- política de auditoría configurada, política de auditoría permanente, 585–587
- política de auditoría `group`
  - descripción, 572
  - `token group y`, 657
  - y `token groups`, 572
- política de auditoría `path`, descripción, 572
- política de auditoría permanente, política de auditoría configurada, 585–587
- política de auditoría `perzone`
  - configuración, 587
  - cuándo utilizar, 561–562
  - descripción, 572
  - uso, 565, 610–611, 645
- política de auditoría `public`
  - descripción, 573
  - eventos de sólo lectura, 573
- política de auditoría `seq`
  - descripción, 573
  - y `token sequence`, 573, 661
- política de auditoría temporal
  - configuración, 586–587
  - política de auditoría activa, 585–587
- política de auditoría `trail`
  - descripción, 573
  - y `token trailer`, 573
- política de auditoría `zonename`
  - descripción, 573
  - uso, 565, 645
- política de dispositivos
  - auditoría de cambios, 74
  - comando `add_drv`, 85
  - comando `update_drv`, 85
  - comandos, 85
  - configuración, 73–75
  - descripción general, 41–42
  - gestión de dispositivos, 73–74
  - mapa de tareas, 73–74
  - protección en núcleo, 84–92
  - visualización, 74
- política de seguridad, predeterminada (RBAC), 210
- política extendida, privilegios, 150
- políticas
  - administración, 471–510
  - contraseñas y, 516
  - creación (Kerberos), 482
  - creación de nuevas (Kerberos), 495–496
  - descripción general, 31–32
  - en dispositivos, 74
  - especificación de algoritmo de contraseña, 59–62
  - mapa de tareas para administrar, 490–491
  - modificación, 497–498
  - paneles de la herramienta SEAM para, 499–502

políticas (*Continuación*)

- para auditoría, 571–573
- supresión, 498–499
- visualización de atributos, 493–495
- visualización de la lista de, 491–493
- prefijos para clases de auditoría, 646–647
- preselección, clases de auditoría, 580–581
- preselección de auditoría, 550
- prevención, desbordamiento de pista de auditoría, 623–624
- prevención de desbordamiento, pista de auditoría, 623–624
- prevención de desbordamiento de almacenamiento, pista de auditoría, 623–624
- primario, en nombres de principales, 352–353
- principal
  - adición de principal de servicio a keytab, 504, 505–506
  - adición de principales de administración, 384
  - administración, 471–510
  - automatización de la creación de, 477–478
  - comparación de ID de usuario, 401
  - configuración de valores predeterminados, 487–488
  - creación, 482–484
  - creación de `clntconfig`, 379, 386
  - creación de host, 378, 385
  - duplicación, 485
  - eliminación de un principal de servicio de keytab, 506–507
  - eliminación del archivo keytab, 507
  - Kerberos, 352–353
  - mapa de tareas para administrar, 476–477
  - modificación, 485–486
  - nombre de principal, 352–353
  - paneles de la herramienta SEAM para, 499–502
  - principal de servicio, 353
  - principal de usuario, 353
  - supresión, 487
  - visualización de atributos, 480–482
  - visualización de la lista de, 478–480
  - visualización de sublista de principales, 479
- principal `clntconfig`
  - creación, 379, 386

- principal de servicio
  - adición a archivo keytab, 504, 505–506
  - descripción, 353
  - eliminación del archivo keytab, 506–507
  - planificación para nombres, 364
- principal de usuario, descripción, 353
- principal host
  - creación, 378, 385
- principal root, adición a keytab de host, 504
- principio de privilegio mínimo, 145
- privacidad
  - disponibilidad, 523
  - Kerberos y, 347
  - servicio de seguridad, 355
- privilegio de lista, herramienta SEAM y, 502
- privilegio mínimo, principio de, 145
- privilegio `PRIV_PROC_LOCK_MEMORY`, 147
- privilegios
  - administración, 194
  - agregación a comando en perfil de derechos, 177
  - archivos, 216–217
  - asignación a rol, 189
  - asignación a un comando, 150
  - asignación a un usuario, 150
  - asignación a usuario, 164
  - asignar a secuencia de comandos, 152
  - auditoría y, 217
  - búsqueda de faltantes, 201–202
  - categorías, 145
  - comandos, 215
  - depuración, 153
  - descripción, 135, 145, 146
  - determinación de privilegios asignados directamente, 196–197
  - diferencias con modelo de superusuario, 146
  - dispositivos y, 152
  - efectos en la herramienta SEAM, 503
  - ejecución de comandos con privilegios, 151
  - eliminación de conjunto básico, 176
  - eliminación de conjunto límite, 164
  - eliminación de conjunto límite en perfil de derechos, 177
  - eliminar de un usuario, 151

privilegios (*Continuación*)

