

Guía de administración de Oracle® ZFS Storage Appliance, versión OS8.8.x



Referencia: F39450-01
Agosto de 2021

Referencia: F39450-01

Copyright © 2009, 2021, Oracle y/o sus filiales.

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

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

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

U.S. GOVERNMENT END USERS: Oracle programs (including any operating system, integrated software, any programs embedded, installed or activated on delivered hardware, and modifications of such programs) and Oracle computer documentation or other Oracle data delivered to or accessed by U.S. Government end users are "commercial computer software" or "commercial computer software documentation" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, reproduction, duplication, release, display, disclosure, modification, preparation of derivative works, and/or adaptation of i) Oracle programs (including any operating system, integrated software, any programs embedded, installed or activated on delivered hardware, and modifications of such programs), ii) Oracle computer documentation and/or iii) other Oracle data, is subject to the rights and limitations specified in the license contained in the applicable contract. The terms governing the U.S. Government's use of Oracle cloud services are defined by the applicable contract for such services. No other rights are granted to the U.S. Government.

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

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

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

Este software o hardware y la documentación pueden proporcionar acceso a, o información sobre contenidos, productos o servicios de terceros. Oracle Corporation o sus filiales no son responsables y por ende desconocen cualquier tipo de garantía sobre el contenido, los productos o los servicios de terceros a menos que se indique otra cosa en un acuerdo en vigor formalizado entre Ud. y Oracle. Oracle Corporation y sus filiales no serán responsables frente a cualesquiera pérdidas, costos o daños en los que se incurra como consecuencia de su acceso o su uso de contenidos, productos o servicios de terceros a menos que se indique otra cosa en un acuerdo en vigor formalizado entre Ud. y Oracle.

Accesibilidad a la documentación

Para obtener información acerca del compromiso de Oracle con la accesibilidad, visite el sitio web del Programa de Accesibilidad de Oracle en <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc>.

Acceso a Oracle Support

Los clientes de Oracle que hayan adquirido servicios de soporte disponen de acceso a soporte electrónico a través de My Oracle Support. Para obtener información, visite <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info> O <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs> si tiene problemas de audición.

Contenido

Acerca de Oracle ZFS Storage Appliance	19
Características principales de Oracle ZFS Storage Appliance	20
Accesibilidad, diversidad e inclusión	20
Accesibilidad	20
Diversidad e inclusión	21
Protocolos admitidos	21
Servicios de datos de dispositivos	22
Disponibilidad de datos	22
Interfaz de usuario basada en explorador (BUI)	23
Íconos de red	32
Íconos del panel de control	32
Íconos de la barra de herramientas de análisis	33
Íconos de asignación de identidades	34
Exploradores admitidos	34
Interfaz de línea de comandos (CLI)	35
Contextos de la CLI	37
Propiedades de la CLI	43
Trabajo con secuencias de comandos de la CLI	45
Uso de comandos por lotes	46
Descripción de la creación de secuencias de comandos de la CLI	47
▼ Acceso al entorno de secuencias de comandos de la CLI	47
Descripción de las funciones incorporadas de la CLI	48
▼ Uso de la función Elementos secundarios	49
▼ Uso de la función Opciones	50
▼ Uso de las funciones de alertas personalizadas	51
▼ Uso de la función Obtener	51
▼ Uso de la función Lista	52
▼ Uso de la función Prop	55
▼ Uso de la función Ejecutar	57

Uso de las funciones para generación de salidas	57
Descripción de errores de secuencias de comandos de la CLI	58
Configuración del dispositivo	61
Configuración inicial del dispositivo	61
Configuración de clusters de dispositivos	62
Vista de configuración de clusters de la BUI	63
▼ Comprobación de estado de enlaces de cluster (CLI)	65
▼ Actualización de un dispositivo independiente a una configuración en clusters (BUI)	66
▼ Cierre de una configuración en clusters (BUI)	68
▼ Cierre de una configuración en clusters (CLI)	71
▼ Anulación de la configuración de un nodo de cluster	73
Terminología de clusters	74
Descripción de la agrupación en clusters	75
Estados de los controladores de cluster	75
E/S de interconexión del cluster	76
Gestión de recursos de clusters	78
Toma de control y failback en clusters	81
Cambios de configuración en un entorno en cluster	82
Consideraciones de la agrupación en clusters para almacenamiento	83
Consideraciones de la agrupación en clusters para redes	86
Interfaces IP locales privadas	88
Consideraciones de la agrupación en clusters para InfiniBand	89
Prevención de situaciones de cerebro dividido	92
Estimación y reducción del impacto de la toma de control	93
Configuración de red	96
Uso de la BUI para configurar las redes	97
Uso de la CLI para configurar la red	99
Configuración de enlaces de datos de red	99
Configuración de interfaces de red	104
Configuración de interfaces de gestión	110
Configuración de rutas múltiples de redes IP (IPMP)	117
Configuración de rendimiento y disponibilidad de red	121
Configuración de enrutamiento de red	121
Configuración del almacenamiento	127
▼ Creación de una agrupación de almacenamiento (BUI)	128

▼ Creación de una agrupación de almacenamiento (CLI)	132
▼ Importación de una agrupación de almacenamiento existente (BUI)	134
▼ Importación de una agrupación de almacenamiento existente (CLI)	135
▼ Configuración de una agrupación de almacenamiento solo con unidades flash (BUI)	137
▼ Configuración de una agrupación de almacenamiento solo con unidades flash (CLI)	139
▼ Agregación de un estante de discos a una agrupación de almacenamiento existente (BUI)	141
▼ Agregación de un estante de discos a una agrupación de almacenamiento existente (CLI)	143
▼ Agregación de un dispositivo de caché, log o un metadispositivo a una agrupación de almacenamiento existente (BUI)	145
▼ Agregación de un dispositivo de caché, log o un metadispositivo a una agrupación de almacenamiento existente (CLI)	147
▼ Eliminación de un dispositivo de caché o un dispositivo de log de una agrupación de almacenamiento existente (BUI)	149
▼ Eliminación de un dispositivo de caché o un dispositivo de log de una agrupación de almacenamiento existente (CLI)	150
▼ Desconfiguración de una agrupación de almacenamiento (BUI)	152
▼ Desconfiguración de una agrupación de almacenamiento (CLI)	153
▼ Cambio de nombre de una agrupación de almacenamiento (BUI)	154
▼ Cambio de nombre de una agrupación de almacenamiento (CLI)	155
▼ Limpieza manual de una agrupación de almacenamiento (BUI)	156
▼ Limpieza manual de una agrupación de almacenamiento (CLI)	157
▼ Limpieza programada de una agrupación de almacenamiento (BUI)	159
▼ Limpieza programada de una agrupación de almacenamiento (CLI)	160
▼ Visualización del estado de la agrupación y el dispositivo (BUI)	161
▼ Visualización del estado de la agrupación y del dispositivo (CLI)	163
Conceptos de agrupaciones de almacenamiento	164
Perfiles de datos para agrupaciones de almacenamiento	167
Configuración de copia de seguridad en la nube	171
Preparación para una copia de seguridad en la nube	173
Configuración de operaciones de restauración y copia de seguridad en la nube	175
Gestión del servicio de nube	194
Propiedades de nube	203
Descripción del estado del dispositivo	208

Panel de control de estado	208
Resumen de uso de agrupación	214
Resumen de uso de memoria	215
Panel de control de actividad de disco	215
Panel de control de la CLI	217
▼ Ejecución continua del panel de control	219
Configuración del panel de control de estado	219
▼ Modificación de las estadísticas de las actividades desplegadas	221
▼ Modificación de los umbrales de las actividades	222
Estado de NDMP	222
Estados de NDMP	224
Configuración de una red de área de almacenamiento (SAN)	224
▼ Configuración de modo de los puertos FC (BUI)	225
▼ Detección de puertos FC (BUI)	226
▼ Creación de grupos de iniciadores de FC (BUI)	228
▼ Asociación de un LUN con un grupo de iniciadores FC (BUI)	230
▼ Cambio de modo de los puertos FC (CLI)	231
▼ Detección de puertos FC (CLI)	231
▼ Creación de grupos de iniciadores de FC (CLI)	232
▼ Asociación de un LUN con un grupo de iniciadores FC (CLI)	233
▼ Asignación de alias a iniciadores y grupos de iniciadores mediante secuencias de comandos (CLI)	233
▼ Creación de una hoja de trabajo de análisis (BUI)	235
▼ Configuración de destinos iSER de SAN	236
▼ Agregación de un destino iSCSI con un IQN generado automáticamente (CLI)	239
▼ Agregación de un destino iSCSI con un IQN específico y autenticación RADIUS (CLI)	239
▼ Agregación de iniciador iSCSI con autenticación CHAP (CLI)	240
▼ Agregación de un grupo de destinos iSCSI (CLI)	241
▼ Agregación de un grupo de iniciadores iSCSI (CLI)	241
▼ Configuración de destinos SRP (BUI)	242
▼ Configuración de destinos SRP (CLI)	243
Descripción de SAN	244
Configuración de canal de fibra de SAN	246
Configuración de iSCSI de SAN	250
Configuración de iniciador iSCSI de SAN	252
Configuración de SRP de SAN	253

Terminología de SAN	255
Configuración de usuarios	257
▼ Agregación de un administrador o usuario (BUI)	258
▼ Agregación de un administrador o usuario (CLI)	260
▼ Cambio de una contraseña de usuario (BUI)	263
▼ Cambio de una contraseña de usuario (CLI)	264
▼ Edición de excepciones de un usuario (BUI)	264
▼ Edición de excepciones de un usuario (CLI)	265
▼ Agregación de un rol (BUI)	266
▼ Agregación de un rol (CLI)	267
▼ Edición de autorizaciones de un rol (BUI)	269
▼ Edición de autorizaciones de un rol (CLI)	270
▼ Agregación de un usuario que pueda ver solamente el panel de control (BUI)	271
▼ Agregación de un usuario que pueda ver solamente el panel de control (CLI)	271
▼ Determinación del usuario actual conectado	272
Descripción de usuarios y roles	273
Autorizaciones de usuarios	274
Administración de propiedades de usuario	278
Configuración de preferencias del dispositivo	280
▼ Definición de preferencias (BUI)	280
▼ Establecimiento de preferencias (CLI)	281
▼ Configuración de claves SSH públicas (BUI)	283
▼ Configuración de claves SSH públicas (CLI)	284
Propiedades de preferencias	285
Configuración de alertas	286
Agregación de acciones de alerta	287
Agregación de alertas de umbral	300
Configuración de certificados	303
▼ Creación de un certificado de servidor nuevo (BUI)	304
▼ Creación de un certificado de servidor nuevo (CLI)	306
▼ Carga de certificados de CA que no son raíz (BUI)	307
▼ Carga de certificados de CA que no son raíz (CLI)	308
▼ Visualización de detalles de certificados y CSR (BUI)	308
▼ Visualización de detalles de certificados y CSR (CLI)	309
▼ Destrucción de una CSR o un certificado (BUI)	311

▼ Destrucción de una CSR o un certificado (CLI)	311
▼ Configuración del certificado por defecto del dispositivo (BUI)	312
▼ Configuración del certificado por defecto del dispositivo (CLI)	312
▼ Carga de certificados de confianza (BUI)	313
▼ Carga de certificados de confianza (CLI)	313
▼ Visualización de detalles de certificados de confianza (BUI)	314
▼ Visualización de detalles de certificados de confianza (CLI)	314
▼ Destrucción de un certificado de confianza (BUI)	315
▼ Destrucción de un certificado de confianza (CLI)	315
▼ Asignación de un certificado a un servicio (BUI)	316
▼ Asignación de un certificado a un servicio (CLI)	316
HTTP con seguridad de transporte estricta	316
▼ Activación de HTTP con seguridad de transporte estricta (BUI)	317
▼ Activación de HTTP con seguridad de transporte estricta (CLI)	317
Configuración de cifrados y versiones de SSL/TLS	318
▼ Configuración de SSL/TLS (BUI)	318
▼ Configuración de SSL/TLS (CLI)	319
Configuración de la complejidad de contraseña	319
▼ Configuración de la complejidad de contraseña (BUI)	320
▼ Configuración de la complejidad de contraseña (CLI)	320
Propiedades de la complejidad de contraseña	321
Servicios de dispositivos	323
Gestión de servicios	324
▼ Visualización de un servicio en la BUI	324
▼ Selección de un servicio en la CLI	325
▼ Activación de un servicio (BUI)	325
▼ Activación de un servicio (CLI)	326
▼ Desactivación de un servicio (BUI)	326
▼ Desactivación de un servicio (CLI)	327
▼ Visualización de los estados de los servicios en la CLI	327
▼ Visualización de la ayuda de un servicio en la CLI	328
▼ Configuración de las propiedades de los servicios (BUI)	328
▼ Configuración de las propiedades de los servicios (CLI)	329
▼ Visualización de logs de servicio (BUI)	330
▼ Visualización de logs de servicio (CLI)	331
Lista de servicios de dispositivo disponibles	332

Puertos de servicio necesarios	334
Configurando servicios	335
Configuración de Active Directory	335
Configuración de DNS	341
Configuración de enrutamiento dinámico	351
Configuración de FTP	352
Configuración de HTTP	355
Configuración de HTTPS	362
Configuración de asignación de identidades	363
Configuración de IPMP	375
Configuración de iSCSI	376
Configuración de Kerberos	377
Configuración de LDAP	393
Configuración de NDMP	411
Configuración de NFS	423
Configuración de NIS	429
Configuración de NTP	430
Configuración de la asistencia técnica remota	434
Configuración de la API de RESTful	437
Configuración de etiquetas de servicio	438
Configuración de SFTP	438
Configuración de la migración shadow	442
Configuración de SMB	442
Configuración de SMTP	464
Configuración de SNMP	465
Configuración de SRP	469
Configuración de SSH	469
Configuración de Syslog	470
Configuración de identidad del sistema	476
Configuración de TFTP	477
Configuración de análisis de virus	478
Recursos compartidos y proyectos	483
▼ Creación de un proyecto (BUI)	484
▼ Creación de un proyecto (CLI)	485
▼ Edición de un proyecto (BUI)	485
▼ Edición de un proyecto (CLI)	486

▼ Cambio de nombre de un proyecto (BUI)	487
▼ Cambio de nombre de un proyecto (CLI)	487
▼ Supresión de un proyecto (BUI)	488
▼ Supresión de un proyecto (CLI)	488
▼ Creación de un sistema de archivos o un LUN en un proyecto (BUI)	489
▼ Creación de un sistema de archivos o un LUN en un proyecto (CLI)	490
▼ Edición de un sistema de archivos o un LUN (BUI)	492
▼ Edición de un sistema de archivos o un LUN (CLI)	492
▼ Cambio de nombre de un sistema de archivos o un LUN (BUI)	493
▼ Cambio de nombre de un sistema de archivos o un LUN (CLI)	494
▼ Movimiento de un sistema de archivos o un LUN a otro proyecto (BUI)	495
▼ Movimiento de un sistema de archivos o un LUN a otro proyecto (CLI)	495
▼ Supresión de un sistema de archivos o un LUN (BUI)	496
▼ Supresión de un sistema de archivos o un LUN (CLI)	497
▼ Configuración de cuotas de usuarios o grupos (BUI)	497
▼ Configuración de cuotas de usuarios o grupos (CLI)	498
Acerca de las agrupaciones de almacenamiento, los proyectos y los recursos compartidos	500
Propiedades de proyectos y recursos compartidos	502
Propiedades heredadas	503
Propiedades locales del LUN	511
Otras propiedades	512
Propiedades estáticas	513
Propiedades de proyecto	517
Propiedades de sistema de archivos	525
Propiedades de LUN	534
Gestión de espacio de recursos compartidos	539
Terminología de recursos compartidos	540
Gestión de espacio de sistemas de archivos y proyectos	541
Configuración de cuotas de usuarios o grupos	542
Trabajo con gestión de identidad	543
Trabajo con espacio de nombres del sistema de archivos	544
Estadísticas de uso del recurso compartido	546
Protocolos de recursos compartidos y proyectos	547
Protocolo NFS	547
Protocolo SMB	555
Protocolo HTTP	563

Protocolo FTP	563
Protocolo SFTP	563
Protocolo TFTP	564
Listas de control de acceso para sistemas de archivos	564
Acceso a directorio raíz	564
Comportamiento de la ACL en cambio de modo	566
Comportamiento de valores heredados de ACL	566
ACL de directorio raíz	568
Trabajo con esquemas	571
▼ Creación de esquemas (BUI)	571
▼ Creación de esquemas (CLI)	572
Propiedades de esquema	573
Migración shadow	575
Descripción de migración shadow	576
Creación de un sistema de archivos shadow	579
Gestión de la migración en segundo plano	579
Tratamiento de errores de migración	580
Seguimiento de una migración en curso	580
▼ Supervisión del progreso y de los errores de migración (BUI)	581
▼ Supervisión del progreso y de los errores de migración (CLI)	581
Cancelación de migración	583
Toma de instantáneas de sistemas de archivos shadow	584
Copias de seguridad de sistemas de archivos shadow	584
Replicación de sistemas de archivos shadow	584
Migración de sistemas de archivos locales	585
Uso de análisis de migración shadow	585
▼ Prueba de una posible migración shadow con la CLI	586
▼ Migración de datos desde un servidor NFS activo con la CLI	586
Instantáneas y clones	589
Gestión del espacio de instantáneas	591
▼ Toma de una instantánea (BUI)	592
▼ Toma de una instantánea (CLI)	593
▼ Programación de instantáneas (BUI)	594
▼ Programación de instantáneas (CLI)	595
▼ Configuración de una etiqueta de instantáneas programadas (BUI)	598

▼ Configuración de una etiqueta de instantáneas programadas (CLI)	599
▼ Visualización de instantáneas y programas (BUI)	599
▼ Visualización de instantáneas y programas (CLI)	600
▼ Edición de una política de retención de instantáneas (BUI)	601
▼ Edición de una política de retención de instantáneas (CLI)	602
▼ Eliminación de un programa de instantáneas (BUI)	603
▼ Eliminación de un programa de instantáneas (CLI)	604
▼ Visibilidad de un directorio de instantáneas del sistema de archivos (BUI)	605
▼ Visibilidad de un directorio de instantáneas del sistema de archivos (CLI)	606
▼ Acceso a un directorio oculto de instantáneas del sistema de archivos (CLI)	607
▼ Acceso a un directorio visible de instantáneas del sistema de archivos (CLI)	608
▼ Cambio de nombre de una instantánea (BUI)	608
▼ Cambio de nombre de una instantánea (CLI)	610
▼ Reversión de una instantánea (BUI)	611
▼ Reversión de una instantánea (CLI)	612
▼ Destrucción de una instantánea (BUI)	612
▼ Destrucción de una instantánea (CLI)	613
▼ Clonación de una instantánea (BUI)	615
▼ Clonación de una instantánea (CLI)	617
▼ Clonación de un clon	619
▼ Visualización de clones de una instantánea (BUI)	619
▼ Visualización de clones de una instantánea (CLI)	620
▼ Visualización del origen de un clon (BUI)	620
▼ Visualización del origen de un clon (CLI)	621
Replicación remota	623
▼ Flujo de trabajo de replicación remota	623
Configuración de la replicación remota	624
▼ Comprobación de la compatibilidad de origen y destino	625
▼ Configuración de interfaces de red y enrutamiento estático (BUI)	626
▼ Configuración de interfaces de red y enrutamiento estático (CLI)	628
▼ Creación de un destino de replicación (BUI)	629
▼ Creación de un destino de replicación (CLI)	631
▼ Creación de una acción de replicación (BUI)	632
▼ Creación de una acción de replicación (CLI)	636
▼ Configuración de retención de instantáneas automáticas en un destino (BUI)	638

▼ Configuración de retención de instantáneas automáticas en un destino (CLI)	639
▼ Envío manual de una actualización de replicación (BUI)	641
▼ Envío manual de una actualización de replicación (CLI)	642
▼ Configuración de replicación para una configuración en cluster	642
Configuración de replicación fuera de línea (BUI)	643
Configuración de replicación fuera de línea (CLI)	648
▼ Desactivación de la compresión de replicación (BUI)	659
▼ Desactivación de la compresión de replicación (CLI)	659
▼ Prueba de la conexión (BUI)	660
▼ Prueba de la conexión (CLI)	661
▼ Edición de un destino de replicación (BUI)	663
▼ Edición de un destino de replicación (CLI)	664
▼ Edición de una acción de replicación (BUI)	665
▼ Edición de una acción de replicación (CLI)	666
Supervisión de la replicación remota	666
▼ Supervisión del avance de la replicación (BUI)	667
▼ Supervisión del avance de la replicación (CLI)	668
▼ Supervisión de demoras de replicación y RPO (BUI)	669
▼ Supervisión de demoras de replicación y RPO (CLI)	670
Acciones de auditoría de replicación	672
▼ Configuración de alertas de inicio y de finalización de replicación (BUI)	673
▼ Configuración de alertas de inicio y de finalización de replicación (CLI)	674
Uso de análisis de replications	675
Gestión de paquetes de replicación	675
Gestión de instantáneas generadas por el usuario	677
▼ Cancelación de una actualización de replicación (BUI)	677
▼ Cancelación de una actualización de replicación (CLI)	678
▼ Clonación de un paquete de replicación (BUI)	679
▼ Clonación de un paquete de replicación (CLI)	684
▼ Clonación de una instantánea en un paquete de replicación (BUI)	687
▼ Clonación de una instantánea en un paquete de replicación (CLI)	691
▼ Corte de un paquete de replicación (BUI)	695
▼ Corte de un paquete de replicación (CLI)	696
▼ Edición de un paquete de replicación (BUI)	696
▼ Edición de un paquete de replicación (CLI)	697

▼ Desactivación de un paquete de replicación (BUI)	699
▼ Desactivación de un paquete de replicación (CLI)	699
Recuperación ante desastres con replicación remota	700
▼ Configuración de un destino de replicación en un sitio de recuperación (BUI)	700
▼ Conmutación de operaciones hacia el sitio de recuperación (BUI)	701
▼ Actualización del sitio de producción (BUI)	702
▼ Reversión de la replicación al sitio de producción (BUI)	703
▼ Configuración de un destino de replicación en un sitio de recuperación (CLI)	704
▼ Conmutación de operaciones hacia el sitio de recuperación (CLI)	704
▼ Actualización del sitio de producción (CLI)	706
▼ Reversión de la replicación al sitio de producción (CLI)	707
Conceptos de replicación remota	708
Terminología de replicación	710
Destinos de replicación	711
Acciones y paquetes de replicación	714
Propiedades de las acciones de replicación	716
Propiedades del paquete de replicación	723
Agrupaciones de almacenamiento de replicación	724
Replicación de proyectos frente a replicación de recursos compartidos	725
Autorizaciones de replicación	726
Replicación con deduplicación	727
Configuración de replicación para dispositivos agrupados en clusters	729
Ejemplo: Configuración de replicación para dispositivos agrupados en clusters	730
Instantáneas de replicación y coherencia de datos	737
Gestión de instantáneas de replicación	738
Configuraciones de iSCSI y replicación	741
Replicación reanudable	742
Alertas de replicación	742
Fallos de replicación	744
Replicación comprimida	746
Paquetes de replicación	747
Clonación de un recurso compartido o un paquete de replicación	748
Reversión a varios destinos	750
Replicación en cascada	768
Exportación de sistemas de archivos replicados	788

Corte de replicación	789
Reversión de la dirección de replicación	790
Dstrucción de un paquete de replicación	793
Copias de seguridad de réplicas de destino	793
Cifrado de datos	795
▼ Flujo de trabajo de cifrado de datos	796
▼ Configuración de cifrado de almacén de claves LOCAL (BUI)	797
▼ Configuración de cifrado de almacén de claves LOCAL (CLI)	799
▼ Configuración de cifrado de almacén de claves de OKM (BUI)	800
▼ Configuración de cifrado de almacén de claves de OKM (CLI)	802
▼ Configuración de cifrado de almacén de claves de KMIP (BUI)	803
▼ Configuración de cifrado de almacén de claves de KMIP (CLI)	806
▼ Creación de una agrupación cifrada (BUI)	810
▼ Creación de una agrupación cifrada (CLI)	812
▼ Cambio de clave de cifrado de agrupación (BUI)	814
▼ Cambio de clave de cifrado de agrupación (CLI)	815
▼ Creación de un proyecto cifrado (BUI)	816
▼ Creación de un proyecto cifrado (CLI)	817
▼ Cambio de clave de cifrado de un proyecto (BUI)	819
▼ Cambio de clave de cifrado de proyecto (CLI)	820
▼ Creación de sistemas de archivos o LUN cifrados (BUI)	821
▼ Creación de sistemas de archivos o LUN cifrados (CLI)	823
▼ Cambio de clave de cifrado de recurso compartido (BUI)	824
▼ Cambio de clave de cifrado de recurso compartido (CLI)	825
▼ Copia de seguridad de una clave LOCAL (BUI)	826
▼ Copia de seguridad de una clave LOCAL (CLI)	827
▼ Supresión de una clave de cifrado (BUI)	827
▼ Supresión de una clave de cifrado (CLI)	828
▼ Restauración de una clave LOCAL (BUI)	830
▼ Restauración de una clave LOCAL (CLI)	831
Propiedades de cifrado	832
Gestión de claves de cifrado	833
Almacén de claves de Oracle Key Manager (OKM)	834
Almacén de claves del protocolo de interoperabilidad de gestión de claves (KMIP)	835
Mantenimiento de claves	836

Descripción de los valores de claves de cifrado	836
Impacto del cifrado en el rendimiento	837
Ciclo de vida de clave de cifrado	838
Copia de seguridad, replicación y restauración de proyectos y recursos compartidos cifrados	838
Configuración de la propiedad heredada después de la restauración de la copia de seguridad	839
Flujos de trabajo de mantenimiento	841
Descripción de flujos de trabajo	842
Descripción de los parámetros de flujos de trabajo	843
Parámetros restringidos de flujos de trabajo	844
Parámetros de flujo de trabajo opcionales	845
Manejo de errores de flujo de trabajo	846
Validación de entradas de flujo de trabajo	847
Auditoría y generación de informes de ejecución de flujos de trabajo	848
Descripción de control de versiones de flujos de trabajo	850
Uso de los flujos de trabajo para acciones de alerta	852
Creación y publicación de alertas personalizadas dentro de un flujo de trabajo	853
Creación de una alerta personalizada	854
Publicación de una alerta personalizada	856
Uso de flujos de trabajo programados	858
Uso de flujo de trabajo programado	859
Codificación de programas de flujo de trabajo	860
Crear una hoja de trabajo basada en un tipo de unidad especificado	862
Carga y ejecución de flujos de trabajo con la BUI	864
▼ Descarga de flujos de trabajo mediante el uso de la CLI	865
▼ Mostrar flujos de trabajo mediante el uso de la CLI	866
▼ Ejecución de flujos de trabajo con la CLI	866
▼ Auditoría de flujos de trabajo mediante el uso de la CLI	867
Integración	869
Configuración de Oracle ZFS Storage Appliance para clientes de Oracle Database ...	869
Protocolo de almacenamiento inteligente de Oracle	870

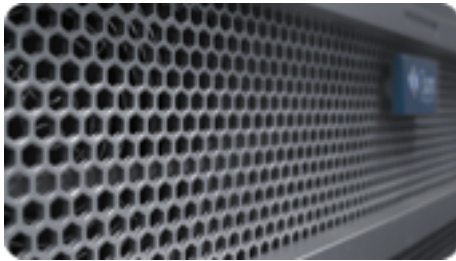
Acerca de Oracle ZFS Storage Appliance

La familia de productos Oracle ZFS Storage Appliance proporciona servicios eficaces de datos de bloque y archivos a clientes a través de una red, así como un conjunto enriquecido de servicios de datos que se pueden aplicar a los datos almacenados en el sistema.

Para obtener información sobre cómo configurar y trabajar con el producto Oracle ZFS Storage Appliance, consulte las siguientes secciones:

- [Características principales de Oracle ZFS Storage Appliance](#)
- [Accesibilidad, inclusión y diversidad](#)
- [Protocolos admitidos](#)
- [Servicios de datos de Oracle ZFS Storage Appliance](#)
- [Disponibilidad de datos](#)
- [Interfaz de usuario basada en explorador \(BUI\)](#)
- [Íconos de red](#)
- [Íconos de panel de control](#)
- [Íconos de la barra de herramientas de análisis](#)
- [Íconos de asignación de identidades](#)
- [Exploradores admitidos](#)
- [Interfaz de línea de comandos \(CLI\)](#)
- [Trabajo con secuencias de comandos de la CLI](#)

Características principales de Oracle ZFS Storage Appliance



Oracle ZFS Storage Appliance incluye tecnologías para brindar la mejor relación precio/rendimiento para el almacenamiento y una capacidad de observación sin precedentes de las cargas de trabajo en producción, como:

- DTrace Analytics, un sistema para observar de manera dinámica el comportamiento del sistema en tiempo real y visualizar los datos gráficamente.
- Agrupación de almacenamiento híbrido de ZFS, que está compuesta por dispositivos opcionales de memoria flash para la aceleración de las operaciones de lectura y escritura, discos de baja potencia y alta capacidad, y memoria DRAM, todos gestionados de manera transparente como una única jerarquía de datos.
- Compatibilidad con una variedad de hardware.

Para obtener más información sobre análisis y hardware, consulte la documentación en el [Centro de ayuda de Oracle \(https://docs.oracle.com/en/storage/\)](https://docs.oracle.com/en/storage/).

Accesibilidad, diversidad e inclusión

En esta sección, se documentan las características de accesibilidad de Oracle ZFS Storage Appliance y también el compromiso de Oracle con el uso de lenguaje étnica y culturalmente diverso e inclusivo.

Accesibilidad

La interfaz de línea de comandos (CLI) de Oracle ZFS Storage Appliance es una forma alternativa y equivalente de acceder a las características y la funcionalidad de la interfaz de

usuario basada en explorador (BLI). Como los sistemas operativos que se ejecutan en los sistemas Oracle ZFS Storage Appliance admiten tecnologías de asistencia para leer el contenido de la pantalla, puede usar la CLI como un medio equivalente de acceso a las utilidades basadas en colores, el mouse u otras características visuales que son parte de la BUI. Por ejemplo, puede usar un teclado para introducir comandos de la CLI a fin de identificar componentes de hardware defectuosos, comprobar el estado del sistema y supervisar el estado del sistema.

Oracle se esfuerza por permitir que los usuarios de la comunidad que tienen alguna discapacidad puedan acceder a los productos, servicios y la documentación que los acompaña, y utilizarlos. Con ese fin, los productos, los servicios y la documentación incluyen características que hacen que el producto sea accesible para los usuarios de tecnologías de asistencia. Para obtener más información acerca del compromiso de Oracle con la accesibilidad, visite el sitio web [Programa de accesibilidad de Oracle](#).

Diversidad e inclusión

Oracle asume un compromiso absoluto con la diversidad y la inclusión. Oracle respeta y valora el hecho de contar con una fuerza laboral diversa que aumenta el liderazgo en el pensamiento y la innovación. Como parte de nuestra iniciativa para crear una cultura más inclusiva que tenga un impacto positivo en nuestros empleados, clientes y socios, estamos trabajando para eliminar términos insensibles de nuestros productos y nuestra documentación. Además, somos conscientes de la necesidad de mantener la compatibilidad con la tecnología existente de nuestros clientes y la necesidad de garantizar la continuidad del servicio a medida que las ofertas y los estándares industriales de Oracle evolucionan. Debido a estas restricciones técnicas, nuestro esfuerzo para eliminar términos insensibles llevará tiempo y demandará cooperación externa.

Protocolos admitidos

Oracle ZFS Storage Appliance admite una variedad de protocolos de cliente estándar del sector, como NFS, iSCSI, SMB, FTP, HTTP, NDMP, canal de fibra, SRP, iSER y SFTP.

Para obtener información sobre estos protocolos, consulte las siguientes secciones:

- [“Configuración de canal de fibra de SAN” \[246\]](#)
- [Configuración de destinos iSER de SAN \[236\]](#)
- [“Configuración de NFS” \[423\]](#)
- [“Configuración de iSCSI” \[376\]](#)
- [“Configuración de SMB” \[442\]](#)

- [“Configuración de FTP” \[352\]](#)
- [“Configuración de HTTP” \[355\]](#)
- [“Configuración de NDMP” \[411\]](#)
- [“Configuración de SFTP” \[438\]](#)
- [“Configuración de SRP” \[469\]](#)

Servicios de datos de dispositivos

Para gestionar los datos que exporta con estos protocolos, puede configurar el dispositivo con la recopilación incorporada de servicios de datos avanzados, que incluyen:

- Configuración de disco RAID-Z (RAID-5 y RAID-6), reflejado y segmentado (consulte [“Configuración del almacenamiento” \[127\]](#))
- Instantáneas ilimitadas de solo lectura y de lectura y escritura, con programación de instantáneas (consulte [Instantáneas y clones \[589\]](#))
- Control de la eliminación de copias de datos duplicadas (consulte [“Desduplicación de datos” \[505\]](#))
- Compresión de datos integrada (consulte [“Compresión de datos” \[507\]](#))
- Replicación remota de datos para recuperación ante desastres (consulte [Replicación remota \[623\]](#))
- Agrupación en clusters activa-activa para alta disponibilidad (consulte [“Configuración de clusters de dispositivos” \[62\]](#))
- Aprovisionamiento fino de LUN iSCSI (consulte [“Configuración de iSCSI” \[376\]](#))
- Análisis de virus y cuarentena (consulte [“Configuración de análisis de virus” \[478\]](#))
- Copia de seguridad y restauración NDMP (consulte [“Configuración de NDMP” \[411\]](#))

Nota - La replicación y la clonación son características que se ofrecen con licencia para determinados modelos. Para obtener información detallada, consulte "Acuerdo de licencia de software (SLA) de Oracle y derecho de sistemas de hardware con opciones de software integrado" y el Manual de usuario de información sobre licencias para la versión de software.

Disponibilidad de datos

Para maximizar la disponibilidad de los datos en producción, el dispositivo incluye una arquitectura completa de extremo a extremo para proteger la integridad de los datos, con

redundancias en cada nivel de la pila. A continuación, se mencionan las características principales:

- Reparación automática predictiva y diagnóstico de todos los fallos de hardware del sistema: CPU, DRAM, tarjetas de E/S, discos, ventiladores, fuentes de alimentación.
- Totales de control de datos de ZFS de extremo a extremo para todos los datos y metadatos, lo que protege los datos en toda la pila.
- RAID-6 (paridad doble y triple) y RAID-6 opcional en los estantes de discos.
- Agrupación en clusters activa-activa para alta disponibilidad (consulte [“Configuración de clusters de dispositivos” \[62\]](#))
- Agregación de enlaces y rutas múltiples de IP para protección contra fallos en la red (consulte [“Configuración de red” \[96\]](#))
- Rutas múltiples de E/S entre el controlador y los estantes de discos
- Reinicio de software integrado en todos los servicios de software del sistema (consulte [Servicios de dispositivos \[323\]](#))
- Servicio de asistencia técnica remota para todos los problemas de software y hardware (consulte [“Configuración de la asistencia técnica remota” \[434\]](#))
- Gestión fuera de banda de cada sistema para control de encendido remoto y acceso a la consola.

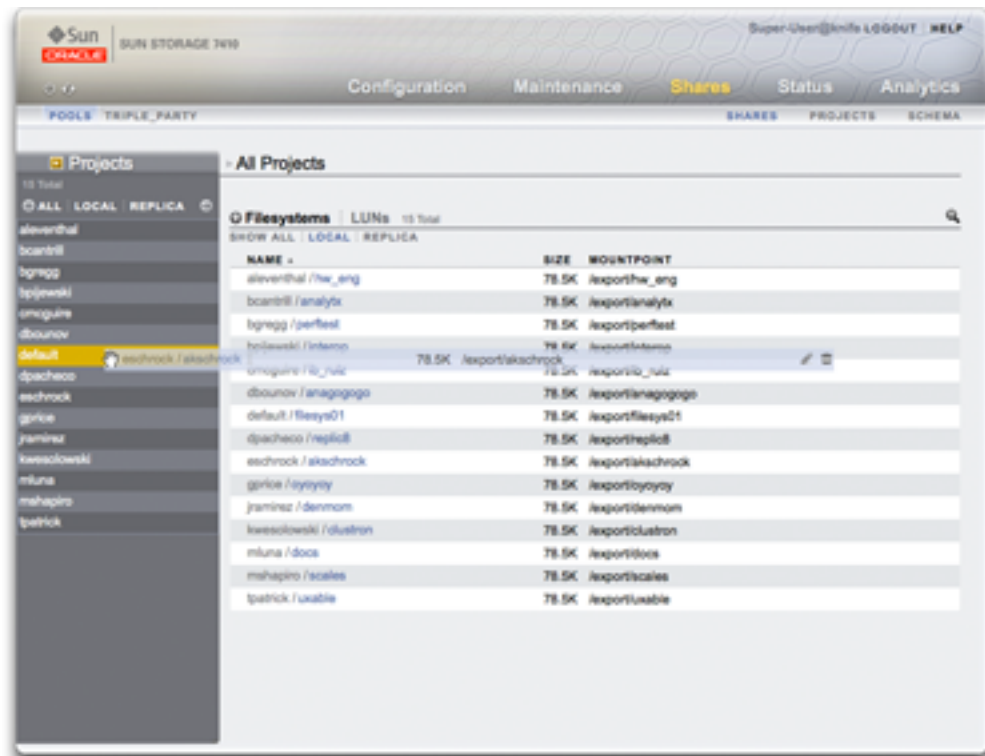
Interfaz de usuario basada en explorador (BUI)

La interfaz de usuario basada en explorador (BUI) del dispositivo Oracle ZFS Storage Appliance es la herramienta gráfica para la administración del dispositivo. La BUI proporciona un entorno intuitivo para las tareas de administración, la visualización de conceptos y el análisis de datos de rendimiento. La BUI proporciona un entorno que permite visualizar fácilmente el comportamiento del sistema e identificar problemas de rendimiento con el dispositivo.



Dirija el explorador al sistema mediante la *dirección IP* o el *nombre de host* asignado al puerto NET-0 durante la configuración inicial, de la siguiente manera: <https://ipaddress:215> o <https://hostname:215>. Aparece la pantalla de inicio de sesión.

La ayuda en pantalla cuyo enlace aparece en la esquina superior derecha de la BUI es contextual. Para cada pantalla principal y secundaria de la BUI, la página de ayuda asociada aparece al hacer clic en el botón Help (Ayuda).



Modificación de las propiedades de un sistema de archivos moviéndolo a otro proyecto mediante el panel lateral Projects (Proyectos).

La cabecera contiene varios elementos de la interfaz para navegación y notificaciones, además de funciones principales. A la izquierda, de arriba hacia abajo, se encuentran el logotipo de Sun/Oracle, un identificador del modelo de hardware y los botones de apagado y reinicio del hardware. Hacia la derecha, nuevamente de arriba hacia abajo: identificación de inicio de sesión, cerrar sesión, ayuda, navegación principal y navegación secundaria.

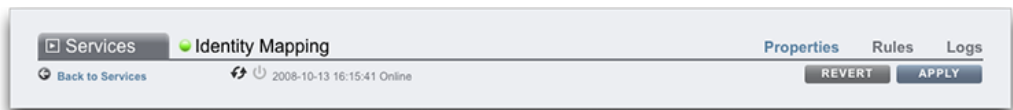


Cuando se activan, las alertas del sistema aparecen en la cabecera. Si se activan varias alertas en secuencia, consulte la lista de alertas recientes que aparece en la pantalla Panel de control o el registro completo disponible en la pantalla Registros.

Use los enlaces de navegación principal para alternar entre las áreas Configuración, Mantenimiento, Recursos compartidos, Estado y Análisis de la BUI. Use los enlaces de navegación secundaria para acceder a las características y funciones de cada área.

Si proporciona una anotación de sesión, aparece debajo de su ID de inicio de sesión y el control de cierre de sesión. Para cambiar la anotación de la sesión para las acciones administrativas posteriores sin cerrar sesión, haga clic en el enlace del texto. Para obtener detalles acerca de las anotaciones de sesión, consulte [“Configuración de usuarios” \[257\]](#).

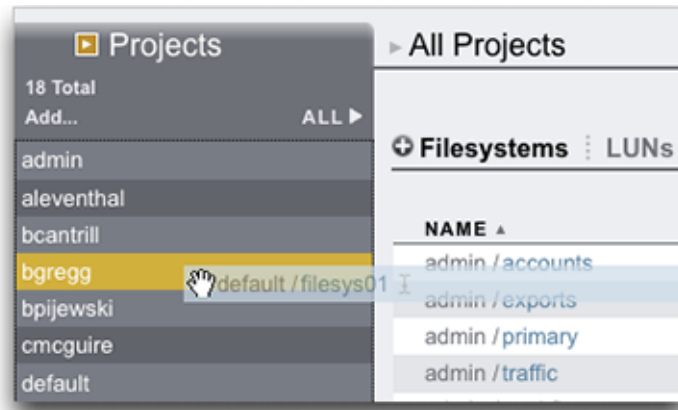
La barra de título aparece debajo de la cabecera y proporciona la función de navegación local y otras funciones que varían según la vista actual.



Por ejemplo, la barra de título del servicio Asignación de identidad activa las siguientes opciones:

- Navegación a la lista completa de servicios mediante el panel lateral
- Controles para activar o desactivar el servicio de asignación de identidad
- Una vista del tiempo de actividad de la asignación de identidad
- Navegación a las pantallas Properties (Propiedades), Rules (Reglas) y Logs (Registros) del servicio de asignación de identidad
- Botón para aplicar cambios de configuración hechos en la pantalla actual
- Botón para revertir cambios de configuración aplicados en la pantalla actual

Para alternar con rapidez entre las vistas de servicios y proyectos, abra y cierre el panel lateral; para ello, haga clic en el título o la flecha .



Para agregar proyectos, haga clic en el enlace Add (Agregar...) que se encuentra en la barra lateral.

Para mover recursos compartidos entre proyectos, haga clic en el ícono de movimiento  y arrastre el recurso compartido del sistema de archivos hasta el proyecto deseado en el panel lateral.

Tenga en cuenta que al arrastrar un recurso compartido a otro proyecto, se modifican las propiedades del recurso cuya configuración indique que se heredan del proyecto principal.

La mayoría de los controles de la BUI utilizan entradas de formularios web estándar, pero hay algunas excepciones que se deben tener en cuenta:

TABLA 1 Excepciones de pantalla web clave

Resumen de controles de la BUI	
Modificar una propiedad	Haga clic en el ícono de edición  y complete el cuadro de diálogo.
Agregar un elemento de lista o una entrada de propiedad	Haga clic en el ícono de agregación 
Quitar un elemento de lista o una entrada de propiedad	Haga clic en el ícono de eliminación 
Guardar cambios	Haga clic en el botón Aplicar.
Deshacer cambios guardados	Haga clic en el botón Revertir.
Suprimir un elemento de una lista	Haga clic en el ícono de la papelera  (deslice el puntero del mouse sobre la fila del elemento para ver el ícono).

Resumen de controles de la BUI	
Buscar un elemento en una lista	Haga clic en el ícono de búsqueda  que se encuentra en la parte superior derecha de la lista.
Ordenar por cabeceras de lista	Haga clic en las cabeceras secundarias en negrita para volver a ordenar la lista.
Mover o arrastrar un elemento	Haga clic en el ícono de movimiento . 
Renombrar un elemento	Haga clic en el ícono para cambiar nombre . 
Ver detalles del sistema	Consulte el logotipo de Oracle o haga clic en el identificador del modelo para ir a la página web oracle.com del modelo.
Abrir automáticamente el panel lateral	Arrastre un elemento al panel lateral.

Al configurar los permisos, se puede hacer clic en las casillas RWX. Al hacer clic en la etiqueta del grupo de acceso (User [Usuario], Group [Grupo], Other [Otro]), se alternan la activación y la desactivación de todos los permisos para esa etiqueta.



Para editar las propiedades de los recursos compartidos, quite la selección de la casilla de verificación Heredar del proyecto.

Properties ☒ Inherit from project

Mountpoint

Read only ☐

Update access time on read ☒

Non-blocking mandatory locking ☐

Data deduplication ☐

Data compression

Checksum

Cache device usage

Synchronous write bias

Database record size

Additional replication

Virus scan ☐

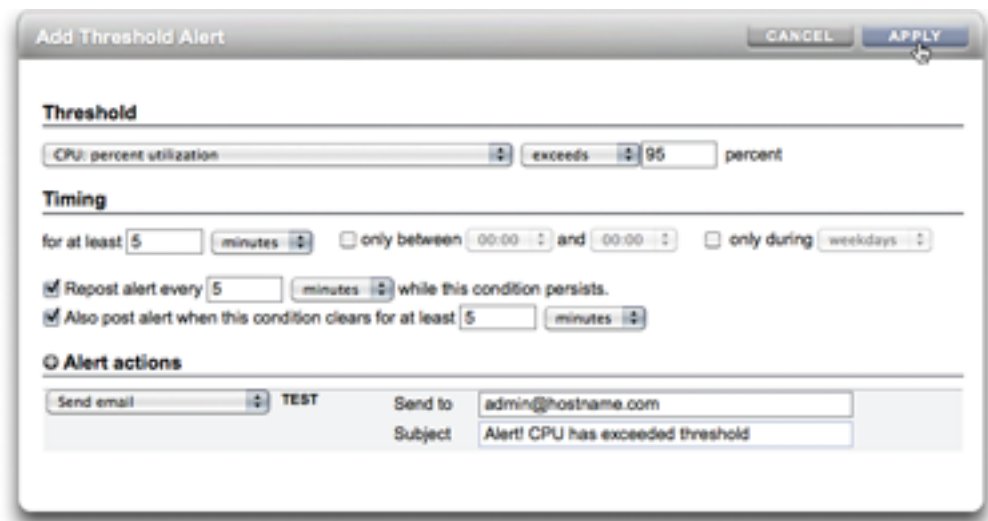
Para ver los controles de un elemento de una lista, deslice el puntero del mouse sobre la fila.

Filesystems LUNs 20 Total

SHOW ALL LOCAL REPLICA

NAME	SIZE	MOUNTPOINT
admin / accounts	78.5K	/export/accounts
admin / exports	78.5K	/export/exports
admin / primary	78.5K	/export/primary
admin / traffic	78.5K	/export/traffic
admin / workflow	78.5K	/export/workflow

Todos los cuadros de diálogo modales tienen títulos y botones que identifican y confirman o cancelan la acción actual que se encuentra en la parte superior y el contenido que se encuentra en la parte inferior. El área de contenido de modos sigue las mismas convenciones de interfaz que el área de contenido principal, pero se diferencia en que para poder realizar otras acciones se la debe descartar mediante los botones de la barra de título.



Los íconos indican el estado del sistema y brindan acceso a las funciones, y en la mayoría de los casos se utilizan como botones en los que se hace clic para realizar acciones. Puede pasar el puntero del mouse sobre los íconos de la interfaz para ver la pista. En las siguientes tablas, se proporciona una clave de las convenciones de la interfaz de usuario.

Las luces de estado son los indicadores básicos del estado del sistema y su mantenimiento:

TABLA 2 Indicadores de estado

Ícono	Descripción	Ícono	Descripción
	encendido		advertencia
	apagado		desactivado

Los siguientes íconos se encuentran en toda la interfaz de usuario y abarcan la mayoría de las funciones básicas:

TABLA 3 Íconos de la BUI

Ícono*		Descripción	Ícono*		Descripción
--		cambiar nombre (editar texto)	--		cortar
--		mover	--		clonar
		editar	--		revertir

ícono*		Descripción	ícono*		Descripción
		destruir	--		encender dispositivo
		agregar	--		aplicar
		eliminar	--		revertir
		cancelar/cerrar	--		información
--		error	--		ordenar columna de lista (en orden descendente)
--		alerta	--		ordenar columna de lista (en orden ascendente)
		alternar encendido/apagado			primera página
		reiniciar			página anterior
--		ubicar			página siguiente
		desactivar/sin conexión			última página
		bloquear	--		buscar
--		esperar			menú
--		revertir dirección			panel

* Los íconos desactivados se muestran a la izquierda.

Los siguientes íconos se usan para distinguir diferentes tipos de objetos y proporcionar información de importancia secundaria.

TABLA 4 Íconos varios

ícono	Descripción	ícono	Descripción
	permitir		SAS
	denegar		Puerto SAS
	agrupación de almacenamiento		

Íconos de red

Estos íconos indican el estado de los dispositivos de red y el tipo de enlaces de datos de la red:

TABLA 5 Íconos de red

Ícono	Descripción	Ícono	Descripción
	dispositivo de red activo		puerto InfiniBand activo
	dispositivo de red inactivo		puerto InfiniBand inactivo
	enlace de datos de red		Enlace de datos de red para una partición InfiniBand
	VLAN de enlace de datos de red		
	agregación de enlaces de datos de red		
	VLAN de agregación de enlaces de datos de red		

Íconos del panel de control

Los siguientes íconos indican el estado actual de las estadísticas supervisadas con respecto a los umbrales que puede configurar el usuario en Settings (Configuración).

TABLA 6 Íconos del panel de control

Ícono	Descripción	Ícono	Descripción
	soleado		huracán
	parcialmente nublado		huracán clase 2
	nublado		huracán clase 3
	lluvia		huracán clase 4
	tormenta		huracán clase 5

Íconos de la barra de herramientas de análisis

Este conjunto de íconos se usa en una barra de herramientas para manipular la manera en la que se despliega la información en las hojas de trabajo de Análisis.

TABLA 7 Íconos de la barra de herramientas de análisis

Ícono	Descripción	Ícono	Descripción
	atrás		mostrar mínimo
	adelante		mostrar máximo
	adelantar hasta ahora		mostrar gráfico de líneas
	pausar		mostrar gráfico de picos
	alejar		recortar valores atípicos
	acercar		sincronizar hoja de trabajo con esta estadística
	mostrar un minuto		anular sincronización de estadísticas de hoja de trabajo
	mostrar una hora		aumentar detalle
	mostrar un día		exportar datos estadísticos (descargar a cliente)
	mostrar una semana		guardar datos estadísticos
	mostrar un mes		archivar juego de datos
			enviar hoja de trabajo con paquete de asistencia

Para obtener más información sobre Análisis, consulte la documentación en [Oracle Technology Network \(https://docs.oracle.com/en/storage/\)](https://docs.oracle.com/en/storage/).

Íconos de asignación de identidades

Estos íconos indican el tipo de rol que se aplica al asignar usuarios y grupos entre Windows y UNIX.

TABLA 8 Íconos de asignación de identidades

ícono*	Descripción	ícono*	Descripción
	permitir Windows a UNIX		permitir UNIX a Windows
	denegar Windows a UNIX		denegar UNIX a Windows
	permitir bidireccional		

*Los íconos desactivados se muestran a la izquierda.

Temas relacionados

- [“Descripción del estado del dispositivo” \[208\]](#)
- [“Configuración de red” \[96\]](#)
- [“Configuración del almacenamiento” \[127\]](#)
- [“Configuración de alertas” \[286\]](#)
- [Servicios de dispositivos \[323\]](#)

Para obtener más información sobre Análisis, consulte la documentación en [Oracle Technology Network \(https://docs.oracle.com/en/storage/\)](https://docs.oracle.com/en/storage/).

Exploradores admitidos

En esta sección, se define la compatibilidad de los exploradores con la BUI.

La BUI incluye todas las características y funciones en los siguientes exploradores:

- Firefox 10 y posteriores
- Internet Explorer 9 y posteriores
- Safari 5 y posteriores
- Google Chrome 31 y posteriores

En los siguientes exploradores, los elementos de la BUI pueden aparecer con alguna imperfección visual, y algunas de las funciones pueden no estar disponibles, pero todas las

características necesarias funcionan correctamente. Durante el inicio de sesión, aparece un mensaje de advertencia si está utilizando uno de los siguientes exploradores:

- Firefox 6 a 9
- Internet Explorer 7 y 8
- Google Chrome 21 a 30
- Opera 23 y anteriores

Los siguientes exploradores son incompatibles, no se admiten y se sabe que tienen problemas; no permiten completar el inicio de sesión.

