Gestión de Kerberos y otros servicios de autenticación en Oracle® Solaris 11.2

Referencia: E53968-02
Septiembre de 2014

ORACLE

Contenido

Lista de tablas

Lista de ejemplos

Uso de esta documentación

- **Descripción general**: describe cómo administrar la autenticación segura en uno o más sistemas Oracle Solaris. Esta guía abarca Módulos de autenticación conectable (PAM), Kerberos, la autenticación sencilla y capa de seguridad (SASL) y RPC segura para NIS y NFS. Un apéndice describe sondeos de DTrace para Kerberos con ejemplos de su uso.
- **Destinatarios**: administradores de la seguridad, el sistema y la red.
- **Conocimientos necesarios**: requisitos de acceso y de seguridad de red.

Biblioteca de documentación del producto

En la biblioteca de documentación, que se encuentra en http://www.oracle.com/pls/topic/lookup?ctx=E56339, se incluye información de última hora y problemas conocidos para este producto.

Acceso a My 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.

Comentarios

Envíenos comentarios acerca de esta documentación mediante http://www.oracle.com/goto/docfeedback.

♦ ♦ ♦ CAPÍTULO 1

Uso de módulos de autenticación conectables

En este capítulo, se trata el módulo de autenticación conectable (PAM). El PAM proporciona una estructura para conectar comprobaciones para usuarios de aplicaciones en Sistema operativo Oracle Solaris. El PAM proporciona una estructura central para gestionar el uso de las aplicaciones, incluidos autenticar al usuario, gestionar cambios de contraseña, abrir y cerrar la sesión del usuario y realizar un seguimiento de las limitaciones de cuenta, como la hora del día. El PAM es extensible a aplicaciones de terceros y, por lo tanto, puede proporcionar una gestión ininterrumpida de acceso a servicios en un sistema.

En este capítulo, se tratan los siguientes temas:

Novedades de autenticación en Oracle Solaris 11.2

Esta sección destaca información importante para clientes existentes sobre nuevas funciones importantes en las tecnologías del PAM y Kerberos en esta versión.

Novedades del PAM

Las nuevas funciones para la estructura del PAM en la versión Oracle Solaris 11.2 incluyen lo siguiente:

- El módulo `pam_unix_account` admite el control de acceso basado en tiempo para todos los servicios del PAM o aquellos especificados. Por lo tanto, las operaciones relacionadas con la seguridad que llaman al PAM se puede restringir a determinados días y horas. Opcionalmente, puede proporcionar una zona horaria. Consulte la página del comando man `pam_unix_account`(5).

- Las palabras clave `access_times` y `access_tz` se pueden asignar a usuarios y roles. Al igual que todos los atributos de seguridad del usuario, estas palabras clave se admite en todos los servicios de nombres. Para obtener más información, consulte la página del comando man `user_attr(4)`.

Novedades de Kerberos

Las nuevas funciones de Kerberos en la versión Oracle Solaris 11.2 incluyen lo siguiente:

- Kerberos admite los trabajos por lotes autenticados que se ejecutan en momentos arbitrarios. Los comandos que permiten la ejecución retrasada, `at`, `batch` y `cron`, pueden utilizar servicios Kerberos sin necesidad de intervención manual para proporcionar autenticación. Para obtener más información, consulte “Configuración de la ejecución pospuesta para el acceso a servicios Kerberos” [123].
- Puede configurar automáticamente los clientes Kerberos con Automated Installer (AI). Estos clientes son capaces, de manera intermedia, de alojar servicios kerberizados. Aprovisionar automáticamente un sistema cliente Kerberos durante la instalación permite a los administradores implementar de forma rápida y sencilla una infraestructura segura, que libera valiosos recursos del administrador del sistema.
  - Los sistemas cliente instalados no requieren pasos adicionales para especificar la configuración de Kerberos y crear las claves de servicio de Kerberos para el sistema.
  - Existen diferentes opciones posibles al proporcionar claves de servicio Kerberos para los sistemas cliente.

  Para obtener más información sobre la configuración de Kerberos mediante Automated Installer, consulte “Cómo configurar clientes Kerberos mediante AI” de “Instalación de sistemas Oracle Solaris 11.2 ”.
- El servicio `ktkt_warn` está desactivado de manera predeterminada. Debe activarlo explícitamente para advertir a los usuarios sobre la caducidad de la credencial de TGT inicial o para renovar automáticamente una credencial inicial del usuario. Para obtener más información, consulte “Renovación automática de todos los tickets de otorgamiento de tickets” [113].

Para obtener información sobre el historial de Kerberos en Oracle Solaris, consulte “Componentes de las distintas versiones de Kerberos” en “Administración de : Servicios de seguridad”.

Acerca del PAM

El PAM proporciona una estructura para que las aplicaciones realicen varias funciones de autenticación. Proporciona autenticación central, gestión de la sesión, gestión de contraseñas

y limitaciones de cuenta para los usuarios de aplicaciones, incluidos programas del sistema central. El PAM permite que estos programas, como `login`, `su` y `ssh`, permanezcan sin cambios cuando cambian los detalles de gestión de usuarios. Las aplicaciones de sitio pueden utilizar el PAM para gestionar sus propias cuentas, credenciales, sesiones y requisitos de contraseña. El PAM está “conectado” a estas aplicaciones.

Introducción a la estructura PAM

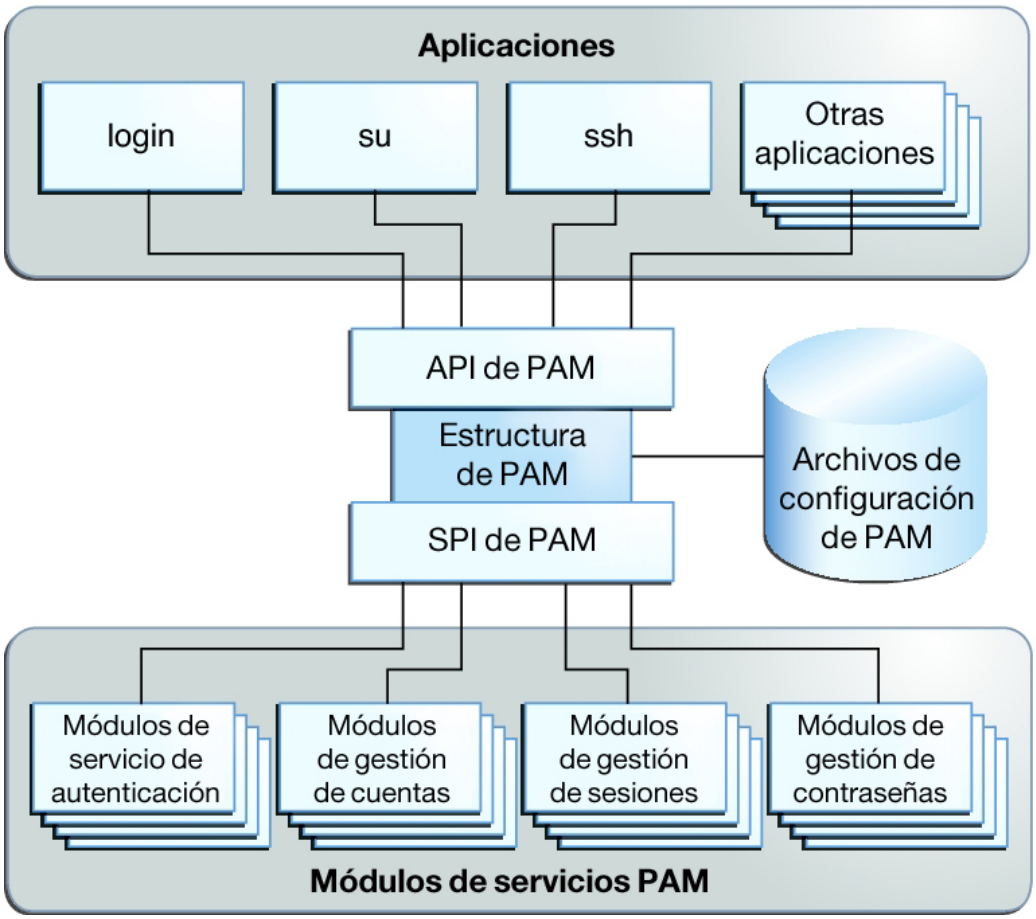
La estructura del PAM consta de cuatro partes:

- Aplicaciones que utilizan el PAM
- Estructura del PAM
- Módulos de servicios del PAM
- Configuración del PAM, incluidas la selección de módulos y la asignación de usuario

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 del PAM sin tener que conocer la semántica de la política de autenticación. Con PAM, los administradores pueden adaptar el proceso de autenticación a las necesidades de un determinado sistema sin tener que cambiar ninguna aplicación. En su lugar, los administradores ajustar la configuración del PAM.

La siguiente figura ilustra la arquitectura PAM.

FIGURA 1-1 Arquitectura del PAM



La arquitectura funciona de la siguiente manera:

- Las aplicaciones se comunican con la estructura del PAM a través de la interfaz de programación de aplicaciones (API) del PAM.

  Para obtener información sobre el uso de API, consulte la página del comando man `pam`(3PAM) y Capítulo 3, “Writing PAM Applications and Services” de “Developer’s Guide to Oracle Solaris 11 Security ”.
- Los módulos de servicio del PAM se comunican con la estructura del PAM a través de la interfaz del proveedor de servicios (SPI) del PAM. Para obtener más información, consulte la página del comando man `pam_sm`(3PAM).

Para obtener una descripción breve de los módulos de servicio seleccionados, consulte "Módulos de servicios del PAM" [38] y las páginas del comando man `pam.conf`(4) y `pam_user_policy`(5).

Los administradores pueden configurar una o más series de módulos para gestionar los requisitos del sitio. Esta serie de módulos se denomina *pila* del PAM. La pila se evalúa en orden. Si una aplicación necesita más de una pila del PAM, el desarrollador de la aplicación debe crear más de un *nombre de servicio*. Por ejemplo, el daemon `sshd` proporciona y requiere varios nombres de servicio para el PAM. Para conocer la lista de nombres de servicio del PAM para el daemon `sshd`, busque la palabra `PAM` en la página del comando man `sshd`(1M). Para obtener detalles de la pila del PAM, consulte "Apilamiento del PAM" [33]. Pasos "Ejemplo de apilamiento del PAM" [37] de una pila de autenticación del PAM.

Ventajas del uso de PAM

La estructura del PAM permite configurar los requisitos que los usuarios deben cumplir para utilizar una aplicación. A continuación, incluimos algunas de las ventajas que ofrece el PAM:

- Política de configuración del PAM flexible
  - Política de autenticación por nombre de servicio
  - Política del PAM de todo el sitio y política del PAM por usuario
  - Opción administrativa de una política de autenticación predeterminada
  - Cumplimiento de varios requisitos del usuario en sistemas de seguridad elevada
- Facilidad de uso para el usuario final
  - No hay necesidad de volver a escribir contraseñas idénticas para diferentes servicios de autenticación
  - Petición de datos de usuario por parte de varios servicios de autenticación en lugar de hacer que un usuario escriba varios comandos
- Facilidad de configuración para el administrador
  - Capacidad de transferir opciones al módulo de servicio del PAM
  - La capacidad de implementar una política de seguridad específica del sitio sin tener que cambiar las aplicaciones

Planificación de una configuración del PAM específica del sitio

Cuando se entrega, la configuración del PAM implementa una política de seguridad estándar que abarca servicios de sistema que requieren autenticación, como `login` y `ssh`. Si debe

implementar una política de seguridad distinta para algunos de los servicios del sistema o crear una política para aplicaciones de terceros, tenga en cuenta lo siguiente:

- Determine que los archivos de configuración proporcionados no satisfacen sus necesidades.

  Pruebe la configuración predeterminada. Pruebe los archivos por usuario en el directorio `/etc/security/pam_policy`. Pruebe si el nombre de servicio predeterminado `other` maneja los requisitos. Pasos de "Ejemplo de apilamiento del PAM" [37] por una pila `other`.
- Identifique los nombres de servicio cuya pila se deba modificar. Para obtener un ejemplo de la modificación de un nombre de servicio de la pila del PAM, consulte Cómo crear un archivo de configuración del PAM específico del sitio [21].
- Para cualquier aplicación de terceros que está codificada para utilizar la estructura del PAM, determine los nombres de servicio del PAM que utiliza la aplicación.
- Para cada nombre de servicio, determine qué módulos utilizará el PAM.

  Revise las páginas del comando man de la sección 5 para los módulos del PAM. Estas páginas del comando man describen cómo funciona cada módulo, qué opciones están disponibles y las interacciones entre los módulos apilados. Para obtener un breve resumen de los módulos seleccionados, consulte "Módulos de servicios del PAM" [38]. Los módulos del PAM también están disponibles desde sistemas externos.
- Por nombre de servicio, decida el orden en el que desea ejecutar los módulos.
- Seleccione el indicador de control para cada módulo. Para obtener más información sobre los indicadores de control, consulte "Apilamiento del PAM" [33]. Tenga en cuenta que los indicadores de control puede tener implicaciones de seguridad.

  Para obtener una representación visual, consulte Figura 1-2, "Apilamiento PAM: efecto de los indicadores de control" y Figura 1-3, "Apilamiento PAM: cómo se determina el valor integrado".
- Seleccione las opciones que son necesarias para cada módulo. La página del comando man para cada módulo muestra las opciones que están disponibles para ese módulo.
- Pruebe el uso de la aplicación con la configuración del PAM. Pruebe como el rol `root`, otros roles, usuarios con privilegios y usuarios comunes. Si algunos usuarios no están autorizados a utilizar la aplicación, pruebe dichos usuarios.

Asignación de una política del PAM por usuario

El módulo del PAM `pam_user_policy` permite a los administradores del sistema asignar configuraciones del PAM específicas en función de cada usuario. Cuando este módulo es el primer módulo en una pila del PAM y el atributo de seguridad `pam_policy` para el usuario especifica un archivo de configuración del PAM, el archivo especifica la política del PAM para el usuario.

Para obtener más información, consulte las siguientes direcciones:

- Página del comando man `pam_user_policy`(5)

- “Apilamiento del PAM” [33]
- Cómo crear un archivo de configuración del PAM específico del sitio [21]
- Ejemplo 1-3, “Configuración de la política del PAM por usuario mediante un perfil de derechos”

Configuración del PAM

Puede utilizar el PAM tal como está. Esta sección proporciona ejemplos de configuraciones del PAM que no están en vigor de manera predeterminada.

TABLA 1-1 Mapa de tareas del PAM

Tarea	Descripción	Para obtener instrucciones
Planificar la instalación de PAM.	Abarca cómo planificar la personalización del PAM para el sitio.	“Planificación de una configuración del PAM específica del sitio” [19]
Asignar una nueva política PAM a un usuario.	Personaliza los requisitos de autenticación por usuario para varios servicios.	Cómo crear un archivo de configuración del PAM específico del sitio [21]
Crear usuarios con los directorios de inicio cifrados.	Modifica una pila del PAM para permitir la creación de directorios de inicio cifrados.	Ejemplo 1-1, “Uso de una pila del PAM modificada para crear un directorio de inicio cifrado”
Agregar nuevos módulos PAM.	Explica cómo instalar y probar los módulos del PAM personalizados.	Cómo agregar un módulo PAM [23]
Asignar una política del PAM no predeterminada a los usuarios.	Muestra cómo agregar una política del PAM a un perfil de derechos para la asignación a un rango de usuarios en los sitios que usan Kerberos, LDAP o una combinación de inicios de sesión.	Cómo asignar una política del PAM modificada [26]
Asignar una política del PAM no predeterminada a los usuarios.	Distribuye pilas del PAM personalizadas a todas las imágenes del sistema.	Cómo asignar una política del PAM modificada [26]
Iniciar el registro de errores.	Registra mensajes de error del PAM a través de `syslog`.	Cómo registrar los informes de errores de PAM [29]
Solucionar errores del PAM.	Proporciona los pasos para localizar, corregir y probar errores en la configuración del PAM.	Cómo solucionar problemas de errores de configuración del PAM [30]

▼ Cómo crear un archivo de configuración del PAM específico del sitio

En la configuración predeterminada, los servicios de entrada `ssh` y `telnet` están abarcados por el nombre de servicio `other`. El archivo de configuración del PAM en este procedimiento cambia los requisitos para `ssh` y `telnet`.

Antes de empezar Debe asumir el rol `root`. Para obtener más información, consulte "Uso de sus derechos administrativos asignados" de "Protección de los usuarios y los procesos en Oracle Solaris 11.2 ".

1. **Cree un nuevo archivo de configuración de política PAM.**
   Utilice el comando `pfedit` para crear el archivo. Coloque el archivo en un directorio de configuración de sitio como `/opt`. También puede colocarlo en el directorio `/etc/security/pam_policy`.

   Nota - No modifique los archivos existentes en el directorio `/etc/security/pam_policy`.

   Incluya comentarios explicativos en el archivo.

   ```
   # pfedit /opt/local_pam/ssh-telnet-conf
   #
   # PAM configuration which uses UNIX authentication for console logins,
   # (see pam.d/login), and LDAP for SSH keyboard-interactive logins
   # This stack explicitly denies telnet logins.
   #
   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. **Proteja el archivo.**
   Proteja el archivo con la propiedad de `root` y permisos de `444`.

   ```
   # ls -l /opt/local_pam

   total 5
   -r--r--r--   1 root         4570 Jun 21 12:08 ssh-telnet-conf
   ```

3. **Asigne la política.**
   Consulte Cómo asignar una política del PAM modificada [26].

ejemplo 1-1 Uso de una pila del PAM modificada para crear un directorio de inicio cifrado

De manera predeterminada, el módulo `zfs_pam_key` no está en el archivo `/etc/security/pam_policy/unix`. En este ejemplo, el administrador crea una versión de la política del PAM `unix` por usuario y, luego, utiliza la nueva versión para crear los usuarios cuyos directorios de inicio se cifran.

```
# cp /etc/security/pam_policy/unix /opt/local_pam/unix-encrypt
```

```
# pfedit /opt/local_pam/unix-encrypt.conf
...
other   auth required          pam_unix_auth.so.1
other   auth required          pam_unix_cred.so.1
## pam_zfs_key auto-creates an encrypted home directory
##
other auth required           pam_zfs_key.so.1 create
```

El administrador utiliza este archivo de política al agregar usuarios. Tenga en cuenta que no se puede agregar cifrado a un sistema de archivos. El sistema de archivos se debe crear con el cifrado activado. Para obtener más información, consulte `zfs_encrypt`(1M).

El administrador crea un usuario y asigna una contraseña.

```
# useradd -K pam_policy=/opt/local_pam/unix-encrypt.conf jill
# passwd jill
New Password: xxxxxxxx
Re-enter new Password: xxxxxxxx
passwd: password successfully changed for jill
```

Luego, el administrador crea el directorio de inicio cifrado mediante el inicio de sesión como usuario.

```
# su - jill
Password: xxxxxxxx
Creating home directory with encryption=on.
Your login password will be used as the wrapping key.
Oracle Corporation      SunOS 5.11      11.2    July 2014

# logout
```

Para conocer las opciones del módulo de servicio ZFS, consulte la página del comando man `pam_zfs_key`(5).

Por último, el administrador verifica que el nuevo directorio principal sea un sistema de archivos cifrados.

```
# mount -p | grep ~jill
rpool/export/home/jill - /export/home/jill zfs - no
rw,devices,setuid,nonbmand,exec,rstchown,xattr,atime
# zfs get encryption,keysource rpool/export/home/jill
NAME                   PROPERTY    VALUE              SOURCE
rpool/export/home/jill  encryption  on                 local
rpool/export/home/jill  keysource   passphrase,prompt  local
```

▼ Cómo agregar un módulo PAM

Este procedimiento muestra cómo agregar, proteger y probar un nuevo módulo del PAM. Los nuevos módulos pueden ser necesarios para políticas de seguridad específicas del sitio o para

admitir aplicaciones de terceros. Para crear un módulo del PAM, consulte Capítulo 3, “Writing PAM Applications and Services” de “Developer’s Guide to Oracle Solaris 11 Security ”.

Nota - Debe instalar una versión de 32 bits y una de 64 bits del módulo de servicio del PAM.

Antes de empezar Complete “Planificación de una configuración del PAM específica del sitio” [19].

Debe asumir el rol `root`. Para obtener más información, consulte “Uso de sus derechos administrativos asignados” de “Protección de los usuarios y los procesos en Oracle Solaris 11.2 ”.

1. **Instale y, luego, proteja ambas versiones del módulo de servicio del PAM en el disco.**
   Asegúrese de que la propiedad y los permisos protejan los archivos del módulo con la propiedad de `root` y los permisos de `444`.

```
# cd /opt/pam_modules
# ls -lR
.:
total 4
-r--r--r--   1 root     root        4570 Nov 27 12:34 pam_app1.so.1
drwxrwxrwx   2 root     root           3 Nov 27 12:38 sparcv9

./64:
total 1
-r--r--r--   1 root     root        4862 Nov 27 12:38 pam_app1.so.1
```

   El módulo de 32 bits está en el directorio `/opt/pam_modules` y el módulo de 64 bits en el subdirectorio `64`.

2. **Agregue el módulo al archivo de configuración del PAM apropiado.**
   En el ejemplo siguiente, el módulo es para una aplicación nueva, `app1`. Su nombre de servicio es el mismo nombre que el de la aplicación. Cree un archivo de nombre de servicio `app1` en el directorio `/etc/pam.d`. La primera entrada en el archivo permite al servicio `app1` ser asignado a usuarios individuales.

```
# cd /etc/pam.d
# pfedit app1
...
# PAM configuration
#
# app1 service
#
auth definitive         pam_user_policy.so.1
auth required           /opt/pam_modules/$ISA/pam.app1.so.1  debug
```

   El token `$ISA` en la ruta del módulo dirige la estructura del PAM a la versión correspondiente de la arquitectura de 32o 64 bits del módulo de servicio para la aplicación de llamada. Para las aplicaciones de 32 bits, */a/b/*$ISA/*module*.so se convierte en */a/b/module*.so. y para las

aplicaciones de 64 bits, se convierte en */a/b/*64/*module*.so. En este ejemplo, instaló el módulo de servicio de 32 bits `pam.app1.so.1` service en el directorio `/opt/pam_modules` y el módulo de 64 bits, en el directorio `/opt/pam_modules/64`.

Si desea obtener más información, consulte las páginas del comando man `pfedit`(1M) y `pam.conf`(4).

Para limitar la política del PAM `app1` a usuarios seleccionados, consulte Ejemplo 1-2, “Agregar un módulo nuevo a un archivo de política del PAM por usuario”.

3. **Pruebe el nuevo servicio.**

   Inicie sesión directamente mediante `login` o `ssh`. A continuación, ejecute los comandos que se ven afectados por el nuevo módulo. Pruebe los usuarios que tienen permitido y prohibido el uso de los comandos afectados. Para obtener ayuda con la resolución de problemas, consulte Cómo solucionar problemas de errores de configuración del PAM [30].

4. **Asigne la política.**

   Consulte Cómo asignar una política del PAM modificada [26].

ejemplo 1-2 Agregar un módulo nuevo a un archivo de política del PAM por usuario

En este ejemplo, el servicio `app1` no es utilizado por todos los usuarios, de modo que el administrador agrega la política como un servicio por usuario.

```
# cd /etc/pam.d
# cp app1 /opt/local_pam/app1-conf
# pfedit /opt/local_pam/app1-conf

## app1 service
##
app1 auth definitive         pam_user_policy.so.1
app1 auth required           /opt/pam_modules/$ISA/pam_app1.so.1  debug
```

El administrador suprime el archivo `app1` del directorio `pam.d`.

```
# rm /etc/pam.d/app1
```

A continuación, el administrador agrega la política `app1-conf` a la política del PAM del administrador del sistema.

```
# rolemod -K pam_policy=/opt/local_pam/app1-conf sysadmin
```

ejemplo 1-3 Configuración de la política del PAM por usuario mediante un perfil de derechos

En este ejemplo se utiliza el atributo de seguridad `pam_policy` para permitir que los usuarios de diferentes servicios de nombres se autentiquen. El archivo de política del PAM `any` se

proporciona en el directorio `/etc/security/pam_policy`. Los comentarios en el archivo describen esta política.

No modifique los archivos de este directorio.

```
# profiles -p "PAM Per-User Policy of Any" \
'set desc="Profile which sets pam_policy=any";
set pam_policy=any; exit;'
```

Para asignar este perfil de derechos, consulte Cómo asignar una política del PAM modificada [26].

▼ Cómo asignar una política del PAM modificada

En este procedimiento, debe configurar una política del PAM no predeterminada en todas las imágenes del sistema. Después de que se copian todos los archivos, puede asignar la política del PAM nueva o modificada a usuarios individuales o a todos los usuarios.

Antes de empezar Ha modificado y ha probado los archivos de configuración del PAM que implementan la nueva política.

Debe asumir el rol `root`. Para obtener más información, consulte "Uso de sus derechos administrativos asignados" de "Protección de los usuarios y los procesos en Oracle Solaris 11.2 ".

1. **Agregue los archivos del PAM no predeterminados a todas las imágenes del sistema.**

   Debe agregar todos los nuevos módulos del PAM y los archivos de configuración del PAM nuevos y modificados a todas las imágenes del sistema.

   a. **En primer lugar, agregue los nuevos módulos del PAM para cada imagen del sistema.**

      i. **Agregue el módulo del PAM de 32 bits al directorio de arquitectura adecuada.**

      ii. **Agregue el módulo del PAM de 64 bits al directorio de arquitectura adecuada.**

      Para obtener un ejemplo de configuración de directorio, consulte Paso 1 in Cómo agregar un módulo PAM [23].

   b. **A continuación, agregue nuevos archivos de configuración del PAM para cada imagen del sistema.**

Por ejemplo, agregue el archivo `/opt/local_pam/ssh-telnet-conf` a cada imagen del sistema.

c. A continuación, copie cualquier archivos de configuración del PAM modificado a cada imagen del sistema.

Por ejemplo, copie un archivo `/etc/pam.conf` modificado y cualquier `/etc/pam.d/`*service-name-files* a cada imagen del sistema.

2. Asigne una política del PAM no predeterminada a todos los usuarios.

a. Modifique el archivo `policy.conf` en una de las siguientes formas:

- **Agregue un archivo de configuración del PAM a la palabra clave `PAM_POLICY` en el archivo `policy.conf`.**

```
# pfedit /etc/security/policy.conf
...
# PAM_POLICY=
PAM_POLICY=/opt/local_pam/ssh-telnet-conf
...
```

- **Agregue un perfil de derechos a la palabra clave `PROFS_GRANTED` en el archivo `policy.conf`.**

Por ejemplo, asigne la política del PAM por usuario de cualquier perfil de derechos desde Ejemplo 1-3, “Configuración de la política del PAM por usuario mediante un perfil de derechos”.

```
# pfedit /etc/security/policy.conf
...
AUTHS_GRANTED=
# PROFS_GRANTED=Basic Solaris User
PROFS_GRANTED=PAM Per-User Policy of Any,Basic Solaris User
...
```

b. Copie el archivo `policy.conf` modificado a cada imagen del sistema.

3. Para asignar una política del PAM no predeterminada a usuarios individuales, puede asignar la política directamente a un usuario o agregar la política al perfil de derecho que se asigna a los usuarios.

- **Asigne la política del PAM directamente a usuarios individuales.**

```
# usermod -K pam_policy="/opt/local_pam/ssh-telnet-conf" jill
```

- **Incluya la política del PAM en un perfil de derechos y asigne el perfil a usuarios individuales.**

En este ejemplo, se utiliza la política del PAM `ldap`.

```
# profiles -p "PAM Per-User Policy of LDAP" \
'set desc="Profile which sets pam_policy=ldap";
set pam_policy=ldap; exit;'
```

Luego, asigne el perfil de derechos a un usuario.

```
# usermod -P +"PAM Per-User Policy of LDAP" jill
```

ejemplo 1-4 Límite de la pila del PAM `ktelnet` a usuarios seleccionados

El administrador desea permitir a un número limitado de los usuarios la capacidad de utilizar `telnet` en un dominio Kerberos. Por lo tanto, antes de activar el servicio `telnet`, el administrador cambia el archivo de configuración `ktelnet` predeterminado y coloca el archivo `ktelnet` predeterminado en el directorio `pam_policy`.

En primer lugar, el administrador configura un archivo `ktelnet` por usuario.

```
# cp /etc/pam.d/ktelnet /etc/security/pam_policy/ktelnet-conf
# pfedit /etc/security/pam_policy/ktelnet-conf
...
# Kerberized telnet service
#
ktelnet  auth required          pam_unix_cred.so.1
ktelnet  auth required          pam_krb5.so.1
```

El comando protege el archivo con permisos de `444`.

```
# chmod 444 /etc/security/pam_policy/ktelnet-conf
# ls -l /etc/security/pam_policy/ktelnet-conf
-r--r--r--   1 root     root         228 Nov 27 15:04 ktelnet-conf
```

Luego, el administrador modifica el archivo `ktelnet` en el directorio `pam.d`.

- La primera entrada permite la asignación por usuario.
- La segunda entrada deniega el uso de `ktelnet` a menos que el administrador le asigne `pam_policy=ktelnet`.

```
# cp /etc/pam.d/ktelnet /etc/pam.d/ktelnet.orig
               # pfedit /etc/pam.d/ktelnet
...
# Denied Kerberized telnet service
#
auth definitive         pam_user_policy.so.1
auth required           pam_deny.so.1
```

El administrador prueba la configuración con un usuario con privilegios, un usuario común y el rol root. Cuando la configuración pasa, el administrador activa el servicio `telnet` y asigna la política por usuario a los administradores de Kerberos.

```
# svcadm enable telnet
# rolemod -S ldap -K pam_policy=ktelnet-conf kerbadmin
```

El administrador copia los archivos modificados en todos los servidores Kerberos y activa `telnet` en esos servidores.

▼ Cómo registrar los informes de errores de PAM

Antes de empezar Debe asumir el rol `root`. Para obtener más información, consulte “Uso de sus derechos administrativos asignados” de “Protección de los usuarios y los procesos en Oracle Solaris 11.2 ”.

1. **Determine qué instancia de 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
```

2. **Configure el archivo `syslog.conf` para el nivel de registro que necesita.**

   Consulte la sección `DESCRIPCIÓN` de la página del comando man `syslog.conf`(4) para obtener información sobre los niveles de registro. La mayoría de los informes de errores del PAM se realiza mediante la utilidad `LOG_AUTH`.

   Por ejemplo, cree un archivo para la salida de depuración.

```
# touch /var/adm/pam_debuglog
```

   A continuación, agregue la entrada `syslog.conf` para enviar la salida de depuración a ese archivo.

Nota - Si la instancia de servicio `rsyslog` está en línea, modifique el archivo `rsyslog.conf`.

```
# pfedit /etc/syslog.conf
...
*.debug        /var/adm/pam_debuglog
...
```

3. **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.

▼ Cómo solucionar problemas de errores de configuración del PAM

Antes de empezar Debe asumir el rol `root`. Para obtener más información, consulte “Uso de sus derechos administrativos asignados” de “Protección de los usuarios y los procesos en Oracle Solaris 11.2 ”.

1. **Para cada entrada del PAM cuyos problemas está solucionado, agregue la opción `debug`.**
   Por ejemplo, las siguientes entradas en el archivo `/etc/pam.d/cron` crean la salida de depuración para el servicio.

   ```
   account definitive      pam_user_policy.so.1     debug
   account required        pam_unix_account.so.1    debug
   ```

2. **Registre los errores del PAM en el nivel correspondiente y actualice el daemon `syslog`.**
   Para obtener detalles, consulte Cómo registrar los informes de errores de PAM [29].

3. **Si el problema es una configuración del PAM dañada, realice las siguientes acciones:**

   a. **Ejecute la aplicación desde una ventana de terminal y modifique el archivo de configuración del PAM en otra ventana.**

   b. **Verifique que se hayan corregido los errores mediante la prueba los cambios en la ventana de la aplicación.**

4. **Si el problema es una configuración del PAM dañada que impide el inicio de sesión, inicie en modo de un solo usuario, luego, corrija el archivo, reinicie y pruebe.**

   - **Para iniciar un sistema SPARC, escriba el siguiente comando en el indicador de PROM:**

     ```
     ok > boot -s
     ```

   - **Para iniciar un sistema x86, agregue la opción `-s` a la línea de opciones de núcleo en el menú de GRUB.**

   Para obtener más información, consulte las páginas del comando man `boot`(1M) y `grub`(5).

5. **Verifique que se hayan corregido los errores.**
   Inicie sesión directamente mediante `login` o `ssh`. Pruebe que los usuarios comunes, los usuarios con privilegios y roles puedan utilizar los comandos.

Referencia de configuración del PAM

Esta sección proporciona detalles adicionales sobre el PAM, incluido el apilamiento del PAM.

Archivos de configuración del PAM

Las aplicaciones del sistema, como `login` y `ssh`, que utilizan la estructura del PAM están configuradas en los archivos de configuración del PAM en el directorio `/etc/pam.d`. El archivo `/etc/pam.conf` también se puede utilizar. Los cambios que se realizan en estos archivos afectan a todos los usuarios del sistema.