- en comparación con modelo de superusuario, 144–153
- enumeración, 195–196
- enumeración en un proceso, 199–200
- escalada, 217
- heredados por procesos, 149
- implementados en conjuntos, 148
- limitación del uso en un perfil de derechos, 176
- mapa de tareas, 194
- modo de uso, 194–204
- política extendida, 150
- PRIV\_PROC\_LOCK\_MEMORY, 147
- procesos con privilegios asignados, 149
- programas para privilegios, 149
- proteger procesos del núcleo, 144
- resolución de problemas de requisitos
  - para, 201–202
- solución de problemas
  - a usuarios, 182–186
- uso en secuencia de comandos de shell, 203–204

privilegios de proceso, 145

privilegios FILE, 145

privilegios IPC, 145

privilegios NET, 145

privilegios PROC, 145

privilegios SYS, 145

procedimientos de usuario

- agregación de complementos a KMF, 273–274
- asignación de dispositivos, 75–81
- asunción de un rol, 161–162
- cifrado de archivos, 229–230
- cifrado de clave privada del usuario NIS, 342
- comando chkey, 343
- creación de un certificado autofirmado, 263–264
- cálculo de MAC de un archivo, 236–238
- cálculo de resumen de un archivo, 234–235
- descifrado de archivos, 238–241
- exportación de certificados, 266–267
- generación de frases de contraseña para almacén de clave, 267–268
- generación de una clave simétrica
  - uso del comando `pktool`, 230–234
- importación de certificados, 264–265

procedimientos de usuario (*Continuación*)

- protección de archivos, 119–120
- uso de Secure Shell, 304–305
- uso de un rol asignado, 161–162
- uso del comando `pktool`, 262–263

proceso de shell, enumeración de privilegios, 199–200

programas

- comprobación de autorizaciones RBAC, 182
- para privilegios, 148, 149

propagación

- base de datos de Kerberos, 430–431
- base de datos del KDC, 367

propiedad de archivos

- ACL de UFS y, 118
- ACL y, 48–49
- cambio, 112, 121–122
- cambio de propiedad de grupo, 122

propiedades del sistema, privilegios relacionados con, 145

protección

- archivos con estructura criptográfica, 229–230
- archivos ejecutables de 32 bits que ponen en riesgo la seguridad, 118–119
- BIOS, puntero hacia, 65–66
- contenidos de almacén de claves, 266
- directorío de transferencia `sftp`, 303–304
- mapa de tareas de contraseñas, 55–56
- mapa de tareas de inicios de sesión, 55–56
- mediante contraseñas con estructura criptográfica, 262–263
- PROM, 65–66
- protección de sistema contra programas riesgosos, 126
- red durante la instalación, 46
- secuencias de comandos, 182

protección de archivos

- con ACL de UFS, 118
- con permisos UNIX, 111–118, 119–120
- mapa de tareas con permisos UNIX, 119
- procedimientos de usuario, 119–120

protección segura, inicio de sesión, 307–308

protocolo de hora de red, *Ver* NTP

protocolo v1, Secure Shell, 294

protocolo v2, Secure Shell, 294



- proveedor de nivel de usuario `pkcs11_kernel.so`, 242
- proveedor de nivel de usuario
  - `pkcs11_softtoken.so`, 242
- proveedor de núcleo AES, 242
- proveedor de núcleo ARCFOUR, 242
- proveedor de núcleo ECC, 242
- proveedor de núcleo RSA, 242
- proveedor de núcleo SHA1, 242
- proveedor de núcleo SHA2, 242
- proveedores
  - agregación de biblioteca, 247
  - agregación de proveedor de software, 246–247
  - agregación de un proveedor de software de nivel de usuario, 247
  - conexión a la estructura criptográfica, 227
  - definición como complementos, 223
  - definición como componentes, 223
  - definición en la estructura criptográfica, 224
  - desactivación de mecanismos de
    - hardware, 255–256
  - firma, 227
  - impedir el uso de un proveedor de software de núcleo, 251–254
  - lista de la estructura criptográfica, 242–246
  - lista de proveedores de hardware, 254
  - registro, 227
  - restauración del uso de un proveedor de software de núcleo, 252
- proveedores de hardware
  - activación de mecanismos y funciones en, 256
  - carga, 254
  - desactivación de mecanismos
    - criptográficos, 255–256
  - lista, 254
- proveedores de núcleo, listing, 242
- pseudo-tty, uso en Secure Shell, 319
- puertas de enlace, *Ver* sistemas de cortafuegos
- puertos, para el KDC de Kerberos, 365
- puertos con privilegios, alternativa a RPC seguras, 52
- punto (.)
  - separador de nombre de autorización, 209
  - visualización de archivos ocultos, 120
- punto y coma (;), archivo `device_allocate`, 89

- páginas del comando `man`
  - asignación de dispositivo, 87
  - comandos que requieren autorizaciones, 214–215
  - política, 31–32
  - RBAC, 213–214
  - Secure Shell, 329–330
  - servicio de auditoría, 643–644