- Firefox 5 y anteriores
- Internet Explorer 6 y anteriores
- Google Chrome 20 y anteriores
- Safari 4 y anteriores
- Opera 22 y anteriores

Temas relacionados

- [“Configuración de usuarios” \[257\]](#)
- [“Configuración de preferencias del dispositivo” \[280\]](#)

Interfaz de línea de comandos (CLI)

La CLI está diseñada para imitar las capacidades de la BUI y, a su vez, proporcionar un entorno de scripts eficaz para realizar tareas repetitivas. La línea de comandos es una herramienta eficaz y potente para tareas administrativas repetitivas. El dispositivo presenta una CLI que está disponible desde la consola o el SSH. Hay varias situaciones en las que es preferible interactuar con el sistema mediante la CLI:

- **Red no disponible:** si la red no está disponible, es imposible la gestión basada en explorador. En este caso, el único vector para la gestión es la consola, que permite el uso de interfaces basadas en texto solamente.
- **Conveniencia:** el inicio de un explorador puede resultar poco eficaz en cuanto al tiempo necesario para hacerlo, especialmente si se desea examinar solo algún aspecto en particular del sistema o se desea hacer un cambio de configuración rápido.
- **Precisión:** en algunas situaciones, la información proporcionada por el explorador puede ser de naturaleza más cualitativa que cuantitativa, y tal vez se necesite una respuesta más exacta.
- **Automatización:** la interacción basada en explorador no se puede automatizar con facilidad; si hay que llevar a cabo tareas repetitivas o de definición rígida, se pueden ejecutar secuencias de comandos para realizarlas.

- **Accesibilidad:** la CLI es una manera alternativa, y equivalente, de acceder a las características y la funcionalidad de la BUI. Como los sistemas operativos que se ejecutan en los sistemas Oracle ZFS Storage Appliance admiten tecnologías de asistencia para leer el contenido de la pantalla, puede usar la CLI como un medio equivalente de acceso a las utilidades basadas en colores, el mouse u otras características visuales que son parte de la BUI. Por ejemplo, puede usar un teclado para introducir comandos de la CLI a fin de identificar componentes de hardware defectuosos, comprobar el estado del sistema y supervisar el estado del sistema.

Oracle se esfuerza por permitir que los usuarios de la comunidad que tienen alguna discapacidad puedan acceder a los productos, servicios y la documentación que los acompaña, y utilizarlos. Con ese fin, los productos, los servicios y la documentación incluyen características que hacen que el producto sea accesible para los usuarios de tecnologías de asistencia. Para obtener más información acerca del compromiso de Oracle con la accesibilidad, visite el [sitio web del Programa de Accesibilidad de Oracle \(http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc\)](http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc).

Al navegar por la CLI, hay dos principios que se deben tener en cuenta:

- **La finalización con tabulación se utiliza en gran medida:** si no sabe con certeza qué es lo que debe escribir en un contexto dado, pulse la tecla de tabulación para ver las opciones posibles. En toda la documentación, la acción de pulsar la tecla de tabulación se indica con la palabra "tab" en cursiva y negrita.
- **Siempre hay ayuda disponible:** el comando `help` proporciona ayuda específica para el contexto. Para obtener ayuda sobre un tema en particular, especifique el tema como argumento de `help`, por ejemplo `help commands`. Para ver los temas disponibles, finalice con tabulación el comando `help` o escriba `help topics`.

Puede combinar estos dos principios de la siguiente manera:

```
hostname:> help tab
builtins      commands      general      help          properties    script
```

Para iniciar sesión de manera remota mediante la CLI, use un cliente `ssh`. Si no ha seguido las instrucciones en “[Configuración de usuarios](#)” [257] para administrar el dispositivo, deberá iniciar sesión como usuario `root`. Cuando inicie sesión, la CLI mostrará un indicador, que es el nombre de host seguido por dos puntos y por el signo mayor que:

```
$ ssh root@hostname
Password:
Last login: Mon Oct 14 15:43:05 2019 from kiowa.sf.fishpo
hostname:>
```

Temas relacionados

- “[Interfaz de usuario basada en explorador \(BUI\)](#)” [23]
- “[Contextos de la CLI](#)” [37]
- “[Propiedades de la CLI](#)” [43]

Contextos de la CLI

Uno de los principios centrales de la CLI es el *contexto* en el que se ejecutan los comandos. El contexto dicta cuáles son los elementos del sistema que se pueden gestionar y cuáles son los comandos que están disponibles. Los contextos tienen una estructura de árbol en la que los contextos en sí pueden contener otros contextos anidados y la estructura por lo general refleja la de las vistas de la BUI.

El contexto inicial al iniciar sesión es el *contexto raíz*, que actúa como contexto principal o ascendiente de todos los contextos. Para navegar a un contexto, ejecute el nombre del contexto como comando. Por ejemplo, las funciones disponibles en la vista Configuración del explorador están disponibles en el contexto `configuration` de la CLI. Para tener acceso, desde el contexto raíz, escriba directamente lo siguiente:

```
hostname:> configuration
hostname:configuration>
```

Tenga en cuenta que el indicador cambia para reflejar el contexto, y el contexto se proporciona entre los dos puntos y el signo mayor que del indicador.

El comando `show` muestra los contextos secundarios. Por ejemplo, desde el contexto `configuration`:

```
hostname:configuration> show
Children:
    net => Configure networking
    services => Configure services
    version => Display system version
    users => Configure administrative users
    roles => Configure administrative roles
    preferences => Configure user preferences
    alerts => Configure alerts
    storage => Configure Storage
```

Estos contextos secundarios corresponden a las vistas disponibles en la vista Configuración del explorador, que incluye Red, Servicios, Usuarios, Preferencias, etc. Para seleccionar uno de estos contextos secundarios, escriba el nombre correspondiente:

```
hostname:configuration> preferences
hostname:configuration preferences>
```

Puede navegar a un contexto descendiente directamente desde uno ascendiente; para ello, especifique los contextos intermedios separados por espacios. Por ejemplo, para navegar directamente a `configuration preferences` desde el contexto raíz, simplemente escríbalo:

```
hostname:> configuration preferences
hostname:configuration preferences>
```

Algunos contextos secundarios son *dinámicos* porque corresponden no a vistas fijas del explorador, sino a entidades dinámicas que fueron creadas por el usuario o el sistema. Se puede navegar hasta estos contextos de dos maneras: puede usar el comando `select` seguido

del nombre del contexto dinámico, o puede encerrar el nombre del contexto dinámico entre comillas dobles. Los nombres de los contextos dinámicos incluidos en un contexto dado se muestran con el comando `list`. Por ejemplo, el contexto `users` es estático, pero cada usuario es su propio contexto dinámico.

```
hostname:> configuration users
hostname:configuration users> list
NAME                USERNAME                UID      TYPE
John Doe            bmc                    12345    Dir
Super-User          root                   0        Loc
```

Para seleccionar el usuario llamado `bmc`, ejecute el comando `select bmc` o `"bmc"`:

```
hostname:configuration users> "bmc"
hostname:configuration users bmc>
```

De manera alternativa, se pueden utilizar las comillas dobles, y los comandos `select` y `destroy` para seleccionar una entidad en función de sus propiedades en algunos contextos. Por ejemplo, se puede ejecutar el siguiente comando para seleccionar las entradas de log emitidas por el módulo `reboot` del contexto `maintenance logs system`:

```
hostname:maintenance logs system> select module=reboot
hostname:maintenance logs system entry-034> show
Properties:
  timestamp = 2019-10-14 06:24:41
  module = reboot
  priority = crit
  text = initiated by root on /dev/console syslogd: going down on signal 15
```

Como con otros comandos, se puede agregar `select` o comillas dobles a un comando de modificación de contexto. Por ejemplo, para seleccionar el usuario llamado `bmc` desde el contexto raíz:

```
hostname:> configuration users select bmc
hostname:configuration users bmc>
```

Use el comando `last` para navegar hasta un contexto creado o seleccionado con anterioridad. En el siguiente ejemplo, se crea una acción de replicación y, a continuación, se usan los comandos `last` y `get id` para recuperar el ID de la acción de replicación. Luego, se selecciona una acción diferente y se usan los comandos `last` y `get id` para recuperar el ID de la acción de replicación más recientemente visitada.

Con el comando `last`, se puede volver al último nodo visitado:

```
hostname:configuration net interfaces> "igb4"
hostname:configuration net interfaces igb4> done
hostname:configuration net interfaces> last
hostname:configuration net interfaces igb4>
```

El comando `last` también es útil para recuperar valores establecidos de forma automática por el dispositivo durante la creación de un nodo dinámico. Por ejemplo, el dispositivo le asigna un ID a cada acción de replicación cuando se crea. El comando `last` junto con el comando `get id` sirven para recuperar el ID sin usar el nombre de la acción de replicación:

```

hostname:shares p1/share replication> create
hostname:shares p1/share action (uncommitted)> set target=hostname
                                     target = hostname (uncommitted)
hostname:shares p1/share action (uncommitted)> set pool=p0
                                     pool = p0 (uncommitted)
hostname:shares p1/share action (uncommitted)> commit
hostname:shares p1/share replication> last get id
                                     id = 7034367a-d4d8-e26f-fa93-c3b454e3b595
hostname:shares p1/share replication>

```

Se debe tener en cuenta que cuando el comando `last` se combina con otro comando (en este caso, `get id`), se ejecuta en el contexto del último nodo visitado, pero el nodo actual permanece sin modificaciones.

Debido a que el comando `last` permite recuperar el último nodo visitado y sus valores sin especificar el nombre del nodo, el comando es muy conveniente para crear secuencias de comandos:

```

script
    project = 'myproj';
    target = 'mytarget';
    target_pool = 'notmypool';

    run('cd /');
    run('shares select ' + project);
    run('replication');
    run('create');
    set('target', target);
    set('pool', target_pool);
    run('commit');
    run('last');
    id = get('id');
    printf("Sending update for replication action id %s ...", id);
    run('sendupdate');
    while (get('state') != 'idle') {
        printf(".");
        run('sleep 1');
    }
    printf("done\n");
.

```

Para regresar al contexto previo, use el comando `done`:

```

hostname:configuration> done
hostname:>

```

De esta manera, se regresa al contexto previo, que no es necesariamente el contexto principal:

```

hostname:> configuration users select bmc
hostname:configuration users bmc> done
hostname:>

```

El comando `done` se puede usar varias veces para regresar sucesivamente a contextos anteriores:

```

hostname:> configuration
hostname:configuration> users
hostname:configuration users> select bmc
hostname:configuration users bmc> done
hostname:configuration users> done

```

```
hostname:configuration> done
hostname:>
```

Para navegar a un contexto principal, use el comando `cd`. Inspirado por el comando clásico de UNIX, `cd` usa el argumento `..` para denotar que se pasa al contexto principal:

```
hostname:> configuration users select bmc
hostname:configuration users bmc> cd ..
hostname:configuration users>
```

Y, como con el comando de UNIX, con `cd /` se pasa al contexto raíz:

```
hostname:> configuration
hostname:configuration> users
hostname:configuration users> select bmc
hostname:configuration users bmc> cd /
hostname:>
```

También como con su análogo de UNIX, `cd ../../` se puede usar para navegar al contexto de dos niveles de ascendencia:

```
hostname:> configuration
hostname:configuration> users
hostname:configuration users> select bmc
hostname:configuration users bmc> cd ../../
hostname:configuration>
```

Tenga en cuenta que los comandos `cd /` y `cd ..` admiten variaciones limitadas. Para mayor versatilidad, use el comando `top` y el comando `up`.

Use el comando `top` para navegar hasta el contexto raíz:

```
hostname:> configuration
hostname:configuration> users
hostname:configuration users> select bmc
hostname:configuration users bmc> top
hostname:>
```

Use el comando `top` seguido por un nombre de contexto para navegar directamente hasta el contexto especificado con respecto al contexto raíz. Por ejemplo, para navegar directamente desde el contexto `configuration users` al contexto `configuration services`, use el comando `top configuration services`:

```
hostname:> configuration
hostname:configuration> users
hostname:configuration users> top configuration services
hostname:configuration services>
```

Cuando se usa el comando `top` en combinación con un contexto específico, se puede usar el comando `done` para regresar al contexto antes de que se ejecutara el comando `top`. En el siguiente ejemplo, el primer comando `done` regresa al contexto previo. El segundo comando `done` regresa al contexto anterior al comando `top`. El tercer comando `done` regresa al contexto dos nodos antes del comando `top`.

```
hostname:> maintenance system
hostname:maintenance system> updates
```

```

hostname:maintenance system updates> top configuration services
hostname:configuration services> ftp
hostname:configuration services ftp> done
hostname:configuration services> done
hostname:maintenance system updates> done
hostname:>

```

Al igual que el comando `cd ..`, el comando `up` se puede usar para navegar hasta el contexto principal:

```

hostname:> configuration
hostname:configuration> users
hostname:configuration users> select bmc
hostname:configuration users bmc> up
hostname:configuration users>

```

Asimismo, puede ir a un contexto n nodos más arriba del contexto actual mediante la repetición del comando `up` n veces:

```

hostname:> configuration
hostname:configuration> users
hostname:configuration users> select bmc
hostname:configuration users bmc> up up
hostname:configuration>

```

Para regresar a un contexto específico con respecto al contexto principal actual, introduzca el nombre del contexto después del comando `up`. De manera similar, use el comando `up up` seguido por un nombre de contexto para regresar a un contexto específico con respecto al contexto con dos niveles de ascendencia desde el actual. Por ejemplo, para ir desde el contexto `configuration users bmc` al contexto `configuration services`, use el comando `up up services`:

```

hostname:> configuration
hostname:configuration> users
hostname:configuration users> select bmc
hostname:configuration users bmc> up up services
hostname:configuration services>

```

Cuando se usa el comando `up` en combinación con un contexto específico, se puede usar el comando `done` para regresar al contexto antes de que se ejecute el comando `up`. En el siguiente ejemplo, el primer comando `done` regresa al contexto anterior al comando `up`. El segundo comando `done` regresa al contexto que está dos nodos antes del comando `up` y el tercer comando `done` regresa al contexto que está tres nodos antes del comando `up`.

```

hostname:> configuration
hostname:configuration> services
hostname:configuration services> ftp
hostname:configuration services ftp> up http
hostname:configuration services http> done
hostname:configuration services ftp> done
hostname:configuration services> done
hostname:configuration> done
hostname:>

```

Los nombres de los contextos se pueden finalizar con la tecla de tabulación, sean contextos estáticos (por medio del modo de finalización normal de comandos) o dinámicos (mediante la finalización del comando `select`). A continuación, se presenta un ejemplo de selección del

usuario llamado `bmc` desde el contexto raíz con solamente quince pulsaciones de teclas, en lugar de las treinta y un veces que se necesitarían si no se usara la finalización con tabulación:

```
hostname:> configtab
hostname:> configuration utab
hostname:> configuration users setab
hostname:> configuration users select tab
bmc    root
hostname:> configuration users select btab
hostname:> configuration users select bmcenter
hostname:configuration users bmc>
```

Una vez dentro de un contexto, se pueden ejecutar comandos específicos de ese contexto. Por ejemplo, para obtener las preferencias del usuario actual, ejecute el comando `get` desde el contexto `configuration preferences`:

```
hostname:configuration preferences> get
      locale = C
      login_screen = status/dashboard
      session_timeout = 15
      session_annotation =
      advanced_analytics = false
```

Si se escribe algo después de un comando que cambia el contexto, ese comando se ejecutará en el contexto de destino, pero el control regresará al contexto original. Por ejemplo, para obtener las preferencias del contexto raíz sin cambiar de contexto, agregue el comando `get` a los comandos de navegación de contexto:

```
hostname:> configuration preferences get
      locale = C
      login_screen = status/dashboard
      session_timeout = 15
      session_annotation =
      advanced_analytics = false
```

Al crear una nueva entidad en el sistema, el contexto asociado con ella normalmente se crea en un estado *no confirmado*. Por ejemplo, cree una alerta de umbral mediante la ejecución del comando `create` desde el contexto `configuration alerts threshold`:

```
hostname:> configuration alerts thresholds create
hostname:configuration alerts threshold (uncommitted)>
```

El texto `(uncommitted)` del indicador denota que se trata de un contexto no confirmado. Para confirmar una entidad no confirmada, se debe usar el comando `commit`; si se intenta salir del contexto no confirmado, se solicitará la confirmación:

```
hostname:configuration alerts threshold (uncommitted)> cd /
Leaving will abort creation of "threshold". Are you sure? (Y/N)
```

Al confirmar una entidad no confirmada, se validan las propiedades asociadas con la nueva entidad y se genera un error si no se puede crear la entidad. Por ejemplo, la creación de una nueva alerta de umbral requiere que se especifique un nombre estadístico; de no hacerlo, se genera un error:

```
hostname:configuration alerts threshold (uncommitted)> commit
```

```
error: missing value for property "statname"
```

Para resolver el problema, solucione el error y vuelva a intentar la confirmación:

```
hostname:configuration alerts threshold (uncommitted)> set statname=cpu.utilization
      statname = cpu.utilization (uncommitted)
hostname:configuration alerts threshold (uncommitted)> commit
error: missing value for property "limit"
hostname:configuration alerts threshold (uncommitted)> set limit=90
      limit = 90 (uncommitted)
hostname:configuration alerts threshold (uncommitted)> commit
hostname:configuration alerts thresholds> list
THRESHOLD      LIMIT      TYPE STATNAME
threshold-000      90      normal cpu.utilization
```

Temas relacionados

- [“Interfaz de línea de comandos \(CLI\)” \[35\]](#)
- [“Propiedades de la CLI” \[43\]](#)

Propiedades de la CLI

Las *propiedades* son pares de nombre/valor asociados con un contexto. Para determinar las propiedades de un contexto dado, se puede ejecutar el comando "help properties". A continuación, se presenta un ejemplo de recuperación de las propiedades asociadas con las preferencias de un usuario:

```
hostname:configuration preferences> help properties
Properties that are valid in this context:

locale           => Locality

login_screen      => Initial login screen

session_timeout   => Session timeout

session_annotation => Current session annotation

advanced_analytics => Make available advanced analytics statistics
```

Las propiedades de un contexto dado se pueden recuperar con el comando `get`. A continuación, se presenta un ejemplo del uso del comando `get` para recuperar las preferencias de un usuario:

```
hostname:configuration preferences> get
      locale = C
      login_screen = status/dashboard
      session_timeout = 15
      session_annotation =
      advanced_analytics = false
```

El comando `get` devuelve todas las propiedades que se incluyan como argumentos. Por ejemplo, para obtener el valor de la propiedad `login_screen`:

```
hostname:configuration preferences> get login_screen
```

```
login_screen = status/dashboard
```

El comando `get` finalizará con tabulación con los nombres de las propiedades disponibles. Por ejemplo, para ver una lista de las propiedades disponibles para el servicio iSCSI:

```
hostname:> configuration services iscsi get tab
<status>          isns_server          radius_secret      target_chap_name
isns_access        radius_access        radius_server      target_chap_secret
```

El comando `select`, o un comando escrito entre comillas dobles, se usa para seleccionar un nodo dinámico por propiedad. Por ejemplo, para seleccionar `key-000` por usuario:

```
hostname:configuration services sftp keys> show
Keys:

NAME      MODIFIED          CIPHER  USER  COMMENT
key-000  2019-6-5 19:48:23  RSA     u1     1

hostname:configuration services sftp keys> "user=u1"
hostname:configuration services sftp key-000>
```

El comando `set` configurará una propiedad con un valor especificado; el nombre de la propiedad y su valor se separan con el signo igual. Por ejemplo, para configurar la propiedad `login_screen` como `"shares"`:

```
hostname:configuration preferences> set login_screen=shares
login_screen = shares (uncommitted)
```

Tenga en cuenta que en el caso de las propiedades que constituyen el estado del dispositivo, la configuración de las propiedades *no* cambia el valor, sino que registra el valor definido e indica que el valor de la propiedad no está confirmado.

Para forzar que los valores definidos para una propiedad surtan efecto, se los debe confirmar explícitamente, lo que permite que se modifiquen varios valores como un único cambio coherente. Para confirmar los valores de propiedades que no estén confirmados, use el comando `commit`:

```
hostname:configuration preferences> get login_screen
login_screen = shares (uncommitted)
hostname:configuration preferences> commit
hostname:configuration preferences> get login_screen
login_screen = shares
```

Si intenta salir de un contexto que contiene propiedades no confirmadas, se le advertirá que al hacerlo se abandonarán los valores definidos para las propiedades y se le solicitará que confirme que desea salir. Por ejemplo:

```
hostname:configuration preferences> set login_screen=maintenance/hardware
login_screen = maintenance/hardware (uncommitted)
hostname:configuration preferences> done
You have uncommitted changes that will be discarded. Are you sure? (Y/N)
```

Si se configura una propiedad de un contexto desde otro contexto, es decir, si se agregó el comando `set` a un comando que cambia de contexto, la confirmación es *implícita* y se realiza antes de que el control regrese al contexto de origen. Por ejemplo:


```
hostname:> configuration preferences set login_screen=analytics/worksheets
login_screen = analytics/worksheets
hostname:>
```

Algunas propiedades tienen una lista de valores. Para estas propiedades, los elementos de la lista se deben separar con comas. Por ejemplo, la propiedad `servers` de NTP se puede configurar con una lista de servidores NTP:

```
hostname:configuration services ntp> set servers=0.pool.ntp.org,1.pool.ntp.org
servers = 0.pool.ntp.org,1.pool.ntp.org (uncommitted)
hostname:configuration services ntp> commit
```

Si el valor de una propiedad contiene una coma, un signo igual, comillas o un espacio, todo el valor se debe escribir entre comillas dobles. Por ejemplo, la propiedad de recurso compartido `share nfs` del proyecto por defecto se puede configurar para que sea de solo lectura, pero permita acceso de lectura y escritura al host `kiowa`. Para obtener más información, consulte [Recursos compartidos y proyectos \[483\]](#).

```
hostname:> shares select default
hostname:shares default> set sharenfs="ro,rw=kiowa"
sharenfs = ro,rw=kiowa (uncommitted)
hostname:shares default> commit
```

Algunas propiedades son inmutables; es posible obtener sus valores, pero no se las puede definir. Si se intenta configurar una propiedad inmutable, se genera un error. Por ejemplo, si se intenta configurar la propiedad inmutable `space_available` del proyecto predeterminado. Para obtener más información, consulte [Recursos compartidos y proyectos \[483\]](#).

```
hostname:> shares select default
hostname:shares default> get space_available
space_available = 1.15T
hostname:shares default> set space_available=100P
error: cannot set immutable property "space_available"
```

Hay propiedades que son inmutables solamente en ciertas condiciones. Para estas propiedades, el comando `set` no es válido. Por ejemplo, si el usuario llamado `bmc` es un usuario de red, la propiedad `fullname` será inmutable:

```
hostname:> configuration users select bmc set fullname="Rembrandt Q. Einstein"
error: cannot set immutable property "fullname"
```

Temas relacionados

- [“Interfaz de usuario basada en explorador \(BUI\)” \[23\]](#)
- [“Interfaz de línea de comandos \(CLI\)” \[35\]](#)

Trabajo con secuencias de comandos de la CLI

La CLI está diseñada para proporcionar un entorno de secuencias de comandos eficaz para realizar tareas repetitivas.

Puede usar los comandos por lotes o la creación de secuencias de comandos (o alguna combinación de ellos); pero, en cualquiera de los casos, la infraestructura automatizada requiere acceso al dispositivo. Esto se debe llevar a cabo a través de la configuración de usuario, las autorizaciones de usuario y la configuración de claves públicas SSH con la CLI.

Para obtener información acerca de la configuración de usuarios, consulte lo siguiente:

- [“Configuración de usuarios” \[257\]](#)
- [“Autorizaciones de usuarios” \[274\]](#)
- [Configuración de claves SSH públicas \(CLI\) \[284\]](#)

Para usar la secuencia de comandos de la CLI, use las siguientes secciones:

- [“Uso de comandos por lotes” \[46\]](#)
- [“Descripción de la creación de secuencias de comandos de la CLI” \[47\]](#)
- [Acceso al entorno de secuencias de comandos de la CLI \[47\]](#)
- [“Descripción de las funciones incorporadas de la CLI” \[48\]](#)
- [Uso de la función Elementos secundarios \[49\]](#)
- [Uso de la función Opciones \[50\]](#)
- [Uso de las funciones de alertas personalizadas \[51\]](#)
- [Uso de la función Obtener \[51\]](#)
- [Uso de la función Lista \[52\]](#)
- [Uso de la función Prop \[55\]](#)
- [Uso de la función Ejecutar \[57\]](#)
- [“Uso de las funciones para generación de salidas” \[57\]](#)
- [“Descripción de errores de secuencias de comandos de la CLI” \[58\]](#)

Uso de comandos por lotes

El mecanismo más simple para usar secuencias de comandos es ejecutar comandos de shell del dispositivo por lotes. Por ejemplo, para generar automáticamente una instantánea llamada newsnap en el proyecto myproj y el sistema de archivos myfs, escriba los siguientes comandos en un archivo:

```
shares
select myproj
select myfs
snapshots snapshot newsnap
```

A continuación, use ssh en el dispositivo, de manera de redirigir la entrada estándar para que sea el archivo:

```
$ ssh root@hostname < myfile.txt
```

En muchos shells, es posible abreviar esto mediante un indicador "here file", mediante el cual la entrada hasta un token se envía a la entrada estándar. A continuación, se presenta el ejemplo anterior con un indicador "here file":

```
$ '''ssh root@hostname << EOF
shares
select myproj
select myfs
snapshots snapshot newsnap
EOF'''
```

Este mecanismo es suficiente para la clase más simple de automatización, y puede ser suficiente si se utiliza con lógica de programación en un lenguaje de secuencias de comandos de shell de nivel superior en un cliente, pero por lo general esto deja mucho que desear.

Descripción de la creación de secuencias de comandos de la CLI

Si bien el uso de comandos por lotes es suficiente para las operaciones más simples, puede ser tedioso utilizarlo en la lógica de programación. Por ejemplo, si desea obtener información acerca del uso de espacio para cada recurso compartido, se necesita invocar muchas veces a la CLI utilizando un lenguaje de nivel superior en el cliente que analizó la salida de comandos específicos. El resultado es una infraestructura de automatización frágil y lenta. Para permitir una automatización más rápida y robusta, el dispositivo tiene un *entorno de secuencias de comandos* enriquecido basado en ECMAScript 3. En este documento no se incluye una guía de ECMAScript, pero es un lenguaje dinámico con sintaxis similar a C que permite:

- Flujo de código condicional (*if/else*).
- Flujo de código iterativo (*while, for, etc.*).
- Manipulación de datos estructurales y de matriz mediante los tipos de objeto y de matriz de nivel superior.
- Expresiones regulares similares a las de Perl y manipulación de cadenas (*split(), join(), etc.*)
- Excepciones
- Funciones de lenguaje funcional sofisticadas, como cierres.

▼ Acceso al entorno de secuencias de comandos de la CLI

1. En la CLI, use el comando `script` para introducir el entorno de secuencia de comandos:

```
hostname:> script
("." to run)>
```

2. **En la petición de datos del entorno de secuencia de comandos, puede escribir la secuencia de comandos y finalizar con un carácter de punto (.) en una línea para ejecutar la secuencia de comandos:**

```
hostname:> script
("." to run)> for (i = 10; i > 0; i--)
("." to run)>   printf("%d... ", i);
("." to run)> printf("Blastoff!\n");
("." to run)> .
10... 9... 8... 7... 6... 5... 4... 3... 2... 1... Blastoff!
```

3. **Si la secuencia de comandos está formada por una sola línea, simplemente puede escribirla como argumento del comando `script`, lo que simplifica la exploración del uso de secuencias de comandos:**

```
hostname:> script print("It is now " + new Date())
It is now Tue Oct 15 2019 05:33:01 GMT+0000 (UTC)
```

Descripción de las funciones incorporadas de la CLI

Las siguientes funciones incorporadas permiten que las secuencias de comandos interactúen con el sistema.

TABLA 9 Funciones incorporadas para admitir interacciones entre sistemas

Función	Descripción
<code>children</code>	Devuelve una matriz de elementos secundarios estáticos. Consulte Uso de la función Elementos secundarios [49] .
<code>choices</code>	Devuelve una selección de los valores válidos de cualquier propiedad para la cual se conoce el conjunto de valores y se puede enumerar. Consulte Uso de la función Opciones [50] .
<code>createalert, postalert</code>	Crea o publica una alerta personalizada. Consulte Uso de las funciones de alertas personalizadas [51] .
<code>get</code>	Permite obtener el valor de la propiedad especificada. Tenga en cuenta que esta función devuelve el valor en formato nativo. Por ejemplo, las fechas se devuelven como objetos Fecha. Consulte Uso de la función Obtener [51] .
<code>list</code>	Devuelve una matriz de tokens que corresponden a los objetos secundarios dinámicos del contexto actual. Consulte Uso de la función Lista [52] .

Función	Descripción
<code>prop</code>	Devuelve el valor de la propiedad especificada en el contexto de nodo actual o establece la propiedad especificada en un valor determinado. Los valores de entrada y salida tienen un formato programable. Los valores que devuelve <code>prop</code> pueden ser diferentes a los que devuelve <code>get</code> . Consulte Uso de la función Prop [55] .
<code>props</code>	Devuelve una matriz de los nombres de las propiedades para el nodo actual.
<code>run</code>	Ejecuta el comando especificado en el shell y devuelve la salida como una cadena. Tenga en cuenta que si la salida tiene varias líneas, la cadena devuelta contendrá nuevas líneas incrustadas. Consulte Uso de la función Ejecutar [57] .
<code>set</code>	Toma dos argumentos de cadena y configura la propiedad especificada con el valor especificado.

▼ Uso de la función Elementos secundarios

Incluso en un contexto con elementos secundarios estáticos, puede resultar útil iterar entre esos elementos secundarios mediante programación. Para ello se puede utilizar la función `children`, que devuelve una matriz de elementos secundarios estáticos.

1. **Por ejemplo, esta secuencia de comandos itera cada servicio e imprime el estado correspondiente:**

```
configuration services
script
    var svcs = children();
    for (var i = 0; i < svcs.length; ++i) {
        run(svcs[i]);
        try {
            printf("%-10s %s\n", svcs[i], get('<status>'));
        } catch (err) { }
        run("done");
    }
}
```

2. **Esta es la salida de la ejecución de la secuencia de comandos, suponiendo que se haya guardado en un archivo llamado `svcinfo.aksh`:**

```
$ ssh root@hostname < svcinfo.aksh
Password:
cifs      disabled
dns       online
ftp       disabled
http      disabled
identity  online
idmap     online
ipmp      online
iscsi     online
```

ldap	disabled
ndmp	online
nfs	online
nis	online
ntp	online
scrk	online
sftp	disabled
smtp	online
snmp	disabled
ssh	online
tags	online
vscan	disabled

▼ Uso de la función Opciones

La función `choices` devuelve una selección de los valores válidos de cualquier propiedad para la cual se conoce el juego de valores y se puede enumerar. Por ejemplo, la siguiente secuencia de comandos recupera la lista de todas las agrupaciones en el nodo de recursos compartidos mediante la función `choices` y, luego, itera todas las agrupaciones para enumerar los proyectos y recursos compartidos junto con el espacio disponible.

1. **Por ejemplo, la siguiente secuencia de comandos recupera la lista de todas las agrupaciones en el nodo de recursos compartidos mediante la función `choices` y, luego, itera todas las agrupaciones para enumerar los proyectos y recursos compartidos junto con el espacio disponible.**

```
fmt = '%-40s %-15s %-15s\n';
printf(fmt, 'SHARE', 'USED', 'AVAILABLE');
run('cd /');
run('shares');
pools = choices('pool');
for (p = 0; p < pools.length; p++) {
    set('pool', pools[p]);
    projects = list();
    for (i = 0; i < projects.length; i++) {
        run('select ' + projects[i]);
        shares = list();
        for (j = 0; j < shares.length; j++) {
            run('select ' + shares[j]);
            share = pools[p] + ':' + projects[i] + '/' + shares[j];
            printf(fmt, share, get('space_data'),
                get('space_available'));
            run('cd ..');
        }
        run('cd ..');
    }
}
```

2. **Esta es la salida de la ejecución del comando:**

SHARE	USED	AVAILABLE
pond:projectA/fs1	31744	566196178944
pond:projectA/fs2	31744	566196178944

pond:projectB/lun1	21474836480	587670999040
puddle:deptA/share1	238475	467539219283
puddle:deptB/share1	129564	467539219283
puddle:deptB/share2	19283747	467539219283

▼ Uso de las funciones de alertas personalizadas

La función `createalert` crea una alerta personalizada y la función `postalert` publica la alerta. Es posible llamar a la función `createalert` desde una secuencia de comandos o un flujo de trabajo. La función `postalert` se debe llamar desde un flujo de trabajo. Consulte [“Creación y publicación de alertas personalizadas dentro de un flujo de trabajo” \[853\]](#).

1. La siguiente llamada a función crea una alerta personalizada minimalista.

```
createalert([{'handler': 'syslog', 'args': {}}, {description: 'Writes to syslog'}]);
```

2. La siguiente secuencia de comandos especifica parámetros adicionales y captura el valor de retorno.

Se necesita el valor de retorno para publicar la alerta. Si bien se muestra la llamada `postalert` en esta secuencia de comandos, es necesario llamar a `postalert` desde un flujo de trabajo en respuesta a un evento que se produce en el flujo de trabajo.

```
script
("." to run)> var actions = [{
("." to run)>   handler: 'email',
("." to run)>   args: {
("." to run)>     address: 'admin@example.com',
("." to run)>     subject: 'Custom Alert Response'
("." to run)>   }
("." to run)> }];
("." to run)> var params = {
("." to run)>   severity: 'Minor',
("." to run)>   description: 'Custom alert description',
("." to run)>   response: 'What the alert action does',
("." to run)>   impact: 'What happened to the appliance',
("." to run)>   recommended_action: 'What the administrator should do'
("." to run)> };
("." to run)> var cuuid = createalert(actions, params);
("." to run)> print(cuuid);
("." to run)> var puuid = postalert(cuuid);
("." to run)> .
54c24732-b9c5-4b57-9aee-aeaf195afdae
```

▼ Uso de la función Obtener

Como la función `run` es potente, puede resultar tentador recurrir solamente al análisis de la salida para obtener información del sistema, pero esto tiene la desventaja de que deja salidas de análisis de secuencias de comandos legibles para el ojo humano, que pueden cambiar o

no en el futuro. Para recopilar información del sistema de manera más sólida, use la función incorporada `get`. En el caso de la propiedad `boot_time`, no devuelve la cadena, sino que devuelve el objeto `Date` de ECMAScript, que permite la manipulación del valor de la propiedad mediante programación. Para obtener valores programables más confiables, consulte [Uso de la función Prop \[55\]](#).

1. **Por ejemplo, tal vez desee usar la propiedad `boot_time` en combinación con la hora actual para determinar el tiempo transcurrido desde el inicio:**

```
script
run('configuration version');
now = new Date();
uptime = (now.valueOf() - get('boot_time').valueOf()) / 1000;
printf('up %d day%s, %d hour%s, %d minute%s, %d second%s\n',
    d = uptime / 86400, d < 1 || d >= 2 ? 's' : '',
    h = (uptime / 3600) % 24, h < 1 || h >= 2 ? 's': '',
    m = (uptime / 60) % 60, m < 1 || m >= 2 ? 's': '',
    s = uptime % 60, s < 1 || s >= 2 ? 's': '');
```

2. **Suponiendo que lo anterior se guarda como `uptime.aksh`, lo puede ejecutar de la siguiente manera:**

```
$ ssh root@hostname < uptime.aksh
Pseudo-terminal will not be allocated because stdin is not a terminal.
Password:
up 2 days, 10 hours, 47 minutes, 48 seconds
```

El mensaje sobre la asignación pseudoterminal se debe al cliente SSH. A fin de gestionar el problema al que hace referencia este mensaje, se puede especificar la opción `-t` para SSH.

▼ Uso de la función Lista

En un contexto con elementos secundarios dinámicos, puede resultar muy útil iterar entre esos elementos secundarios mediante programación. Para ello se puede utilizar la función `list`, que devuelve una matriz de elementos secundarios dinámicos.

1. **En el siguiente ejemplo, una secuencia de comandos itera todos los recursos compartidos de cada proyecto e imprime la cantidad de espacio consumido y el espacio disponible:**

```
script
run('shares');
projects = list();

for (i = 0; i < projects.length; i++) {
    run('select ' + projects[i]);
    shares = list();

    for (j = 0; j < shares.length; j++) {
        run('select ' + shares[j]);
        printf("%s/%s %1.64g %1.64g\n", projects[i], shares[j],
```



```

        get('space_data'), get('space_available'));
    run('cd ..');
}

run('cd ..');
}

```

2. Esta es la salida de la ejecución de la secuencia de comandos, suponiendo que se haya guardado en un archivo llamado `space.aksh`:

```

$ ssh root@hostname < space.aksh
Password:
admin/accounts 18432 266617007104
admin/exports 18432 266617007104
admin/primary 18432 266617007104
admin/traffic 18432 266617007104
admin/workflow 18432 266617007104
aleventhal/hw_eng 18432 266617007104
bcantrill/analytx 1073964032 266617007104
bgregg/dashbd 18432 266617007104
bgregg/filesys01 26112 107374156288
bpijewski/access_ctrl 18432 266617007104
...

```

3. Si se deseara una variante más "estética" (si bien sería más difícil desde el punto de vista de la programación), se puede analizar directamente la salida del comando `get`:

```

script
run('shares');
projects = list();

printf('%-40s %-10s %-10s\n', 'SHARE', 'USED', 'AVAILABLE');

for (i = 0; i < projects.length; i++) {
    run('select ' + projects[i]);
    shares = list();

    for (j = 0; j < shares.length; j++) {
        run('select ' + shares[j]);

        share = projects[i] + '/' + shares[j];
        used = run('get space_data').split(/\s+/)[3];
        avail = run('get space_available').split(/\s+/)[3];

        printf('%-40s %-10s %-10s\n', share, used, avail);
        run('cd ..');
    }

    run('cd ..');
}

```

4. Esta es la salida de la ejecución de esta nueva secuencia de comandos, suponiendo que se le asignó el nombre `prettyspace.aksh`:

```

$ ssh root@hostname < prettyspace.aksh
Password:
SHARE                                USED      AVAILABLE
admin/accounts                       18K       248G

```

admin/exports	18K	248G
admin/primary	18K	248G
admin/traffic	18K	248G
admin/workflow	18K	248G
aleventhal/hw_eng	18K	248G
bcantrill/analytx	1.00G	248G
bgregg/dashbd	18K	248G
bgregg/filesys01	25.5K	100G
bpijewski/access_ctrl	18K	248G
...		

5. La función `list` admite los argumentos opcionales `depth` y `filter`.

El formato es: `list ([depth, [filter]])`. El argumento `depth` se puede definir con un número. Cuanto mayor sea el número de `depth`, mayor será el nivel de detalle devuelto. El formato del argumento `filter` es `{<prop1>:<val1>, <prop2>:<val2> ...}`. Si se especifica `filter`, también se debe especificar `depth`.

Uso y comportamiento de la entrada:

- `list()`: devuelve solo nombres de nodos.
- `list(0)`: devuelve propiedades de nodos y solo nombres de elementos secundarios.
- `list(0, {kiosk_mode: true})`: devuelve una lista filtrada para `kiosk_mode true` con nombres de elementos secundarios.
- `list(1)`: devuelve propiedades de nodos, nombres y propiedades de elementos secundarios, solo nombres de elementos terciarios.
- `list(1, {kiosk_mode: true})`: devuelve una lista filtrada para `kiosk_mode true` con detalles hasta `depth=1`.
- `list(2)`: devuelve propiedades de nodos, nombres y propiedades de elementos secundarios y la salida de `list(0)` de elementos terciarios.
- `list(2, {fullname: 'Super*', kiosk_mode: true})`: devuelve una lista filtrada para `fullname` que contiene `Super` y `kiosk_mode` con el valor `true` con detalles hasta `depth=2`.

6. En el siguiente ejemplo, se muestra la salida correspondiente a una lista con `depth=2`:

La etiqueta `name` muestra el nombre del elemento de la lista (es decir, un nodo). La etiqueta `properties` muestra las propiedades del elemento de la lista. La etiqueta `children` muestra los elementos secundarios estáticos del elemento de la lista. La etiqueta `list` muestra los elementos secundarios dinámicos del elemento de la lista.

```
script
("." to run)> dump(list(2));
("." to run)> .

[
  {
    name: 'restuser',
    properties: {
      kiosk_screen: 'status/dashboard',
      kiosk_mode: false,
      roles: ['basic'],
```

```

        require_annotation: false,
        initial_password: 'DummyPassword',
        fullname: 'REST User',
        logname: 'restuser'
    },
    children: [{
        name: 'preferences',
        properties: {
            advanced_analytics: false,
            session_timeout: 15,
            login_screen: 'status/dashboard',
            locale: 'C'
        }
    }, {
        name: 'exceptions',
        list: [{
            name: 'auth-000',
            properties: {
                allow_configure: false,
                scope: 'alert'
            }
        }, {
            name: 'auth-001',
            properties: {
                allow_workgroup: false,
                allow_domain: false,
                name: '*',
                scope: 'ad'
            }
        }
    ]
    }]
}]

```

▼ Uso de la función Prop

En la mayoría de los casos, las funciones `get` y `prop` devuelven el mismo valor. La diferencia entre estas dos funciones es que `get` no siempre devuelve un valor programable, mientras que la función `prop` siempre devuelve un valor programable. Un valor programable tiene el mismo formato estable para cada tipo de propiedad.

1. Devuelva el valor programable de una propiedad en el contexto de nodo actual.

Para la mayoría de las propiedades, las funciones `get` y `prop` devuelven valores idénticos, como se muestra en el siguiente ejemplo de la propiedad `version`:

```

> ls
version = 2019.02.28,1-0
> script get('version')
'2019.02.28,1-0'
> script prop('version')
'2019.02.28,1-0'

```

En el siguiente ejemplo de la propiedad `date`, tenga en cuenta la diferencia entre el valor que devuelve la función `get` y el valor programable que devuelve la función `prop`:

```
> ls
date = 2019-2-28 10:43:11
> script get('date')
Tue Feb 28 2019 10:43:11 GMT+0000 (UTC) (Date object)
> script prop('date')
'2019-02-28T10:43:11Z'
```

2. Defina el valor de una propiedad dentro del contexto de nodo actual en un valor programable.

Incluya un valor en la llamada a la función `prop` para definir el valor de la propiedad denominada. Se emite un mensaje de error si el valor dado no tiene el formato programable especificado para esa propiedad. De lo contrario, el formato definido de la función `prop` no devuelve ningún valor.

```
> ls
date = 2019-2-28 10:43:11
> script prop('date', '2019-03-09T12:34:56Z')
> ls
date = 2019-3-09 12:34:56
> script prop('date')
'2019-03-09T12:34:56Z'
```

3. Defina el valor de una propiedad booleana.

Como la función `prop` puede usarse para devolver un valor de propiedad o para definirlo, la función `prop` no tiene la capacidad que tiene `set` para definir una propiedad booleana en `true` sin especificar el valor.

En el siguiente ejemplo, se muestra la forma de usar la versión abreviada de la función `set` para establecer una propiedad booleana en el valor `true`:

```
set('booleanproperty')
```

La forma abreviada de la función `prop` devuelve el valor de la propiedad booleana, ya sea `true` o `false`:

```
script prop('booleanproperty')
'false'
```

A fin de usar la función `prop` para definir el valor de una propiedad booleana, debe proporcionar el siguiente valor:

```
script prop('booleanproperty', true)
script prop('booleanproperty')
'true'
```

4. Defina el valor de una propiedad List.

A fin de definir un valor programable para una propiedad con el modificador `List`, debe especificar una matriz de valores:

```
> ls
stringlist = a,string,list
> script prop('stringlist', ['a', 'b', 'c', 'd'])
```

```
> script prop('stringlist')
['a', 'b', 'c', 'd']
> ls
stringlist = a,b,c,d
```

A fin de especificar un solo valor para una propiedad List, especifique el único valor como una matriz de tamaño uno:

```
> ls
stringlist = a,string,list
> script prop('stringlist', ['a'])
> script prop('stringlist')
['a']
> ls
stringlist = a
```

A fin de especificar un valor vacío para una propiedad con el modificador Empty o List, especifique una matriz vacía:

```
> ls
emptystringlist = a,string,list
> script prop('emptystringlist', [])
> script prop('emptystringlist')
[]
> ls
emptystringlist =
```

▼ Uso de la función Ejecutar

1. La manera más simple para que las secuencias de comandos interactúen con el sistema es utilizar la función `run`. La función `run` toma un comando para ejecutarlo y devuelve la salida de ese comando como una cadena. Por ejemplo:

```
hostname:> configuration version script dump(run('get boot_time'))
'
          boot_time = 2019-10-12 07:02:17\n'
```

2. La función incorporada `dump` vuelca el argumento, sin expandir ninguna de las nuevas líneas incrustadas. Se pueden usar las características de manipulación de cadenas de ECMAScript para separar la salida. Por ejemplo, si se divide lo anterior en función de los espacios en blanco:

```
hostname:> configuration version script dump(run('get boot_time').split(/\s+/))
['', 'boot_time', '=', '2019-10-12', '07:02:17', '']
```

Uso de las funciones para generación de salidas

Para informar el estado del sistema, se debe generar una salida. Las secuencias de comandos tienen varias funciones incorporadas que pueden utilizar para generar salidas:

TABLA 10 Funciones incorporadas para generación de salidas

Función	Descripción
dump	Vuelca el argumento especificado en el terminal sin expandir las nuevas líneas incrustadas. Los objetos se despliegan en formato similar al de JSON. Es útil para depuraciones.
print	Imprime el objeto especificado como cadena, seguida por una nueva línea. Si el objeto no tiene un método toString, se lo imprime de manera opaca.
printf	Al igual que printf(3C) de C, imprime los argumentos especificados según la cadena de aplicación de formato especificada.

Descripción de errores de secuencias de comandos de la CLI

Cuando se genera un error, el sistema arroja una excepción. Por lo general, la excepción es un objeto que contiene los siguientes miembros:

- **code:** código numérico asociado con el error
- **message:** mensaje asociado con el error legible para el ojo humano

Las excepciones se pueden capturar y resolver, o se las puede quitar del entorno de secuencia de comandos. Si un entorno de secuencia de comandos tiene una excepción no capturada, los detalles aparecen en la CLI. Por ejemplo:

```
hostname:> script run('not a cmd')
error: uncaught error exception (code EAKSH_BADCMD) in script: invalid command
       "not a cmd" (encountered while attempting to run command "not a cmd")
```

Para ver más detalles sobre la excepción, puede capturarla y volcarla:

```
hostname:> script try { run('not a cmd') } catch (err) { dump(err); }
{
  toString: <function>,
  code: 10004,
  message: 'invalid command "not a cmd" (encountered while attempting to
           run command "not a cmd")'
}
```

Esto también le permite un tratamiento enriquecido de los errores, por ejemplo:

```
#!/usr/bin/ksh -p

ssh -T root@hostname <<EOF
script
  try {
    run('shares select default select $1');
  } catch (err) {
```

```
        if (err.code == EAKSH_ENTITY_BADSELECT) {
            printf('error: "$1" is not a share in the ' +
                  'default project\n');
            exit(1);
        }
        throw (err);
    }
    printf("default/$1: compression is %s\n", get('compression'));
    exit(0);
EOF
```

Si esta secuencia de comandos se llama `share.ksh` y se ejecuta con un nombre de recurso compartido no válido, se genera un mensaje de error enriquecido:

```
$ ksh ./share.ksh bogus
error: "bogus" is not a share in the default project
```


Configuración del dispositivo

Para configurar un dispositivo, use las siguientes secciones:

- [“Configuración inicial del dispositivo” \[61\]](#)
- [“Configuración de clusters de dispositivos” \[62\]](#)
- [“Configuración de red” \[96\]](#)
- [“Configuración del almacenamiento” \[127\]](#)
- [“Configuración de copia de seguridad en la nube” \[171\]](#)
- [“Descripción del estado del dispositivo” \[208\]](#)
- [“Configuración de una red de área de almacenamiento \(SAN\)” \[224\]](#)
- [“Configuración de usuarios” \[257\]](#)
- [“Configuración de preferencias del dispositivo” \[280\]](#)
- [“Configuración de alertas” \[286\]](#)
- [“Configuración de certificados” \[303\]](#)
- [“Configuración de cifrados y versiones de SSL/TLS” \[318\]](#)
- [“Configuración de la complejidad de contraseña” \[319\]](#)

Configuración inicial del dispositivo

Si está configurando un dispositivo nuevo, siga los pasos de configuración inicial que se describen en [“Configuración inicial del dispositivo” en la *Guía de instalación de Oracle ZFS Storage Appliance*](#).

Puede repetir la configuración inicial más adelante; para ello, haga clic en el botón "Instalación inicial" de la pantalla Mantenimiento > Sistema o vaya al contexto `maintenance system setup` en la CLI.

Temas relacionados

- [“Configuración de clusters de dispositivos” \[62\]](#)
- [“Configuración de red” \[96\]](#)

- [“Configuración del almacenamiento” \[127\]](#)

Configuración de clusters de dispositivos

El dispositivo Oracle ZFS Storage Appliance admite la agrupación en clusters cooperativa de dos controladores. La agrupación de controladores en clusters puede ser parte de un enfoque integrado para mejorar la disponibilidad, que también puede incluir equilibrio de carga en el cliente, planificación de sitio adecuada, reparaciones y mantenimiento preventivo y reactivo, y redundancia de hardware de un solo dispositivo incorporada en todos los dispositivos.

Nota - Si está configurando una agrupación en clusters de dos controladores nuevos, siga el procedimiento de la BUI para la configuración inicial de controladores nuevos que se describe en [“Configuración inicial del dispositivo” en *Guía de instalación de Oracle ZFS Storage Appliance*](#).

Para los procedimientos relacionados con la agrupación de dispositivos en clusters, consulte:

- [“Conexión de cables de cluster” en la *Guía de cableado de Oracle ZFS Storage Appliance*](#)
- [“Vista de configuración de clusters de la BUI” \[63\]](#)
- [Comprobación de estado de enlaces de cluster \(CLI\) \[65\]](#)
- [Actualización de un dispositivo independiente a una configuración en clusters \(BUI\) \[66\]](#)
- Cierre de una configuración en clusters: [BUI](#), [CLI](#)
- [Anulación de la configuración de un nodo de cluster \[73\]](#)

Para comprender mejor la agrupación de dispositivos en clusters, consulte:

- [“Terminología de clusters” \[74\]](#)
- [“Descripción de la agrupación en clusters” \[75\]](#)
- [“Estados de los controladores de cluster” \[75\]](#)
- [“E/S de interconexión del cluster” \[76\]](#)
- [“Gestión de recursos de clusters” \[78\]](#)
- [“Toma de control y failback en clusters” \[81\]](#)
- [“Cambios de configuración en un entorno en cluster” \[82\]](#)
- [“Consideraciones de la agrupación en clusters para almacenamiento” \[83\]](#)
- [“Consideraciones de la agrupación en clusters para redes” \[86\]](#)
- [“Interfaces IP locales privadas” \[88\]](#)
- [“Consideraciones de la agrupación en clusters para InfiniBand” \[89\]](#)
- [“Prevención de situaciones de cerebro dividido” \[92\]](#)

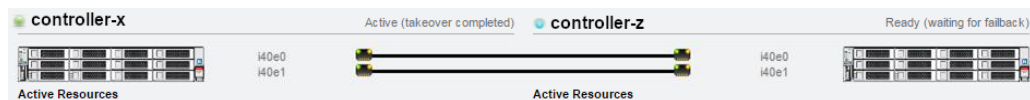
- “Estimación y reducción del impacto de la toma de control” [93]

Vista de configuración de clusters de la BUI

La vista Configuración > Cluster proporciona una visión general gráfica del estado de la tarjeta de cluster, los estados de los controladores de cluster y los recursos de cluster.

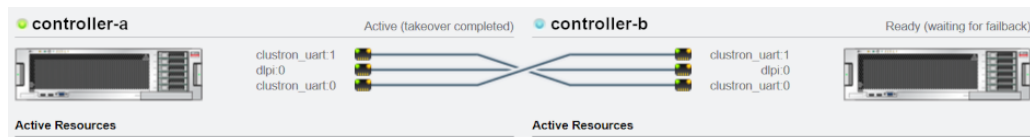
En la siguiente figura, se muestran las conexiones de cluster entre dos controladores ZS9-2.

FIGURA 1 Conexiones de cluster para controladores ZS9-2



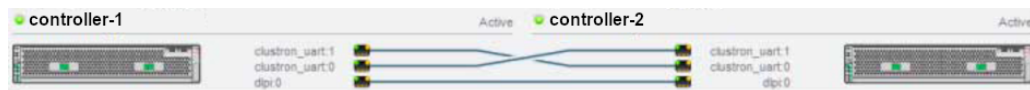
En la siguiente figura, se muestran las conexiones de cluster entre dos controladores ZS7-2, ZS5-x, ZS4-4, ZS3-4 o 7x20.