Además, el directorio `/etc/security/pam_policy` contiene archivos de configuración del PAM. Estos archivos abarcan varios servicios y están diseñados para la asignación por usuario. Los archivos de este directorio no deben modificarse.

- **Directorio** `/etc/pam.d`: contiene archivos de configuración del PAM específicos de servicio, incluido el archivo comodín, `other`. Para agregar un servicio para una aplicación, agregue un único archivo *service-name* que es el nombre de servicio utilizado por la aplicación. Si corresponde, la aplicación puede utilizar la pila del PAM en el archivo `other`.

  Los archivos de servicio del directorio `/etc/pam.d` proporcionan la configuración predeterminada en la mayoría de las implementaciones del PAM. Se ensamblan automáticamente mediante el mecanismo de IPS como se describe en la página del comando man `pkg`(5). Este valor predeterminado simplifica la interoperabilidad con otras aplicaciones del PAM entre plataformas. Para obtener más información, consulte la página del comando man `pam.conf`(4).
- **Archivo** `/etc/pam.conf`: el archivo de política y configuración del PAM antiguo. Este archivo se envía vacío. El mecanismo preferido para la configuración del PAM es utilizar los archivos del directorio `/etc/pam.d`. Para obtener más información, consulte la página del comando man `pam.conf`(4).
- **Directorio** `/etc/security/pam_policy`: contiene archivos de política del PAM que contienen políticas para varios servicios. Estos archivos se pueden asignar a un individuo, a un grupo de individuos o a todos los usuarios, según sea necesario. Dicha asignación sustituye los archivos de configuración del PAM del sistema en el directorio `pam.conf` o `/etc/pam.d`. No modifique estos archivos. Para agregar un archivo por usuario, consulte Cómo crear un archivo de configuración del PAM específico del sitio [21]. Para obtener información sobre los archivos por usuario, consulte la página del comando man `pam_user_policy`(5).

El administrador del sistema gestiona los archivos de configuración del PAM. Un orden incorrecto de entradas, es decir, una pila del PAM incorrecta, 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 ayuda, consulte “Apilamiento del PAM” [33] y Cómo solucionar problemas de errores de configuración del PAM [30].

Orden de búsqueda de configuración PAM

Las aplicaciones llaman para la búsqueda en la estructura del PAM para los servicios del PAM configurados en el siguiente orden:

1. El nombre del servicio se busca en el archivo `/etc/pam.conf`.
2. Se utilizan servicios específicos en el archivo `/etc/pam.d/`*service-name*.
3. El nombre de servicio `other` se comprueba en el archivo `/etc/pam.conf`.
4. Se utiliza el archivo `/etc/pam.d/other`.

Este orden permite que un archivo `/etc/pam.conf` existente trabaje con los archivos de configuración del PAM por servicio en el directorio `/etc/pam.d`.

Sintaxis de archivo de configuración de PAM

El archivo `pam.conf` y los archivos por usuario del PAM utilizan una sintaxis que es diferente de los archivos específicos del servicio en el directorio `pam.d`.

- Las entradas en los archivos `/etc/pam.conf` y `/etc/security/pam_policy` se realizan en uno de dos formatos:

  service-name module-type control-flag module-path module-options

  service-name module-type `include` *path-to-included-PAM-configuration*

- Las entradas en los archivos *service-name* en el directorio `/etc/pam.d` omiten el nombre del servicio. El nombre del archivo proporciona el nombre del servicio.

  module-type control-flag module-path module-options

  module-type `include` *path-to-included-PAM-configuration*

Los elementos de la sintaxis del archivo de configuración del PAM son los siguientes:

service-name

El nombre del servicio que no distingue mayúsculas de minúsculas, por ejemplo, `login` o `ssh`. Una aplicación puede utilizar distintos nombres para los servicios que la aplicación

proporciona. Por ejemplo, busque la palabra `PAM` en la página del comando man `sshd`(1M) para los nombres de servicio para los servicios diferentes que el daemon `sshd` proporciona.

El nombre de servicio predefinido "`other`" es el nombre del servicio predeterminado si no se proporciona una configuración de servicio específica.

module-type

Indica 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 del servicio. Los indicadores de control válidos se describen en "Apilamiento del PAM" [33].

module-path

La ruta de acceso al módulo que implementa el tipo de módulo. Si el nombre de la ruta no es absoluto, se asume que es relativo a la ruta `/usr/lib/security/$ISA/`. La macro o el token `$ISA` le indica a la estructura del PAM que busque en el directorio específico de la arquitectura de la ruta del módulo.

module-options

Opciones como `nowarn` y `debug` que se pueden transferir a los módulos de servicios. Una página del comando man de un módulo describe las opciones de ese módulo.

path-to-included-PAM-configuration

Especifica la ruta de acceso completa a un archivo de configuración del PAM o un nombre de archivo que es relativo al directorio `/usr/lib/security`.

Apilamiento del PAM

Cuando una aplicación llama a una de las siguientes funciones, la estructura del PAM lee los archivos de configuración del PAM para determinar qué módulos implementan el nombre de servicio del PAM de esta aplicación:

- `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, 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` en el archivo `/etc/pam.d/passwd`.

```
auth required           pam_passwd_auth.so.1
```