## R

- opción -R
  - `bart create`, 97, 100
  - comando `ssh`, 312–313
- ranura, definición en la estructura criptográfica, 225
- RBAC
  - agregación de roles, 171–173
  - agregación de usuarios con privilegios, 163–164
  - auditoría de roles, 174–175
  - autorizaciones, 138–139
  - base de datos de autorización, 211
  - base de datos de perfil de derechos, 211
  - bases de datos, 209–212
  - cambio de contraseñas de rol, 187–188
  - comandos de administración, 213–214
  - comandos para gestionar, 213–214
  - comprobación de autorizaciones en secuencias de comandos o programas, 182
  - conceptos básicos, 135–137
  - configuración, 168–186
  - creación de autorizaciones, 180–181
  - creación de perfiles de derechos, 175–177
  - elementos, 135–137
  - en comparación con modelo de superusuario, 131–135
  - modificación de roles, 188–189
  - modificación de usuarios, 162–164
  - obtención de derechos administrativos, 164–167
  - perfiles de auditoría, 644
  - perfiles de derechos, 141
  - planificación, 169–171
  - protección de secuencias de comandos, 182
  - restricción de derechos, 190–191
  - servicios de nombres y, 210
  - shells de perfil, 142



RBAC (*Continuación*)

- solución de problemas, 182–186
- uso de contraseña de usuario para asumir rol, 189–190, 191–192
- valores predeterminados, 156–167
- visualización de sus derechos, 158–160
- visualización de todos los atributos de seguridad de RBAC, 157–158

RC4, *Ver* proveedor de núcleo ARCFOUR

red, privilegios relacionados con, 145

## reducción

- archivos de auditoría, 616–618
- espacio en disco necesario para archivos de auditoría, 637–638
- requisitos de espacio de almacenamiento para archivos de auditoría, 575

## reemplazo

- clases de auditoría preseleccionadas, 580–581
- superusuario con roles, 169–171

reenvío de datos, Secure Shell, 319

## reenvío de X11

- configuración en archivo `ssh_config`, 322
- en Secure Shell, 319

## reenvío del puerto

- configuración en Secure Shell, 301
- Secure Shell, 312, 313

## refrescamiento

- servicio de auditoría, 611–613

refrescar, servicios criptográficos, 256–257

registro, transferencias de archivos de ftp, 639–640

registro de proveedores, estructura criptográfica, 227

## registros de auditoría

- Ver también* archivos de auditoría
- archivo `/var/adm/auditlog`, 606
- comparación de resúmenes binarios y de texto, 555
- configuración, 592–607
- configuración de registros de auditoría de resumen de texto, 605–607
- conversión a formato legible, 621
- copia a un único archivo, 620
- descripción, 549
- descripción general, 553
- ejemplo de formato, 615
- eventos que generan, 559

registros de auditoría (*Continuación*)

- formato, 651
- fusión, 616–618
- modificadores de eventos, 657
- modos, 555
- reducción de archivos de auditoría, 616–618
- secuencia de tokens, 651
- visualización, 620–622
- visualización de definiciones de procedimiento, 615–616
- visualización de formatos de un programa, 615–616
- visualización de formatos de una clase de auditoría, 616
- visualización en formato XML, 621

## reinicio

- daemon `sshd`, 301
- servicio `ssh`, 301
- servicios criptográficos, 256–257

repositorio, instalación de proveedores de terceros, 246

requisitos de espacio en disco, archivos de auditoría, 574–575

requisitos de reutilización de objetos

- para dispositivos, 91–92
- secuencias de comandos `device-clean`
- redacción de secuencias de comandos nuevas, 92

## resolución de problemas

- acceso `rootremoto`, 64
- asignación de un dispositivo, 82
- auditoría, 625–626
- búsqueda de archivos con permisos `setuid`, 126
- clases de auditoría
  - personalizadas, 627
  - personalizado, 591
- comando `encrypt`, 240
- comando `list_devices`, 78
- comando `praudit`, 622
- complemento activo, 627
- demasiados registros de auditoría en cola, 601
- evitar que programas utilicen pilas ejecutables, 127–128
- falta de privilegio, 201–202
- Kerberos, 466
- montaje de un dispositivo, 83

resolución de problemas (*Continuación*)

- requisitos de privilegios, 201–202
- root como un rol, 194
- terminal donde el comando su se originó, 63
- usuario que ejecuta comandos con privilegios, 198–199

## restauración, proveedores criptográficos, 252

## restricciones de acceso de inicio de sesión,

- svc:/system/name-service/switch:default, 36

## restricción

- acceso root, 62–65
- acceso root remoto, 63–65
- privilegios de usuario en un perfil de derechos asignado, 176

## restricción de acceso para servidores KDC, 449

## resúmenes

- cálculo para archivo, 234–235
- de archivos, 234–235, 235

## RETRIES en Secure Shell, 325

## rol root

- asunción de rol, 161–162
- cambio a usuario root, 192–194
- cambio de contraseña, 56
- cambio de usuario root, 194
- resolución de problemas, 194
- rol proporcionado, 133

## roles

- asignación con comando usermod, 173–174
- asignación de privilegios a, 189
- asumir en una ventana de terminal, 142
- asumir tras inicio de sesión, 142
- asunción, 161–162
- asunción del rol root, 161–162
- asunción en una ventana de terminal, 161–162
- auditoría, 174–175
- autenticación con contraseña de usuario, 189–190, 191–192
- cambio de contraseña de, 187–188
- cambio de propiedades de, 188–189
- cambio del rol root a usuario, 192–194
- creación, 171–173
  - rol de gestión de criptografía, 174
- descripción, 141–142

roles (*Continuación*)