FIGURA 2 Conexiones de cluster para controladores ZS7-2, ZS5-x, ZS4-4, ZS3-4 y 7x20



En la siguiente figura, se muestran las conexiones de cluster entre dos controladores ZS3-2.

FIGURA 3 Conexiones de cluster para controladores ZS3-2



La interfaz contiene los siguientes objetos:

- Una vista en miniatura de cada controlador. El controlador en el que el usuario inició sesión se muestra en el lado izquierdo de la vista. Arriba de cada vista en miniatura del controlador, se muestra el nombre del controlador a la izquierda y el estado de cluster actual del controlador (como Activo o Listo) a la derecha. Para obtener descripciones de los estados de controlador, consulte [“Estados de los controladores de cluster” \[75\]](#).
- Una línea que representa cada conexión de tarjeta de cluster. Estas líneas se actualizan dinámicamente con el hardware. Una línea continua indica que el enlace está conectado y activo. Una línea con guiones indica que el enlace está roto de uno de los siguientes modos:
 - El otro controlador se está reiniciando.
 - El enlace no se cableó correctamente o los cables del cluster no están firmes en sus conectores. Para obtener instrucciones sobre el cableado del cluster, consulte [“Conexión de cables de cluster” en la Guía de cableado de Oracle ZFS Storage Appliance](#).

Asegúrese de que todos los enlaces estén conectados y activos antes de realizar la configuración inicial del cluster. Consulte [Actualización de un dispositivo independiente a una configuración en clusters \(BUI\) \[66\]](#).

- Debajo de cada vista en miniatura del controlador, se muestra una lista de los recursos PRIVADOS y ÚNICOS que se encuentran asignados a ese controlador, además de algunos atributos de esos recursos, como dirección IP o tamaño.
- También se muestra el propietario de cada recurso. El propietario del recurso es el controlador que proporcionará el recurso cuando ambos controladores se encuentren en el estado EN CLUSTER. Para cambiar el propietario, haga clic en el nombre del propietario actual, seleccione el controlador par y haga clic en el botón APLICAR en la esquina superior derecha de la vista.
- A la derecha del propietario, se encuentra un ícono de reinicio  que permite intentar reparar el recurso.
- Para cada recurso, un ícono de candado  indica si el recurso es PRIVADO. Cuando el controlador actual se encuentra en los estados PROPIETARIO o EN CLUSTER, es posible bloquear un recurso (hacerlo PRIVADO) o desbloquearlo (hacerlo ÚNICO). Para bloquear un recurso en el controlador o desbloquear un recurso del controlador, haga clic en el ícono de candado y, a continuación, haga clic en el botón APLICAR en la esquina superior derecha de la vista. Tenga en cuenta que los recursos PRIVADOS que pertenecen al par remoto no se muestran en ninguna de las listas de recursos.

En la siguiente tabla, se describen los botones en la parte superior de la vista Configuración > Cluster.

TABLA 11 Botones de la interfaz del cluster

Botón	Descripción
Configurar	La operación Configurar es un paso de la configuración inicial del cluster. Consulte Actualización de un dispositivo independiente a una configuración en clusters (BUI) [66] .

Botón	Descripción
Desconfigurar	La operación Desconfigurar configura un nodo de cluster para el funcionamiento independiente. Consulte Anulación de la configuración de un nodo de cluster [73].
Failback	La operación Failback cambia la configuración del cluster de PROPIETARIO-SEGMENTADO (activo-pasivo) a EN CLUSTER-EN CLUSTER (activo-activo). Consulte Actualización de un dispositivo independiente a una configuración en clusters (BUI) [66] y “Toma de control y failback en clusters” [81].
Toma de control	La toma de control se realiza automáticamente en ciertas situaciones. Es posible realizarla manualmente, lo que puede ser útil para fines de prueba. Consulte “Toma de control y failback en clusters” [81].
Revertir	Si existen modificaciones de recursos pendientes (las filas de recursos se resaltan en amarillo), se deshacen esos cambios y se muestra la configuración actual del cluster.
Aplicar	Si existen modificaciones de recursos pendientes (las filas de recursos se resaltan en amarillo), se confirman esos cambios en el cluster.

Temas relacionados

- [“Configuración inicial \(BUI\)” en la Guía de instalación de Oracle ZFS Storage Appliance](#)
- [Actualización de un dispositivo independiente a una configuración en clusters \(BUI\)](#) [66]
- [“Estados de los controladores de cluster”](#) [75]

▼ Comprobación de estado de enlaces de cluster (CLI)

Siga este procedimiento para determinar si los enlaces de cluster están conectados y activos.

Antes de realizar la configuración inicial del cluster (consulte [Actualización de un dispositivo independiente a una configuración en clusters \(BUI\)](#) [66]), debe comprobar que todos los enlaces de cluster estén conectados y activos. Una interrupción en la conexión puede significar que el otro nodo de cluster se está reiniciando, que el enlace no se cableó correctamente o que los cables de cluster no están firmes en sus conectores. Para obtener instrucciones sobre el cableado del cluster, consulte [“Conexión de cables de cluster” en la Guía de cableado de Oracle ZFS Storage Appliance](#).

1. **Vaya a `configuration cluster`.**
2. **Introduzca el comando `links`.**

En los siguientes ejemplos, todos los enlaces están conectados y activos (el estado es AKCIOS_ACTIVE). Un enlace inactivo muestra un estado diferente, por ejemplo, AKCIOS_TIMEDOUT.

En el siguiente ejemplo, se muestran las conexiones de cluster entre dos controladores ZS9-2.

```
hostname:configuration cluster> links

lio_dev/i40e0 = AKCIOS_ACTIVE
lio_dev/i40e1 = AKCIOS_ACTIVE
```

En el siguiente ejemplo, se muestran las conexiones de cluster entre dos controladores ZS7-2 o ZS5-2.

```
hostname:configuration cluster> links

clustron3_ng3:0/clustron_uart:0 = AKCIOS_ACTIVE
clustron3_ng3:0/clustron_uart:1 = AKCIOS_ACTIVE
clustron3_ng3:0/dlpi:0 = AKCIOS_ACTIVE
```

Otros controladores muestran salidas `links` similares. La única diferencia se encuentra en la porción anterior a `/clustron` o `/dlpi`. Por ejemplo, `clustron3_ng3:0` en el ejemplo anterior es `clustron3:0` para los controladores ZS5-4, `clustron2:0` para los controladores ZS4-4 y `clustron2_embedded:0` para los controladores ZS3-2.

Temas relacionados

Para obtener instrucciones sobre la forma de ver el estado de cada controlador, consulte [Cierre de una configuración en clusters \(CLI\) \[71\]](#). Para obtener descripciones de los estados de controlador, consulte [“Estados de los controladores de cluster” \[75\]](#).

▼ Actualización de un dispositivo independiente a una configuración en clusters (BUI)

Siga este procedimiento para configurar un dispositivo independiente de modo que sea un nodo de una configuración en cluster.

Nota - Se recomienda firmemente usar la BUI como la interfaz para configurar controladores en cluster.

Antes de empezar Verifique lo siguiente:

- Los dos controladores que estarán en el cluster nuevo deben ser del mismo modelo. Es posible agrupar en cluster un controlador 7420 con una CPU de 2 GHz o 2,40 GHz y un controlador 7420 con una CPU de 1,86 GHz o 2,00 GHz.
- El segundo controlador es nuevo o se restableció a los valores de configuración de fábrica. Consulte [“Restablecimiento de configuración de fábrica” en el Manual de servicio del cliente de Oracle ZFS Storage Appliance](#).

- Que el dispositivo independiente esté encendido. No es necesario apagar el dispositivo independiente durante este procedimiento.

1. Conecte los cables del cluster entre el dispositivo independiente y el segundo controlador.

Para obtener instrucciones sobre el cableado del cluster, consulte [“Conexión de cables de cluster” en la Guía de cableado de Oracle ZFS Storage Appliance](#).

2. En el segundo controlador, conecte los cables de alimentación en la fuente de alimentación 0 y la fuente de alimentación 1. A continuación, conecte cada cable a la fuente de alimentación externa.

El segundo controlador se enciende automáticamente.

3. Conecte el segundo controlador a los estantes de discos.

Consulte la documentación que vino incluida con el dispositivo o consulte [“Introducción al cableado” en la Guía de cableado de Oracle ZFS Storage Appliance](#).

4. En el controlador independiente, vaya a Configuración > Cluster.

5. Confirme que los enlaces de comunicación entre los dos controladores estén conectados y activos.

Todas las conexiones de cluster deben ser líneas continuas como se muestra en [“Vista de configuración de clusters de la BUI” \[63\]](#) o deben tener el estado AKCIOS_ACTIVE como se muestra en [Comprobación de estado de enlaces de cluster \(CLI\) \[65\]](#). Una interrupción en la conexión puede significar que el otro controlador se está reiniciando, que el enlace no se cableó correctamente o que los cables de cluster no están firmes en sus conectores. Para obtener instrucciones sobre el cableado del cluster, consulte [“Conexión de cables de cluster” en la Guía de cableado de Oracle ZFS Storage Appliance](#).

6. Haga clic en CONFIGURAR.

7. Introduzca el nombre del host correspondiente al segundo controlador y la misma contraseña root configurada en el primer controlador.

Nota - La configuración inicial del cluster puede tardar varios minutos en finalizar.

8. En el controlador independiente, vaya a Configuración > Cluster y bloquee la interfaz de gestión.

Haga clic en el ícono de candado  de la interfaz de gestión para bloquearla.

El bloqueo de la interfaz de gestión para el controlador impide que se haga una transferencia de recursos cuando se produce un failback.

9. **Desde el controlador independiente, configure la interfaz de gestión para el segundo controlador.**
 - a. **Vaya a Configuración > Red y haga clic en el ícono de agregación  que se encuentra junto a Interfaces.**
 - b. **Introduzca un nombre para la interfaz de gestión y seleccione las casillas Activar interfaz y Permitir administración.**
 - c. **Seleccione una dirección IP y haga clic en Aplicar.**
10. **Vaya a Configuración > Cluster y haga clic en FAILBACK para pasar el cluster al modo activo-activo.**

Los dos controladores quedan configurados como pares en cluster.
11. **En el segundo controlador, vaya a Configuración > Cluster y bloquee la interfaz de gestión.**

Haga clic en el ícono de candado  de la interfaz de gestión para bloquearla.

Temas relacionados

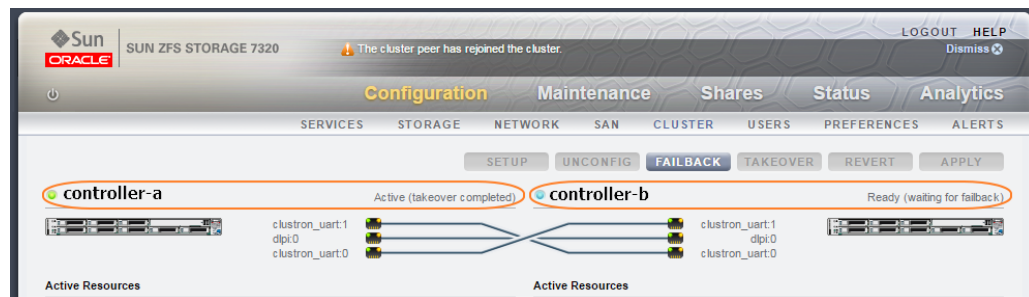
- [“Conexión de cables de cluster” en la Guía de cableado de Oracle ZFS Storage Appliance](#)
- [“Vista de configuración de clusters de la BUI” \[63\]](#)
- [Comprobación de estado de enlaces de cluster \(CLI\) \[65\]](#)
- [“Toma de control y failback en clusters” \[81\]](#)

▼ Cierre de una configuración en clusters (BUI)

Use este procedimiento para cerrar una configuración en clusters. Es posible encender ambos controladores para restaurar un cluster que se cerró a la misma configuración de cluster previa al cierre.

1. **Desde uno de los controladores par, vaya a Configuration (Configuración) > Cluster.**
2. **Determine el estado del cluster de cada controlador.**

En la siguiente figura, el controlador activo es controller-a, y el controlador en espera es controller-b.



En la siguiente tabla, se describen los pares válidos de estados de controlador (controladores activos y en espera) que se pueden ver.

controller-a	controller-b	Estado
 Activo	 Activo	Ambos controladores están funcionando en un estado de cluster normal.
 Activo (toma de control completada)	 Listo (esperando failback)	controller-a es el propietario de los recursos y es el controlador activo. controller-b se encuentra en modo de energía en espera y no tiene recursos. Para limitar el número de veces que se mueve una agrupación, apague primero el controlador en espera.
 Activo (toma de control completada)	 Volviendo a unirse al cluster...	El controller-b se está reiniciando y el controller-a tiene todos los recursos.
 Activo (toma de control completada)	Desconocido (desconectado o reiniciando)	controller-b está apagado o se está reiniciando, o bien todos los enlaces de interconexión del cluster están inactivos.

3. Inicie sesión en la BUI de controller-b y haga clic en el ícono de encendido  ubicado en la parte izquierda debajo de la cabecera.

Nota - Para limitar el número de veces que se mueve una agrupación, apague primero el controlador en espera.

4. **En la BUI de `controller-a`, vaya a Configuración > Cluster para confirmar que `controller-b` está apagado, con el estado de cluster Desconocido (desconectado o reiniciando).**

5. **En la BUI de `controller-a`, haga clic en el ícono de encendido  ubicado en la parte izquierda debajo de la cabecera.**

6. **(Opcional) Use Oracle ILOM para confirmar que ambos controladores están apagados.**

Introduzca el siguiente comando en Oracle ILOM:

```
->show /SYS power_state
```

Para obtener información sobre cómo acceder a ILOM, consulte [“Inicio de sesión en Oracle ILOM de manera remota mediante una interfaz de línea de comandos”](#) en el *Manual de servicio del cliente de Oracle ZFS Storage Appliance*.

7. **Apague los estantes de discos.**
 - a. **Coloque los interruptores de encendido/apagado de la fuente de alimentación en la posición de apagado "O".**
 - b. **Desconecte los cables de alimentación de la fuente de alimentación externa del armario.**

Nota - Se deben desconectar todos los cables de alimentación para cortar por completo la energía del estante de discos.

Para obtener más información, consulte [“Powering Off a Disk Shelf”](#) in *Oracle ZFS Storage Appliance Installation Guide*.

Temas relacionados

- [“Descripción de la agrupación en clusters”](#) [75]
- [“Gestión de recursos de clusters”](#) [78]
- [“Toma de control y failback en clusters”](#) [81]
- [“Cambios de configuración en un entorno en cluster”](#) [82]

▼ Cierre de una configuración en clusters (CLI)

Use este procedimiento para cerrar una configuración en clusters. Es posible encender ambos controladores para restaurar un cluster que se cerró a la misma configuración de cluster previa al cierre.

1. **Vaya a configuration cluster.**
2. **Determine el estado del cluster de cada controlador.**

En el siguiente ejemplo, controller-a es el propietario y está en estado activo. Su par, controller-b, es el controlador en espera y está en estado segmentado.

```
controller-a:>configuration cluster
controller-a:configuration cluster> get
      state = AKCS_OWNER
      description = Active (takeover completed)
      peer_asn = 365ed33c-3b9d-c533-9349-8014e9da0408
      peer_hostname = controller-b
      peer_state = AKCS_STRIPPED
      peer_description = Ready (waiting for failback)
```

En la siguiente tabla, se describen los pares de estados de controlador (state y peer_state) que se pueden ver.

controller-a	controller-b	Estado
AKCS_CLUSTERED	AKCS_CLUSTERED	Ambos controladores están funcionando en un estado de cluster normal.
AKCS_OWNER	AKCS_STRIPPED	controller-a es el propietario de los recursos y es el controlador activo. controller-b se encuentra en modo de energía en espera y no tiene recursos. Para limitar el número de veces que se mueve una agrupación, apague primero el controlador SEGMENTADO.
AKCS_OWNER	REINICIANDO	controller-a tiene todos los recursos. controller-b se está reiniciando.
AKCS_OWNER	DESCONOCIDO	controller-a tiene todos los recursos. controller-b está apagado o se está reiniciando, o bien todos los enlaces de interconexión del cluster están inactivos.

3. **Apague controller-b.**

```
controller-b:configuration cluster> cd /
controller-b:> maintenance system poweroff
This will turn off power to the appliance. Are you sure? (Y/N)Y
```

Nota - Si ambos controladores tienen el estado AKCS_CLUSTERED, se inicia automáticamente una toma de control en el controlador superviviente.

4. **En controller-a, verifique que controller-b se haya apagado y se encuentre en el estado OWNER/unknown.**

```
controller-a:configuration cluster> get
      state = AKCS_OWNER
      description = Active (takeover completed)
      peer_asn = 365ed33c-3b9d-c533-9349-8014e9da0408
      peer_hostname = controller-b
      peer_state = OWNER/unknown
      peer_description =
```

5. **Apague controller-a.**

```
controller-a:configuration cluster> cd /
controller-a:> maintenance system poweroff
This will turn off power to the appliance. Are you sure? (Y/N) Y
```

6. **(Opcional) Use Oracle ILOM para confirmar que ambos controladores están apagados.**

Introduzca el siguiente comando en Oracle ILOM:

```
->show /SYS power_state
```

Para obtener información sobre cómo acceder a ILOM, consulte [“Inicio de sesión en Oracle ILOM de manera remota mediante una interfaz de línea de comandos”](#) en el *Manual de servicio del cliente de Oracle ZFS Storage Appliance*.

7. **Apague los estantes de discos.**
- a. **Coloque los interruptores de encendido/apagado de la fuente de alimentación en la posición de apagado "O".**
 - b. **Desconecte los cables de alimentación de la fuente de alimentación externa del armario.**

Nota - Se deben desconectar todos los cables de alimentación para cortar por completo la energía del estante de discos.

Para obtener más información, consulte [“Powering Off a Disk Shelf”](#) in *Oracle ZFS Storage Appliance Installation Guide*.

Temas relacionados

- [“Descripción de la agrupación en clusters” \[75\]](#)
- [“Gestión de recursos de clusters” \[78\]](#)
- [“Toma de control y failback en clusters” \[81\]](#)
- [“Cambios de configuración en un entorno en cluster” \[82\]](#)

▼ Anulación de la configuración de un nodo de cluster

En este procedimiento, se describe la forma de anular la configuración de un nodo de cluster para el funcionamiento independiente. Un nodo de cluster con la configuración anulada no se puede restaurar a la misma configuración de cluster, ya que la operación de anulación de la configuración es destructiva y produce una pérdida de datos.



Atención - En general, no debe anular la configuración de un nodo de cluster por cuenta propia. La anulación de la configuración de un nodo de cluster produce una pérdida de datos. Póngase en contacto con el soporte de Oracle.

A continuación, se enumeran los motivos por los que se puede anular la configuración de una agrupación en clusters:

- Ya no se desea usar la agrupación en clusters. En cambio, se desea configurar dos dispositivos de almacenamiento independientes.
- Se reemplaza un controlador de almacenamiento con fallos por lo siguiente:
 - Hardware nuevo
 - Un controlador de almacenamiento con software de dispositivo recién recibido de la fábrica

Nota - El proveedor de servicios debe realizar este reemplazo.

1. **Realice una copia de seguridad de los recursos de almacenamiento del cluster.**
2. **En el primer controlador (controlador A), realice un restablecimiento de fábrica.**
Consulte [“Restablecimiento de fábrica de controladores en cluster”](#) en el *Manual de mantenimiento del cliente de Oracle ZFS Storage Appliance*.

3. **Cuando el controlador A comience a reiniciarse, desactive inmediatamente su energía.**

Verifique el estado de apagado del controlador. Consulte [“Estados de los controladores de cluster” \[75\]](#).

4. **Desconecte por completo el controlador A, incluidos todos los cables de cluster, SAS y de red.**

5. **En el segundo controlador (controlador B), vaya a Configuración > Cluster y haga clic en DESCONFIGURAR.**

El controlador B puede seguir entregando datos.

6. **(Opcional) Vuelva a configurar el cluster.**

El controlador B ahora es un dispositivo independiente, y el controlador A se restablece a los valores de fábrica y se apaga. Si desea volver a configurarlos en un cluster, siga las instrucciones en [Actualización de un dispositivo independiente a una configuración en clusters \(BUI\) \[66\]](#).

Terminología de clusters

Los estados de cluster y los tipos de recursos se describen en [“Descripción de la agrupación en clusters” \[75\]](#).

- **Exportar:** permite que un recurso quede inactivo en un controlador determinado.
- **Failback:** permite pasar del estado AKCS_OWNER al estado AKCS_CLUSTERED, en el que todos los recursos externos (los que se asignaron al par) son exportados y, luego, importados por el par.
- **Importar:** permite que un recurso quede activo en un controlador determinado.
- **Par:** el otro controlador en un cluster, también llamado controlador en espera en algunas ocasiones.
- **Volver a unir:** permite recuperar y volver a sincronizar el mapa de recursos del par.
- **Recurso:** un objeto físico o virtual presente, y posiblemente activo, en uno o ambos controladores.
- **Toma de control:** permite pasar del estado AKCS_CLUSTERED o AKCS_STRIPPED al estado AKCS_OWNER, en el que se importan todos los recursos.

Descripción de la agrupación en clusters

Un cluster es un metasistema compuesto por dos controladores de dispositivos y un almacenamiento compartido. El subsistema de agrupación en clusters se compone de tres bloques de creación principales:

- Subsistema de E/S de cluster: el subsistema de E/S de cluster y el dispositivo de hardware (los puertos de E/S de cluster) proporcionan el transporte para la comunicación entre los controladores en el cluster y son responsables de la supervisión del estado de cada par. Consulte [“E/S de interconexión del cluster” \[76\]](#).
- Gestor de recursos: utiliza el transporte de modo que los proveedores de servicios de datos y otros subsistemas de gestión puedan interactuar con el sistema de agrupación en clusters. Consulte [“Gestión de recursos de clusters” \[78\]](#).
- Interfaces de usuario de gestión de cluster: proporcionan las operaciones de configuración, asignación de recursos, supervisión, fallback y toma de control.

Un cluster aumenta la disponibilidad y reduce las interrupciones de las actividades de las siguientes maneras:

- Si uno de los controladores experimenta algún fallo de hardware o software, el segundo controlador presta el servicio hasta que se repara o se reemplaza el primer controlador.
- La actualización gradual del software puede reducir las interrupciones de las actividades comerciales asociadas con la migración a software más reciente.

Cada controlador puede recibir asignaciones de almacenamiento, redes y otros recursos del juego de recursos disponible para el cluster. Según la forma en que se asignan recursos a los controladores, el cluster puede tener una de las siguientes topologías:

- *activo-activo*: a cada controlador del cluster se le asignan al menos una agrupación de almacenamiento y los recursos de red que los clientes necesitan para acceder a los datos almacenados en esa agrupación.
- *activo-pasivo*: al controlador designado como *activo* se le asignan una sola agrupación de almacenamiento y los recursos de red que los clientes necesitan para acceder a los datos almacenados en esa agrupación.

Si uno de los controladores falla, el otro controlador (el *par*) toma el control de todos los recursos conocidos y proporciona los servicios asociados con esos recursos.

Estados de los controladores de cluster

Los nodos de controlador en clusters se encuentran en uno de los siguientes estados en cualquier momento dado.

TABLA 12 Estados de clusters

Estado de BUI/CLI	Descripción
 La agrupación en clusters no está configurada AKCS_UNCONFIGURED	Todavía no se configuró la agrupación en clusters. El cluster se está configurando o la tarea de configuración del cluster nunca se completó. Normalmente, el controlador par se encuentra en el estado Desconocido (desconectado o reiniciando).
Desconocido (desconectado o reiniciando) DESCONOCIDO	El controlador está apagado o se está reiniciando, todos los enlaces de interconexión del cluster están inactivos o todavía no se configuró la agrupación en clusters.
 Activo (toma de control completada) AKCS_OWNER	Se configuró la agrupación en clusters y este controlador tomó el control de todos los recursos compartidos del cluster. Un controlador ingresa en este estado en los siguientes casos: ■ Inmediatamente después de que se completa la configuración del cluster desde la interfaz de usuario del controlador. ■ Cuando este controlador detecta que su par falló, por ejemplo, después de una toma de control. El controlador permanece en este estado hasta que un administrador ejecuta manualmente una operación de failback. Consulte “Toma de control y failback en clusters” [81].
 Listo (esperando failback) AKCS_STRIPPED	Se configuró la agrupación en clusters y este controlador no controla ninguno de los recursos compartidos. Un controlador ingresa en este estado en los siguientes casos: ■ Inmediatamente después de que se completa la configuración del cluster desde la interfaz de usuario del controlador par de este controlador. ■ Después de un reinicio, una desconexión de la energía o algún otro fallo. El controlador permanece en este estado hasta que un administrador ejecuta manualmente una operación de failback. Consulte “Toma de control y failback en clusters” [81].
 Activo CLUSTERED	La agrupación en clusters está configurada, y ambos nodos son propietarios de recursos compartidos según las asignaciones de recursos. Si cada nodo es propietario de una agrupación ZFS y se encuentra en el estado En cluster, los dos nodos forman lo que comúnmente se denomina un cluster activo-activo.
 Volviendo a unirse al cluster... REINICIANDO	El dispositivo se reinició recientemente, o el software de gestión del dispositivo se está reiniciando después de un fallo interno. El estado de los recursos se está resincronizando.

E/S de interconexión del cluster

Todas las comunicaciones entre los controladores constan de uno o varios mensajes transmitidos por los enlaces de E/S de cluster redundantes que proporciona la tarjeta de interfaz de cluster de controlador. Para obtener más información sobre las tarjetas de interfaz de cluster

y el cableado de clusters, consulte [“Puertos de E/S de cluster de controladores”](#) en la *Guía de cableado de Oracle ZFS Storage Appliance* y [“Conexión de cables de cluster”](#) en la *Guía de cableado de Oracle ZFS Storage Appliance*.

- Los controladores ZS9-2 utilizan la agrupación en clusters basada en Ethernet con dos puertos Ethernet en el adaptador Ethernet de cuatro puertos 10GBASE-T de Oracle.
- Los controladores ZS7-2, ZS5-x, ZS4-4, ZS3-x y 7x20 utilizan la agrupación en clusters en serie con dos enlaces de cluster serie y brindan conectividad Ethernet a través de un enlace. El enlace Ethernet aumenta el rendimiento del transporte para los mensajes sin latido, como la sincronización para volver a unirse, y proporciona un latido de respaldo.

Los controladores en clusters únicamente se comunican entre sí mediante una red privada segura establecida por las interconexiones del cluster, nunca mediante interfaces de red previstas para mantenimiento o administración. El mensaje pertenecerá a una de dos categorías generales: los latidos regulares utilizados para detectar el fallo de un controlador remoto y el tráfico de nivel superior asociado con el gestor de recursos y el subsistema de gestión del cluster.

Los latidos se envían, y se esperan, en todos los enlaces. Los latidos se transmiten de forma continua en intervalos fijos. Nunca se confirma la recepción de los latidos y estos no se retransmiten, ya que todos los latidos son idénticos y no contienen información exclusiva. Existe otro tipo de tráfico. Este tráfico se confirma, se verifica y se retransmite según sea necesario para mantener un transporte confiable para el software de nivel superior.

En los controladores ZS9-2, los mensajes de latidos se envían en intervalos de 200 ms. Si no se recibe ningún mensaje después de 1 segundo, se considera que el enlace falló. En los demás controladores, los mensajes de latidos se envían por todos los enlaces de E/S del cluster en intervalos de 50 ms. Si no se recibe ningún mensaje después de 200 ms (enlaces serie) o 500 ms (enlaces Ethernet), se considera que el enlace falló. En todos los controladores, si se produce un fallo en todos los enlaces, se supone que el fallo es del par y se realiza el arbitraje de la toma de control.

Si se produce un aviso grave en un controlador ZS9-2, el sistema de agrupación en clusters puede detectar que el par falló en 1200 ms. No se envía ningún mensaje de aviso grave.

Si se produce un aviso grave en un controlador ZS7-2, ZS5-x, ZS4-4, ZS3-x o 7x20, el controlador que genera el aviso transmite un único mensaje de notificación por cada enlace serie. El controlador par inicia la toma de control de inmediato, independientemente del estado de los demás enlaces. Dadas estas características, el subsistema de agrupación en clusters normalmente puede detectar que el par falló dentro de un período de:

- 550 ms si el par dejó de responder o se apagó.
- 30 ms si el par encontró un error fatal de software que generó un aviso grave del sistema operativo.

Todos los valores que se describen en esta sección son fijos. El dispositivo no brinda la posibilidad de ajustar estos parámetros. Los parámetros se proporcionan aquí únicamente con fines informativos y se pueden cambiar en cualquier momento sin previo aviso.

Nota - Para evitar daños en los datos tras la reubicación física de un cluster, verifique que todo el cableado del cluster esté correctamente instalado en la nueva ubicación. Para obtener más información, consulte [“Prevención de situaciones de cerebro dividido” \[92\]](#).

Temas relacionados

- [“Estados de los controladores de cluster” \[75\]](#)

Gestión de recursos de clusters

El gestor de recursos es responsable de garantizar que se haya conectado el juego correcto de interfaces de red, que estén activas las agrupaciones de almacenamiento correctas y que los numerosos parámetros de configuración permanezcan sincronizados entre dos controladores en clusters. La mayoría de las actividades de este subsistema son invisibles para los administradores. Sin embargo, se expone un aspecto importante. Los recursos se clasifican en varios tipos que dictan si el recurso se importa (se hace activo) y, de ser así, cuándo se hace. Tenga en cuenta que la definición de "activo" varía según la clase de recurso. Por ejemplo, una interfaz de red pertenece a la clase neta y se activa cuando se abre la interfaz.

Los tres tipos de recursos más importantes son réplica, único y privado:

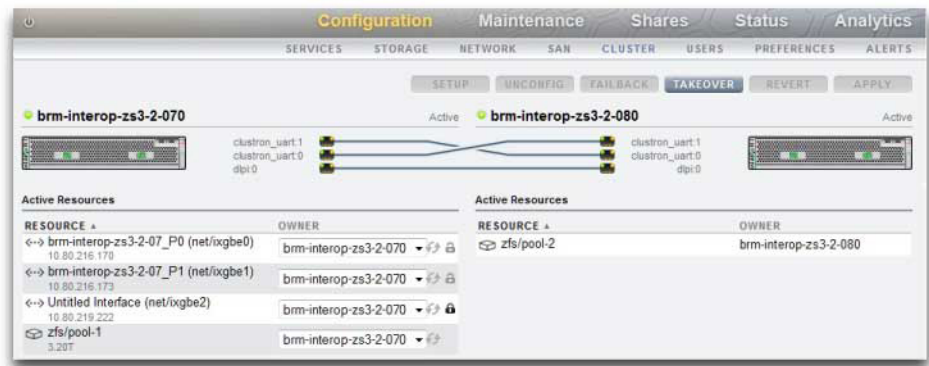
- **Recursos de réplica:** las réplicas son el tipo de recurso más simple; no se exponen nunca a los administradores y no aparecen en la pantalla de configuración del cluster. Las réplicas existen siempre y están siempre activas en ambos controladores. Normalmente, estos recursos simplemente actúan como contenedores de propiedades de servicio que se deben sincronizar entre los dos controladores.
- **Recursos únicos:** al igual que las réplicas, los recursos únicos se utilizan para sincronizar el estado. Sin embargo, se encuentran siempre activos en exactamente uno de los controladores. Los administradores pueden elegir el controlador en el que cada recurso único debe estar activo. Si se produce un fallo en ese controlador, su par importa el recurso único. Los recursos únicos son clave para las características de disponibilidad de la agrupación en clusters. Los únicos son los recursos que los usuarios suelen imaginar que pasan de un controlador con fallos al par superviviente. Estos incluyen las interfaces de red y las agrupaciones de almacenamiento. Como una interfaz de red es una recopilación de direcciones IP utilizadas por los clientes para encontrar un juego conocido de servicios de almacenamiento, es fundamental que se asigne a cada interfaz el mismo controlador que los clientes de la agrupación de almacenamiento esperan ver al acceder a las direcciones de esa interfaz.

- **Recursos privados:** los recursos privados son conocidos solo por el controlador al que se asignan, y nunca se toma el control de ellos al producirse un fallo. Normalmente, esto es útil solamente para las interfaces de red. Consulte el siguiente análisis de casos de uso específicos.

Otro tipo de dato es el *simbionte*. Un simbionte permite que un recurso siga a otro cuando se importa y se exporta. Por ejemplo, se utiliza un simbionte para representar los discos y los dispositivos flash de la agrupación de almacenamiento.

En la siguiente figura, se muestra un ejemplo de una configuración en cluster con recursos compartidos.

FIGURA 4 Ejemplo de configuración en cluster de ZS3-2



En la tabla siguiente, se describen las características de los diferentes tipos de recursos de cluster.

TABLA 13 Tipos de recursos de cluster

Recurso	ícono	Omnipresente	Toma de control cuando hay un fallo
ÚNICO		No	Sí
RÉPLICA	Ninguno	Sí	N/D
PRIVADO		No	No
SIMBIONTE	Ninguno	Mismo tipo que el principal	Mismo tipo que el principal

Cuando se crea un nuevo recurso, inicialmente se lo asigna al controlador en el que se está creando. No se puede cambiar el propietario, a menos que ese controlador se encuentre en el estado AKCS_OWNER. Por lo tanto, es necesario crear recursos en el controlador que debería ser su propietario o tomar el control antes de cambiar la propiedad del recurso. En general, es posible destruir los recursos de cualquier controlador, pero no se pueden destruir las agrupaciones de almacenamiento que se exportan. Normalmente, los mejores resultados se obtienen cuando se destruyen los recursos en el controlador que los controla en ese momento, sin importar qué controlador es el propietario asignado.

La mayoría de los parámetros de configuración, incluidas las propiedades de los servicios, los usuarios, los roles, las reglas de asignación de identidad, las reglas de directorio raíz automático de SMB y las definiciones de iniciador iSCSI se replican automáticamente en ambos controladores. Nunca es necesario configurar estos parámetros en ambos controladores, independientemente del estado del cluster. Si un dispositivo no funciona cuando se realiza el cambio de configuración, el cambio se replicará en el otro dispositivo cuando este se vuelva a unir al cluster en el siguiente inicio, antes de proporcionar servicio. Existen algunas excepciones:

- Las definiciones y las opciones de recursos compartidos y LUN se pueden configurar únicamente en el controlador que tiene el control de la agrupación subyacente, sin importar cuál sea el controlador al que se suele asignar la agrupación.
- La configuración del servicio de identidad (el nombre y la ubicación del dispositivo) no se replica.
- Los nombres proporcionados al chasis son visibles solo en el controlador al que fueron asignados.
- Cada ruta de red está vinculada a una interfaz específica. Si cada controlador tiene asignada una interfaz cuya dirección está en una subred en particular, y esa subred contiene un enrutador al que los dispositivos deben dirigir el tráfico, se debe crear una ruta para cada interfaz, aun cuando se utilice la misma dirección de puerta de enlace. Esto permite que cada ruta pueda estar activa individualmente cuando el control de los recursos de red subyacentes cambie entre los dos controladores. Para obtener más información, consulte [“Consideraciones de la agrupación en clusters para redes” \[86\]](#).
- Las claves de host SSH no se replican y nunca se comparten. Por lo tanto, si no se configuró ninguna interfaz administrativa privada, se pueden esperar discrepancias en las claves al intentar iniciar sesión en la CLI con una dirección asignada a un nodo que falló. Las mismas limitaciones se aplican a los certificados SSL utilizados para acceder a la BUI.

El modelo básico implica que la configuración común se replica de manera transparente y los administradores asignan una recopilación de recursos a cada controlador del dispositivo. Esas asignaciones de recursos forman el enlace de las direcciones de red para los recursos de almacenamiento que los clientes esperan ver. Independientemente de cuál sea el dispositivo que controla la recopilación de recursos, los clientes pueden acceder al almacenamiento que necesitan en las ubicaciones de red que esperan.

Temas relacionados

- [“Consideraciones de la agrupación en clusters para almacenamiento” \[83\]](#)
- [“Consideraciones de la agrupación en clusters para redes” \[86\]](#)

Toma de control y failback en clusters

La toma de control permite que el servicio continúe o vuelva a la normalidad cuando un controlador del cluster falla o pierde energía.

Uno de los controladores intenta automáticamente tomar el control del cluster cuando el controlador detecta que su par está ausente (por ejemplo, se apaga o se reinicia). Después de la toma de control, el controlador que la ejecutó se vuelve el propietario de todos los recursos del cluster y brinda todos los servicios.

Si ambos controladores experimentan un fallo o se apagan, luego de un inicio simultáneo, el software del dispositivo realiza un procedimiento de arbitraje para determinar qué controlador debe continuar con la toma de control.

También es posible realizar la toma de control manualmente, lo que puede ser útil para fines de prueba.

La operación Failback cambia la configuración del cluster de PROPIETARIO-SEGMENTADO (activo-pasivo) a EN CLUSTER-EN CLUSTER (activo-activo). El failback nunca se realiza de manera automática.

Normalmente, el failback se realiza:

- Cuando un controlador vuelve a estar en línea después de una toma de control.
- Como el último paso de configuración de un cluster. Consulte [Actualización de un dispositivo independiente a una configuración en clusters \(BUI\) \[66\]](#).

Si el controlador B de un cluster experimenta un fallo o pierde energía, el controlador A de ese cluster toma el control de los recursos asignados al controlador B y brinda todos los servicios del cluster. Una vez reparado y reiniciado el controlador B, un administrador ejecuta la operación de failback para devolver el controlador B al servicio de producción.

Cuando se repara y se inicia, el controlador B:

- Se vuelve a unir al cluster y resincroniza su vista de todos los recursos, sus propiedades y su propietario.
- Espera que un administrador ejecute una operación de failback.

Mientras el controlador B espera, el controlador A continúa brindando todos los servicios. El controlador A se encuentra en estado Activo (se completó la toma de control) o AKCS_OWNER, y el controlador B se encuentra en estado Listo (a la espera del failback) o AKCS_STRIPPED.

La operación de failback devuelve el controlador B al servicio de producción. El controlador A ha estado brindando todos los servicios desde el fallo en el controlador B. La operación de failback restaura al controlador B los recursos de los que el controlador B era propietario antes del fallo. La operación de failback exporta del controlador A todos los recursos asignados al controlador B, el controlador B importa estos recursos. Después de un failback correcto, tanto el controlador A como el controlador B quedan en estado Activo o EN CLUSTER.

Durante el failback, si el controlador B no puede importar una agrupación debido a un fallo en esta, el controlador B se reinicia. Se produce un fallo en la operación de failback, y el controlador A continúa brindando todos los servicios.

Al programar una operación de failback, tenga en cuenta lo siguiente:

- El failback interrumpe la actividad de los clientes del cluster.
- Demorar el failback genera interrupciones iguales o mayores si se produce un fallo en el único controlador activo antes de que se ejecute el failback.

Para minimizar el tiempo de inactividad del servicio, no se recopilan datos, y las estadísticas y los juegos de datos no están disponibles durante las operaciones de failback y toma de control. Se demoran las solicitudes para suspender o reanudar las estadísticas hasta que se completan las operaciones de failback y toma de control. La recopilación de datos se reanuda automáticamente una vez completadas las operaciones de failback y toma de control.

Temas relacionados

- [“Estados de los controladores de cluster” \[75\]](#)
- [Estimación y reducción del impacto de la toma de control](#)

Cambios de configuración en un entorno en cluster

La mayor parte de la configuración del dispositivo se representa como propiedades de servicio o propiedades de recursos compartidos o LUN. Las propiedades de recursos compartidos y LUN se almacenan con los datos de usuario en la agrupación de almacenamiento para que el propietario actual de ese recurso de almacenamiento pueda acceder a ellas siempre, mientras que la configuración de los servicios se almacena en cada controlador. Para garantizar que

ambos controladores proporcionen un servicio coherente, es necesario sincronizar todas las propiedades de los servicios cuando se produce algún cambio o cuando uno de los controladores que estaba inactivo vuelve a unirse a su par. Como todos los servicios están representados por recursos de réplica, esta sincronización es realizada automáticamente por el software del dispositivo cada vez que se cambia una propiedad en alguno de los controladores.

Por lo tanto, es redundante e innecesario que los administradores repliquen los cambios de configuración. Los procedimientos operativos estándar deberían reflejar este atributo y requerir hacer cambios solamente en uno de los dos controladores del cluster una vez que se haya completado la configuración inicial. El proceso de configuración inicial del cluster replica toda la configuración existente en el par recientemente configurado.

A continuación, se detallan las mejores prácticas para realizar cambios en la configuración en cluster:

- Realizar todos los cambios de configuración de almacenamiento y red en el controlador que actualmente controla (o controlará, si se está creando un nuevo recurso) los recursos de almacenamiento o interfaz de red subyacentes.
- Hacer todos los demás cambios en uno de los controladores, no en los dos. El controlador que especifique como el controlador *maestro* debe depender de cuál de los controladores está funcionando y cuántas agrupaciones de almacenamiento se configuraron.

Oracle ZFS Storage Appliance no tiene ningún mecanismo para realizar cambios independientes en la configuración del sistema de cada controlador. Esta simplificación alivia la necesidad de tener repositorios de configuración centralizados. Se supone que el controlador en funcionamiento en un momento dado tiene la configuración correcta y su par se sincroniza con este al iniciarse. El par adopta un juego de parámetros de configuración que ya están en uso en el sistema de producción existente y, por lo tanto, es altamente probable que sean los parámetros correctos. La mejor práctica es comprobar que el controlador con el fallo vuelva a unirse al cluster tan pronto como se repare.

Temas relacionados

- [“Consideraciones de la agrupación en clusters para almacenamiento” \[83\]](#)
- [“Consideraciones de la agrupación en clusters para redes” \[86\]](#)

Consideraciones de la agrupación en clusters para almacenamiento

Al evaluar un sistema Oracle ZFS Storage Appliance para utilizarlo en una configuración de cluster, tenga en cuenta los siguientes puntos:

- Si todas las agrupaciones son propiedad del mismo controlador o si estas se dividen entre los dos controladores.
- Si desea que haya agrupaciones configuradas con NSPF (No Single Point of Failure, ningún punto único de fallo).

Asignación de propietarios de agrupaciones de almacenamiento: es probable que la decisión más importante sea si el propietario de todas las agrupaciones de almacenamiento será el mismo controlador o si estas agrupaciones se dividirán entre los dos controladores. Hay varias ventajas y desventajas para considerar, como se muestra en [Tabla 14, “Consideraciones de agrupación en clusters para agrupaciones almacenamiento”](#).

Por lo general, las agrupaciones se deben configurar en un único controlador, excepto cuando se esté optimizando la configuración para el rendimiento durante el funcionamiento nominal o cuando no sea relevante el rendimiento en caso de conmutación por error. Los cambios exactos en las características de rendimiento cuando un controlador se encuentre en estado de failover dependerán de la naturaleza y el tamaño de las cargas de trabajo. Por lo general, cuanto más cerca esté un controlador de proporcionar un rendimiento máximo en cualquier eje en particular, mayor será la degradación del rendimiento en ese eje cuando la carga de trabajo sea tomada por el par de ese controlador. Naturalmente, si hay varias agrupaciones, esta degradación corresponderá a ambas cargas de trabajo.

Los dispositivos de caché de lectura se encuentran en el controlador o el estante de discos, según la configuración.

Los dispositivos de caché de lectura, ubicados en una ranura del controlador (L2ARC interna), no siguen a las agrupaciones de datos en las situaciones de toma de control o failback. Los dispositivos de caché de lectura solo están activos en un nodo específico del cluster cuando la agrupación que se asigna al dispositivo de caché de lectura se importa al nodo en el que reside el dispositivo. A menos que se realicen pasos de configuración adicionales, el almacenamiento en caché de lectura no estará disponible para una agrupación que se haya migrado debido a un evento de failover. Para activar un dispositivo de caché de lectura para una agrupación que no es propiedad del par del cluster, se debe tomar el control de la agrupación en el nodo que no es el propietario y, a continuación, agregar almacenamiento y seleccionar los dispositivos de caché para configuración. Los dispositivos de caché de lectura de un nodo de cluster se deben configurar como se describe en [“Configuración del almacenamiento” \[127\]](#). Los dispositivos de log optimizados para escritura se encuentran en el tejido de almacenamiento y siempre están accesibles para el controlador que haya importado la agrupación.

Si los dispositivos de caché de lectura se encuentran en un estante de discos (L2ARC externa), la caché de lectura está siempre disponible. Durante una operación de failback o toma de control, la caché de lectura sigue estando compartida entre los controladores. En este caso, el rendimiento de lectura se mantiene. Para obtener información detallada sobre la configuración de caché de lectura externa, consulte [“Configuraciones de estantes de discos” en el *Manual de servicio del cliente de Oracle ZFS Storage Appliance*](#).

Configuración de NSPF: una segunda consideración importante para el almacenamiento es el uso de configuraciones de agrupación que no tengan puntos únicos de fallo (NSPF). Como el uso de la agrupación en clusters significa que la aplicación valora mucho la disponibilidad, rara vez existe un buen motivo para configurar agrupaciones de almacenamiento que permitan que el fallo de un único estante de discos ocasione una pérdida de disponibilidad. La desventaja de este enfoque es que las configuraciones NSPF requieren una cantidad mayor de estantes de discos que las configuraciones con un único punto de fallo. Cuando la capacidad requerida es muy pequeña, la instalación de suficientes estantes de discos para lograr una configuración NSPF con el nivel RAID deseado puede no ser económica.

En la siguiente tabla, se describen los propietarios de las agrupaciones de almacenamiento en las configuraciones de cluster.

TABLA 14 Consideraciones de agrupación en clusters para agrupaciones almacenamiento

Variable	Controlador único como propietario de las agrupaciones	Varias agrupaciones con diferentes controladores como propietario
Rendimiento total (funcionamiento nominal)	Se puede usar hasta 50% del total de los recursos de la CPU, 50% de DRAM y 50% de la conectividad total de red para proporcionar servicios en cualquier momento dado. Es directo: solo un controlador responde a las solicitudes de los clientes, de manera que el otro está inactivo.	Se puede utilizar la totalidad de los recursos de CPU y DRAM para proporcionar servicio en cualquier momento dado. Se puede usar hasta el 50 % de la conectividad total de red en cualquier momento dado (se necesitan dispositivos de red no visibles en cada controlador para responder en caso de failover).
Rendimiento total (failover)	No hay cambios en el rendimiento en comparación con el funcionamiento nominal.	Se usa el 100 % de los recursos del controlador superviviente para proporcionar servicio. El rendimiento total en comparación con el funcionamiento nominal puede variar entre aproximadamente 40% y 100%, en función de la utilización durante el funcionamiento nominal.
Latencia de E/S	La caché de lectura interna no está disponible durante una operación de failback o toma de control, lo que puede aumentar de manera significativa las latencias para cargas de trabajo con muchas operaciones de lectura que entran en la caché de lectura disponible. La latencia de las operaciones de escritura no se ve afectada. Con configuraciones de caché de lectura externa (EL2ARC), el rendimiento de lectura no se ve afectado. La caché de lectura se comparte entre los pares del	La caché de lectura interna no está disponible durante una operación de failback o toma de control, lo que puede aumentar de manera significativa las latencias para cargas de trabajo con muchas operaciones de lectura que entran en la caché de lectura disponible. La latencia de las operaciones de lectura y escritura puede aumentar debido a una mayor disputa por los recursos del controlador. Esto se debe a que en el controlador superviviente se están ejecutando dos cargas de trabajo en lugar de una sola, como es normalmente el caso. Cuando las cargas de trabajo nominales de cada controlador se aproximan a la capacidad máxima del controlador, las latencias en el estado de conmutación por error pueden ser extremadamente altas. Con configuraciones de caché de lectura externa (EL2ARC), el rendimiento de lectura no se ve afectado.

Variable	Controlador único como propietario de las agrupaciones	Varias agrupaciones con diferentes controladores como propietario
	cluster durante las operaciones de failback o toma de control, lo que hace que no haya latencia de lectura.	La caché de lectura se comparte entre los pares del cluster durante las operaciones de failback o toma de control, lo que hace que no haya latencia de lectura.
Flexibilidad de almacenamiento	Todo el almacenamiento físico disponible puede ser utilizado por los recursos compartidos y los LUN.	Solo el almacenamiento asignado a una agrupación en particular puede ser utilizado por los recursos compartidos y los LUN de esa agrupación. El almacenamiento no se comparte entre las agrupaciones, de manera que si una agrupación se llena, pero otra tiene espacio libre, puede quedar almacenamiento libre sin utilizarse.
Conectividad de red	Todos los dispositivos de red de cada controlador se pueden utilizar mientras ese controlador esté brindando servicio.	Solo la mitad de los dispositivos de red de cada controlador se pueden utilizar mientras ese controlador esté brindando servicio. Por lo tanto, cada agrupación se puede conectar solo a la mitad de las redes físicamente separadas existentes.

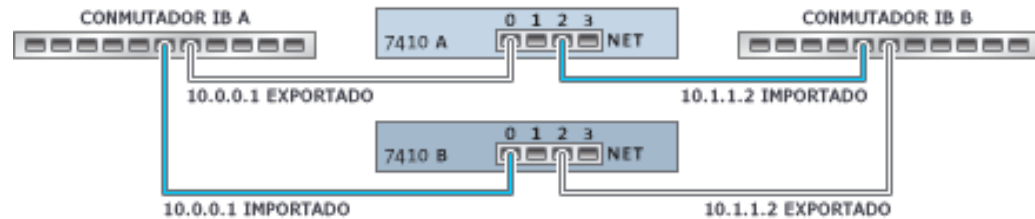
Temas relacionados

- [“Estados de los controladores de cluster” \[75\]](#)

Consideraciones de la agrupación en clusters para redes

Los fallos de los dispositivos de red, los enlaces de datos y las interfaces no ocasionan el fallo de los controladores de un subsistema agrupado en clusters. Para protegerse contra fallos de red, tanto dentro como fuera del dispositivo, se debe usar IPMP y/o LACP. Para que el enfoque relacionado con la disponibilidad sea integral, es necesario configurar correctamente la red y contar con un plan de redundancia que incluya a toda la red.

Las interfaces de red se pueden configurar como recursos únicos o privados, siempre que tengan una configuración de IP estática. Las interfaces configuradas con DHCP deben ser privadas. No se recomienda usar DHCP en clusters. Si se las configura como recurso único, todos los enlaces de datos y los dispositivos utilizados para construir una interfaz pueden estar activos solamente en un controlador a la vez. De manera similar, los dispositivos correspondientes de cada controlador deben estar conectados a las mismas redes para que el servicio se proporcione en un estado de conmutación por error. En la siguiente figura, se muestra un ejemplo.

FIGURA 5 Agrupación en clusters para redes

Para que un cluster funcione correctamente al construir interfaces de red a partir de dispositivos y enlaces de datos, es esencial que cada interfaz única tenga un dispositivo que use el mismo identificador y las mismas capacidades disponibles en ambos controladores. Como los identificadores de los dispositivos dependen del tipo de dispositivo y el orden en el que el dispositivo los detectó originalmente, los controladores en clusters DEBEN tener instalado hardware idéntico. Cada una de las ranuras de ambos controladores debe completarse con hardware idéntico y se las debe completar en el mismo orden en ambos controladores. Su proveedor o representante de servicio autorizado de Oracle lo ayudará a planificar actualizaciones de hardware que cumplan con estos requisitos.

Una ruta siempre está vinculada explícitamente con una única interfaz de red. Las rutas se representan en el gestor de recursos como simbioses. Estas pueden pasar al modo activo solo cuando las interfaces a las que están vinculadas se encuentran en estado operativo. Por lo tanto, una ruta vinculada a una interfaz que se encuentra en el modo de energía en espera (exportada) no tiene efecto hasta que se activa la interfaz durante el proceso de toma de control. Esto es importante cuando hay dos agrupaciones configuradas y ambas están disponibles para una subred común. Si esa subred aloja una ruta que los dispositivos utilizan para alcanzar una o varias redes adicionales, se debe configurar una ruta separada (por ejemplo, una segunda ruta por defecto), la cual se debe vincular con cada una de las interfaces activas y en espera conectadas a esa subred.

Ejemplo:

- La interfaz e1000g3 está asignada a "alice" y la interfaz e1000g4 está asignada a "bob".
- Cada interfaz tiene una dirección en la red 172.16.27.0/24 y puede ser utilizada para proporcionar servicio a clientes de la red 172.16.64.0/22, a la que se accede por medio de 172.16.27.1.
- Se deben crear dos rutas hasta 172.16.64.0/22 vía 172.16.27.1: una vinculada a e1000g3 y la otra a e1000g4.