Si, por otro lado, varios módulos implementan un servicio, se dice que esos módulos están *apilados*, es decir, existe una pila del PAM para ese nombre de servicio. Por ejemplo, tenga en cuenta las entradas de un servicio `/etc/pam.d/login` de ejemplo:

```
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 crean una pila `auth` para el nombre de 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 del 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, el fallo de un módulo `requisite` o `definitive` termina la pila. Si no hay fallos anteriores, el éxito de un módulo `sufficient`, `definitive` o `binding` también finaliza la pila. Después del procesamiento de la pila, los resultados individuales se combinan en un único resultado general que se proporciona a la aplicación. Para obtener una representación gráfica, consulte Figura 1-2, “Apilamiento PAM: efecto de los indicadores de control” y Figura 1-3, “Apilamiento PAM: cómo se determina el valor integrado”.

El indicador de control señala el rol que un módulo del 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 se han registrado fallos anteriores. 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 se han registrado fallos anteriores.

  Si se registró un módulo anterior, ese fallo se devuelve inmediatamente a la aplicación, sin ejecuciones adicionales de módulos. Un fallo provoca la devolución inmediata de error un sin ejecuciones adicionales de módulos.
- **Include**: agrega líneas de un archivo de configuración del PAM independiente que se utilizará en este momento en la pila del PAM. Este indicador no controla el comportamiento de éxito o error. Cuando se lee un archivo nuevo, la pila del PAM `include` aumenta. Cuando finaliza la comprobación de la pila en el nuevo archivo, el valor de la pila `include`

disminuye. Cuando se llega al final de un archivo y la pila del PAM `include` es `0`, finaliza el procesamiento de la pila. El número máximo para la pila del PAM `include` 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 que la pila sea correcta. El éxito final de la pila se devuelve solamente si ningún módulo binding o required ha informado fallos.

  Un fallo provoca la devolución de un error tras la ejecución de los módulos restantes de este servicio.
- **Requisite**: el éxito en el cumplimiento de los requisitos de un módulo requisite es necesario para que la pila sea correcta. Todos los módulos requisite de una pila deben devolver un valor de éxito para que la pila pueda devolver un valor de éxito a la aplicación.

  Un fallo provoca la devolución inmediata de error un sin ejecuciones adicionales de módulos.
- **Sufficient**: si no se han registrado 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 conectados siguientes muestran cómo se determina un resultado en el proceso de integración.

- El primer diagrama muestra cómo se registra el éxito o error para cada tipo de indicador de control. Los resultados se muestran en el segundo diagrama.
- El segundo diagrama muestra cómo se determina el valor integrado. El fallo opcional y el fallo requerido devuelven error, y el éxito devuelve éxito. La aplicación determina cómo controlar estos códigos de retorno.

FIGURA 1-2 Apilamiento PAM: efecto de los indicadores de control

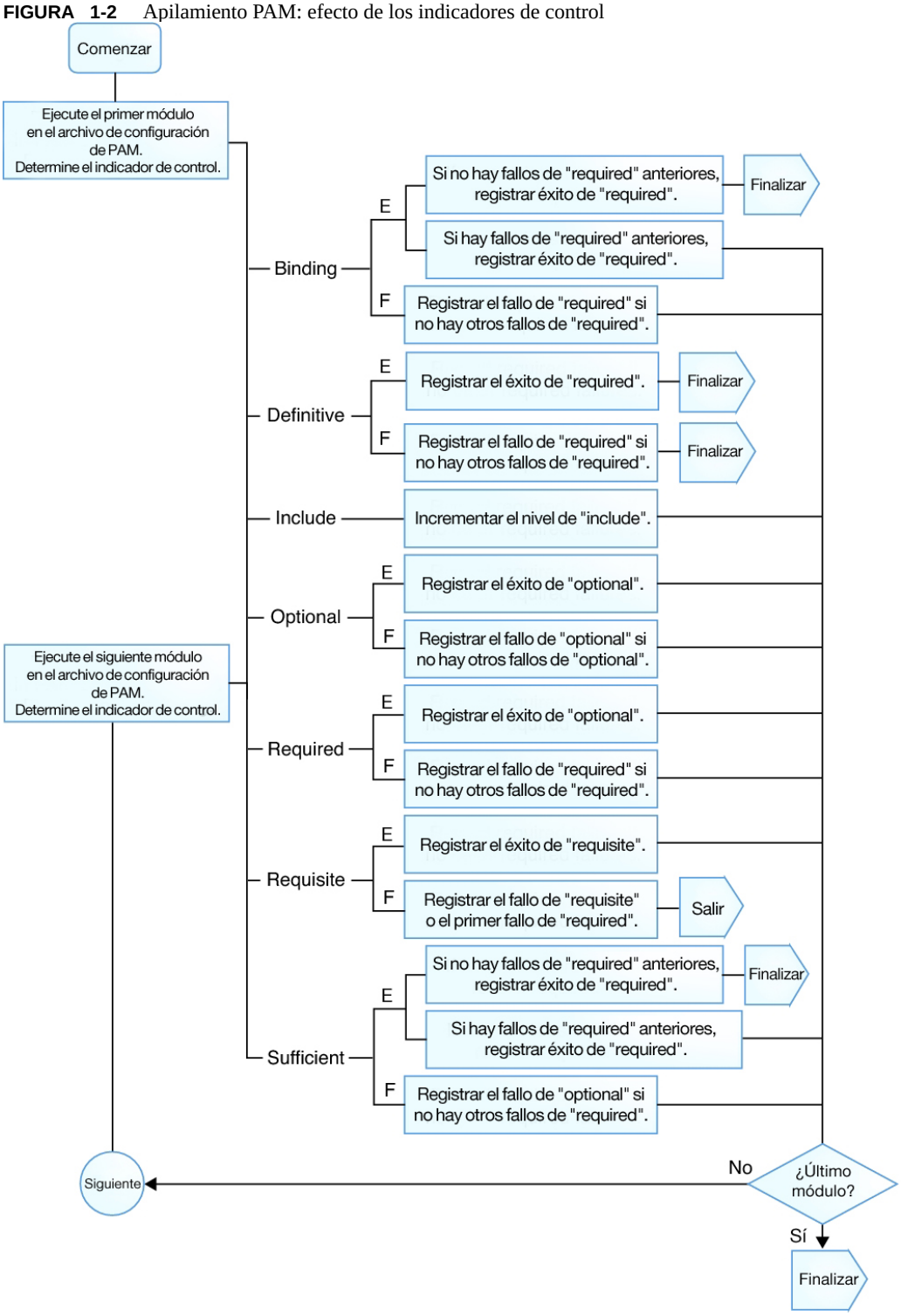
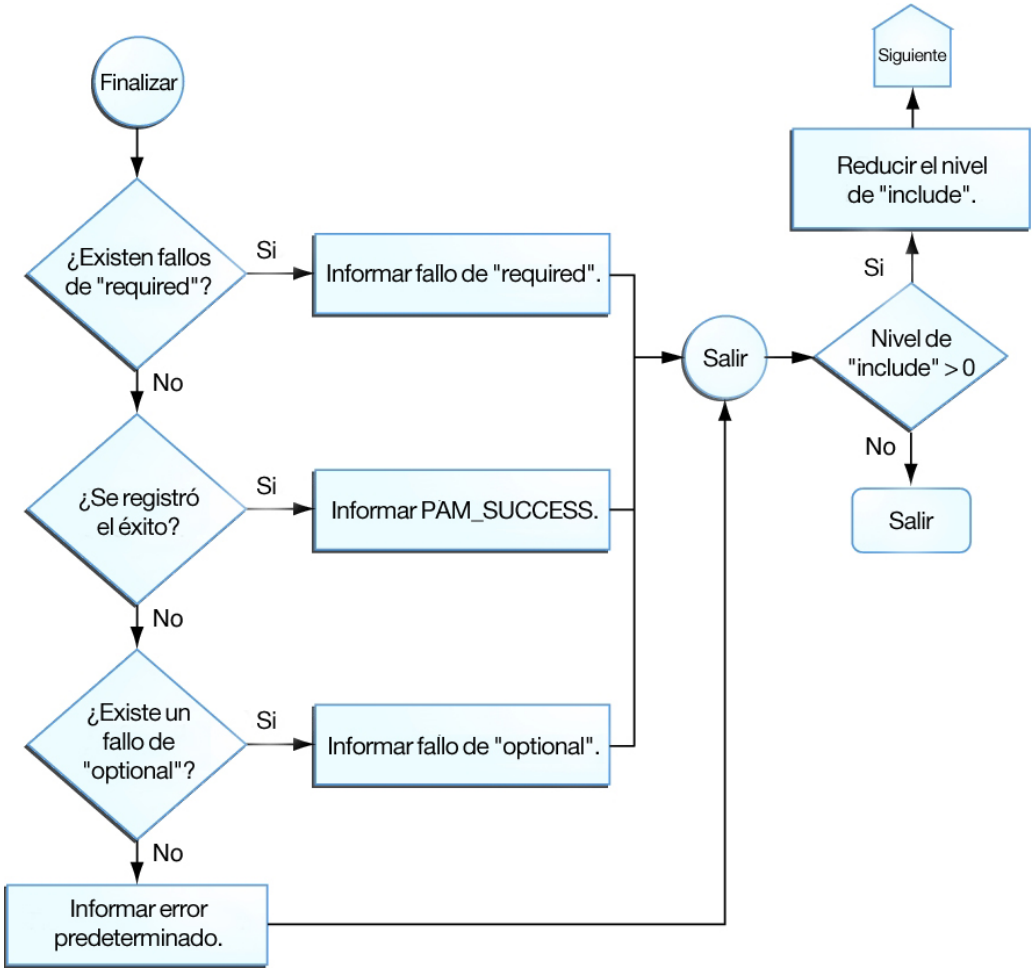


FIGURA 1-3 Apilamiento PAM: cómo se determina el valor integrado



Ejemplo de apilamiento del PAM

El siguiente ejemplo muestra las definiciones predeterminadas para la gestión de autenticación en el archivo `/etc/pam.d/other` de ejemplo. Estas definiciones se utilizan para la autenticación si no se han configurado definiciones de autenticación 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 del PAM para el usuario se comprueba mediante el módulo `pam_user_policy.so`. El indicador de control `definitive` indica que si la evaluación de la pila del PAM configurada se realiza con éxito, se devuelve un aviso de éxito a la aplicación, ya que ningún otro módulo se habrá comprobado en ese punto. Si la evaluación de la pila del PAM configurada falla, se devuelve un código de fallo a la aplicación y no se realizan más comprobaciones. Si no hay ninguna política del PAM por usuario asignada a este usuario, se ejecuta el módulo siguiente.

Si no se asigna una política del PAM por usuario para este usuario, se ejecuta el módulo `pam_authtok_get`. El indicador de control de este módulo se estableció en `requisite`. Si `pam_authtok_get` falla, finaliza el proceso de autenticación y se devuelve un valor de error a la aplicación.

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 de integración 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 se han realizado correctamente, se devuelve un valor de éxito a la aplicación. Si `pam_dhkeys`, `pam_unix_auth` o `pam_unix_cred` devuelve un fallo, el fallo se devuelve a la aplicación.

Módulos de servicios del PAM

Esta sección muestra los módulos de servicio del PAM seleccionados. Los módulos se muestran por página del comando man, seguidos por una breve descripción de dónde y cuándo se utilizan. Para obtener más información, lea la página del comando man.

Para obtener una lista de todos los módulos de servicios del PAM que proporciona Oracle Solaris, consulte la sección 5 de las páginas del comando man. Se agregan módulos nuevos de forma regular. Por ejemplo, en esta versión, se agrega un número de módulos para la autenticación con los sistemas Windows. Es posible que el sitio también agregue módulos del PAM de terceros.

`pam_allow(5)` — Devuelve `PAM_SUCCESS` para todas las llamadas. Consulte también la página del comando man `pam_deny(5)`.

`pam_authtok_check(5)` — Valida el token de contraseña para el cambio de contraseña.

pam_authtok_get(5)	Proporciona la funcionalidad de una solicitud de contraseña para la pila del PAM.
pam_authtok_store(5)	Actualiza el token de la contraseña para PAM_USER.
pam_deny(5)	Devuelve el código de retorno fallos predeterminados de tipo de módulo para todas las llamadas. Consulte también la página del comando man pam_allow(5).
pam_dhkeys(5)	Proporciona funcionalidad para dos servicios del PAM: autenticación RPC segura y gestión de token de autenticación RPC segura.
pam_krb5(5)	Proporciona funciones para verificar la identidad de un usuario Kerberos y para gestionar la caché de credenciales de Kerberos.
pam_krb5_migrate(5)	Ayuda a migrar PAM_USER al dominio Kerberos local del cliente.
pam_ldap(5)	Proporciona una funcionalidad para las pilas de gestión de cuentas y autenticación del PAM mediante el servidor de directorio LDAP configurado.
pam_list(5)	Proporciona funciones para validar la cuenta del usuario en este host. La validación se basa en una lista de usuarios y grupos de red en el host.
pam_passwd_auth(5)	Proporciona la funcionalidad de autenticación para la pila de contraseñas.
pam_pkcs11(5)	Permite que un usuario inicie sesión en un sistema con un certificado X.509 y su clave privada dedicada que se almacenan en un token PKCS#11.
pam_roles(5)	Verifica que un usuario tiene autorización para asumir un rol y evita el inicio de sesión directo por un rol.
pam_smb_passwd(5)	Admite cambiar o agregar contraseñas SMB para los usuarios Oracle Solaris locales. Consulte también la página del comando man smb(4).
pam_smbfs_login(5)	Sincroniza las contraseñas entre clientes Oracle Solaris y sus servidores CIFS/SMB.
pam_tsol_account(5)	Verifica las limitaciones de cuenta Trusted Extensions que están relacionadas con etiquetas.
pam_tty_tickets(5)	Proporciona un mecanismo para comprobar un ticket que se creó con una autenticación correcta anterior.
pam_unix_account(5)	Proporciona funciones para validar que la cuenta del usuario no esté bloqueada o caducada y que la contraseña del usuario no deba cambiarse.

	Incluye comprobaciones de `access_times` y `access_tz`.
`pam_unix_auth`(5)	Proporciona funciones para verificar que la contraseña es la contraseña correcta para `PAM_USER`.
`pam_unix_cred`(5)	Proporciona funciones que establecen información sobre las credenciales del usuario. Permite que la funcionalidad se sustituya de forma independiente de la funcionalidad de credenciales de autenticación.
`pam_unix_session`(5)	Abre y cierra una sesión, y también actualiza el archivo `/var/adm/lastlog`.
`pam_user_policy`(5)	Llama a una configuración del PAM específica del usuario.
`pam_zfs_key`(5)	Proporciona funciones para cargar y cambiar la frase de contraseña de cifrado ZFS para el directorio de inicio cifrado de un usuario.

♦ ♦ ♦ CAPÍTULO 2

Acerca del servicio Kerberos

En este capítulo, se brinda una introducción al servicio Kerberos. Este capítulo contiene la información siguiente:

¿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*, lo que significa que sólo debe autenticarse con el servicio una vez por sesión. Todas las transacciones realizadas posteriormente durante la sesión se protegen 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 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). Si utilizó el producto Kerberos V5, la versión de Oracle Solaris le resultará muy familiar. Dado que el protocolo Kerberos V5 es un estándar del sector *de facto* para la seguridad de la red, la versión Oracle Solaris permite a las transacciones seguras 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 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

En esta sección se proporciona una descripción general del sistema de autenticación de Kerberos. Para obtener una descripción más detallada, consulte “De qué manera las credenciales de Kerberos proporcionan acceso a servicios” [54].

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 solicita un archivo montados en NFS), 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 al servidor NFS. La expresión "de manera transparente" implica que no necesita solicitar un ticket de manera explícita. La solicitud se produce cuando se intenta

acceder al servidor. Debido a que sólo los clientes que están autenticados pueden obtener un ticket para un servicio específico, los demás clientes no pueden acceder al servidor NFS 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 mayor detalle en “De qué manera las credenciales de Kerberos proporcionan acceso a servicios” [54].

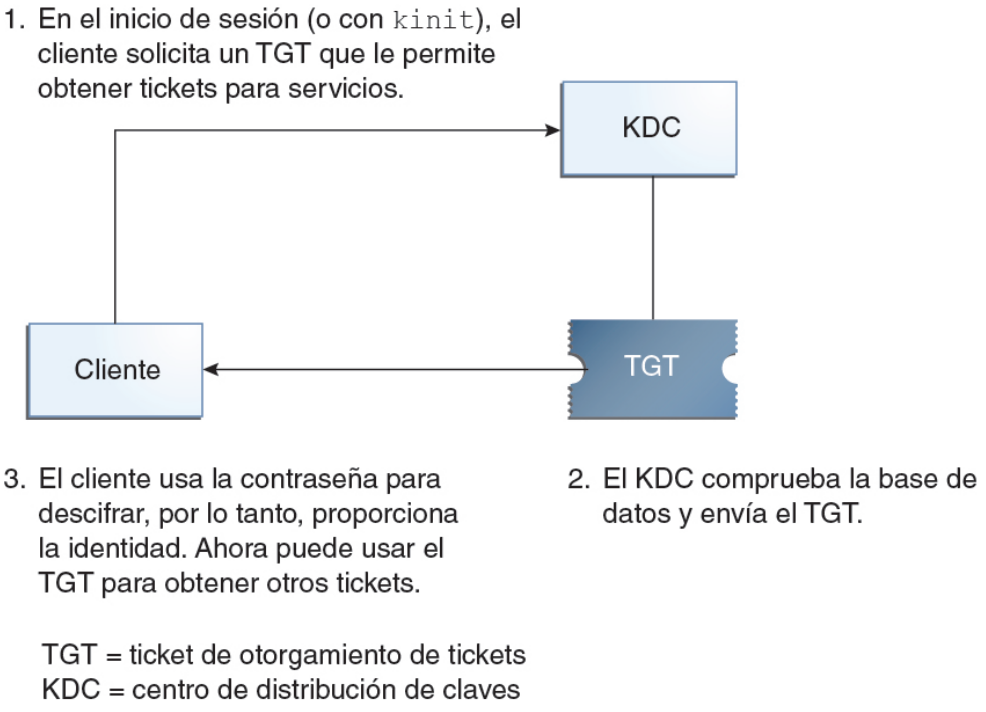
Las siguientes secciones explican más detalladamente el proceso de autenticación Kerberos.

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 2-1 Autenticación inicial para una sesión Kerberos



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

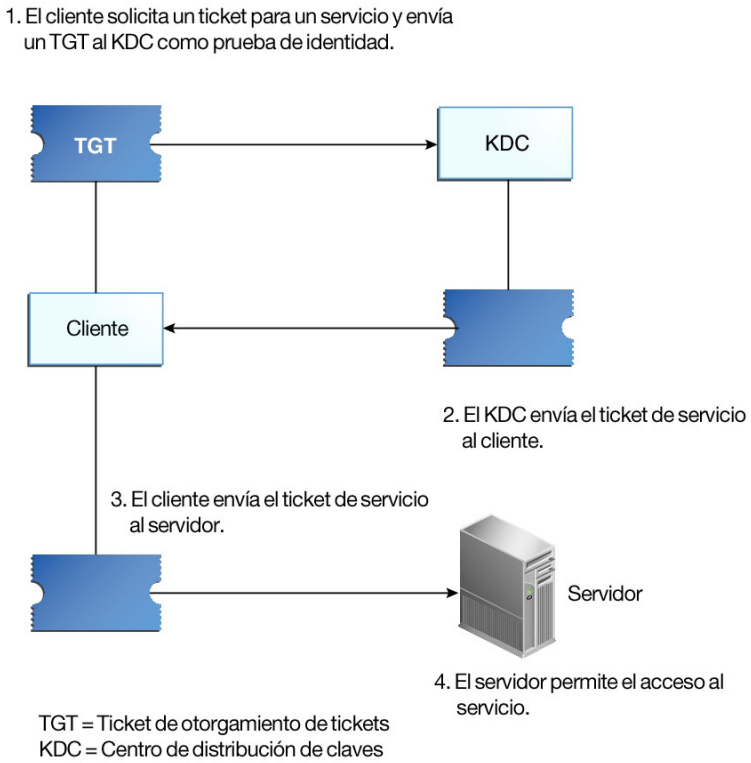
centro. La diferencia radica en que los comandos basados en Kerberos detectan que tiene un pase de esquí para el fin de semana y entonces obtienen un ticket de ascenso para usted.

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 `nfs` o `ssh`, 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 2-2 Obtención de acceso a un servicio con la autenticación Kerberos



1. El cliente solicita al KDC un ticket para un servicio en particular; por ejemplo, para iniciar sesión en otra máquina 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.

   Suponga que el usuario `jdoe` quiere acceder a un sistema de archivos NFS que se ha compartido con la autenticación `krb5` requerida. Como `jdoe` ya se encuentra autenticado (es decir, `jdoe` ya tiene un ticket de otorgamiento de tickets), cuando `jdoe` intenta acceder a los archivos, el sistema de cliente NFS obtiene un ticket del KDC de manera automática y transparente para el servicio NFS. Para utilizar otro servicio kerberizado,`jdoe` 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.

Si bien estos pasos implican que el servidor nunca se comunica con el KDC, el servidor se registra a sí mismo con el KDC, como lo hace el primer cliente. A fin de simplificar el proceso, esa sección se excluye.

Autenticación Kerberos de trabajos por lotes

Los trabajos por lotes, como cron, at y batch, son procesos de ejecución retrasada. En un entorno de Kerberos, todos los procesos, incluidos los procesos de ejecución de retrasada, requieren credenciales. Sin embargo, las credenciales de los usuarios tienen relativamente breve duración. De manera predeterminada, las credenciales de usuario son válidas por 8 horas y renovables por una semana. Estos horario están diseñados para limitar la exposición de claves confidenciales a usuarios no autorizados, pero puede evitar que la ejecución de trabajos en momentos arbitrarios.

En Oracle Solaris, los trabajos por lotes que acceden a los servicios Kerberos pueden ejecutarse sin exponer las claves de larga duración del usuario. La solución implica el almacenamiento de credenciales que incluyen el servicio Kerberos, el nombre de usuario y el nombre de host del cliente en una caché de credencial de usuario por sesión. Se utiliza un módulo del PAM para autenticar el trabajo por lotes. Para qué servicios un host puede obtener tickets puede almacenarse centralmente en el servidor de directorios LDAP.

Para obtener más información, consulte las páginas del comando man `pam_krb5_keytab`(5) y `pam_gss_s4u`(5) y “Configuración de la ejecución pospuesta para el acceso a servicios Kerberos” [123].

Kerberos, DNS y el servicio de nombres

El servicio Kerberos se compila a fin de usar el DNS para resolver nombres de host. El servicio `nsswitch` no se comprueba para resolver los nombres de host.

Componentes de Kerberos

Kerberos incluye dominios, programas de red, principales, servidores y otros componentes. Para obtener una lista de comandos y módulos, consulte “Utilidades de Kerberos” [51].

Programas de red de Kerberos

Nota - En esta versión de Oracle Solaris, todos los comandos de inicio de sesión remoto excepto `ssh` están anticuados. Si desea utilizar uno de los siguientes comandos anticuados para alcanzar un sistema antiguo, puede hacerlo. Si desea utilizar un comando antiguo en el sistema porque el comando se utiliza en una secuencia de comandos antigua, debe activar el servicio SMF para ese comando, como en `svcadm enable login:rlogin`. Como alternativa, puede modificar las secuencias de comandos para utilizar el comando `ssh`. Del mismo modo, para que un sistema anterior llegue a este sistema con un comando antiguo, el servicio para el comando debe estar activado en este sistema.

Los comandos anticuados, como `telnet`, pueden requerir claves de cifrado débiles. De manera predeterminada, estas teclas no están permitidas en el archivo `krb5.conf`. Para obtener más información, consulte “Tipos de cifrado admitidos en Kerberos” [62] y la página del comando man `krb5.conf`(4).

Para obtener más información, consulte “Control de acceso a recursos del equipo” de “Protección de sistemas y dispositivos conectados en Oracle Solaris 11.2 ”. Consulte también las páginas del comando man que se muestran en “Comandos de usuario de Kerberos” [171].

Los comandos basados en Kerberos (“Kerberizados”) disponibles para los usuarios son los siguientes:

- `ftp`
- `rcp`, `rlogin`, `rsh`
- `ssh`, `scp`, `sftp`
- `telnet`

Estas aplicaciones son iguales a la aplicación de Oracle 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. Para obtener información sobre los principales, consulte “Principales de Kerberos” [48].

Estos comandos se analizan detalladamente en “Comandos de usuario de Kerberos” [171].

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 `jdoe`, o un servicio, como `nfs`.

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, `jdoe/admin@CORP.EXAMPLE.COM`. En este ejemplo:

- `jdoe` 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 `jdoe` a veces actúa como administrador del sistema, el principal `jdoe/admin` puede distinguir entre el administrador de la identidad de usuario. Del mismo modo, si `jdoe` tiene cuentas en dos hosts diferentes, las cuentas pueden utilizar dos nombres de principal con instancias diferentes, por ejemplo, `jdoe/denver.example.com` y `jdoe/boston.example.com`. Tenga en cuenta que el servicio Kerberos trata `jdoe` y `jdoe/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.corp.example.com`. La combinación nombre primario/instancia para este ejemplo podría ser `ftp/bigmachine.corp.example.com` o `host/bigmachine.corp.example.com`.
- `CORP.EXAMPLE.COM` es el dominio Kerberos. En “Dominios Kerberos” [49], se analizan los dominios.

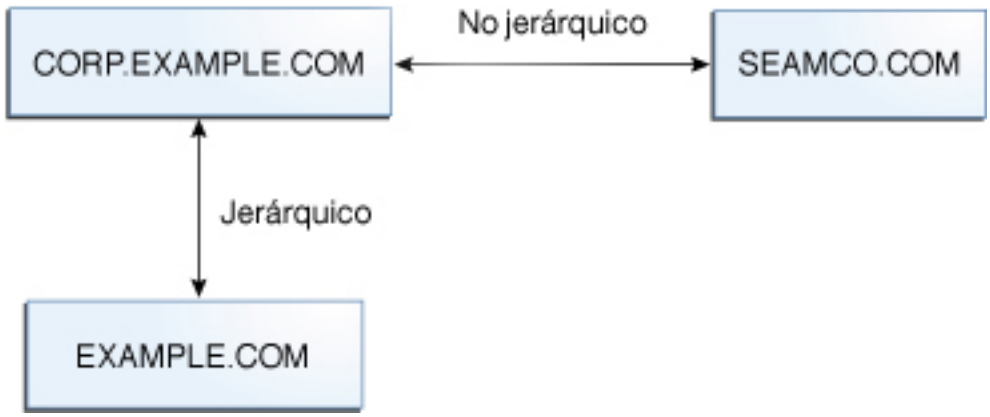
Todos los nombres de principal que aparecen a continuación son válidos:

- `jdoe`
- `jdoe/admin`
- `jdoe/admin@CORP.EXAMPLE.COM`
- `nfs/host.corp.example.com@CORP.EXAMPLE.COM`
- `host/corp.example.com@CORP.EXAMPLE.COM`

Dominios Kerberos

Un *dominio* es una red lógica, similar a un dominio, que define un grupo de sistemas con el mismo *KDC principal*. La Figura 2-3, “Dominios Kerberos” 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. La *autenticación entre dominios* de Kerberos permite la autenticación entre dominios. Cada dominio sólo necesita una entrada de principal para el otro dominio en su KDC.

FIGURA 2-3 Dominios 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 una copia duplicada 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`, `ssh` y NFS.

La siguiente figura muestra lo que un dominio hipotético puede llegar a contener.

FIGURA 2-4 Un dominio de Kerberos típico

Utilidades 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 de red: `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 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 Oracle Solaris incluye lo siguiente:

- Módulos 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. Los módulos hacen que la autenticación Kerberos sea transparente para el usuario.
- Pilas del PAM por usuario de Kerberos V5: proporciona archivos de configuración del PAM para escenarios diferentes en el directorio `/etc/security/pam_policy`.
- 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.
- Interfaz gráfica de usuario de la administración de Kerberos (`gkadmin`): le permite administrar los principales y las políticas de los principales en una interfaz gráfica de usuario basada en tecnología Java™ como alternativa al comando `kadmin`.

Para obtener más información, consulte Capítulo 7, Referencia del servicio Kerberos.

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.

Tipos de cifrado Kerberos

Los tipos de cifrado identifican los algoritmos criptográficos y el modo en que se deben usar cuando se realizan las operaciones criptográficas. Para obtener una lista de los tipos de cifrado admitidos, consulte las páginas del comando man `krb5.conf`(4) y `kdb5_util`(1M).

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. El protocolo Kerberos permite al cliente solicitar que el KDC utilice determinados tipos de cifrado para la parte del cliente de la respuesta del ticket. El protocolo no permite que el servidor especifique tipos de cifrado para el KDC.

Tenga en cuenta las siguientes cuestiones 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 que se generan para el principal sean compatibles con los sistemas que 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. Los dos métodos recomendados de restringir los tipos de cifrado son mediante el indicador `-e` en el comando `kadmin addprinc` o la definición del parámetro `supported_enctypes` en el archivo `kdc.conf` de

este subconjunto. Utilice el parámetro `supported_enctypes` cuando la mayoría de los sistemas de un dominio Kerberos admiten un subconjunto del conjunto predeterminado de tipos de cifrado. Al definir `supported_enctypes`, se especifica el conjunto predeterminado de tipos de cifrado que `kadmin addprinc` utiliza cuando crea un principal para un dominio en particular.

- 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.
- El parámetro `master_key_enctype` 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_enctype` 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 `aes256-cts-hmac-sha1-96` a un tipo de cifrado diferente. Cuando configure los KDC esclavos, asegúrese de que todos admitan el tipo de cifrado seleccionado y tengan una entrada `master_key_enctype` idéntica en su archivo `kdc.conf`. Asimismo, asegúrese de que `master_key_enctype` se encuentre definido en uno de los tipos de cifrado en `supported_enctypes` si `supported_enctypes` 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 las solicitudes del tipo de cifrado procedentes del KDC mediante parámetros en el archivo `krb5.conf`. El parámetro `default_tkt_enctypes` 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_enctypes` 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_enctypes` 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, no debe definir `default_tkt_enctypes` 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_enctypes` 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_enctypes` = `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 este parámetro, 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 que acepta con el parámetro `permitted_enctypes` en el archivo `kdc.conf`. Además, puede especificar los tipos de cifrado utilizados en la creación de entradas keytab. Intente evitar utilizar 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.

Tipos de cifrado de Kerberos y algoritmos de FIPS 140

Puede configurar Kerberos para que se ejecute en Modo FIPS 140 en Oracle Solaris. Si el dominio contiene sistemas o aplicaciones antiguos que no cumplen con FIPS 140, el dominio no se puede ejecutar en Modo FIPS 140.

Cuando se ejecuta en Modo FIPS 140, se dice que Kerberos es un *consumidor* del *proveedor* de FIPS 140. En Oracle Solaris, el proveedor es la estructura criptográfica. El único tipo de cifrado de Kerberos que está validado por FIPS 140 para la estructura criptográfica es `des3-cbc-sha1`. No es el predeterminado. Para obtener instrucciones, consulte Cómo configurar Kerberos para que se ejecute en modo FIPS 140 [73].

Nota - Si debe cumplir con un requisito estricto de usar únicamente criptografía validada por FIPS 140-2, debe estar ejecutando la versión Oracle Solaris 11.1 SRU 5.5 o la versión Oracle Solaris 11.1 SRU 3. Oracle completó una validación de FIPS 140-2 respecto de la estructura criptográfica en estas dos versiones específicas. Oracle Solaris 11.2 parte de esta base validada e incluye mejoras de software que se centran en el rendimiento, la funcionalidad y la confiabilidad. Siempre que sea posible, debe configurar Oracle Solaris 11.2 en FIPS 140-2 para aprovechar estas mejoras.

De qué manera las credenciales de Kerberos proporcionan acceso a servicios

Los servicios remotos permiten el acceso 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 `nfs` en un servidor que se llama `boston` se requiere una credencial. Para acceder al servicio `nfs` en otro servidor se necesita la credencial independiente.

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 (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.

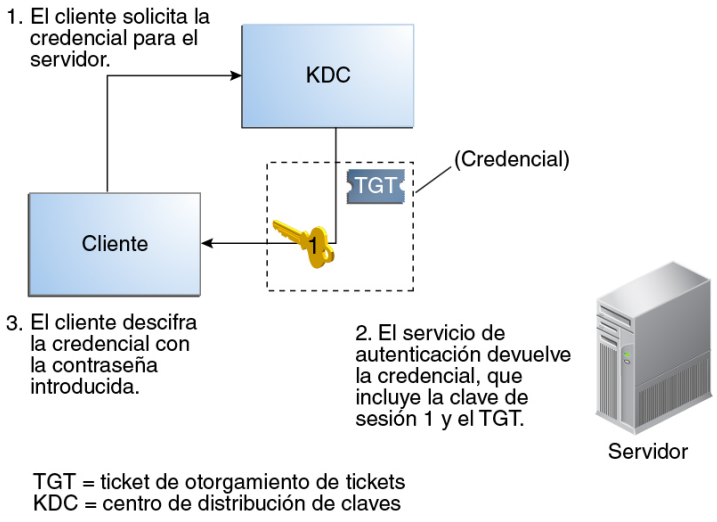
El proceso de creación y almacenamiento de las credenciales es transparente. Las credenciales las crea el KDC que las envía al solicitante. Cuando se recibe, la credencial se almacena en una caché de credenciales.

Obtención de una credencial para el servicio de otorgamiento de tickets

1. A fin de iniciar el proceso de autentificación, 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 caché 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. A continuación, el cliente tiene una credencial para utilizar con el servicio de otorgamiento de tickets y está listo para solicitar una credencial para un servidor.

FIGURA 2-5 Obtención de una credencial para el servicio de otorgamiento de tickets

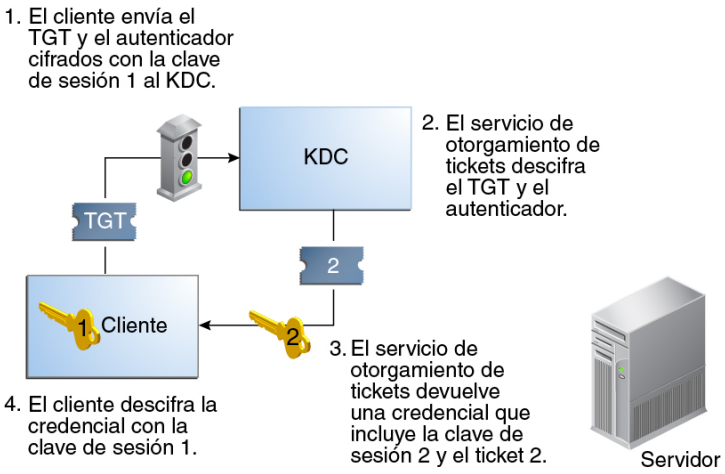


Obtención de una credencial para un servidor Kerberizado

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" [55]. 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 caché 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 2-6 Obtención de una credencial para un servidor

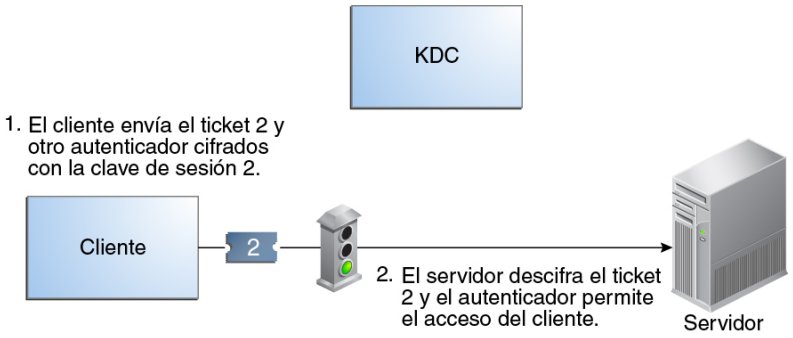


Obtención de acceso a un servicio Kerberos específico

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” [55] y “Obtención de una credencial para un servidor Kerberizado” [56]. 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 2-7 Obtención de acceso a un servicio específico



Diferencias importantes entre Oracle Solaris Kerberos y MIT Kerberos

Las mejoras que se incluyen en Oracle Solaris pero no en MIT Kerberos son:

- Compatibilidad de Kerberos con las aplicaciones remotas de Oracle Solaris
- Propagación progresiva de 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 thread de Kerberos con GSS-API
- Uso de la estructura de cifrado para la criptografía

♦ ♦ ♦ CAPÍTULO 3

Planificación del servicio Kerberos

En el capítulo abarca diferentes opciones de instalación y configuración que los administradores deben determinar antes de configurar o implementar el servicio Kerberos:

Planificación de una implementación Kerberos

Antes de instalar el servicio Kerberos, debe resolver varios problemas de configuración. Si bien puede cambiar la configuración después de la instalación inicial, algunos cambios pueden ser difíciles de implementar. Además, algunos cambios necesitan que se reconstruya el KDC, por lo que considere objetivos a largo plazo antes de implementar 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 Kerberos

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 mantiene un nombre que es familiar. Puede utilizar cualquier cadena, pero puede que la configuración y el mantenimiento requieran más trabajo. Utilice nombres de dominio que sigan la estructura estándar de nombres de Internet.

Número de dominios Kerberos

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. Planee crear al menos dos servidores KDC por dominio, un servidor maestro y al menos 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 Kerberos

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. Cuando todos los dominios en la cadena jerárquica están configurados correctamente, estas rutas automáticas pueden facilitar la carga administrativa. Sin embargo, si hay muchos niveles de dominios, es posible que no desee utilizar la ruta automática porque requiere demasiadas transacciones.

También puede decidir establecer la relación de confianza directamente. Una relación de confianza directa es 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 que se requiere trabajo adicional. La relación de confianza directa también se denomina como una relación transitiva. Para obtener una ilustración, consulte “Dominios Kerberos” [49]. Para conocer los procedimientos de configuración, consulte “Configuración de autenticación entre dominios” [125].

Asignación de nombres de host para dominios Kerberos

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.

También puede utilizar DNS para buscar información sobre los KDC. El uso de DNS facilita el cambio de la información porque no es necesario editar el archivo `krb5.conf` en todos los clientes Kerberos para cada cambio.

Nota - Los procedimientos descritos en esta guía asumen el uso de DNS.

Para obtener más información, consulte la página del comando man `krb5.conf`(4).

Los clientes Kerberos en Oracle Solaris interoperan bien con servidores 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 Kerberos

Kerberos en Oracle Solaris no utiliza el servicio `name-service/switch`. En su lugar, el servicio Kerberos utiliza DNS para resolver los nombres de host. Por lo tanto, DNS debe estar activado 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 esta guía 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 es la forma canónica del nombre de host del sistema que proporciona el servicio.

El siguiente ejemplo muestra cómo el servicio Kerberos aplica el formato canónico a los nombres de host. Si un usuario ejecuta el comando `ssh alpha.example.com` donde `alpha.example.com` es un alias de host para el cname `beta.example.com`, el servicio Kerberos pone en forma canónica `alpha.example.com` a `beta.example.com`. El KDC procesa el ticket como una solicitud para el principal del servicio *host*`/beta.example.com`.

Para los nombres de principal que incluyen el FQDN de un host, asegúrese de 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, el nombre de dominio DNS puede ser `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 (SMF) 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 activar el servicio de cliente DNS en todos los hosts.

Sincronización de reloj dentro de un dominio Kerberos

Los relojes internos de todos los hosts que participan en el sistema de autenticación de Kerberos deben estar 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). Para obtener más información, consulte “Sincronización de relojes entre clientes Kerberos y KDC” [128]. Se pueden utilizar otras maneras de sincronizar los relojes; sin embargo, se necesita alguna forma de sincronización.

Tipos de cifrado admitidos en 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 que especifica el algoritmo criptográfico y el modo que se utilizará cuando el servicio realice operaciones criptográficas con la clave. Para obtener una lista de los tipos de cifrado admitidos, consulte las páginas del comando man `krb5.conf`(4) y `kdb5_util`(1M).

Si desea cambiar el tipo de cifrado, debe 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. Para obtener más información, consulte “Tipos de cifrado Kerberos” [52].

Los tipos de cifrado débil, como `des`, no se permiten de manera predeterminada. Si necesita utilizar tipos de cifrado débil para la compatibilidad con versiones anteriores o la interoperabilidad, establezca la entrada `allow_weak_crypto` en la sección `libdefaults` del archivo `/etc/krb5/krb5.conf` en `true`.

Planificación de KDC

Los KDC utilizan puertos específicos, requieren servidores adicionales para controlar cargas mayores de tickets y, luego, requieren técnicas de propagación para mantener los servidores sincronizados. Además, los tipos de cifrado se gestionan de forma centralizada. Tiene varias opciones para configurar el KDC por primera vez.

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. Puede 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, debe actualizar el archivo `/etc/krb5/kdc.conf` en cada KDC.

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. Planee crear al menos un KDC esclavo por dominio.

Es posible que se requieran KDC esclavos adicionales según los siguientes 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 agregación de más servidores KDC, puede reducir la carga en los servidores actuales.

Evite agregar demasiados KDC esclavos. Dado 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.

Configure uno o más KDC esclavos 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 para que se convierta en KDC maestro. Para obtener instrucciones, consulte “Intercambio de un KDC maestro y un KDC esclavo” [129].

Propagación de bases de datos de Kerberos

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 información sobre la propagación de base de datos, consulte “Administración de la base de datos de Kerberos” [134].

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 necesaria para 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 la complejidad administrativa. Para obtener más información, consulte “Configuración de la propagación en paralelo para Kerberos” [143].

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. Para obtener referencias de instrucciones para el uso de este comando, consulte “Configuración de servidores KDC” [71].

También puede utilizar LDAP para gestionar los archivos de la base de datos para Kerberos. Para obtener instrucciones, consulte Cómo configurar el KDC maestro para utilizar un servidor de directorios LDAP [86]. LDAP simplifica la administración de sitios que requieren coordinación entre las bases de datos Kerberos y la configuración de servidor de directorios existente.

Planificación para clientes Kerberos

Los clientes Kerberos se pueden instalar automáticamente, instalarse desde una secuencia de comandos, o configurarse de forma manual mediante la edición de archivos de configuración. Para conexiones de red protegida, la estructura del PAM proporciona el módulo `pam_ldap`. Consulte la página del comando man `pam_ldap`(5). Asimismo, cuando el cliente solicita un servicio, este puede otorgarse mediante un servidor distinto del KDC maestro.

Planificación de la instalación automática de los clientes Kerberos

Los clientes Kerberos puede configurarse de forma rápida y sencilla mediante la función Automated Installer (AI) de Oracle Solaris. Los administradores de servidores crean y asignan perfiles de configuración Kerberos a clientes de AI. Además, el servidor de AI proporciona las claves de cliente. Por lo tanto, en la instalación, el cliente Kerberos es un sistema Kerberos aprovisionado completamente, capaz de alojar servicios seguros. El uso de Automated Installer puede reducir los costes de administración y mantenimiento del sistema.

Puede utilizar el comando `kclient` para crear una instalación automatizada para clientes de cualquier tipo de KDC.

- Puede utilizar AI para clientes que no son clientes de un KDC de Oracle Solaris. Para obtener la lista de proveedores de KDC, consulte la página del comando man `kclient`(1M).

  Para todos los tipos de KDC, se admite la transferencia keytab generada previamente. Los KDC y MS AD de Oracle Solaris también admiten el registro automático.
- Ejecute el comando `kclient` para crear perfiles de configuración de Kerberos para AI. Para obtener más información, consulte la página del comando man `kclient`(1M) y “Opciones de configuración del cliente Kerberos” [66]. Para obtener instrucciones para configurar

clientes Kerberos mediante AI, consulte "Cómo configurar clientes Kerberos mediante AI" de "Instalación de sistemas Oracle Solaris 11.2 ".

Opciones de configuración del cliente Kerberos

Puede configurar clientes Kerberos mediante la utilidad de configuración `kclient` o editando manualmente archivos. La utilidad se ejecuta en modo interactivo y el modo no interactivo. En modo interactivo, se le pedirá que indique valores de parámetros específicos de Kerberos, de modo que puede realizar cambios al configurar el cliente. En el modo no interactivo, debe proporcionar un archivo con los valores de parámetros. También se pueden agregar opciones de línea de comandos en el modo no interactivo. Dado que los modos interactivos y no interactivo necesitan menos pasos que la configuración manual, son más rápidos y menos proclives a errores.

Si la siguiente configuración está en vigor, no es necesaria una configuración explícita de su cliente 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 claves distintas de las claves del servidor KDC.

Aún puede que desee configurar explícitamente el cliente Kerberos por los siguientes motivos:

- El proceso de configuración cero realiza más búsquedas de DNS y, por lo tanto, es menos eficaz que la configuración directa que un cliente configurado directamente.
- Si las referencias no se utilizan, la lógica de configuración cero depende del nombre de dominio DNS del host para determinar el dominio. Esta configuración 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 archivo keytab. Si bien es posible desactivar este requisito en el archivo `krb5.conf`, esto no se recomienda por razones de seguridad. Para obtener más información, consulte "Seguridad de inicio de sesión de cliente Kerberos" [66] y la página del comando man `krb5.conf`(4).

Para obtener una descripción completa de la configuración de cliente, consulte "Configuración de clientes Kerberos" [94].

Seguridad de inicio de sesión de cliente Kerberos

En el inicio de sesión, un cliente utiliza el módulo `pam_krb5` para verificar que el KDC que emitió los últimos TGT sea el mismo KDC que emitió el principal de host de cliente que se almacena en el archivo `/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

desactivar. Para desactivar esta verificación, debe definir la opción `verify_ap_req_nofail` en el archivo `krb5.conf` como `false`. Para obtener más información, consulte “Cómo desactivar la verificación del ticket de otorgamiento de tickets” [107].

Servicios de delegación de confianza en Kerberos

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 puede 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 parte cifrada de la respuesta de KDC para el cliente puede incluir una copia de indicadores de tickets de credenciales con el conjunto de opciones `ok_to_auth_as_delegate`. Un cliente puede utilizar esta configuración para determinar si delegar credenciales (concediendo un proxy o TGT reenviado) a este servidor. Al definir esta opción, considere la seguridad y la ubicación del servidor en que se ejecuta el servicio, así como si el servicio requiere el uso de credenciales delegadas.

Planificación del uso de Kerberos de credenciales y nombres de 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. Asimismo, los usuarios UNIX que no tengan cuentas de usuario válidas en el dominio Kerberos predeterminado se pueden migrar automáticamente mediante la estructura del PAM.

Asignación de credenciales GSS a credenciales UNIX

El algoritmo de asignación predeterminado utiliza el nombre primario del principal de Kerberos para buscar el UID. La consulta se produce en el dominio predeterminado o en cualquier dominio permitido mediante el parámetro `auth_to_local_realm` en el archivo `/etc/krb5/`

`krb5.conf`. Por ejemplo, el nombre de principal de usuario `jdoe@EXAMPLE.COM` se asigna al UID del usuario UNIX denominado `jdoe` con la tabla de contraseña. El nombre de principal de usuario `jdoe/admin@EXAMPLE.COM` no se ha asignado porque el nombre de principal incluye el componente de la instancia `admin`.

Si las asignaciones predeterminadas para las credenciales de usuario son suficientes, no es necesario completar la tabla de credenciales GSS. Si la asignación predeterminada no es suficiente, como cuando desea asignar un nombre de principal que contenga un componente de instancia, se deben utilizar otros métodos. Para obtener más información, consulte las siguientes direcciones:

- Cómo crear y modificar una tabla de credenciales [119]
- Cómo proporcionar asignación de credenciales entre dominios [120]
- "Observación de asignación de credenciales GSS a credenciales UNIX" [199]

Tabla `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 UID 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 contraseña. La tabla debe crearse y administrarse una vez que se haya rellenado la base de datos del KDC.

Cuando se recibe una solicitud de cliente, el servicio NFS intenta asignar el nombre de la credencial a un UID de UNIX. Si la asignación falla, se comprueba la tabla `gsscred`.

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 del PAM. Específicamente, puede agregar el módulo `pam_krb5_migrate.so` a la pila de autenticación del servicio del 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 con contraseña correcto en un sistema, un principal de Kerberos se crearía de manera automática para dicho usuario. La nueva contraseña de principal es, entonces, la misma que la contraseña de UNIX. Para obtener instrucciones sobre el uso del módulo `pam_krb5_migrate.so`, consulte Cómo configurar la migración automática de usuarios en un dominio Kerberos [109].

♦ ♦ ♦ CAPÍTULO 4

Configuración del servicio Kerberos

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 `root`, por lo que deben ser realizados por administradores del sistema o usuarios avanzados. También se incluyen procedimientos de configuración entre dominios y otros temas relacionados con servidores KDC.

En este capítulo, se tratan los siguientes temas:

Configuración del servicio Kerberos

Dado que algunos de los procedimientos en el proceso de configuración dependen de otros procedimientos, 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.

Nota - Los ejemplos incluidos en estas secciones utilizan los tipos de cifrado predeterminados, que no están validados por FIPS 140 para Oracle Solaris. Para ejecutar Modo FIPS 140, debe limitar los tipos de cifrado al tipo de cifrado `des3-cbc-sha1` para la base de datos, los servidores y las comunicaciones con los clientes. Antes de crear el KDC, edite los archivos que se incluyen en Cómo configurar Kerberos para que se ejecute en modo FIPS 140 [73].

TABLA 4-1 Mapa de tareas de la configuración del servicio Kerberos

Tarea	Descripción	Para obtener instrucciones
1. Planificar la instalación de Kerberos.	Resuelve problemas de configuración antes de iniciar el proceso de configuración de software. La planificación anticipada permite ahorrar tiempo y otros recursos más tarde.	Capítulo 3, Planificación del servicio Kerberos
2. 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.	"Configuración de servidores KDC" [71]
2a. (Opcional) Configure Kerberos para que se ejecute en Modo FIPS 140.	Activa el uso de algoritmos validados por FIPS 140 únicamente.	Cómo configurar Kerberos para que se ejecute en modo FIPS 140 [73]
2b. Configurar Kerberos para ejecutarse en LDAP (opcional).	Configura el KDC para utilizar un servidor de directorios LDAP.	"Gestión de un KDC en un servidor de directorios LDAP" [93]
3. Instalar el software de protocolo de hora de red (NTP).	Crea un reloj central que proporciona el tiempo para todos los sistemas de la red.	"Sincronización de relojes entre clientes Kerberos y KDC" [128]
4. Configurar los servidores KDC intercambiables (opcional).	Facilita la tarea de intercambio del servidor KDC maestro y un servidor KDC esclavo.	Cómo configurar un KDC esclavo intercambiable [130]
4. Aumentar la seguridad en los servidores KDC (opcional).	Evita infracciones de seguridad en los servidores KDC.	"Restricción de acceso a servidores KDC" [148]

Configuración de servicios Kerberos adicionales

Una vez que se hayan completado los pasos necesarios, se podrán utilizar los procedimientos siguientes, cuando corresponda.

TABLA 4-2 Mapa de tareas de la configuración de servicios Kerberos adicionales

Tarea	Descripción	Para obtener instrucciones
Configurar la autenticación entre dominios.	Permite comunicaciones de un dominio a otro dominio.	"Configuración de autenticación entre dominios" [125]
Configurar los servidores de aplicaciones Kerberos.	Permite que un servidor admita servicios como, por ejemplo, `ftp` mediante la autenticación Kerberos.	"Configuración de servidores de aplicaciones de red de Kerberos" [114]
Configurar servicios de ejecución retrasada.	Permite a un host `cron` ejecutar tareas en momentos arbitrarios.	"Configuración de la ejecución pospuesta para el acceso a servicios Kerberos" [123]

Tarea	Descripción	Para obtener instrucciones
Configurar el servidor NFS con Kerberos.	Permite que un servidor comparta un sistema de archivos que requiere la autenticación Kerberos.	“Configuración de servidores NFS con Kerberos” [117]
Configurar los clientes Kerberos.	Permite que un cliente utilice servicios Kerberos.	“Configuración de clientes Kerberos” [94]
Sincronizar los relojes para ayudar a la autenticación.	Configura un protocolo de sincronización de relojes.	“Sincronización de relojes entre clientes Kerberos y KDC” [128]
Gestionar la base de datos de Kerberos.	Mantiene la base de datos de Kerberos.	“Administración de la base de datos de Kerberos” [134]
Gestionar el archivo intermedio de la base de datos de Kerberos.	Gestiona las claves para la base de datos de Kerberos.	“Administración del archivo intermedio para la base de datos de Kerberos” [145]

Configuración de servidores KDC

Después de instalar el software Kerberos, debe configurar los servidores Centro de distribución de claves (KDC). La configuración del 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 configurar antes de intentar otras tareas.

La diferencia más importante entre un KDC maestro y un KDC esclavo es que sólo el KDC maestro puede controlar solicitudes de administración de bases de datos. Por ejemplo, el cambio de una contraseña o la agregación 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. Los KDC esclavos proporcionan redundancia cuando el KDC maestro no puede responder.

Puede elegir configurar y crear el servidor KDC maestro, la base de datos y servidores adicionales de diversas maneras:

- Automático: se recomienda para secuencias de comandos
- Interactivo: suficiente para la mayoría de las instalaciones
- Manual: necesario para instalaciones más complejas
- Manual con LDAP: necesaria si se utiliza LDAP con el KDC

TABLA 4-3 Mapa de tareas de la configuración de servidores KDC

Tarea	Descripción	Para obtener instrucciones
Instale el depósito de paquetes de KDC.	Depósito de paquetes necesario para la creación de KDC.	Cómo instalar el paquete KDC [72]
(Opcional) Configure Kerberos para que se ejecute en Modo FIPS 140.	Activa el uso de algoritmos validados por FIPS 140 únicamente.	Cómo configurar Kerberos para que se ejecute en modo FIPS 140 [73]
Utilizar una secuencia de comandos para configurar el KDC maestro.	Simplifica la configuración inicial.	Cómo utilizar `kdcmgr` para configurar el KDC maestro [73]

Tarea	Descripción	Para obtener instrucciones
		Ejemplo 4-1, “Ejecución del comando `kdcmgr` sin argumentos”
Utilizar una secuencia de comandos para configurar un servidor KDC esclavo.	Simplifica la configuración inicial.	Cómo utilizar `kdcmgr` para configurar un KDC esclavo [76]
Configurar manualmente el servidor KDC maestro.	Ofrece control sobre cada entrada en los archivos de configuración KDC durante la instalación inicial.	Cómo configurar manualmente un KDC maestro [77]
Configurar manualmente un servidor KDC esclavo.	Ofrece control sobre cada entrada en los archivos de configuración KDC durante la instalación inicial.	Cómo configurar manualmente un KDC esclavo [82]
Configurar manualmente el KDC maestro para utilizar LDAP.	Configura el servidor KDC maestro para utilizar LDAP.	Cómo configurar el KDC maestro para utilizar un servidor de directorios LDAP [86]
Reemplazar las claves del principal en un servidor KDC.	Actualiza la clave de la sesión en un servidor KDC antiguo para utilizar tipos de cifrado más sólidos.	“Sustitución de las claves del servicio de otorgamiento de tickets en un servidor maestro” [92]

▼ Cómo instalar el paquete KDC

De manera predeterminada, el software de cliente Kerberos está instalado en el sistema. Para instalar un Centro de distribución de claves (KDC), debe agregar el depósito de paquetes de KDC.

Antes de empezar Debe tener asignado el perfil de derechos de instalación de software para agregar paquetes al sistema. Para obtener más información, consulte “Uso de sus derechos administrativos asignados” de “Protección de los usuarios y los procesos en Oracle Solaris 11.2 ”.

1. Instale el depósito de paquetes de KDC.

```
$ pkg install system/security/kerberos-5
```

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

2. (Opcional) Enumere los servicios Kerberos.

Con la agregación del depósito de paquetes de servidores, el sistema tiene dos servicios Kerberos adicionales. Al igual que el software de cliente Kerberos, estos servicios están desactivados de manera predeterminada. Configure Kerberos antes de activar estos servicios.

```
$ svcs krb5
STATE          STIME    FMRI
disabled       Sep_10   svc:/network/security/krb5kdc:default
disabled       Sep_10   svc:/network/security/krb5_prop:default
$ svcs | grep kerb
STATE          STIME    FMRI
disabled       Sep_07   svc:/system/kerberos/install:default
```

Cómo configurar Kerberos para que se ejecute en modo FIPS 140

Antes de empezar Para que Kerberos se ejecute en Modo FIPS 140, debe activar Modo FIPS 140 en su sistema. Consulte “Creación de un entorno de inicio con FIPS 140 activado ” de “Gestión de cifrado y certificados en Oracle Solaris 11.2 ”.

1. **Edite los tipos de cifrado para el KDC.**
   En la sección `[realms]` del archivo `kdc.conf`, defina el tipo de clave maestra para la base de datos del KDC:

   ```
   # pfedit  /etc/krb5/kdc.conf
   ...
   master_key_type = des3-cbc-sha1-kd
   ```

2. **En el mismo archivo, prohíba explícitamente otros tipos de cifrado.**
   Dado que también puede definir el cifrado al ejecutar un comando, los archivos de configuración deben impedir el uso de un argumento de algoritmo que no pertenece a FIPS 140 para un comando.

   ```
   supported_enctypes = des3-cbc-sha1-kd:normal
   ```

3. **Edite los tipos de cifrado para transacciones en la sección `[libdefaults]` del archivo `krb5.conf`.**
   Estos parámetros limitan los tipos de cifrado para los clientes, los servicios y los servidores Kerberos.

   ```
   # pfedit /etc/krb5/krb5.conf
          default_tgs_enctypes = des3-cbc-sha1-kd
          default_tkt_enctypes = des3-cbc-sha1-kd
          permitted_enctypes = des3-cbc-sha1-kd
   ```

4. **En el mismo archivo, prohíba explícitamente tipos de cifrado débiles.**

   ```
   allow_weak_enctypes = false
   ```

Errores más frecuentes Consulte “Tipos de cifrado Kerberos” [52].

Cómo utilizar `kdcmgr` para configurar el KDC maestro

La secuencia de comandos `kdcmgr` proporciona una interfaz de línea de comandos para instalar los KDC maestro y esclavos. Para el maestro, debe crear una contraseña para la base de datos

de Kerberos y una contraseña para el administrador. En los KDC esclavos, debe proporcionar estas contraseñas para terminar la instalación. Para obtener más información sobre estas contraseñas, consulte la página del comando man kdcmgr(1M).

Antes de empezar Debe asumir el rol root. Para obtener más información, consulte "Uso de sus derechos administrativos asignados" de "Protección de los usuarios y los procesos en Oracle Solaris 11.2 ".

1. **Cree el KDC maestro.**

   En la línea de comandos, ejecute el comando kdcmgr y designe administrador y el dominio. Se le solicita la contraseña de la base de datos Kerberos, llamada la *clave maestra* y la contraseña para el principal administrativo. La secuencia de comandos solicita las contraseñas.

```
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 strong password **/
Re-enter KDC database master key to verify: xxxxxxxx

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 strong password **/
Re-enter password for principal "kws/admin@EXAMPLE.COM": xxxxxxxx
Principal "kws/admin@EXAMPLE.COM" created.

Setting up /etc/krb5/kadm5.acl.

-------------------------------------------------
Setup COMPLETE.

kdc1#
```

   Nota - Guarde y almacene estas contraseñas en una ubicación segura.

2. **(Opcional) Muestre el estado del KDC maestro.**

```
# kdcmgr status
```

3. **Sincronice el reloj de este sistema con otros relojes en el dominio mediante NTP u otro mecanismo.**

Para que la autenticación se realice correctamente, cada reloj debe estar dentro de la hora predeterminada que está definida en la sección libdefaults del archivo krb5.conf. Para obtener más información, consulte la página del comando man krb5.conf(4). Para obtener información sobre el protocolo de hora de red (NTP), consulte “Sincronización de relojes entre clientes Kerberos y KDC” [128].

Nota - El KDC maestro no puede estar en el servidor NTP. Si no dispone de un servidor NTP, regrese al KDC maestro después de que el servidor NTP se haya instalado y convierta al KDC maestro en un cliente del servidor NTP.

---

ejemplo 4-1 Ejecución del comando kdcmgr sin argumentos

En este ejemplo, el administrador proporciona el nombre de dominio y el administrador principal cuando se lo solicita la secuencia de comandos.