- determinación de comandos con privilegios de rol, 198–199
- determinación de privilegios asignados directamente, 197
- enumeración de roles locales, 161
- enumerar roles locales, 213
- modificación, 188–189
- resumen, 136
- roles recomendados, 132
- uso de contraseña de usuario, 192
- uso de contraseñas de usuarios, 137
- uso de un rol asignado, 161–162
- uso en RBAC, 132
- uso para acceder al hardware, 65–66

## RPC segura

- alternativa, 52
- descripción, 335
- descripción general, 51–52
- implementación de, 337–340
- servidor de claves, 337
- y Kerberos, 336

**S**

## opción -S, secuencia de comandos st\_clean, 92

## SASL

- complementos, 332
- descripción general, 331
- opciones, 333
- variable de entorno, 332

## sección admin\_server

- archivo krb5.conf, 377, 383

## sección default\_realm

- archivo krb5.conf, 377, 383

## sección domain\_realm

- archivo krb5.conf, 363, 377, 383

## secuencia de comandos, secuencia de comandos

- audit\_warn, 643

## secuencia de comandos audit\_warn

- configuración, 589
- descripción, 643

## secuencia de comandos fd\_clean, descripción, 92

## secuencia de comandos sr\_clean, descripción, 92

- secuencia de comandos `st_clean`, 91
- secuencias de comandos
  - comprobación de autorizaciones RBAC, 182
  - ejecutar con privilegios, 152
  - ejemplo de supervisión de archivos de auditoría, 576
  - para limpieza de dispositivos, 91–92
  - procesamiento de salida de `praudit`, 621–622
  - protección, 182
  - secuencia de comandos `audit_warn`, 589
  - secuencias de comandos `device-clean`
    - Ver también* secuencias de comandos `device-clean`
  - uso de privilegios en, 203–204
- secuencias de comandos de shell, escritura con privilegios, 203
- secuencias de comandos `device-clean`
  - descripción, 91–92
  - medios, 90, 91–92
  - opciones, 92
  - redacción de secuencias de comandos nuevas, 92
  - reutilización de objetos, 91–92
- Secure Shell
  - administración, 317–319
  - administración de ZFS, 310–311
  - archivos, 326
  - autenticación
    - requisitos para, 294–295
  - autenticación de clave pública, 294
  - base de OpenSSH, 296–297
  - cambio de frase de contraseña, 307
  - cambios en la versión actual, 296–297
  - comando `scp`, 313–314
  - compatibilidad con FIPS-140, 297–298
  - conexión fuera de cortafuegos
    - de archivo de configuración, 314–315
    - desde la línea de comandos, 315
  - conexión por medio de un cortafuegos, 314
  - configuración de clientes, 320
  - configuración de reenvío del puerto, 301
  - configuración de servidor, 320
  - configuración del directorio `chroot`, 303–304
  - copia de archivos, 313–314
  - creación de claves, 305–307
  - Secure Shell (*Continuación*)
    - denominación de archivos de identidad, 326
    - descripción, 293
    - ejecución de comandos, 319
    - especificación de excepciones para valores predeterminados del sistema, 302–303
    - generación de claves, 305–307
    - inicio de sesión en host remoto, 307–308
    - inicio de sesión para mostrar una GUI remota, 308
    - mapa de tareas de administrador, 298
    - menos indicadores de inicio de sesión, 309–310
    - métodos de autenticación, 294–295
    - palabras clave, 320–326
    - paquete `xauth`, 308
    - pasos de autenticación, 318–319
    - procedimientos de usuario, 304–305
    - reenvío de correo, 312
    - reenvío de datos, 319
    - reenvío del puerto local, 312, 313
    - reenvío del puerto remoto, 313
    - sesión típica, 317–319
    - TCP y, 301
    - uso de reenvío del puerto, 312–313
    - uso sin contraseña, 309–310
    - variables de entorno de inicio de sesión y, 325–326
    - versiones del protocolo, 294
  - seguridad
    - archivos de cifrado, 238–241
    - asignación de dispositivo, 73–92
    - auditoría, 547–562
    - auditoría y, 558–559
    - autenticación DH, 337–340
    - BART, 93–109
    - cifrado de contraseña, 38
    - cliente-servidor NFS, 337–340
    - cálculo de MAC de archivos, 236–238
    - cálculo de resumen de archivos, 234–235
    - descripción general de políticas, 31–32
    - dispositivos, 41–42
    - estructura criptográfica, 221–228
    - estructura de gestión de claves, 259–274
    - hardware del sistema, 65–66
    - impedir el inicio de sesión remoto, 63–65
    - opciones de instalación, 46

seguridad (*Continuación*)

- opción de instalación netservices limited, 46
- por medio de red no segura, 314
- protección contra caballos de Troya, 44
- protección contra denegación del servicio, 46
- protección de dispositivos, 91–92
- protección de hardware, 65–66
- protección de PROM, 65–66
- Secure Shell, 293–315
- seguridad predeterminada, 46
- sistemas, 35–54

## seguridad de red

- autenticación, 51–52
- autorizaciones, 51–52
- comunicación de problemas, 54
- control de acceso, 50–54
- descripción general, 50
- sistemas de cortafuegos
  - hosts de confianza, 53
  - interceptación de paquetes, 53–54
  - necesidad de, 53