Es buena idea asignar una dirección IP que se use solo para administración a cada controlador en cluster (probablemente sobre una red de gestión dedicada) y designar la interfaz como

recurso privado. Esto garantiza que sea posible alcanzar un controlador que esté en funcionamiento desde la red de gestión aunque se encuentre en el estado AKCS_STRIPPED y esperando el failback. Esto es importante si se utilizan servicios, como LDAP y Active Directory, y se requiere acceso a otros recursos de red cuando el controlador no esté proporcionando servicio. Si esto no resulta práctico, el procesador de servicio debe estar conectado a una red confiable y/o a un concentrador terminal serie para que se pueda gestionar el controlador desde la consola del sistema.

Si no se realiza ninguna de estas acciones, es imposible gestionar o supervisar un controlador recientemente iniciado hasta que se complete el failback. Se recomienda supervisar o gestionar el controlador que proporciona el servicio para una agrupación de almacenamiento determinada. Es probable que esto sea útil cuando desee modificar algún aspecto del almacenamiento en sí, como una propiedad de un recurso compartido, o para crear un nuevo LUN. Para ello, se puede utilizar una de las interfaces de servicio para realizar tareas administrativas o se puede asignar una interfaz única independiente que se utilice solamente para gestionar la agrupación a la que fue asignada. Cualquiera sea el caso, la interfaz debe asignarse al mismo controlador que la agrupación que se utiliza para gestionar.

Impacto en los clientes de NFSv4.1: ciertos cambios de red en una configuración de cluster pueden afectar negativamente la prestación de servicios de solicitudes de clientes de NFSv4. 1. Si la relación entre una dirección IP y su propietario cambia, la práctica recomendada es volver a montar el sistema de archivos desde el cliente. A diferencia de NFSv4.0, el protocolo NFSv4.1 permite que se asocien conexiones de clientes en varias direcciones IP con la misma concesión de protocolo NFSv4.1. Cuando cambia la relación entre una dirección IP y su propietario, el grupo de direcciones IP que realizan la conmutación por error juntas no es el mismo, lo cual obliga al cliente a restablecer las relaciones de concesión mediante un nuevo montaje de los sistemas de archivos.

Temas relacionados

- [“Interfaces IP locales privadas” \[88\]](#)
- [“Consideraciones de la agrupación en clusters para InfiniBand” \[89\]](#)
- [“Estados de los controladores de cluster” \[75\]](#)

Interfaces IP locales privadas

Use las siguientes directrices al crear interfaces IP locales privadas:

- Si se crea una interfaz IP con el mismo nombre que una interfaz IP privada de un par de cluster, se produce la creación local de una interfaz IP privada.
- Los enlaces de datos que utilizan las interfaces privadas del par no se pueden suprimir, y el botón para suprimir aparece desactivado.

- Todas las interfaces IP que pertenecen a un grupo IPMP deben ser del mismo tipo y pertenecer al mismo controlador. Para crear un grupo IPMP, las interfaces IP utilizadas deben ser todas únicas o todas privadas, y el nodo principal del cluster debe ser el propietario de las interfaces.
- El tipo de grupo IPMP se configura solo en el momento de la creación y está determinado por el tipo de los enlaces subyacentes.
- Las interfaces IP que pertenecen a grupos IPMP no aparecen en la página Recursos del cluster porque la propiedad de la interfaz IP no se puede modificar independientemente de la propiedad del grupo IPMP.
- Los grupos IPMP privados no aparecen en la página Recursos del cluster porque este tipo o propiedad no se puede modificar.

Temas relacionados

- [Consideraciones de la agrupación en clusters para redes](#)

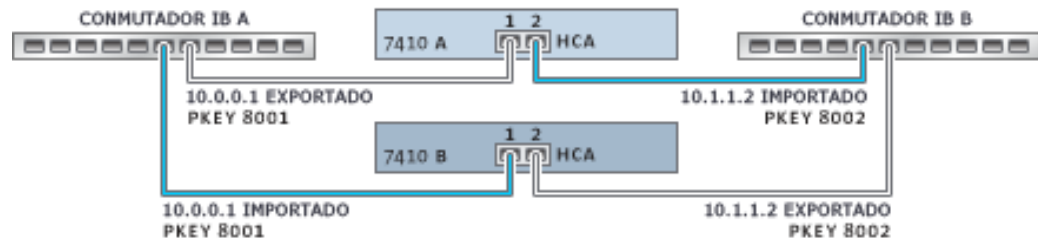
Consideraciones de la agrupación en clusters para InfiniBand

Nota - Los controladores ZS9-2 no admiten InfiniBand.

Al igual que las redes armadas sobre dispositivos Ethernet, las redes InfiniBand necesitan ser parte de una topología de tejido redundante para proteger contra fallos de la red dentro y fuera del dispositivo. La topología de red debe incluir IPMP para proteger contra fallos de red en el nivel del enlace con un plan más amplio para la redundancia de los adaptadores de canal de host, los conmutadores y los gestores de subred.

Para garantizar la configuración adecuada del cluster, cada controlador se debe completar con adaptadores de canal de host idénticos en ranuras idénticas. Asimismo, cada puerto de adaptador de canal de host correspondiente debe configurarse en la misma partición (pkey) del gestor de subred con privilegios de pertenencia idénticos y debe conectarse a la misma red. Para reducir la complejidad y garantizar una redundancia correcta, se recomienda que cada puerto pertenezca solo a una partición de la subred InfiniBand. Las interfaces de red se pueden configurar como recursos únicos o privados, siempre que tengan una configuración de IP estática. Si se configuran como recurso único, todos los enlaces de datos y los dispositivos de la partición InfiniBand utilizados para construir una interfaz pueden estar activos en un solo controlador en cualquier momento dado. En la siguiente figura, se muestra un ejemplo de esto.

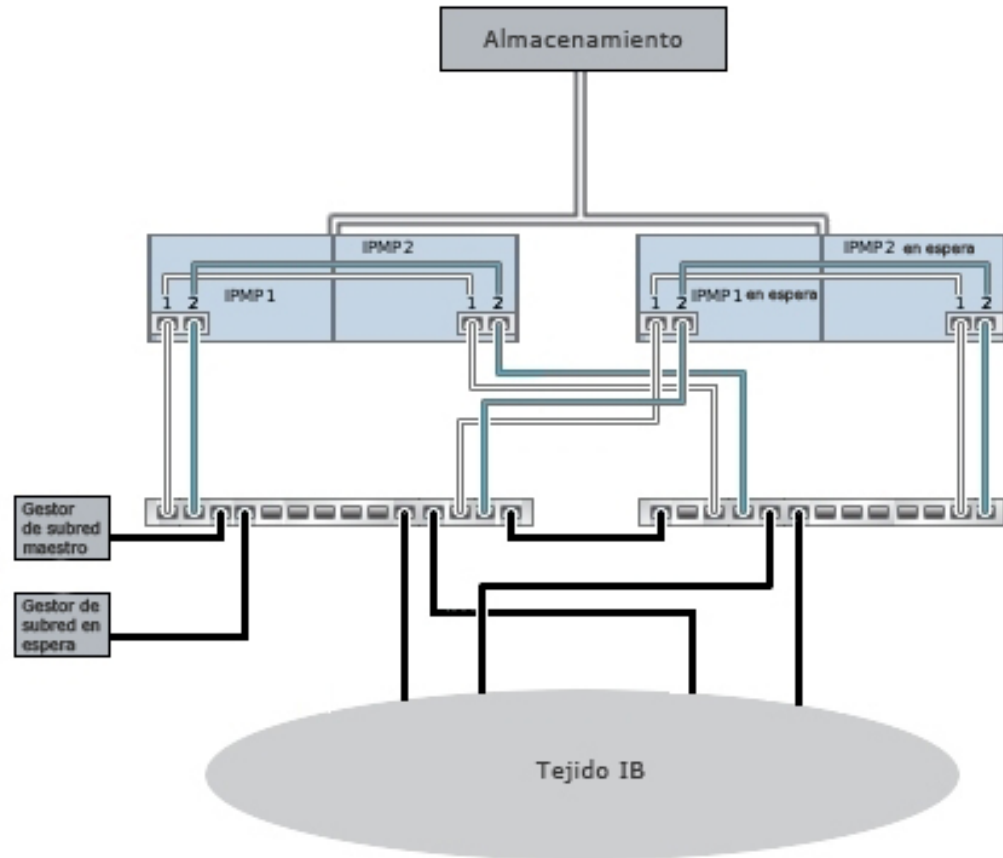
FIGURA 6 Consideraciones de la agrupación en clusters para InfiniBand



Los cambios de pertenencia a la partición de los puertos correspondientes se deben realizar al mismo tiempo. Su proveedor o representante de servicio autorizado de Oracle lo ayudará a planificar actualizaciones de hardware que cumplan con estos requisitos.

En la siguiente figura, se muestra la configuración del cluster para obtener redundancia del gestor de subredes. Se logra una mayor redundancia conectando dos adaptadores de canal de host de puerto doble a un par redundante de conmutadores de servidor.

FIGURA 7 Configuración de clusters para redundancia de gestor de subred



Temas relacionados

- [Consideraciones de la agrupación en clusters para redes](#)

Prevención de situaciones de cerebro dividido

Un modo de fallo común en los sistemas en clusters es el que se conoce como *cerebro dividido*. En este estado, cada uno de los controladores en cluster actúa como si su par hubiera fallado e intenta tomar el control. La causa más común de esta condición es el fallo del medio de comunicación compartido entre los controladores. En Oracle ZFS Storage Appliance, el medio de comunicación compartido son los enlaces de E/S de cluster. Sin embargo, los enlaces de E/S de cluster de Oracle ZFS Storage Appliance tienen redundancia de enlaces incorporada. En los controladores ZS9-2, se requiere un solo enlace Ethernet de E/S de cluster para evitar que se dispare la toma de control. En los demás controladores, se requiere un solo enlace serie de E/S de cluster para evitar que se dispare la toma de control.

El software del dispositivo realiza un procedimiento de arbitraje para determinar cuál es el controlador que debe continuar con la toma de control.

La solución de agrupación en clusters de Oracle ZFS Storage Appliance se diseñó para garantizar que no haya un único punto de fallo y proteger tanto los datos como la disponibilidad contra fallos. Es posible evitar la mayoría de los fallos si se instala correctamente el hardware y se implementan las mejores prácticas de configuración y gestión de clusters. Verifique lo siguiente:

- Todos los enlaces de E/S de cluster (dos para un controlador ZS9-2 y tres para los demás controladores) están conectados y funcionan como se muestra en [“Vista de configuración de clusters de la BUI” \[63\]](#) y [Comprobación de estado de enlaces de cluster \(CLI\) \[65\]](#).
- Todos los cables de almacenamiento están conectados como se muestra en la documentación de configuración que se incluye con los dispositivos.

Es particularmente importante que se detecten dos rutas a cada estante de discos (como se muestra en la siguiente figura) antes de pasar el cluster a producción y que estas rutas se encuentren disponibles en todo momento de allí en adelante, excepto en los cambios transitorios de cables para aumentar la capacidad o reemplazar componentes defectuosos. Utilice las alertas para supervisar el estado de los enlaces de interconexión del cluster y las rutas de los estantes de discos, y corregir con rapidez los posibles fallos. Garantizando la conectividad adecuada, se protege tanto la disponibilidad como la integridad de los datos si falla algún componente de hardware o software.

FIGURA 8 Dos rutas a cada estante de discos en un cluster

Temas relacionados

- [“Estados de los controladores de cluster” \[75\]](#)

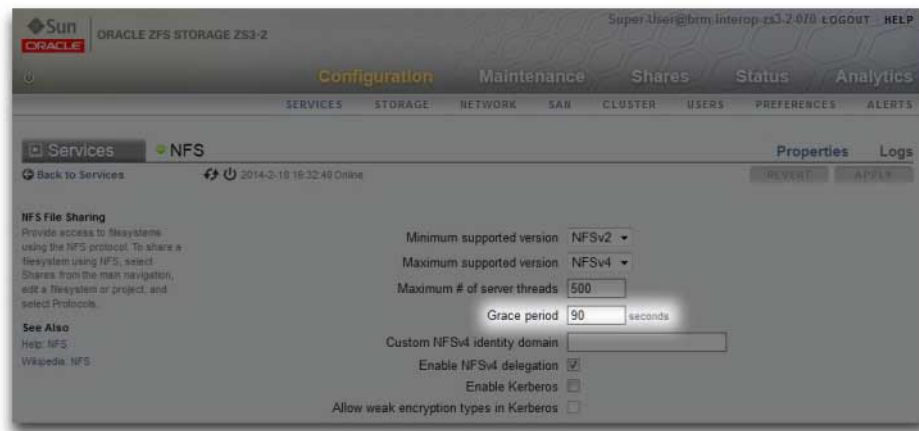
Estimación y reducción del impacto de la toma de control

Durante la toma de control y el failback, existe un intervalo en el cual no se puede proporcionar acceso al almacenamiento para los clientes. La duración de este intervalo varía según la configuración, y los efectos exactos para los clientes dependen de los protocolos que utilizan para obtener acceso a los datos. La comprensión y la mitigación de estos efectos pueden marcar la diferencia entre una implementación de cluster exitosa y un fallo costoso en el peor momento posible.

Los clientes NFS (todas las versiones) normalmente no dejan que el software de la aplicación vea las interrupciones, lo que hace que las operaciones de E/S se demoren mientras el servidor no está disponible. NFSv2 y NFSv3 son protocolos sin estado que se recuperan casi de inmediato cuando se restaura el servicio. NFSv4.0 y NFSv4.1 incorporan un período de gracia de cliente en el inicio durante el cual, generalmente, no se puede realizar E/S. La duración de este período de gracia se puede ajustar en Oracle ZFS Storage Appliance. Si se reduce el período de gracia, se reduce el impacto evidente de la toma de control y el failback. Para interrupciones planificadas, el dispositivo ofrece una recuperación sin período de gracia para

clientes NFSv4.0 y NFSv4.1, lo cual evita la demora del período de gracia. Para obtener más información acerca de la recuperación sin período de gracia, consulte la descripción del período de gracia en [“Propiedades del servicio NFS” \[423\]](#).

FIGURA 9 Propiedad de período de gracia de NFS



El comportamiento de iSCSI durante las interrupciones de servicio depende del iniciador, pero los iniciadores normalmente se recuperan si el servicio se restaura dentro de un período de espera específico del cliente. Consulte la documentación de su iniciador para obtener información detallada adicional. El destino iSCSI normalmente puede proporcionar servicio tan pronto como se completa la toma de control, sin demoras adicionales.

SMB, FTP y HTTP/WebDAV son protocolos orientados a la conexión. Como los estados de sesión asociados con estos servicios no se pueden transferir junto con el almacenamiento y la conectividad de red subyacentes, todos los clientes que usan uno de estos protocolos se desconectan durante la toma de control o el failback, y se deben volver a conectar después de que se completa la operación.

Si bien existen varios factores que afectan la duración de la toma de control y el failback, en la mayoría de las configuraciones, estos tiempos varían según el tiempo requerido para importar los recursos del juego de discos. Los tiempos de importación típicos para cada conjunto de discos varían entre 15 y 20 segundos y de manera lineal con respecto a la cantidad de conjuntos de discos. Un juego de discos está compuesto por la mitad de un estante de discos, siempre que los alojamientos de discos de ese medio estante de discos se hayan completado y asignado a una agrupación de almacenamiento. Los discos no asignados y los alojamientos de discos vacíos no

afectan la duración de la toma de control. El tiempo necesario para importar los recursos de un juego de discos no se ve afectado por los parámetros que los administradores pueden ajustar o alterar. Por lo tanto, si planea utilizar un despliegue en cluster, debe realizar lo siguiente:

- Limitar el almacenamiento instalado de manera que los clientes puedan tolerar los tiempos de toma de control asociados
- Ajustar los valores de timeout en el cliente por encima del tiempo de toma de control máximo esperado

Tenga en cuenta que, si bien la importación de los conjuntos de discos normalmente cubre el grueso del tiempo necesario para llevar a cabo la toma de control, no es el único factor en juego. Durante el proceso de importación de la agrupación, se deben volver a reproducir todos los logs del archivo de intención, y se debe compartir cada recurso compartido y cada LUN mediante los servicios apropiados. La cantidad de tiempo requerida para realizar estas actividades para un único recurso compartido o LUN es muy pequeña (del orden de las decenas de milisegundos), pero si la cantidad de recursos compartidos es muy grande, puede representar una contribución importante para el tiempo total de la toma de control. Dado que se mantiene una cantidad relativamente pequeña de recursos compartidos (unos pocos miles o menos), se puede reducir bastante la duración del proceso.

La duración del failback suele ser mayor que la de la toma de control para cualquier configuración dada. Esto se debe a que el failback es una operación de dos pasos: primero, el dispositivo de origen exporta todos los recursos de los que no es el propietario asignado y, a continuación, el dispositivo de destino realiza el procedimiento de toma de control estándar sobre los recursos que le fueron asignados solamente. Por lo tanto, siempre se necesitará más tiempo para hacer el failback del controlador A al controlador B que el que se necesitará para que el controlador A tome el control sobre el controlador B en caso de fallo. Este tiempo adicional necesario para failback depende mucho menos de la cantidad de conjuntos de discos que se exporta que el tiempo de la toma de control, de manera que una cantidad pequeña de recursos compartidos y LUN puede afectar más la duración del failback que la de la toma de control. También es importante tener presente que el failback es un proceso que siempre debe iniciar un administrador, de manera que se puede programar que la interrupción más prolongada que acarrea ocurra en un horario en el que el nivel de interrupción de las actividades de la empresa sea el menor posible.

Nota - Las duraciones estimadas en esta sección pueden variar según la versión de software/firmware. Es importante hacer una prueba de la operación de toma de control para evaluar el impacto exacto que esta tiene en las aplicaciones de los clientes antes de desplegar una configuración en cluster en un entorno de producción.

Temas relacionados

- [“Toma de control y failback en clusters” \[81\]](#)

- [“Estados de los controladores de cluster” \[75\]](#)

Configuración de red

Las funciones de configuración de red permiten crear una variedad de configuraciones de red avanzadas usando los puertos de red físicos, por ejemplo, agregaciones de enlaces, NIC virtuales (VNIC), LAN virtuales (VLAN) y grupos de rutas múltiples. Puede definir cualquier número de direcciones IPv4 e IPv6 para que estos objetos se conecten con los diversos servicios de datos en el sistema.

La configuración de red de un dispositivo tiene los siguientes componentes. Para configurar las redes, cree enlaces de datos en los dispositivos e interfaces en los enlaces de datos. Seleccione un objeto para ver su relación con otros objetos.

Dispositivos

Los dispositivos de red representan las conexiones de red físicas o las particiones de IP a través de InfiniBand (IPoIB) que corresponden a su red física. El sistema crea los dispositivos de red, que no tienen opciones configurables.

Los dispositivos que representan puertos físicos de la tarjeta de interfaz de red (NIC) del controlador normalmente tienen las etiquetas igb0, igb1, igb2 e igb3. Por ejemplo, el dispositivo igb0 representa el puerto NET-0, mientras que el dispositivo igb1 representa el puerto NET-1. Un puerto de NIC por controlador debe estar configurado como *interfaz de gestión*.

Los dispositivos que representan puertos de InfiniBand físicos en el controlador normalmente tienen las etiquetas ibp0, ibp1, ibp2 e ibp3.

Enlaces de datos

Los enlaces de datos son objetos de la capa 2 para enviar y recibir paquetes de dispositivos de red específicos. Utilice los enlaces de datos para aplicar configuraciones como LACP a los dispositivos de red. Los enlaces de datos pueden tener una correspondencia 1:1 con un dispositivo o una partición IB, o bien se pueden definir enlaces de datos de agregación, VLAN y VNIC compuestos por otros dispositivos y enlaces de datos. Se necesitan los enlaces de datos para completar la configuración de red, aunque estos enlaces no apliquen valores de configuración específicos a los dispositivos de red. Consulte [“Configuración de enlaces de datos de red” \[99\]](#)

Interfaces

Las interfaces son objetos de la capa 3 para IP, configuración de direcciones IP y otras propiedades para enlaces de datos. Cada interfaz IP está asociada con un único enlace de datos o se define como un grupo de acceso de rutas múltiples IP (IPMP) conformado por una agrupación de enlaces de datos, lo cual permite efectuar la migración automática de

direcciones IP desde enlaces de datos con errores a enlaces de datos en funcionamiento. Consulte [“Configuración de interfaces de red” \[104\]](#).

El siguiente ejemplo muestra la configuración de una única dirección IP en un único puerto:

- Dispositivo: igb0
- Enlace de datos: datalink1
- Interfaz: *hostname (IP-address/mask)*

El siguiente ejemplo muestra una configuración para una agregación de enlaces de 3 niveles:

- Dispositivos: igb1, igb2, igb3
- Datalink (Enlace de datos): aggr1 (agregación de LACP)
- Interfaz: *hostname (IP-address/mask)*

Enrutamiento

La configuración del enrutamiento IP controla la manera en la que el sistema dirige los paquetes IP. Consulte [“Configuración de enrutamiento de red” \[121\]](#).

Para configurar la red para el dispositivo, use las siguientes secciones:

- [“Configuración de enlaces de datos de red” \[99\]](#)
- [“Configuración de interfaces de red” \[104\]](#)
- [“Configuración de rutas múltiples de redes IP \(IPMP\)” \[117\]](#)
- [“Configuración de rendimiento y disponibilidad de red” \[121\]](#)
- [“Configuración de enrutamiento de red” \[121\]](#)

Uso de la BUI para configurar las redes

Para asegurarse de mantener la conexión del explorador mientras realiza cambios en la configuración de red, asigne una dirección IP y un dispositivo de red particulares para uso administrativo, como se describe en [“Configuración de interfaces de gestión” \[110\]](#).

La página Configuración > Red > Configuración muestra dispositivos, enlaces de datos e interfaces. La lista Dispositivos muestra el estado del enlace en la parte derecha y un ícono junto al nombre de dispositivo para indicar el estado del puerto de red. Si uno de estos íconos muestra que el dispositivo está inactivo (consulte la tabla a continuación), compruebe que el dispositivo esté conectado correctamente en la red.

Se pueden modificar algunas opciones de configuración arrastrando y soltando una entrada de dispositivo en la columna de enlaces de datos, o una entrada de enlace de datos en la columna de interfaces. Esto puede ser útil en configuraciones complejas. Los movimientos válidos se resaltan.

La página Configuración > Red > Direcciones muestra el nombre de interfaz, la dirección IP y el nombre de host de cada enlace de datos.

La página Configuración > Red > Enrutamiento incluye lo siguiente:

- Muestra el modelo de multiorigen: flexible, adaptable o estricto
- Muestra el destino, la puerta de enlace, la familia, el tipo, el estado y la interfaz de cada ruta
- Permite agregar una ruta estática

La siguiente tabla muestra íconos que se utilizan en la configuración de red.

TABLA 15 Íconos de configuración de red

ícono	Descripción
	Puerto de red conectado
	Puerto de red conectado con actividad de E/S
	Puerto de red desconectado (enlace caído, problema de cable)
	Puerto InfiniBand activo
	Puerto InfiniBand activo con actividad de E/S
	Puerto InfiniBand inactivo (estado caído, inicializando o ARM)
	La partición InfiniBand del dispositivo está en funcionamiento
	La partición InfiniBand del dispositivo no está en funcionamiento (problema de gestor de subred)
	Enlace de datos de red
	VLAN o VNIC de enlace de datos de red
	Agregación de enlaces de datos de red
	VLAN o VNIC de agregación de enlaces de datos de red
	Partición IB de enlace de datos de red
	La interfaz se está utilizando para enviar y recibir paquetes (en funcionamiento o degradada)
	La interfaz fue desactivada por el usuario
	La interfaz está fuera de línea (el propietario es el par de cluster)
	La interfaz presentó un fallo o se la configuró con una dirección IP duplicada

Uso de la CLI para configurar la red

La configuración de red se encuentra en la ruta de acceso `configuration net`, que tiene comandos secundarios para `devices`, `datalinks`, `interfaces` y `routing`.

Utilice el comando `available` para ver qué valores pueden asignarse a la propiedad `links` al crear un componente de red, como se ilustra en el siguiente ejemplo:

```
hostname:configuration net interfaces> ip
hostname:configuration net interfaces ip (uncommitted)> available
igb0,vnic1
```

Configuración de enlaces de datos de red

Los enlaces de datos de red se encargan de gestionar dispositivos y son utilizados por las interfaces. Un enlace de datos puede ser una VLAN, una VNIC, una partición IB o una agregación LACP de dispositivos.

- **LAN virtual (VLAN):** las VLAN se usan para mejorar la seguridad y el aislamiento de la red local. Las VLAN son recomendadas para administrar el dispositivo, de lo contrario, use VNIC.
- **Tarjeta de interfaz de red virtual (VNIC):** las VNIC permiten que los enlaces de datos Ethernet únicos o agregados se separen en varios enlaces de datos (Ethernet) virtuales. De manera opcional, las VNIC se pueden etiquetar con ID de VLAN y pueden permitir el uso compartido de puertos de red físicos en un cluster, como se describe en [“Consideraciones de la agrupación en clusters para redes” \[86\]](#).
- **Particiones InfiniBand (IB):** las particiones InfiniBand se conectan a los dominios de tejido IB aislados por lógica.
- **Protocolo de control de agregación de enlaces (LACP):** LACP se usa para agrupar varios dispositivos de red para que actúen como si fuera uno solo. Esto mejora el rendimiento al aumentar el ancho de banda y mejorar la fiabilidad, gracias a la protección contra fallos en los puertos de red. El dispositivo debe estar conectado con un conmutador que admita LACP y lo tenga activado en esos puertos.

Nota - Los enlaces de datos basados en VNIC y en VLAN no pueden compartir el mismo ID de VLAN.

El estándar de agregación de enlaces IEEE802.3ad no admite explícitamente agregaciones entre varios conmutadores, pero algunos proveedores incluyen compatibilidad para varios conmutadores mediante extensiones propias patentadas. Si un conmutador configurado con esas extensiones respeta el estándar IEEE y las extensiones son transparentes para los nodos de los extremos, el dispositivo admite su uso. Si se encuentra un problema, el servicio de asistencia de Oracle puede necesitar que se reproduzca el problema en una configuración de un solo conmutador.

En la siguiente tabla, se describen las opciones disponibles para configurar enlaces de datos.

TABLA 16 Propiedades del enlace de datos

Propiedad de la BUI	Propiedad de la CLI	Descripción
Nombre	label	Use el nombre personalizado definido. Por ejemplo: "internal", "external", "adminnet", etcétera. El valor por defecto es "Enlace de datos sin título".
Velocidad	speed	Use la velocidad definida. Los valores válidos son auto, 10, 100, 1000 y 10000, que representan negociación automática, 10 Mbit/s forzado, 100 Mbit/s forzado, 1 Gbit/s forzado y 10 Gbit/s forzado. La velocidad y la propiedad dúplex deben coincidir en su configuración, es decir, ambas propiedades deben tener un valor específico forzado o deben estar configuradas con negociación automática. No todos los dispositivos de red admiten el forzado en todas las combinaciones posibles de velocidad y dúplex. No es recomendable desactivar la negociación automática. Sin embargo, si el conmutador tiene la negociación automática desactivada, es posible que se deba forzar una velocidad (y dúplex) para garantizar que el enlace de datos funcione según las propiedades de velocidad y dúplex esperadas.
Dúplex	duplex	Use la dirección de transmisión definida. Los valores válidos de la CLI son auto, half y full, que representan negociación automática, medio dúplex y dúplex completo, respectivamente. La velocidad y la propiedad dúplex deben coincidir en su configuración, es decir, ambas propiedades deben tener un valor específico forzado o deben estar configuradas con negociación automática. Consulte más información en la descripción de la propiedad de velocidad anterior.
VLAN	class=vlan	Use cabeceras de VLAN.
ID de VLAN	id	Use el identificador de VLAN definido; opcional para VNIC.
VNIC	class=vnic	Use una VNIC.
MTU	mtu	Use el tamaño de la unidad de transmisión máxima (MTU) definido. La MTU por defecto tiene 1500 bytes. Especifique una MTU más pequeña (1280 como mínimo) para dejar espacio para paquetes (por ejemplo, para protocolos de túnel). Especifique una MTU más grande (9000 como máximo) para mejorar el rendimiento de red. Todos los sistemas y conmutadores de la misma LAN se deben

Propiedad de la BUI	Propiedad de la CLI	Descripción
		configurar con el valor elegido de MTU. Después de configurar el valor de MTU y haber confirmado la nueva configuración de red para el sistema, puede regresar a la pantalla de la red y ver el estado del enlace de datos para conocer el valor exacto seleccionado de MTU en bytes. Tenga en cuenta que no se puede configurar una VLAN o una VNIC con un valor de MTU mayor que el del enlace de datos subyacente.
Agregación de LACP	aggregation	Use la agregación de LACP de varios dispositivos de red.
Política de LACP	policy	Use la política de LACP definida para seleccionar un puerto saliente. L2 aplica el algoritmo hash a la dirección MAC de origen y destino; L3 utiliza la dirección IP de origen y destino; L4 utiliza el puerto de nivel de transporte de origen y destino.
Modo de LACP	mode	Use el modo de comunicación de LACP definido. En el modo activo, se envía y recibe mensajes de LACP para negociar conexiones y supervisar el estado del enlace. En el modo pasivo, se escucha para recibir mensajes de LACP solamente. En el modo desactivado, se utiliza el enlace agregado pero no se detectan los fallos que pueda haber ni los cambios en la configuración del conmutador. Algunas configuraciones de conmutador de red, como Cisco EtherChannel, no utilizan el protocolo de LACP: el modo de LACP se debe configurar con el valor "desactivado" si en la red se usan agregaciones que no sean LACP.
Temporizador de LACP	timer	Use el intervalo definido entre los mensajes de LACP para el modo activo.
Partición IB	partition	Use particiones IB.
Clave de partición	pkey	Use la partición (dominio de tejido) a la que pertenece el dispositivo del puerto subyacente. La clave de partición se encuentra en el gestor de subredes, donde se configura. La clave de partición se puede definir antes de configurar el gestor de subredes, pero el enlace de datos permanecerá inactivo hasta que se haya configurado la partición de la subred con la GUID del puerto como miembro. La partición de los puertos HCA debe ser congruente con las reglas de “Configuración de IPMP” [375] y “Configuración de clusters de dispositivos” [62] del gestor de subredes.
Modo de enlace IB	linkmode	Use el modo de enlace IB definido. IPoIB proporciona dos modos de enlace: Conectado, que es el valor por defecto, y Datagrama no confiable. Se recomienda usar el modo Conectado en lugar de Datagrama no confiable. Solo deberá usar Datagrama no confiable cuando se requiera por motivos técnicos. El modo Conectado ofrece mayor rendimiento que Datagrama no confiable. El modo Conectado utiliza una MTU de 65520. El modo Unreliable Datagram (Datagrama no confiable) usa una MTU de 2044. El modo Conectado usa pares de colas IB y destina un par de colas locales a la comunicación con un par de colas remotas dedicado. Datagrama no confiable permite que un par de colas locales se

Propiedad de la BUI	Propiedad de la CLI	Descripción
		comunique con varios pares de colas en cualquier host, y los mensajes se comunican sin reconocerse en la capa IB.

▼ Configuración de un enlace de datos de red (BUI)

Use este procedimiento para configurar enlaces de datos, que luego podrán utilizarse para configurar interfaces.

- Vaya a Configuración > Red > Configuración.**
- Haga clic en el ícono de agregación  que se encuentra junto a Enlaces de datos.**
- (Opcional) En el cuadro de diálogo Enlace de datos de red, escribe un Nombre para el enlace de datos.**
Por defecto, el nombre del enlace de datos es "Enlace de datos sin título".
- (Opcional) Configure una MTU personalizada.**
En la propiedad Unidad de transmisión máxima (MTU), especifique lo siguiente:
 - Haga clic en el botón Personalizada.**
 - Escriba el valor 9000 en el campo de texto.**
- (Opcional) Configure las opciones Velocidad de enlace, Dúplex de enlace y Control de flujo.**
Estas opciones están disponibles si no seleccionó las casillas de control VLAN o VNIC en la parte superior del cuadro de diálogo.
- (Opcional) Configure una ID de VLAN.**
Este campo está disponible si seleccionó las casillas de control VLAN o VNIC en la parte superior del cuadro de diálogo.
- Elija uno de los dispositivos de la lista Dispositivos.**
- Haga clic en Aplicar.**
El enlace de datos aparece en la lista Enlaces de datos.

Pasos siguientes

Para modificar un enlace de datos, haga doble clic en el enlace de datos o desplácese sobre el enlace de datos, haga clic en el ícono de edición , realice los cambios y haga clic en el botón Aplicar.

Para suprimir un enlace de datos, desplácese sobre el enlace de datos, haga clic en el ícono de supresión  y confirme que desea suprimir el enlace de datos.

Temas relacionados

- [Configuración de una interfaz de gestión \(BUI\) \[110\]](#)

▼ Configuración de un enlace de datos de red (CLI)

Use este procedimiento para configurar enlaces de datos, que luego podrán utilizarse para configurar interfaces.

1. **Vaya a configuration net datalinks e introduzca el comando device.**

```
hostname:configuration net datalinks> device
```

2. **(Opcional) Configure el nombre del enlace de datos.**

Por defecto, la opción `label` es "Enlace de datos sin título".

```
hostname:configuration net datalinks device (uncommitted)> set label=datalink2
label = datalink2 (uncommitted)
```

3. **Configure un dispositivo para este enlace de datos.**

Configure el valor de la propiedad `links` con el nombre de un dispositivo existente. Use el comando `available` para ver un listado de los dispositivos existentes.

```
hostname:configuration net datalinks device (uncommitted)> available
igb0, igb1
hostname:configuration net datalinks device (uncommitted)> set links=igb1
links = igb1 (uncommitted)
```

4. **(Opcional) Configure la MTU.**

Por defecto, la opción `mtu` o Unidad de transmisión máxima (MTU) está configurada con el valor 1500.

5. **Confirme los cambios.**

```
hostname:configuration net datalinks device (uncommitted)> commit
hostname:configuration net datalinks> show
Datalinks:
```

DATALINK	CLASS	LINKS	STATE	ID	LABEL
igb0	device	igb0	up	-	datalink1
igb1	device	igb1	up	-	datalink2

Temas relacionados

- [Configuración de una interfaz de gestión \(CLI\) \[113\]](#)

Configuración de interfaces de red

Las interfaces configuran las direcciones IP mediante enlaces de datos. Las interfaces admiten las siguientes funciones:

- Protocolos IPv4 e IPv6.
- IPMP: rutas múltiples de redes IP, para mejorar la fiabilidad de la red al permitir que las direcciones IP migren automáticamente de enlaces de datos con errores a enlaces de datos en funcionamiento.

Las interfaces tienen las siguientes opciones de configuración disponibles:

TABLA 17 Propiedades de interfaz

Propiedad de la BUI	Propiedad de la CLI	Descripción
Nombre	label	Nombre personalizado de la interfaz.
Activar interfaz	enable	Se activa el uso de la interfaz para tráfico IP. Si una interfaz está desactivada, el dispositivo ya no enviará ni recibirá tráfico IP por medio de ella, ni usará ninguna de las direcciones IP configuradas en ella. Actualmente, la desactivación de una interfaz IP activa en un grupo IPMP no genera la activación de una interfaz en espera.
Permitir administración	allow	Permite conexiones a la BUI o la CLI de administración del dispositivo por medio de esta interfaz. Si el entorno de red incluye una red de administración independiente, se puede activar solamente para la red de administración para mejorar la seguridad. Consulte Configuración de una interfaz de gestión: BUI , CLI .
Configuración de IPv4 con	v4addrs O v4dhcp	Seleccione Lista de direcciones estáticas (o introduzca valores para v4addrs) o DHCP (o configure v4dhcp con el valor true) para una solicitud dinámica.
Dirección/máscara IPv4	v4addrs	Una o varias direcciones IPv4 en notación CIDR (192.168.1.1/24).
Configuración de IPv6 con	v6addrs O v6dhcp	Seleccione Lista de direcciones estáticas (o introduzca valores para v6addrs) o Configuración automática de IPv6 (o configure v6dhcp con el valor true) para utilizar direcciones locales de enlaces generadas automáticamente (y locales de sitios si responde un enrutador IPv6).
Dirección/máscara IPv6	v6addrs	Una o varias direcciones IPv6 en notación CIDR (1080::8:800:200C:417A/32).

Propiedad de la BUI	Propiedad de la CLI	Descripción
Redes accesibles de manera directa	v4directnets 0 v6directnets	Subredes accesibles de manera directa, expresadas como una dirección IP y una máscara en notación CIDR, a las que la dirección IP local no pertenece, pero con las que el enlace de datos de la interfaz está conectado físicamente. Esto mejora la escalabilidad, ya que conserva las direcciones IP y podría aliviar la congestión de tráfico mediante conmutadores centrales y enrutadores.
Grupo de rutas múltiples IP	links	Configuración de rutas múltiples IP de redes, que permite el uso de una agrupación de enlaces de datos para redundancia.

▼ Creación de una interfaz con un solo puerto (BUI)

Use este procedimiento para configurar un dispositivo de red con un solo puerto.

Antes de empezar Debe existir al menos un enlace de datos. Para crear un enlace de datos, consulte [Configuración de un enlace de datos de red \(BUI\) \[102\]](#).

1. **Vaya a Configuración > Red > Configuración.**
2. **Arrastre un enlace de datos desde la lista Enlaces de datos hasta la lista Interfaces o haga clic en el ícono del elemento para agregar una interfaz .**
3. **En el cuadro de diálogo Interfaz de red, configure las propiedades correspondientes.**
 - **Name (Nombre):** escriba un nombre para la interfaz. Es conveniente que el nombre de la interfaz indique si se trata de una interfaz de gestión.
 - **Activar interfaz:** seleccione esta casilla de control para activar la interfaz.
 - **Use IPv4 Protocol (Usar protocolo IPv4) o Use IPv6 Protocol (Usar protocolo IPv6):** seleccione un protocolo y el tipo de dirección, e introduzca una o varias direcciones IP en notación CIDR.

Para la propiedad Permitir administración, consulte [Configuración de una interfaz de gestión \(BUI\) \[110\]](#).

4. **Elija uno de los enlaces de datos en la lista Enlaces de datos.**
5. **En el cuadro de diálogo Interfaz de red, haga clic en Aplicar.**
La interfaz aparece en la lista Interfaces.
6. **En la esquina superior derecha de la página Configuración > Red > Configuración, haga clic en Aplicar.**

La configuración de red del dispositivo en ejecución no se modificará hasta que realice este paso.

Pasos siguientes

Repita este procedimiento para todas las direcciones IP necesarias. La propiedad de una interfaz se define por el nodo en que se creó esa interfaz. Si se trata de una configuración en clusters, debe crear interfaces en el segundo controlador.

Para modificar esta interfaz, haga doble clic en la interfaz o desplácese sobre la interfaz, haga clic en el ícono de edición , realice los cambios y haga clic en el botón Aplicar.

Para suprimir esta interfaz, desplácese sobre la interfaz, haga clic en el ícono de supresión  y confirme que desea suprimir esta interfaz.

Nota - Cuando se suprime una interfaz, todas las rutas asociadas con la interfaz también se eliminan.

Temas relacionados

- [Configuración de un enlace de datos de red \(BUI\) \[102\]](#)
- [Configuración de una interfaz de gestión \(BUI\) \[110\]](#)

▼ Desbloqueo de interfaces de datos (BUI)

1. Navegue hasta Configuración > Cluster.
2. Elija una interfaz de datos en la lista Recurso.
3. Si el ícono de bloqueo se muestra en negro , haga clic en el ícono para desbloquear la interfaz.

El ícono de bloqueo se mostrará de color gris  cuando se desbloquee la interfaz.

4. Haga clic en Aplicar en la esquina superior derecha de la página.

▼ Desbloqueo de interfaces de datos (CLI)

1. Vaya a `configuration cluster resources` e introduzca el comando `show`.

2. Asegúrese de que todas las interfaces de datos tengan la propiedad `type` configurada con el valor `singleton`.
3. Si una interfaz de datos tiene la opción `type` configurada con el valor `private`, seleccione la interfaz de datos y configure el tipo como `singleton`.

```
hostname:configuration cluster resources zfs/data1> set type=singleton
type = singleton (uncommitted)
hostname:configuration cluster resources zfs/data1> commit
```

▼ Creación de una interfaz y un enlace de datos de partición InfiniBand (BUI)

1. Vaya a Configuración > Red > Configuración.
2. Haga clic en el ícono de agregación de elemento de enlaces de datos .
3. De manera opcional, defina un nombre.
4. Haga clic en la casilla de verificación Partición IB.
5. Elija uno de los dispositivos de la lista Dispositivos de partición.
6. Introduzca un número hexadecimal de cuatro dígitos para la clave de partición, que debe coincidir con la configuración del gestor de subred de InfiniBand.
7. Seleccione el modo de enlace desde el menú desplegable.
8. Haga clic en Aplicar.
El nuevo enlace de datos de la partición aparece en la lista Enlaces de datos.
9. Haga clic en el ícono de agregación de elemento de interfaz .
10. Configure las propiedades deseadas y elija el enlace de datos que creó en el paso anterior.
11. Haga clic en Aplicar.
La interfaz aparece en la lista de interfaces.
12. La configuración de red del dispositivo en ejecución todavía no ha cambiado. Cuando termine de configurar las interfaces, haga clic en Aplicar, en la parte superior, para confirmar la configuración.

▼ Creación de una VNIC sin un ID de VLAN para los controladores en clusters (BUI)

Este ejemplo corresponde a una configuración activa-activa con la mitad de los puertos de red en espera. Esta tarea crea una interfaz IP sobre un enlace de datos del dispositivo y la asigna a un nodo principal. Se crea una VNIC sobre el mismo enlace de datos y se configura una interfaz IP sobre la VNIC y se asigna al otro nodo principal. La configuración de una en lugar de varias VNIC en un enlace de datos determinado garantiza un rendimiento máximo. El tráfico fluye a través del cable asociado con el puerto activo subyacente en un nodo principal, además del puerto en espera subyacente en el otro nodo principal. Por lo tanto, el puerto en espera que de otro modo estaría inactivo se puede usar con las VNIC.

1. **Vaya a Configuración > Red > Configuración.**
2. **Cuando el cluster tiene el estado AKCS_CLUSTERED, haga clic en el ícono de agregación de elemento de enlaces de datos .**
3. **De manera opcional, defina un nombre y un valor para MTU.**
4. **Elija un dispositivo de la lista Dispositivos y haga clic en Aplicar.**
El enlace de datos aparece en la lista Enlaces de datos.
5. **Haga clic en el ícono de agregación de elemento de interfaz .**
6. **Configure las propiedades deseadas, elija el enlace de datos antes creado y haga clic en Aplicar.**
La interfaz aparece en la lista Interfaces.
7. **Haga clic en el ícono de agregación de elemento de enlaces de datos .**
8. **Seleccione la casilla de control VNIC, de manera opcional defina un nombre y una MTU (igual o menor que el valor del paso 2) y haga clic en Aplicar.**
El nuevo enlace de datos VNIC aparece en la lista Enlaces de datos.
9. **Haga clic en el ícono de agregación de elemento de interfaz .**
10. **Configure las propiedades deseadas, elija el enlace de datos VNIC antes creado y haga clic en Aplicar.**
La interfaz aparece en la lista Interfaces.

11. **La configuración de red del dispositivo en ejecución todavía no ha cambiado. Cuando termine de configurar las interfaces, haga clic en Aplicar, en la parte superior, para confirmar la configuración.**
12. **Haga clic en la ficha Cluster.**
Las dos interfaces recientemente creadas aparecen en la sección Recurso con los propietarios por defecto.
13. **Use la lista desplegable Propietario para asignar una de las dos interfaces al otro nodo principal y haga clic en Aplicar.**

▼ Creación de VNIC con el mismo ID de VLAN para controladores en clusters (BUI)

Este ejemplo corresponde a una configuración activa-activa con la mitad de los puertos de red en espera. Esta tarea crea dos VNIC con ID de VLAN idénticos sobre el mismo enlace de datos del dispositivo. Cada VNIC se configura con una interfaz, y cada interfaz se asigna a un nodo principal diferente. El tráfico fluye a través del cable asociado con el puerto activo subyacente en un nodo principal, además del puerto en espera subyacente en el otro nodo principal. Por lo tanto, el puerto en espera que de otro modo estaría inactivo se puede usar con las VNIC.

1. **Vaya a Configuración > Red > Configuración.**
2. **Cuando el cluster tiene el estado AKCS_CLUSTERED, haga clic en el ícono de agregación de elemento de enlaces de datos .**
3. **Seleccione la casilla de control VNIC, de manera opcional defina un nombre y una MTU, defina el ID de VLAN, elija un dispositivo de la lista Dispositivos y haga clic en Aplicar.**
El nuevo enlace de datos VNIC aparece en la lista Enlaces de datos.
4. **Haga clic en el ícono de agregación de elemento de interfaz .**
5. **Configure las propiedades deseadas, elija el enlace de datos VNIC antes creado y haga clic en Aplicar.**
La interfaz aparece en la lista Interfaces.
6. **Cree otra VNIC como se describe en los pasos 2 y 3 con el mismo dispositivo e ID de VLAN, y cree una interfaz para ella como se describe en los pasos 4 y 5.**

7. **La configuración de red del dispositivo en ejecución todavía no ha cambiado. Cuando termine de configurar las interfaces, haga clic en Aplicar, en la parte superior, para confirmar la configuración.**
8. **Haga clic en la ficha Cluster.**

Las dos interfaces recientemente creadas aparecen en la sección Recurso con los propietarios por defecto.
9. **Use la lista desplegable Propietario para asignar una de las dos interfaces al otro nodo principal y haga clic en Aplicar.**

Configuración de interfaces de gestión

Si no configuró una interfaz de gestión durante la configuración inicial, configure un puerto de tarjeta de interfaz de red (NIC) como interfaz de gestión. Una interfaz de gestión es una interfaz de red con acceso administrativo.

Todos los controladores independientes deben tener al menos un puerto NIC configurado como interfaz de gestión. Todas las instalaciones de cluster deben tener al menos un puerto NIC en cada controlador configurado como interfaz de gestión.

Defina la siguiente configuración para controladores en cluster:

- El número de instancia de NIC debe ser único en cada controlador.
- Las interfaces de gestión deben estar bloqueadas.

Una interfaz de gestión permite conexiones con la BUI en el puerto 215 y conexiones con la CLI en el puerto 22 de `ssh`.

Para configurar interfaces de gestión y bloquear las interfaces de gestión del cluster, use los siguientes procedimientos:

- Configuración de una interfaz de gestión: [BUI](#), [CLI](#).
- Bloqueo de una interfaz de gestión del cluster: [BUI](#), [CLI](#)

▼ Configuración de una interfaz de gestión (BUI)

Use este procedimiento para configurar una interfaz de gestión o administrativa.

1. **Vaya a Configuración > Red > Configuración.**

2. Seleccione un enlace de datos.

Puede modificar un enlace de datos existente con la propiedad VNIC configurada o puede crear un nuevo enlace de datos para esta interfaz.

Para crear un nuevo enlace de datos, complete los siguientes pasos. Consulte también [Configuración de un enlace de datos de red \(BUI\) \[102\]](#).

- a. **Haga clic en el ícono de agregación  que se encuentra junto a Enlaces de datos.**
- b. **Haga clic en la casilla de control VNIC.**
- c. **Escriba un nombre para el enlace de datos.**
Es conveniente que el nombre del enlace de datos indique que es para una interfaz de gestión.
- d. **En el cuadro de diálogo Enlace de datos de red, haga clic en Aplicar.**
El enlace de datos aparece en la lista Enlaces de datos.

3. Arrastre este enlace de datos desde la lista Enlaces de datos hasta la lista Interfaces o haga clic en el ícono del elemento para agregar una interfaz .**4. En el cuadro de diálogo Interfaz de red, configure las siguientes propiedades.**

- **Nombre:** escriba un nombre para la interfaz.
- **Activar interfaz:** seleccione esta casilla de control para activar la interfaz.
- **Usar protocolo IPv4 o Usar protocolo IPv6:** seleccione un protocolo y el tipo de dirección, e introduzca una o varias direcciones IP en notación CIDR.

5. Haga clic en la casilla de control Permitir administración.

Seleccione esta casilla de control para configurar esta interfaz como interfaz de gestión. Una interfaz de gestión permite conexiones con la BUI en el puerto 215 y conexiones con la CLI en el puerto 22 de ssh.

6. Elija uno de los enlaces de datos en la lista Enlaces de datos.**7. En el cuadro de diálogo Interfaz de red, haga clic en Aplicar.**

La interfaz aparece en la lista Interfaces.

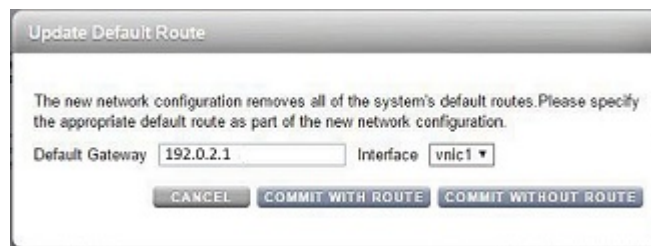
8. En la esquina superior derecha de la página Configuración > Red > Configuración, haga clic en Aplicar.

La configuración de red del dispositivo en ejecución no se modificará hasta que realice este paso.

9. En el cuadro de diálogo Actualizar ruta predeterminada, configure las siguientes propiedades.

- **Puerta de enlace por defecto:** esta es la dirección IP por defecto del enrutador.
- **Interfaz:** seleccione el enlace de datos que asignó a la primera interfaz de gestión.

Nota - Se recomienda especialmente completar este paso, ya que establecer una ruta posibilita la comunicación con el dispositivo por medio de la BUI y la CLI. Sin una ruta, el único medio de comunicación con el dispositivo es una conexión de Oracle ILOM con el SP.



10. Haga clic en Confirmar con ruta.

11. Si se trata de una configuración en clusters, bloquee la interfaz.

Consulte [Bloqueo de una interfaz de gestión del cluster \(BUI\) \[115\]](#). Este paso es opcional pero aconsejable.

Pasos siguientes

Si se trata de una configuración en clusters, repita este procedimiento en el segundo controlador. La propiedad de una interfaz se define por el nodo en que se creó esa interfaz. Si se necesita una interfaz para el segundo controlador en un cluster, cree la interfaz en ese segundo controlador.

Para modificar esta interfaz, haga doble clic en la interfaz o desplácese sobre la interfaz, haga clic en el ícono de edición , realice los cambios y haga clic en el botón Aplicar.

Para suprimir esta interfaz, desplácese sobre la interfaz, haga clic en el ícono de supresión  y confirme que desea suprimir esta interfaz.

Nota - Cuando se suprime una interfaz, todas las rutas asociadas con la interfaz también se eliminan.

Temas relacionados

- [Configuración de un enlace de datos de red \(BUI\) \[102\]](#)
- [Bloqueo de una interfaz de gestión del cluster \(BUI\) \[115\]](#)

▼ Configuración de una interfaz de gestión (CLI)

Use este procedimiento para configurar una interfaz de gestión o administrativa.

1. Vaya a `configuration net datalinks`.

2. Seleccione un enlace de datos.

Utilice el comando `show` para determinar si desea modificar un enlace de datos de clase `vnic` existente o crear un nuevo enlace de datos para esta interfaz.

Para crear un nuevo enlace de datos, complete los siguientes pasos. Consulte también [Configuración de un enlace de datos de red \(CLI\) \[103\]](#).

a. Introduzca el comando `vnic`.

```
hostname:configuration net datalinks> vnic
```

b. Configure un nombre para el enlace de datos.

Es conveniente que el nombre del enlace de datos indique que es para una interfaz de gestión.

```
hostname:configuration net datalinks device (uncommitted)> set label=this-hostname-mgmt-d1
label = this-hostname-mgmt-d1 (uncommitted)
```

c. (Opcional) Configure la MTU.