```
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 strong password **/
Re-enter KDC database master key to verify: xxxxxxxx

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 strong password **/
Re-enter password for principal "kws/admin@EXAMPLE.COM": xxxxxxxx
Principal "kws/admin@EXAMPLE.COM" created.

Setting up /etc/krb5/kadm5.acl.

--------------------------------------------------
Setup COMPLETE.

kdc1#
```

▼ Cómo utilizar kdcmgr para configurar un KDC esclavo

Antes de empezar El servidor KDC maestro está configurado.

Debe asumir el rol root. Para obtener más información, consulte "Uso de sus derechos administrativos asignados" de "Protección de los usuarios y los procesos en Oracle Solaris 11.2 ".

1. **Cree un KDC esclavo.**

   En la línea de comandos, ejecute el comando kdcmgr y designe el administrador, el dominio y el KDC maestro.

   La secuencia de comandos solicita las dos contraseñas que creó en Cómo utilizar kdcmgr para configurar el KDC maestro [73], una para el principal administrativo y una para la base de datos del KDC.

```
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: xxxxxxxx

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: xxxxxxxx

-------------------------------------------------
Setup COMPLETE.

kdc2#
```

2. **(Opcional) Muestre el estado del KDC.**

```
# kdcmgr status
```

3. **Sincronice el reloj de este sistema con otros relojes en el dominio mediante NTP u otro mecanismo.**

Si no dispone de un servidor NTP, puede utilizar este sistema como servidor NTP.

Para que la autenticación se realice correctamente, cada reloj debe estar dentro de la hora predeterminada que está definida en la sección `libdefaults` del archivo `krb5.conf`. Para obtener más información, consulte la página del comando man `krb5.conf`(4). Para obtener información sobre el protocolo de hora de red (NTP), consulte “Sincronización de relojes entre clientes Kerberos y KDC” [128].

Pasos siguientes Regrese al KDC maestro después de que el servidor NTP esté instalado para que el KDC maestro sea cliente del servidor NTP.

▼ Cómo configurar manualmente un KDC maestro

En este procedimiento, 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`
- 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 apuntar a la ubicación de la ayuda en pantalla, como se describe en “Interfaz gráfica de usuario `gkadmin`” [152].

Antes de empezar El host está 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” [129].

Debe asumir el rol `root`. Para obtener más información, consulte “Uso de sus derechos administrativos asignados” de “Protección de los usuarios y los procesos en Oracle Solaris 11.2 ”.

1. **Instale el depósito de paquetes de KDC.**
   Siga las instrucciones en Cómo instalar el paquete KDC [72].

2. **Edite el archivo de configuración de Kerberos,`krb5.conf`.**
   Para obtener una descripción de este archivo, consulte la página del comando man `krb5.conf`(4).

En este ejemplo, el administrador cambia las líneas de `default_realm`, `kdc`, `admin_ servery` todas las entradas de `domain_realm`, y edita la entrada `help_url`.

```
kdc1 # pfedit /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
}
```

Nota - Si debe comunicarse con un sistema Kerberos anterior, es posible deba restringir los tipos de cifrado. Para obtener una descripción de los problemas relacionados con la restricción de los tipos de cifrado, consulte “Tipos de cifrado Kerberos” [52].

3. **Designe el dominio en el archivo de configuración de KDC, `kdc.conf`.**

   Para obtener una descripción de este archivo, consulte la página del comando man `kdc.conf`(4).

   En este ejemplo, además de la definición del nombre del dominio, el administrador cambia la propagación incremental y los valores predeterminados del registro.

```
kdc1 # pfedit /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
}
```

Nota - Si debe comunicarse con un sistema Kerberos anterior, es posible deba restringir los tipos de cifrado. Para obtener una descripción de los problemas relacionados con la restricción de los tipos de cifrado, consulte "Tipos de cifrado Kerberos" [52].

4. 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. Para obtener más información, consulte las páginas del comando man `kdb5_util`(1M), `kadmind`(1M) y `krb5kdc`(1M).

```
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 strong password **/
Re-enter KDC database master key to verify: xxxxxxxx
```

Sugerencia - Si este paso falla, verifique que el KDC principal se identifique por su FQDN.

```
# getent hosts IP-address-of-KDC
IP-address-of-KDC  kdc       /** This entry does not include FQDN **/
```

A continuación, agregue el FQDN como la primera entrada de KDC en el archivo `/etc/hosts`, por ejemplo:

IP-address-of-KDC **kdc.***kdc-principal***.example.com kdc**

5. 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 anterior da al principal `kws/admin` en el dominio `EXAMPLE.COM` la capacidad de modificar los principales y las políticas en el KDC. La entrada de principal predeterminada es un asterisco (*), lo que coincide con todos los `admin` de principales. Esta entrada puede representar un riesgo para la seguridad. Modifique el archivo para mostrar explícitamente cada `admin` de principal y sus derechos. Para obtener más información, consulte la página del comando man `kadm5.acl`(4).

6. 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 strong password **/
Re-enter password
for principal kws/admin@EXAMPLE.COM: xxxxxxxx
Principal "kws/admin@EXAMPLE.COM" created.
kadmin.local:
```

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

7. Inicie los daemons Kerberos.

```
kdc1 # svcadm enable -r network/security/krb5kdc
kdc1 # svcadm enable -r network/security/kadmin
```

8. Inicie `kadmin` y agregue más principales.

```
kdc1 # /usr/sbin/kadmin -p kws/admin
Enter password: xxxxxxxx
kadmin:
```

a. Cree el principal de `host` de 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 de red, 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 `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. Para obtener más información, consulte la página del comando man `kclient`(1M).

```
kadmin: addprinc clntconfig/admin
Enter password for principal clntconfig/admin@EXAMPLE.COM:      /** Type strong  password **/
Re-enter password for principal clntconfig/admin@EXAMPLE.COM: xxxxxxxx
Principal "clntconfig/admin@EXAMPLE.COM" created.
```

```
kadmin:
```

Nota - Guarde y almacene esta contraseña en una ubicación segura.

c. Agregue privilegios al principal `clntconfig/admin`.

Edite el archivo `kadm5.acl` para otorgar al principal `clntconfig` suficientes privilegios para realizar tareas de instalación de `kclient`.

```
# pfedit /etc/krb5/kadm5.acl
...
clntconfig/admin@EXAMPLE.COM  acdilm
```

d. 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 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.
kadmin:
```

e. Salga de `kadmin`.

```
kadmin: quit
```

9. Sincronice el reloj de este sistema con otros relojes en el dominio mediante NTP u otro mecanismo.

Para que la autenticación se realice correctamente, cada reloj debe estar dentro de la hora predeterminada que está definida en la sección `libdefaults` del archivo `krb5.conf`. Para obtener más información, consulte la página del comando man `krb5.conf`(4). Para obtener información sobre el protocolo de hora de red (NTP), consulte “Sincronización de relojes entre clientes Kerberos y KDC” [128].

Nota - El KDC maestro no puede estar en el servidor NTP. Si no dispone de un servidor NTP, regrese al KDC maestro después de que el servidor NTP se haya instalado y convierta al KDC maestro en un cliente del servidor NTP.

10. Configure los KDC esclavos.

Para proporcionar redundancia, asegúrese de instalar, al menos, un KDC esclavo. Siga las instrucciones en How Cómo utilizar `kdcmgr` para configurar un KDC esclavo [76] Cómo configurar manualmente un KDC esclavo [82]

▼ 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 está configurado. Si este esclavo se va a intercambiar, siga las instrucciones en Cómo intercambiar un KDC maestro y un KDC esclavo [130].

Debe asumir el rol `root` en el servidor KDC. Para obtener más información, consulte "Uso de sus derechos administrativos asignados" de "Protección de los usuarios y los procesos en Oracle Solaris 11.2 ".

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: xxxxxxxx
   kadmin:
   ```

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

   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 para la propagación incremental.

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. Para obtener una descripción de este archivo, consulte la página del comando man `krb5.conf`(4).

```
kdc1 # pfedit /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 # pfedit /etc/krb5/kadm5.acl
*/admin@EXAMPLE.COM *
kiprop/kdc2.example.com@EXAMPLE.COM p
```

4. En el KDC maestro, reinicie el servicio `kadmind` para utilizar las nuevas entradas en el archivo `kadm5.acl`.

```
kdc1 # svcadm restart network/security/kadmin
```

5. En todos los KDC esclavos, copie los archivos de administración KDC del servidor KDC maestro.

Cada KDC esclavo debe tener información actualizada sobre el servidor KDC maestro. Puede utilizar `sftp` o un mecanismo de transferencia similar para obtener 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.acl`.**

   Esta información se debe actualizar en todos los servidores KDC esclavos.

   ```
   kdc2 # pfedit /etc/krb5/kpropd.acl
   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.acl`, no esté relleno.**

   Un archivo `kadm5.acl` sin modificaciones sería el siguiente ejemplo:

   ```
   kdc2 # pfedit /etc/krb5/kadm5.acl
   */admin@___default_realm___ *
   ```

   Si el archivo tiene entradas `kiprop`, elimínelas.

8. **En el nuevo esclavo, defina el intervalo de sondeo en el archivo `kdc.conf`.**

   Reemplace la entrada `sunw_dbprop_master_ulogsize` por una entrada que defina el intervalo de sondeo del esclavo. La siguiente entrada establece el tiempo de sondeo en dos minutos.

   ```
   kdc1 # pfedit /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
   }
   ```

9. **En el nuevo esclavo, inicie el comando `kadmin`.**

   Inicie 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: xxxxxxxx
   kadmin:
   ```

   a. **Agregue el principal del esclavo al archivo keytab del esclavo mediante `kadmin`.**

Esta entrada permite que el comando `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. Para obtener más información, consulte la página del comando man `kprop`(1M).

```
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.
kadmin:
```

b. Agregue el principal `kiprop` al archivo keytab del KDC esclavo.

La agregación 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.
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 el comando `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: xxxxxxxx
```

Para obtener más información, consulte la página del comando man `kdb5_util`(1M).

12. Sincronice el reloj de este sistema con otros relojes en el dominio mediante NTP u otro mecanismo.

Para que la autenticación se realice correctamente, cada reloj debe estar dentro de la hora predeterminada que está definida en la sección `libdefaults` del archivo `krb5.conf`. Para obtener más información, consulte la página del comando man `krb5.conf`(4). Para obtener información sobre el protocolo de hora de red (NTP), consulte “Sincronización de relojes entre clientes Kerberos y KDC” [128].

13. **En el nuevo esclavo, inicie el daemon del KDC.**

```
kdc2 # svcadm enable network/security/krb5kdc
```

Pasos siguientes Regrese al KDC maestro después de que el servidor NTP esté instalado para que el KDC maestro sea cliente del servidor NTP.

▼ Cómo configurar el KDC maestro para utilizar un servidor de directorios LDAP

Este procedimiento utiliza 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 apuntar a la ubicación de la ayuda en pantalla, como se describe en “Interfaz gráfica de usuario `gkadmin`” [152].

Antes de empezar El host está 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 con Oracle Directory Server Enterprise Edition. Para obtener más información, consulte Oracle Identity Management - Documentation.

Debe asumir el rol `root` en el servidor KDC. Para obtener más información, consulte “Uso de sus derechos administrativos asignados” de “Protección de los usuarios y los procesos en Oracle Solaris 11.2 ”.

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.

   a. **En el servidor de directorios, exporte el certificado 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.cert.der \
   label=defaultCert dir=/var/ldap
   ```

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

   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.

   ```
   master# /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` debe 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 de LDAP.**

   ```
   # 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_kadmind_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 una clave maestra `/var/krb5/.k5.EXAMPLE.COM` y un archivo intermedio para la clave. Para obtener información sobre las opciones del comando, consulte la página del comando man `kdb5_ldap_util`(1M).

```
# kdb5_ldap_util -D "cn=directory manager" create
   -P master-key -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 servidor de directorios. El KDC utiliza diferentes roles según el tipo de acceso que el KDC está utilizando.

```
# kdb5_ldap_util stashsrvpw "cn=kdc service,ou=profile,dc=example,dc=com"
# kdb5_ldap_util stashsrvpw "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: xxxxxxxx

dn: cn=kadmin service,ou=profile,dc=example,dc=com
cn: kadmin service
sn: kadmin service
objectclass: top
objectclass: person
userpassword: xxxxxxxx
```

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 `kadmin`.**

```
# 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`.**

Debe asignar un nombre a los dominios y los servidores. Para obtener una descripción de este archivo, consulte la página del comando man `krb5.conf`(4).

```
kdc1 # pfedit /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
}
```

Nota - Ajuste la dirección URL para apuntar a la ubicación de la ayuda en pantalla, como se describe en “Interfaz gráfica de usuario gkadmin” [152].

En este ejemplo, se modificaron las líneas para las entradas `default_realm` , `kdc`, `admin_server` y `domain_realm`. Además, la dirección URL de ayuda en pantalla se ha cambiado.

Nota - Si debe comunicarse con un sistema Kerberos anterior, es posible deba restringir los tipos de cifrado. Para obtener una descripción de los problemas relacionados con la restricción de los tipos de cifrado, consulte “Tipos de cifrado Kerberos” [52].

9. **Edite el archivo de configuración de KDC, `kdc.conf`.**

   Necesita designar el nombre del dominio. Para obtener una descripción de este archivo, consulte la página del comando man `kdc.conf`(4).

   En este ejemplo, además de la definición del nombre del dominio, el administrador cambia la propagación incremental y los valores predeterminados del registro.

```
kdc1 # pfedit /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
}
```

   Nota - Si debe comunicarse con un sistema Kerberos anterior, es posible deba restringir los tipos de cifrado. Para obtener una descripción de los problemas relacionados con la restricción de los tipos de cifrado, consulte “Tipos de cifrado Kerberos” [52].

10. **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 anterior da al principal `kws/admin` en el dominio `EXAMPLE.COM` la capacidad de modificar los principales y las políticas en el KDC. La entrada de principal predeterminada

es un asterisco (*), lo que coincide con todos los `admin` de principales. Esta entrada puede representar un riesgo para la seguridad. Modifique el archivo para mostrar explícitamente cada `admin` de principal y sus derechos. Para obtener más información, consulte la página del comando man `kadm5.acl`(4).

11. Inicie el comando `kadmin.local` y crear los principales `admin`.

```
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 crear, al menos, un principal `admin` para completar el proceso de configuración del KDC. Para este ejemplo, se crea el 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 strong password **/
Re-enter password for principal kws/admin@EXAMPLE.COM: xxxxxxxx
Principal "kws/admin@EXAMPLE.COM" created.
kadmin.local:
```

b. Salga de `kadmin.local`.

```
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 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 `kadmin`.

```
# svccfg -s security/kadmin
svc:/network/security/kadmin> addpg dsins1 dependency
svc:/network/security/kadmin> setprop dsins1/entities =\
fmri: "svc:/application/sun/ds:ds--var-opt-SUNWdsee-dsins1"
svc:/network/security/kadmin> setprop dsins1/grouping = astring: "require_all"
```

```
svc:/network/security/kadmin> setprop dsins1/restart_on = astring: "restart"
svc:/network/security/kadmin> setprop dsins1/type = astring: "service"
svc:/network/security/kadmin> exit
```

13. **Complete la configuración de Kerberos en LDAP mediante la realización de Paso 7 a Paso 9 en Cómo configurar manualmente un KDC maestro [77].**

14. **Configure los KDC esclavos.**

    Para proporcionar redundancia, asegúrese de instalar, al menos, un KDC esclavo. Para obtener instrucciones, consulte Cómo configurar manualmente un KDC esclavo [82].

Sustitución de las claves del servicio de otorgamiento de tickets en un servidor maestro

Nota - Sustituya las claves cuando desee utilizar un nuevo tipo de cifrado más seguro para todas las claves de sesión.

Cuando el principal del servicio de otorgamiento de tickets (TGS) sólo tiene una clave DES, la clave restringe el tipo de cifrado de la clave de sesión del ticket de otorgamiento de tickets (TGT) a DES. Cuando el KDC se actualiza a una versión que admite tipos de cifrado más seguros, debe sustituir la clave DES del principal TGS para que el principal pueda generar un cifrado más potente para todas las claves de sesión.

Puede sustituir la clave de forma remota o en el servidor maestro. Debe ser un principal `admin` que tenga asignado el privilegio `changepw`.

- Para sustituir la clave del principal del servicio TGS desde cualquier sistema Kerberos, utilice el comando `kadmin`.

  ```
  kdc1 % /usr/sbin/kadmin -p kws/admin
  Enter password: xxxxxxxx
  kadmin: cpw -randkey krbtgt/EXAMPLE.COM@EXAMPLE.COM
  Enter TGS key: xxxxxxxx
  Enter new TGS key:      /** Type strong password **/
  Re-enter TGS key to verify: xxxxxxxx
  ```

  `cpw` es un alias para el comando `change_password`. La opción `-randkey` solicita la nueva contraseña.

- Si ha iniciado sesión en el KDC maestro como `root`, puede utilizar el comando `kadmin.local`. Se le pedirá que introduzca la nueva contraseña de base de datos.

  ```
  kdc1 # kadmin.local -q 'cpw -randkey krbtgt/EXAMPLE.COM@EXAMPLE.COM'
  ```

Nota - Guarde y almacene esta contraseña en una ubicación segura.

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. Algunas tareas nuevas son específicas para trabajar con LDAP.

TABLA 4-4 Mapa de tareas de la configuración de servidores KDC para utilizar LDAP

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 con el KDC.	Cómo configurar el KDC maestro para utilizar un servidor de directorios LDAP [86]
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.	Cómo mezclar atributos de principales de Kerberos en un tipo de clase de objeto que no es de Kerberos [93]
Destruir un dominio.	Elimina todos los datos asociados con un dominio.	Cómo destruir un dominio en un servidor de directorios LDAP [94]

▼ Cómo mezclar atributos de principales de Kerberos en un tipo de clase de objeto que no es de Kerberos

En este procedimiento, los atributos `krbprincipalaux`, `krbTicketPolicyAux` y `krbPrincipalName` están asociados con la clase de objeto de personas.

Este procedimiento utiliza los siguientes parámetros de configuración:

- Servidor de directorios = `dsserver.example.com`
- Principal de usuario = `mre@EXAMPLE.COM`

Antes de empezar Debe asumir el rol `root`. Para obtener más información, consulte "Uso de sus derechos administrativos asignados" de "Protección de los usuarios y los procesos en Oracle Solaris 11.2 ".

1. Prepare cada entrada en la clase de objeto de personas.

En el servidor de directorios, repita este paso para cada entrada.

```
cat << EOF | ldapmodify -h dsserver.example.com -D "cn=directory manager"
dn: uid=mre,ou=people,dc=example,dc=com
changetype: modify
objectClass: krbprincipalaux
objectClass: krbTicketPolicyAux
krbPrincipalName: mre@EXAMPLE.COM
```

```
EOF
```

2. **Agregue un atributo de subárbol al contenedor del dominio.**

   Este ejemplo 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 mre'
```

▼ 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 “Uso de sus derechos administrativos asignados” de “Protección de los usuarios y los procesos en Oracle Solaris 11.2 ”.

- **Destruya el dominio.**

```
# kdb5_ldap_util -D "cn=directory manager" destroy
```

Configuración de clientes Kerberos

Los clientes Kerberos incluyen cualquier host en la red que no es un servidor KDC y que necesita utilizar servicios Kerberos. Esta sección proporciona procedimientos para instalar un

cliente Kerberos, así como información sobre el uso de la autenticación de `root` para montar sistemas de archivos NFS.

Las opciones de configuración de cliente son similares a las opciones del servidor, con la agregación de Automated Installer (AI):

- AI: se recomienda para la instalación fácil y rápida de múltiples clientes Kerberos
- Automático: se recomienda para secuencias de comandos
- Interactivo: suficiente para la mayoría de las instalaciones
- Manual: necesario para instalaciones más complejas

En el siguiente mapa de tareas, se describen las tareas que se tratan en esta sección.

TABLA 4-5 Mapa de tareas de la configuración de clientes Kerberos

Tarea	Descripción	Para obtener instrucciones
Instalar clientes con Automated Installer (AI).	Adecuado cuando desea que el cliente Kerberos se configure durante la instalación del sistema.	"Cómo configurar clientes Kerberos mediante AI" de "Instalación de sistemas Oracle Solaris 11.2 "
Crear un perfil de instalación para los clientes Kerberos similares.	Crea un perfil de instalación de cliente reutilizable.	Cómo crear un perfil de instalación de cliente Kerberos [95]
Instalar clientes con una secuencia de comandos.	Adecuado cuando los parámetros de instalación para cada cliente son los mismos.	Cómo configurar automáticamente un cliente Kerberos [96]
Instalar clientes mediante la respuesta a preguntas.	Adecuado si sólo algunos de los parámetros de instalación deben cambiarse.	Cómo configurar interactivamente un cliente Kerberos [98]
Instalar clientes de forma manual.	Adecuado si la instalación de cada cliente requiere parámetros de instalación únicos.	Cómo configurar manualmente un cliente Kerberos [101]
Unirse a un cliente Kerberos para un servidor de Active Directory.	Instala automáticamente un cliente Kerberos de un servidor de Active Directory.	Cómo unir un cliente Kerberos a un servidor de Active Directory [100]
Desactivar la verificación del KDC que ha emitido un ticket de otorgamiento de tickets (TGT) de cliente.	Perfecciona la verificación de KDC cuando los clientes Kerberos no tienen un principal de host almacenado en el archivo keytab local.	"Cómo desactivar la verificación del ticket de otorgamiento de tickets" [107]
Permitir que un cliente acceda a un sistema de archivos NFS como el usuario `root`.	Permite al cliente montar un sistema de archivos NFS con acceso `root`. Además, permite al cliente acceder al sistema de archivos NFS para que se puedan ejecutar trabajos cron.	Cómo acceder a un sistema de archivos NFS protegido con Kerberos como el usuario `root` [108]

▼ 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, se reducen las probabilidades de errores de escritura. Asimismo, el uso del perfil reduce la intervención del usuario, en comparación con el proceso interactivo.

Nota - Para crear sistemas que se inician como clientes Kerberos completamente configurados, consulte “Configuración de la seguridad” en “Instalación de Sistemas Oracle Solaris 11.2”.

Antes de empezar Debe asumir el rol `root`. Para obtener más información, consulte “Uso de sus derechos administrativos asignados” de “Protección de los usuarios y los procesos en Oracle Solaris 11.2 ”.

1. **Cree un perfil de instalación `kclient`.**

   A continuación, se muestra un ejemplo del perfil `kclient`:

```
client# pfedit kcprofile
REALM EXAMPLE.COM
KDC kdc1.example.com
ADMIN clntconfig
FILEPATH /net/denver.example.com/export/install/krb5.conf
NFS 1
DNSLOOKUP none
```

2. **Proteja el archivo y almacénelo para que lo utilicen otros clientes.**

```
client# cp kcprofile /net/denver.example.com/export/install
denver# chown root kcprofile; chmod 644 kcprofile
```

▼ Cómo configurar automáticamente un cliente Kerberos

Antes de empezar Debe asumir el rol `root`. Para obtener más información, consulte “Uso de sus derechos administrativos asignados” de “Protección de los usuarios y los procesos en Oracle Solaris 11.2 ”.

1. **Cree un perfil kclient.**

   Utilice el perfil de instalación de Cómo crear un perfil de instalación de cliente Kerberos [95].

2. **Ejecute el comando `kclient` con un argumento de perfil.**

   Debe proporcionar la contraseña para el principal `clntconfig` con el fin de completar el proceso. Creó esta contraseña cuando configuró el KDC maestro en “Configuración de servidores KDC” [71]. Para obtener más información, consulte la página del comando man `kclient`(1M).

```
client# /usr/sbin/kclient -p /net/denver.example.com/export/install/kcprofile
```

```
Starting client setup
-------------------------------------------------

kdc1.example.com

Setting up /etc/krb5/krb5.conf.

Obtaining TGT for clntconfig/admin ...
Password for clntconfig/admin@EXAMPLE.COM: xxxxxxxx

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 4-2 Uso de un perfil de instalación para configurar un cliente Kerberos

El ejemplo siguiente utiliza el perfil de cliente `kcprofile` y dos sustituciones de línea de comandos para configurar el cliente.

```
# /usr/sbin/kclient -p /net/denver.example.com/export/install/kcprofile \
-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:  xxxxxxxx

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. Si el cliente se unirá a un servidor Active Directory, vaya a Cómo unir un cliente Kerberos a un servidor de Active Directory [100].

Antes de empezar Debe asumir el rol `root`. Para obtener más información, consulte “Uso de sus derechos administrativos asignados” de “Protección de los usuarios y los procesos en Oracle Solaris 11.2 ”.

1. **Ejecute el comando `kclient` sin argumentos.**

   ```
   client# /usr/sbin/kclient
   ```

   La secuencia de comandos le solicita 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 autentificación Kerberos

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

2. **Si el servidor KDC no ejecuta una versión Oracle Solaris, responda `y` y defina el tipo de servidor que está ejecutando el KDC.**

   Para obtener la lista de servidores disponibles, consulte la opción `-T` en la página del comando man `kclient`(1M).

3. **Si se debe utilizar DNS para las consultas de Kerberos, responda `y` e indique la opción de búsqueda de DNS que se debe utilizar.**

   Las opciones válidas son `dns_lookup_kdc`, `dns_lookup_realm` y `dns_fallback`. Para obtener más información sobre estos valores, consulte la página del comando man `krb5.conf`(4).

4. **Defina el nombre del dominio Kerberos y el nombre de host de KDC maestro.**

   Esta información se ha agregado al archivo de configuración `/etc/krb5/krb5.conf`.

5. **Si KDC esclavos se encuentran en el dominio, responda `y` y proporcione los nombres de host del KDC esclavo.**

   Esta información se utiliza para crear entradas KDC adicionales en el archivo de configuración del cliente.

6. **Si el servicio o las claves de host son necesarios, responda `y`.**

   Normalmente, el servicio o las claves de host no son necesarios, a menos que el sistema cliente aloje servicios kerberizados.

7. **Si el cliente es un miembro de un clúster, responda `y` y proporcione 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.

8. **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.

9. **Especifique si el cliente utilizará NFS Kerberizado.**

   Las claves de servicio NFS se deben crear si el cliente alojará servicios NFS mediante Kerberos.

10. **Indique si se debe crear una nueva política del PAM.**

    Para definir qué servicios del PAM utiliza Kerberos para la autenticación, se proporciona el nombre del servicio y un indicador que especifica 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

    Para obtener información acerca de los servicios del PAM proporcionados para Kerberos, consulte los archivos en `/etc/security/pam_policy`.

11. **Especifique 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 4-3 Ejecución de ejemplo de la secuencia de comandos `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 host name 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: corphdqtrs.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.
```

▼ Cómo unir un cliente Kerberos a un servidor de Active Directory

Este procedimiento utiliza el comando `kclient` sin un perfil de instalación.

Antes de empezar Debe asumir el rol `root`. Para obtener más información, consulte “Uso de sus derechos administrativos asignados” de “Protección de los usuarios y los procesos en Oracle Solaris 11.2 ”.

1. **(Opcional) Active la creación de registros de recursos DNS para el cliente.**

   ```
   client# sharectl set -p ddns_enable=true smb
   ```

2. **Ejecute el comando `kclient`.**

   La siguiente salida muestra un ejemplo de resultado de la ejecución del comando `kclient` para unir el cliente al dominio AD, `EXAMPLE.COM`.

La opción -T selecciona un tipo de servidor KDC, en este caso, un tipo de servidor Active Directory (AD) de Microsoft. De manera predeterminada, debe proporcionar la contraseña del principal de administrador del servidor AD.

```
client# /usr/sbin/kclient -T ms_ad
Starting client setup
-----------------------------------------------

Attempting to join 'CLIENT' to the 'EXAMPLE.COM' domain.
Password for Administrator@EXAMPLE.COM: xxxxxxxx
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.
#
```

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

▼ Cómo configurar manualmente un cliente Kerberos

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`
- 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`

Antes de empezar Debe asumir el rol `root`. Para obtener más información, consulte “Uso de sus derechos administrativos asignados” de “Protección de los usuarios y los procesos en Oracle Solaris 11.2 ”.

1. **Edite el archivo de configuración de Kerberos, `krb5.conf`.**

Cambie los nombres del dominio y los nombres del servidor en el archivo de configuración de Kerberos. También puede especificar la ruta de acceso a los archivos de ayuda para `gkadmin`.

```
kdc1 # pfedit /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://www.example.com/doclib/OSMKA/aadmin-23.html
```

Nota - Si debe comunicarse con un sistema Kerberos anterior, es posible deba restringir los tipos de cifrado. Para obtener una descripción de los problemas relacionados con la restricción de los tipos de cifrado, consulte “Tipos de cifrado Kerberos” [52].

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`.
   - 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`. Para obtener más información, consulte `krb5.conf`(4). 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.
- 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`. Para obtener más información, consulte la página del comando man `krb5.conf`(4). Tenga en cuenta que las referencias siempre se intentan en primer lugar.

4. Sincronice el reloj del cliente con el reloj del KDC maestro mediante NTP u otro mecanismo de sincronización de relojes.

Para que la autenticación se realice correctamente, 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 obtener más información, consulte la página del comando man `krb5.conf`(4). Para obtener información sobre el protocolo de hora de red (NTP), consulte “Sincronización de relojes entre clientes Kerberos y KDC” [128].

5. Cree principales de Kerberos.

```
denver # /usr/sbin/kadmin -p kws/admin
Enter password: xxxxxxxx
kadmin:
```

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

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 strong password **/
Re-enter password for principal mre@EXAMPLE.COM: xxxxxxxx
kadmin:
```

b. (Opcional) Cree un principal `root` y agregue el principal al archivo keytab del servidor.

Nota - Si el cliente no requiere acceso `root` a un sistema de archivos montados en NFS remoto, puede omitir este paso.

Si se necesita acceso `root` no interactivo, como la ejecución de trabajos cron como `root`, realice este paso.

El principal de `root` debe ser un principal de dos componentes. El segundo componente debe ser el nombre de host del sistema cliente Kerberos para evitar la creación de un principal `root` de todo el dominio. 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.
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.
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.
kadmin:
```

e. Salga de `kadmin`.

```
kadmin: quit
```

6. (Opcional) Active Kerberos con NFS.

a. Active los modos de seguridad de Kerberos en el archivo `/etc/nfssec.conf`.

En el archivo `/etc/nfssec.conf`, elimine el símbolo "#" que comenta los modos de seguridad de Kerberos.

```
# pfedit /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. Para obtener más información, consulte la página del comando man `resolv.conf`(4).

```
# svcadm enable network/dns/client:default
```

c. Reinicie el servicio `gss`.

```
# svcadm restart network/rpc/gss
```

7. (Opcional) 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`.

Para obtener más información, consulte la página del comando man `warn.conf`(4) y "Renovación automática de todos los tickets de otorgamiento de tickets" [113].

ejemplo 4-4 Configuración de un cliente Oracle Solaris para que funcione con varios KDC maestros

El servicio Kerberos de Active Directory (AD) de Microsoft, proporciona un KDC que se ejecuta en varios servidores maestros. Para que un cliente Oracle Solaris actualice información, la declaración `admin_server` o `kpasswd_server` en el archivo `/etc/krb5/krb5.conf` debe enumerar todos los servidores. En este ejemplo, se muestra cómo permitir al cliente actualizar información sobre el KDC que `kdc1` y `kdc2` comparten.

```
[realms]
EXAMPLE.COM = {
```

```
kdc = kdc1.example.com
kdc = kdc2.example.com
admin_server = kdc1.example.com
admin_server = kdc2.example.com
}
```

ejemplo 4-5 Configuración de un cliente Kerberos para un KDC que no es Oracle Solaris

Es posible configurar un cliente Kerberos para que funcione con un KDC no Oracle Solaris, mediante la agregación de 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. En el fragmento siguiente, se muestra 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 4-6 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 4-7 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 0 464 kdc1.example.com
_kpasswd._udp.EXAMPLE.COM           IN      SRV 0 0 464 kdc1.example.com
```

Cómo desactivar la verificación del ticket de otorgamiento de tickets

De manera predeterminada, Kerberos comprueba que el KDC del principal del host que está 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, `verify_ap_req_nofail`, evita ataques de falsificación de DNS.

Sin embargo, esta comprobación debe estar desactivada para las configuraciones de cliente donde el principal del host no está disponible. Las siguientes configuraciones requieren que esta comprobación esté desactivada:

- A la dirección IP del cliente se le 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.

Para desactivar la verificación TGT, establezca la opción `verify_ap_req_nofail` en `false` en el archivo `krb5.conf`. La opción `verify_ap_req_nofail` se puede introducir en la sección `[libdefaults]` o `[realms]` del archivo `krb5.conf`. En la sección `[libdefaults]`, este valor se utiliza para todos los dominios:

```
client # pfedit /etc/krb5/krb5.conf
[libdefaults]
default_realm = EXAMPLE.COM
verify_ap_req_nofail = false
...
```

Si la opción está en la sección `[realms]`, el valor sólo se aplica al dominio definido. Para obtener más información sobre esta opción, consulte la página del comando man `krb5.conf`(4).

▼ 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 se comparte con opciones como: -o sec=krb5,root=client1.example.com.

1. **Ejecute el comando kadmin.**

```
denver # /usr/sbin/kadmin -p kws/admin
Enter password: xxxxxxxx
kadmin:
```

2. **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 de root debe ser un principal de dos componentes. El segundo componente debe ser el nombre de host del sistema cliente Kerberos para evitar la creación de un principal raíz 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:
```

3. **Agregue el principal root al archivo keytab del servidor.**

Este paso es necesario para que el cliente tenga acceso root a sistemas de archivos montados mediante el servicio NFS. Este paso también es necesario para el 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.
kadmin:
```

4. **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 mediante PAM. Personaliza archivos de configuración del PAM por sistema en el servidor de migración y el servidor maestro para controlar el reconocimiento de credenciales UNIX y la nueva autenticación en el dominio Kerberos.

Para obtener información sobre PAM, consulte Capítulo 1, Uso de módulos de autenticación conectables y la página del comando man `pam.conf`(4).

En este procedimiento, los nombres del servicio de inicio de sesión se configuran para usar la migración automática. Este ejemplo utiliza 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 Debe asumir el rol `root`. Para obtener más información, consulte "Uso de sus derechos administrativos asignados" de "Protección de los usuarios y los procesos en Oracle Solaris 11.2 ".

1. **Asegúrese de que 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
   ...
   ```

   Para obtener información sobre las opciones del comando, consulte la página del comando man `klist`(1).