## seguridad de sistema

- acceso, 35–54
- descripción general, 35–54

## seguridad del equipo

*Ver* seguridad del sistema

## seguridad del sistema

- acceso al equipo, 35–36
- ACL de UFS, 118
- cambio
  - contraseña root, 56
- cifrado de contraseña, 38
- contraseñas, 37
- control de acceso basado en roles (RBAC), 44
- control de accesos basado en roles (RBAC), 131–135
- cuentas especiales, 40
- descripción general, 35
- mapa de tareas, 126
- privilegios, 144–153
- protección contra programas riesgosos, 126
- protección de hardware, 35–36, 65–66
- restricciones de acceso de inicio de sesión, 36
- restricciones de acceso root, 49, 63–65

seguridad del sistema (*Continuación*)

- restricción de acceso root remoto, 63–65
- shell restringido, 45
- sistemas de cortafuegos, 53
- supervisión de comando su, 62–63
- supervisión del comando su, 43–44
- visualización
  - estado de inicio de sesión de usuario, 57–58
  - usuarios sin contraseñas, 58
- seguridad física, descripción, 35–36
- selección
  - clases de auditoría, 580–581
  - eventos de pista de auditoría, 618–620
  - registros de auditoría, 618–620
- selección posterior en auditoría, 550
- servicio
  - definición en Kerberos, 531
  - desactivación en un host, 508–510
  - obtención de acceso a un servicio específico, 540
- servicio de auditoría
  - Ver también* auditoría
  - activación, 613–614
  - configuración de controles de colas, 587–588
  - configuración de política, 585–587
  - creación de pista de auditoría, 651
  - desactivación, 613
  - política, 571
  - refrescamiento de núcleo, 611
  - resolución de problemas, 626–628
  - valores predeterminados, 641–642
- servicio de nombres LDAP
  - contraseñas, 37
  - especificación de algoritmo de contraseña, 61–62
- servicio de nombres NIS
  - autenticación, 335
  - contraseñas, 37
  - especificación de algoritmo de contraseña, 61
- servicio de otorgamiento de tickets, *Ver* TGS
- servicio de seguridad, Kerberos y, 355
- servicios criptográficos, *Ver* estructura criptográfica
- servicios de nombres
  - Ver* servicios de nombres individuales
  - ámbito y RBAC, 142
- servidor de aplicaciones, configuración, 395–398

- servidor de auditoría remota (ARS), gestión, 558
- servidor de claves
  - descripción, 337
  - inicio, 340–341
- servidores
  - configuración para Secure Shell, 320
  - definición en Kerberos, 531
  - dominios y, 354
  - obtención de acceso con Kerberos, 537–540
  - obtención de credencial para, 539
  - sesión cliente-servidor AUTH\_DH, 337–340
- servidores NFS, configuración para Kerberos, 399–401
- sesgo de reloj, planificación de Kerberos y, 367
- shell, versiones con privilegios, 142
- shell Bourne, versión con privilegios, 142
- shell Korn, versión con privilegios, 142
- shell restringido (rsh), 45
- shells de perfil, descripción, 142
- shells de perfiles
  - apertura, 164–167
  - restricción de derechos, 190–191
- signo de almohadilla (#)
  - archivo device\_allocate, 90
  - archivo device\_maps, 89
- signo de dólar doble (\$\$), número de proceso de shell principal, 199
- signo de intercalación (^)
  - en prefijos de clase de auditoría, 581–585, 633
  - uso de prefijo en valor audit\_flags, 583
- signo igual (=), símbolo de permisos de archivo, 117
- signo menos (-)
  - entrada en el archivo su\_log, 63
  - prefijo de clase de auditoría, 646–647
  - símbolo de permisos de archivo, 117
  - símbolo de tipo de archivo, 112
- signo más (+)
  - entrada en el archivo su\_log, 63
  - prefijo de clase de auditoría, 646–647
  - símbolo de permisos de archivo, 117
- signo-más (+), en prefijos de clase auditoría, 605
- sincronización de reloj
  - KDC maestro con Kerberos y, 386
  - planificación de Kerberos y, 367
- sincronización de relojes
  - descripción general, 424–425
  - esclavo KDC, 440
  - KDC esclavo, 392
  - KDC esclavo con Kerberos y, 392
  - KDC maestro, 379, 386
  - KDC maestro con Kerberos y, 379
  - servidor esclavo Kerberos y, 440
- sintaxis de comillas en BART, 108
- sistema de archivo de auditoría, descripción, 548
- sistema de archivos TMPFS, seguridad, 115
- sistema de inicio de sesión único, 520–526
  - Kerberos y, 347
- sistema de ventanas X, y herramienta SEAM, 473–474
- sistemas
  - protección contra programas riesgosos, 126
  - seguimiento de integridad de archivos, 93–109
- sistemas de archivos
  - activación de análisis de virus, 70
  - agregación de un motor de análisis de virus, 70
  - análisis de virus, 69–70
  - exclusión de archivos del análisis de virus, 72
  - NFS, 335
  - seguridad
    - autenticación y NFS, 335
    - sistema de archivos TMPFS, 115
    - TMPFS, 115
    - uso compartido de archivos, 49
- sistemas de archivos NFS
  - acceso seguro con AUTH\_DH, 343
  - autenticación, 335
  - proporcionar seguridad cliente-servidor, 337–340
- sistemas de archivos ZFS, creación para archivos de auditoría binarios, 593–597
- sistemas de cortafuegos
  - conexiones seguras de host, 314
  - conexión desde fuera, 315
  - fuera de conexiones con Secure Shell
    - de archivo de configuración, 314–315
    - desde la línea de comandos, 315
  - hosts de confianza, 53
  - interceptación de paquetes, 53–54
  - seguridad, 53
  - transferencias de paquetes, 53–54