Por defecto, la opción `mtu` o Unidad de transmisión máxima (MTU) está configurada con el valor 1500.

d. (Opcional) Configure una ID de VLAN (`id`).

e. Confirme los cambios.

```
hostname:configuration net datalinks device (uncommitted)> commit
hostname:configuration net datalinks> show
Datalinks:
```

DATALINK	CLASS	LINKS	STATE	ID	LABEL
igb0	device	igb0	up	-	datalink1
vnic1	vnic	igb0	up	-	this-hostname-mgmt-d1

3. Vaya a `configuration net interfaces` e introduzca el comando `ip`.

```
hostname:configuration net interfaces> ip
```

4. Configure el nombre de esta interfaz.

Configure el valor de la propiedad `label` con el nombre de esta interfaz. Es posible que deba usar el nombre del host para esta VNIC. Si la propiedad `admin` está configurada como `true`, quizás deba indicar que se trata de una interfaz de gestión.

```
hostname:configuration net interfaces ip (uncommitted)> set label="this-hostname-mgmt-if"
label = this-hostname-mgmt-if (uncommitted)
```

5. Defina la propiedad `enable`.

6. Asegúrese de que la propiedad `admin` esté definida con el valor `true`.

7. Configure un enlace de datos para esta interfaz.

Configure el valor de la propiedad `links` con el nombre de un enlace de datos existente. Use el comando `available` para ver un listado de enlaces de datos existentes.

```
hostname:configuration net interfaces ip (uncommitted)> set links=vnic1
links = vnic1 (uncommitted)
```

8. Especifique las direcciones para esta interfaz.

Configure la propiedad `v4addrs` o la propiedad `v6addrs` con las direcciones correspondientes a esta interfaz. Introduzca una o varias direcciones IP en notación CIDR.

9. Confirme los cambios.

```
hostname:configuration net interfaces ip (uncommitted)> commit
hostname:configuration net interfaces> show
```

Interfaces:

INTERFACE	STATE	CLASS	LINKS	ADDRS	LABEL
vnic1	up	ip	vnic1	nn.nn.nnn.nn/nn	this-hostname-mgmt-if

10. Escriba `done`.

11. Configure el enrutamiento.

- Vaya a `configuration net routing` e introduzca el comando `create`.**
- Defina la propiedad `family` con el valor `IPv4` o `IPv6`.**
- Defina la dirección IP de destino (`destination`) y la máscara (`mask`).**
- Configure la dirección IP de la puerta de enlace (`gateway`).**

- e. Defina la opción `interface` con el nombre de la interfaz que creó anteriormente en este procedimiento.
 - f. Introduzca el comando `commit`.
 - g. Escriba `done`.
12. Si se trata de una configuración en clusters, bloquee la interfaz.
- Consulte [Bloqueo de una interfaz de gestión del cluster \(CLI\) \[116\]](#). Este paso es opcional pero aconsejable.

Pasos siguientes

Si se trata de una configuración en clusters, repita este procedimiento en el segundo controlador. La propiedad de una interfaz se define por el nodo en que se creó esa interfaz. Si se necesita una interfaz para el segundo controlador en un cluster, cree la interfaz en ese segundo controlador.

Temas relacionados

- [Configuración de un enlace de datos de red \(CLI\) \[103\]](#)
- [Bloqueo de una interfaz de gestión del cluster \(CLI\) \[116\]](#)

▼ Bloqueo de una interfaz de gestión del cluster (BUI)

Después de la configuración inicial, los controladores en cluster se encuentran en el estado activo-activo. Cuando se produce un failover, el controlador activo toma el control de todas las interfaces no privadas, y el controlador par pasa al modo pasivo y queda inaccesible para la BUI y la CLI. Para mantener el acceso a un controlador independientemente de su estado, bloquee su interfaz de gestión para convertirla en privada. Utilice este procedimiento para bloquear la interfaz de gestión de cada uno de los controladores en un cluster.

Nota - Si no se configuran las interfaces de gestión bloqueadas de los controladores en cluster, es posible que los tiempos de diagnóstico y resolución de fallos sean más extensos.

1. Navegue hasta **Configuración > Cluster**.
2. Elija la interfaz de gestión en la lista **Recurso**.
3. Haga clic en el ícono del candado  para bloquear la interfaz de gestión para este controlador.

La interfaz muestra el ícono de bloqueo .

4. Haga clic en **Aplicar** en la esquina superior derecha de la página.

Pasos siguientes

Repita este procedimiento en el segundo controlador.

Temas relacionados

- [Configuración de una interfaz de gestión \(BUI\) \[110\]](#)

▼ Bloqueo de una interfaz de gestión del cluster (CLI)

Después de la configuración inicial, los controladores en cluster se encuentran en el estado activo-activo. Cuando se produce un failover, un controlador activo toma el control de todas las interfaces no privadas y el controlador par pasa al modo pasivo y queda inaccesible para la BUI y la CLI. Para mantener el acceso a un controlador independientemente de su estado, bloquee la interfaz de gestión para convertirla en una interfaz privada. El siguiente procedimiento bloquea la interfaz de gestión en cada uno de los controladores en cluster.



Atención - Si no se configuran las interfaces de gestión bloqueadas de los controladores en cluster, es posible que los tiempos de diagnóstico y resolución de fallos sean más extensos que lo necesario.

1. Vaya a `configuration cluster resources` e introduzca el comando `show`.
2. Seleccione la interfaz de gestión, precedida por `net/`
3. Para bloquear la interfaz, defina el tipo como privado:

```
hostname:configuration cluster resources net/vnic1> set type=private
type = private (uncommitted)
hostname:configuration cluster resources net/vnic1> commit
```

Pasos siguientes

Repita este procedimiento en el segundo controlador.

Temas relacionados

- [Configuración de una interfaz de gestión \(CLI\) \[113\]](#)

Configuración de rutas múltiples de redes IP (IPMP)

Utilice grupos de rutas múltiples IP de red para proporcionar direcciones IP que seguirán estando disponibles aunque se produzca un fallo en la interfaz IP (por ejemplo, desconexión del cable físico o fallo en la conexión entre un dispositivo de red y su conmutador) o aunque se produzca un fallo de ruta de acceso entre el sistema y sus puertas de enlace de red. Para detectar los fallos, el sistema supervisa el enlace de datos subyacente de la interfaz IP y recibe notificaciones de enlace en funcionamiento y enlace caído; de manera opcional, puede hacer pruebas con direcciones asignadas a tal efecto a cada interfaz IP del grupo, como se describe a continuación. Un grupo IPMP puede tener la cantidad de interfaces IP que se desee, siempre y cuando se encuentren todas en el mismo enlace (LAN, partición IB o VLAN); se puede asignar la cantidad que se desee de direcciones de alta disponibilidad a un grupo IPMP.

Cada interfaz IP de un grupo IPMP se designa como *activa* o *en espera*:

- **Activa:** la interfaz IP se usa para enviar y recibir datos, siempre y cuando IPMP haya determinado que está funcionando correctamente.
- **En espera:** la interfaz IP se usa solamente para enviar y recibir datos si una interfaz activa (o una interfaz en espera que se activó con anterioridad) deja de funcionar.

Se pueden configurar varias interfaces IP activas y en espera, pero cada grupo IPMP debe tener configurada al menos una interfaz IP activa. IPMP intentará activar la mayor cantidad posible de interfaces en espera como sea necesario para mantener la cantidad configurada de interfaces activas. Por ejemplo, si un grupo IPMP se configura con dos interfaces activas y dos interfaces en espera y todas las interfaces están funcionando correctamente, se utilizan solo las dos interfaces activas para enviar y recibir datos. Si una de las interfaces activas presenta un fallo, se activa una de las interfaces en espera. Si la otra interfaz activa presenta un fallo (o la interfaz en espera que se activó), se activa la segunda interfaz en espera. Si posteriormente se reparan las interfaces activas, las interfaces en espera se vuelven a desactivar.

Los fallos de la interfaz IP se pueden detectar mediante la detección basada en enlaces o la detección basada en sondeos (es decir, se configura una dirección de prueba).

Si se activa la detección de fallos basada en sondeos para una interfaz IP, el sistema determina cuáles sistemas de destino se sondearán dinámicamente. Primero se analiza la tabla de enrutamiento para determinar las puertas de enlace (enrutadores) que se encuentran en la misma subred que la dirección de prueba de la interfaz IP y se seleccionan hasta cinco. Si no se encuentran puertas de enlace en la misma subred, el sistema envía un mensaje de sondeo multidifusión ICMP (a 224.0.0.1 para IPv4 o ff02::1 para IPv6) y selecciona los cinco primeros sistemas que respondan de la misma subred. Por lo tanto, para la detección de fallos de red y su reparación con IPMP, debe asegurarse de que al menos un vecino de cada enlace o la puerta de enlace por defecto respondan a las solicitudes de eco de ICMP. IPMP funciona con

configuraciones de direcciones IPv4 e IPv6. En el caso de IPv6, se usa la dirección local de enlace de la interfaz como dirección de prueba.

Nota - No use la detección de fallos basada en sondeos si no hay sistemas (además del par del cluster) en la misma subred que las direcciones de prueba de IPMP que estén configurados para responder solicitudes de eco de ICMP.

El sistema sondeará los sistemas de destino seleccionados en modo de operación por turnos. Si hay cinco sondeos consecutivos que no reciben respuesta, se considera que la interfaz IP presentó un fallo. A la inversa, si hay diez sondeos consecutivos que reciben respuesta, el sistema considera que la interfaz IP que había fallado ya se reparó. Puede configurar el tiempo de detección de fallos de sondeo IPMP del sistema desde la pantalla IPMP. Este tiempo controla de manera indirecta la velocidad de sondeo y el intervalo de reparación; por ejemplo, un tiempo de detección de fallos de 10 segundos significa que el sistema sondea aproximadamente cada dos segundos y que el sistema necesita 20 segundos para detectar una reparación de interfaz a partir del sondeo. No se pueden controlar directamente los sistemas de destino seleccionados por el sistema, pero se pueden controlar de manera indirecta mediante la tabla de enrutamiento.

El sistema supervisará la tabla de enrutamiento y ajustará automáticamente los sistemas de destino seleccionados según sea necesario. Por ejemplo, si el sistema usa destinos detectados por multidifusión, pero posteriormente se agrega una ruta cuya puerta de enlace se encuentra en la misma subred que la dirección de prueba de la interfaz IP, el sistema envía automáticamente un sondeo a la puerta de enlace. De manera similar, si se envían sondeos a destinos detectados por multidifusión, el sistema actualiza periódicamente el conjunto de destinos seleccionados (por ejemplo, porque algunos de los destinos seleccionados anteriormente pueden no estar respondiendo).

Si desea obtener instrucciones paso a paso para crear grupos IPMP, consulte [“Configuración de IPMP” \[375\]](#).

Para obtener información acerca de interfaces locales privadas, consulte [“Configuración de clusters de dispositivos” \[62\]](#).

▼ Creación de un grupo IPMP mediante la detección de fallos por estado del enlace y basada en sondeos (BUI)

Cree una o varias interfaces IP "subyacentes" que se utilizarán como componentes del grupo IPMP. Cada interfaz debe tener una dirección IP que se use como origen del sondeo (consulte [Creación de una interfaz con un solo puerto \(BUI\) \[105\]](#)).

No use la detección de fallos basada en sondeos si no hay sistemas (además del par del cluster) en la misma subred que las direcciones de prueba de IPMP que estén configurados para responder solicitudes de eco de ICMP.

1. Vaya a Configuración > Red > Configuración.
2. Haga clic en el ícono de agregación de elemento de interfaz .
3. De manera opcional, cambie el nombre de la interfaz.
4. Haga clic en la casilla de verificación Grupo de rutas múltiples IP.
5. Haga clic en Usar protocolo IPv4 o Usar protocolo IPv6 y especifique las direcciones IP para la interfaz IPMP.
6. En la lista de interfaces, elija las interfaces creadas en el primer paso.
7. Configure cada una de las interfaces seleccionadas para que estén Activas o En espera, según lo desee.
8. Haga clic en Aplicar.

▼ Creación de un grupo IPMP mediante la detección de fallos por estado del enlace únicamente (BUI)

Cree una o varias interfaces IP "subyacentes" con la dirección IP 0.0.0.0/8 para utilizarlas como componentes del grupo IPMP (consulte [Creación de una interfaz con un solo puerto \(BUI\) \[105\]](#)).

1. Vaya a Configuración > Red > Configuración.
2. Haga clic en el ícono de agregación de elemento de interfaz .
3. De manera opcional, cambie el nombre de la interfaz.
4. Haga clic en la casilla de verificación Grupo de rutas múltiples IP.
5. Haga clic en Usar protocolo IPv4 o Usar protocolo IPv6 y especifique las direcciones IP para la interfaz IPMP.
6. En la lista de interfaces, elija las interfaces creadas en el primer paso.
7. Configure cada una de las interfaces seleccionadas para que estén Activas o En espera, según lo desee.

8. Haga clic en Aplicar.

▼ Ampliación de un grupo IPMP (BUI)

1. Vaya a Configuración > Red > Configuración.
2. Pase el puntero del mouse sobre una de las interfaces de la lista de interfaces.
3. Haga clic en el ícono de movimiento  y, a continuación, arrastre y suelte el dispositivo sobre una interfaz IPMP.
4. Haga clic en Aplicar en la parte superior de la página para confirmar esta configuración.

▼ Creación de una interfaz de enlaces agregados de LACP (BUI)

1. Vaya a Configuración > Red > Configuración.
2. Haga clic en el ícono de agregación de elemento de enlaces de datos .
3. De manera opcional, defina el nombre del enlace de datos.
4. Seleccione Agregación de LACP.
5. Seleccione dos dispositivos o más de la lista de dispositivos y haga clic en Aplicar.
6. Haga clic en el ícono de agregación de elemento de interfaces .
7. Configure las propiedades deseadas, elija el enlace agrupado de la lista de enlaces de datos y haga clic en Aplicar.
8. Haga clic en Aplicar en la parte superior para confirmar la configuración.

▼ Ampliación de una agregación de LACP (BUI)

1. Vaya a Configuración > Red > Configuración.

2. **Pase el puntero del mouse sobre uno de los dispositivos de la lista Dispositivos.**
3. **Haga clic en el ícono de movimiento  y, a continuación, arrastre y suelte el dispositivo sobre un enlace de datos de agregación.**
4. **Haga clic en Aplicar en la parte superior de la página para confirmar esta configuración.**

Configuración de rendimiento y disponibilidad de red

IPMP y la agregación de enlaces son tecnologías diferentes disponibles en el dispositivo para lograr un mejor rendimiento de red y mantener la disponibilidad de la red. Por lo general, se utiliza la agregación de enlaces para obtener un mejor rendimiento de red y se usa IPMP para garantizar una alta disponibilidad. Las dos tecnologías se complementan entre sí y se pueden implementar juntas para proporcionar las ventajas combinadas de rendimiento y disponibilidad de red.

En las agregaciones de enlaces, el tráfico de entrada se distribuye entre los diversos enlaces que componen la agregación. Por lo tanto, el rendimiento de la red mejora a medida que aumenta la cantidad de NIC instaladas para agregar enlaces a la agregación. El tráfico de IPMP usa las direcciones de datos de la interfaz IPMP según su vinculación con las interfaces activas disponibles. Si, por ejemplo, todo el tráfico de datos se transmite entre dos direcciones IP solamente, pero no necesariamente por la misma conexión, la agregación de más NIC no mejorará el rendimiento con IPMP porque sigue habiendo solo dos direcciones IP que se pueden utilizar.

El rendimiento puede verse afectado por el número de VNIC/VLAN configuradas en un enlace de datos para un dispositivo determinado, además de por el uso de un ID de VLAN. La configuración de varias VNIC en un dispositivo determinado puede afectar hasta en un 5 % el rendimiento de todos los enlaces de datos para ese dispositivo, aun cuando no se utilicen VNIC. Si se configuran más de ocho VNIC/VLAN en un enlace de datos determinado, es posible que el rendimiento se reduzca significativamente. Además, si un enlace de datos usa un ID de VLAN, es posible que el rendimiento de todos los enlaces de datos para ese dispositivo se vea afectado en un 5 % adicional.

Configuración de enrutamiento de red

El sistema proporciona una única tabla de enrutamiento IP. Cuando se envía un paquete IP a un destino dado, el sistema selecciona la ruta cuyo destino se asemeje más a la dirección

de destino del paquete (sujeto a la política de multiorigen del sistema). Consulte [“Política de multiorigen” \[124\]](#).

El sistema utiliza la información de la entrada de enrutamiento para determinar desde qué interfaz IP enviará el paquete y, si no es posible alcanzar el destino de manera directa, cuál será la puerta de enlace del siguiente salto.

Si no hay ninguna entrada de enrutamiento que coincida con el destino, el paquete se descarta.

Si hay varias entradas de enrutamiento que son opciones igualmente similares (y la política de multiorigen no les asigna ninguna prioridad por otros motivos), el sistema distribuye la carga entre esas entradas en función de la conexión.

El sistema no actúa como enrutador.

La tabla de enrutamiento tiene las siguientes propiedades para cada ruta.

TABLA 18 Propiedades de ruta

Propiedad de la BUI	Propiedad de la CLI	Descripción
Destino	destination y mask	Rango de direcciones IP de destino (en notación CIDR) que pueden coincidir con la ruta. Una entrada de enrutamiento con un valor de Destino 0.0.0.0/0 coincide con cualquier paquete (si no hay ninguna otra ruta cuya coincidencia sea mayor), por lo que se conoce como la ruta Por defecto. En el cuadro de diálogo de la BUI Insertar ruta estática, puede seleccionar Por defecto o Red como valor de la opción Tipo de ruta.
Puerta de enlace	gateway	Salto (dirección IP) siguiente donde se enviará el paquete (excepto las rutas del tipo "sistema").
Familia	family	Protocolo de Internet: IPv4 o IPv6
Tipo	type	Origen de la ruta: estática, dinámica, dhcp, sistema o directa.
Estado	status	Estado de ruta: activa o inactiva. El estado de ruta inactiva se aplica a una ruta estática o directa asociada con una interfaz IP desactivada o fuera de línea.
Interfaz	interface	Interfaz IP sobre la que se enviará el paquete. Si se especifica una interfaz IPMP, entonces una de las interfaces IP activas del grupo IPMP se elige al azar en función de la conexión y se actualiza automáticamente si posteriormente la interfaz IP seleccionada se vuelve inutilizable. A la inversa, si una interfaz IP dada es parte de un grupo IPMP, no es posible especificarla en la propiedad Interfaz, porque no sería una ruta de alta disponibilidad.

Las entradas de enrutamiento provienen de una serie de orígenes diferentes, según se identifica en la propiedad Tipo. Si bien el origen de una entrada de enrutamiento no incide en el uso que

hace el sistema de ella, el origen controla si se puede editar o suprimir, y cómo se hace. El sistema admite los siguientes tipos de rutas.

TABLA 19 Tipos de ruta admitidos

Tipo	Descripción
Estática	Creada y gestionada por el administrador del dispositivo. Consulte Agregación de una ruta estática: BUI , CLI .
Dinámica	Creada automáticamente por el dispositivo mediante los protocolos de enrutamiento dinámico RIP y RIPng (si están activados).
DHCP	Creada automáticamente por el dispositivo como parte de la activación de una interfaz IP que se configura para usar DHCP. Se crea una ruta DHCP por cada ruta predeterminada proporcionada por el servidor DHCP.
Sistema	Creada automáticamente por el dispositivo como parte de la activación de una interfaz IP. Se crea una ruta de sistema para cada subred IP que el dispositivo puede alcanzar directamente. Como el dispositivo tiene acceso directo a estas rutas, el campo "puerta de enlace" identifica la dirección IP del dispositivo en esa subred.
Directa	Creada y administrada como propiedad de interfaz de red: redes a las que puede accederse de manera directa. Subred a la que puede accederse de manera directa, a la que la dirección IP local no pertenece, pero con la que el enlace de datos de la interfaz está conectado físicamente. Esto mejora la escalabilidad, ya que conserva las direcciones IP y podría aliviar la congestión de tráfico mediante conmutadores centrales y enrutadores. Las rutas directas se configuran como interfaces de red en la pantalla Configuración > Red > Configuración de la BUI o en el contexto <code>configuration net interfaces</code> de la CLI.

Rutas estáticas

Para garantizar que se utilicen las interfaces de red adecuadas para las conexiones de replicación entre los dispositivos de origen y destino, configure rutas estáticas /32 (específicas para el host).

Si está configurando la replicación para una configuración de cluster, seleccione una interfaz de red única (desbloqueada) para que, después de una toma de control o un failback en el cluster, la interfaz pase al nodo en el que se está realizando el trabajo de replicación. Los dos nodos del cluster de origen pueden replicarse en el mismo nodo de destino solo si el nodo de destino proporciona dos direcciones IP, una para cada nodo del cluster de origen. No se puede utilizar la misma dirección IP de destino con ambos nodos de un cluster de origen para hacer la replicación.

Nota - Cuando se suprime una interfaz, todas las rutas asociadas con la interfaz también se eliminan.

- [Flujo de trabajo de replicación remota \[623\]](#)

- [“Conceptos de replicación remota” \[708\]](#)

Política de multiorigen

Si un sistema se configura con más de una interfaz IP, ese sistema puede tener varias rutas equivalentes para un destino dado, lo que obliga al sistema a elegir una interfaz IP sobre la cual enviar el paquete. De manera similar, un paquete puede llegar sobre una interfaz IP pero estar destinado a una dirección IP alojada en otra interfaz IP. El comportamiento del sistema en estas situaciones está determinado por la política de multiorigen seleccionada.

El valor de la política de multiorigen controla la política del sistema para aceptar y transmitir paquetes IP cuando hay varias interfaces IP activadas simultáneamente. El valor de la política de multiorigen puede ser flexible (por defecto), adaptable o estricto.

TABLA 20 Políticas de multiorigen

Política	Descripción
Flexible	No se aplica ninguna vinculación entre un paquete IP y la interfaz IP usada para enviar o recibir el paquete. ■ El paquete IP se acepta sobre la interfaz IP si la dirección IP de destino se encuentra en el dispositivo. ■ El paquete IP se transmite sobre la interfaz IP vinculada a la ruta que mejor coincide con la dirección de destino del paquete IP, sin tener en cuenta las direcciones IP alojadas en esa interfaz IP. Si no hay ninguna ruta elegible, el paquete se descarta.
Adaptativa	Es idéntica a la flexible, excepto que se prefieren las rutas cuya dirección de puerta de enlace se encuentra en la misma subred que la dirección IP de origen del paquete. ■ El paquete IP se acepta sobre la interfaz IP si la dirección IP de destino se encuentra en el dispositivo. ■ El paquete IP se transmite sobre la interfaz IP vinculada a la ruta que mejor coincide con la dirección de destino del paquete IP. Si hay varias rutas que son igualmente específicas, se prefieren las rutas cuya dirección de puerta de enlace se encuentre en la misma subred que la dirección de origen del paquete. Si no hay ninguna ruta elegible, el paquete se descarta.
Estricta	Se requiere una vinculación estricta entre un paquete IP y la interfaz IP usada para enviarlo o recibirlo: ■ El paquete IP se acepta sobre la interfaz IP si la dirección IP de destino se encuentra en esa interfaz IP. ■ El paquete IP se transmite sobre una interfaz IP solamente si la dirección IP de origen se encuentra en esa interfaz IP. Para aplicar esto, al buscar coincidencias con las rutas disponibles, el dispositivo no tiene en cuenta las rutas cuyas direcciones de puerta de enlace se encuentren en una subred que no sea la de la dirección de origen del paquete.

Política	Descripción
	Si no hay ninguna ruta elegible, el paquete se descarta.

Al seleccionar la política de multiorigen, es fundamental considerar si alguna de las interfaces IP del dispositivo estará dedicada a la administración (por ejemplo, para el acceso dedicado de la BUI), lo que significa que se tendrá acceso a ella a través de una red de administración independiente. En particular, si se crea una ruta por defecto para proporcionar acceso remoto a la red de administración y se crea una ruta por defecto independiente para proporcionar acceso remoto a los protocolos de almacenamiento, la política por defecto del sistema (Flexible) puede hacer que la ruta administrativa por defecto se use para tráfico de almacenamiento. Si se cambia a la opción Adaptable o Estricta, el dispositivo considerará la dirección IP asociada con la solicitud como parte de la selección de la ruta para la respuesta. Si no se puede encontrar ninguna ruta en la misma interfaz IP, con la opción de política Adaptable, el sistema usará cualquier ruta disponible, mientras que con la opción Estricta descartará el paquete.

▼ Agregación de una ruta estática (BUI)

Después de definir la ruta estática desde el dispositivo de origen al dispositivo de destino, repita estos pasos en el dispositivo de destino para definir la ruta estática desde el destino al origen.

- Vaya a Configuración > Red > Enrutamiento en el dispositivo de origen.**
- Haga clic en el ícono de agregación de elemento  ubicado a la izquierda de Entradas de tabla de enrutamiento.**
- En el cuadro de diálogo Insertar ruta estática, defina las propiedades.**
 Seleccione un protocolo para la opción Familia (IPv4 o IPv6).
 En la opción Tipo, seleccione Red.
 Especifique una dirección en la opción Destino (la dirección IP del dispositivo de origen) y una dirección en la opción Puerta de enlace.
 Seleccione una interfaz.
- Haga clic en Agregar.**
 La nueva ruta aparece en la tabla.
- Vaya a Configuración > Red > Enrutamiento en el dispositivo de destino.**
- Repita los pasos 2 a 4.**

El valor de Destino es la dirección IP del dispositivo de origen.

▼ Agregación de una ruta estática (CLI)

Después de definir la ruta estática desde el dispositivo de origen al dispositivo de destino, repita estos pasos en el dispositivo de destino para definir la ruta estática desde el destino al origen.

Use una ruta estática /32 (específica para el host) hasta la dirección IP del sistema de destino mediante la interfaz de red dedicada.

1. **Vaya a `configuration services routing` en el dispositivo de origen.**

2. **Introduzca `create`.**

3. **Escriba `show` o `get` para mostrar las propiedades.**

4. **Defina las propiedades.**

Defina `family`, `destination`, `mask`, `gateway` e `interface`.

El valor de `destination` es la dirección IP del dispositivo de destino.

El valor de `mask` debe ser 32; esto indica que se trata de una ruta estática y específica del host.

Puede utilizar la finalización con tabulación para ver una lista de valores para `family` e `interface`.

5. **Introduzca el comando `commit`.**

6. **Vaya a `configuration services routing` en el dispositivo de destino.**

7. **Repita los pasos 2 a 5.**

El valor de `destination` es la dirección IP del dispositivo de origen.

Pasos siguientes Para asegurarse de que el tráfico se redirija a través de las interfaces de origen y destino correctas, use el comando `traceroute`.

▼ Supresión de una ruta estática (BUI)

1. **Vaya a Configuración > Red > Enrutamiento.**

2. **Mueva el cursor sobre la entrada de la ruta y haga clic en el ícono de la papelera  a la derecha.**

▼ Supresión de una ruta estática (CLI)

1. Vaya a `configuration net routing`.
2. Escriba `show` o `get` para mostrar las rutas y sus nombres.
3. Introduzca `destroy route-name`.

▼ Cambio de la propiedad de multiorigen a Estricta (BUI)

1. Vaya a Configuración > Red > Enrutamiento.
2. En el área Modelo de multiorigen, en la parte superior de la página, haga clic en Estricta.

▼ Cambio de la propiedad de hosts de conexión múltiple a estricto (CLI)

1. Vaya a `configuration net routing`.
2. Escriba `set multihoming=strict`.
3. Introduzca el comando `commit`.

Configuración del almacenamiento

El dispositivo usa agrupaciones de almacenamiento para gestionar dispositivos de almacenamiento físico. Después de configurar estas agrupaciones en función de las características físicas y el nivel deseado de redundancia de datos, puede almacenar sistemas de archivos y LUN, que en su conjunto se denominan recursos compartidos, en estas agrupaciones. Los recursos compartidos, que están incluidos en los proyectos, crecen automáticamente dentro del espacio de disco asignado a la agrupación, y las agrupaciones pueden abarcar varios dispositivos de almacenamiento. Si bien no hay necesidad de asignar un tamaño estático a los recursos compartidos, puede controlar el uso del espacio mediante cuotas y reservas. Para obtener más información, consulte [“Gestión de espacio de recursos compartidos” \[539\]](#).

Para configurar y gestionar el almacenamiento, realice las siguientes tareas:

- Creación de una agrupación de almacenamiento: [BUI](#), [CLI](#).
- Importación de una agrupación de almacenamiento existente: [BUI](#), [CLI](#).
- Configuración de una agrupación de almacenamiento solo con unidades flash: [BUI](#), [CLI](#).
- Agregación de un estante de discos a una agrupación de almacenamiento existente: [BUI](#), [CLI](#).
- Agregación de un dispositivo de caché, un metadispositivo o un dispositivo de log a una agrupación de almacenamiento existente: [BUI](#), [CLI](#).
- Eliminación de un dispositivo de caché o log de una agrupación de almacenamiento existente: [BUI](#), [CLI](#).
- Desconfiguración de una agrupación de almacenamiento: [BUI](#), [CLI](#).
- Cambio de nombre de una agrupación de almacenamiento: [BUI](#), [CLI](#).
- Limpieza manual de una agrupación de almacenamiento: [BUI](#), [CLI](#).
- Limpieza programada de una agrupación de almacenamiento: [BUI](#), [CLI](#).
- Visualización de agrupación y estado de dispositivo: [BUI](#), [CLI](#).

Para comprender los conceptos básicos de almacenamiento, consulte estos temas:

- [Conceptos de agrupaciones de almacenamiento](#)
- [Perfiles de datos para agrupaciones de almacenamiento](#)
- [Gestión de espacio de recursos compartidos](#)

▼ Creación de una agrupación de almacenamiento (BUI)

Las agrupaciones de almacenamiento almacenan datos y se pueden crear durante o después de la configuración inicial. Las agrupaciones pueden incluir unidades de datos, dispositivos de log, dispositivos de caché de lectura y metadispositivos.

Las agrupaciones pueden estar cifradas. Utilice este procedimiento para crear una agrupación no cifrada. Para crear una agrupación cifrada, consulte [Creación de una agrupación cifrada \(BUI\) \[810\]](#). No puede agregar información de cifrado a una agrupación que se creó sin cifrar.

En este procedimiento, se supone que ya finalizó la configuración inicial. La creación y la configuración de una agrupación de almacenamiento es un proceso de dos pasos. Primero, los dispositivos de almacenamiento se verifican para determinar que estén presentes y ofrezcan un mínimo de funcionalidad, y se asignan unidades o incluso estantes de discos completos a la agrupación. En segundo lugar, debe seleccionar un perfil para las unidades en función de las

necesidades de almacenamiento. Si por algún motivo se desconfigura una agrupación, la puede importar como se describe en [Importación de una agrupación de almacenamiento existente \(BUI\) \[134\]](#).

Para reducir los datos redundantes, que pueden ser especialmente considerables en las cargas de trabajo de replicación, tenga en cuenta los beneficios de usar la deduplicación. Asigne metadispositivos si la deduplicación se activará para proyectos o recursos compartidos de esta agrupación. Para obtener más información, consulte [Data Deduplication](#). También existe una agrupación de almacenamiento que solo tiene unidades flash, que utiliza SSD como dispositivos de datos y dispositivos de log opcionales, pero no incluye dispositivos de caché de lectura ni metadispositivos. Consulte [Configuración de una agrupación de almacenamiento solo con unidades flash \(BUI\) \[137\]](#).

- Antes de empezar**
- Para obtener recomendaciones sobre la cantidad de unidades que se deben seleccionar por agrupación, consulte [“Número de dispositivos por agrupación” \[165\]](#).
 - Para comprender los distintos perfiles de datos, consulte [“Perfiles de datos para agrupaciones de almacenamiento” \[167\]](#).
 - No realice una operación de configuración de agrupación cuando haya una actualización de firmware de disco en curso. Para comprobar si hay alguna actualización en curso, navegue hasta Maintenance (Mantenimiento) > System (Sistema).
 - Para usar la función de deduplicación de datos mejorada en una agrupación de almacenamiento, actualice a la versión OS8.7.0 o posterior del software y acepte todas las actualizaciones diferidas, incluso la deduplicación de datos v2. Consulte [“Data Deduplication v2 Deferred Update” in Oracle ZFS Storage Appliance Customer Service Manual](#).

1. **Vaya a Configuración > Almacenamiento.**
2. **Haga clic en el ícono de agregación , junto a Agrupaciones disponibles.**
3. **Escriba un nombre para la agrupación de almacenamiento y haga clic en Aplicar.**
4. **Seleccione el número de unidades de datos para la agrupación de almacenamiento para cada estante de discos deseado. También puede seleccionar dispositivos de caché, log y metadispositivos disponibles.**

Para obtener más información sobre dispositivos de log, caché y metadispositivos, consulte [“Perfiles de datos para agrupaciones de almacenamiento” \[167\]](#).

Confirm that all devices are present and minimally functional, and allocate them to a storage pool. ABORT COMMIT

Verify and allocate devices Step 1 of 2

Verify that storage is correctly attached and functioning. If devices are missing or malfunctioning, they will not be available for use and cannot be added without reconfiguring the pool. It is recommended that you fix any problems before configuring storage on the appliance. Mixing device types and speeds is strongly discouraged.

NAME	MODEL	TYPE	RPM	DATA	LOG	CACHE	META
chena	Sun Netra X4270 M3	System	--	-	-	-	-
1236FMT002	Oracle Storage DE2-24C	HDD	7200	5 (13.6T)	-	0 (1G)	0 (1G)
1236FMT001	Oracle Storage DE2-24C	HDD	7200	24 (65.5T)	-	0 (1G)	0 (1G)
1237FMT00H	Oracle Storage DE2-24C	HDD	7200	20 (54.6T)	2 (137G)	0 (1G)	0 (1G)



Atención - Una vez que un disco de datos se agrega a una agrupación, ya no se puede eliminar sin destruir la agrupación por completo y perder todos los datos.

Si no aparecen todos los estantes de discos conectados, haga clic en Abortar, compruebe los cables y la alimentación del estante de discos y vuelva a iniciar este procedimiento.

- Si todas las unidades son del mismo tamaño o tienen la misma velocidad de rotación, o si se selecciona uno de los tamaños, por defecto se asigna el número máximo de unidades disponibles. Si el dispositivo de almacenamiento incluye unidades de distintos modelos o distintas velocidades de rotación, no se asigna ninguna unidad por defecto.
- Nota: Se recomienda que la agrupación incluya únicamente los dispositivos que comparten el mismo tamaño y la misma velocidad de rotación, a fin de que las características de rendimiento sean coherentes.
- Supervise o limite el uso de espacio ya que puede experimentar rendimiento reducido cuando las agrupaciones alcanzan la capacidad total.

5. Haga clic en Confirmar.

Las unidades se asignan a la agrupación de almacenamiento y se las verifica para determinar que estén presentes y ofrezcan un mínimo de funcionalidad. Si la verificación falla, haga clic en Abortar, corrija el problema y vuelva a iniciar este procedimiento. Si asigna una agrupación con dispositivos defectuosos o faltantes, no podrá agregar los dispositivos defectuosos o faltantes más adelante.

6. En la pantalla Seleccionar perfil de almacenamiento, seleccione el perfil de datos que cumpla con los objetivos de confiabilidad, disponibilidad, facilidad de mantenimiento y rendimiento.

Para obtener una descripción de cada perfil, haga clic en el nombre del perfil de datos o consulte [“Perfiles de datos para agrupaciones de almacenamiento” \[167\]](#).

7. Si asignó dispositivos de log, caché o metadispositivos, seleccione los perfiles apropiados.

- Para dispositivos de log, haga clic en Log Profile (Perfil de log) y seleccione el perfil reflejado o segmentado. Seleccione el perfil reflejado si asignó un número par de dispositivos de log a la agrupación.



Atención - Si se produce un fallo doble, se pueden perder datos de un log en una configuración segmentada. Se recomienda configurar un perfil de log reflejado para la redundancia agregada. Para obtener más información, consulte [“Perfiles de datos para agrupaciones de almacenamiento” \[167\]](#).

- Para los dispositivos de caché, el perfil siempre es segmentado, tal como se muestra en Cache Profile (Perfil de caché).
- Para metadispositivos, haga clic en Metadata Profile (Perfil de metadatos) y seleccione el perfil reflejado o segmentado.

Nota - Una vez que se agregan metadispositivos a una agrupación de almacenamiento, ya no se pueden eliminar de la agrupación.

8. Haga clic en Confirmar.

Temas relacionados

- [“Perfiles de datos para agrupaciones de almacenamiento” \[167\]](#)
- [Importación de una agrupación de almacenamiento existente \(BUI\) \[134\]](#)
- [Agregación de un estante de discos a una agrupación de almacenamiento existente \(BUI\) \[141\]](#)
- [Cambio de nombre de una agrupación de almacenamiento \(BUI\) \[154\]](#)
- [“Conceptos de agrupaciones de almacenamiento” \[164\]](#)
- [Desduplicación de datos](#)

▼ Creación de una agrupación de almacenamiento (CLI)

Las agrupaciones de almacenamiento almacenan datos y se pueden crear durante o después de la configuración inicial. Las agrupaciones pueden incluir unidades de datos, dispositivos de log, dispositivos de caché de lectura y metadispositivos.

Las agrupaciones pueden estar cifradas. Utilice este procedimiento para crear una agrupación no cifrada. Para crear una agrupación cifrada, consulte [Creación de una agrupación cifrada \(CLI\) \[812\]](#). No puede agregar información de cifrado a una agrupación que se creó sin cifrar.

En este procedimiento, se supone que ya finalizó la configuración inicial. La creación y la configuración de una agrupación de almacenamiento es un proceso de dos pasos. Primero, los dispositivos de almacenamiento se verifican para determinar que estén presentes y ofrezcan un mínimo de funcionalidad, y se asignan unidades o incluso estantes de discos completos a la agrupación. En segundo lugar, debe seleccionar un perfil para las unidades en función de las necesidades de almacenamiento. Si por algún motivo se desconfigura una agrupación, la puede importar como se describe en [Importación de una agrupación de almacenamiento existente \(CLI\) \[135\]](#).

Para reducir los datos redundantes, que pueden ser especialmente considerables en las cargas de trabajo de replicación, tenga en cuenta los beneficios de usar la deduplicación. Asigne metadispositivos si la deduplicación se activará para proyectos o recursos compartidos de esta agrupación. Para obtener más información, consulte [Data Deduplication](#). También existe una agrupación de almacenamiento que solo tiene unidades flash, que utiliza SSD como dispositivos de datos y dispositivos de log opcionales, pero no incluye dispositivos de caché de lectura ni metadispositivos. Consulte [Configuración de una agrupación de almacenamiento solo con unidades flash \(CLI\) \[139\]](#).

- Antes de empezar**
- Para obtener recomendaciones sobre la cantidad de unidades que se deben seleccionar por agrupación, consulte [“Número de dispositivos por agrupación” \[165\]](#).
 - Para comprender los distintos perfiles de datos, consulte [“Perfiles de datos para agrupaciones de almacenamiento” \[167\]](#).
 - No realice una operación de configuración de agrupación cuando haya una actualización de firmware de disco en curso. Para comprobar si hay alguna actualización en curso, navegue hasta `maintenance system updates`.
 - Para usar la función de deduplicación de datos mejorada en una agrupación de almacenamiento, actualice a la versión OS8.7.0 o posterior del software y acepte todas las actualizaciones diferidas, incluso la deduplicación de datos v2. Consulte [“Data Deduplication v2 Deferred Update” in Oracle ZFS Storage Appliance Customer Service Manual](#).

1. Vaya a configuration storage.**2. Introduzca config y un nombre para la agrupación de almacenamiento nueva.**

```
hostname: configuration storage> config pool0
hostname: configuration storage (pool0) verify>
```

3. Introduzca show para ver la información de dispositivo de la agrupación:

```
hostname:configuration storage (pool0) verify> show
ID STATUS ALLOCATION DATA LOG CACHE META RPM
0 ok custom 0 0 0/4 0/4 1.86T
1 ok custom 0 0/2 34G 0 0 15000
2 ok custom 0 0/2 34G 0 0 15000
```

4. Introduzca set y el ID de controlador o de estante de discos, además del número de unidades de datos que desea usar. También puede seleccionar dispositivos de caché, log y metadispositivos disponibles.

Para obtener más información sobre dispositivos de log, caché y metadispositivos, consulte [“Perfiles de datos para agrupaciones de almacenamiento” \[167\]](#).



Atención - Una vez que un disco de datos se agrega a una agrupación, ya no se puede eliminar sin destruir la agrupación por completo y perder todos los datos.

El ID "0" es el controlador, y los ID restantes son los estantes de discos. En el siguiente ejemplo, se usa 1-data=8 para asignar ocho unidades de datos del primer estante de discos.

```
hostname:configuration storage (pool1) verify> set 1-data=8
1-data = 8
```

En este ejemplo, se asigna un dispositivo de caché del controlador:

```
hostname:configuration storage (pool1) verify> set 0-cache=1
0-cache = 1
```

En este ejemplo, se asigna un metadispositivo del controlador:

```
hostname:configuration storage (pool1) verify> set 0-meta=1
0-meta = 1
```

5. Escriba done.

```
hostname:configuration storage (pool1) verify> done
```

6. Escriba show para visualizar el perfil.

```
hostname:configuration storage (pool1) config> show
PROFILE CAPACITY NSPF DESCRIPTION
log_profile = log_stripe 17G no Striped log
```

Nota - Si asignó dispositivos de caché a la agrupación, el perfil siempre está segmentado.

7. Si asignó dispositivos de log a la agrupación, introduzca `set log_profile=` y configure el perfil de log como `log_mirror` o `log_stripe`. Use `log_mirror` si la agrupación incluye un número par de dispositivos de log.



Atención - Si se produce un fallo doble, se pueden perder datos de un log en una configuración segmentada. Se recomienda configurar un perfil de log reflejado para la redundancia agregada. Para obtener más información, consulte [“Perfiles de datos para agrupaciones de almacenamiento” \[167\]](#).

```
hostname:configuration storage (pool1)> set log_profile=log_mirror
```

8. Si asignó metadispositivos a la agrupación, introduzca `set meta_profile=` y configure el metaperfil como `meta_mirror` o `meta_stripe`.

```
hostname:configuration storage (pool1)> set meta_profile=meta_mirror
```

9. Escriba `done` para completar la tarea.

```
hostname:configuration storage (pool1)> done
```

Temas relacionados

- [“Perfiles de datos para agrupaciones de almacenamiento” \[167\]](#)
- [Importación de una agrupación de almacenamiento existente \(CLI\) \[135\]](#)
- [Agregación de un estante de discos a una agrupación de almacenamiento existente \(CLI\) \[143\]](#)
- [Cambio de nombre de una agrupación de almacenamiento \(CLI\) \[155\]](#)
- [“Conceptos de agrupaciones de almacenamiento” \[164\]](#)
- [Desduplicación de datos](#)

▼ Importación de una agrupación de almacenamiento existente (BUI)

La acción de importación permite importar una agrupación de almacenamiento desconfigurada. Una agrupación de almacenamiento puede estar desconfigurada a causa de una acción involuntaria, un restablecimiento de fábrica o una operación de servicio para recuperar datos de usuario. Para importar una agrupación de almacenamiento es necesario escanear todos los dispositivos de almacenamiento conectados y detectar el estado existente. Este proceso puede llevar mucho tiempo durante el cual no es posible realizar otras actividades de configuración de almacenamiento.

Antes de empezar No realice una operación de configuración de agrupación cuando haya una actualización de firmware de disco en curso. Para comprobar si hay alguna actualización en curso, navegue hasta Mantenimiento > Sistema.

1. Vaya a Configuración > Almacenamiento.

Se muestra una lista de agrupaciones de almacenamiento con algunas características de identificación. Si el almacenamiento se destruyó o está incompleto, no se puede importar la agrupación de almacenamiento. A diferencia de la configuración de almacenamiento, el nombre de la agrupación de almacenamiento no se muestra inicialmente, pero sí se lo muestra después de seleccionar la agrupación de almacenamiento.

2. Haga clic en IMPORTAR.

3. Seleccione la agrupación de almacenamiento que desea importar.

Por defecto, se muestran los nombres de la agrupación de almacenamiento anterior.

4. Para cambiar el nombre de la agrupación de almacenamiento, haga clic en el nombre de la agrupación y cámbielo.

5. Haga clic en Confirmar.

Temas relacionados

- [Desconfiguración de una agrupación de almacenamiento \(BUI\) \[152\]](#)
- [Cambio de nombre de una agrupación de almacenamiento \(BUI\) \[154\]](#)

▼ Importación de una agrupación de almacenamiento existente (CLI)

La acción de importación permite importar una agrupación de almacenamiento desconfigurada. Una agrupación de almacenamiento puede estar desconfigurada a causa de una acción involuntaria, un restablecimiento de fábrica o una operación de servicio para recuperar datos de usuario. Para importar una agrupación de almacenamiento, es necesario iterar por todos los dispositivos de almacenamiento conectados y detectar el estado existente que tengan. Este proceso puede llevar mucho tiempo durante el cual no es posible realizar otras actividades de configuración de almacenamiento.

Antes de empezar No realice una operación de configuración de agrupación cuando haya una actualización de firmware de disco en curso. Para comprobar si hay alguna actualización en curso, navegue hasta maintenance system updates.

1. Vaya a configuration storage.

2. Introduzca import.

```
hostname:configuration storage (pool0)> import
```

Search for storage. Begin the process of searching for existing storage pools.

Subcommands that are valid in this context:

```
help [topic]      => Get context-sensitive help. If [topic] is specified,
                    it must be one of "builtins", "commands", "general",
                    "help" or "script".

show              => Show information pertinent to the current context

abort            => Abort this task (potentially resulting in a
                    misconfigured system)

done             => Finish operating on "discover"
```

```
hostname:configuration storage (pool0) discover>
```

3. Escriba done.

4. Introduzca show.

```
hostname:configuration storage (pool0)> show
```

Pools:

POOL	OWNER	DATA PROFILE	LOG PROFILE	STATUS	ERRORS
-> pool0	hostname	mirror	log_stripe	online	0
pool1	hostname	-	-	exported	-

Properties:

```
pool = pool0
status = online
errors = 0
owner = hostname
profile = mirror
log_profile = log_stripe
cache_profile = cache_stripe
scrub = none requested
```

5. Introduzca set pool= y el nombre de la agrupación que desea importar.

Nota - Si tiene una sola agrupación, el nombre de agrupación no se muestra, pero está seleccionado.

```
hostname:configuration storage select> set pool=pool1
pool = pool1
```

Aparece un mensaje para recordarle que verifique que el almacenamiento esté bien conectado y en funcionamiento.

6. Escriba done.

Temas relacionados

- [Desconfiguración de una agrupación de almacenamiento \(CLI\) \[153\]](#)
- [Cambio de nombre de una agrupación de almacenamiento \(CLI\) \[155\]](#)

▼ Configuración de una agrupación de almacenamiento solo con unidades flash (BUI)

Una agrupación de almacenamiento que solo tiene unidades flash utiliza SSD como dispositivos de datos y dispositivos de log opcionales, pero no incluye dispositivos de caché de lectura ni metadispositivos. Las agrupaciones que solo tienen unidades flash son adecuadas para entornos de virtualización o cargas de trabajo de copia de seguridad.

- Antes de empezar**
- Siga las directrices de cableado para estantes que tienen solo unidades flash, según se describe en [“Directrices de cableado y armarios” en la Guía de cableado de Oracle ZFS Storage Appliance](#).
 - Para obtener recomendaciones sobre la cantidad de unidades que se deben seleccionar por agrupación y otras consideraciones y directrices, consulte [“Conceptos de agrupaciones de almacenamiento” \[164\]](#).
 - Para comprender los distintos perfiles de datos, consulte [“Perfiles de datos para agrupaciones de almacenamiento” \[167\]](#).

Nota - No realice una operación de configuración de agrupación cuando haya una actualización de firmware de disco en curso. Para comprobar si hay alguna actualización en curso, navegue hasta Maintenance (Mantenimiento) > System (Sistema).

1. **Vaya a Configuración > Almacenamiento.**
2. **Haga clic en el ícono de agregación  que está arriba de la lista de agrupaciones de almacenamiento.**
3. **Desde la pantalla Verificación y asignación de dispositivos, seleccione la SSD de tipo de almacenamiento y, a continuación, seleccione un tamaño de dispositivo.**

Verify and allocate devices Step 1 of 2

Verify that storage is correctly attached and functioning. If devices are missing or malfunctioning, they will not be available for use and cannot be added without reconfiguring the pool. It is recommended that you fix any problems before configuring storage on the appliance. Mixing device types and speeds is strongly discouraged.

Storage type: ☐ HDD ☒ SSD
 Device size: Any

NAME	MODEL	TYPE	RPM	DATA	LOG	CACHE
sbm-7440b	Oracle ZFS Storage ZS4-4	System	--	-	-	-
1504NMK01M	Oracle Storage DE3-24C	HDD	7200	-	-	-
1407NM400E	Oracle Storage DE3-24P	SSD	--	0 (1.46T)	-	-
1504NMK01W	Oracle Storage DE3-24C	HDD	7200	-	-	-
1242FM4003	Oracle Storage DE2-24P	HDD	10000	-	-	-
1452NMK00T	Oracle Storage DE3-24C	HDD	7200	-	-	-

- Para cada estante de discos de SSD, seleccione el número de unidades que desea incluir en la agrupación.

Nota - Una agrupación que incluye solo unidades flash no puede incluir dispositivos de caché de lectura ni metadispositivos.

- (Opcional) Seleccione los dispositivos de log que desea agregar a la agrupación que incluye solo unidades flash.
- Haga clic en Confirmar.
- En la pantalla Configurar almacenamiento agregado, seleccione el perfil de datos adecuado para la carga de trabajo que equilibre rendimiento, disponibilidad y capacidad.
 Para ver una descripción de los perfiles disponibles, consulte [“Perfiles de datos para agrupaciones de almacenamiento” \[167\]](#).
- (Opcional) Si asignó dispositivos de log, seleccione un perfil adecuado.
- Haga clic en Confirmar.

Temas relacionados

- Configuración de almacenamiento solo con unidades flash
- “Configuración de una alerta de umbral para resistencia de SSD (BUI)” en el *Manual de servicio del cliente de Oracle ZFS Storage Appliance*

▼ Configuración de una agrupación de almacenamiento solo con unidades flash (CLI)

Una agrupación de almacenamiento que solo tiene unidades flash utiliza SSD como dispositivos de datos y dispositivos de log opcionales, pero no incluye dispositivos de caché de lectura ni metadispositivos. Las agrupaciones que solo tienen unidades flash son adecuadas para entornos de virtualización o cargas de trabajo de copia de seguridad.

- Antes de empezar**
- Siga las directrices de cableado para estantes que tienen solo unidades flash, según se describe en [“Directrices de cableado y armarios” en la Guía de cableado de Oracle ZFS Storage Appliance](#).
 - Para obtener recomendaciones sobre la cantidad de unidades que se deben seleccionar por agrupación y otras consideraciones y directrices, consulte [“Conceptos de agrupaciones de almacenamiento” \[164\]](#).
 - Para comprender los distintos perfiles de datos, consulte [“Perfiles de datos para agrupaciones de almacenamiento” \[167\]](#).

Nota - No realice una operación de configuración de agrupación cuando haya una actualización de firmware de disco en curso. Para comprobar si hay alguna actualización en curso, navegue hasta `maintenance system updates`.

1. Verifique que las SSD estén bien conectadas y en funcionamiento.

Si falta algún dispositivo o alguno de los dispositivos no está funcionando bien, haga las correcciones necesarias.

Nota - Una agrupación que incluye solo unidades flash no puede incluir dispositivos de caché de lectura ni metadispositivos.

2. Vaya a `configuration storage`, introduzca `config` y un nombre único para la agrupación:

```
hostname:configuration storage> config allflashpool
```

Se muestran las instrucciones y los subcomandos que se pueden usar en este contexto.

3. Muestre los dispositivos disponibles para la agrupación.

```
hostname:configuration storage verify> show
```

ID	STATUS	ALLOCATION	DATA	LOG	CACHE	RPM	TYPE
0	ok	custom	0	0	0		system
1	ok	custom	0/7 3.46T	0/2 373G	0		ssd
2	ok	custom	0/24 6.55T	0	0		ssd

0 0 0

4. Muestre las propiedades disponibles:

```
hostname:configuration storage verify> help properties
0                               => Chassis 0
1-data                          => Chassis 1 data
1-log                           => Chassis 1 log
2                               => Chassis 2
2-data                          => Chassis 2 data
```

5. Asigne los dispositivos a la agrupación, como se muestra en este ejemplo:

```
hostname:configuration storage verify> set 1-data=3 2-data=3
1-data = 3
2-data = 3
```

En este ejemplo, se asignan 3 dispositivos del chasis 1 (1-data=3) y 3 dispositivos del chasis 2 (2-data=3) a la agrupación.

6. (Opcional) Seleccione los dispositivos de log que desea agregar a la agrupación que incluye solo unidades flash.

7. Escriba `done` para cerrar la verificación.

```
hostname:configuration storage verify> done
```

8. Muestre los tipos de perfil de almacenamiento disponibles:

```
hostname:configuration storage config> show
```

9. Seleccione el perfil de datos adecuado para la carga de trabajo, que equilibre rendimiento, disponibilidad y capacidad.