2. **Si `server1` no aparece, configúrelo como un cliente Kerberos del dominio `EXAMPLE.COM`.**

   Para conocer los pasos, consulte los ejemplos en "Configuración de clientes Kerberos" [94].

3. **Modifique la política del PAM para `server1`.**

   Para obtener más información, consulte "Asignación de una política del PAM por usuario" [20].

   a. **Determine qué política de Kerberos está en uso en `server1`.**

```
% grep PAM_POLICY /etc/security/policy.conf
# PAM_POLICY specifies the system-wide PAM policy (see pam_user_policy(5))
...
PAM_POLICY=krb5_first
```

b. Copie ese archivo de política del PAM y, a continuación, modifique el archivo de la nueva política que desea agregar al módulo `pam_krb5_migrate.so.1` para cada pila de autenticación.

```
server1 # cd /etc/security/pam_policy/; cp krb5_first krb5_firstmigrate
server1 # pfedit /etc/security/pam_policy/krb5_firstmigrate.
# login service (explicit because of pam_dial_auth)
#
login auth requisite    pam_authtok_get.so.1
...
login auth required  pam_unix_auth.so.1
login    auth optional  pam_krb5_migrate.so.1
#
# rlogin service (explicit because of pam_rhost_auth)
#
rlogin auth sufficient  pam_rhosts_auth.so.1
...
rlogin auth required    pam_unix_auth.so.1
rlogin   auth optional        pam_krb5_migrate.so.1
#
# Kerberized rlogin service
#
krlogin auth required  pam_unix_cred.so.1
krlogin auth required  pam_krb5.so.1
krlogin auth optional  pam_krb5_migrate.so.1
#
# rsh service (explicit because of pam_rhost_auth)
#
rsh auth sufficient  pam_rhosts_auth.so.1
rsh auth required    pam_unix_cred.so.1
rsh auth optional    pam_krb5_migrate.so.1
#
# Kerberized rsh service
#
krsh auth required  pam_unix_cred.so.1
krsh auth required  pam_krb5.so.1
krsh auth optional  pam_krb5_migrate.so.1
#
# Kerberized telnet service
#
ktelnet auth required  pam_unix_cred.so.1
ktelnet auth required  pam_krb5.so.1
ktelnet auth optional  pam_krb5_migrate.so.1
#
# PPP service (explicit because of pam_dial_auth)
#
ppp auth requisite    pam_authtok_get.so.1
```

```
...
ppp auth required  pam_unix_auth.so.1
ppp auth optional  pam_krb5_migrate.so.1
#
# GDM Autologin (explicit because of pam_allow).  These need to be
# here as there is no mechanism for packages to amend pam.conf as
# they are installed.
#
gdm-autologin auth  required    pam_unix_cred.so.1
gdm-autologin auth  sufficient  pam_allow.so.1
gdm-autologin auth optional    pam_krb5_migrate.so.1
#
# Default definitions for Authentication management
# Used when service name is not explicitly mentioned for authentication
#
OTHER auth requisite    pam_authtok_get.so.1
...
OTHER auth required  pam_unix_auth.so.1
OTHER auth optional  pam_krb5_migrate.so.1
#
# passwd command (explicit because of a different authentication module)
#
passwd auth required  pam_passwd_auth.so.1
#
# cron service (explicit because of non-usage of pam_roles.so.1)
#
cron account required pam_unix_account.so.1
#
# cups service (explicit because of non-usage of pam_roles.so.1)
#
cups account required pam_unix_account.so.1
#
# GDM Autologin (explicit because of pam_allow) This needs to be here
# as there is no mechanism for packages to amend pam.conf as they are
# installed.
#modified
gdm-autologin account  sufficient  pam_allow.so.1
#
.
.
.
```

c. (Opcional) Fuerce un cambio inmediato de contraseña.

Para las cuentas de Kerberos recientemente creadas, establezca el tiempo de caducidad de la contraseña a la hora actual agregando la opción `expire_pw` a las entradas `pam_krb5_migrate`. Para obtener más información, consulte la página del comando man `pam_krb5_migrate`(5).

```
service-name auth optional     pam_krb5_migrate.so.1 expire_pw
```

d. En este archivo de configuración, modifique la pila de cuentas `OTHER` para bloquear el acceso si la contraseña de Kerberos ha caducado.

```
# Definition for Account management
# Used when service name is not explicitly mentioned for account management
# Re-ordered pam_krb5 causes password expiration in Kerberos to block access
#
OTHER account requisite   pam_roles.so.1
OTHER account required pam_krb5.so.1
OTHER account required pam_unix_account.so.1
OTHER account required pam_tsol_account.so.1
# OTHER account required pam_krb5.so.1
#
.
.
.
```

e. Cambie la entrada `PAM_POLICY` en el archivo `policy.conf` para utilizar el archivo de configuración modificado.

```
server1 # pfedit /etc/security/policy.conf
...
# PAM_POLICY=krb5_first
PAM_POLICY=krb5_firstmigrate
```

Para obtener más información, lea el archivo `policy.conf`.

4. En el KDC maestro, actualice el archivo de control de acceso `kadm5.acl`.

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`. Use el privilegio `U` para enumerar los usuarios que no se deben migrar. Estas entradas deben preceder a la entrada `ui` o permitir todo. Para obtener más información, consulte la página del comando man `kadm5.acl`(4).

```
kdc1 # pfedit /etc/krb5/kadm5.acl
host/server1.example.com@EXAMPLE.COM U root
host/server1.example.com@EXAMPLE.COM ui *
*/admin@EXAMPLE.COM *
```

5. En el KDC maestro, active el daemon `kadmind` para usar el servicio del PAM `k5migrate`.

Si un archivo de servicio `k5migrate` no está en el directorio `/etc/pam.d`, agregue el archivo de servicio al directorio. Para obtener más información, consulte la página del comando man `pam.d`(4).

Esta modificación permite la validación de contraseñas de usuario de UNIX para las cuentas que necesitan migración.

```
kdc1 # pfedit /etc/pam.d/k5migrate
...
# Permits validation of migrated UNIX accounts
auth    required        pam_unix_auth.so.1
account required        pam_unix_account.so.1
```

Nota - `k5migrate` es el nombre de un servicio del PAM. El archivo debe tener el nombre `k5migrate`.

6. **Compruebe la configuración antes de ponerla en producción.**

   - **Como usuario común, pruebe cada servicio del PAM modificado.**
   - **Como usuario `root`, pruebe cada servicio del PAM modificado.**
   - **Fuerce un cambio de contraseña y, a continuación, pruebe los servicios del PAM modificados.**

Renovación automática de todos los tickets de otorgamiento de tickets

Para facilitar la administración, puede configurar la renovación de tickets y mensajes de advertencia sobre la caducidad del ticket de otorgamiento de tickets (TGT). Los administradores pueden definir advertencias para todos los usuarios, y los usuarios pueden personalizar sus propias advertencias. Para obtener más información, consulte las páginas del comando man `warn.conf`(4) y `ktkt_warnd`(1M).

Nota - El servicio `ktkt_warn` está desactivado de manera predeterminada. Para activar el servicio en los clientes Kerberos existentes, ejecute el comando `svcadm enable ktkt_warn`.

EJEMPLO 4-8 Configuración de mensajes de caducidad de TGT para todos los usuarios

Este ejemplo muestra varias formas de configurar la renovación y el sistema de mensajes para TGT.

```
# pfedit /etc/krb5/warn.conf
##
## renew the TGT 30 minutes before expiration and send message to users terminal
##
mre@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 -
```

Después de configurar los mensajes, ejecute el comando `kclient` en los nuevos clientes.

```
client# /usr/sbin/kclient -p /net/denver.example.com/export/install/kcprofile
```

En los clientes existentes, active el servicio.

```
# svcadm enable network/security/ktkt_warn
```

EJEMPLO 4-9 Configuración de mensajes de caducidad de TGT para un usuario

Cada usuario puede configurar un archivo de configuración `warnd` individual, que se denomina `/var/user/`*$USER*`/krb-warn.conf`. La existencia de este archivo impide que el archivo del administrador se lea.

```
% pfedit /var/user/mre/krb-warn.conf
mre@EXAMPLE.COM renew:log mail 25m &
```

El TGT se renueva 25 minutos antes de la caducidad, la renovación se registra y se envía correo electrónico al usuario `mre` de Kerberos en ese momento.

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 activar la versión de Kerberos de estas aplicaciones 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 El KDC maestro está configurado. Los relojes se sincronizan, como se describe en “Sincronización de relojes entre clientes Kerberos y KDC” [128]. Para probar completamente el proceso, necesita varios clientes.

Debe asumir el rol `root` en el servidor de aplicación. Para obtener más información, consulte “Uso de sus derechos administrativos asignados” de “Protección de los usuarios y los procesos en Oracle Solaris 11.2 ”.

1. **Determine si un principal de host existe para el nuevo 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 devuelve un principal, ha terminado. Si no devuelve un principal, cree nuevos principales mediante los siguientes pasos.

2. **Inicie sesión en el servidor con uno de los nombres de principales `admin` que creó cuando configuró el KDC maestro.**

   ```
   boston # /usr/sbin/kadmin -p kws/admin
   Enter password: xxxxxxxx
   kadmin:
   ```

3. **Cree el principal `host` del servidor.**

   ```
   kadmin: addprinc -randkey host/boston.example.com
   Principal "host/boston.example.com" created.
   kadmin:
   ```

   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`. Esta capacidad 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 mediante el formulario FQDN del nombre de host.

4. **Agregue el principal `host` del servidor al archivo keytab del servidor.**

   Si el comando `kadmin` no se está ejecutando, reinícielo 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.
kadmin:
```

5. **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 de red de 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 “Uso de sus derechos administrativos asignados” de “Protección de los usuarios y los procesos en Oracle Solaris 11.2 ”.

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: xxxxxxxx
kadmin:
```

   b. **Agregue el principal de servicio `ftp` al servidor FTP.**

```
kadmin: addprinc -randkey ftp/ftpserver1.example.com
```

c. **Agregue el principal de servicio `ftp` a un nuevo archivo keytab.**

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
```

Para obtener más información, consulte la página del comando man `ktadd` command in the `kadmin`(1M).

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`.

```
# pfedit /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, puede que necesite crear una tabla de credenciales que asigne credenciales de usuario a UID de UNIX. Para obtener información sobre la asignación de credenciales predeterminada, consulte “Asignación de credenciales GSS a credenciales UNIX” [67]. 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 4-6 Mapa de tareas de la configuración de servidores NFS con Kerberos

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.	Cómo configurar servidores NFS con Kerberos [118]

Tarea	Descripción	Para obtener instrucciones
Crear una tabla de credenciales y modificarla.	Crea una tabla de credenciales para la asignación de credenciales GSS a los UID de UNIX cuando la asignación predeterminada no es suficiente y, a continuación, agrega una entrada.	Cómo crear y modificar una tabla de credenciales [119]
Asignar credenciales de usuario de otro dominio a los UID de UNIX.	Actualiza la información en la tabla de credenciales.	Ejemplo 4-10, “Agregación de un principal de un dominio diferente en la tabla de credenciales Kerberos”
Crear asignaciones de credenciales entre dos dominios similares.	Asigna los UID de un dominio a otro donde los dominios comparten un archivo de contraseña.	Cómo proporcionar asignación de credenciales entre dominios [120]
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.	Cómo configurar un entorno NFS seguro con varios modos de seguridad de Kerberos [121]

▼ Cómo configurar servidores NFS con Kerberos

Este procedimiento utiliza 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 “Uso de sus derechos administrativos asignados” de “Protección de los usuarios y los procesos en Oracle Solaris 11.2 ”.

El KDC maestro está configurado. Los relojes se sincronizan, como se describe en “Sincronización de relojes entre clientes Kerberos y KDC” [128]. Para probar completamente el proceso, necesita varios clientes.

1. **Configure el servidor NFS como un cliente Kerberos.**

   Siga las instrucciones en “Configuración de clientes Kerberos” [94].

2. **Agregue el principal del servicio NFS.**

   Use el comando `kadmin`.

```
denver # /usr/sbin/kadmin -p kws/admin
Enter password: xxxxxxxx
kadmin:
```

   a. **Cree el principal del servicio NFS.**

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 que creó en el Paso 2.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.
kadmin:
```

c. Salga de `kadmin`.

```
kadmin: quit
```

3. 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” [67]. Si la asignación predeterminada no es suficiente, consulte Cómo crear y modificar una tabla de credenciales [119] para obtener más información.

4. Comparta el sistema de archivos NFS con modos de seguridad de Kerberos.

Para obtener más información, consulte Cómo configurar un entorno NFS seguro con varios modos de seguridad de Kerberos [121].

▼ Cómo crear y modificar una tabla de credenciales

La tabla de credenciales `gsscred` es utilizada por un servidor NFS para asignar credenciales Kerberos a un UID de UNIX. De manera predeterminada, la parte principal del nombre del principal se compara con un nombre de inicio de sesión de UNIX. Puede crear esta tabla si la asignación predeterminada no es suficiente.

Antes de empezar Debe asumir el rol `root`. Para obtener más información, consulte "Uso de sus derechos administrativos asignados" de "Protección de los usuarios y los procesos en Oracle Solaris 11.2 ".

1. **Asegúrese de que el mecanismo de seguridad indicado en `/etc/gss/gsscred.conf` sea `files`.**

```
# cat /etc/gss/gsscred.conf
...
#
files
#
#
# Syslog (auth.debug) a message for GSS cred to Unix cred mapping
#SYSLOG_UID_MAPPING=yes
```

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`. Si no desea incluir las entradas de contraseñas locales en la tabla de credenciales, puede eliminar de forma temporal la entrada `files`. Para obtener más información, consulte la página del comando man `gsscred`(1M).

3. **(Opcional) Agregue una entrada a la tabla de credenciales.**

Por ejemplo, como el rol `root` en el servidor NFS, agregue una entrada para asignar el principal `sandy/admin` al `3736` del UID. La opción `-a` agrega la entrada a la tabla de credenciales.

```
# gsscred -m kerberos_v5 -n sandy/admin -u 3736 -a
```

ejemplo 4-10 Agregación de un principal de un dominio diferente en la tabla de credenciales Kerberos

En este ejemplo, utilice un nombre de dominio completo (FQDN) para especificar un principal de un dominio diferente.

```
# 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 *username*@CORP.EXAMPLE.COM y *username*@SALES.EXAMPLE.COM están asignadas al mismo UID.

Antes de empezar Debe asumir el rol root. Para obtener más información, consulte "Uso de sus derechos administrativos asignados" de "Protección de los usuarios y los procesos en Oracle Solaris 11.2 ".

- **En el sistema cliente, agregue las entradas `default_realm` y `auth_to_local_realm` al archivo `krb5.conf`.**

```
# pfedit /etc/krb5/krb5.conf
[libdefaults]
default_realm = CORP.EXAMPLE.COM
.
[realms]
CORP.EXAMPLE.COM = {
.
auth_to_local_realm = SALES.EXAMPLE.COM
.
}
```

Errores más frecuentes Para obtener ayuda con la resolución de problemas de asignación de credenciales, consulte "Observación de asignación de credenciales GSS a credenciales UNIX" [199].

▼ 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 varios modos de seguridad. Cuando un cliente negocia un modo de seguridad con el servidor NFS, el cliente utiliza el primer modo ofrecido por el servidor. Este modo se utiliza para todas las solicitudes de cliente posteriores del sistema de archivos compartidas por dicho servidor.

Antes de empezar Debe asumir el rol root en el servidor NFS. Para obtener más información, consulte "Uso de sus derechos administrativos asignados" de "Protección de los usuarios y los procesos en Oracle Solaris 11.2 ".

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 [118].

```
# 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
```

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

2. **Active los modos de seguridad de Kerberos en el archivo `/etc/nfssec.conf`.**

   En el archivo `/etc/nfssec.conf`, elimine el símbolo "#" que comenta los modos de seguridad de Kerberos.

```
# pfedit /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*

   mode — 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.

   file-system — 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) Monte un sistema de archivos mediante un modo de seguridad distinto del predeterminado.**

   No realice este procedimiento si el modo de seguridad predeterminado es aceptable.

   - **Si el montador automático se está utilizando, edite la base de datos `auto_master` para introducir un modo de seguridad distinto del predeterminado.**

     file-system `auto_home -nosuid,sec=`*mode*

   - **Emita manualmente el comando `mount` para acceder al sistema de archivos mediante un modo que no esté predeterminado.**

```
# mount -F nfs -o sec=mode file-system
```

ejemplo 4-11 Uso compartido de un sistema de archivos con un modo de seguridad de Kerberos

En este ejemplo, la autenticación con el modo de seguridad `krb5` debe realizarse correctamente antes de poder acceder a los archivos mediante el servicio NFS.

```
# share -F nfs -o sec=krb5 /export/home
```

ejemplo 4-12 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. Para obtener más información, consulte la página del comando man `nfssec`(5).

```
# share -F nfs -o sec=krb5:krb5i:krb5p /export/home
```

Configuración de la ejecución pospuesta para el acceso a servicios Kerberos

En el entorno de Kerberos predeterminado, las credenciales caducan después de una cantidad limitada de tiempo. Para los procesos que pueden ejecutarse en momentos arbitrarios, como `cron` y `at`, el tiempo limitado presenta un problema. Este procedimiento describe cómo configurar el entorno de Kerberos para admitir procesos de ejecución retrasada que requieren servicios autenticados mediante Kerberos. Oracle Solaris proporciona módulos PAM y utiliza claves de servicio y opciones de configuración `kclient` para hacer que la ejecución con autenticación Kerberos sea posible y más segura que las soluciones alternativas.

Nota - Si el servidor `cron` se ve comprometido, un usuario no autorizado podría suplantar a los usuarios para obtener acceso a los servicios de destino que se han configurado para el servidor `cron`. Por lo tanto, considere el host `cron` que está configurado en este procedimiento como un sistema más sensible, ya que proporciona servicios intermedios para los usuarios.

▼ Cómo configurar un host de cron para acceder a servicios Kerberos

Este procedimiento utiliza los siguientes parámetros de configuración:

- Host de `cron` = `host1.example.com`

- Servidor NFS = `host2.example.com`
- Servidor LDAP = `host3.example.com`

1. **Configure el servicio `cron` para que admita Kerberos.**

   - **Si el host de `cron` no está configurado para Kerberos, ejecute el comando `kclient` del sistema.**

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

     Por ejemplo, el siguiente comando configura el cliente en el dominio `EXAMPLE.COM`. El comando incluye el archivo `pam_gss_s4u` en el servicio `/etc/pam.d/cron` mediante el mecanismo `include`.

     ```
     # kclient -s cron:optional -R EXAMPLE.COM
     ```

   - **Si el host de `cron` ya está configurado para Kerberos, debe modificar la configuración del PAM para el servicio `cron` en ese host de forma manual.**

     Asegúrese de que la configuración del PAM para el servicio de `cron` incluya el archivo `pam_gss_s4u`.

     ```
     # cd /etc/pam.d ; cp cron cron.orig
     # pfedit cron
           # PAM include file for optional set credentials
           # through Kerberos keytab and GSS-API S4U support
           auth include          pam_gss_s4u
     ```

2. **Active el host de `cron` para actuar como delegado.**

   Por ejemplo:

   ```
   # kadmin -p kws/admin
   Enter password: xxxxxxxx
   kadmin: modprinc +ok_as_delegate host/host1.example.com@EXAMPLE.COM
   Principal “host/host1.example.com@EXAMPLE.COM” modified.
   ```

3. **Active el host de `cron` para solicitar tickets para sí mismo en nombre del usuario que creó el trabajo `cron`.**

   ```
   kadmin: modprinc +ok_to_auth_as_delegate host/host1.example.com@EXAMPLE.COM
   Principal “host/host1.example.com@EXAMPLE.COM” modified.
   kadmin: quit
   ```

4. **En LDAP, configure el host de `cron` para especificar los servicios que utiliza como delegado.**

   Por ejemplo, para activar que el host de `cron` acceda al directorio de inicio del usuario en `host2`, un servidor NFS kerberizado, agregue el host NFS al parámetro `krbAllowedToDelegateTo` en la definición de LDAP del servidor `cron`.

a. **Cree la asignación de delegado.**

```
# pfedit /tmp/delghost.ldif
dn: krbprincipalname=host/
host1.example.com@EXAMPLE.COM,cn=EXAMPLE.COM,cn=krbcontainer,dc=example,dc=com
changetype: modify
krbAllowedToDelegateTo: nfs/host2.example.com@EXAMPLE.COM
```

b. **Agregue la asignación a LDAP.**

```
# ldapmodify -h host3 -D "cn=directory manager" -f delghost.ldif
```

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. Para obtener más información, consulte “Jerarquía de dominios Kerberos” [60].

▼ Cómo establecer la autenticación entre dominios jerárquica

El ejemplo de este procedimiento establece la autenticación entre dominios entre `CORP.EAST.EXAMPLE.COM` y `EAST.EXAMPLE.COM` en ambas direcciones. Este procedimiento debe realizarse en el KDC maestro de ambos dominios.

Antes de empezar El KDC maestro para cada dominio se configura. Para probar completamente el proceso de autenticación, necesita varios clientes.

Debe asumir el rol `root` en ambos servidores KDC. Para obtener más información, consulte “Uso de sus derechos administrativos asignados” de “Protección de los usuarios y los procesos en Oracle Solaris 11.2 ”.

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: xxxxxxxx
```

```
kadmin: addprinc krbtgt/CORP.EAST.EXAMPLE.COM@EAST.EXAMPLE.COM
Enter password for principal krbtgt/CORP.EAST.EXAMPLE.COM@EAST.EXAMPLE.COM:      /** Type strong
 password **/
kadmin: addprinc krbtgt/EAST.EXAMPLE.COM@CORP.EAST.EXAMPLE.COM
Enter password for principal krbtgt/EAST.EXAMPLE.COM@CORP.EAST.EXAMPLE.COM:      /** Type strong
 password **/
kadmin: quit
```

Nota - Guarde y almacene estas contraseñas en una ubicación segura.

2. **Agregue entradas al archivo de configuración de Kerberos para definir nombres de dominio para cada dominio.**

```
# pfedit /etc/krb5/krb5.conf
[libdefaults]
.
.
[domain_realm]
.corp.east.example.com = CORP.EAST.EXAMPLE.COM
.east.example.com = EAST.EXAMPLE.COM
```

En este ejemplo, se definen nombres de dominio para los dominios `CORP.EAST.EXAMPLE.COM` y `EAST.EXAMPLE.COM`. El subdominio debe preceder al nombre de dominio en el archivo, porque el archivo se busca de arriba hacia 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 utilizar la versión de del KDC maestro de `/etc/krb5/krb5.conf`.

4. **Repita este procedimiento en el segundo dominio.**

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/CORP.EAST.EXAMPLE.COM@EAST.EXAMPLE.COM` debe ser la misma en ambos dominios.

▼ Cómo establecer la autenticación entre dominios directa

El ejemplo de este procedimiento utiliza dos dominios, `CORP.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 se configura. Para probar completamente el proceso de autenticación, necesita varios clientes.

Debe asumir el rol `root` en ambos servidores KDC. Para obtener más información, consulte "Uso de sus derechos administrativos asignados" de "Protección de los usuarios y los procesos en Oracle Solaris 11.2 ".

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: xxxxxxxx
   kadmin: addprinc krbtgt/CORP.EAST.EXAMPLE.COM@SALES.WEST.EXAMPLE.COM
   Enter password for principal
   krbtgt/CORP.EAST.EXAMPLE.COM@SALES.WEST.EXAMPLE.COM:      /** Type strong password **/
   kadmin: addprinc krbtgt/SALES.WEST.EXAMPLE.COM@CORP.EAST.EXAMPLE.COM
   Enter password for principal
   krbtgt/SALES.WEST.EXAMPLE.COM@CORP.EAST.EXAMPLE.COM:      /** Type strong password **/
   kadmin: quit
   ```

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 `CORP.EAST.EXAMPLE.COM`. Para agregar las definiciones adecuadas en el dominio `SALES.WEST.EXAMPLE.COM`, intercambie los nombres de dominio.

   ```
   # pfedit /etc/krb5/krb5.conf
   [libdefaults]
   .
   .
   [capaths]
   CORP.EAST.EXAMPLE.COM = {
   SALES.WEST.EXAMPLE.COM = .
   }

   SALES.WEST.EXAMPLE.COM = {
   CORP.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 usar la nueva versión del archivo de configuración de Kerberos, `/etc/krb5/krb5.conf`.

4. **Repita este procedimiento para el segundo dominio.**

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 sesgo de reloj también determina el tiempo durante el cual los servidores de aplicaciones deben realizar un seguimiento de 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.

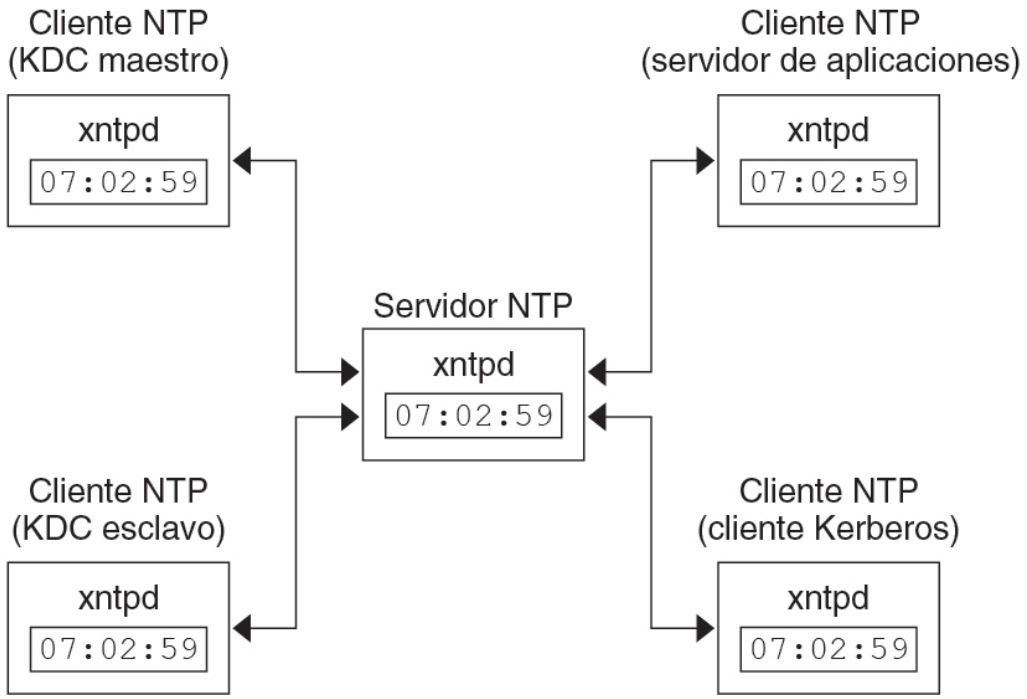
El valor predeterminado para el desfase máximo del reloj es de 300 s (5 min). Puede cambiar este valor predeterminado en la sección `libdefaults` del archivo `krb5.conf`.

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, utilice 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. Encontrará documentación disponible en NTP Documentation.

El NTP permite gestionar la sincronización de relojes de red o el tiempo preciso, o ambos, en un entorno de red. NTP es un protocolo de servidor-cliente. Un sistema es el reloj maestro, el servidor NTP. Todos los demás sistemas son clientes NTP que sincronizar sus relojes con el reloj maestro. 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. La siguiente imagen muestra un ejemplo de esta implementación de NTP de servidor y cliente.

FIGURA 4-1 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.
2. Al realizar la configuración de los clientes Kerberos y los KDC en la red, configúrelos para que sean clientes NTP del servidor NTP. Vuelva al KDC maestro para configurarlo como cliente NTP.
3. Active el servicio NTP en todos los sistemas.

Intercambio de un KDC maestro y un KDC esclavo

Los procedimientos de esta sección facilitan 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 un dominio que utiliza la propagación incremental en el servidor KDC esclavo que desea que esté disponible para convertirse en el KDC maestro.

Antes de empezar Debe asumir el rol `root`. Para obtener más información, consulte "Uso de sus derechos administrativos asignados" de "Protección de los usuarios y los procesos en Oracle Solaris 11.2 ".

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. **Instale un KDC esclavo.**

   Antes de realizar un intercambio, este servidor debe funcionar como cualquier otro KDC esclavo en el dominio. Para obtener más información, consulte Cómo configurar manualmente un KDC esclavo [82].

3. **Después de la instalación, mueva los comandos del KDC maestro.**

   Los comandos del KDC maestro no se deben ejecutar desde este KDC esclavo.

```
kdc4 # mv /usr/lib/krb5/kprop /usr/lib/krb5/kprop.save
kdc4 # mv /usr/lib/krb5/kadmind /usr/lib/krb5/kadmind.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 Complete el procedimiento Cómo configurar un KDC esclavo intercambiable [130].

Debe asumir el rol `root`. Para obtener más información, consulte "Uso de sus derechos administrativos asignados" de "Protección de los usuarios y los procesos en Oracle Solaris 11.2 ".

1. **En el nuevo KDC maestro, inicie `kadmin`.**

```
kdc4 # /usr/sbin/kadmin -p kws/admin
Enter password: xxxxxxxx
kadmin:
```

2. **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@EXAMPLE.COM" created.
kadmin: addprinc -randkey -allow_tgs_req -clearpolicy kadmin/kdc4.example.com
Principal "kadmin/kdc4.example.com@EXAMPLE.COM" created.
kadmin:
```

3. **Salga de `kadmin`.**

```
kadmin: quit
```

4. **En el nuevo KDC maestro, fuerce la sincronización.**

   Los siguientes pasos fuerzan una actualización completa del KDC en el servidor esclavo.

   a. **Desactive el servicio `krb5kdc` y elimine su archivo log.**

```
kdc4 # svcadm disable network/security/krb5kdc
kdc4 # rm /var/krb5/principal.ulog
```

   b. **Verifique que la actualización se haya completado.**

```
kdc4 # /usr/sbin/kproplog -h
```

   c. **Reinicie el servicio KDC.**

```
kdc4 # svcadm enable -r network/security/krb5kdc
```

   d. **Reinicialice el log de actualización para el nuevo servidor KDC maestro.**

```
kdc4 # svcadm disable network/security/krb5kdc
kdc4 # rm /var/krb5/principal.ulog
```

5. **En el KDC maestro antiguo, termine los servicios `kadmin` y `krb5kdc`.**

   Al terminar el servicio `kadmin`, evita que se realicen cambios en la base de datos del KDC.

```
kdc1 # svcadm disable network/security/kadmin
kdc1 # svcadm disable network/security/krb5kdc
```

6. **En el KDC maestro antiguo, especifique el tiempo de sondeo para solicitar propagaciones.**

Elimine el comentario de la entrada `sunw_dbprop_master_ulogsize` en `/etc/krb5/kdc.conf` y agregue una entrada que defina el intervalo de sondeo del esclavo. Esta entrada establece el tiempo de sondeo en dos minutos.

```
kdc1 # pfedit /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
}
```

7. **En el KDC maestro antiguo, mueva los comandos del KDC maestro y el archivo `kadm5.acl`.**

   Los comandos del KDC maestro no se deben ejecutar desde el KDC maestro antiguo.

   ```
   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
   ```

8. **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
   ```

9. **En el servidor DNS, vuelva a cargar la nueva información de alias.**

   ```
   # svcadm refresh network/dns/server
   ```

10. **En el nuevo KDC maestro, mueva los comandos del KDC maestro y el archivo `kpropd.acl` esclavo.**

    Movió los comandos del KDC maestro en Paso 3 of Cómo configurar un KDC esclavo intercambiable [130].

    ```
    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
    ```

11. **En el nuevo KDC maestro, cree el archivo de 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 pueden realizar solicitudes de propagación incremental. Para obtener más información, consulte la página del comando man `kadm5.acl`(4).