- SMF
    - activación de servidor de claves, 341
    - administración de la configuración de seguridad
      - predeterminada, 46
    - reinicio de la estructura criptográfica, 256–257
    - reinicio de Secure Shell, 301
    - servicio auditd, 641–642
    - servicio de asignación de dispositivos, 86
    - servicio de estructura criptográfica, 226
    - servicio kcfld, 226
    - servicio ssh, 301
  - solicitudes de firma de certificados (CSR), *Ver* certificados
  - solución de problemas, propiedades de seguridad, 182–186
  - SPARC T4 series, optimizaciones criptográficas, 228
  - archivo .ssh/config
    - descripción, 328
    - valor de sustitución, 328
  - archivo .ssh/environment, descripción, 327
  - archivo .ssh/id\_dsa, 328
  - archivo .ssh/id\_rsa, 328
  - archivo .ssh/identity, 328
  - archivo .ssh/known\_hosts
    - descripción, 327
    - valor de sustitución, 328
  - archivo .ssh/rc, descripción, 327
  - subcomando export, comando pktool, 266–267
  - subcomando gencert, comando pktool, 263–264
  - subcomando import, comando pktool, 264–265
  - subcomando install, comando cryptoadm, 247
  - subcomando list, comando pktool, 263
  - subcomando list plugin, comando kmcfg, 273–274
  - subcomando setpin, comando pktool, 267–268
  - SUPATH en Secure Shell, 326
  - superusuario
    - Ver también* rol root
    - diferencias con modelo de privilegios, 146
    - eliminar en RBAC, 142
    - en comparación con modelo de privilegios, 144–153
    - en comparación con modelo RBAC, 131–135
    - resolución de problemas al convertirse en root como un rol, 194
  - supervisión
    - acceso root, 62–65
    - intentos de acceso root, 63–65
    - intentos de comando su, 62–63
    - intentos del comando su, 43–44
    - pista de auditoría en tiempo real, 575
    - uso de comandos con privilegios, 174–175
    - uso del sistema, 47
  - supresión
    - archivos de auditoría, 616
    - archivos de auditoría almacenados, 624
    - archivos de auditoría not\_terminated, 622–623
    - políticas (Kerberos), 498–499
    - principal (Kerberos), 487
    - servicio de host, 509
  - svc:/system/device/allocate, servicio de asignación de dispositivos, 86
  - SYSLOG\_FAILED\_LOGINS, en Secure Shell, 325
  - System V IPC
    - privilegios, 145
    - token de auditoría ipc, 658–659
    - token de auditoría IPC\_perm, 659
- T**
- T4, *Ver* SPARC T4 series
  - tabla cred
    - autenticación DH y, 337
    - información almacenada por el servidor, 339
  - tabla de credenciales, agregación de una sola entrada a, 401–402
  - tabla gsscred, uso, 543
  - tablas, gsscred, 543
  - tamaño de archivos de auditoría
    - reducción, 616–618
    - reducción de requisitos de espacio de almacenamiento, 575
  - TCP
    - direcciones, 658
    - Secure Shell y, 301, 319
  - tecnologías de clave pública, *Ver* PKI
  - terminología
    - específica de Kerberos, 531
    - específica de la autenticación, 531–532

terminología (*Continuación*)

Kerberos, 531–536

TGS, obtención de credencial para, 537–538

TGT, en Kerberos, 349–351

ticket de otorgamiento de tickets, *Ver* TGT

ticket inicial, definición, 533

ticket no válido, definición, 533

ticket posfechado

definición, 533

descripción, 349

ticket proxy, definición, 533

ticket que admite proxy, definición, 533

ticket renovable, definición, 534

tickets

advertencia sobre caducidad, 416

archivo

*Ver* antememoria de credenciales

comando klist, 513–514

creación, 511–512

creación con kinit, 512–513

definición, 348

definición en Kerberos, 532

destrucción, 514–515

duración, 534–535

duración máxima renovable, 535

inicial, 533

no válido, 533

o credenciales, 349

obtención, 511–512

opción -F o -f, 522

opción -k, 522

posfechados, 349, 533

proxy, 533

que admite proxy, 533

reenviables, 349, 512, 523–524, 533

renovables, 534

solicitud de dominio específico, 522

tipos de, 532–536

visualización, 513–514

tickets reenviables

con la opción -F, 522, 523–524

con la opción -f, 521, 523–524

definición, 533

descripción, 349

tickets reenviables (*Continuación*)