Para ver una descripción de los perfiles disponibles, consulte [“Perfiles de datos para agrupaciones de almacenamiento” \[167\]](#).

```
hostname:configuration storage config> set profile=
```

10. (Opcional) Si asignó dispositivos de log, seleccione un perfil adecuado.

11. Escriba `done`.

```
hostname:configuration storage config> done
```

Temas relacionados

- [Configuración de almacenamiento solo con unidades flash](#)
- [“Configuración de una alerta de umbral para resistencia de SSD \(CLI\)” en el *Manual de servicio del cliente de Oracle ZFS Storage Appliance*](#)

▼ Agregación de un estante de discos a una agrupación de almacenamiento existente (BUI)

Use la siguiente tarea para agregar un estante de discos a una agrupación de almacenamiento existente.

- Antes de empezar**
- Para obtener recomendaciones sobre la cantidad de unidades que se deben seleccionar por agrupación y otras consideraciones y directrices, consulte [“Conceptos de agrupaciones de almacenamiento” \[164\]](#).
 - Debe seleccionar el mismo perfil de datos que el que se está usando en la agrupación existente. Para comprender los distintos perfiles de datos, consulte [“Perfiles de datos para agrupaciones de almacenamiento” \[167\]](#).
 - Si el almacenamiento es insuficiente para configurar el sistema para el perfil de datos y sus opciones, tal vez algunos atributos no sean admitidos. Por ejemplo, es imposible conservar las características NSPF al agregar un único estante de discos a una configuración RAID de doble paridad con la opción NSPF. Puede agregar el estante de discos, pero no puede usar la opción NSPF.
 - No realice una operación de configuración de agrupación cuando haya una actualización de firmware de disco en curso. Para comprobar si hay alguna actualización en curso, navegue hasta Maintenance (Mantenimiento) > System (Sistema).



Atención - Una vez que un disco se agrega a una agrupación, ya no se puede eliminar sin destruir la agrupación por completo y perder todos los datos.

1. Para instalar el nuevo estante de discos, use [“Agregación de un nuevo estante de discos” en el Manual de servicio del cliente de Oracle ZFS Storage Appliance](#).
2. Vaya a Configuración > Almacenamiento.
3. En la lista Agrupaciones disponibles, seleccione una agrupación en línea a la que desee agregar el estante de discos.
4. Haga clic en Agregar.
5. Para este estante de discos, seleccione el número de unidades de datos para la agrupación de almacenamiento.

Si no aparece el estante de discos nuevo, haga clic en Abortar, compruebe los cables y la alimentación del estante de discos y vuelva a iniciar este procedimiento.

- Si todas las unidades son del mismo tamaño o tienen la misma velocidad de rotación, o si se selecciona uno de los tamaños, por defecto se asigna el número máximo de unidades

disponibles. Si el dispositivo de almacenamiento incluye unidades de distintos modelos o distintas velocidades de rotación, no se asigna ninguna unidad por defecto.

- Nota: Se recomienda que la agrupación incluya únicamente los dispositivos que compartan el mismo tamaño y la misma velocidad de rotación, a fin de que las características de rendimiento sean coherentes.
- Supervise o limite el uso de espacio ya que puede experimentar rendimiento reducido cuando las agrupaciones alcanzan la capacidad total.

6. (Opcional) Agregue los dispositivos de caché o log del estante de discos a la agrupación.

7. Haga clic en Confirmar.

8. Para las unidades de datos, seleccione el mismo perfil de datos usado en la agrupación existente.

9. Si asignó dispositivos de log o caché, seleccione los perfiles apropiados.

- Para dispositivos de log, haga clic en Log Profile (Perfil de log) y seleccione el perfil reflejado o segmentado. Seleccione el perfil reflejado si asignó un número par de dispositivos de log a la agrupación.



Atención - Si se produce un fallo doble, se pueden perder datos de un log en una configuración segmentada. Se recomienda configurar un perfil de log reflejado para la redundancia agregada. Para obtener más información, consulte [“Perfiles de datos para agrupaciones de almacenamiento” \[167\]](#).

- Para los dispositivos de caché, el perfil siempre es segmentado, tal como se muestra en Cache Profile (Perfil de caché).

10. Haga clic en Confirmar.

Temas relacionados

- [Desconfiguración de una agrupación de almacenamiento \(BUI\) \[152\]](#)
- [Agregación de un dispositivo de caché, log o un metadispositivo a una agrupación de almacenamiento existente \(BUI\) \[145\]](#)

▼ Agregación de un estante de discos a una agrupación de almacenamiento existente (CLI)

Use la siguiente tarea para agregar un estante de discos a una agrupación de almacenamiento existente.

Antes de empezar

- Para obtener recomendaciones sobre la cantidad de unidades que se deben seleccionar por agrupación y otras consideraciones y directrices, consulte [“Conceptos de agrupaciones de almacenamiento” \[164\]](#).
- Debe seleccionar el mismo perfil de datos que el que se está usando en la agrupación existente. Para comprender los distintos perfiles de datos, consulte [“Perfiles de datos para agrupaciones de almacenamiento” \[167\]](#).
- Si el almacenamiento es insuficiente para configurar el sistema para el perfil de datos y sus opciones, tal vez algunos atributos no sean admitidos. Por ejemplo, es imposible conservar las características NSPF al agregar un único estante de discos a una configuración RAID de doble paridad con la opción NSPF. Puede agregar el estante de discos, pero no puede usar la opción NSPF.
- No realice una operación de configuración de agrupación cuando haya una actualización de firmware de disco en curso. Para comprobar si hay alguna actualización en curso, navegue hasta `maintenance system updates`.



Atención - Una vez que un disco se agrega a una agrupación, ya no se puede eliminar sin destruir la agrupación por completo y perder todos los datos.

1. **Para instalar el nuevo estante de discos, use [“Agregación de un nuevo estante de discos” en el *Manual de servicio del cliente de Oracle ZFS Storage Appliance*](#).**
2. **Vaya a `configuration storage`.**
3. **Si tiene varias agrupaciones, se selecciona y se muestra una agrupación por defecto. Si no es la agrupación a la que desea agregar el dispositivo, introduzca `set pool=` y especifique otra agrupación en línea.**

Nota - Si tiene una sola agrupación, el nombre de agrupación no se muestra, pero está seleccionado.

```
hostname:configuration storage (pool0)> set pool=pool1
pool = pool1
```

Aparece un mensaje para recordarle que debe verificar que el dispositivo esté instalado correctamente. Tenga en cuenta que no se recomienda mezclar tipos y velocidades de dispositivo.

4. Introduzca add.

```
hostname:configuration storage (pool1)> add
```

5. Introduzca show para ver la información de dispositivo de la agrupación:

```
hostname:configuration storage (pool1) verify> show
ID STATUS ALLOCATION DATA LOG CACHE RPM
0 ok custom 0 0 0/4 1.86T
1 ok custom 0 0/2 34G 0 15000
2 ok custom 0 0/2 34G 0 15000
```

6. Especifique el estante de discos o el controlador y el número de unidades de datos que desea utilizar.

El ID "0" es el controlador, y los ID restantes son los estantes de discos. En el siguiente ejemplo, se usa 1-data=8 para asignar ocho unidades de datos del primer estante de discos.

```
hostname:configuration storage (pool1) verify> set 1-data=8
1-data = 8
```

7. (Opcional) Especifique el estante de discos o el controlador y el número de dispositivos de log o dispositivos de caché que desea utilizar.

El ID "0" es el controlador, y los ID restantes son los estantes de discos. En el siguiente ejemplo, set 0-cache=1 asigna un dispositivo de caché del controlador:

```
hostname:configuration storage (pool1) verify> set 0-cache=1
0-cache = 1
```

8. Escriba done.

```
hostname:configuration storage (pool1) verify> done
```

Los dispositivos de almacenamiento se verifican para determinar que estén presentes y ofrezcan un mínimo de funcionalidad. Si la verificación falla, corrija el problema y vuelva a iniciar este procedimiento. Si asigna una agrupación con dispositivos defectuosos o faltantes, no podrá agregar los dispositivos defectuosos o faltantes más adelante.

9. Escriba show para visualizar el perfil.

```
hostname:configuration storage (pool1) config> show
PROFILE CAPACITY NSPF DESCRIPTION
log_profile 17G no Striped log
```

10. Introduzca el mismo perfil de datos que el del resto de la agrupación. Para ello, introduzca set profile= y el nombre del perfil.**11. Escriba done.****12. Si asignó dispositivos de log a la agrupación, introduzca set log_profile= y log_mirror O log_stripe. Use log_mirror si la agrupación incluye un número par de dispositivos de log.**

```
hostname:configuration storage (pool1)> set log_profile=log_mirror
```

Nota - Si asignó dispositivos de caché a la agrupación, el perfil siempre está segmentado.

13. Escriba done.

Temas relacionados

- [Desconfiguración de una agrupación de almacenamiento \(CLI\) \[153\]](#)
- [Agregación de un dispositivo de caché, log o un metadispositivo a una agrupación de almacenamiento existente \(CLI\) \[147\]](#)

▼ **Agregación de un dispositivo de caché, log o un metadispositivo a una agrupación de almacenamiento existente (BUI)**

Use la siguiente tarea para agregar un dispositivo de log, un dispositivo de caché de lectura o un metadispositivo a una agrupación de almacenamiento existente.

- Antes de empezar**
- Para obtener recomendaciones sobre la cantidad de unidades que se deben seleccionar por agrupación y otras consideraciones y directrices, consulte [“Conceptos de agrupaciones de almacenamiento” \[164\]](#).
 - Debe seleccionar el mismo perfil de datos que el que se está usando en la agrupación existente. Para comprender los distintos perfiles de datos, consulte [“Perfiles de datos para agrupaciones de almacenamiento” \[167\]](#).
 - No realice una operación de configuración de agrupación cuando haya una actualización de firmware de disco en curso. Para comprobar si hay alguna actualización en curso, navegue hasta Maintenance (Mantenimiento) > System (Sistema).
 - Un metadispositivo debe ser una SSD de 3,2 TB (como mínimo) para admitir la característica de deduplicación de datos mejorada disponible en la versión de software OS8.7.0 o posterior.
1. **Instale el dispositivo de log, el dispositivo de caché de lectura o el metadispositivo nuevo en la primera ranura disponible y apropiada. Para determinar si una ranura es apropiada, consulte [“Disk Shelf Configurations” in Oracle ZFS Storage Appliance Customer Service Manual](#).**
 2. **Vaya a Configuración > Almacenamiento.**

3. **En la lista Agrupaciones disponibles, seleccione una agrupación en línea a la que desee agregar el dispositivo.**
4. **Haga clic en Agregar.**
5. **Seleccione el dispositivo que desea agregar a la agrupación y haga clic en Confirmar.**
6. **Seleccione los perfiles adecuados.**
 - Para dispositivos de log, haga clic en Log Profile (Perfil de log) y seleccione el perfil reflejado o segmentado. Use el perfil reflejado si la agrupación ahora incluye un número par de dispositivos de log.



Atención - Si se produce un fallo doble, se pueden perder datos de un log en una configuración segmentada. Se recomienda configurar un perfil de log reflejado para la redundancia agregada. Para obtener más información, consulte [“Perfiles de datos para agrupaciones de almacenamiento” \[167\]](#).

- Para los dispositivos de caché, el perfil siempre es segmentado, tal como se muestra en Cache Profile (Perfil de caché).
 - Para metadispositivos, haga clic en Metadata Profile (Perfil de metadatos) y seleccione el perfil reflejado o segmentado. Se recomienda el perfil segmentado para lograr un mejor rendimiento en caso de un fallo del metadispositivo.
7. **Haga clic en Confirmar.**

Temas relacionados

- [Eliminación de un dispositivo de caché o un dispositivo de log de una agrupación de almacenamiento existente \(BUI\) \[149\]](#)
- [Agregación de un estante de discos a una agrupación de almacenamiento existente \(BUI\) \[141\]](#)
- [“Perfiles de datos para agrupaciones de almacenamiento” \[167\]](#)
- [“Conceptos de agrupaciones de almacenamiento” \[164\]](#)

▼ Agregación de un dispositivo de caché, log o un metadispositivo a una agrupación de almacenamiento existente (CLI)

Realice la siguiente tarea para agregar un dispositivo de caché de lectura o un dispositivo de log a una agrupación de almacenamiento existente.

- Antes de empezar**
- Para obtener recomendaciones sobre la cantidad de unidades que se deben seleccionar por agrupación y otras consideraciones y directrices, consulte [“Conceptos de agrupaciones de almacenamiento” \[164\]](#).
 - Debe seleccionar el mismo perfil de datos que el que se está usando en la agrupación existente. Para comprender los distintos perfiles de datos, consulte [“Perfiles de datos para agrupaciones de almacenamiento” \[167\]](#).
 - No realice una operación de configuración de agrupación cuando haya una actualización de firmware de disco en curso. Para comprobar si hay alguna actualización en curso, navegue hasta `maintenance system updates`.
 - Un metadispositivo debe ser una SSD de 3,2 TB (como mínimo) para admitir la característica de deduplicación de datos mejorada disponible en la versión de software OS8.7.0 o posterior.
1. **Instale el dispositivo de log, el dispositivo de caché de lectura o el metadispositivo nuevo en la primera ranura disponible y apropiada. Para determinar si una ranura es apropiada, consulte [“Disk Shelf Configurations” in Oracle ZFS Storage Appliance Customer Service Manual](#).**
 2. **Vaya a `configuration storage`.**
 3. **Si tiene varias agrupaciones, se selecciona y se muestra una agrupación por defecto. Si no es la agrupación a la que desea agregar un dispositivo, introduzca `set pool=` y especifique otra agrupación en línea.**

Nota - Si tiene una sola agrupación, el nombre de agrupación no se muestra, pero está seleccionado.

```
hostname:configuration storage (pool0)> set pool=pool1
pool = pool1
```

Aparece un mensaje para recordarle que verifique que el almacenamiento esté bien conectado y en funcionamiento.

4. Introduzca `add`:

```
hostname:configuration storage (pool1)> add
```

5. Introduzca **show** para mostrar la información de dispositivo de la agrupación.

```
hostname:configuration storage (pool1) verify> show
ID STATUS ALLOCATION DATA LOG CACHE META RPM
0 ok custom 0 0 0/4 0/4 1.86T
1 ok custom 0 0/2 34G 0 0 15000
2 ok custom 0 0/2 34G 0/2 0 15000
```

6. Introduzca **set** y utilice la finalización con tabulación para ver si hay dispositivos de caché, log o metadispositivos disponibles.

```
hostname:configuration storage (pool1) verify> set
0-cache 1-data 2-cache 2-meta 2-log
```

7. Introduzca **set** y el ID de controlador o de estante de discos, así como el número de dispositivos de log, de caché o metadispositivos que desea usar.

El ID "0" es el controlador, y los ID restantes son los estantes de discos. En el siguiente ejemplo, se usa 2-log=1 para asignar un dispositivo de log del segundo estante de discos.

```
hostname:configuration storage (pool1) verify> set 2-log=1
2-log = 1
```

Nota - El valor "1-log=2" asignaría dos dispositivos de log del primer estante de discos.

En este ejemplo, se asigna un dispositivo de caché del segundo estante de discos.

```
hostname:configuration storage (pool1) verify> set 2-cache=1
2-cache = 1
```

En este ejemplo, se asigna un metadispositivo del segundo estante de discos:

```
hostname:configuration storage (pool1) verify> set 2-meta=1
2-meta = 1
```

8. Escriba **done**.

```
hostname:configuration storage (pool1) verify> done
```

9. Escriba **show** para visualizar el perfil.

```
hostname:configuration storage (pool1) config> show
PROFILE CAPCTY NSPF DESCRIPTION
log_profile = log_stripe 17G no Striped log
```

Nota - Si asignó dispositivos de caché a la agrupación, el perfil siempre está segmentado.

10. Si asignó dispositivos de log a la agrupación, introduzca **set log_profile=** y configure el perfil de log como **log_mirror** o **log_stripe**. Use **log_mirror** si la agrupación ahora incluye un número par de dispositivos de log.



Atención - Si se produce un fallo doble, se pueden perder datos de un log en una configuración segmentada. Se recomienda configurar un perfil de log reflejado para la redundancia agregada. Para obtener más información, consulte [“Perfiles de datos para agrupaciones de almacenamiento” \[167\]](#).

```
hostname:configuration storage (pool1)> set log_profile=log_mirror
```

11. **Si asignó metadispositivos a la agrupación, introduzca `set meta_profile=` y configure el metaperfil como `meta_mirror` o `meta_stripe`.**

```
hostname:configuration storage (pool1)> set meta_profile=meta_mirror
```

12. **Escriba `done` para completar la tarea.**

```
hostname:configuration storage (pool1)> done
```

Temas relacionados

- [Eliminación de un dispositivo de caché o un dispositivo de log de una agrupación de almacenamiento existente \(CLI\) \[150\]](#)
- [Agregación de un estante de discos a una agrupación de almacenamiento existente \(CLI\) \[143\]](#)
- [“Perfiles de datos para agrupaciones de almacenamiento” \[167\]](#)
- [“Conceptos de agrupaciones de almacenamiento” \[164\]](#)

▼ Eliminación de un dispositivo de caché o un dispositivo de log de una agrupación de almacenamiento existente (BUI)

Realice la siguiente tarea para eliminar un dispositivo de log o un dispositivo de caché de lectura de una agrupación de almacenamiento existente. Esta capacidad es útil al prepararse para una actualización de sistema que requiera la eliminación de algunos dispositivos de caché.

Nota - Los metadispositivos no se pueden eliminar de una agrupación de almacenamiento.

Si una agrupación tiene dispositivos de caché en ambos controladores de una configuración en cluster, debe realizar este procedimiento en cada controlador.

Para agregar un dispositivo a otra agrupación de almacenamiento existente, consulte [Agregación de un dispositivo de caché, log o un metadispositivo a una agrupación de almacenamiento existente \(BUI\) \[145\]](#).

Antes de empezar No realice una operación de configuración de agrupación cuando haya una actualización de firmware de disco en curso. Para comprobar si hay alguna actualización en curso, navegue hasta Maintenance (Mantenimiento) > System (Sistema).

1. **Vaya a Configuración > Almacenamiento.**
2. **En la lista Agrupaciones disponibles, seleccione una agrupación en línea de la que desee eliminar el dispositivo.**
3. **Haga clic en ELIMINAR.**
4. **Seleccione el número de dispositivos de log y dispositivos de caché que desea eliminar de la agrupación de almacenamiento.**

Nota - Si los dispositivos de log usan un perfil reflejado, aparece un mensaje para recordarle que seleccione un número par de dispositivos de log para eliminar. Si usan un perfil segmentado, puede eliminar un número par o impar de dispositivos.

5. **Haga clic en Confirmar.**

Temas relacionados

- [Agregación de un dispositivo de caché, log o un metadispositivo a una agrupación de almacenamiento existente \(BUI\) \[145\]](#)

▼ Eliminación de un dispositivo de caché o un dispositivo de log de una agrupación de almacenamiento existente (CLI)

Realice la siguiente tarea para eliminar un dispositivo de log o un dispositivo de caché de lectura de una agrupación de almacenamiento existente. Esta capacidad es útil al prepararse para una actualización de sistema que requiera la eliminación de algunos dispositivos de caché.

Nota - Los metadispositivos no se pueden eliminar de una agrupación de almacenamiento.

Si una agrupación tiene dispositivos de caché en ambos controladores de una configuración en cluster, debe realizar este procedimiento en cada controlador.

Para agregar un dispositivo a otra agrupación de almacenamiento existente, consulte [Agregación de un dispositivo de caché, log o un metadispositivo a una agrupación de almacenamiento existente \(CLI\) \[147\]](#).

Antes de empezar No realice una operación de configuración de agrupación cuando haya una actualización de firmware de disco en curso. Para comprobar si hay alguna actualización en curso, navegue hasta `maintenance system updates`.

1. **Vaya a configuration storage.**
2. **Si tiene varias agrupaciones, se selecciona y se muestra una agrupación por defecto. Si no es la agrupación a la que desea agregar el dispositivo, introduzca `set pool=` y especifique otra agrupación en línea.**

Nota - Si tiene una sola agrupación, el nombre de agrupación no se muestra, pero está seleccionado.

```
hostname:configuration storage (pool0)> set pool=pool1
pool = pool1
```

3. **Introduzca `show` para ver la información de dispositivo de la agrupación.**

```
hostname:configuration storage (pool1) verify> show
ID STATUS ALLOCATION DATA LOG CACHE META RPM
0 ok custom 0 0 0/4 0/4 1.86T
1 ok custom 0 0/2 34G 0 0 15000
2 ok custom 0 0/2 34G 0/2 0 15000
```

4. **Introduzca `remove`.**

```
hostname:configuration storage (pool1)> remove
```

5. **Especifique el controlador o el estante de discos y el número de dispositivos de log o de caché que desea eliminar.**

El ID "0" es el controlador, y los ID restantes son los estantes de discos. En el siguiente ejemplo, se usa `1-log=2` para eliminar dos dispositivos de log del primer estante de discos:

```
hostname:configuration storage (pool1) remove> set 1-log=2
1-log = 2
```

En este ejemplo, se elimina un dispositivo de caché del controlador:

```
hostname:configuration storage (pool1) remove> set 0-cache=1
0-cache = 1
```

6. **Escriba `done`.**

```
hostname:configuration storage (pool1) remove> done
```

Nota - Si los dispositivos de log usan un perfil reflejado, aparece un mensaje para recordarle que seleccione un número par de dispositivos de log para eliminar. Si los dispositivos de log usan un perfil segmentado, puede eliminar un número par o impar de dispositivos.

Temas relacionados

- [Agregación de un dispositivo de caché, log o un metadispositivo a una agrupación de almacenamiento existente \(CLI\) \[147\]](#)

▼ Desconfiguración de una agrupación de almacenamiento (BUI)

Al desconfigurar una agrupación de almacenamiento, se eliminan los sistemas de archivos y los LUN activos, y el almacenamiento raw queda disponible para una configuración de almacenamiento futura. Este proceso se puede deshacer importando la agrupación de almacenamiento desconfigurada, siempre y cuando no se haya utilizado el almacenamiento raw como parte de una agrupación de almacenamiento activa.



Atención - La desconfiguración de una agrupación imposibilita el acceso a los datos, crea una posible pérdida de datos y falla al realizar replicaciones entrantes.

Antes de empezar

- No anule la configuración de una agrupación cuando haya un cambio de versión de firmware de disco en curso. Para comprobar si hay alguna actualización en curso, navegue hasta Maintenance (Mantenimiento) > System (Sistema).
- No desconfigure una agrupación mientras el controlador par no está en funcionamiento o está inaccesible.
- Si un mensaje de error informa que el destino está en uso, espere y vuelva a intentar la operación.

1. **Vaya a Configuración > Almacenamiento.**
2. **Desde la lista Agrupaciones disponibles, seleccione una agrupación en línea para desconfigurar.**
3. **Haga clic en DESCONFIGURAR.**

Temas relacionados

- [Importación de una agrupación de almacenamiento existente \(BUI\) \[134\]](#)
- [Cambio de nombre de una agrupación de almacenamiento \(BUI\) \[154\]](#)

▼ Desconfiguración de una agrupación de almacenamiento (CLI)

Al desconfigurar una agrupación de almacenamiento, se eliminan los sistemas de archivos y los LUN activos, y el almacenamiento raw queda disponible para una configuración de almacenamiento futura. Este proceso se puede deshacer importando la agrupación de almacenamiento desconfigurada, siempre y cuando no se haya utilizado el almacenamiento raw como parte de una agrupación de almacenamiento activa.



Atención - La desconfiguración de una agrupación imposibilita el acceso a los datos, crea una posible pérdida de datos y falla al realizar replicaciones entrantes.

Antes de empezar

- No realice una operación de configuración de agrupación cuando haya una actualización de firmware de disco en curso. Para comprobar si hay alguna actualización en curso, navegue hasta `maintenance system updates`.
- No desconfigure una agrupación mientras el controlador par no está en funcionamiento o está inaccesible.
- Si un mensaje de error informa que el destino está en uso, espere y vuelva a intentar la operación.

1. **Vaya a configuration storage.**
2. **Si tiene varias agrupaciones, se selecciona y se muestra una agrupación por defecto. Si no es la agrupación que desea desconfigurar, introduzca `set pool=` y especifique otra agrupación en línea.**

Nota - Si tiene una sola agrupación, el nombre de agrupación no se muestra, pero está seleccionado.

```
hostname:configuration storage (pool0)> set pool=pool1
pool = pool1
```

3. **Introduzca `unconfig`.**
4. **Escriba `done`.**

```
hostname:configuration storage (pool1)> unconfig
```

Temas relacionados

- [Importación de una agrupación de almacenamiento existente \(CLI\) \[135\]](#)
- [Cambio de nombre de una agrupación de almacenamiento \(CLI\) \[155\]](#)

▼ Cambio de nombre de una agrupación de almacenamiento (BUI)

Para cambiar el nombre de una agrupación de almacenamiento, desconfigúrela e, inmediatamente después, impórtela con otro nombre. Mientras se desconfigura el almacenamiento, no se podrá acceder a los datos y existirá una posible pérdida de datos. La importación de una agrupación de almacenamiento puede tardar un tiempo considerable.

- Antes de empezar**
- No realice una operación de configuración de agrupación cuando haya una actualización de firmware de disco en curso. Para comprobar si hay alguna actualización en curso, navegue hasta **Mantenimiento > Sistema**.
 - No cambie el nombre de una agrupación mientras el controlador par no está en funcionamiento o está inaccesible.

1. **Vaya a Configuración > Almacenamiento.**
2. **Desde la lista Agrupaciones disponibles, seleccione la agrupación en línea cuyo nombre desea cambiar.**
3. **Haga clic en UNCONFIG (Desconfigurar) y, luego, en COMMIT (Confirmar).**
4. **Haga clic en IMPORT (Importar) y, luego, seleccione la agrupación de almacenamiento que acaba de desconfigurar.**
5. **Haga clic en el nombre de la agrupación de almacenamiento y cámbielo.**
El nombre debe tener entre 1 y 64 caracteres de longitud. El nombre no puede comenzar con un punto (.) ni puede incluir espacios. Los caracteres permitidos son los alfanuméricos y los siguientes caracteres especiales:

_ - . :

6. **Haga clic en Confirmar.**

Temas relacionados

- [Desconfiguración de una agrupación de almacenamiento \(BUI\) \[152\]](#)
- [Importación de una agrupación de almacenamiento existente \(BUI\) \[134\]](#)

▼ Cambio de nombre de una agrupación de almacenamiento (CLI)

Para cambiar el nombre de una agrupación de almacenamiento, desconfigúrela e, inmediatamente después, impórtela con otro nombre. Mientras se desconfigura el almacenamiento, no se podrá acceder a los datos y existirá una posible pérdida de datos. La importación de una agrupación de almacenamiento puede tardar un tiempo considerable.

- Antes de empezar**
- No realice una operación de configuración de agrupación cuando haya una actualización de firmware de disco en curso. Para comprobar si hay alguna actualización en curso, navegue hasta `maintenance system updates`.
 - No cambie el nombre de una agrupación mientras el controlador par no está en funcionamiento o está inaccesible.

1. Vaya a `configuration storage`.

2. Seleccione la agrupación a la que desea cambiarle el nombre.

Si tiene varias agrupaciones, se selecciona y se muestra una agrupación por defecto. Si no es la agrupación cuyo nombre desea cambiar, introduzca `set pool=` y especifique otra agrupación en línea.

Nota - Si tiene una sola agrupación, el nombre de agrupación no se muestra, pero está seleccionado.

```
hostname:configuration storage (pool0)> set pool=pool1
pool = pool1
```

3. Introduzca `unconfig`.

```
hostname:configuration storage (pool1)> unconfig
```

4. Escriba `done`.

5. Introduzca `import`.

```
hostname:configuration storage> import
```

Search for storage. Begin the process of searching for existing storage pools.

Subcommands that are valid in this context:

```
help [topic]          => Get context-sensitive help. If [topic] is specified,
                        it must be one of "builtins", "commands", "general",
                        "help" or "script".

show                  => Show information pertinent to the current context
```

```
abort                => Abort this task (potentially resulting in a
                        misconfigured system)

done                 => Finish operating on "discover"

hostname:configuration storage discover>
```

6. Escriba done.

7. Para seleccionar la agrupación de almacenamiento que acaba de desconfigurar, introduzca `set pool=` y el nombre de la agrupación.

```
hostname:configuration storage select> set pool=pool1
pool = pool1
```

8. Para cambiar el nombre de la agrupación de almacenamiento, introduzca `set name=` y un nombre nuevo.

El nombre debe tener entre 1 y 64 caracteres de longitud. El nombre no puede comenzar con un punto (.) ni puede incluir espacios. Los caracteres permitidos son los alfanuméricos y los siguientes caracteres especiales:

```
_ - . :

hostname:configuration storage (pool1)> set name=NewPool
pool = NewPool
```

9. Escriba done.

Temas relacionados

- [Desconfiguración de una agrupación de almacenamiento \(CLI\) \[153\]](#)
- [Importación de una agrupación de almacenamiento existente \(CLI\) \[135\]](#)

▼ Limpieza manual de una agrupación de almacenamiento (BUI)

El proceso de limpieza de una agrupación de almacenamiento busca errores para verificar el contenido.

La limpieza programada de una agrupación de almacenamiento está activada de forma predeterminada, como se describe en [Limpieza programada de una agrupación de almacenamiento \(BUI\) \[159\]](#).

La operación de limpieza no continuará si ya hay una limpieza o reconstrucción en curso. Si hay una operación de limpieza en curso cuando comienza la reconstrucción, la operación de reconstrucción suspende la limpieza en curso y la reinicia una vez concluida la reconstrucción.

Se recomienda realizar la limpieza de manera trimestral como mínimo.

- Se debe realizar una limpieza como mínimo con la misma frecuencia con la que caducan las copias de seguridad antiguas.
- También se debe realizar una limpieza antes de realizar una actualización de software.

1. **Vaya a Configuración > Almacenamiento.**
2. **Desde la lista Agrupaciones disponibles, seleccione la agrupación en línea que desea limpiar.**
3. **(Opcional) Compruebe el estado de la última limpieza.**

El campo Estado de limpieza muestra cuándo se realizó la última limpieza en la hora local (o durante cuánto tiempo se ejecutó la limpieza en el caso de que no haya finalizado) y la cantidad de errores que informó.

El comando `zpool status` también informa la hora de finalización de la última limpieza, durante cuánto tiempo se ejecutó y si se encontraron errores y fueron corregidos.
4. **Haga clic en LIMPIAR.**

El campo Estado de limpieza se actualiza.
5. **(Opcional) Para detener la limpieza, haga clic en CANCELAR.**

Haga clic en LIMPIAR nuevamente para reiniciar la limpieza.

Temas relacionados

- [“Conceptos de agrupaciones de almacenamiento” \[164\]](#)
- [Limpieza programada de una agrupación de almacenamiento \(BUI\) \[159\]](#)

▼ Limpieza manual de una agrupación de almacenamiento (CLI)

El proceso de limpieza de una agrupación de almacenamiento busca errores para verificar el contenido.

La limpieza programada de una agrupación de almacenamiento está activada de forma predeterminada, como se describe en [Limpieza programada de una agrupación de almacenamiento \(CLI\) \[160\]](#).

La operación de limpieza no continuará si ya hay una limpieza o reconstrucción en curso. Si hay una operación de limpieza en curso cuando comienza la reconstrucción, la operación de reconstrucción suspende la limpieza en curso y la reinicia una vez concluida la reconstrucción.

Se recomienda realizar la limpieza de manera trimestral como mínimo.

- Se debe realizar una limpieza como mínimo con la misma frecuencia con la que caducan las copias de seguridad antiguas.
- También se debe realizar una limpieza antes de realizar una actualización de software.

1. Vaya a configuration storage.

2. Seleccione la agrupación en línea que desea limpiar.

Si tiene una sola agrupación, el nombre de agrupación no se muestra, pero está seleccionado.

Si tiene varias agrupaciones, se selecciona y se muestra una de las agrupaciones. Use el comando `set pool` para seleccionar otra agrupación.

```
hostname:configuration storage (pool0)> set pool=pool1
pool = pool1
```

3. (Opcional) Compruebe el estado de la última limpieza.

Use el comando `ls`, `show` o `get` para ver cuándo finalizó la última limpieza en GMT (o durante cuánto tiempo se ejecutó en el caso de que no haya finalizado) y la cantidad de errores que informó:

```
hostname:configuration storage (pool1)> get scrub
scrub = scrub completed after 2d20h with 0 errors on Mon May 6 10:35:16 2019
```

El comando `zpool status` también informa la hora de finalización de la última limpieza, durante cuánto tiempo se ejecutó y si se encontraron errores y fueron corregidos.

4. Introduzca `scrub start`.

```
hostname:configuration storage (pool1)> scrub start
```

5. (Opcional) Detenga el proceso de limpieza antes de que finalice. Para ello, introduzca `scrub stop`.

```
hostname:configuration storage (pool1)> scrub stop
```

Si introduce `scrub start` nuevamente, se reiniciará la limpieza.

Temas relacionados

- [“Conceptos de agrupaciones de almacenamiento” \[164\]](#)
- [Limpieza programada de una agrupación de almacenamiento \(CLI\) \[160\]](#)

▼ Limpieza programada de una agrupación de almacenamiento (BUI)

El proceso de limpieza de una agrupación de almacenamiento busca errores para verificar el contenido. De forma predeterminada, la limpieza programada de una agrupación de almacenamiento está activada y configurada para que se realice cada 30 días. Use el control Programación de limpieza para especificar otro intervalo de limpieza o desactivar la programación de limpieza.

No puede cambiar la prioridad de limpieza explícitamente. La prioridad de limpieza se ajusta automáticamente según el intervalo de limpieza especificado, el progreso de la limpieza y la carga del sistema. La prioridad de limpieza aumenta automáticamente en un sistema inactivo.

La operación de limpieza no continuará si ya hay una limpieza o reconstrucción en curso. Si hay una operación de limpieza en curso cuando comienza la reconstrucción, la operación de reconstrucción suspende la limpieza en curso y la reinicia una vez concluida la reconstrucción.

1. **Vaya a Configuración > Almacenamiento.**
2. **Desde la lista Agrupaciones disponibles, seleccione la agrupación en línea para la que desea configurar la limpieza programada.**
3. **(Opcional) Compruebe el estado de la última limpieza.**

El campo Estado de limpieza muestra cuándo se realizó la última limpieza en la hora local (o durante cuánto tiempo se ejecutó la limpieza en el caso de que no haya finalizado) y la cantidad de errores que informó.

El comando `zpool status` también informa la hora de finalización de la última limpieza, durante cuánto tiempo se ejecutó y si se encontraron errores y fueron corregidos.

4. **Seleccione Programación de limpieza.**

Las opciones del menú desplegable de Programación de limpieza son las siguientes:

- Desactivada
- 15 días
- 30 días
- 45 días
- 60 días
- 75 días
- 90 días

Por defecto, la limpieza está programada cada 30 días. Puede seleccionar otro intervalo de limpieza o seleccionar la opción Desactivada para desactivar la limpieza programada.

5. Haga clic en el botón PROGRAMAR.

Temas relacionados

- [“Conceptos de agrupaciones de almacenamiento” \[164\]](#)
- [Limpieza manual de una agrupación de almacenamiento \(BUI\) \[156\]](#)

▼ Limpieza programada de una agrupación de almacenamiento (CLI)

El proceso de limpieza de una agrupación de almacenamiento busca errores para verificar el contenido. De forma predeterminada, la limpieza programada de una agrupación de almacenamiento está activada y configurada para que se realice cada 30 días. Use la propiedad `scrub_schedule` para especificar otro intervalo de limpieza o desactivar la programación de limpieza.

No puede cambiar la prioridad de limpieza explícitamente. La prioridad de limpieza se ajusta automáticamente según el intervalo de limpieza especificado, el progreso de la limpieza y la carga del sistema. La prioridad de limpieza aumenta automáticamente en un sistema inactivo.

La operación de limpieza no continuará si ya hay una limpieza o reconstrucción en curso. Si hay una operación de limpieza en curso cuando comienza la reconstrucción, la operación de reconstrucción suspende la limpieza en curso y la reinicia una vez concluida la reconstrucción.

1. Vaya a configuration storage.

2. Seleccione la agrupación en línea que desea limpiar.

Si tiene una sola agrupación, el nombre de agrupación no se muestra, pero está seleccionado.

Si tiene varias agrupaciones, se selecciona y se muestra una de las agrupaciones. Use el comando `set pool` para seleccionar otra agrupación.

```
hostname:configuration storage (pool0)> set pool=pool1
pool = pool1
```

3. (Opcional) Compruebe el estado de la última limpieza.

Use el comando `ls`, `show` o `get` para ver cuándo finalizó la última limpieza en GMT (o durante cuánto tiempo se ejecutó en el caso de que no haya finalizado) y la cantidad de errores que informó:

```
hostname:configuration storage (pool1)> get scrub scrub_schedule
scrub = scrub completed after 2d20h with 0 errors on Mon May 6 10:35:16 2019
scrub_schedule = 30 days
```

El comando `zpool status` también informa la hora de finalización de la última limpieza, durante cuánto tiempo se ejecutó y si se encontraron errores y fueron corregidos.

4. Defina el valor de la propiedad `scrub_schedule`.

Defina el valor de la propiedad `scrub_schedule` en `off` para desactivar la programación de limpieza, por ejemplo, si prefiere realizar una limpieza manual.

Para activar la limpieza programada de una agrupación de almacenamiento, defina el valor de la propiedad `scrub_schedule` en la cantidad de días comprendidos entre las limpiezas programadas. Puede definir el valor `scrub_schedule` en 15, 30, 45, 60, 75 o 90 días.

```
hostname:configuration storage (p0)> set scrub_schedule=60
scrub_schedule = 60
hostname:configuration storage (p0)> get scrub_schedule
scrub_schedule = 60 days
```

Temas relacionados

- [“Conceptos de agrupaciones de almacenamiento” \[164\]](#)
- [Limpieza manual de una agrupación de almacenamiento \(CLI\) \[157\]](#)

▼ Visualización del estado de la agrupación y el dispositivo (BUI)

Puede comprobar el estado de una agrupación y los dispositivos. Si existe un problema con una agrupación, también se mostrarán los detalles sobre el estado del dispositivo.

1. **Navegue hasta Configuration (Configuración) > Storage (Almacenamiento).**
2. **Haga clic en una agrupación para seleccionarla y ver más detalles.**
Consulte la siguiente tabla para obtener una descripción del estado de la agrupación.

Estado de agrupación	Descripción
En línea	Una agrupación cuyos dispositivos funcionan con normalidad.
Degradado	Una agrupación con uno o varios dispositivos fallidos, pero cuyos datos permanecen disponibles debido a una configuración redundante.
Con fallos	Uno o más dispositivos están fuera de línea y no hay replicas suficientes para continuar con el funcionamiento.

Estado de agrupación	Descripción
Fuera de línea	Una agrupación se puso fuera de línea de manera explícita.
No disponible	Una agrupación con metadatos dañados o uno o más dispositivos no disponibles y replicas insuficientes para continuar con el funcionamiento.
Exportado	Una agrupación está activa en el par de cluster y preparada para un failback de cluster.

3. Visualice las propiedades de cifrado de la agrupación.

Si la versión de software del dispositivo es OS8.8.0 o posterior y está aplicada la actualización diferida Activación de cifrado de agrupación (consulte [“Activación de actualización diferida de cifrado de agrupación” en el Manual de servicio del cliente de Oracle ZFS Storage Appliance](#)), se muestra una columna CIFRADA.

Si la agrupación no está cifrada, la columna CIFRADA está en blanco.

Si la agrupación está cifrada, se muestra un ícono de candado  en la columna CIFRADA y, si pasa el cursor sobre ese ícono, aparece el tipo de cifrado.

Si la agrupación seleccionada está cifrada, se muestra la información sobre el tipo de cifrado, el almacén de claves y el nombre de clave. Consulte [“Propiedades de cifrado” \[832\]](#).

- Si el valor del campo Estado de la clave es "no disponible", significa que la clave se ha suprimido. Además, aparece un indicador  a la derecha del ícono de candado  que muestra que se suprime la clave para esta agrupación.
- Si el campo Última actualización de la clave está en blanco, el valor de clave no se ha modificado desde que se creó la agrupación.

4. Vea los estados del dispositivo de la agrupación seleccionada en la sección Device Status (Estado de dispositivo).

Consulte la siguiente tabla para obtener una descripción de los estados del dispositivo.

Estado de dispositivo	Descripción
En línea	El dispositivo está en línea y funcionando. Es posible que no pueda visualizar este estado y que, en su lugar, vea el mensaje "No device faults have been detected in the storage pool" (No se detectaron fallos del dispositivo en la agrupación de almacenamiento).
Degradado	El dispositivo no se encuentra en un estado óptimo. Se espera que falle pronto o aún no se terminó de reconstruir uno de reserva.
Con fallos	El dispositivo está defectuoso; se puede obtener más información en los log de mantenimiento.
Fuera de línea	El dispositivo se puso fuera de línea de manera explícita; no se producirán lecturas o escrituras en este dispositivo hasta que se ponga en línea.
Eliminado	El dispositivo se eliminó de manera física.

Estado de dispositivo	Descripción
Disco de reserva	Un dispositivo de reserva se usa activamente como un disco de datos en la agrupación como reemplazo de un dispositivo que falló.
No disponible	No se pudo abrir el dispositivo o la agrupación no pudo detectar este dispositivo.

5. **Para ver información detallada de errores de la agrupación y el dispositivo, navegue hasta Maintenance (Mantenimiento) > Problems (Problemas) para errores activos o hasta Maintenance (Mantenimiento) > Logs para obtener un historial de todos los problemas.**

▼ Visualización del estado de la agrupación y del dispositivo (CLI)

1. **Vaya a `configuration storage`.**

Se selecciona y se muestra la agrupación por defecto.

2. **(Opcional) Si tiene varias agrupaciones, seleccione otra para ver.**

Si la agrupación por defecto no es la agrupación que desea ver, introduzca `set pool=` y especifique otra agrupación en línea.

```
hostname:configuration storage (pool0)> set pool=pool1
pool = pool1
```

3. **Introduzca `show`.**

Consulte la tabla en el paso 2 de [Visualización del estado de la agrupación y el dispositivo \(BUI\) \[161\]](#) para ver una descripción del valor del estado de la agrupación.

Consulte la tabla en el paso 4 de [Visualización del estado de la agrupación y el dispositivo \(BUI\) \[161\]](#) para ver una descripción del valor del estado del dispositivo.

4. **Visualice las propiedades de cifrado de la agrupación.**

Si la versión de software del dispositivo es OS8.8.0 o posterior y está aplicada la actualización diferida Activación de cifrado de agrupación (consulte [“Activación de actualización diferida de cifrado de agrupación” en el Manual de servicio del cliente de Oracle ZFS Storage Appliance](#)), se muestra una columna CIFRADA.

Si la agrupación no está cifrada, el valor de la columna CIFRADA es un guion (-) y el valor de la propiedad `encryption` es `off`.

Si la agrupación está cifrada, la columna CIFRADA muestra el tipo de cifrado. Consulte [“Propiedades de cifrado” \[832\]](#).

Si la agrupación seleccionada está cifrada, la propiedad `encryption` muestra el tipo de cifrado. Además, se muestran las cuatro propiedades siguientes:

- `keystatus`. Puede ser `available` o `unavailable`. Si el valor de la propiedad `keystatus` es `unavailable`, la clave se ha suprimido.
- `keychangedate`. La fecha en que se modificó la clave por última vez. Si el valor de la propiedad `keychangedate` está en blanco, el valor de la clave no se ha modificado desde que se creó la agrupación.
- `keyname`. El nombre de la clave.
- `keystore`. El nombre del almacén de claves.

```
hostname:configuration storage (pool1)> ls
Pools:
  POOL          OWNER   DATA PROFILE LOG PROFILE STATUS  ERRS  ENCRYPTED
->pool1         hostname mirror   -          -       online  0     aes-128-ccm
  pool2         hostname mirror   -          -       online  0     -
  pool3         hostname stripe  -          -       online  0     -

Properties:
      pool = pool1
      status = online
      errors = 0
      profile = mirror
      log_profile = -
      cache_profile = -
      meta_profile = -
      scrub = none requested
      encryption = aes-128-ccm
      keystatus = available
      keychangedate =
      keyname = MyKey
      keystore = LOCAL
```

Si la agrupación no está cifrada, los cuatro valores `key` no se muestran, pero siguen estando disponibles mediante el uso de los comandos `get` o `script`.

5. **Para ver más información detallada de errores de la agrupación y del dispositivo, vaya a `maintenance problems` para errores activos o a `maintenance logs` para obtener un historial de todos los problemas.**

Conceptos de agrupaciones de almacenamiento

El almacenamiento se configura en agrupaciones que se caracterizan por su redundancia de datos subyacente y proporciona espacio compartido entre todos los sistemas de archivos y LUN. En la sección [“Acerca de las agrupaciones de almacenamiento, los proyectos y los recursos compartidos” \[500\]](#), puede encontrar más información sobre la manera en la que las agrupaciones de almacenamiento se relacionan con los sistemas de archivos o los LUN individuales.

Configuración de agrupación de almacenamiento

Para crear una agrupación, se puede configurar una agrupación nueva o se puede importar una existente. La importación de una agrupación existente se utiliza solamente para importar agrupaciones configuradas anteriormente en un dispositivo Oracle ZFS Storage Appliance. La importación de una agrupación existente es útil en casos de reconfiguración accidental, como la transferencia de agrupaciones entre controladores o fallos catastróficos del controlador.

Varias agrupaciones

Cada controlador puede tener la cantidad de agrupaciones que se desee, y se puede asignar el propietario de cada agrupación del cluster de manera independiente. Con la capacidad de controlar el acceso a los dispositivos de caché y log por recurso compartido, el modo recomendado de funcionamiento es con una única agrupación. Si bien se admite una cantidad arbitraria de agrupaciones, no se recomienda la creación de varias agrupaciones con las mismas características de redundancia cuyo propietario sea el mismo nodo principal de cluster. De hacerlo, el rendimiento sería malo, la asignación de recursos no sería la óptima, la partición del almacenamiento sería artificial y aumentaría la complejidad administrativa. La configuración de varias agrupaciones en el mismo host se recomienda solamente cuando se desea contar con características de rendimiento o redundancia drásticamente diferentes; por ejemplo, una agrupación reflejada para bases de datos y una agrupación RAID-Z para cargas de trabajo de transmisión.

Número de dispositivos por agrupación

Las unidades dentro de todo el chasis se pueden asignar de manera individual, pero se debe tener cuidado al asignar discos de los estantes de discos para asegurarse de que las configuraciones de las agrupaciones sean óptimas. Por lo general, se prefiere una menor cantidad de agrupaciones con más discos por agrupación, ya que simplifican la gestión y proporcionan un mayor porcentaje de capacidad utilizable total.

Si bien el sistema puede asignar almacenamiento con el incremento que se desee, se recomienda que cada asignación incluya un mínimo de 8 discos en todos los estantes de discos e, idealmente, muchos más.

Características y rendimiento de la unidad

Siga estas restricciones al configurar las agrupaciones de almacenamiento:

- Todos los discos de datos que se encuentran dentro de un nodo principal o de un estante de discos deben tener la misma velocidad de rotación (velocidad de rotación del medio).

El software del dispositivo detecta configuraciones erróneas y genera un fallo para la condición.

- Debido a problemas de rendimiento impredecibles, evite combinar diferentes velocidades de rotación de disco en una misma agrupación.
- Para obtener un rendimiento óptimo, no combine estantes de discos de diferentes velocidades de rotación de disco en el mismo tejido SAS (conexión HBA). Este tipo de combinaciones funciona correctamente, pero es probable que reduzca el rendimiento de los dispositivos más rápidos.
- Al crear una agrupación nueva, evite mezclar diferentes capacidades de disco porque todos los discos quedan limitados al disco de menor capacidad de la agrupación. Al agregar un disco de mayor capacidad a una agrupación existente, se mantiene la capacidad mayor del disco. Sin embargo, el sistema escribe preferentemente en discos nuevos hasta que comienzan a alcanzar la misma capacidad de utilización que los discos antiguos. Para mantener el rendimiento, agregue muchos discos de mayor capacidad que el número de discos total en la agrupación original.
- Un metadispositivo debe ser una SSD de 3,2 TB (como mínimo) para admitir la característica de deduplicación de datos mejorada disponible en la versión de software OS8.7.0 o posterior.

Capacidad de agrupación de almacenamiento

Al asignar almacenamiento sin formato a las agrupaciones, tenga en cuenta que si las agrupaciones se llenan por completo, se reducirá marcadamente el rendimiento, especialmente en las operaciones de escritura en recursos compartidos o LUN. Estos efectos se vuelven más notables a medida que la agrupación alcanza la capacidad total.

Configuración de almacenamiento solo con unidades flash

Oracle Storage Drive Enclosure DE3-24P se puede configurar como almacenamiento solo con unidades flash con dispositivos de datos SSD basados en flash totalmente completos y dispositivos de log opcionales. Un almacenamiento solo con unidades flash proporciona operaciones de E/S de baja latencia, lo que aumenta el rendimiento de la carga de trabajo.

Una agrupación de almacenamiento que solo incluye unidades flash contiene SSD de datos y dispositivos de log opcionales. Los dispositivos de caché flash de lectura y los metadispositivos no pueden ser parte de una agrupación que solo incluye unidades flash. La vida útil restante de las SSD se puede supervisar mediante el uso de alertas de umbral.

Reclamación de espacio de agrupación de almacenamiento

Al suprimir un proyecto, sistema de archivos o LUN, puede ver la cantidad de espacio que se reclamará en la agrupación de almacenamiento si se aceptó la actualización diferida de supresión asíncrona de juego de datos (OS8.7.0). En la BUI, se muestra el campo Asynchronous Dataset Destroy (Destrucción asíncrona de juego de datos) durante estas operaciones de supresión. De manera similar, en la CLI, la propiedad `async_destroy_reclaim_space` refleja la cantidad de espacio que se reclamará y muestra 0 (cero) cuando finaliza la operación. Los procedimientos individuales para suprimir un proyecto, sistema de archivos o LUN incluyen un paso para supervisar el espacio reclamado en una agrupación de almacenamiento.

Temas relacionados

- Configuración de una agrupación de almacenamiento solo con unidades flash [BUI](#), [CLI](#)
- “Configuraciones de estantes de discos” en el *Manual de servicio del cliente de Oracle ZFS Storage Appliance*
- “Resistencia de SSD” en el *Manual de servicio del cliente de Oracle ZFS Storage Appliance*

Perfiles de datos para agrupaciones de almacenamiento

Después de haber verificado físicamente los dispositivos de almacenamiento y haber asignado los recursos para una agrupación de almacenamiento, el siguiente paso es elegir un perfil de almacenamiento que refleje los objetivos de confiabilidad, disponibilidad, facilidad de mantenimiento (RAS) y rendimiento deseados. El conjunto de perfiles posibles presentado depende del almacenamiento disponible. En la siguiente tabla, se muestran todos los perfiles posibles y sus descripciones.

TABLA 21 Perfiles de datos

Perfil de datos	Descripción
Opciones de paridad doble	
Reflejo triple	Los datos se reflejan por triplicado, lo que genera un sistema muy confiable y de muy alto rendimiento (por ejemplo, almacenamiento para una base de datos crítica). Esta configuración está destinada a situaciones en las que se necesita un rendimiento y disponibilidad máximos. Comparado con el reflejo de dos niveles, el reflejo de tres niveles agrega operaciones IOPS adicionales por bloque almacenado y un mayor nivel de protección contra fallos. Nota: Un controlador sin almacenamiento de expansión no debe configurarse con reflejo triple.