```
kdc4 # pfedit /etc/krb5/kadm5.acl
kws/admin@EXAMPLE.COM   *
kiprop/kdc1.example.com@EXAMPLE.COM p
```

12. **En el nuevo KDC maestro, especifique el tamaño de log 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`. Esta entrada establece el tamaño de log en 1.000 entradas.

```
kdc1 # pfedit /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
}
```

13. **En el nuevo KDC maestro, active los servicios `kadmin` y `krb5kdc`.**

```
kdc4 # svcadm enable -r network/security/krb5kdc
kdc4 # svcadm enable -r network/security/kadmin
```

14. **En el KDC maestro antiguo, agregue el principal de servicio `kiprop`.**

    La agregación 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: xxxxxxxx
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.
kadmin: quit
```

15. **En el KDC maestro antiguo, agregue una entrada para cada KDC en el archivo `krb5.conf` al archivo de configuración de propagación.**

```
kdc1 # pfedit /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
```

16. **En el KDC maestro antiguo, active los servicios `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 para 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 [77].

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. Luego, 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.

Asegúrese 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 sobre el resto de los métodos de propagación. La propagación manual de la base de datos requiere más sobrecarga administrativa y la propagación completa es ineficaz.

Atención - Para evitar la pérdida de datos, debe propagar manualmente la base de datos si agrega actualizaciones importantes a la base de datos de Kerberos antes de una propagación programada con regularidad.

Archivo `kpropd.acl`

El archivo `kpropd.acl` 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.acl` 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 descritos en esta guía le indican que utilice el mismo archivo `kpropd.acl` en el KDC maestro y 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. La copia idéntica en todos los KDC facilita el mantenimiento.

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.

Copia de seguridad de la base de datos de Kerberos

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. La corrupción de datos no

es un problema en un KDC esclavo, 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. La copia de seguridad dañada también sobrescribe el archivo de copia de seguridad anterior que no está dañado en el KDC maestro.

Para proteger en este escenario, configure 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`. A fin de proteger contra el acceso no autorizado, propague el archivo de volcado de la base de datos con el comando `kprop`, porque este comando 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.

EJEMPLO 4-13 Copia de seguridad manual de la base de datos de Kerberos

Utiliza el comando `dump` del comando `kdb5_util` para realizar una copia de seguridad de la base de datos. Ejecute este comando en un directorio que sea propiedad de `root`.

```
# /usr/sbin/kdb5_util dump
```

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. Dado que no se especifican principales, se realiza una copia de seguridad de toda la base de datos.

```
# kdb5_util dump -verbose /var/user/kadmin/dumpfile
kadmin/kdc1.corp.example.com@CORP.EXAMPLE.COM
krbtgt/CORP.EXAMPLE.COM@CORP.EXAMPLE.COM
kadmin/history@CORP.EXAMPLE.COM
pak/admin@CORP.EXAMPLE.COM
pak@CORP.EXAMPLE.COM
changepw/kdc1.corp.example.com@CORP.EXAMPLE.COM
```

En el ejemplo siguiente, el volcado contiene sólo los principales `pak` y `pak/admin`.

```
# kdb5_util dump -verbose pakfile pak/admin@CORP.EXAMPLE.COM pak@CORP.EXAMPLE.COM
pak/admin@CORP.EXAMPLE.COM
pak@CORP.EXAMPLE.COM
```

Para obtener más información, consulte la página del comando man `kdb5_util`(1M).

▼ Cómo restaurar una copia de seguridad de la base de datos de Kerberos

Antes de empezar En KDC maestro, debe asumir el rol `root`. Para obtener más información, consulte “Uso de sus derechos administrativos asignados” de “Protección de los usuarios y los procesos en Oracle Solaris 11.2 ”.

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`.**

   Por ejemplo, cargue la copia de seguridad `dumpfile` de Ejemplo 4-13, “Copia de seguridad manual de la base de datos de Kerberos”.

```
# /usr/sbin/kdb5_util load /var/user/kadmin/dumpfile
```

3. **Inicie los daemons del KDC.**

```
kdc1 # svcadm enable -r network/security/krb5kdc
kdc1 # svcadm enable -r network/security/kadmin
```

ejemplo 4-14 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`. Dado que la opción `-update` no se especifica, se crea una base de datos nueva.

```
# 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 una versión anterior, la conversión de la base de datos permite aprovechar el formato de base de datos mejorado.

Antes de empezar Utilice este procedimiento sólo si la base de datos está utilizando un formato antiguo.

En KDC maestro, debe asumir el rol `root`. Para obtener más información, consulte “Uso de sus derechos administrativos asignados” de “Protección de los usuarios y los procesos en Oracle Solaris 11.2 ”.

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. 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 Debe asumir el rol `root`. Para obtener más información, consulte “Uso de sus derechos administrativos asignados” de “Protección de los usuarios y los procesos en Oracle Solaris 11.2 ”.

1. **Agregue entradas a `kdc.conf`.**

Necesita activar la propagación incremental y seleccionar el número de actualizaciones que el KDC maestro mantiene en el log. Para obtener más información, consulte la página del comando man kdc.conf(4).

```
kdc1 # pfedit /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: xxxxxxxx
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 # pfedit /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/krb5/kprop_script kdc2.example.com
```

5. **Reinicie `kadmind`.**

```
kdc1 # svcadm restart network/security/kadmin
```

6. **Reconfigure todos los servidores KDC esclavos que utilicen la propagación incremental.**
   Para obtener instrucciones completas, consulte Cómo reconfigurar un KDC esclavo para utilizar la propagación incremental [140].

▼ Cómo reconfigurar un KDC esclavo para utilizar la propagación incremental

Antes de empezar Debe asumir el rol `root`. Para obtener más información, consulte "Uso de sus derechos administrativos asignados" de "Protección de los usuarios y los procesos en Oracle Solaris 11.2 ".

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 # pfedit /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 `kiprop` al archivo `krb5.keytab`.**

```
kdc2 # /usr/sbin/kadmin -p kws/admin
Enter password: xxxxxxxx
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.
kadmin: quit
```

3. **Reinicie `kpropd`.**

```
kdc2 # svcadm restart network/security/krb5_prop
```

▼ Cómo verificar que los servidores KDC estén sincronizados

Si la propagación incremental se ha configurado, este procedimiento garantiza que la información sobre el KDC esclavo se ha actualizado.

Antes de empezar Debe asumir el rol `root`. Para obtener más información, consulte “Uso de sus derechos administrativos asignados” de “Protección de los usuarios y los procesos en Oracle Solaris 11.2 ”.

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 4-15 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.ulog)
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: Wed Dec 4 00:59:27 2013
Last time stamp: Wed Dec 4 01:06:13 2013
```

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.ulog)
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: Wed Dec 4 01:06:13 2013
```

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 log 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.

Propagación manual de la base de datos de Kerberos a los KDC esclavos

Normalmente, un trabajo `cron` propaga la base de datos de Kerberos a KDC esclavos. Si necesita sincronizar un KDC esclavo con el KDC maestro fuera del trabajo `cron` periódico, tiene dos opciones, los comandos `/usr/lib/krb5/kprop_script` y `kprop`. Para obtener más información, consulte la secuencia de comandos y la página del comando man `kprop`(1M).

Atención - No utilice estos comandos si la propagación incremental está activada en el KDC esclavo.

▼ Cómo propagar manualmente la base de datos de Kerberos a un KDC esclavo

1. **Verifique que la propagación incremental no esté activada en el KDC esclavo.**

```
slave# grep sunw_dbprop_enable /etc/krb5/kdc.conf
sunw_dbprop_enable = true
```

2. **Si el valor es `true`, desactive la propagación incremental y reinicie el servicio `krb5_prop`.**

```
slave# cp /etc/krb5/kdc.conf /etc/krb5/kdc.conf.sav
slave# pfedit /etc/krb5/kdc.conf
...
sunw_dbprop_enable = false
...

slave# svcadm restart krb5_prop
```

3. **En el KDC maestro, utilice uno de los siguientes comandos para propagar la base de datos del KDC maestro para el KDC esclavo.**

   - **El comando `kprop_script` realiza una copia de seguridad de la base de datos antes de sincronizar el KDC esclavo.**

     ```
     master# /usr/lib/krb5/kprop_script slave-KDC
     ```

   - **El comando `kprop` propaga la copia de seguridad de base de datos actual sin realizar primero una nueva copia de seguridad de la base de datos de Kerberos.**

     ```
     master# /usr/lib/krb5/kprop -f /var/krb5/slave_datatrans slave-KDC
     ```

4. **(Opcional) Después de que la propagación manual se completa, restaure el archivo `krb5.conf` original.**

```
slave# mv /etc/krb5/kdc.conf.sav /etc/krb5/kdc.conf
```

Configuración de la propagación en paralelo para Kerberos

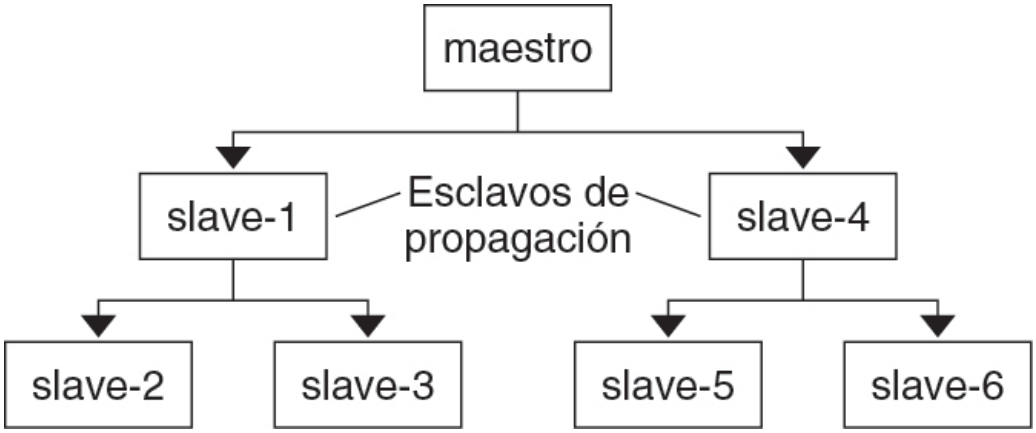
En la mayoría de los casos, el KDC maestro se utiliza, exclusivamente, para propagar su base de datos de Kerberos a los KDC esclavos. Sin embargo, si su sitio tiene muchos KDC esclavos, es posible que deba considerar el uso compartido de carga del proceso de propagación, conocido como *propagación en paralelo*.

Atención - No configure la propagación en paralelo si utiliza 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 4-2, “Ejemplo de configuración de propagación en paralelo en Kerberos”), 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 `slave-4`. A su vez, los KDC esclavos pueden propagar la base de datos a los KDC esclavos de su grupo.

FIGURA 4-2 Ejemplo de configuración de propagación en paralelo en Kerberos



Pasos de configuración para la propagación en paralelo

Los pasos de configuración de alto nivel para activar la propagación en paralelo son los siguientes:

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 - La cantidad de 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 para propagarse agregando el nombre del principal host de su KDC de propagación a su archivo `kpropd.acl`.

EJEMPLO 4-16 Configuración de la propagación en paralelo en Kerberos

Mediante el ejemplo de la Figura 4-2, “Ejemplo de configuración de propagación en paralelo en Kerberos”, 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 para la base de datos de Kerberos

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 manualmente.

Para eliminar el archivo intermedio, utilice el comando `rm`:

```
# rm stash-file
```

Donde *stash-file* es la ruta al archivo intermedio. De manera predeterminada, el archivo intermedio se encuentra en `/var/krb5/.k5.`*realm*.

Nota - Si necesita volver a crear el archivo intermedio, puede utilizar la opción `-f` del comando `kdb5_util`.

▼ Cómo crear, utilizar y almacenar una nueva clave maestra para la base de datos de Kerberos

Antes de empezar Debe asumir el rol `root`. Para obtener más información, consulte "Uso de sus derechos administrativos asignados" de "Protección de los usuarios y los procesos en Oracle Solaris 11.2 ".

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 strong password **/
Re-enter KDC database master key to verify: xxxxxxxx
```

2. Verifique que exista la nueva clave maestra.

```
# kdb5_util list_mkeys
Master keys for Principal: K/M@EXAMPLE.COM
KNVO: 2, Enctype: AES-256 CTS mode with 96-bit SHA-1 HMAC, No activate time set
KNVO: 1, Enctype: AES-128 CTS mode with 96-bit SHA-1 HMAC, Active on: Fri Dec 31 18:00:00 CST
 2011 *
```

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 11 17:57:00 CDT 2014
# kdb5_util use_mkey 2 'now+2days'
# kdb5_util list_mkeys
Master keys for Principal: K/M@EXAMPLE.COM
KNVO: 2, Enctype: AES-256 CTS mode with 96-bit SHA-1 HMAC,
Active on: Sun Jul 13 17:57:15 CDT 2014
KNVO: 1, Enctype: AES-128 CTS mode with 96-bit SHA-1 HMAC,
Active on: Fri Dec 31 18:00:00 CST 2011 *
```

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 tamiko' |egrep 'Principal|MKey'
Authenticating as principal root/admin@EXAMPLE.COM with password.
Principal: tamiko@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:   tamiko@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-256 CTS mode with 96-bit SHA-1 HMAC,
Active on: Sun Jul 13 17:57:15 CDT 2014 *
```

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 05/11/2014 18:03 K/M@EXAMPLE.COM
```

Aumento de la seguridad en servidores Kerberos

Esta sección proporciona consejos sobre el aumento de la seguridad en servidores de aplicaciones Kerberos y en servidores KDC.

Restricción de 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.

- Restrinja el acceso físico al hardware que admite el KDC.

  Asegúrese de que el servidor KDC y su monitor se encuentren en una instalación segura. Los usuarios normales no deben poder acceder a este servidor de ninguna forma.
- 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.

  La práctica recomendada es almacenar estos archivos en un sistema de archivos local que no se comparta con otros sistemas. El sistema de archivos de almacenamiento puede estar en el servidor KDC maestro o en cualquier KDC esclavo.

Uso de 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 para 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.

Necesita agregar una línea para el archivo de configuración de KDC, `kdc.conf`, para indicar al servicio que utilice un archivo de diccionario. En este ejemplo, el administrador utiliza el diccionario que se incluye con la utilidad `spell` y, luego, reinicia los servicios Kerberos. Para obtener una descripción completa de este archivo de configuración, consulte la página del comando man `kdc.conf`(4).

```
kdc1 # pfedit /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
}
kdc1 #
kdc1 # svcadm restart -r network/security/krb5kdc
kdc1 # svcadm restart -r network/security/kadmin
```

♦ ♦ ♦ CAPÍTULO 5

Administración de las políticas y los principales de Kerberos

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.

En este capítulo, se tratan los siguientes temas:

Para obtener más información acerca de los principales y las políticas, consulte Capítulo 2, Acerca del servicio Kerberos y Capítulo 3, Planificación del servicio Kerberos.

Maneras de administrar las políticas y los principales de Kerberos

La base de datos de Kerberos en el KDC maestro contiene todas las principales de Kerberos del dominio, sus contraseñas, políticas y otra información administrativa. Para crear y suprimir 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. También puede ejecutar secuencias de comandos que automatizan la creación del principal. El comando `kadmin` tiene una versión local y una versión remota:

- `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

Las capacidades de las dos versiones son idénticas. Debe configurar la base de datos lo suficiente con la versión local antes de poder utilizar la versión remota.

La versión Oracle Solaris también proporciona una interfaz gráfica de usuario (GUI) interactiva, `gkadmin`.

En esta sección se describen las capacidades de secuencias de comandos del comando `kadmin.local` y se comparan las interfaces de la línea de comandos con la interfaz gráfica de usuario.

Automatización de la creación de nuevos principales de Kerberos

Puede utilizar el comando `kadmin.local` en una secuencia de comandos para automatizar la creación de nuevos principales de Kerberos. La automatización es útil si desea agregar muchos nuevos principales a la base de datos.

La siguiente secuencia de comandos de shell muestra 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 anterior está dividido en dos líneas para su legibilidad.

- La secuencia de comandos lee en un archivo llamado `princnames`. Este archivo 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.
- El comando `ank` agrega una nueva clave. `ank` es un alias para el comando `add_principal`.
- La opción `+needchange` configura el principal de modo que al usuario que es el principal se le pida una contraseña nueva en el primer inicio de sesión.

  Solicitar el cambio de contraseña 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.

Interfaz gráfica de usuario `gkadmin`

La interfaz gráfica de usuario `gkadmin` de Kerberos proporciona la mayoría de las capacidades de la CLI e incluye la ayuda en pantalla. En la siguiente tabla se describen las diferencias entre la CLI y la interfaz gráfica de usuario.

TABLA 5-1 Equivalentes de la línea de comandos de la interfaz gráfica de usuario `gkadmin`

Procedimiento Interfaz gráfica de usuario gkadmin	Comando `kadmin` equivalente
Ver lista de principales	`list_principals` o `get_principals`
Ver atributos de un principal	`get_principal`
Crear un principal nuevo	`add_principal`
Duplicar un principal	No hay equivalente de línea de comandos
Modificar un principal	`modify_principal` o `change_password`
Suprimir un principal	`delete_principal`
Configurar valores predeterminados para crear principales nuevos	No hay equivalente de línea de comandos
Ver lista de políticas	`list_policies` o `get_policies`
Ver atributos de una política	`get_policy`
Crear una política nueva	`add_policy`
Duplicar una política	No hay equivalente de línea de comandos
Modificar una política	`modify_policy`
Suprimir una política	`delete_policy`

La interfaz gráfica de usuario `gkadmin` de Kerberos proporciona ayuda contextual. Para obtener acceso con el explorador, utilice la URL de Oracle (http://docs.oracle.com/cd/E23824_01/html/821-1456/aadmin-23.html). Puede copiar este archivo a una dirección URL. Especifique la dirección URL de la ayuda en pantalla en el archivo `krb5.conf` al configurar un host para utilizar la interfaz gráfica de usuario `gkadmin`.

Administración de los principales de Kerberos

En esta sección se proporcionan ejemplos del uso del comando `kadmin` y la interfaz gráfica de usuario `gkadmin` para administrar principales. Para obtener más información, consulte las páginas del comando man `kadmin`(1M) y `gkadmin`(1M).

Visualización de los principales de Kerberos y sus atributos

Los siguientes ejemplos muestran cómo enumerar los principales y sus atributos. Puede utilizar comodines para crear las listas. Para obtener información sobre los posibles comodines, revise la definición de `expression` en la página del comando man `kadmin`(1M).

EJEMPLO 5-1 Visualización de los principales de Kerberos

En este ejemplo, el subcomando `list_principals` se utiliza para mostrar todos los principales que coinciden con `kadmin*`. Sin un argumento, `list_principals` muestra todos los principales que se definen en la base de datos de Kerberos.

```
# /usr/sbin/kadmin
kadmin: list_principals kadmin*
kadmin/changepw@EXAMPLE.COM
kadmin/kdc1.example.com@EXAMPLE.COM
kadmin/history@EXAMPLE.COM
```

EJEMPLO 5-2 Visualización de los atributos de los principales de Kerberos

El ejemplo siguiente muestra los atributos del principal de `jdb/admin`.

```
kadmin: get_principal jdb/admin
Principal: jdb/admin@EXAMPLE.COM

Expiration date: [never]
Last password change: [never]

Password expiration date: Fri Sep 13 11:50:10 PDT 2013
Maximum ticket life: 1 day 16:00:00
Maximum renewable life: 1 day 16:00:00
Last modified: Thu Aug 15 13:30:30 PST 2013 (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
Attributes: REQUIRES_HW_AUTH
Policy: [none]
kadmin: quit
```

EJEMPLO 5-3 Uso de la interfaz gráfica de usuario `gkadmin` para enumerar y definir los valores predeterminados para los principales de Kerberos

En este ejemplo, el administrador desea mostrar a un nuevo administrador la lista de principales y sus atributos, de modo que utiliza la interfaz gráfica de usuario `gkadmin`. El administrador también define los nuevos valores predeterminados para futuros principales.

```
# /usr/sbin/gkadmin
```

La ventana muestra los campos Nombre de principal, Contraseña, Dominio y KDC maestro.

El administrador navega hasta la lista de todos los nombres de principales y, a continuación, muestra al nuevo administrador cómo utilizar el filtro que distingue entre mayúsculas y minúsculas.

Luego, el administrador hace clic en el menú Editar y selecciona Propiedades. Después de hacer clic en Requerir cambio de contraseña, el administrador aplica el cambio.

Para ver los atributos de un principal actual, el administrador navega hasta la lista de principales y elige un principal de la lista. El primer cuadro de diálogo muestra atributos básicos. El administrador hace clic en el botón Siguiente para mostrar todos los atributos.

Creación de un nuevo principal de Kerberos

Si un nuevo principal requiere una nueva política, debe crear la nueva política antes de crear el principal. Para la creación de políticas, consulte Ejemplo 5-10, “Creación de una nueva política de contraseñas de Kerberos”. La mayoría de las políticas de Kerberos especifican requisitos de contraseña.

EJEMPLO 5-4 Creación de un nuevo principal de Kerberos

El siguiente ejemplo crea un nuevo principal denominado `pak` y establece la política del principal en `testuser`. Los otros valores requeridos, como el tipo de cifrado, utilizan los valores predeterminados.

```
# /usr/sbin/kadmin
kadmin: add_principal -policy testuser pak
Enter password for principal "pak@EXAMPLE.COM": xxxxxxxx
Re-enter password for principal "pak@EXAMPLE.COM": xxxxxxxx
Principal "pak@EXAMPLE.COM" created.
kadmin: quit
```

Normalmente, pocos usuarios tienen privilegios para administrar la base de datos de Kerberos. Si este nuevo principal necesita privilegios administrativos, continúe con “Modificación de los privilegios de administración de los principales de Kerberos” [157].

Modificación de un principal de Kerberos

Los siguientes ejemplos muestran cómo modificar los atributos de contraseña de un principal de Kerberos.

EJEMPLO 5-5 Modificación del número máximo de reintentos de contraseña para un principal de Kerberos

```
# /usr/sbin/kadmin
kadmin: modify_principal jdb
kadmin: maxtries=5
kadmin: quit
```

EJEMPLO 5-6 Modificación de la contraseña de un principal de Kerberos

```
# /usr/sbin/kadmin
kadmin: change_password jdb
Enter password for principal "jdb": xxxxxxxx
Re-enter password for principal "jdb": xxxxxxxx
Password for "jdb@EXAMPLE.COM" changed.
kadmin: quit
```

Supresión de un principal de Kerberos

El siguiente ejemplo muestra cómo suprimir un principal. Cumpla con el mensaje en línea antes de continuar.

```
# /usr/sbin/kadmin
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
```

Para eliminar este principal de todas las ACL, consulte “Modificación de los privilegios de administración de los principales de Kerberos” [157].

Duplicación de un principal de Kerberos con la interfaz gráfica de usuario `gkadmin`

Puede duplicar un principal mediante el interfaz gráfica de usuario `gkadmin`. No hay equivalente de línea de comandos para este procedimiento.

1. Después de iniciar la interfaz gráfica de usuario con el comando `/usr/sbin/gkadmin`, haga clic en la ficha Principales y seleccione un principal para duplicar.
2. Haga clic en el botón Duplicar. Esta acción duplica todos los atributos del principal seleccionado, excepto el nombre y la contraseña del principal.

3. Especifique un nuevo nombre y contraseña y, a continuación, haga clic en Guardar para crear un duplicado exacto.
4. Para modificar el duplicado, especifique los valores de 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.

Normalmente, pocos usuarios tienen privilegios para administrar la base de datos de Kerberos. Si este nuevo principal necesita privilegios administrativos, continúe con "Modificación de los privilegios de administración de los principales de Kerberos" [157].

Modificación de los privilegios de administración de los principales de Kerberos

Los pocos usuarios que tienen privilegios para administrar la base de datos de Kerberos se especifican en la lista de control de acceso de Kerberos (ACL). Esta lista se mantiene como entradas de un archivo, `/etc/krb5/kadm5.acl`. Para obtener más información, consulte la página del comando man `kadm5.acl`(4).

Para agregar entradas al archivo `kadm5.acl`, utilice el comando `pfedit`.

```
# pfedit /usr/krb5/kadm5.acl
```

Una entrada en el archivo `kadm5.acl` tiene el siguiente formato:

principal privileges [*principal-target*]

- *principal*: especifica el principal al que se le otorgan los privilegios. Cualquier parte del nombre del principal puede incluir el comodín '*', que es útil para proporcionar los mismos privilegios para un grupo de principales. Por ejemplo, si desea especificar todos los principales con la instancia `admin`, debe utilizar `*/admin@`*realm*.

  Tenga en cuenta que un uso común de una instancia `admin` es conceder privilegios independientes (por ejemplo, acceso administrativo a la base de datos de Kerberos) a un principal de Kerberos individual. Por ejemplo, el usuario `jdb` puede tener un principal para el uso administrativo, denominado `jdb/admin`. Al tener dos principales, el usuario `jdb` obtiene tickets de `jdb/admin` sólo cuando se necesitan privilegios administrativos.
- *privilegios*: especifica qué operaciones puede realizar el principal. Este campo consta de una cadena compuesta por uno o varios caracteres de la siguiente lista. 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.
  - [A]a: permite o prohíbe la agregación de principales o políticas.

- [C]c: permite o prohíbe el cambio de contraseñas para principales.
- [D]d: permite o prohíbe la eliminación de principales o políticas.
- [I]i: permite o prohíbe la base de datos de Kerberos.
- [L]l: permite o prohíbe la enumeración de principales o políticas.
- [M]m: permite o prohíbe la modificación de principales o políticas.
- x o *: permite todos los privilegios (admcil).

- *destino_principal*: cuando se especifica un principal en este campo, los privilegios del principal se aplican únicamente al principal. Para asignar privilegios a un grupo de principales, utilice el comodín '*' en *destino_principal*.

EJEMPLO 5-7 Modificación de privilegios de un principal de Kerberos

La siguiente entrada en el archivo kadm5.acl 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.acl le otorga al principal jdb@EXAMPLE.COM los privilegios para mostrar y consultar cualquier principal que tenga la instancia root.

```
jdb@EXAMPLE.COM li */root@EXAMPLE.COM
```

Administración de las políticas de Kerberos

En esta sección se proporcionan ejemplos del uso del comando kadmin y la interfaz gráfica de usuario gkadmin para administrar políticas de Kerberos. La mayoría de las políticas de Kerberos especifican requisitos de contraseña.

Los pasos para administrar políticas son similares a los pasos para administrar principales. Para obtener más información, consulte las páginas del comando man kadmin(1M) y gkadmin(1M).

EJEMPLO 5-8 Visualización de la lista de las políticas de Kerberos

En este ejemplo, el subcomando list_policies se utiliza para mostrar todas las políticas que coinciden con *user*. Sin un argumento, list_policies muestra todas las políticas que se definen en la base de datos de Kerberos.

```
# kadmin
kadmin: list_policies *user*
testuser
```

```
financeuser
kadmin: quit
```

EJEMPLO 5-9 Visualización de los atributos de una política de Kerberos

En este ejemplo, el subcomando `get_policy` se utiliza para ver los atributos de la política `financeuser`.

```
# /usr/sbin/kadmin.local
kadmin.local: get_policy financeuser
Policy: financeuser
Maximum password life: 13050000
Minimum password life: 10886400
Minimum password length: 8
Minimum number of password character classes: 2
Number of old keys kept: 3
Reference count: 8
Maximum password failures before lockout: 5
Password failure count reset interval: 200
Password lockout duration: 300
kadmin: quit
```

El recuento de referencia (Reference count) es el número de principales que se asignan a esta política.

EJEMPLO 5-10 Creación de una nueva política de contraseñas de Kerberos

En este ejemplo, el subcomando `add_policy` 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
```

EJEMPLO 5-11 Manejo de la política de bloqueo de una cuenta de Kerberos

En este ejemplo, tres fallos de autenticación durante un máximo de `300` segundos provocan un bloqueo de cuenta de `900` segundos.

```
kadmin: add_policy -maxfailure 3 -failurecountinterval "300 seconds"\
-lockoutduration "900 seconds" default
```

Para liberar el bloqueo en el transcurso de 15 minutos, se requiere una acción de la administración.

```
# /usr/sbin/kadmin -p kws/admin
Enter password: xxxxxxxx
kadmin: modify_principal -unlock principal
```

EJEMPLO 5-12 Modificación de una política Kerberos

En este ejemplo, el subcomando `modify_policy` se utiliza para cambiar la longitud mínima de una contraseña por ocho caracteres para la política `build11`.

```
# kadmin
kadmin: modify_policy -minlength 8 build11
kadmin: quit
```

EJEMPLO 5-13 Supresión de una política de Kerberos

En este ejemplo, el subcomando `delete_policy` se utiliza para suprimir la política `build11`.

1. El administrador elimina la política de todos los principales que la utilizan.

   ```
   # kadmin
   kadmin: modify_principal -policy build11 *admin*
   ```

2. A continuación, el administrador suprime la política.

   ```
   kadmin: delete_policy build11
   Are you sure you want to delete the policy "build11"? (yes/no): yes
   kadmin: quit
   ```

El comando `delete_policy` fallará si la política está asignada a un principal.

EJEMPLO 5-14 Duplicación de una política de Kerberos con la interfaz gráfica de usuario `gkadmin`

En la interfaz gráfica de usuario `gkadmin`, puede duplicar una política seleccionada haciendo clic en el botón Duplicar. En el campo Nombre de la política, nombre la nueva política. También puede modificar los atributos de política que duplica. Los pasos son similares a los pasos en “Duplicación de un principal de Kerberos con la interfaz gráfica de usuario `gkadmin`” [156].

Administración de los archivos keytab

Cada host que proporciona un servicio debe tener un archivo local, denominado archivo keytab, que es 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 la clave de servicio para el 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` en un proceso `kadmin`.

Como está agregando un principal de servicio a un archivo keytab, el principal ya debe existir en la base de datos de Kerberos. En los servidores de aplicaciones que proporcionan servicios Kerberizados, el archivo keytab es `/etc/krb5/krb5.keytab` de manera predeterminada.

Un archivo keytab es análogo a la contraseña de un usuario. Al igual que los usuarios deben proteger sus contraseñas, los servidores de aplicaciones deben proteger 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.

Circunstancias especiales pueden requerir que agregue 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.

Atención - El montaje de los servidores NFS como `root` es un riesgo para la seguridad.

También puede utilizar el comando `ktutil` para administrar archivos keytab. Este comando interactivo le permite gestionar el archivo keytab de un host local sin tener privilegios de administración de Kerberos, porque este comando no interactúa con la base de datos de Kerberos como lo hace `kadmin`. Después de agregar un principal a un archivo keytab, puede usar `ktutil` para ver la lista de claves en un archivo keytab o para desactivar 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.

Agregación de un principal de servicio Kerberos a un archivo keytab

Puede agregar un principal a un archivo keytab después de asegurarse de que el principal existe en la base de datos de Kerberos. Para obtener más información, consulte “Visualización de los principales de Kerberos y sus atributos” [153].

En el host que requiere que se agregue un principal al archivo keytab, ejecute el comando `ktadd` en un proceso `kadmin`. Para obtener más información, consulte la página del comando man `kadmin`(1M).

```
# /usr/sbin/kadmin
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`.
-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 agregar al archivo keytab. Se pueden agregar los siguientes principales de servicio: `host`, `root`, `nfs` y `ftp`.
`-glob` *principal-exp*	Especifica las expresiones de principal. Todos los principales que coinciden con las *expresiones_principal* se agregan al archivo keytab. Las reglas de expresión de principal son las mismas que para el comando `list_principals` de `kadmin`. Para obtener expresiones posibles, revise la definición de `expression` en la página del comando man `kadmin`(1M).

EJEMPLO 5-15 Agregación de un principal de servicio a un archivo keytab

En este 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.
kadmin: quit
```

Eliminación de un principal de servicio de un archivo keytab

Puede eliminar un principal de un archivo keytab. En el host que requiere que se elimine un principal de su archivo keytab, primero debe ver la lista de principales. Consulte “Visualización de principales en un archivo keytab” [163].

A continuación, ejecute el comando `ktadd` en un proceso `kadmin`. Para obtener más información, consulte la página del comando man `kadmin`(1M).

```
# /usr/sbin/kadmin
```

```
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*.
`Todas`	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.

EJEMPLO 5-16 Eliminación de un principal de servicio de un archivo keytab

En este 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
```

Visualización de principales en un archivo keytab

En el host con el archivo keytab, ejecute el comando `ktutil`, lea el archivo keytab y, a continuación, enumere los principales. Los principales también se conocen como *keylist*.

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`.