ejemplo, 512

TIMEOUT en Secure Shell, 325

tipos de tickets, 532–536

todos (RBAC), perfil de derechos, 206

token, definición en la estructura criptográfica, 225

token de auditoría acl, formato, 654–655

token de auditoría argument, formato, 655

token de auditoría attribute, 655

token de auditoría cmd, 655

token de auditoría exec\_args

formato, 656

política argv y, 656

token de auditoría exec\_envn, formato, 656

token de auditoría file, formato, 656

token de auditoría fmri, formato, 657

token de auditoría group

formato, 657

política de auditoría y, 657

token de auditoría header

modificadores de eventos, 657

orden en registro de auditoría, 657–658

token de auditoría ip address, formato, 658

token de auditoría ip port, formato, 658

token de auditoría ipc, 658–659

formato, 658–659

token de auditoría IPC\_perm, formato, 659

token de auditoría path, formato, 659

token de auditoría path\_attr, 659–660

token de auditoría privilege, 660

token de auditoría process, formato, 660

token de auditoría return, formato, 660

token de auditoría sequence

formato, 661

y política de auditoría seqy, 661

token de auditoría socket, 661

token de auditoría subject, formato, 661–662

token de auditoría text, formato, 662

token de auditoría trailer

formato, 662

orden en registro de auditoría, 662

visualización praudit, 662

token de auditoría use of authorization, 662

token de auditoría use of privilege, 662



- token de auditoría user, 663
- token de auditoría vnode, formato, 655
- token de auditoría vnode de archivo, 655
- token de auditoría xclient, 663
- token de auditoría zonename, 663
- token de auditoríaheader, formato, 657–658
- tokens de auditoría
  - Ver también nombres de token de auditoría individuales
  - agregados por política de auditoría, 648
  - descripción, 549, 554
  - formato, 653
  - formato de registros de auditoría, 651
  - listas de, 653
  - token xclient, 663
- tokens de auditoría relacionados con Internet
  - token ip address, 658
  - token ip port, 658
  - token socket, 661
- transacciones reproducidas, 339
- transferencia de paquetes, seguridad de cortafuegos, 53
- transferencias de archivos, auditoría, 639–640
- transferencias de paquetes, interceptación de paquetes, 53–54
- transparencia, definición en Kerberos, 348
- TZ en Secure Shell, 325

## U

- opción -U, comando allocate, 88
- UDP
  - direcciones, 658
  - reenvío del puerto y, 301
  - Secure Shell y, 301
  - uso para registros de auditoría remotos, 555
- unidades de CD-ROM
  - asignación, 83
  - seguridad, 92
- URL para ayuda en pantalla, herramienta gráfica de Kerberos, 370
- uso
  - asignación de dispositivos, 81–82
  - BART, 96
  - comando allocate, 81–82

- uso (*Continuación*)
  - comando cryptoadm, 241
  - comando deallocate, 84
  - comando digest, 234–235
  - comando encrypt, 238–241
  - comando mac, 236–238
  - comando pktool, 230–234, 268–272
  - comando ppriv, 199
  - comando rolemod, 189
  - comando ssh-add, 309–310
  - comando truss, 201
  - comando umount, 84
  - comando usermod, 164
  - daemon ssh-agent, 309–310
  - mapa de tareas de configuración predeterminada de RBAC, 156–157
  - mapa de tareas de privilegios, 194
  - mapa de tareas de RBAC, 155–156
  - mapa de tareas de Secure Shell, 304–305
  - nuevo algoritmo de contraseña, 60
  - valores predeterminados de RBAC, 156–167
- uso compartido de archivos
  - con autenticación DH, 343–344
  - y seguridad de red, 49
- uso de la estructura de gestión de claves (mapa de tareas), 262–263
- usuario de la consola (RBAC), perfil de derechos, 206
- usuario de Solaris básico (RBAC), perfil de derechos, 206
- usuario nobody, 49
- usuario root
  - cambio a rol root, 194
  - mostrar intentos de acceso en la consola, 63–65
  - reemplazar en RBAC, 142
  - restricción de acceso, 49
  - restricción de acceso remoto, 63–65
  - seguimiento de inicios de sesión, 43–44
  - supervisión de intentos de comando su, 62–63
  - supervisión de intentos del comando su, 43–44
- usuarios
  - asignación de autorización para, 77
  - asignación de dispositivos, 81–82
  - asignación de perfiles de derechos, 163–164
  - asignación de privilegios a, 164



usuarios (*Continuación*)

- asignar valores predeterminados de RBAC, 212
- auditoría de todos sus comandos, 630–632
- auditoría de usuarios individuales, 583–584
- autenticación para perfil de derechos, 189–190, 192
- autenticación para rol, 189–190, 191–192
- cifrado de archivos, 238–241
- conjunto básico de privilegios, 149
- creación de perfil de derechos para un grupo, 584–585
- creación de usuario root, 192–194
- cálculo de MAC de archivos, 236–238
- cálculo de resumen de archivos, 234–235
- desactivación de inicio de sesión, 58–59
- desasignación de dispositivos, 84
- desmontaje de dispositivos asignados, 84
- determinación de comandos con privilegios propios, 198–199
- determinación de privilegios asignados directamente, 196–197
- eliminación de indicadores de auditoría, 584
- excepciones para valores predeterminados de Secure Shell, 302–303
- generación de una clave simétrica, 230–234
- modificación de máscara de preselección de auditoría de, 581–585
- modificación de propiedades (RBAC), 162–164
- montaje de dispositivos asignados, 82–83
- privilegios heredables iniciales, 149
- resolución de problemas de ejecución de comandos con privilegios, 198–199
- sin contraseñas, 58
- uso de perfil de derechos, 189–190, 192
- visualización de estado de inicio de sesión, 57–58
- utilidad de gestión de servicios, refrescar la estructura criptográfica, 247
- Utilidad de gestión de servicios (SMF), *Ver* SMF