Perfil de datos	Descripción
RAID de paridad doble	RAID en el que cada segmento contiene dos discos de paridad. Al igual que el reflejo por triplicado, el resultado es una alta disponibilidad, ya que los datos permanecen disponibles aunque fallen dos discos. El RAID de paridad doble es una opción de mayor capacidad que las opciones de reflejo y está destinado para cargas de trabajo de acceso secuencial y rendimiento elevado (por ejemplo, copia de seguridad) o para almacenar grandes cantidades de datos con un componente bajo de lectura aleatoria.
Opciones de paridad simple	
Reflejado	Los datos se reflejan, lo que reduce la capacidad a la mitad pero genera un sistema de alta confiabilidad y alto rendimiento. Se recomienda cuando se considera que el espacio disponible es amplio y el rendimiento es muy valioso (por ejemplo, almacenamiento de bases de datos).
RAID de paridad simple, segmentos estrechos	RAID en el que cada segmento tiene tres discos de datos y un único disco de paridad. Para situaciones en las que es aceptable la protección de paridad simple, la configuración RAID de paridad simple ofrece una opción de capacidad mucho mayor que el simple reflejo. Esta mayor capacidad se debe equilibrar con una menor capacidad de lectura aleatoria que las opciones reflejadas. La configuración RAID de paridad simple se puede considerar para aplicaciones no críticas con un componente de lectura aleatoria moderado. Para cargas de trabajo de transmisión de datos solamente, es preferible antes que la opción de RAID de paridad doble, que ofrece mayor capacidad y rendimiento.
Otros	
Segmentado	Los datos se segmentan entre varios discos, sin redundancia. Si bien esta opción maximiza tanto el rendimiento como la capacidad, si se produce un fallo en un disco, se pierden datos. Esta configuración no se recomienda. Para cargas de trabajo de transmisión de datos solamente, considere usar una configuración de RAID de paridad doble. Debido a la no redundancia, los discos configurados en un perfil segmentado no recibirán actualizaciones de firmware, salvo que las agrupaciones de almacenamiento configuradas se encuentren en un estado exportado.
RAID de paridad triple, segmentos anchos	Configuración RAID en la que cada segmento tiene tres discos para paridad. Es la opción de mayor capacidad con la excepción de la opción de datos segmentados. La reconstrucción de los datos cuando se producen fallos en una o varias unidades puede llevar bastante más tiempo debido a los segmentos anchos y el bajo rendimiento de E/S aleatoria. Al igual que con las demás configuraciones RAID, la presencia de caché puede mitigar los efectos

Perfil de datos	Descripción
	sobre el rendimiento de lectura. Por lo general, no se recomienda esta configuración.

Nota - Las versiones anteriores del software admitían el uso de paridad doble con segmentos anchos. Esto fue suplantado por la paridad triple con segmentos anchos, ya que esta configuración aumenta marcadamente la fiabilidad. Las agrupaciones configurados como paridad doble con segmentos anchos con una versión previa del software siguen siendo compatibles, pero las nuevas agrupaciones que se configuren o las que se reconfiguren no pueden seleccionar esa opción.

Opción de NSPF

Para sistemas ampliables, algunos perfiles pueden estar disponibles con una opción "NSPF". Esta sigla viene del inglés "no single point of failure", que significa que no hay puntos únicos de fallo, e indica que los datos se organizan en estructuras reflejadas o segmentos RAID de manera tal que si se produce un fallo patológico de algún estante de discos, no se pierden datos. Tenga en cuenta que los sistemas ya están configurados con redundancia entre casi todos los componentes. Cada estante de discos tiene rutas redundantes, controladores redundantes y fuentes de alimentación y ventiladores redundantes. El único fallo contra el que protege la configuración NSPF es el fallo de placa posterior del disco (que es un componente mayormente pasivo) o faltas administrativas graves (por ejemplo, desconectar las dos rutas de un estante de discos). Por lo general, la adopción de NSPF reduce la capacidad, ya que tiene requisitos más estrictos con respecto al ancho de los segmentos.

Dispositivos de log

Los dispositivos de log se pueden configurar solamente con perfiles segmentados o reflejados. Los dispositivos de log se utilizan solo si se produce un fallo en el nodo. Para que se pierdan datos con logs no reflejados, es necesario que el dispositivo falle y el nodo se reinicie inmediatamente después del fallo. Esta situación es altamente improbable; el reflejo de los dispositivos de log haría que fuera literalmente imposible, ya que tendrían que producirse dos fallos de dispositivo simultáneos y un fallo de nodo en un margen de tiempo muy pequeño.

Nota - Si se usan dispositivos de log de diferente tamaño en chasis diferentes, solo se pueden crear perfiles de log segmentados.

Dispositivos de caché

En una configuración de cluster, los dispositivos de caché instalados en las ranuras del controlador están disponibles solo para el controlador para el que se importa la agrupación de almacenamiento. En un cluster, es posible configurar que los dispositivos de caché de ambos controladores sean parte de la misma agrupación. Para hacerlo, tome control de la agrupación del nodo pasivo, agregue almacenamiento y seleccione los dispositivos de caché. Como resultado, en cualquier momento dado se tiene la mitad de los dispositivos de caché globales configurados. Si bien los datos de los dispositivos de caché se pierden en una conmutación por error, los nuevos dispositivos de caché se pueden utilizar en el nuevo controlador.

Los dispositivos de caché instalados en ranuras de estantes de discos, cuando se los agrega a una agrupación, se importan automáticamente durante la operación de failback o toma de control del cluster. No es necesario realizar ninguna configuración adicional de agrupación.

Metadispositivos

Un metadispositivo es un dispositivo de caché usado para almacenar metadatos con deduplicación y otros metadatos para proyectos y recursos compartidos. Los metadispositivos se pueden asignar a una agrupación de almacenamiento, pero no a una agrupación de almacenamiento que solo incluye unidades flash, durante la creación de la agrupación de almacenamiento y después de ella. Sin embargo, no se pueden volver a configurar como dispositivos de caché normales para una agrupación ni se pueden eliminar de una agrupación. Un metadispositivo debe ser una SSD de 3,2 TB (como mínimo) para admitir la característica de deduplicación de datos mejorada disponible en la versión de software OS8.7.0 (2013.1.7.0) o posterior.

Antes de usar metadispositivos y la función de deduplicación para agrupaciones de almacenamientos nuevas y existentes, acepte la actualización de software diferida para la deduplicación de datos v2 incluida en la versión de software OS8.7.0 (2013.1.7.0). Si se replica en otros sistemas, tanto el origen como los destinos de replicación deben tener esta actualización diferida. Para obtener más información, consulte [Data Deduplication](#), and [“Data Deduplication v2 Deferred Update” in Oracle ZFS Storage Appliance Customer Service Manual](#).

Discos de reserva

Las reservas activas se asignan como porcentaje del tamaño total de la agrupación y son independientes del perfil elegido (con la excepción del perfil segmentado, que no admite reservas activas). Como las reservas activas se asignan para cada paso de la configuración de almacenamiento, es mucho más eficaz configurar el almacenamiento como un todo en lugar de agregar almacenamiento en incrementos pequeños.

Temas relacionados:

- Creación de una agrupación de almacenamiento ([BUI](#), [CLI](#)).
- Agregación de un dispositivo de caché, log o metadispositivo a una agrupación de almacenamiento existente ([BUI](#), [CLI](#))

Configuración de copia de seguridad en la nube

Las copias de seguridad en la nube proporcionan la capacidad de respaldar instantáneas de recursos compartidos completas e incrementales de una ubicación local Oracle ZFS Storage Appliance en destinos de nube en una cuenta Infraestructura de nube de Oracle. Las instantáneas de recursos compartidos se crean del modo habitual, mientras que las instantáneas individuales se seleccionan para una copia de seguridad en la nube. En un mismo destino de nube, puede crearse una copia de seguridad de más de un dispositivo. Las copias de seguridad en la nube pueden restaurarse como nuevos recursos compartidos clonados en cualquier instancia de Oracle ZFS Storage Appliance que tenga acceso al destino de nube.

Mediante el uso del formato de archivo "tar" en lugar del formato por defecto "zfs" para las copias de seguridad en la nube, es posible crear copias de seguridad de instantáneas del sistema de archivos (no del LUN) completas e incrementales. Estas copias de seguridad pueden restaurarse en cualquier sistema, independientemente de su sistema operativo, que pueda acceder al destino de nube. Sin embargo, una copia de seguridad en la nube con formato "tar" no conserva las propiedades originales del sistema de archivos.

Después de establecer una cuenta Infraestructura de nube de Oracle y de crear cubos en Almacenamiento de objeto, puede preparar sistemas Oracle ZFS Storage Appliance para usar la copia de seguridad en la nube, definir destinos de nube y crear copias de seguridad en la nube que luego podrán restaurarse.

En la BUI, hay cinco fichas para el servicio de datos en la nube: Propiedades, Destinos, Copias de seguridad, Trabajos y Logs (log de servicio). En la CLI, el servicio de datos en la nube tiene tres nodos secundarios: `backups`, `targets` y `jobs`. Los objetos en cada uno de estos nodos secundarios de la CLI tienen nombres ordinales, como `backup-001`. En la BUI o la CLI, al crear una copia de seguridad en la nube, se crea un trabajo en la nube con una operación de tipo `backup`. Las otras operaciones para trabajos en la nube son `restore` y `delete`. Al igual que en otros servicios, las operaciones de los usuarios se registran en el log de auditoría, mientras que los resultados de las operaciones se registran en el log de alertas. Los cambios de estado del servicio de nube se registran en el log de servicio.

Para gestionar el almacenamiento en la nube, puede ver los trabajos en la nube, cancelar y reiniciar trabajos, modificar o suprimir destinos de nube, ver y filtrar copias de seguridad en

la nube, y restaurar y suprimir las copias de seguridad en la nube. Para analizar las copias de seguridad y restaurar operaciones, consulte [“Data Movement: Cloud Bytes \(Movimiento de datos: bytes de nube\)”](#) de *Guía de análisis de Oracle® ZFS Storage Appliance versión OS8.8.x* y [“Data Movement: Cloud Requests \(Movimiento de datos: solicitudes de nube\)”](#) de *Guía de análisis de Oracle® ZFS Storage Appliance versión OS8.8.x*. Para establecer alertas, consulte [“Configuración de alertas”](#) [286].

Antes de usar una copia de seguridad en la nube en controladores en cluster, es importante comprender, además de esta función, el comportamiento de la agrupación en clusters. El servicio de datos en la nube tiene detección de cluster, y cada controlador utiliza sus propias interfaces de red disponibles para comunicarse con los destinos de nube configurados a fin de realizar operaciones de restauración y copias de seguridad, y para refrescar su lista de copias de seguridad en la nube disponibles. Por lo tanto, un controlador quizás no presente de inmediato una lista actualizada de copias de seguridad en la nube de su controlador del mismo nivel. Asimismo, aunque ambos controladores comparten configuraciones del servicio, destinos de nube y copias de seguridad en la nube, cada controlador tiene su propia lista Trabajos. Después de un reinicio o un evento de failover, las operaciones de restauración o copia de seguridad en la nube que se estén llevando a cabo en el controlador afectado se vuelven a enviar automáticamente en el controlador del mismo nivel, y las operaciones se reinician desde cero.

Esta sección contiene los siguientes temas y tareas:

- [“Preparación para una copia de seguridad en la nube”](#) [173]
 - [“Configuración de su cuenta Infraestructura de nube de Oracle”](#) [173]
 - [“Agregación de autorizaciones de nube a un rol de usuario”](#) [174]
 - Activación del servicio de datos en la nube: [BUI](#), [CLI](#)
- [“Configuración de operaciones de restauración y copia de seguridad en la nube”](#) [175]
 - Definición de un destino de nube: [BUI](#), [CLI](#)
 - Creación de una copia de seguridad en la nube: [BUI](#), [CLI](#)
 - Visualización y filtrado de copias de seguridad en la nube: [BUI](#), [CLI](#)
 - Restauración de una copia de seguridad en la nube: [BUI](#), [CLI](#)
- [“Gestión del servicio de nube”](#) [194]
 - Supresión de una copia de seguridad en la nube: [BUI](#), [CLI](#)
 - Visualización de trabajos en la nube: [BUI](#), [CLI](#)
 - Cancelación y reinicio de un trabajo en la nube: [BUI](#), [CLI](#)
 - Modificación de un destino de nube: [BUI](#), [CLI](#)
 - Supresión de un destino de nube: [BUI](#), [CLI](#)
- [“Propiedades de nube”](#) [203]

Preparación para una copia de seguridad en la nube

A modo de preparación para realizar una copia de seguridad en la nube, lleve a cabo las siguientes tareas:

- [“Configuración de su cuenta Infraestructura de nube de Oracle” \[173\]](#)
- [“Agregación de autorizaciones de nube a un rol de usuario” \[174\]](#)
- Activación del servicio de datos en la nube: [BUI](#), [CLI](#)

Configuración de su cuenta Infraestructura de nube de Oracle

Infraestructura de nube de Oracle ofrece dos capas de almacenamiento distintas que son sólidas y escalables: el almacenamiento estándar es para el almacenamiento de acceso frecuente, mientras que el almacenamiento de archivos es para el almacenamiento de acceso menos frecuente y requiere más tiempo para recuperar los datos. Por lo tanto, las dos capas permiten un rendimiento máximo a un costo mínimo. Oracle Cloud Infrastructure Object Storage aborda las necesidades de almacenamiento, recuperación ante desastres, migración de datos y replicación de imágenes principales, a la vez que proporciona cifrado de datos en reposo y durante el transporte.

Cree una cuenta Infraestructura de nube de Oracle y configúrela; incluya la creación de cubos para sus datos. La capa de un cubo puede ser "estándar" o de "archivos", y no es posible cambiarla una vez creado el cubo. La copia de seguridad en la nube almacena los datos y la instantánea de recursos compartidos. Los metadatos almacenan información sobre los datos. Opcionalmente, puede almacenar metadatos y datos en diferentes cubos. Si utiliza un cubo de archivos, los metadatos deben guardarse en un cubo estándar.

Cada destino de nube usa un punto final (ubicación) de API regional, y varios dispositivos pueden usar cada cubo. Si necesita crear varios destinos de nube con el mismo punto final, cree suficientes cubos distintos para contenerlos. En la Consola de Infraestructura de nube de Oracle, tenga en cuenta lo siguiente:

- Las URL de punto final de API regional, como `https://objectstorage.us-phoenix-1.oraclecloud.com`.
- El nombre de arrendamiento y el Oracle Cloud Identifier (OCID).
Para conocer el OCID, vaya a su compartimento. En la ficha Información de arrendamiento, haga clic en **Mostrar** o en **Copiar** para el OCID.
- Nombre de usuario y OCID.
Para el OCID, seleccione su nombre de usuario en el ícono de usuario en la esquina superior derecha. En la ficha Información de usuario, haga clic en **Mostrar** o en **Copiar** para el OCID.

- Clave privada: cree un par de claves RSA pública y privada. La clave debe tener el formato de correo de privacidad mejorada (PEM). Para obtener más información, consulte "Claves y OCID necesarios" en la documentación de la API de Infraestructura de nube de Oracle disponible en <https://docs.oracle.com/en-us/iaas/Content/API/Concepts/apisigningkey.htm>.
- Nombres de cubos.

Para obtener más información sobre la API de servicio Oracle Cloud Infrastructure Object Storage, consulte "API de servicio de almacenamiento de objeto" en la documentación de la API de Infraestructura de nube de Oracle disponible en <https://docs.oracle.com/en-us/iaas/api/#/en/objectstorage/20160918/>. Aquí encontrará información como los puntos finales (ubicaciones) de las API regionales, cómo crear y gestionar cubos, y la gestión opcional del ciclo de vida de un objeto.



Atención - Si modifica los objetos de la copia de seguridad en la nube del cubo y los transforma en cubos de Oracle Cloud Infrastructure Object Storage, generará inconsistencias respecto del contenido almacenado localmente. Por lo tanto, se recomienda usar cubos dedicados para la copia de seguridad en la nube.

Agregación de autorizaciones de nube a un rol de usuario

Para los roles de usuario correspondientes, y si todos los servicios no están autorizados globalmente, agregue autorizaciones para el filtro de Nube en el ámbito Servicios. Al igual que en otros servicios, hay tres autorizaciones disponibles: administrar (activa y desactiva el servicio), configurar (cambia la configuración del servicio) y reiniciar (reinicia el servicio).

Además, agregue el ámbito Destinos de Nube, seleccione todos los destinos de nube o uno específico, y seleccione las autorizaciones:

- **copia de seguridad:** realiza la copia de seguridad de los datos de una instantánea en la nube.
- **suprimir:** suprime las copias de seguridad en la nube.
- **restaurar:** restaura las copias de seguridad en la nube en recursos compartidos locales.

Para el ámbito Proyectos y recursos compartidos, establezca filtros globales o específicos, y agregue las autorizaciones:

- **copia de seguridad:** lee los datos compartidos que se incluirán en una copia de seguridad en un destino de nube si la copia de seguridad en la nube está autorizada para ese destino de nube.
- **restaurar:** escribe los datos de la copia de seguridad en la nube si restaurar en la nube está autorizada para ese destino de nube.

Use el rol de usuario adecuado con las correspondientes autorizaciones requeridas para configurar y gestionar el servicio de datos en la nube y las copias de seguridad en la nube.

Para obtener información acerca de la configuración de usuarios, consulte [“Configuración de usuarios” \[257\]](#).

▼ Activación del servicio de datos en la nube (BUI)

Utilice el siguiente procedimiento para activar el servicio de datos en la nube.

1. **Vaya a Configuración > Servicios.**
2. **En Servicios de datos, haga clic en el ícono de encendido  para que Cloud active el servicio.**
El ícono de estado cambia al color verde.

▼ Activación del servicio de datos en la nube (CLI)

Utilice el siguiente procedimiento para activar el servicio de datos en la nube.

1. **Vaya a `configuration services cloud`.**
`hostname:> configuration services cloud`
2. **Active el servicio de nube.**
Introduzca `get` para determinar si el servicio de nube está activado y con el estado `online`. Si el servicio está desactivado, introduzca `enable`.
`hostname:configuration services cloud> get`
Properties:
 <status> = disabled
 .
 .
 .
`hostname:configuration services cloud> enable`
3. **Para confirmar que el estado del servicio de nube es `online`, introduzca `get`.**
`hostname:configuration services cloud> get`
Properties:
 <status> = online

Configuración de operaciones de restauración y copia de seguridad en la nube

Para configurar operaciones de restauración y de copia de seguridad en la nube, realice las siguientes tareas:

- Definición de un destino de nube: [BUI](#), [CLI](#)
- Creación de una copia de seguridad en la nube: [BUI](#), [CLI](#)
- Visualización y filtrado de copias de seguridad en la nube: [BUI](#), [CLI](#)
- Restauración de una copia de seguridad en la nube: [BUI](#), [CLI](#)

▼ Definición de un destino de nube (BUI)

Después de activar el servicio de datos en la nube, puede crear un destino de nube, que combina la ubicación, el cubo y el cubo de datos. Cada destino de nube usa certificados HTTPS asignados al servicio de datos en la nube a partir de la cadena de confianza del sistema y otros certificados de confianza cargados que estén asignados al servicio. Para obtener información acerca de la asignación de un certificado al servicio de datos en la nube, consulte [Asignación de un certificado a un servicio \(BUI\) \[316\]](#).

1. **Vaya a Configuración > Servicios.**
2. **En Servicios de datos, haga clic en Cloud.**
3. **(Opcional) Para establecer los cifrados y la versión de TLS, vaya a la ficha Propiedades, haga clic en el ícono de edición  para Cifrados y versiones de SSL/TLS y complete el cuadro de diálogo.**
4. **Vaya a la ficha Destinos y haga clic en el ícono de agregación  que se encuentra junto a Destinos.**
5. **En el cuadro de diálogo Agregar Destino de Nube, introduzca la siguiente información de configuración y haga clic en Agregar.**
 - **Nombre** : su nombre para este destino de nube, que debe ser exclusivo para su sistema.
 - **Ubicación**: la URL de punto final (ubicación) de API regional, como `https://objectstorage.us-phoenix-1.oraclecloud.com`.
 - **Usar cubo de datos**: seleccione esta casilla de control si sus datos y metadatos se encuentran en diferentes cubos. Los datos se guardarán en `Data Bucket`, mientras que los metadatos se guardarán en `Bucket`. Si utiliza un cubo de archivos, los metadatos deben guardarse en un cubo estándar.
 - **Cubo**: el nombre de cubo establecido. Los datos pueden guardarse en un cubo estándar o de archivos. La combinación de `Location`, `Bucket` y `Data Bucket` debe ser exclusiva para su sistema. Si seleccionó `Use data bucket`, este campo corresponde al cubo de metadatos. Si no seleccionó `Use data bucket`, este campo corresponde a los datos y metadatos. Para especificar un espacio de nombre, inclúyalo en el nombre del cubo, como `namespace/bucket`; por ejemplo, `export/test2/bucket`, donde `export/test2` es el espacio de nombre. Este método

puede usarse para especificar otro nombre de recurso compartido para el dispositivo de destino, donde el nombre de espacio se utiliza como punto de montaje.

- **Cubo de Datos:** si seleccionó `use data bucket`, este campo corresponde al cubo de datos. Si no seleccionó `use data bucket`, este campo no está disponible. La combinación de `Location`, `Bucket` y `Data Bucket` debe ser exclusiva para su sistema.
- **Usuario:** su OCID de nombre de usuario para la cuenta Infraestructura de nube de Oracle.
- **Arrendamiento:** su OCID de nombre de arrendamiento para la cuenta Infraestructura de nube de Oracle.
- **Clave Privada:** su clave privada para la cuenta, que debe coincidir con la clave pública cargada en la cuenta Infraestructura de nube de Oracle. Introduzca la clave en el formato de correo de privacidad mejorada (PEM).
- **Usar proxy web:** seleccione esta casilla de control para usar un proxy en las comunicaciones del sistema con la Web y complete los campos para el número y el nombre de puerto del host. Los campos Nombre de usuario y Contraseña son opcionales.
- **Write limit bandwidth** (Ancho de banda de límite de escritura) (opcional): seleccione esta casilla de control para limitar el ancho de banda del tráfico de escritura al cargar una copia de seguridad de nube al destino de nube. Introduzca un valor y seleccione una unidad de medida. Por ejemplo, `5 M/s` limita las escrituras en el destino de nube a 5 megabytes por segundo.
- **Read limit bandwidth** (Ancho de banda de límite de lectura) (opcional): seleccione esta casilla de control para limitar el ancho de banda del tráfico de lectura al restaurar una copia de seguridad de nube del destino de nube. Introduzca un valor y seleccione una unidad de medida. Por ejemplo, `4 M/s` limita las lecturas del destino de nube a 4 megabytes por segundo.

Temas relacionados

- [Modificación de un destino de nube \(BUI\) \[200\]](#)
- [Supresión de un destino de nube \(BUI\) \[202\]](#)
- [“Propiedades de nube” \[203\]](#)

▼ Definición de un destino de nube (CLI)

Después de activar el servicio de datos en la nube, puede crear un destino de nube, que combina la ubicación, el cubo y el cubo de datos. Cada destino de nube usa certificados HTTPS asignados al servicio de datos en la nube a partir de la cadena de confianza del sistema y otros certificados de confianza cargados que estén asignados al servicio. Para obtener información acerca de la asignación de un certificado al servicio de datos en la nube, consulte [Asignación de un certificado a un servicio \(CLI\) \[316\]](#).

1. **Vaya a** `configuration services cloud`.

```
hostname:> configuration services cloud
```

2. **(Opcional) Para establecer los cifrados y las versiones de TLS, introduzca `ls` a fin de mostrar las propiedades y luego establezca las propiedades `tls_version` y `ciphers`.**

3. **Introduzca `targets`.**

4. **Introduzca `get` para mostrar las propiedades.**

```
hostname:configuration services cloud targets> get
Properties:
    name = (unset)
    location = (unset)
    user = (unset)
    databucket_on = false
    bucket = (unset)
    data_bucket = (unset)
    tenancy = (unset)
    key = (unset)
    proxy_on = false
    proxy_host = (unset)
    proxy_user = (unset)
    proxy_password = (unset)
    writelimit = (unset)
    readlimit = (unset)
```

5. **Para modificar las propiedades, use el comando `set`, por ejemplo, `set name=oci-phoenix`. Las propiedades de configuración son las siguientes:**

- **nombre:** su nombre para este destino de nube, que debe ser exclusivo para su sistema.
- **ubicación:** la URL de punto final (ubicación) de API regional, como `https://objectstorage.us-phoenix-1.oraclecloud.com`.
- **usuario:** su OCID de nombre de usuario para la cuenta Infraestructura de nube de Oracle.
- **databucket_on:** establézcalo en `true` si los datos y metadatos se encuentran en diferentes cubos. Los datos se guardarán en `data_bucket`, mientras que los metadatos se guardarán en `bucket`. Si utiliza un cubo de archivos, los metadatos deben guardarse en un cubo estándar.
- **cubo:** el nombre de cubo establecido. Los datos pueden guardarse en un cubo estándar o de archivos. La combinación de `location`, `bucket` y `data_bucket` debe ser exclusiva para su sistema. Si establece `databucket_on` en `true`, esta propiedad corresponde al cubo de metadatos. Si establece `databucket_on` en `false`, esta propiedad corresponde a los datos y metadatos. Para especificar un espacio de nombre, inclúyalo en el nombre del cubo, como `namespace/bucket`; por ejemplo, `export/test2/bucket`, donde `export/test2` es el espacio de nombre. Este método puede usarse para especificar otro nombre de recurso compartido para el dispositivo de destino, donde el nombre de espacio se utiliza como punto de montaje.
- **data_bucket:** si establece `databucket_on` en `true`, esta propiedad corresponde al cubo de datos. Si establece `databucket_on` en `false`, esta propiedad no se puede establecer. La combinación de `location`, `bucket` y `data_bucket` debe ser exclusiva para su sistema.

- **arrendamiento:** su OCID de nombre de arrendamiento para la cuenta Infraestructura de nube de Oracle.
- **clave:** su clave privada para la cuenta, que debe coincidir con la clave pública cargada en la cuenta Infraestructura de nube de Oracle. Introduzca la clave en el formato de correo de privacidad mejorada (PEM).

Use el comando `setkey` para introducir la clave en modo interactivo y así permitir múltiples líneas. Cuando termine de introducir todas las líneas, introduzca un punto (".").

```
hostname:configuration services cloud targets> setkey
("." to end)> - - - -BEGIN RSA PRIVATE KEY- - - -
("." to end)> MD0CAQACCQDJCnSbjr7nUQIDAQABAggQMmdyF9wgQIFAQayRsCBQDhoGQDAgRr
("." to end)> NWanAGQeHthbAgQeJsyk
("." to end)> - - - -END RSA PRIVATE KEY- - - -
("." to end)> .
```

- **proxy_on:** establézcalo en `true` para usar un proxy en las comunicaciones del sistema con la Web y complete la propiedad de `proxy_host` (número y nombre de puerto del host). Las propiedades `proxy_user` (nombre de usuario) y `proxy_password` (contraseña del usuario) son opcionales. Ejemplo de `proxy_host`: `www-proxy.us.ejemplo.com:80`.
- **writelimit** (opcional): establezca esto en un valor y una unidad de medida para limitar el ancho de banda del tráfico de escritura al cargar una copia de seguridad de nube al destino de nube. Por ejemplo, `5 M/s` limita las escrituras en el destino de nube a 5 megabytes por segundo.
- **readlimit** (opcional): establezca esto en un valor y una unidad de medida para limitar el ancho de banda del tráfico de lectura al restaurar una copia de seguridad de nube del destino de nube. Por ejemplo, `4 M/s` limita las lecturas del destino de nube a 4 megabytes por segundo.

6. Al finalizar, introduzca `commit`.

```
hostname:configuration services cloud (uncommitted)> commit
```

Temas relacionados

- [Modificación de un destino de nube \(CLI\) \[201\]](#)
- [Supresión de un destino de nube \(CLI\) \[203\]](#)
- [“Propiedades de nube” \[203\]](#)

▼ Creación de una copia de seguridad en la nube (BUI)

Después de definir los destinos de nube, puede crear una copia de seguridad en la nube de la instantánea de un recurso compartido (sistema de archivos o LUN) en un destino de nube. Puede seleccionar una instantánea incremental si hay disponible una instantánea principal en

el sistema local y en copia de seguridad en el mismo destino de nube. Una copia de seguridad de instantánea incremental solo realiza una copia de la diferencia existente entre la instantánea anterior y la actual. Al crear una copia de seguridad en la nube, se crea un trabajo en la nube con una operación de tipo `backup`. Las instantáneas en diferentes sistemas pueden tener el mismo nombre, como `snap2`, porque a las instantáneas se les asigna una identificación exclusiva para cada sistema.

Existen dos formatos para las copias de seguridad en la nube: "zfs" y "tar". La misma instantánea del mismo sistema puede usarse en dos copias de seguridad en la nube: una con el formato `zfs` y otra con el formato `tar`. Los formatos admiten las funciones que aparecen en la tabla siguiente.

Función	Formato ZFS	Formato tar
Restauración solo en Oracle ZFS Storage Appliance o en un servidor Oracle Solaris	✓	
Restauración en cualquier sistema independientemente de su sistema operativo		✓
Compatibilidad con instantáneas del sistema de archivos y del LUN	✓	
Compatibilidad solo con instantáneas del sistema de archivos		✓
Conservación de propiedades del sistema de archivos	✓	
Conservación de propiedades del LUN	✓	
Compatibilidad con copias de seguridad completas e incrementales	✓	✓
Compatibilidad con el mismo cubo Infraestructura de nube de Oracle	✓	✓
Compresión de alta eficacia:	✓	
■ Si el recurso compartido subyacente está comprimido, se transfieren menos datos y, por lo tanto, la copia de seguridad es más rápida. ■ Las copias de seguridad incrementales se realizan en el nivel de bloque.		
Compresión de eficacia media:		✓
■ Los archivos se leen y se comprimen durante la operación de copia de seguridad. ■ Las copias de seguridad incrementales se realizan en el nivel del archivo. No es eficaz en particular si se modifica un archivo grande, ya que el archivo completo será parte de la copia de seguridad incremental.		

Nota - Después de incluir una instantánea local en una copia de seguridad en la nube en su cuenta Infraestructura de nube de Oracle, puede suprimirla localmente, según sus políticas. No obstante, conserve las instantáneas locales que puedan ser instantáneas principales de futuras instantáneas incrementales.

1. Asegúrese de que los destinos de nube estén en línea.

- a. Vaya a Configuración > Servicios y haga clic en Cloud.
 - b. Haga clic en el separador Destinos.
 - c. Para cada destino de nube que se use, asegúrese de que el ícono de estado sea verde. Si no tiene este color, pero el ícono del servicio de datos en la nube sí es verde, compruebe que las propiedades del destino de nube sean válidas. Consulte [Definición de un destino de nube \(BUI\) \[176\]](#).
2. Vaya a Recursos compartidos > Recursos compartidos y haga clic en Sistemas de archivos o en LUN, según corresponda.
 3. Mueva el cursor sobre el recurso compartido que se incluirá en la copia de seguridad y haga clic en el ícono de edición .
 4. Haga clic en la ficha Instantáneas.
 5. Mueva el cursor sobre la instantánea que se incluirá en la copia de seguridad y haga clic en el ícono de copia de seguridad en la nube .
 6. **Seleccione un destino de nube.**
 Realice los siguientes pasos para cada destino de nube donde se almacenará la copia de seguridad de nube. Para cada destino de nube se crea un trabajo nuevo de copia de seguridad en la nube.
 - a. En el cuadro de diálogo Crear copia de seguridad, seleccione un destino de nube.
 - b. Seleccione un formato haciendo clic en ZFS o en Tar.
 ZFS es el valor por defecto.
 - c. Para seleccionar una instantánea incremental, haga clic en la casilla de control Incremental y seleccione una instantánea principal.
 La instantánea principal debe estar disponible en el sistema local y en copia de seguridad en el mismo destino de nube. La instantánea principal también debe estar en el mismo formato que la instantánea incremental: zfs o tar.
 - d. Haga clic en Aplicar.

Aparece el cuadro de diálogo Detalles de la copia de seguridad, que muestra dinámicamente la ratio de transferencia de la copia de seguridad, la cantidad de datos transferidos y el estado `in-progress`. El estado cambia a `completed` una vez finalizado el proceso. Si se estableció la propiedad de límite de escritura para el destino de nube, el ancho de banda del tráfico de escritura se limita al valor establecido al cargar la copia de seguridad de nube al destino de nube. Haga clic en OK (Aceptar) para cerrar el cuadro de diálogo.

- 7. Para ver más detalles del progreso, incluido el porcentaje de finalización, vaya a Configuración > Servicios y haga clic en Cloud; luego, haga clic en la ficha Trabajos.**

La lista Trabajos contiene los trabajos activos y finalizados recientemente en el servicio de datos en la nube y se muestra en orden cronológico. La columna Actualizaciones contiene la fecha y la hora en que se creó el trabajo, así como la fecha y la hora en que se inició o se actualizó la copia de seguridad. La columna Estado indica el porcentaje de finalización, la cantidad de datos transferidos y la ratio de transferencia de la copia de seguridad.

- 8. Para ver los detalles del trabajo, haga clic en él en la lista Trabajos.**

Haga clic en OK (Aceptar) para cerrar el cuadro de diálogo. Una vez completado el trabajo, los datos de la copia de seguridad estarán disponibles en otros sistemas Oracle ZFS Storage Appliance configurados con el mismo destino de nube.

Si se seleccionó el formato `tar`, la copia de seguridad en la nube puede restaurarse en cualquier sistema, independientemente de su sistema operativo, que pueda acceder al destino de nube.

Temas relacionados

- [Cancelación y reinicio de un trabajo en la nube \(BUI\) \[199\]](#)
- [Visualización de trabajos en la nube \(BUI\) \[196\]](#)
- [Definición de un destino de nube \(BUI\) \[176\]](#)
- [Modificación de un destino de nube \(BUI\) \[200\]](#)
- [Supresión de un destino de nube \(BUI\) \[202\]](#)
- [Supresión de una copia de seguridad en la nube \(BUI\) \[195\]](#)
- [“Propiedades de nube” \[203\]](#)

▼ Creación de una copia de seguridad en la nube (CLI)

Después de definir los destinos de nube, puede crear una copia de seguridad en la nube de la instantánea de un recurso compartido (sistema de archivos o LUN) en un destino de nube. Puede seleccionar una instantánea incremental si hay disponible una instantánea principal en el sistema local y en copia de seguridad en el mismo destino de nube. Una copia de seguridad

de instantánea incremental solo realiza una copia de la diferencia existente entre la instantánea anterior y la actual. Al crear una copia de seguridad en la nube, se crea un trabajo en la nube con una operación de tipo `backup`. Las instantáneas en diferentes sistemas pueden tener el mismo nombre, como `snap2`, porque a las instantáneas se les asigna una identificación exclusiva para cada sistema.

Existen dos formatos para las copias de seguridad en la nube: "zfs" y "tar". La misma instantánea del mismo sistema puede usarse en dos copias de seguridad en la nube: una con el formato `zfs` y otra con el formato `tar`. Los formatos admiten las funciones que aparecen en la tabla siguiente.

Función	Formato ZFS	Formato tar
Restauración solo en Oracle ZFS Storage Appliance o en un servidor Oracle Solaris	✓	
Restauración en cualquier sistema independientemente de su sistema operativo		✓
Compatibilidad con instantáneas del sistema de archivos y del LUN	✓	
Compatibilidad solo con instantáneas del sistema de archivos		✓
Conservación de propiedades del sistema de archivos	✓	
Conservación de propiedades del LUN	✓	
Compatibilidad con copias de seguridad completas e incrementales	✓	✓
Compatibilidad con el mismo cubo Infraestructura de nube de Oracle	✓	✓
Compresión de alta eficacia:	✓	
■ Si el recurso compartido subyacente está comprimido, se transfieren menos datos y, por lo tanto, la copia de seguridad es más rápida. ■ Las copias de seguridad incrementales se realizan en el nivel de bloque.		
Compresión de eficacia media:		✓
■ Los archivos se leen y se comprimen durante la operación de copia de seguridad. ■ Las copias de seguridad incrementales se realizan en el nivel del archivo. No es eficaz en particular si se modifica un archivo grande, ya que el archivo completo será parte de la copia de seguridad incremental.		

Nota - Después de incluir una instantánea local en una copia de seguridad en la nube en su cuenta Infraestructura de nube de Oracle, puede suprimirla localmente, según sus políticas. No obstante, conserve las instantáneas locales que puedan ser instantáneas principales de futuras instantáneas incrementales.

Antes de empezar (Opcional) Para determinar si una copia de seguridad en la nube de una instantánea es incremental y para ver sus elementos principales, vaya a la instantánea (pasos 1 a 7), introduzca

el nodo `targets`, enumere y seleccione el destino, y enumere las propiedades del destino. La propiedad `parents` se carga si la copia de seguridad en la nube tiene elementos principales, como se muestra en el siguiente ejemplo.

```
hostname:shares default/fs-1@snap3> targets
hostname:shares default/fs-1@snap3 targets> select target-000
hostname:shares default/fs-1@snap3 target-000> ls
Properties:
    name = oci-phoenix
      id = a9aea6e0-55b8-4cd5-bdf0-ba0637be44b2
    format = zfs
    parents = snap1,snap2
```

1. **Asegúrese de que los destinos de nube estén en línea.**
 - a. **Vaya a** `configuration services cloud targets`.
 - b. **Introduzca** `ls` **para mostrar los destinos de nube y seleccione el destino correspondiente.**
 - c. **Para confirmar que la propiedad** `state` **es** `online`, **introduzca** `ls`. **Si es** `offline`, **pero el servicio de datos en la nube aparece** `online`, **compruebe que las propiedades del destino de nube sean válidas. Consulte** [Definición de un destino de nube \(CLI\) \[177\]](#).
2. **Introduzca** `top` **para volver al contexto raíz.**
3. **Navegue hasta** `shares` **e introduzca** `ls` **para mostrar los proyectos.**
4. **Seleccione el proyecto con la instantánea de recursos compartidos que se incluirá en la copia de seguridad e introduzca** `ls` **para mostrar las propiedades y los recursos compartidos.**

```
hostname:shares> select default
hostname:shares default> ls
```
5. **Seleccione el recurso compartido con la instantánea que se incluirá en la copia de seguridad.**

```
hostname:shares default> select fs-1
```
6. **Vaya a** `snapshots` **e introduzca** `ls` **para mostrar las instantáneas.**

```
hostname:shares default/fs-1> snapshots
hostname:shares default/fs-1 snapshots> ls
```
7. **Seleccione la instantánea para la copia de seguridad en la nube.**

```
hostname:shares default/fs-1 snapshots> select snap2
hostname:shares default/fs-1@snap2>
```

8. Vaya a backups.

```
hostname:shares default/fs-1@snap2> backups
hostname:shares default/fs-1@snap2 backups>
```

9. Introduzca create.

```
hostname:shares default/fs-1@snap2 backups> create
hostname:shares default/fs-1@snap2 backup-001 (uncommitted)>
```

10. Establezca el destino con un nombre de destino de nube existente.

Si el nombre del destino de nube tiene espacios, use el comando `select name="target name"`.

Sugerencia: Use la finalización con tabulación para el nombre del destino de nube.

```
hostname:shares default/fs-1@snap2 backup-001 (uncommitted)> set target=oci-phoenix
target = oci-phoenix
hostname:shares default/fs-1@snap2 backup-001 (uncommitted)>
```

11. Para especificar el formato tar, establezca format en tar. De lo contrario, se usará el formato por defecto, que es zfs.

```
hostname:shares default/fs-1@snap2 backup-001 (uncommitted)> set format=tar
format = tar
hostname:shares default/fs-1@snap2 backup-001 (uncommitted)>
```

12. Para establecer la instantánea actual como una instantánea incremental, establezca incremental en true y establezca la instantánea parent por nombre.

La instantánea principal debe estar disponible en el sistema local y en copia de seguridad en el mismo destino de nube. La instantánea principal también debe estar en el mismo formato que la instantánea incremental: zfs o tar.

Sugerencia: Use la finalización con tabulación para ver una lista de nombres de instantáneas principales en el sistema local y en el destino de nube.

```
hostname:shares default/fs-1@snap2 backup-001 (uncommitted)> set incremental=true
incremental = true
hostname:shares default/fs-1@snap2 backup-001 (uncommitted)> set parent=snap0
parent = snap0
hostname:shares default/fs-1@snap2 backup-001 (uncommitted)>
```

13. Introduzca el comando commit.

Para enviar la copia de seguridad en la nube a otro destino de nube, repita los pasos 9 a 13 a fin de crear un nuevo trabajo de copia de seguridad en la nube con un destino de nube diferente.

```
hostname:shares default/fs-1@snap2 backup-001 (uncommitted)> commit
hostname:shares default/fs-1@snap2 backups>
```

14. Para supervisar el progreso a medida que se vaya realizando la copia de seguridad de los datos, introduzca top y vaya a configuration services cloud jobs.

```
hostname:configuration services cloud backups> top
hostname:> configuration services cloud jobs
```

15. Introduzca `ls` para ver los trabajos en la nube.

La lista Trabajos contiene los trabajos activos y finalizados recientemente en el servicio de datos en la nube y se muestra en orden cronológico. Se muestra un máximo de 100 trabajos en la nube. Utilice el comando `next` para ver los próximos 100 trabajos y utilice el comando `previous` para ver los 100 trabajos anteriores.

```
hostname:configuration services cloud jobs> ls
Jobs:
JOB      OPERATION  CREATED
job-000  backup     2019-8-03 15:05:53
```

16. Busque y seleccione el trabajo en la nube por número e introduzca `ls` para ver los detalles.

Una vez completado el trabajo, los datos de la copia de seguridad estarán disponibles en otros sistemas Oracle ZFS Storage Appliance configurados con el mismo destino de nube. Si se seleccionó el formato `tar`, la copia de seguridad en la nube puede restaurarse en cualquier sistema, independientemente de su sistema operativo, que pueda acceder al destino de nube. La ruta de acceso al juego de datos en la propiedad `details` refleja el formato de la copia de seguridad en la nube:

- Formato ZFS: `zfs/backups/zfs`
- Formato `tar`: `zfs/backups/tar`

Si se estableció la propiedad de límite de escritura para el destino de nube, el ancho de banda del tráfico de escritura se limita al valor establecido al cargar la copia de seguridad de nube al destino de nube.

```
hostname:configuration services cloud jobs> select job-000
hostname:configuration services cloud job-000> ls
Properties:
      op = backup
      target = e641f83d-4628-42ba-8757-d66c4c98c0d9
      targetName = oci-phoenix
      created = 2020-10-22 22:23:40
      updated = 2020-10-22 22:27:33
      id = 3babb944-07f6-4b69-8de1-f6dcfeab5fb2
      status = in-progress
      format = zfs
      rate = 6MB/s
      transferred = 1.46G
      estimated_size = 40.1G
      dataset = p1/local/default/f-1
      backup = 3e035b7e546e0d02/1cbfdb5ff2259b76
      snapshot = snap9
      details = uploading backup to zfs/backups/zfs
                3e035b7e546e0d02/1cbfdb5ff2259b76/000000001
```

Temas relacionados

- [Cancelación y reinicio de un trabajo en la nube \(CLI\) \[199\]](#)
- [Visualización de trabajos en la nube \(CLI\) \[198\]](#)

- [Definición de un destino de nube \(CLI\) \[177\]](#)
- [Modificación de un destino de nube \(CLI\) \[201\]](#)
- [Supresión de un destino de nube \(CLI\) \[203\]](#)
- [Supresión de una copia de seguridad en la nube \(CLI\) \[195\]](#)
- [“Propiedades de nube” \[203\]](#)

▼ Visualización y filtrado de copias de seguridad en la nube (BUI)

Este procedimiento permite ver en varias páginas las copias de seguridad en la nube finalizadas y filtrarlas con una búsqueda básica por nombre de destino de nube, nombre de origen, formato o nombre del juego de datos. La función de búsqueda avanzada permite buscar los mismos criterios en simultáneo y, además, buscar por el nombre principal.

1. **Vaya a Configuración > Servicios y haga clic en Cloud.**
2. **Haga clic en la ficha Copias de seguridad.**
La lista Copias de seguridad contiene las copias de seguridad en la nube finalizadas y las muestra en orden cronológico.
3. **Si hay varias páginas de copias de seguridad en la nube, use las teclas de flecha doble para navegar entre las páginas. Para ir a la primera página, haga clic en la tecla de flecha simple que apunta hacia la izquierda. Para ir a la última página, haga clic en la tecla de flecha simple que apunta hacia la derecha.**
4. **Para filtrar las copias de seguridad en la nube con una búsqueda básica, haga clic en el ícono de búsqueda , introduzca el nombre de destino, el nombre de origen, el formato o el nombre del juego de datos, y pulse Intro.**
Solo puede introducir una propiedad. El nombre de destino debe ser una coincidencia exacta; las otras propiedades pueden ser valores parciales.
Para volver a ver la lista completa sin filtrar, borre el campo de búsqueda y pulse Intro.
5. **Para filtrar las copias de seguridad en la nube con una búsqueda avanzada, haga clic en el ícono de flecha hacia abajo  que aparece debajo del ícono de búsqueda . En el cuadro de diálogo Buscar, complete los campos según corresponda y haga clic en Aplicar.**
Seleccione el destino y el formato de las listas desplegadas. El nombre de origen, el nombre del juego de datos y el nombre principal pueden ser valores parciales.

Al finalizar, los criterios de búsqueda y los valores aparecen en el campo de búsqueda junto al ícono de búsqueda.

Para volver a ver la lista completa sin filtrar, borre el campo de búsqueda y pulse Intro.

Temas relacionados

- [Restauración de una copia de seguridad en la nube \(BUI\) \[190\]](#)
- [Supresión de una copia de seguridad en la nube \(BUI\) \[195\]](#)
- [“Propiedades de nube” \[203\]](#)

▼ Visualización y filtrado de copias de seguridad en la nube (CLI)

Puede ver a la vez 100 copias de seguridad en la nube finalizadas. Use los comandos `next` y `previous` para ver las 100 copias de seguridad anteriores o posteriores. Asimismo, puede filtrar la lista con cinco propiedades: `target`, `source`, `format`, `dataset` y `parent`.

1. Vaya a `configuration services cloud backups`.

```
hostname:> configuration services cloud backups
```

2. Introduzca `ls` para ver las propiedades y las copias de seguridad en la nube.

La lista Copias de seguridad contiene las copias de seguridad en la nube finalizadas y las muestra en orden cronológico. Se muestra un máximo de 100 copias de seguridad en la nube.

```
hostname:configuration services cloud backups> ls
Properties:
  total      = 68
  selected   = 68
  target     = (unset)
  format     = (unset)
  source     = (unset)
  dataset    = (unset)
  parent     = (unset)
Backups:
BACKUP      UPLOADED      TARGET      SOURCE      DATASET
backup-000  2019-8-04 17:14:08 oci-phoenix hostname p1/local/default/fs-1@snap2
backup-001  2019-8-04 17:25:36 oci-phoenix hostname p1/local/default/fs-1@snap31
backup-002  2019-8-11 10:04:29 oci-phoenix hostname p1/local/default/fs-49@snap100
backup-003  2019-8-15 11:18:32 oci-phoenix hostname p1/local/default/fs-1@snap1192
backup-004  2019-8-16 23:09:16 oci-ashburn hostname p1/local/default/fs-22@snap107
.
.
.
backup-066  2019-8-19 11:28:47 oci-phoenix server38 p1/local/default/fs-386@snap51
backup-067  2019-8-19 18:13:06 oci-phoenix server38 p1/local/default/fs-386@snap54
```

3. Utilice el comando `next` para ver las próximas 100 copias de seguridad y utilice el comando `previous` para ver las 100 copias anteriores.

4. Para filtrar la lista, establezca un valor específico para una propiedad e introduzca `ls`. Para borrar el filtro, anule la definición de la propiedad.

Puede establecer varios filtros y anular su definición. Las propiedades que se pueden filtrar son las siguientes: `target`, `source`, `format`, `dataset` y `parent`. Las propiedades `target` y `parent` deben ser una coincidencia exacta; las otras propiedades pueden ser valores parciales.

Nota - Después del filtrado, la numeración de las copias de seguridad en la nube se reanuda en `backup-000`. Puede realizar una operación de inmediato en los nuevos números de copia de seguridad. Si no filtra la lista de copias de seguridad en la nube y luego realiza una operación, asegúrese de usar los números de copia de seguridad originales.

```
hostname:configuration services cloud backups> set target=oci-ashburn
target = oci-ashburn
hostname:configuration services cloud backups> ls
Properties:
  total      = 68
  selected   = 1
  target     = oci-ashburn
  format     = (unset)
  source     = (unset)
  dataset    = (unset)
  parent     = (unset)
Backups:
BACKUP      UPLOADED          TARGET      SOURCE      DATASET
backup-000  2019-8-16  23:09:16  oci-ashburn hostname p1/local/default/fs-22@snap107
hostname:configuration services cloud backups> unset target
target = (unset)
hostname:configuration services cloud backups> set source=server
source = server
hostname:configuration services cloud backups> ls
Properties:
  total      = 68
  selected   = 2
  target     = (unset)
  format     = (unset)
  source     = server
  dataset    = (unset)
  parent     = (unset)
Backups:
BACKUP      UPLOADED          TARGET      SOURCE      DATASET
backup-000  2019-8-19  11:28:47  oci-phoenix server38  p1/local/default/fs-386@snap51
backup-001  2019-8-19  18:13:06  oci-phoenix server38  p1/local/default/fs-386@snap54
hostname:configuration services cloud backups> unset source
source = (unset)
hostname:configuration services cloud backups> set target=oci-phoenix
target = oci-phoenix
hostname:configuration services cloud backups> set dataset=snap1
dataset = snap1
hostname:configuration services cloud backups> ls
Properties:
  total      = 68
  selected   = 2
  target     = oci-phoenix
  format     = (unset)
  source     = (unset)
  dataset    = snap1
```

```

    parent    = (unset)
Backups:
BACKUP      UPLOADED      TARGET      SOURCE      DATASET
backup-000  2019-8-11  10:04:29  oci-phoenix  hostname  p1/local/default/fs-49@snap100
backup-001  2019-8-15  11:18:32  oci-phoenix  hostname  p1/local/default/fs-1@snap1192
hostname:configuration services cloud backups> unset target
    target = (unset)
hostname:configuration services cloud backups> unset dataset
    dataset = (unset)
hostname:configuration services cloud backups> ls
Properties:
    total      = 68
    selected   = 68
    target     = (unset)
    format     = (unset)
    source     = (unset)
    dataset    = (unset)
    parent     = (unset)
Backups:
BACKUP      UPLOADED      TARGET      SOURCE      DATASET
backup-000  2019-8-04  17:14:08  oci-phoenix  hostname  p1/local/default/fs-1@snap2
backup-001  2019-8-04  17:25:36  oci-phoenix  hostname  p1/local/default/fs-1@snap31
backup-002  2019-8-11  10:04:29  oci-phoenix  hostname  p1/local/default/fs-49@snap100
backup-003  2019-8-15  11:18:32  oci-phoenix  hostname  p1/local/default/fs-1@snap1192
backup-004  2019-8-16  23:09:16  oci-ashburn  hostname  p1/local/default/fs-22@snap107
.
.
.
backup-066  2019-8-19  11:28:47  oci-phoenix  server38  p1/local/default/fs-386@snap51
backup-067  2019-8-19  18:13:06  oci-phoenix  server38  p1/local/default/fs-386@snap54

```

Temas relacionados

- [Restauración de una copia de seguridad en la nube \(CLI\) \[192\]](#)
- [Supresión de una copia de seguridad en la nube \(CLI\) \[195\]](#)
- [“Propiedades de nube” \[203\]](#)

▼ Restauración de una copia de seguridad en la nube (BUI)

Las copias de seguridad en la nube pueden restaurarse como nuevos recursos compartidos clonados en cualquier sistema Oracle ZFS Storage Appliance que tenga acceso al destino de nube.

Las copias de seguridad en la nube del sistema de archivos creadas con el formato tar pueden restaurarse en Oracle ZFS Storage Appliance o en cualquier sistema, independientemente de su sistema operativo, que pueda acceder al destino de nube. Después de restaurar una copia de seguridad en la nube con formato tar en Oracle ZFS Storage Appliance, establezca las propiedades del sistema de archivos como se describe en [Edición de un sistema de archivos o un LUN \(BUI\) \[492\]](#).

1. **Vaya a Configuración > Servicios y haga clic en Cloud.**

2. **Haga clic en la ficha Copias de seguridad.**
3. **Busque la copia de seguridad en la nube que se restaurará y haga clic en el ícono de restauración .**
4. **En el cuadro de diálogo Restaurar copia de seguridad, seleccione una agrupación y un proyecto. Introduzca un nuevo nombre de recurso compartido donde se restaurará el juego de datos.**

5. **Haga clic en Aplicar.**

Después de hacer clic en Aplicar, aparece el cuadro de diálogo Detalles de restauración, que muestra dinámicamente la ratio de transferencia de la restauración, la cantidad de datos transferidos y el estado *in-progress*. El estado cambia a *completed* una vez finalizado el proceso. Si se estableció la propiedad de límite de lectura para el destino de nube, el ancho de banda del tráfico de lectura se limita al valor establecido al restaurar la copia de seguridad de nube del destino de nube. Haga clic en OK (Aceptar) para cerrar el cuadro de diálogo.