EJEMPLO 5-17 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
```

Desactivación temporal de un servicio Kerberos en un host

En algunas ocasiones, es posible que necesite desactivar temporalmente el mecanismo de autenticación de un servicio, como `ssh` 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.

Nota - De manera predeterminada, la mayoría de los servicios necesitan autenticación. Si un servicio no requiere autenticación, la desactivación de la autenticación no tiene ningún efecto. El servicio todavía está disponible.

▼ Cómo desactivar temporalmente la autenticación de un servicio Kerberos en un host

El comando `ktutil` permite a un usuario sin privilegios `kadmin` desactivar un servicio. Este usuario también puede restaurar el servicio. Para obtener más información, consulte la página del comando man `ktutil`(1).

Antes de empezar Debe asumir el rol `root`. Para obtener más información, consulte “Uso de sus derechos administrativos asignados” de “Protección de los usuarios y los procesos en Oracle Solaris 11.2 ”.

1. **Guarde el archivo keytab actual en un archivo temporal.**

   Utiliza este archivo temporal para volver a activar la autenticación en Paso 9.

2. **En el host con el archivo keytab, inicie el comando `ktutil`.**

   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`.

   ```
   # /usr/bin/ktutil
   ```

3. **Lea el archivo keytab en la memoria intermedia de la lista de claves.**

```
ktutil: read_kt keytab
```

4. **Visualice la memoria intermedia de lista de claves.**

```
ktutil: list
```

Aparece la memoria intermedia de lista de claves actual. Anote el número de ranura para el servicio que desea desactivar.

5. **Para desactivar temporalmente un servicio de host, suprima el principal de servicio específico de la memoria intermedia de lista de claves.**

```
ktutil: delete_entry slot-number
```

Donde *slot-number* especifica el número de ranura del principal de servicio que se va a suprimir en la salida `list`.

6. **Escriba la memoria intermedia de lista de claves a un nuevo archivo keytab.**

```
ktutil: write_kt new-keytab
```

7. **Salga del comando `ktutil`.**

```
ktutil: quit
```

8. **Utilice el nuevo archivo keytab para desactivar la autenticación del principal.**

```
# mv new-keytab keytab
```

9. **(Opcional) Para volver a activar el servicio, copie el archivo keytab temporal nuevamente en su ubicación original.**

```
# cp original-keytab keytab
```

ejemplo 5-18 Desactivación temporal de un host de Kerberos

En este ejemplo, el servicio de `host` en el host `denver` está desactivado temporalmente. Para volver a activar el servicio de host en `denver`, el administrador copia el archivo keytab guardado en su ubicación original.

```
denver # cp /etc/krb5/krb5.keytab /etc/krb5/krb5.keytab.save
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/nodenverhost.krb5.keytab
ktutil: quit
denver # cp /etc/krb5/nodenverhost.krb5.keytab /etc/krb5/krb5.keytab
```

El host no está disponible hasta que el usuario copia el archivo guardado a su ubicación original.

```
denver # cp /etc/krb5/krb5.keytab.save /etc/krb5/krb5.keytab
```

♦ ♦ ♦ CAPÍTULO 6

Uso de aplicaciones de Kerberos

En este capítulo, se explica cómo utilizar los servicios y comandos basados en Kerberos que se proporcionan en Oracle Solaris. Ya debe estar familiarizado con estos comandos en sus versiones originales antes de leer sobre ellos aquí.

Debido a que este capítulo está destinado para los usuarios de aplicaciones, 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.

En este capítulo, se tratan los siguientes temas:

- “Gestión de tickets de Kerberos” [167]
- “Gestión de contraseñas de Kerberos” [170]
- “Comandos de usuario de Kerberos” [171]

Para obtener una descripción general de Kerberos, consulte Capítulo 2, Acerca del 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” [42].

En Oracle Solaris, Kerberos está integrado 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).

El comando `ssh` se puede configurar para reenviar copias de los tickets a otros hosts, por lo que no tiene que solicitar explícitamente los tickets para obtener acceso a esos hosts. Por motivos de seguridad, el administrador puede impedir esto. Para obtener más información, consulte el debate sobre el reenvío de agentes en la página del comando man `ssh`(1).

Para obtener información sobre las duraciones de los tickets, consulte “Duración de los tickets” [180].

Creación de un ticket de Kerberos

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 `ssh -l` para iniciar sesión en un sistema 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 6-1 Creación de un ticket de Kerberos

En este ejemplo, se muestra a un usuario, `kdoe`, que crea un ticket en su propio sistema.

```
% kinit
Password for kdoe@CORP.EXAMPLE.COM: xxxxxxxx
```

En este ejemplo, el usuario `kdoe` crea un ticket que tiene una validez de tres horas, con la opción `-l`.

```
% kinit -l 3h kdoe@EXAMPLE.ORG
Password for kdoe@EXAMPLE.ORG: xxxxxxxx
```

Visualización de tickets de Kerberos

No todos los tickets son similares. Por ejemplo, un ticket puede ser `forwardable`, otro ticket puede ser `postdated` y 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” [178], se describen los diferentes atributos que un ticket puede tener.

EJEMPLO 6-2 Visualización de tickets de Kerberos

En este ejemplo, se muestra que el usuario `kdoe` 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: kdoe@EXAMPLE.COM

Valid starting                Expires                Service principal
09 Feb 14 15:09:51  09 Feb 14 21:09:51  nfs/EXAMPLE.COM@EXAMPLE.COM
renew until 10 Feb 14 15:12:51, Flags: Fdi
```

El siguiente ejemplo muestra que el usuario `kdoe` tiene dos tickets que fueron `reenviados` (f) al host del usuario desde otro host. Los tickets también son `reenviables` (F).

```
% klist -f
Ticket cache: /tmp/krb5cc_74287
Default principal: kdoe@EXAMPLE.COM

Valid starting                Expires                Service principal
07 Feb 14 06:09:51  09 Feb 14 23:33:51  host/EXAMPLE.COM@EXAMPLE.COM
renew until 10 Feb 14 17:09:51, Flags: fF

Valid starting                Expires                Service principal
08 Feb 14 08:09:51  09 Feb 14 12:54:51  nfs/EXAMPLE.COM@EXAMPLE.COM
renew until 10 Feb 14 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: kdoe@EXAMPLE.COM

Valid starting                Expires                Service principal
07 Feb 14 06:09:51  09 Feb 14 23:33:51  krbtgt/EXAMPLE.COM@EXAMPLE.COM
renew until 10 Feb 14 17:09:51, Flags: FRIA
Etype(skey, tkt): AES-256 CTS mode with 96-bit SHA-1 HMAC
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 caché de credenciales, que destruye todas las credenciales y los tickets. Si bien la destrucción no suele ser necesaria, la ejecución de `kdestroy` reduce las posibilidades de que la caché 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, debe utilizar el comando `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 Oracle Solaris y una contraseña de Kerberos. Ambas contraseñas pueden ser iguales o pueden ser diferentes.

Modificación de la contraseña

Si el PAM se ha configurado correctamente, puede cambiar la contraseña de Kerberos de dos maneras.

- Utilice el comando `passwd`. Con el servicio Kerberos configurado, el comando `passwd` también solicita automáticamente una nueva contraseña de Kerberos.

  Al usar `passwd`, puede configurar las contraseñas de UNIX y Kerberos al mismo tiempo. Sin embargo, sólo puede cambiar una contraseña con `passwd` y dejar la otra contraseña sin modificar.

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.

- Use el comando `kpasswd`. `kpasswd` sólo cambia las contraseñas de Kerberos. Debe utilizar `passwd` si desea cambiar la contraseña de UNIX.

  Un uso principal de `kpasswd` es cambiar una contraseña para un principal de Kerberos que no es un usuario de UNIX válido. Por ejemplo, `jdoe/admin` es un principal de Kerberos, pero no es un usuario de UNIX real, por lo que debe utilizar `kpasswd` para cambiar la contraseña.

Después de cambiar la contraseña, esta debe propagarse a través de la red. Según el tamaño de la red de Kerberos, el tiempo que se necesita para la propagación puede variar entre unos minutos y 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.

La *política* de Kerberos define los criterios para las contraseñas. Puede definir una política para cada usuario o aplicar una política predeterminada. Para obtener información sobre políticas, consulte “Administración de las políticas de Kerberos” [158]. Para ver un ejemplo que muestra los criterios que se pueden definir para contraseñas de Kerberos, consulte Ejemplo 5-9, “Visualización de los atributos de una política de Kerberos”. Los caracteres de la contraseña son mayúsculas, minúsculas, números, puntuación y el resto de los caracteres.

Inicios de sesión remotos en Kerberos

Como en Oracle Solaris, Kerberos ofrece el comando `ssh` para el acceso remoto. Después de la instalación, el comando `ssh` es el único servicio de red que acepta solicitudes de red. Por lo tanto, otros servicios de red que se modifican para Kerberos, como `rlogin` y `telnet`, están desactivados. Para obtener más información, consulte “Programas de red de Kerberos” [47] y “Comandos de usuario de Kerberos” [171].

Comandos de usuario de Kerberos

El producto Kerberos V5 es un sistema *de inicio de sesión único*, lo que significa que tiene que escribir la contraseña sólo una vez al utilizar aplicaciones de red. Las aplicaciones Kerberos V5 realizan la autenticación y, opcionalmente, el cifrado para usted porque Kerberos se ha integrado en cada paquete de aplicaciones de red familiares existentes. Las aplicaciones

Kerberos V5 son versiones de aplicaciones de red UNIX existentes con las funciones de Kerberos agregadas.

Nota - En general, la aplicación `ssh` debe ser suficientes para sus necesidades de inicio de sesión remoto. Consulte la página del comando man `ssh`(1). Para obtener información sobre cómo activar una aplicación de red antigua, consulte “Programas de red de Kerberos” [47].

Para conocer las funciones de Kerberos en aplicaciones de red existente, consulte las páginas del comando man y, específicamente, las secciones `OPTIONS`:

- `ftp`(1)
- `rcp`(1)
- `rlogin`(1)
- `rsh`(1)
- `telnet`(1)

Al utilizar una aplicación Kerberizada para conectarse a un sistema remoto, la aplicación, el KDC y el sistema remoto realizan un conjunto de negociaciones rápidas. Cuando estas negociaciones están completas y la aplicación ha aprobado su identidad en su nombre para el host remoto, el host remoto le otorga acceso.

Para conocer ejemplos de uso de comandos de inicio de sesión remotos descartados, consulte “Uso de las aplicaciones de Kerberos (tareas)” en *Administración de Oracle Solaris 11.1: Servicios de seguridad*.

♦ ♦ ♦ CAPÍTULO 7

Referencia del servicio Kerberos

En este capítulo, se enumeran muchos de los archivos, comandos y daemons que forman parte del producto Kerberos.

En este capítulo, se aborda la siguiente información de referencia:

Archivos de Kerberos

Los siguientes archivos son utilizados por el servicio Kerberos.

`~/.gkadmin`	Valores predeterminados para la creación de nuevos principales en la interfaz gráfica de usuario de la administración de Kerberos.
`~/.k5login`	Lista de principales que otorgan acceso a una cuenta de Kerberos
`/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/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 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 del PAM
`/tmp/krb5cc_`*UID*	Caché de credenciales predeterminadas, donde *UID* es el UID decimal del usuario
`/tmp/ovsec_adm.`*xxxxxx*	Caché de credenciales temporales por la duración de la operación de cambio de contraseña, donde *xxxxxx* 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 log para `kadmind`
`/var/krb5/kdc.log`	Archivo log 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.ulog`	Log 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 `kprop_script` utiliza para la propagación
`/var/krb5/slave_datatrans_`*esclavo*	Archivo de volcado temporal que se crea cuando se realizan las actualizaciones completas del esclavo especificado
`/var/user/`*$USER*`/krb-warn.conf`	Advertencia de caducidad de ticket por usuario y archivo de configuración de renovación automática

Comandos de Kerberos

Los siguientes comandos se incluyen en el producto Kerberos. Los comandos se enumeran por su página del comando man.

`ftp`(1)	Aplicación de protocolo de transferencia de archivos
`kdestroy`(1)	Destruye los tickets de Kerberos
`kinit`(1)	Obtiene tickets de otorgamiento de tickets de Kerberos y los almacena en la caché
`klist`(1)	Muestra los tickets de Kerberos actuales
`kpasswd`(1)	Cambia una contraseña de Kerberos
`ktutil`(1)	Gestiona los archivos keytab de Kerberos
`kvno`(1)	Enumera los números de versión de clave para los principales de Kerberos
`rcp`(1)	Aplicación de copia de archivos remota
`rlogin`(1)	Aplicación de inicio de sesión remoto
`rsh`(1)	Aplicación de shell remota
`scp`(1)	Aplicación de copia de archivos remota y segura
`sftp`(1)	Aplicación de transferencia de archivos segura
`ssh`(1)	Shell seguro para el inicio de sesión remoto
`telnet`(1)	Aplicación `telnet` Kerberizado
`kprop`(1M)	Programa de propagación de bases de datos de Kerberos
`gkadmin`(1M)	Programa de interfaz gráfica de usuario de administración de bases de datos de Kerberos, que se utiliza para gestionar los principales y las políticas
`gsscred`(1M)	Gestiona las entradas de la tabla de `gsscred`
`kadmin`(1M)	Programa de administración de bases de datos de Kerberos remoto que se utiliza para gestionar los principales, las políticas y los archivos keytab

kadmin.local(1M)	Programa de administración de bases de datos de Kerberos local que se ejecuta en el KDC maestro y se utiliza para gestionar los principales, las políticas y los archivos keytab
kclient(1M)	Secuencia de comandos de instalación de cliente Kerberos que se utiliza con o sin un perfil de instalación
kdb5_ldap_util(1M)	Crea contenedores LDAP para las bases de datos de Kerberos
kdb5_util(1M)	Crea archivos intermedios y bases de datos de Kerberos
kdcmgr(1M)	Configura KDC maestros y esclavos de Kerberos
kproplog(1M)	Contiene un resumen de las entradas del log de actualización

Kerberos Daemons

Los siguientes daemons son utilizados por el producto Kerberos.

/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

Los siguientes términos de Kerberos 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* se suelen usar indistintamente. 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 una contraseña, que se asigna a cada principal de usuario y es conocida sólo para el usuario y el KDC. El otro tipo de clave 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 cuyas claves de sesión son 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
- Registro 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. El KDC emite el ticket integrado en una credencial. 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 que el servidor utiliza 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 de un ticket, un autenticador se utiliza sólo una vez, generalmente, 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” [168].

Los tickets pueden describirse con uno o más de los siguientes términos:

Reenviable/ reenviado
: 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 mientras está en el equipo de `jennifer`, `david` puede iniciar sesión en su propio equipo sin tener que obtener un ticket nuevo (y, por lo tanto, autenticarse nuevamente). Consulte el Ejemplo 6-1, “Creación de un ticket de Kerberos” para ver un ejemplo de un ticket reenviable.

Inicial
: 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 puede ser anterior.

No válido
: 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.

Posfechable/ posfechado
: 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.

Que admite proxy/ proxy
: A veces, es posible que necesite permitir que un principal de servicio realice una operación en su nombre. El nombre de principal del proxy debe especificarse cuando se crea el ticket. Oracle Solaris no admite proxy ni con tickets proxy.

  Un ticket que admite proxy es similar al ticket reenviable, excepto en que sólo es válido para un único servicio. Un ticket 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, suponga que 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” [168].

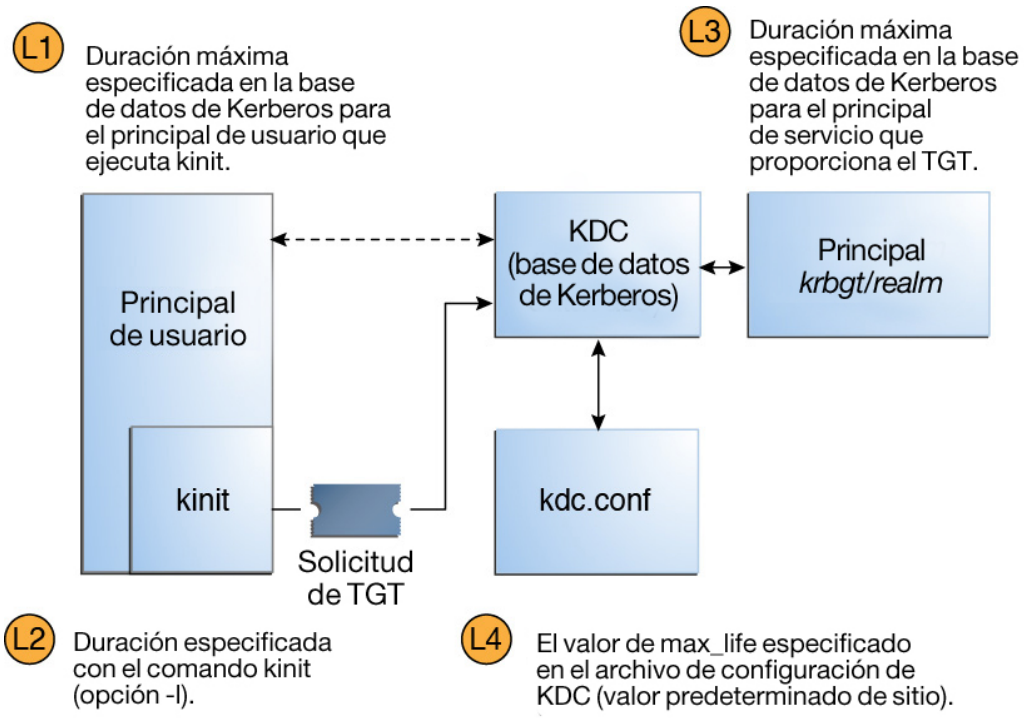
Duración de los tickets

Cuando 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` usa 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 siguiente muestra cómo se determina la duración de un TGT y dónde se originan los cuatro valores de duración. Cuando algún principal obtiene un ticket, la duración del ticket se determina de forma similar. Las únicas dos 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 7-1 Cómo se determina la duración de un TGT



La duración del ticket renovable se determina a partir del mínimo de los cuatro 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. Los siguientes ejemplos muestran los típicos nombres de principal:

`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 `kclient`.
`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 `kadmind`.
`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.
username`/admin@EXAMPLE.COM`	Un principal de `admin` que se puede utilizar para administrar la base de datos del KDC.

♦ ♦ ♦ CAPÍTULO 8

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.

En este capítulo, se tratan los siguientes temas:

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 Interfaz gráfica de usuario gkadmin

```
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: error de Java *
```

Causa: Existe un problema grave con la interfaz nativa de Java que utiliza la interfaz gráfica de usuario `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.

`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 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.

`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`*`' pre-authentication failed`

Causa: falló la autenticación para el principal.

Solución: asegúrese de que el usuario esté utilizando la contraseña correcta.

`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`.

`Communication failure with server while initializing kadmin interface`

Causa: el host que se especificó para el 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 caché de credenciales.

`Operación de E/S de caché de credenciales no satisfactoria` *`XXX`*

Causa: Kerberos tuvo un problema al escribir en la caché de credenciales del sistema (`/tmp/krb5cc_`*`uid`*).

Solución: asegúrese de que la caché 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 las dos condiciones siguientes:

- 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 el comando `klist -k` en el host de destino para asegúrese 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`.

`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 el comando `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.

`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.

`Invalid credential was supplied`

`Service key not available`

Causa: es posible que el ticket de servicio en la caché de credenciales sea incorrecto.

Solución: Destruya la caché de credenciales actual y vuelva a ejecutar el comando `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 reconoció 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.

`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: establezca `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 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 las contraseñas no están sincronizadas, debe especificar una contraseña diferente para completar la autenticación Kerberos. Es posible que el usuario haya olvidado su contraseña original.

`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.

O bien, 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 de configuración del PAM para `login` contiene 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 caché de credenciales.

Solución: Destruya los tickets con `kdestroy` y cree nuevos tickets con `kinit`.

`Message out of order`

Causa: mensajes que se enviaron cuando se utilizaba 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: la suma de comprobación calculada y la suma de comprobación de mensaje no coinciden. 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 y reinicialice los servicios Kerberos que utiliza.

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. De lo contrario, intente ejecutar el comando `kinit`.

```
No credentials were supplied, or the credentials were unavailable or inaccessible
No credential cache found
```

Causa: la caché 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 asignado en el archivo `kadm5.acl`.

Solución: utilice un principal que tenga los privilegios adecuados. O bien, configure el principal que se esté utilizando para que tenga los privilegios adecuados. 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.

```
Permission denied in replay cache code
```

Causa: no se pudo abrir la caché 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 caché de reproducción tenga los permisos adecuados. La caché de reproducción se almacena en el host donde la aplicación de servidor Kerberizada está en ejecución. El archivo de caché de reproducción se denomina `/var/krb5/rcache/`

`rc_`*service_name_uid* para usuarios no `root`. Para los usuarios root, el archivo caché de reproducción se denomina `/var/krb5/rcache/root/rc_`*service_name*.

`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.

`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 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.acl`, 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.

`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`

`El ticket y el autenticador no coinciden.`

Causa: 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.

`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.

Resolución de problemas de Kerberos

Esta sección proporciona información de resolución de problemas para el software de Kerberos.

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. Después de diagnosticar el problema, actualice el archivo `krb5.keytab`.

1. Enumere las entradas keytab .

   El KVNO para cada principal es el primer elemento de cada entrada.

```
# 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 log:

```
Improper format of Kerberos configuration file while initializing krb5 library
```

Si el formato es incorrecto, 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 son seguros de manera predeterminada, el comando `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, desactive el servicio `eklogin`.

```
# svcadm disable svc:/network/login:eklogin
```

Si el acceso remoto no funciona, es posible que los problemas se deban a los archivos keytab en los KDC. Si el acceso remoto 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.acl` 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/rcache/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 activado 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[1]:

  ```
  my.host.name.   A       1.2.3.4
  A       1.2.4.4
  A       1.2.5.4

  my-en0.host.name.       A       1.2.3.4
  my-en1.host.name.       A       1.2.4.4
  my-en2.host.name.       A       1.2.5.4

  4.3.2.1         PTR     my.host.name.
  4.4.2.1         PTR     my.host.name.
  4.5.2.1         PTR     my.host.name.
  ```

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.

[1]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.

Problemas de autenticación como usuario `root`

Si falla la autenticación cuando intenta convertir `root` en el sistema y ya ha agregado el principal `root` al archivo keytab del host, investigue dos áreas. 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, haga que el servicio `gssd` lea el archivo `/etc/gss/gsscred.conf`.

```
# pkill -HUP gssd
```

Ahora puede supervisar las asignaciones de credenciales a medida que `gssd` las solicite. Las asignaciones son registradas por el daemon `syslog` si el archivo `syslog.conf` está configurado para la utilidad de sistema `auth` con el nivel de gravedad `debug`.

Nota - Si la instancia del servicio `rsyslog` está activada, las asignaciones son registradas por el daemon `rsyslog`.

Uso de DTrace con el servicio Kerberos

El mecanismo Kerberos es compatible con varios sondeos de DTrace para decodificar varios mensajes de protocolo. Para obtener una lista, consulte Apéndice A, Sondeos de DTrace para Kerberos. Los sondeos de DTrace tienen una ventaja sobre otros inspectores de protocolos, ya que DTrace permite a un usuario con privilegios ver fácilmente los datos de Kerberos y de aplicación sin cifrar.

En los ejemplos siguientes se indica lo que se puede ver con los sondeos de DTrace de Kerberos.

EJEMPLO 8-1 Uso de DTrace para realizar un seguimiento de los mensajes de Kerberos

La siguiente secuencia de comandos utiliza sondeos de DTrace para visualizar detalles sobre los mensajes de Kerberos que envía y recibe el sistema. Tenga en cuenta que los campos

que aparecen se basan las estructuras que se asignan a los sondeos `krb_message-recv` y `krb_message-send` Para obtener más información, consulte “Definiciones de sondeos de DTrace de Kerberos” [220].

```
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_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");
}
```

La secuencia de comandos anterior se puede llamar desde la línea de comandos o con el daemon `krb5kdc`. A continuación se muestra un ejemplo de la llamada a la secuencia de comandos, que se denomina `krb-dtrace.d`, de la línea de comandos. El comando hace que Kerberos envíe y reciba mensajes. Tenga en cuenta que `LD_NOLAZYLOAD=1` es necesario para forzar la carga de la biblioteca `mech_krb5.so` de Kerberos que contiene los sondeos de DTrace de Kerberos.

```
# LD_NOLAZYLOAD=1 dtrace -s ./krb\-dtrace.d -c kinit
dtrace: script './krb-dtrace' matched 4 probes
kinit: Client 'root@DEV.ORACLE.COM' not found in Kerberos database while g
etting initial credentials
dtrace: pid 3750 has exited
 CPU     ID                    FUNCTION:NAME
   2  74782 k5_trace_message_send:krb_message-send -> krb message sent: KR
B_AS_REQ(10)
-> krb message remote addr: 10.229.168.163
-> krb message ports: local 62029 remote 88
-> krb message protocol: ipv4 transport: udp
```

```
   2  74781 k5_trace_message_recv:krb_message-recv <- krb message recved:
KRB_ERROR(30)
<- krb message remote addr: 10.229.168.163
<- krb message ports: local 62029 remote 88
<- krb message protocol: ipv4 transport: udp

   2  74776     krb5_rd_error:krb_error-read <- krb error code: KDC_ERR_C_
PRINCIPAL_UNKNOWN(6)
<- krb error client: root@DEV.ORACLE.COM server: krbtgt/DEV.ORACLE.COM@DEV
.ORACLE.COM
<- krb error e-text: CLIENT_NOT_FOUND
```

Para utilizar la secuencia de comandos con el daemon `krb5kdc`, el servicio `svc:/network/security/krb5kdc:default` debe estar activado y en línea. Tenga en cuenta que el siguiente comando no utiliza `LD_NOLAZYLOAD=1` porque la biblioteca `mech_krb5.so` carga el daemon `krb5kdc`.

```
# dtrace -s ./krb\-dtrace.d -p $(pgrep -x krb5kdc)
```

EJEMPLO 8-2 Uso de DTrace para ver los tipos de autenticación previa de Kerberos

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]->kdcrep_client,
args[1]->kdcrep_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 `krbtrace.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.

EJEMPLO 8-3 Uso de DTrace para volcar una mensaje de error de Kerberos

```
# dtrace -n 'krb_error-make {
printf("\n{");
printf("\n\tctime = %Y", (uint64_t)(args[1]->kerror_ctime * 1000000000));
printf("\n\tcusec = %d", args[1]->kerror_cusec);
printf("\n\tstime = %Y", (uint64_t)(args[1]->kerror_stime * 1000000000));
printf("\n\tsusec = %d", args[1]->kerror_susec);
```

```
printf("\n\terror_code = %s", args[1]->kerror_error_code);
printf("\n\tclient = %s", args[1]->kerror_client);
printf("\n\tserver = %s", args[1]->kerror_server);
printf("\n\te_text = %s", args[1]->kerror_e_text);
printf("\n\te_data = %s", "");
printf("\n}");
}'
dtrace: description 'krb_error-make ' matched 1 probe
CPU     ID                    FUNCTION:NAME
0  78307     krb5_mk_error:krb_error-make
{
ctime = 2012 May 10 12:10:20
cusec = 0
stime = 2012 May 10 12:10:20
susec = 319090
error_code = KDC_ERR_C_PRINCIPAL_UNKNOWN(6)
client = testuser@EXAMPLE.COM
server = krbtgt/EXAMPLE.COM@EXAMPLE.COM
e_text = CLIENT_NOT_FOUND
e_data =
}
```

EJEMPLO 8-4 Uso de DTrace para ver el ticket de servicio para un servidor SSH

```
# LD_PRELOAD_32=/usr/lib/gss/mech_krb5.so.1 dtrace -q -n '
kerberos$target:::krb_kdc_req-make {
printf("kdcreq_server: %s",args[1]->kdcreq_server);
}' -c "ssh local@four.example.com" -o dtrace.out
Last login: Wed Sep 10 10:10:20 2014
Oracle Solaris 11 X86    July 2014
$ ^D
# cat dtrace.out
kdcreq_server: host/four.example.com@EXAMPLE.COM
```

EJEMPLO 8-5 Uso de DTrace para ver la dirección y el puerto de un KDC no disponible cuando se solicita un TGT inicial

```
# LD_BIND_NOW=1 dtrace -q -n '
kerberos$target:::krb_message-send {
printf("%s:%d\n",args[1]->kconn_remote, args[1]->kconn_remoteport)
}' -c "kinit local4"

10.10.10.14:88
10.10.10.14:750
10.10.10.14:88
10.10.10.14:750
10.10.10.14:88
10.10.10.14:750
kinit(v5): Cannot contact any KDC for realm 'EXAMPLE.COM'
while getting initial credentials
```

EJEMPLO 8-6 Uso de DTrace para ver las solicitudes de los principales de Kerberos

```
# LD_BIND_NOW=1 dtrace -qs /opt/kdebug/mykdtrace.d \
-c 'kadmin -p kdc/admin -w test123 -q listprincs'
Authenticating as principal kdc/admin with password.
krb kdc_req msg type: KRB_AS_REQ(10)
krb kdc_req make client: kdc/admin@TEST.NET server:
kadmin/interop1.example.com@TEST.NET
krb message sent: KRB_AS_REQ(10)
krb message recved: KRB_ERROR(30)
Err code: KDC_ERR_PREAUTH_REQUIRED(25)
Err msg client: kdc/admin@TEST.NET server: kadmin/interop1.example.com@TEST.NET
Err e-text: NEEDED_PREAUTH
krb kdc_req msg type: KRB_AS_REQ(10)
krb kdc_req make client: kdc/admin@TEST.NET server:
kadmin/interop1.example.com@TEST.NET
krb message sent: KRB_AS_REQ(10)
krb message recved: KRB_AS_REP(11)
kadmin: Database error! Required KADM5 principal missing while
initializing kadmin interface
krb kdc_req msg type: KRB_AS_REQ(10)
krb kdc_req make client: kdc/admin@TEST.NET server:
kadmin/interop2.example.com@TEST.NET
krb message sent: KRB_AS_REQ(10)
krb message recved: KRB_ERROR(30)
Err code: KDC_ERR_S_PRINCIPAL_UNKNOWN(7)
Err msg client: kdc/admin@TEST.NET server: kadmin/interop2.example.com@TEST.NET
Err e-text: SERVER_NOT_FOUND
krb kdc_req msg type: KRB_AS_REQ(10)
krb kdc_req make client: kdc/admin@TEST.NET server:
kadmin/interop2.example.com@TEST.NET
```

La siguiente secuencia de comandos se utilizó para producir la salida anterior.

```
kerberos$target:::krb_message-recv
{
printf("krb message recved: %s\n", args[0]->krb_message_type);
}

kerberos$target:::krb_message-send
{
printf("krb message sent: %s\n", args[0]->krb_message_type);
}

kerberos$target:::krb_kdc_req-make
{
printf("krb kdc_req msg type: %s\n", args[0]->krb_message_type);
printf("krb kdc_req make client: %s server: %s\n", args[1]->kdcreq_client,
args[1]->kdcreq_server );
}

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("Err code: %s\n", args[1]->kerror_error_code);
printf("Err msg client: %s server: %s\n", args[1]->kerror_client,
args[1]->kerror_server);
printf("Err e-text: %s\n", args[1]->kerror_e_text);
}
```

♦ ♦ ♦ CAPÍTULO 9

Uso de autenticación simple y capa de seguridad

En este capítulo se incluye información sobre la autenticación sencilla y capa de seguridad (SASL).

Acerca de 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. 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 complementos
- 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

Referencia de SASL

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:

`crammd5.so.1`	CRAM-MD5, que admite sólo autenticación, no autorización.
`digestmd5.so.1`	DIGEST-MD5, que admite autenticación, integridad, privacidad y autorización.
`gssapi.so.1`	GSSAPI, que admite autenticación, integridad, privacidad y autorización. El mecanismo de seguridad GSSAPI requiere una infraestructura Kerberos en funcionamiento.
`plain.so.1`	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 `salauthd` 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:

`auto_transition`	Pasa al usuario automáticamente a otros mecanismos cuando el usuario realiza una autenticación de texto sin formato correcta.
`auxprop_login`	Muestra el nombre de los complementos de propiedad auxiliar que se van a utilizar.
`canon_user_plugin`	Selecciona el complemento canon_user que se va a utilizar.
`mech_list`	Muestra los mecanismos que la aplicación del servidor tiene permitido utilizar.
`pwcheck_method`	Muestra los mecanismos utilizados para verificar las contraseñas. Actualmente, `auxprop` es el único valor permitido.
`reauth_timeout`	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:

`plugin_list`	Muestra los mecanismos disponibles. No se utiliza porque la opción cambia el comportamiento de la carga dinámica de los complementos.
`saslauthd_path`	Define la ubicación de la puerta saslauthd, que se utiliza para la comunicación con el daemon `saslauthd`. El daemon `saslauthd` no se incluye en la versión de Oracle Solaris. Por lo tanto, esta opción tampoco está incluida.
`keytab`	Define la ubicación del archivo `keytab` usado por el complemento GSSAPI. Utilice la variable de entorno `KRB5_KTNAME` en su lugar para establecer la ubicación predeterminada de `keytab`.