**V**

- valor `max_life`, descripción, 534
- valor `max_renewable_life`, descripción, 535
- valor `umask`
  - valores típicos, 115

valor `umask` (*Continuación*)

- y creación de archivos, 115–116
- valores de campo de tipo `ipc` (token `ipc`), 658–659
- valores predeterminados
  - configuración de privilegios en archivo `policy.conf`, 216
  - de todo el sistema en el archivo `policy.conf`, 38
  - servicio de auditoría, 641–642
  - valor `umask`, 115–116
- variable de sistema `KEYBOARD_ABORT`, 66
- variable del entorno `PATH`
  - configuración, 45
  - y seguridad, 44
- variable del sistema `CRYPT_DEFAULT`, 60
- variable del sistema `rstchown`, 122
- variable `noexec_user_stack`, 119, 127–128
- variable `noexec_user_stack_log`, 119, 128
- variables
  - agregación a registro de auditoría, 571
  - agregar a registro de auditoría, 656
  - auditoría de las asociadas con un comando, 655
  - configuración en Secure Shell, 325
  - `KEYBOARD_ABORT`, 66
  - login y Secure Shell, 325–326
  - `noexec_user_stack`, 119
  - `noexec_user_stack_log`, 119
  - para puertos y servidores proxy, 315
  - `rstchown`, 122
- variables de entorno
  - presencia en registros de auditoría, 571, 653
  - Secure Shell y, 325–326
  - sustitución de puertos y servidores proxy, 315
  - uso con comando `ssh-agent`, 329
- variables de entorno login, Secure Shell y, 325–326
- variables de sistema
  - `CRYPT_DEFAULT`, 60
  - `KEYBOARD_ABORT`, 66
  - `noexec_user_stack`, 127–128
  - `noexec_user_stack_log`, 128
  - `rstchown`, 122
- variables del entorno
  - Ver también* variables
  - `PATH`, 44
  - token de auditoría para, 656

## variables del sistema

*Ver también* variables

ver, contenido de perfiles de derechos, 207

verificador de ventana, 338

## verificadores

descripción, 338

devuelto al cliente NFS, 339

ventana, 338

## virus

ataque de denegación de servicio, 46

caballo de Troya, 44

vista, usuarios sin contraseñas, 58

## visualización

archivos de auditoría binarios, 620–622

archivos e información relacionada, 112

atributos de política, 493–495

atributos de principal, 480–482

controles de colas de auditoría, 578–580, 587

definiciones de privilegios, 195–196

definiciones de registros de auditoría, 615–616

definición de registros de auditoría, 615–616

derechos de usuario inicial, 158–160

dispositivos asignables, 78

enumeración detallada de mecanismos

criptográficos, 245

estado de inicio de sesión de usuario, 57–58

excepciones a auditoría en todo el sistema, 578–580

información de archivos, 120–121

información de asignación de dispositivos, 78

lista de políticas, 491–493

lista de principales, 478–480

MAC de un archivo, 237

mapa de tareas de privilegios, 194

mecanismos criptográficos

disponibles, 244, 251

existentes, 243, 244, 251

finalidad, 245

mecanismos criptográficos disponibles, 244, 251

mecanismos criptográficos existentes, 244, 251

memoria intermedia de lista de claves con el

comando `list`, 508, 509

permisos de archivo, 120–121

política de dispositivos, 74

políticas de auditoría, 585

visualización (*Continuación*)

privilegios, 194–204

privilegios asignados directamente, 197

privilegios en un proceso, 199

privilegios en un shell, 197, 199–200

proveedores de la estructura criptográfica, 242–246

registro de auditoría en formato XML, 621

registros de auditoría, 620–622

registros de auditoría seleccionados, 616–618

registros de auditoría XML, 621

resumen de un archivo, 235

roles que puede asumir, 161

sublista de principales (Kerberos), 479

sus derechos RBAC, 158–160

tickets, 513–514

usuarios sin contraseñas, 58

valores predeterminados de auditoría, 578–580

valores predeterminados de política de auditoría, 578–580

**X**

opción -X

comandos Kerberizados, 522

**Z**

## zonas

auditoría y, 561–562, 645

configuración de auditoría en zona global, 586

dispositivos y, 41

estructura criptográfica y, 227

planificación de auditoría en, 564–565

política de auditoría perzone, 561–562, 565, 645

política de auditoría zonename, 565, 645

servicios criptográficos y, 256–257

**ám**

ámbito (RBAC), descripción, 142