Las siguientes son opciones que no se encuentran en Cyrus SASL. Sin embargo, se agregaron a la versión de Oracle Solaris:

`use_authid`	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.
`log_level`	Establece el nivel deseado de registro para un servidor.

♦ ♦ ♦ CAPÍTULO 10

Configuración de autenticación de servicios de red

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:

Acerca de RPC seguras

RPC segura (llamada al 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 a través de 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 las siguientes direcciones:

- Para configurar y administrar Secure NFS, consulte "Administración de sistema NFS seguro" de "Gestión de sistemas de archivos de red en Oracle Solaris 11.2 ".

Autenticación Kerberos

Kerberos es un sistema de autenticación desarrollado en el MIT. 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 [118].

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. El protocolo de hora de red (NTP) se puede utilizar para sincronizar los relojes. El software de dominio público NTP de la Universidad de Delaware se incluye en el software Oracle Solaris. La documentación está disponible en el sitio web de NTP Documentation.

Las claves públicas y privadas se almacenan en una base de datos 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.

Administración de autenticación con RPC segura

Al requerir autenticación para el uso de sistemas de archivos NFS montados, aumenta la seguridad de la red.

El siguiente mapa de tareas indica los procedimientos que configuran RPC segura para NIS y NFS.

TABLA 10-1 Mapa de tareas de la administración de autenticación con RPC segura

Tarea	Descripción	Para obtener instrucciones
1. Iniciar el servidor de claves.	Asegura que se puedan crear claves para que se puedan autenticar los usuarios.	Cómo reiniciar el servidor de claves RPC segura [213]
2. Configurar credenciales en un host NIS.	Asegura que el usuario `root` en un host se pueda autenticar en un entorno NIS.	Cómo configurar una clave Diffie-Hellman para un host NIS [214]
3. Otorgar una clave a un usuario NIS.	Permite que se autentique un usuario en un entorno NIS.	Cómo configurar una clave Diffie-Hellman para un usuario NIS [215]
4. Compartir archivos NFS con autenticación.	Permite a un servidor NFS proteger de manera segura los sistemas de archivos compartidos mediante la autenticación.	Cómo compartir archivos NFS con autenticación Diffie-Hellman [216]

▼ Cómo reiniciar el servidor de claves RPC segura

Antes de empezar Debe asumir el rol `root`. Para obtener más información, consulte “Uso de sus derechos administrativos asignados” de “Protección de los usuarios y los procesos en Oracle Solaris 11.2 ”.

1. **Verifique que el daemon `keyserv` esté en ejecución.**

```
# svcs \*keyserv\*
STATE    STIME   FMRI
disabled Dec_14  svc:/network/rpc/keyserv
```

2. **Active el servicio de servidor de claves si el servidor no está en línea.**

```
# svcadm enable network/rpc/keyserv
```

▼ Cómo configurar una clave Diffie-Hellman para un host NIS

Realice este procedimiento en cada host en el dominio NIS.

Antes de empezar Debe asumir el rol `root`. Para obtener más información, consulte “Uso de sus derechos administrativos asignados” de “Protección de los usuarios y los procesos en Oracle Solaris 11.2 ”.

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 -s name-service/switch setprop config/publickey = astring: "nis"
# svccfg -s name-service/switch:default refresh
```

c. Confirme el valor `publickey`.

```
# 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 10-1 Configuración de una nueva clave para `root` en un cliente NIS

En el siguiente ejemplo, un administrador con un perfil de derechos de seguridad de seguridad del servicio de nombres configura `earth` como un cliente NIS seguro.

```
# newkey -h earth
Adding new key for unix.earth@example.com
New Password: xxxxxxxx
Retype password: xxxxxxxx
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

Realice este procedimiento para cada usuario en el dominio NIS.

Antes de empezar Debe iniciar sesión en el servidor maestro NIS para generar una nueva clave para un usuario. Se debe tener asignado el perfil de derechos de seguridad del servicio de nombres. Para obtener más información, consulte “Uso de sus derechos administrativos asignados” de “Protección de los usuarios y los procesos en Oracle Solaris 11.2 ”.

1. **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.

2. **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 10-2 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: xxxxxxxx
Retype password: xxxxxxxx
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: xxxxxxxx
Please enter the login password for jdoe: xxxxxxxx
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 [214].

Para realizar esta tarea, debe convertirse en un administrador con el perfil de derechos de administración del sistema asignado. Para obtener más información, consulte “Uso de sus derechos administrativos asignados” de “Protección de los usuarios y los procesos en Oracle Solaris 11.2 ”.

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 *sistema de archivos*

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`.

♦ ♦ ♦ APÉNDICE A

Sondeos de DTrace para Kerberos

En este apéndice se describen los sondeos de DTrace y el argumento estructuras. Para ver ejemplos de su uso, consulte “Uso de DTrace con el servicio Kerberos” [199].

Sondeos de DTrace en Kerberos

Los *sondeos* son actividades de ubicaciones de programa a los que DTrace puede enlazar una solicitud para realizar un conjunto de acciones. Los sondeos se definirán e implantarán por un *proveedor*. Los proveedores de núcleo son módulos cargables que activan su sondeos para rastrear datos.

Estos sondeos son para el seguimiento definido estáticamente por el usuario (USDT). Los sondeos de USDT están diseñados para examinar el protocolo Kerberos en el espacio del usuario. No se proporcionan sondeos de núcleo para el seguimiento definido estáticamente.

Crea secuencia de comandos en las que sondeos de DTrace registran la información que desea, por ejemplo, una rastreo de la pila, un registro de hora o el argumento de una función. A medida que los sondeos se completan, DTrace recopila los datos de los sondeos y los reporta a usted. Si no especifica ninguna acción para un sondeo, DTrace registra cada vez que el sondeo se completa y en qué CPU.

Los sondeos de DTrace de Kerberos se modelan según los tipos de mensaje de Kerberos que se describen RFC4120: The Kerberos Network Authentication Service (V5) (http://www.ietf.org/rfc/rfc4120.txt). Los sondeos están disponibles para consumidores de `libkrb5/mech_krb5`, incluidas las aplicaciones que utilizan `mech_krb5` a `libgss`. Los sondeos se dividen entre la creación del mensaje y el consumo, y enviar y recibir. Para obtener más información sobre `libgss`, consulte la página del comando man `libgss`(3LIB).

Para utilizar los sondeos, debe especificar el proveedor de `kerberos`, el nombre de la sonda (por ejemplo `krb_message-recv`) y los argumentos. Para ver ejemplos, consulte “Uso de DTrace con el servicio Kerberos” [199].

Definiciones de sondeos de DTrace de Kerberos

Sondeos para KRB_AP_REP:

```
kerberos$pid:::krb_ap_rep-make
kerberos$pid:::krb_ap_rep-read

args[0]        krbinfo_t *
args[1]        kaprepinfo_t *
```

Sondeos para KRB_AP_REQ:

```
kerberos$pid:::krb_ap_req-make
kerberos$pid:::krb_ap_req-read

args[0]        krbinfo_t *
args[1]        kapreqinfo_t *
args[2]        kticketinfo_t *
args[3]        kauthenticatorinfo_t *
```

Sondeos para KRB_KDC_REP:

```
kerberos$pid:::krb_kdc_rep-make
kerberos$pid:::krb_kdc_rep-read

args[0]        krbinfo_t *
args[1]        kdcrepinfo_t *
args[2]        kticketinfo_t *
```

Sondeos para KRB_KDC_REQ:

```
kerberos$pid:::krb_kdc_req-make
kerberos$pid:::krb_kdc_req-read

args[0]        krbinfo_t *
args[1]        kdcreqinfo_t *
```

Sondeos para KRB_CRED:

```
kerberos$pid:::krb_cred-make
kerberos$pid:::krb_cred-read

args[0]        krbinfo_t *
args[1]        kcredinfo_t *
```

Sondeos para KRB_ERROR:

```
kerberos$pid:::krb_error-make
kerberos$pid:::krb_error-read

args[0]        krbinfo_t *
args[1]        kerrorinfo_t *
```

Sondeos para `KRB_PRIV`:

```
kerberos$pid:::krb_priv-make
kerberos$pid:::krb_priv-read

args[0]        krbinfo_t *
args[1]        kprivinfo_t *
```

Sondeos para `KRB_SAFE`:

```
kerberos$pid:::krb_safe-make
kerberos$pid:::krb_safe-read

args[0]        krbinfo_t *
args[1]        ksafeinfo_t *
```

Sondeos para el envío y la recepción de mensajes

```
kerberos$pid:::krb_message-recv
kerberos$pid:::krb_message-send

args[0]        krbinfo_t *
args[1]        kconninfo_t *
```

Estructuras de argumento de DTrace en Kerberos

En determinadas situaciones, los valores de algunos argumentos pueden ser `0` o estar vacíos. Las estructuras del argumento de Kerberos están diseñadas para ser consistentes con RFC4120: The Kerberos Network Authentication Service (V5) (http://www.ietf.org/rfc/rfc4120.txt).

Información del mensaje de Kerberos en DTrace

```
typedef struct krbinfo {
uint8_t krb_version;                /* protocol version number (5) */
string krb_message_type;            /* Message type (AS_REQ(10), ...) */
uint64_t krb_message_id;            /* message identifier */
uint32_t krb_message_length;        /* message length */
uintptr_t krb_message;              /* raw ASN.1 encoded message */
} krbinfo_t;
```

Nota - El protocolo Kerberos no tiene identificador de mensaje. El identificador `krb_message_id` es específico del proveedor Kerberos y está diseñado para enlazar mensajes entre los sondeos `make/read` y `send/recv`.

Información de conexión en Kerberos en DTrace

```
typedef struct kconninfo {
string kconn_remote;                /* remote host address */
string kconn_local;                 /* local host address */
uint16_t kconn_localport;           /* local port */
uint16_t kconn_remoteport;          /* remote port */
string kconn_protocol;              /* protocol (ipv4, ipv6) */
string kconn_type;                  /* transport type (udp, tcp) */
} kconninfo_t;
```

Información de autenticador de Kerberos en DTrace

```
typedef struct kauthenticatorinfo {
string kauth_client;                /* client principal identifier */
string kauth_cksum_type;            /* type of checksum (des-cbc, ...) */
uint32_t kauth_cksum_length;        /* length of checksum */
uintptr_t kauth_cksum_value;        /* raw checksum data */
uint32_t kauth_cusec;               /* client time, microseconds */
uint32_t kauth_ctime;               /* client time in seconds */
string kauth_subkey_type;           /* sub-key type (des3-cbc-sha1, ...) */
uint32_t kauth_subkey_length;       /* sub-key length */
uintptr_t kauth_subkey_value;       /* sub-key data */
uint32_t kauth_seq_number;          /* sequence number */
string kauth_authorization_data;    /* top-level authorization types
(AD-IF-RELEVANT, ... ) */
} kauthenticatorinfo_t;

typedef struct kticketinfo_t {
string kticket_server;              /* service principal identifier */
uint32_t kticket_enc_part_kvno;     /* key version number */
string kticket_enc_part_etype;      /* enc type of encrypted ticket */
string kticket_enc_flags;           /* ticket flags (forwardable, ...) */
string kticket_enc_key_type;        /* key type (des3-cbc-sha1, ...) */
uint32_t kticket_enc_key_length;    /* key length */
uintptr_t kticket_enc_key_value;    /* key data */
string kticket_enc_client;          /* client principal identifier */
string kticket_enc_transited;       /* list of transited Kerberos realms */
string kticket_enc_transited_type;  /* encoding type */
uint32_t kticket_enc_authtime;      /* time of initial authentication */
uint32_t kticket_enc_starttime;     /* ticket start time in seconds */
uint32_t kticket_enc_endtime;       /* ticket end time in seconds */
uint32_t kticket_enc_renew_till;    /* ticket renewal time in seconds */
string kticket_enc_addresses;       /* addresses associated with ticket */
string kticket_enc_authorization_data;  /* list of top-level auth types */
} kticketinfo_t;

typedef struct kdcreqinfo {
```

```
string kdcreq_padata_types;         /* list of pre-auth types */
string kdcreq_kdc_options;          /* requested ticket flags */
string kdcreq_client;               /* client principal identifier */
string kdcreq_server;               /* server principal identifier */
uint32_t kdcreq_from;               /* requested start time in seconds */
uint32_t kdcreq_till;               /* requested end time in seconds */
uint32_t kdcreq_rtime;              /* requested renewal time in seconds */
uint32_t kdcreq_nonce;              /* nonce for replay detection */
string kdcreq_etype;                /* preferred encryption types */
string kdcreq_addresses;            /* list of requested ticket addresses */
string kdcreq_authorization_data;   /* list of top-level auth types */
uint32_t kdcreq_num_additional_tickets; /* number of additional tickets */
} kdcreqinfo_t;

typedef struct kdcrepinfo {
string kdcrep_padata_types;         /* list of pre-auth types */
string kdcrep_client;               /* client principal identifier */
uint32_t kdcrep_enc_part_kvno;      /* key version number */
string kdcrep_enc_part_etype;       /* enc type of encrypted KDC reply */
string kdcrep_enc_key_type;         /* key type (des3-cbc-sha1, ...) */
uint32_t kdcrep_enc_key_length;     /* key length */
uintptr_t kdcrep_enc_key_value;     /* key data */
string kdcrep_enc_last_req;         /* times of last request of principal */
uint32_t kdcrep_enc_nonce;          /* nonce for replay detection */
uint32_t kdcrep_enc_key_expiration; /* expiration time of client's key */
string kdcrep_enc_flags;            /* ticket flags */
uint32_t kdcrep_enc_authtime;       /* time of authentication of ticket */
uint32_t kdcrep_enc_starttime;      /* ticket start time in seconds */
uint32_t kdcrep_enc_endtime;        /* ticket end time in seconds */
uint32_t kdcrep_enc_renew_till;       /* ticket renewal time in seconds*/
string kdcrep_enc_server;           /* server principal identifier */
string kdcrep_enc_caddr;            /* zero or more client addresses */
} kdcrepinfo_t;

typedef struct kapreqinfo {
string kapreq_ap_options;           /* options (use-session-key,... ) */
uint32_t kapreq_authenticator_kvno; /* key version number */
string kapreq_authenticator_etype;  /* enc type of authenticator */
} kapreqinfo_t;

typedef struct kaprepinfo {
uint32_t kaprep_enc_part_kvno;      /* key version number */
string kaprep_enc_part_etype;       /* enc type of encrypted AP reply */
uint32_t kaprep_enc_ctime;          /* client time in seconds */
uint32_t kaprep_enc_cusec;          /* client time, microseconds portion */
string kaprep_enc_subkey_type;      /* sub-key type */
uint32_t kaprep_enc_subkey_length;  /* sub-key length */
uintptr_t kaprep_enc_subkey_value;  /* sub-key data */
uint32_t kaprep_enc_seq_number;     /* sequence number */
} kaprepinfo_t;

typedef struct kerrorinfo {
uint32_t kerror_ctime;              /* client time in seconds */
uint32_t kerror_cusec;              /* client time, microseconds */
```

```
uint32_t kerror_stime;              /* server time in seconds */
uint32_t kerror_susec;              /* server time, microseconds */
string kerror_error_code;           /* error code (KRB_AP_ERR_SKEW, ...) */
string kerror_client;               /* client principal identifier */
string kerror_server;               /* server principal identifier */
string kerror_e_text;               /* additional error text */
string kerror_e_data;               /* additional error data */
} kerrorinfo_t;

typedef struct ksafeinfo {
uintptr_t ksafe_user_data;          /* raw application specific data */
uint32_t ksafe_timestamp;           /* time of sender in seconds */
uint32_t ksafe_usec;                /* time of sender, microseconds */
uint32_t ksafe_seq_number;          /* sequence number */
string ksafe_s_address;             /* sender's address */
string ksafe_r_address;             /* recipient's address */
string ksafe_cksum_type;            /* checksum type (des-cbc, ...) */
uint32_t ksafe_cksum_length;        /* length of checksum */
uintptr_t ksafe_cksum_value;        /* raw checksum data */
} ksafeinfo_t;

typedef struct kprivinfo {
uint32_t kpriv_enc_part_kvno;       /* key version number */
string kpriv_enc_part_etype;        /* enc type of encrypted message */
uintptr_t kpriv_enc_user_data;      /* raw application specific data */
uint32_t kpriv_enc_timestamp;       /* time of sender in seconds */
uint32_t kpriv_enc_usec;            /* time of sender, microseconds */
uint32_t kpriv_enc_seq_number;      /* sequence number */
string kpriv_enc_s_address;         /* sender's address */
string kpriv_enc_r_address;         /* recipient's address */
} kprivinfo_t;

typedef struct kcredinfo {
uint32_t kcred_enc_part_kvno;       /* key version number */
string kcred_enc_part_etype;        /* enc type of encrypted message */
uint32_t kcred_tickets;             /* number of tickets */
uint32_t kcred_enc_nonce;           /* nonce for replay detection */
uint32_t kcred_enc_timestamp;       /* time of sender in seconds */
uint32_t kcred_enc_usec;            /* time of sender, microseconds */
string kcred_enc_s_address;         /* sender's address */
string kcred_enc_r_address;         /* recipient's address */
} kcredinfo_t;
```

Glosario de seguridad

AES Estándar de cifrado avanzado. 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 principal de usuario como estándar gubernamental.

algoritmo Un algoritmo criptográfico. Se trata de un procedimiento informático establecido que realiza el cifrado o el hashing de una entrada.

algoritmo criptográfico Consulte algoritmo.

almacén de claves 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.

ámbito del servicio de nombres 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.

aplicación con privilegios Una aplicación que puede sustituir los controles del sistema. La aplicación comprueba los atributos de seguridad, como UID, GID, autorizaciones o privilegios específicos.

archivo de ticket Consulte caché de credenciales.

archivo intermedio 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.

archivo keytab 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.

archivos de auditoría Logs de auditoría binarios. Los archivos de auditoría se almacenan de manera independiente en un sistema de archivos de auditoría.

asignación de dispositivos 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.

atributos de seguridad Sustituciones a la política de seguridad que permiten que un comando administrativo se ejecute correctamente al ser ejecutado por un usuario que no sea un superusuario. En el modelo de superusuario, los programas `setuid root` y `setgid` 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 privilegios de núcleo y otros derechos reemplazan a los programas `setuid root` como atributos de seguridad. El modelo de privilegios es compatible con el modelo de superusuario, ya que el modelo de privilegios reconoce también los programas `setuid` y `setgid` como atributos de seguridad.

autenticación Proceso de verificación de la identidad reclamada de un principal.

autenticador Los clientes trasfieren 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.

autorización 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.

2. En la gestión de derechos de usuario, un derecho 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 operaciones que, de lo contrario, están prohibidas por la política de seguridad. Las autorizaciones se aplican en el nivel de aplicación del usuario, no en el núcleo.

blindaje La modificación de la configuración predeterminada del sistema operativo para eliminar las vulnerabilidades de seguridad inherentes al host.

Blowfish 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.

caché de credenciales Un espacio de almacenamiento (generalmente, un archivo) que contiene credenciales recibidas del KDC.

cifrado de clave privada En el cifrado de clave privada, el remitente y el receptor utilizan la misma clave para el cifrado. Consulte también cifrado de clave pública.

cifrado de clave pública 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 cifrado de clave privada.

clave de servicio 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 llave.

clave de sesión 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 llave.

clave privada 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 llave.

clave secreta Consulte clave privada.

cliente 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.

De manera más amplia, un host que: a) recibe una credencial de Kerberos y b) utiliza un servicio proporcionado por un servidor.

Informalmente, un principal que utiliza un servicio.

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.

confidencialidad Consulte privacidad.

conjunto básico 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.

conjunto de privilegios Una recopilación de privilegios. Cada proceso tiene cuatro conjuntos de privilegios que determinan si un proceso puede utilizar un privilegio determinado. Consulte límite definido, conjunto vigente, conjunto permitido y conjunto heredable.

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.

credential 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.

derechos Una alternativa al modelo de superusuario de todo o nada. La gestión de derechos de usuario y la gestión de derechos de proceso permiten a una organización dividir los privilegios de superusuario y asignarlos a usuarios o roles. Los derechos de Oracle Solaris se implementan como privilegios de núcleo, autorizaciones y la capacidad para ejecutar un proceso como un UID o GID determinado. Los derechos se pueden recopilar en un perfil de derechos y en un rol.

DES 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.

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@CORP.EXAMPLE.COM`, el dominio es `CORP.EXAMPLE.COM`. Consulte también nombre de principal.

DSA 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.

ECDSA Algoritmo de firma digital de curva elíptica. Un algoritmo de clave pública que se basa en matemáticas de curva elíptica. El tamaño de una clave ECDSA es significativamente menor que el tamaño de una clave pública DSA necesaria para generar una firma de la misma longitud.

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 derechos asignados, incluidos los derechos que anulan los valores predeterminados. Como resultado, un proceso puede realizar operaciones no autorizadas.

evento asíncrono de auditoría 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 salida y entrada de la PROM, y de inicio del sistema inicial son ejemplos de eventos asíncronos.

evento de auditoría no atribuible Un evento de auditoría cuyo iniciador no se puede determinar, como el evento AUE_BOOT.

evento síncrono de auditoría 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.

FQDN Siglas en inglés de Fully Qualified Domain Name, nombre de dominio completo. Por ejemplo, `central.example.com` (en lugar de simplemente `denver`).

frase de contraseña 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.

GSS-API 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 autenticación, integridad, privacidad.

host Un sistema al que se puede acceder a través de una red.

imagen de único sistema 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.

instancia 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 `host/central.example.com`. Para los principales de usuario, una instancia es opcional. Sin embargo, tenga en cuenta que `jdoe` y `jdoe/admin` son principales únicos. Consulte también nombre primario, nombre de principal, principal de servicio, principal de usuario.

integridad Un servicio de seguridad que, además de la autenticación del usuario, permite validar los datos transmitidos mediante una suma de comprobación criptográfica. Consulte también autenticación y privacidad.

KDC Centro de distribución de claves. Un equipo que tiene tres componentes Kerberos V5:

- Base de datos de claves y principal
- Servicio de autenticación
- Servicio de otorgamiento de tickets

Cada dominio tiene un KDC maestro y debe tener uno o varios KDC esclavos.

KDC esclavo 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 KDC, KDC maestro.

KDC maestro 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.

Kerberos Un servicio de autenticación, el protocolo utilizado por ese servicio o el código utilizado para implementar ese servicio.

La implementación de Kerberos en Oracle Solaris que está estrechamente basada en la implementación de Kerberos V5.

Aunque son técnicamente diferentes, "Kerberos" y "Kerberos V5" suelen utilizarse de forma indistinta en la documentación de Kerberos.

En la mitología griega, Kerberos (también escrito Cerberus) era un mastín feroz de tres cabezas que protegía las puertas de Hades.

kvno 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.

límite definido El límite exterior que indica qué privilegios están disponibles para un proceso y sus procesos secundarios.

Lista de control de acceso 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.

llave 1. Generalmente, uno de los dos tipos principales de claves:

- *Clave simétrica*: una clave de cifrado que es idéntica a la clave de descifrado. Las claves simétricas se utilizan para cifrar archivos.
- *Claves asimétrica* o *clave pública*: 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 *secreta*. La clave pública también se denomina clave *compartida* o clave *común*.

2. Una entrada (nombre de principal) en un archivo keytab. Consulte también archivo keytab.

3. En Kerberos, una clave de cifrado, que puede ser de tres tipos:

- *Clave privada*: una clave de cifrado que comparten un principal y el KDC, y que se distribuye fuera de los límites del sistema. Consulte también clave privada.

- *Clave de servicio*: esta clave tiene el mismo propósito que la clave privada, pero la utilizan servidores y servicios. Consulte también clave de servicio.
- *Clave de sesión*: 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 clave de sesión.

MAC 1. Consulte código de autenticación de mensajes (MAC).

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.

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.

MD5 Una función de hash criptográfica iterativa utilizada para autenticar mensajes, incluso las firmas digitales. Rivest desarrolló esta función en 1991. Su uso está descartado.

mecanismo 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.

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.

mecanismo de seguridad Consulte mecanismo.

minimización 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.

modelo de privilegios 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.

modelo de superusuario 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.

motor de análisis Una aplicación de terceros, que reside en un host externo, que examina un archivo para ver si contiene virus conocidos.

nombre de principal

1. El nombre de un principal, con el formato *nombre primario/instancia@DOMINIO*. Consulte también, instancia, nombre primario, dominio.

2. (RPCSEC_GSS API) Consulte principal de cliente, principal de servidor.

nombre primario

La primera parte de un nombre de principal. Consulte también instancia, nombre de principal, dominio.

NTP

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 desfase de reloj.

nueva autenticación

El requisito de proporcionar una contraseña para realizar una operación informática. Normalmente, las operaciones `sudo` requieren una nueva autenticación. Los perfiles de derechos autenticados pueden contener comandos que requieren una nueva autenticación. Consulte perfil de derechos autenticado.

objeto público

Un archivo que es propiedad del usuario `root` y que todos pueden leer, como cualquier archivo en el directorio `/etc`.

PAM

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.

perfil de derechos

Se conoce también como perfil. Una recopilación de sustituciones de seguridad que se puede asignar a un rol o a un usuario. Un perfil de derechos puede incluir autorizaciones, privilegios, comandos con atributos de seguridad y otros perfiles de derechos que se denominan perfiles complementarios.

perfil de derechos autenticado

Un perfil de derechos que requiere que el usuario o rol asignado escriba una contraseña antes de ejecutar una operación en el perfil. Este comportamiento es similar al comportamiento de `sudo`. El período de tiempo durante el cual la contraseña es válida es configurable.

pista de auditoría

La recopilación de todos los archivos de auditoría de todos los hosts.

política

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 asignen para su uso y que las contraseñas se cambien cada seis semanas.

Para la implementación de la política en áreas específicas de Sistema operativo Oracle Solaris, consulte política de auditoría, política en la estructura criptográfica, política de dispositivos, política de Kerberos, política de contraseñas y política de derechos.

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 derechos La política de seguridad que está asociada a un comando. Actualmente,`solaris` es la política válida para Oracle Solaris. La política `solaris` reconoce privilegios y una política de privilegio extendida, autorizaciones y atributos de seguridad `setuid`.

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 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 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 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 Consulte política de derechos.

políticas de red Los valores configurados por las utilidades de red para proteger el tráfico de red. Para obtener información sobre la seguridad de la red, consulte “Protección de la red en Oracle Solaris 11.2 ”.

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 servicio, principal de usuario.

2. (RPCSEC_GSS API) Consulte principal de cliente, principal de servidor.

principal admin Un principal de usuario con un nombre del tipo *nombre de usuario*`/admin` (como en `jdoe/admin`). Un principal admin puede tener más privilegios (por ejemplo, para modificar las políticas) que un principal de usuario común. Consulte también nombre de principal, principal de usuario.

principal de cliente (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 `rpc_gss_principal_t`.

principal de host 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 `ftp`, `rcp` o `rlogin`. Un ejemplo de un principal de host principal es `host/central.example.com@EXAMPLE.COM`. Consulte también principal de servidor.

principal de servicio 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 `ftp` y su instancia es el nombre de host completo del sistema que proporciona el servicio. Consulte también principal de host, principal de usuario.

principal de servidor (RPCSEC_GSS API) Un principal que proporciona un servicio. El principal de servidor se almacena como una cadena ASCII con el formato *servicio*`@`*host*. Consulte también principal de cliente.

principal de usuario 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, `jdoe` o `jdoe/admin`). También se conoce como instancia de usuario. Consulte también principal de servicio.

principio de privilegio mínimo Consulte privilegio mínimo.

privacidad 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 autenticación, integridad y servicio.

privilegio 1. En general, un poder o una capacidad para realizar una operación en un sistema informático que supera el poder de un usuario común. Los privilegios de superusuario son todos los derechos que se otorgan al superusuario. Una aplicación con privilegios o un usuario con privilegios o es una aplicación o un usuario al que se han concedido derechos adicionales.

2. Un derecho discreto en un proceso de un sistema Oracle Solaris. Los privilegios ofrecen un control más específico de los procesos que `root`. Los privilegios se definen y se aplican en el núcleo. A los privilegios también se los denomina *privilegios de proceso* o *privilegios de núcleo*. Para obtener una descripción completa de los privilegios, consulte la página del comando man `privileges`(5).

privilegio mínimo 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 root, que no tiene acceso a capacidades críticas como la lectura o escritura en archivos de sistema protegidos o la detención del equipo.

protocolo de Diffie-Hellman 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. Kerberos utiliza el protocolo Diffie-Hellman.

proveedor 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 *complementos*. Para ver ejemplos de consumidores, consulte consumidor.

proveedor de hardware 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 proveedor.

proveedor de software 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 proveedor.

QOP 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.

RBAC Control de acceso basado en roles, la función de gestión de derechos de usuario de Oracle Solaris. Consulte derechos.

reconocimiento de privilegios 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 man `privileges`(5).

red privada virtual (VPN) Una red que proporciona comunicaciones seguras al utilizar el cifrado y el establecimiento de túneles para conectar usuarios a través de una red pública.

relación Una variable de configuración o un vínculo definidos en los archivos `kdc.conf` o `krb5.conf`.

resumen Consulte resumen de mensaje.

resumen de mensaje 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.

rol Una identidad especial para ejecutar aplicaciones con privilegios que sólo los usuarios asignados pueden asumir.

RSA Método para la obtención de firmas digitales y criptosistemas de claves públicas. Dicho método lo describieron sus creadores, Rivest, Shamir y Adleman, en 1978.

SEAM El nombre de producto para la primera versión de Kerberos en los sistemas Solaris. Este producto se basa en la tecnología Kerberos V5 desarrollada en Massachusetts Institute of Technology. SEAM ahora se denomina servicio Kerberos. Continúa siendo levemente diferente a la versión del MIT.

Secure Shell Un protocolo especial para el inicio de sesión remoto seguro y otros servicios de red seguros a través de una red no segura.

separación de tareas Parte de la noción de privilegio mínimo. La separación de tareas impide que un usuario realice o apruebe todas las operaciones que permiten completar una transacción. Por ejemplo, en RBAC, 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.

servicio 1. Un recurso proporcionado a clientes de la red, a menudo, por más de un servidor. Por ejemplo, si ejecuta `rlogin` en el equipo `central.example.com`, ese equipo es el servidor que proporciona el servicio `rlogin`.

2. Un servicio de seguridad (ya sea de integridad o privacidad) que proporciona un nivel de protección más allá de la autenticación. Consulte también integridad y privacidad.

servicio de seguridad Consulte servicio.

servidor Un principal que proporciona un recurso a los clientes de la red. Por ejemplo, si ejecuta `ssh` en el sistema `central.example.com`, ese sistema es el servidor que proporciona el servicio `ssh`. Consulte también principal de servicio.

servidor de aplicaciones Consulte servidor de aplicaciones de red.

servidor de aplicaciones de red Un servidor que proporciona aplicaciones de red, como `ftp`. Un dominio puede contener varios servidores de aplicaciones de red.

sesgo 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`.

SHA1 Algoritmo de hash seguro. El algoritmo funciona en cualquier tamaño de entrada que sea inferior a 2^{64} para generar una síntesis del mensaje. El algoritmo SHA-1 es la entrada de DSA.

shell de perfil En la gestión de derechos, 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. Las versiones del shell de perfil corresponden a los shells disponibles en el sistema, como la versión `pfbash` de `bash`.

TGS Siglas en inglés de Ticket-Granting Service, servicio de otorgamiento de tickets. La parte del KDC que es responsable de emitir tickets.

TGT 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.

ticket 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 autenticador, credential, servicio y clave de sesión.

ticket de sustituto 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 ticket reenviable.

ticket inicial 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 `iniciales` 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).

ticket no válido 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 ticket posfechado.

ticket posfechado 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: 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 `renovable`, su duración suele definirse para que coincida con la duración total del ticket de otorgamiento de tickets. Consulte también, ticket no válido, ticket renovable.

ticket reenviable 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`, `david` puede iniciar sesión en su propio equipo sin tener que obtener un ticket nuevo (y, por lo tanto, autenticarse nuevamente). Consulte también ticket de sustituto.

ticket 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: 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.

tipo Históricamente, *tipo de seguridad* y *tipo de autenticación* 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.

tipo de seguridad Consulte tipo.

usuario con privilegios Un usuario a quien se le asignan derechos que se encuentran más allá de los derechos de un usuario común en un sistema informático. Consulte también usuarios de confianza.

usuarios de confianza Los usuarios que se ha decidido que pueden realizar tareas administrativas con cierto nivel de confianza. Normalmente, los administradores crean inicios de sesión para usuarios de confianza y asignan derechos administrativos que coinciden con el nivel de confianza y la capacidad de

los usuarios. Estos usuarios luego pueden ayudar a configurar y a mantener el sistema. También son denominados *usuarios con privilegios*.

índice

B

C

D

E

L

M

N

O

P

R

S

T

U

V