6. **Para ver más detalles del progreso, incluido el porcentaje de finalización, vaya a Configuración > Servicios y haga clic en Cloud; luego, haga clic en la ficha Trabajos.**

La lista Trabajos contiene los trabajos activos y finalizados recientemente en el servicio de datos en la nube y se muestra en orden cronológico. La columna Actualizaciones contiene la fecha y la hora en que se creó/actualizó el trabajo, así como la fecha y la hora en que se inició la restauración. La columna Estado indica el porcentaje de finalización, la cantidad de datos transferidos y la ratio de transferencia de la restauración.

7. **Para ver los detalles del trabajo, haga clic en él en la lista Trabajos.**

Haga clic en OK (Aceptar) para cerrar el cuadro de diálogo.

8. **Una vez finalizada la operación de restauración, puede ver los detalles de la copia de seguridad en la nube:**

- a. **Vaya a Configuración > Servicios y haga clic en Cloud.**

- b. **Haga clic en la ficha Copias de seguridad.**

La lista Copias de seguridad contiene las copias de seguridad en la nube finalizadas y las muestra en orden cronológico.

- c. **Haga doble clic en la copia de seguridad en la nube que se acaba de restaurar.**

- d. Después de ver el cuadro de diálogo Detalles de la copia de seguridad, haga clic en Aceptar.

Temas relacionados

- [Visualización y filtrado de copias de seguridad en la nube \(BUI\) \[187\]](#)
- [Supresión de una copia de seguridad en la nube \(BUI\) \[195\]](#)
- [“Propiedades de nube” \[203\]](#)

▼ Restauración de una copia de seguridad en la nube (CLI)

Las copias de seguridad en la nube pueden restaurarse como nuevos recursos compartidos clonados en cualquier sistema Oracle ZFS Storage Appliance que tenga acceso al destino de nube.

Las copias de seguridad en la nube del sistema de archivos creadas con el formato tar pueden restaurarse en Oracle ZFS Storage Appliance o en cualquier sistema, independientemente de su sistema operativo, que pueda acceder al destino de nube. Después de restaurar una copia de seguridad en la nube con formato tar en Oracle ZFS Storage Appliance, establezca las propiedades del sistema de archivos como se describe en [Edición de un sistema de archivos o un LUN \(CLI\) \[492\]](#).

1. **Vaya a configuration services cloud backups.**

```
hostname:> configuration services cloud backups
```

2. **Introduzca `ls` para ver las propiedades y las copias de seguridad en la nube.**

La lista Copias de seguridad contiene las copias de seguridad en la nube finalizadas y las muestra en orden cronológico. Se muestra un máximo de 100 copias de seguridad en la nube a la vez.

```
hostname:configuration services cloud backups> ls
Properties:
  total      = 68
  selected   = 68
  target     = (unset)
  format     = (unset)
  source     = (unset)
  dataset    = (unset)
  parent     = (unset)
Backups:
BACKUP      UPLOADED      TARGET      SOURCE      DATASET
backup-000  2019-8-04  17:14:08  oci-phoenix  hostname  p1/local/default/fs-1@snap2
backup 001  2019-8-04  17:25:36  oci-phoenix  hostname  p1/local/default/fs-1@snap31
.
.
.
```

3. Busque y seleccione la copia de seguridad en la nube que se restaurará.

```
hostname:configuration services cloud backups> select backup-000
hostname:configuration services cloud backup-000>
```

4. Introduzca `restore`.

```
hostname:configuration services cloud backups> restore
hostname:configuration services cloud backup-000 restore (uncommitted)>
```

5. Introduzca `ls` para ver las propiedades de la operación `restore`.

```
hostname:configuration services cloud backup-000 restore (uncommitted)> ls
Properties:
    pool = (unset)
    project = (unset)
    share = (unset)
```

6. Establezca las propiedades `pool`, `project` y `share` para su sistema. Use un nuevo nombre de recurso compartido donde se restaurará el juego de datos.

```
hostname:configuration services cloud backup-000 restore (uncommitted)> set pool=p1
hostname:configuration services cloud backup-000 restore (uncommitted)> set project=default
hostname:configuration services cloud backup-000 restore (uncommitted)> set share=new-share
hostname:configuration services cloud backup-000 restore (uncommitted)>
```

7. Introduzca el comando `commit`.

```
hostname:configuration services cloud backup-000 restore (uncommitted)> commit
hostname:configuration services cloud>
```

8. Vaya a `jobs` e introduzca `ls` para ver los trabajos en la nube.

La lista Trabajos contiene los trabajos activos y finalizados recientemente en el servicio de datos en la nube y se muestra en orden cronológico.

```
hostname:configuration services cloud jobs> ls
Jobs:
JOB      OPERATION  CREATED
job-000  backup     2019-8-03 15:05:53
job-001  restore    2019-8-06 17:14:36
```

9. Seleccione el trabajo en la nube por número e introduzca `ls` para ver los detalles.

La copia de seguridad en la nube restaurada no estará disponible en los protocolos de almacenamiento configurados hasta que se haya completado el trabajo de restauración.

Si se estableció la propiedad de límite de escritura para el destino de nube, el ancho de banda del tráfico de escritura se limita al valor establecido al cargar la copia de seguridad de nube al destino de nube.

```
hostname:configuration services cloud jobs> select job-001
hostname:configuration services cloud job-001> ls
    op = restore
    target = 9ca87404-24e2-11e9-a929-0b69dceb9c81
    targetName = oci-phoenix
```

```
created = 2019-8-06 17:14:36
updated = 2019-8-11 20:33:09
id = cbb88888852e58088/445c15865cb329c3
status = in-progress
format = zfs
rate = 74KB/s
transferred = 5.98G
estimated_size = 1.00T
dataset = p1/local/default/fs-1
backup = 3e035b7e546e0d02/1cbfdb5ff2259b76
snapshot = snap2
details = uploading backup to zfs/backups/zfs/3e035b7e546e0d02/
db7fd6c55558cea0/000000001
```

10. Una vez finalizada la operación de restauración, puede ver los detalles de la copia de seguridad en la nube:

a. Vaya a configuration services cloud backups.

b. Seleccione la copia de seguridad en la nube por número.

```
hostname:configuration services cloud backups> select backup-000
```

c. Introduzca ls para ver los detalles de la copia de seguridad en la nube.

```
hostname:configuration services cloud backup-000> ls
Properties:
    target = oci-phoenix
    source = hostname
    dataset = p1/local/default/fs-1@snap2
    format = zfs
    tier = standard
    size = 1.00T
    started = 2019-8-03 15:05:53
    uploaded = 2019-8-04 17:14:08
    id = cbb88888852e58088/445c15865cb329c3
```

Temas relacionados

- [Visualización y filtrado de copias de seguridad en la nube \(CLI\) \[188\]](#)
- [Supresión de una copia de seguridad en la nube \(CLI\) \[195\]](#)
- [“Propiedades de nube” \[203\]](#)

Gestión del servicio de nube

Para gestionar el almacenamiento en la nube, realice las siguientes tareas:

- Supresión de una copia de seguridad en la nube: [BUI](#), [CLI](#)
- Visualización de trabajos en la nube: [BUI](#), [CLI](#)
- Cancelación y reinicio de un trabajo en la nube: [BUI](#), [CLI](#)

- Modificación de un destino de nube: [BUI](#), [CLI](#)
- Supresión de un destino de nube: [BUI](#), [CLI](#)

▼ Supresión de una copia de seguridad en la nube (BUI)

Una vez que la copia de seguridad en la nube en Oracle ZFS Storage Appliance ya no sea necesaria, utilice el dispositivo para suprimirla. Tenga en cuenta que no podrá cancelar la operación de supresión de una copia de seguridad en la nube una vez que se haya iniciado.

Si en un dispositivo hay en curso una operación de restauración de una copia de seguridad en la nube y en esa operación se incluyen datos de la copia de seguridad, no podrá suprimirla a menos que confirme la acción. Si la copia de seguridad en la nube es una instantánea principal con instantáneas incrementales (secundarias) con copia de seguridad en la nube, no podrá suprimir esa copia de seguridad en la nube.

1. **Vaya a Configuración > Servicios y haga clic en Cloud.**
2. **Haga clic en la ficha Copias de seguridad.**
La lista Copias de seguridad contiene las copias de seguridad en la nube finalizadas y las muestra en orden cronológico.
3. **Busque la copia de seguridad en la nube que se suprimirá, mueva el cursor sobre ella y haga clic en el ícono de supresión .**
4. **Haga clic en Aceptar para confirmar la acción.**

Temas relacionados

- [Visualización y filtrado de copias de seguridad en la nube \(BUI\) \[187\]](#)
- [Restauración de una copia de seguridad en la nube \(BUI\) \[190\]](#)
- [“Propiedades de nube” \[203\]](#)

▼ Supresión de una copia de seguridad en la nube (CLI)

Una vez que la copia de seguridad en la nube en Oracle ZFS Storage Appliance ya no sea necesaria, utilice el dispositivo para suprimirla. Tenga en cuenta que no podrá cancelar la operación de supresión de una copia de seguridad en la nube una vez que se haya iniciado.

Si en un dispositivo hay en curso una operación de restauración de una copia de seguridad en la nube y en esa operación se incluyen datos de la copia de seguridad, no podrá suprimirla a

menos que confirme la acción. Si la copia de seguridad en la nube es una instantánea principal con instantáneas incrementales (secundarias) con copia de seguridad en la nube, no podrá suprimir esa copia de seguridad en la nube.

1. Vaya a configuration services cloud backups.

```
hostname:> configuration services cloud backups
```

2. Introduzca `ls` para ver las propiedades y las copias de seguridad en la nube.

La lista Copias de seguridad contiene las copias de seguridad en la nube finalizadas y las muestra en orden cronológico.

```
hostname:configuration services cloud backups> ls
Properties:
  total      = 68
  selected   = 68
  target     = (unset)
  format     = (unset)
  source     = (unset)
  dataset    = (unset)
Backups:
BACKUP      UPLOADED          TARGET          SOURCE          DATASET
backup-000  2019-8-04 17:14:08 oci-phoenix hostname p1/local/default/fs-1@snap2
backup 001  2019-8-04 17:25:36 oci-phoenix hostname p1/local/default/fs-1@snap31
.
.
.
```

3. Busque la copia de seguridad en la nube que se suprimirá.

4. Introduzca `destroy` y el nombre de la copia de seguridad en la nube.

```
hostname:configuration services cloud backups> destroy backup-000
This will destroy "backup-000". Are you sure? (Y/N)
```

5. Introduzca `y` para confirmar la acción.

Temas relacionados

- [Visualización y filtrado de copias de seguridad en la nube \(CLI\) \[188\]](#)
- [Restauración de una copia de seguridad en la nube \(CLI\) \[192\]](#)
- [“Propiedades de nube” \[203\]](#)

▼ Visualización de trabajos en la nube (BUI)

La lista Trabajos contiene los trabajos activos y finalizados recientemente en el servicio de datos en la nube y se muestra en orden cronológico. Puede filtrar la lista Trabajos por nombre de destino, operación y estado.

1. **Vaya a Configuración > Servicios y haga clic en Cloud.**
2. **Haga clic en la ficha Trabajos.**
 - **Ícono a la izquierda del trabajo:** un ícono de color verde indica un trabajo que se completó correctamente, mientras que un ícono de color gris indica que se produjo un error o se canceló un trabajo.
 - **Destino:** nombre del destino de nube.
 - **Actualizaciones:** la fecha y la hora en que se creó el trabajo, así como la fecha y la hora en que se inició o se actualizó la operación.
 - **Operación:** indica una operación de tipo backup, restore o delete.
 - **Estado:** indica el porcentaje de finalización, la cantidad de datos transferidos y la ratio de transferencia. Si se estableció una operación de copia de seguridad y la propiedad de límite de escritura para el destino de nube, el ancho de banda del tráfico de escritura se limita al valor establecido. Si se estableció una operación de restauración y la propiedad de límite de lectura para el destino de nube, el ancho de banda del tráfico de lectura se limita al valor establecido.
3. **Para ver los detalles del trabajo, búsquelo y haga clic en él en la lista Trabajos.**
 - **Si hay varias páginas de trabajos en la nube, use las teclas de flecha doble para navegar entre las páginas. Para ir a la primera página, haga clic en la tecla de flecha simple que apunta hacia la izquierda. Para ir a la última página, haga clic en la tecla de flecha simple que apunta hacia la derecha.**
 - **Para buscar un trabajo en la nube por nombre de destino, operación y estado, haga clic en el ícono de flecha hacia abajo ▼ que aparece debajo del ícono de búsqueda 🔍. En el cuadro de diálogo Buscar, complete los campos según corresponda y haga clic en Aplicar.**
Al finalizar, los criterios de búsqueda y los valores aparecen en el campo de búsqueda junto al ícono de búsqueda. Para volver a ver la lista completa sin filtrar, borre el campo de búsqueda y pulse Intro.
 - **Para ver una descripción de cada propiedad detallada del trabajo en la nube, consulte [“Propiedades de nube” \[203\]](#).**
 - **Cuando termine de visualizar los detalles del trabajo, haga clic en Aceptar para cerrar el cuadro de diálogo Detalles de trabajo.**

Temas relacionados

- [“Propiedades de nube” \[203\]](#)

▼ Visualización de trabajos en la nube (CLI)

La lista Trabajos contiene los trabajos activos y finalizados recientemente en el servicio de datos en la nube y se muestra en orden cronológico.

1. Vaya a `configuration services cloud jobs`.

```
hostname:configuration services cloud jobs>
```

2. Introduzca `ls` para ver los trabajos en la nube.

- **TRABAJO:** número del trabajo en la nube.
- **OPERACIÓN:** indica una operación de tipo backup, restore o delete.
- **FECHA DE CREACIÓN:** fecha y hora de creación del trabajo en la nube.

```
hostname:configuration services cloud jobs> ls
Jobs:
JOB      OPERATION  CREATED
job-000  backup     2019-8-03 15:05:53
```

3. Busque y seleccione el trabajo en la nube por número e introduzca `ls` para ver los detalles.

Valores de status: in-progress, pending y completed. Si se estableció una operación de copia de seguridad in-progress y la propiedad de límite de escritura para el destino de nube, el ancho de banda del tráfico de escritura se limita al valor establecido. Si se estableció una operación de restauración in-progress y la propiedad de límite de lectura para el destino de nube, el ancho de banda del tráfico de lectura se limita al valor establecido. Para ver una descripción de todas las propiedades detalladas del trabajo en la nube, consulte [“Propiedades de nube” \[203\]](#).

```
hostname:configuration services cloud jobs> select job-000
hostname:configuration services cloud job-000> ls
Properties:
      op = backup
      target = e641f83d-4628-42ba-8757-d66c4c98c0d9
      targetName = oci-phoenix
      created = 2019-8-03 15:05:53
      updated = 2019-8-03 22:27:33
      id = 3babb944-07f6-4b69-8de1-f6dcfeab5fb2
      status = in-progress
      format = zfs
      rate = 6MB/s
      transferred = 1.46G
      estimated_size = 40.1G
      dataset = p1/local/default/f-1
      backup = 3e035b7e546e0d02/1cbfdb5ff2259b76
      snapshot = snap9
      details = uploading backup to zfs/backups/
                3e035b7e546e0d02/1cbfdb5ff2259b76/000000001
```

Temas relacionados

- [“Propiedades de nube” \[203\]](#)

▼ Cancelación y reinicio de un trabajo en la nube (BUI)

Al cancelar un trabajo en la nube, el trabajo se detiene, pero no se suprime inmediatamente de la lista Trabajos en el dispositivo. Al reiniciar un trabajo en la nube, el trabajo se reanuda desde el comienzo. Por otro lado, tenga en cuenta que, una vez iniciada una operación de supresión de una copia de seguridad en la nube, no es posible cancelarla.

1. **Vaya a Configuración > Servicios y haga clic en Cloud.**
2. **Haga clic en la ficha Trabajos.**
La lista Trabajos contiene los trabajos activos y finalizados recientemente en el servicio de datos en la nube y se muestra en orden cronológico.
3. **Busque el trabajo que se cancelará, mueva el cursor sobre él y haga clic en el ícono de cancelación .**
4. **Haga clic en Aceptar para confirmar la acción de cancelación.**
5. **Para reiniciar un trabajo en la nube, busque el trabajo que se reiniciará, mueva el cursor sobre él y haga clic en el ícono de reinicio .**

Temas relacionados

- [Creación de una copia de seguridad en la nube \(BUI\) \[179\]](#)
- [“Propiedades de nube” \[203\]](#)

▼ Cancelación y reinicio de un trabajo en la nube (CLI)

Al cancelar un trabajo en la nube, el trabajo se detiene, pero no se suprime inmediatamente de la lista Trabajos. Al reiniciar un trabajo en la nube, el trabajo se reanuda desde el comienzo. Por otro lado, tenga en cuenta que, una vez iniciada una operación de supresión de una copia de seguridad en la nube, no es posible cancelarla.

1. **Vaya a `configuration services cloud jobs`.**
`hostname:configuration services cloud jobs>`
2. **Introduzca `ls` para ver los trabajos en la nube.**
La lista Trabajos contiene los trabajos activos y finalizados recientemente en el servicio de datos en la nube y se muestra en orden cronológico.
`hostname:configuration services cloud jobs> ls`
`Jobs:`

JOB	OPERATION	CREATED
job-000	backup	2019-8-03 15:05:53

3. **Busque y seleccione el trabajo en la nube que se cancelará.**

```
hostname:configuration services cloud jobs> select job-000
```

4. **Introduzca `cancel`.**

```
hostname:configuration services cloud job-000> cancel
```

5. **Para reiniciar un trabajo en la nube, busque y seleccione el trabajo que se reiniciará e introduzca `restart`.**

```
hostname:configuration services cloud job-000> restart
```

Temas relacionados

- [Creación de una copia de seguridad en la nube \(CLI\) \[182\]](#)
- [“Propiedades de nube” \[203\]](#)

▼ Modificación de un destino de nube (BUI)

Es posible modificar el nombre del destino de nube y la configuración del proxy web de un destino de nube.

1. **Vaya a Configuración > Servicios y haga clic en Cloud.**
2. **Haga clic en el separador Destinos.**
3. **Mueva el cursor sobre el destino de nube que se modificará y haga clic en el ícono de edición .**
4. **Introduzca valores en los campos correspondientes y haga clic en Aplicar.**
 - **Nombre** : su nombre para este destino de nube, que debe ser exclusivo para su sistema.
 - **Usar proxy web**: seleccione esta casilla de control para usar un proxy en las comunicaciones del sistema con la Web y complete los campos para el número y el nombre de puerto del host. Los campos Nombre de usuario y Contraseña son opcionales.
 - **Write limit bandwidth** (Ancho de banda de límite de escritura) (opcional): seleccione esta casilla de control para limitar el ancho de banda del tráfico de escritura al cargar una copia de seguridad de nube al destino de nube. Introduzca un valor y seleccione una unidad de medida. Por ejemplo, 5 M/s limita las escrituras en el destino de nube a 5 megabytes por segundo.
 - **Read limit bandwidth** (Ancho de banda de límite de lectura) (opcional): seleccione esta casilla de control para limitar el ancho de banda del tráfico de lectura al restaurar una copia

de seguridad de nube del destino de nube. Introduzca un valor y seleccione una unidad de medida. Por ejemplo, 4 M/s limita las lecturas del destino de nube a 4 megabytes por segundo.

Temas relacionados

- [Definición de un destino de nube \(BUI\) \[176\]](#)
- [Supresión de un destino de nube \(BUI\) \[202\]](#)
- [“Propiedades de nube” \[203\]](#)

▼ Modificación de un destino de nube (CLI)

Es posible modificar el nombre del destino de nube y la configuración del proxy web de un destino de nube.

1. **Vaya a configuration services cloud targets.**

```
hostname:configuration services cloud targets>
```

2. **Busque y seleccione el destino de nube que se modificará e introduzca `get` para ver las propiedades.**

```
hostname:configuration services cloud target-000> get
Properties:
    name = oci-phoenix
    location = https://objectstorage.us-phoenix-1.oraclecloud.com
    user = ocid1.user.oc1..aaa56chx6rcm53g4tij74pymqffm4gsxlrhnq
    bucket = test
    tenancy = ocid1.tenancy.oc1..aaaaa06lmlzrvmk2x3uv7cg1gxpan5ldsmq
    key = true
    proxy_on = true
    proxy_host = www-proxy.us.example.com:80
    proxy_user =
    proxy_password =
    online = true
    id = 77e3a201-b4e0-4a2c-9f9d-ae21eda9954
```

3. **Para modificar las propiedades, use el comando `set`, por ejemplo, `set name=oci-phoenix-test`. Se pueden modificar las siguientes propiedades:**

- **nombre:** su nombre para este destino de nube, que debe ser exclusivo para su sistema.
- **proxy_on:** establézcalo en `true` para usar un proxy en las comunicaciones del sistema con la Web y complete la propiedad de `proxy_host` (número y nombre de puerto del host). Las propiedades `proxy_user` (nombre de usuario) y `proxy_password` (contraseña del usuario) son opcionales. Ejemplo de `proxy_host`: `www-proxy.us.ejemplo.com:80`.
- **writelimit** (opcional): establezca esto en un valor y una unidad de medida para limitar el ancho de banda del tráfico de escritura al cargar una copia de seguridad de nube al destino

de nube. Por ejemplo, 5 M/s limita las escrituras en el destino de nube a 5 megabytes por segundo.

- **readlimit** (opcional): establezca esto en un valor y una unidad de medida para limitar el ancho de banda del tráfico de lectura al restaurar una copia de seguridad de nube del destino de nube. Por ejemplo, 4 M/s limita las lecturas del destino de nube a 4 megabytes por segundo.

4. Al finalizar, introduzca `commit`.

```
hostname:configuration services cloud target-000 (uncommitted)> commit
```

Temas relacionados

- [Definición de un destino de nube \(CLI\) \[177\]](#)
- [Supresión de un destino de nube \(CLI\) \[203\]](#)
- [“Propiedades de nube” \[203\]](#)

▼ Supresión de un destino de nube (BUI)

Una vez que el destino de nube ya no sea necesario, utilice Oracle ZFS Storage Appliance para suprimirlo. Al suprimir un destino de nube, no se destruyen ni su cubo ni los objetos de la cuenta Infraestructura de nube de Oracle. Tenga en cuenta que, una vez iniciada una operación de supresión de un destino de nube, no es posible cancelarla.

Si se configuró una instantánea para usar el destino de nube, aparece una advertencia. Puede confirmar la acción de supresión del destino de nube, o bien puede cancelar la acción y abortar los trabajos enviados al destino de nube. Por razones informativas, las instantáneas que ya se hayan incluido en una copia de seguridad mostrarán el destino de nube suprimido como destino de la copia de seguridad.

Si más adelante se crea un nuevo destino de nube que apunta a la misma ubicación, tendrá una nueva identificación. Por lo tanto, todas las acciones en la nube, como las operaciones de restauración y copia de seguridad, deberán volver a crearse para el nuevo destino de nube.

1. **Vaya a Configuración > Servicios y haga clic en Cloud.**
2. **Haga clic en el separador Destinos.**
3. **Mueva el cursor sobre el destino de nube que se suprimirá y haga clic en el ícono de la papelera .**
4. **Haga clic en Aceptar para confirmar la acción.**

Temas relacionados

- [Modificación de un destino de nube \(BUI\) \[200\]](#)
- [“Propiedades de nube” \[203\]](#)

▼ Supresión de un destino de nube (CLI)

Una vez que el destino de nube ya no sea necesario, utilice Oracle ZFS Storage Appliance para suprimirlo. Al suprimir un destino de nube, no se destruyen ni su cubo ni los objetos de la cuenta Infraestructura de nube de Oracle. Tenga en cuenta que, una vez iniciada una operación de supresión de un destino de nube, no es posible cancelarla.

Si se configuró una instantánea para usar el destino de nube, aparece una advertencia. Puede confirmar la acción de supresión del destino de nube, o bien puede cancelar la acción y abortar los trabajos enviados al destino de nube. Por razones informativas, las instantáneas que ya se hayan incluido en una copia de seguridad mostrarán el destino de nube suprimido como destino de la copia de seguridad.

Si más adelante se crea un nuevo destino de nube que apunta a la misma ubicación, tendrá una nueva identificación. Por lo tanto, todas las acciones en la nube, como las operaciones de restauración y copia de seguridad, deberán volver a crearse para el nuevo destino de nube.

1. Vaya a `configuration services cloud targets`.

```
hostname:configuration services cloud targets>
```

2. Busque el destino de nube que se suprimirá.

3. Introduzca `destroy` y el nombre del destino de nube.

```
hostname:configuration services cloud targets> destroy target-000
This will destroy "target-000". Are you sure? (Y/N)
```

4. Introduzca `y` para confirmar la acción.

Temas relacionados

- [Modificación de un destino de nube \(CLI\) \[201\]](#)
- [“Propiedades de nube” \[203\]](#)

Propiedades de nube

Las propiedades de nube se agrupan en las siguientes categorías:

- [Propiedades del servicio de datos en la nube](#)
- [Propiedades del destino de nube](#)
- [Propiedades del trabajo en la nube](#)
- [Propiedades de la copia de seguridad en la nube](#)
- [Propiedades de restauración de la copia de seguridad en la nube](#)

Las propiedades del servicio de datos en la nube se utilizan al configurar dicho servicio.

TABLA 22 Propiedades del servicio de datos en la nube

Nombre del campo de la BUI	Nombre de la CLI	Descripción
ícono de estado verde	status = online	Indica que el servicio de datos en la nube está en línea.
ícono de estado gris	status = offline	Indica que el servicio de datos en la nube está fuera de línea.
Cifrados y versiones de SSL/TLS	tls_version	Para la BUI, seleccione o borre las casillas de control para las versiones de SSL/TLS. Para la CLI, establezca valores específicos para la propiedad, separados por comas. Use la finalización con tabulación para ver una lista de posibles valores.
	ciphers	Para la BUI, seleccione o borre las casillas de control para los cifrados. Para la CLI, establezca valores específicos para la propiedad, separados por comas. Use la finalización con tabulación para ver una lista de posibles valores.

Las propiedades del destino de nube se utilizan al definir o modificar un destino de nube.

TABLA 23 Propiedades del destino de nube

Nombre del campo de la BUI	Nombre de la CLI	Descripción
Nombre	name	Nombre del destino de nube; debe ser exclusivo para el sistema. Esta propiedad se puede modificar una vez definido el destino de nube.
Ubicación	location	Ubicación del destino de nube, que es una URL de punto final de API regional. Consulte también “Configuración de su cuenta Infraestructura de nube de Oracle” [173] .
Usuario	user	Oracle Cloud Identifier (OCID) del nombre de usuario. Consulte también “Configuración de su cuenta Infraestructura de nube de Oracle” [173] .
Usar el cubo de datos	databucket_on	Indica si sus datos y metadatos se encuentran en diferentes cubos. Los datos se guardarán en data_bucket, mientras que los metadatos se guardarán en bucket. Si utiliza un cubo de archivos, los metadatos deben guardarse en un cubo estándar. Para la BUI, seleccione o borre la casilla de control asociada. Para la CLI, establezca la propiedad en true o false.
Cubo	bucket	El nombre de cubo establecido. La combinación de location, bucket y data_bucket debe ser exclusiva para su sistema. Si en la BUI seleccionó use_data_bucket o si en la CLI estableció databucket_on en true, esta propiedad corresponde al cubo de metadatos. Si en

Nombre del campo de la BUI	Nombre de la CLI	Descripción
		la BUI no seleccionó <code>Use data bucket</code> o si en la CLI estableció <code>databucket_on</code> en <code>false</code> , esta propiedad corresponde a los datos y metadatos.
Cubo de datos	<code>data_bucket</code>	El nombre de cubo establecido. La combinación de <code>location</code> , <code>bucket</code> y <code>data_bucket</code> debe ser exclusiva para su sistema. Si en la BUI seleccionó <code>Use data bucket</code> o si en la CLI estableció <code>databucket_on</code> en <code>true</code> , esta propiedad corresponde al cubo de datos. Si en la BUI no seleccionó <code>Use data bucket</code> o si en la CLI estableció <code>databucket_on</code> en <code>false</code> , esta propiedad no se puede establecer.
Arrendamiento	<code>tenancy</code>	OCID del arrendamiento. Consulte también “Configuración de su cuenta Infraestructura de nube de Oracle” [173] .
Clave privada	<code>key</code>	Claves privadas del dispositivo. Consulte también “Configuración de su cuenta Infraestructura de nube de Oracle” [173] .
Use proxy web	<code>proxy_on</code>	Indica si se utiliza un proxy para las comunicaciones del sistema con la Web. Para la BUI, seleccione o borre la casilla de control asociada. Para la CLI, establezca la propiedad en <code>true</code> o <code>false</code> . Esta propiedad se puede modificar una vez definido el destino de nube.
Host: puerto	<code>proxy_host</code>	Nombre de host y número de puerto del proxy web. Esta propiedad se puede modificar una vez definido el destino de nube.
Nombre de usuario	<code>proxy_user</code>	Nombre de usuario necesario para acceder al proxy web. Esta propiedad se puede modificar una vez definido el destino de nube.
Contraseña	<code>proxy_password</code>	Contraseña necesaria para acceder al proxy web. Esta propiedad se puede modificar una vez definido el destino de nube.
ícono de estado verde	<code>online = true</code>	Indica que el destino de nube está en línea y disponible.
Ancho de banda de límite de escritura	<code>writelimit</code>	Valor y unidad de medida para limitar el ancho de banda del tráfico de escritura al cargar una copia de seguridad de nube al destino de nube. Unidades de medida: ■ B/s para bytes por segundo ■ K/s para kilobytes por segundo ■ M/s para megabytes por segundo ■ G/s para gigabytes por segundo
Ancho de banda de límite de lectura	<code>readlimit</code>	Valor y unidad de medida para limitar el ancho de banda del tráfico de lectura al restaurar una copia de seguridad de nube del destino de nube. Unidades de medida: ■ B/s para bytes por segundo ■ K/s para kilobytes por segundo ■ M/s para megabytes por segundo ■ G/s para gigabytes por segundo
ícono de estado gris	<code>online = false</code>	Indica que el destino de nube está fuera de línea y no está disponible.
	<code>id</code>	Identificación del destino de nube.

Las propiedades del trabajo en la nube se utilizan al visualizar un trabajo en la nube.

TABLA 24 Propiedades del trabajo en la nube

Nombre del campo de la BUI	Nombre de la CLI	Descripción
Operación	op	Tipo de operación: backup, delete o restore.
	target	Identificación del destino de nube.
Destino	targetName	Nombre del destino de nube.
Actualizaciones	created	Fecha y hora de creación del trabajo en la nube.
	updated	Fecha y hora de actualización del trabajo en la nube.
	id	Identificación del trabajo en la nube.
Formato	format	Formato de la copia de seguridad en la nube: zfs (por defecto) o tar.
Estado	status	Estado del trabajo en la nube: in-progress, pending, completed o error.
	rate	Velocidad de la transferencia de datos, expresada en una unidad de medida por segundo (consulte "Cantidad de datos transferidos").
	transferred y estimated_size	Cantidad de datos transferidos y tamaño estimado. Si el trabajo está en curso, la BUI muestra el porcentaje de datos transferidos y el tamaño estimado; en la CLI, las propiedades transferred y estimated_size pueden usarse para calcular el porcentaje. Unidades de medida: ■ B para bytes ■ K para kilobytes ■ M para megabytes ■ G para gigabytes ■ T para terabytes ■ P para petabytes ■ E para exabytes
	dataset	Juego de datos. Se define como <i>pool name/local/project name/share name</i> .
	backup	Identificación de la copia de seguridad en la nube. Ejemplo: 3e035b7e546e0d02 / db7fd6c5558cea0
	snapshot	Nombre de la instantánea.
	details	Detalles del trabajo en la nube, como el estado de la copia de seguridad en la nube, el nombre de cubo, el formato de la copia de seguridad en la nube y la identificación de la copia de seguridad. Ejemplo: uploading backup to zfs / backups / zfs / 3e035b7e546e0d02 / db7fd6c5558cea0 / 000000001

Las propiedades de la copia de seguridad en la nube se utilizan al crear o visualizar una copia de seguridad en la nube.

TABLA 25 Propiedades de la copia de seguridad en la nube

Nombre del campo de la BUI	Nombre de la CLI	Descripción
Destino	target	Nombre del destino de nube.
Origen	source	Sistema de origen de la copia de seguridad en la nube.
Juego de datos	dataset	Juego de datos. Se define como <i>pool name/local/project name/share name@snapshot name</i> .
Formato	format	Formato de la copia de seguridad en la nube: <i>zfs</i> (por defecto) o <i>tar</i> .
Capa de almacenamiento	tier	Tipo de capa de almacenamiento: estándar o de archivos.
Size (Tamaño)	size	Tamaño de la copia de seguridad en la nube. Unidades de medida: ■ b para bytes ■ k para kilobytes ■ m para megabytes ■ g para gigabytes ■ t para terabytes ■ p para petabytes ■ e para exabytes
Inicio	started	Fecha y hora de inicio de la copia de seguridad en la nube.
Carga	uploaded	Fecha y hora de inicio de carga de la copia de seguridad en la nube.
	id	Identificación de la copia de seguridad en la nube. Ejemplo: 3e035b7e546e0d02 / db7fd6c55558cea0
Principal	parent	Instantánea principal para una instantánea incremental. Esta propiedad se muestra solo al seleccionar una instantánea incremental.

Las propiedades de restauración de una copia de seguridad en la nube se usan al restaurar una copia de seguridad en la nube en Oracle ZFS Storage Appliance.

Después de restaurar una copia de seguridad en la nube con formato *tar* en Oracle ZFS Storage Appliance, establezca las propiedades del sistema de archivos, ya que este tipo de copia de seguridad no conserva las propiedades originales del sistema de archivos ni hereda las propiedades del proyecto.

TABLA 26 Propiedades de restauración de la copia de seguridad en la nube

Nombre del campo de la BUI	Nombre de la CLI	Descripción
Agrupación	pool	Nombre de agrupación local para la restauración de la copia de seguridad en la nube.
Proyecto	project	Nombre del proyecto local para la restauración de la copia de seguridad en la nube.
Recurso compartido	share	Nombre de recurso compartido local para la restauración de la copia de seguridad en la nube.

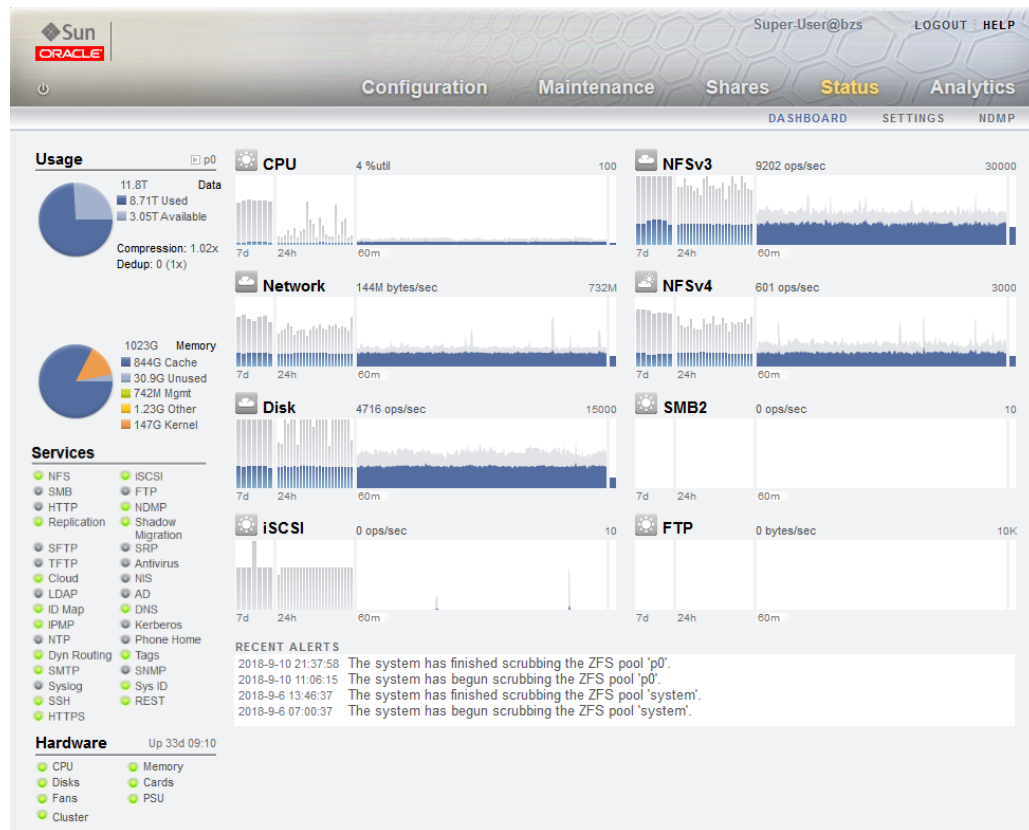
Descripción del estado del dispositivo

La sección Estado proporciona un resumen del estado del dispositivo y las opciones de configuración. Use las siguientes secciones para obtener información de conceptos y procedimientos sobre las vistas del estado del dispositivo y la configuración de servicio relacionada:

- [Acerca de Oracle ZFS Storage Appliance \[19\]](#)
- [“Panel de control de estado” \[208\]](#)
- [“Resumen de uso de agrupación” \[214\]](#)
- [“Resumen de uso de memoria” \[215\]](#)
- [“Panel de control de actividad de disco” \[215\]](#)
- [“Panel de control de la CLI” \[217\]](#)
- [Ejecución continua del panel de control \[219\]](#)
- [“Configuración del panel de control de estado” \[219\]](#)
- [Modificación de las estadísticas de las actividades desplegadas \[221\]](#)
- [Modificación de los umbrales de las actividades \[222\]](#)
- [“Estado de NDMP” \[222\]](#)
- [“Estados de NDMP” \[224\]](#)

Panel de control de estado

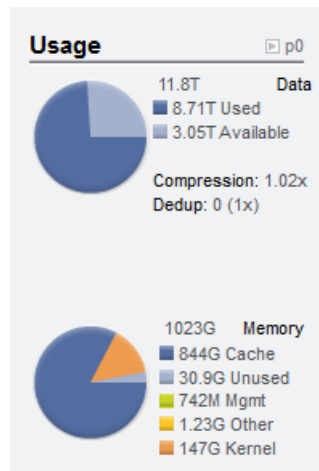
El panel de control resume el estado del dispositivo.



El panel de control de estado proporciona enlaces a todas las pantallas principales de la interfaz de usuario basada en explorador (BUI). En el panel de control, hay más de 100 elementos visibles que se enlazan a pantallas de la BUI asociadas; estos están indicados mediante texto más grueso o resaltado que aparece al pasar el cursor por encima. En las siguientes secciones, se describen detalladamente las áreas del panel de control.

Panel de control de uso

El área de uso del panel de control proporciona un resumen del uso de la agrupación de almacenamiento y la memoria principal. El nombre de la agrupación aparece en la parte superior derecha del área Uso. Si hay varias agrupaciones configuradas, use la lista desplegable para seleccionar la agrupación que desea visualizar.

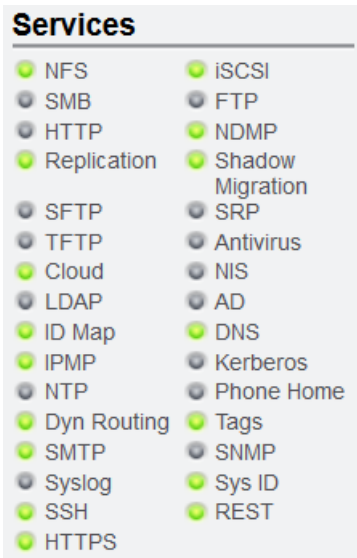


La capacidad total de la agrupación se muestra a la derecha del gráfico circular de uso de almacenamiento. En el gráfico circular de almacenamiento, se detalla el espacio utilizado y el espacio disponible. Para ir a la pantalla Recursos compartidos de la agrupación, haga clic en el gráfico circular de almacenamiento.

La memoria física total del sistema se muestra a la derecha del gráfico circular de memoria. A la izquierda hay un gráfico circular que muestra el uso de memoria por componente. Para ir a la hoja de trabajo de análisis para el uso de memoria dinámica detallado por nombre de aplicación, haga clic en el gráfico circular de memoria.

Panel de control de servicios

El área de servicios del panel de control muestra el estado de los servicios en el dispositivo, con un ícono de luz para indicar el estado de cada servicio.



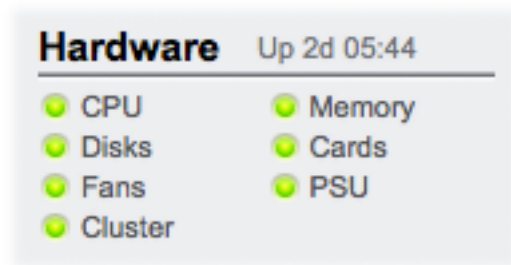
La mayoría de los servicios aparecen en verde, para indicar que el servicio está en línea, o en gris, para indicar que el servicio está desactivado. Para obtener una referencia de todos los estados y colores de íconos posibles, consulte [“Interfaz de usuario basada en explorador \(BUI\)” \[23\]](#).

Para ir a la pantalla de configuración asociada, haga clic en el nombre del servicio. La pantalla Propiedades aparece con campos que se pueden configurar, íconos de reinicio, activación y desactivación y un enlace a la pantalla Logs asociada del servicio.

Panel de control de hardware

El área de hardware del panel de control muestra una visión general del hardware del dispositivo.

FIGURA 10 Panel de control de hardware



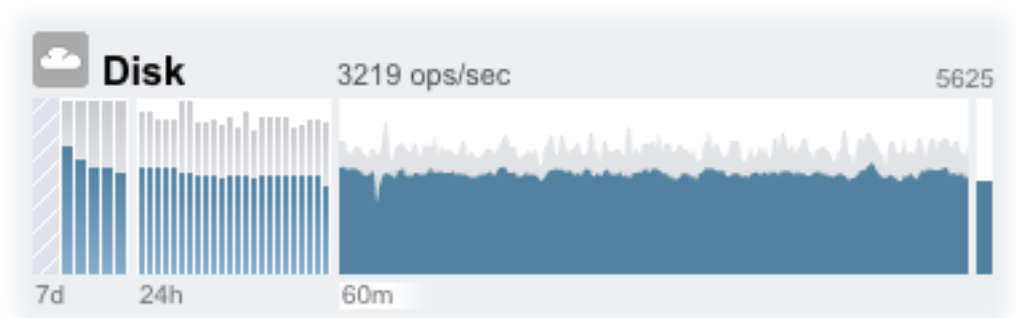
Si hay un fallo conocido, aparece el ícono de fallo de color ámbar 🟡.

Para ir a la pantalla Hardware, en donde se proporciona información detallada del estado del hardware, haga clic en el nombre del componente de hardware.

Panel de control de actividad

Por defecto, el área de actividad del panel de control muestra gráficos de ocho estadísticas de rendimiento. En el ejemplo de esta sección, se muestran las operaciones de disco por segundo. El promedio estadístico se representa en azul, mientras que el máximo aparece en gris claro.

FIGURA 11 Panel de control de actividad de disco



Para ir a la hoja de trabajo de Análisis de una actividad, haga clic en uno de los cuatro gráficos (día, hora, minuto, segundo) de la estadística que desea evaluar.

Para ver el promedio de cada gráfico, pase el puntero del mouse sobre el gráfico y aparecerá un texto que indica cuál es el promedio. El ícono de clima que aparece en la parte superior izquierda proporciona un informe de la actividad en función de los umbrales que puede personalizar para cada estadística en la pantalla [“Configuración del panel de control de estado” \[219\]](#).

TABLA 27 Resumen de gráficos de estadísticas

Resumen de gráficos de estadísticas	
Gráfico de 7 días (7d)	Gráfico de barras; cada barra representa un día.
Gráfico de 24 horas (24h)	Gráfico de barras; cada barra representa una hora.
Gráfico de 60 minutos (60m)	Línea que representa la actividad en el transcurso de una hora (también se puede visualizar como la primera barra de una hora del gráfico de 24 horas).
Gráfico de 1 segundo	Línea que representa un informe instantáneo de la actividad.

El promedio del gráfico seleccionado se muestra numéricamente encima del gráfico. Para cambiar el promedio que aparece, seleccione el promedio deseado, que puede ser 7d, 24h o 60m.

La escala vertical de todos los gráficos se muestra en la parte superior derecha; todos los gráficos se representan con una escala de esta misma altura. La altura se calcula a partir del gráfico seleccionado (más un margen). La escala de la altura se cambia en función de la actividad del gráfico seleccionado, con excepción de los gráficos de uso, que tienen una altura fija del 100%.

Como la escala de la altura puede cambiar, puede suceder que 60 minutos de inactividad se vean similares a 60 minutos de mucha actividad. Compruebe siempre la altura de los gráficos antes de intentar interpretar su significado.

La comprensión de algunas estadísticas puede no ser obvia: por ejemplo, para un dispositivo en particular del entorno, puede preguntarse si 1000 NFSv3 operaciones/s se considera como un estado activo o inactivo. Los gráficos de 24 horas y 7 días resultan útiles en estos casos porque proporcionan datos históricos junto a la actividad actual para fines de comparación.

La altura del gráfico se calcula a partir del gráfico seleccionado. Por defecto, se selecciona el gráfico de 60 minutos. Por lo tanto, la altura es la actividad máxima durante ese intervalo de 60 minutos (más un margen). Para cambiar la escala de todos los gráficos a fin de abarcar la actividad más elevada durante los 7 días previos, seleccione 7d. Esto facilita la comparación visual de la actividad actual con la del último día o la última semana.

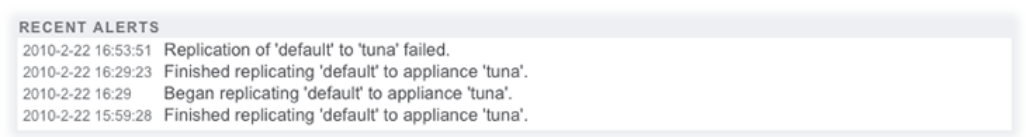
El ícono de clima tiene por objetivo llamar la atención del usuario cuando hay algo que presenta actividad o inactividad inusual. Para ir a la página de configuración de los umbrales de clima, haga clic en el ícono de clima. No hay umbrales buenos ni malos, más bien la BUI proporciona un gradiente de niveles para cada estadística de actividad. Las estadísticas sobre las que se basan los íconos de clima proporcionan información *aproximada* sobre el rendimiento del dispositivo que se debe personalizar para la carga de trabajo, de la siguiente manera:

- Los diferentes entornos tienen diferentes niveles aceptables de rendimiento (latencia), de manera que no hay un único umbral que sea adecuado para todas las situaciones.
- Las estadísticas del panel de control se basan en la cantidad de operaciones/segundo y los bytes/segundo, de manera que es necesario usar hojas de trabajo de Análisis para interpretar correctamente la información sobre el rendimiento del sistema.

Alertas recientes

En esta sección, se muestran las últimas cuatro alertas del dispositivo. Haga clic en el cuadro para ir a la pantalla Logs para examinar en detalle todas las alertas recientes.

FIGURA 12 Alertas recientes



Resumen de uso de agrupación

En la siguiente tabla, se describen las propiedades de uso de la agrupación.

TABLA 28 Resumen de uso de agrupación

Resumen de uso de agrupación	
Usado	Espacio usado por esta agrupación, incluidos los datos, las instantáneas y la primera copia de los datos deduplicados, si corresponde.
Disponible	Cantidad de espacio en disco restante disponible para el usuario.

Resumen de uso de agrupación	
	Hace referencia a la cantidad de espacio disponible; se excluye el espacio sin usar reservado para proyectos y recursos compartidos de una agrupación.
Compresión	Índice de compresión actual de esta agrupación. Si se desactiva la compresión, el índice es x 1.
Eliminar entradas duplicadas	Tamaño actual de datos cuya duplicación se anuló en esta agrupación, con el ratio de deduplicación entre paréntesis. Si se desactiva la deduplicación, el tamaño es 0 y el ratio es (x1).

Resumen de uso de memoria

En la siguiente tabla, se describen las propiedades de uso de memoria.

TABLA 29 Resumen de uso de memoria principal

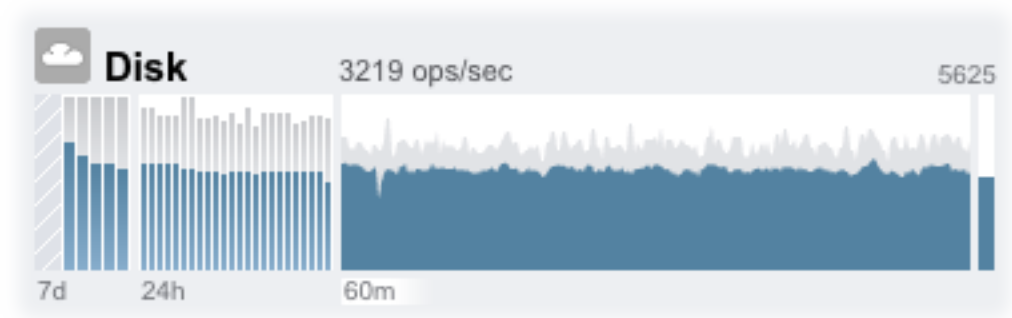
Resumen de uso de la memoria principal (RAM)	
Caché	Bytes en uso por la caché del sistema de archivos para mejorar el rendimiento.
Sin utilizar	Bytes que actualmente no están en uso. Después del inicio, este valor disminuye porque la caché del sistema de archivos utiliza espacio.
Gestión	Bytes en uso por el software de gestión del dispositivo.
Otros	Bytes en uso por otro software del sistema operativo.
Núcleo	Bytes en uso por el núcleo del sistema operativo.

Tenga en cuenta que los usuarios necesitan la autorización `analytics/component create+read` para poder ver el uso de la memoria. Sin esta autorización, los detalles de la memoria no aparecen en el panel de control.

Panel de control de actividad de disco

Por defecto, el área de actividad del panel de control muestra gráficos de ocho estadísticas de rendimiento. En el ejemplo de esta sección, se muestran las operaciones de disco por segundo. El promedio estadístico se representa en azul, mientras que el máximo aparece en gris claro.

FIGURA 13 Panel de control de actividad de disco



Para ir a la hoja de trabajo de Análisis de una actividad, haga clic en uno de los cuatro gráficos (día, hora, minuto, segundo) de la estadística que desea evaluar.

Para ver el promedio de cada gráfico, pase el puntero del mouse sobre el gráfico y aparecerá un texto que indica cuál es el promedio. El ícono de clima que aparece arriba a la izquierda proporciona un informe de la actividad en función de los umbrales que puede personalizar para cada estadística en la pantalla Configuración de estado.

TABLA 30 Resumen de gráficos de estadísticas

Resumen de gráficos de estadísticas	
Gráfico de 7 días (7d)	Gráfico de barras; cada barra representa un día.
Gráfico de 24 horas (24h)	Gráfico de barras; cada barra representa una hora.
Gráfico de 60 minutos (60m)	Línea que representa la actividad en el transcurso de una hora (también se puede visualizar como la primera barra de una hora del gráfico de 24 horas).
Gráfico de 1 segundo	Línea que representa un informe instantáneo de la actividad.

El promedio del gráfico seleccionado se muestra numéricamente encima del gráfico. Para cambiar el promedio que aparece, seleccione el promedio deseado, que puede ser 7d, 24h o 60m.

La escala vertical de todos los gráficos se muestra en la parte superior derecha; todos los gráficos se representan con una escala de esta misma altura. La altura se calcula a partir del

gráfico seleccionado (más un margen). La escala de la altura se cambia en función de la actividad del gráfico seleccionado, con excepción de los gráficos de uso, que tienen una altura fija del 100%.

Como la escala de la altura puede cambiar, puede suceder que 60 minutos de inactividad se vean similares a 60 minutos de mucha actividad. Compruebe siempre la altura de los gráficos antes de intentar interpretar su significado.

La comprensión de algunas estadísticas puede no ser obvia: por ejemplo, para un dispositivo en particular del entorno, puede preguntarse si 1000 NFSv3 operaciones/s se considera como un estado activo o inactivo. Los gráficos de 24 horas y 7 días resultan útiles en estos casos porque proporcionan datos históricos junto a la actividad actual para fines de comparación.

La altura del gráfico se calcula a partir del gráfico seleccionado. Por defecto, se selecciona el gráfico de 60 minutos. Por lo tanto, la altura es la actividad máxima durante ese intervalo de 60 minutos (más un margen). Para cambiar la escala de todos los gráficos a fin de abarcar la actividad más elevada durante los 7 días previos, seleccione 7d. Esto facilita la comparación visual de la actividad actual con la del último día o la última semana.

El ícono de clima tiene por objetivo llamar la atención del usuario cuando hay algo que presenta actividad o inactividad inusual. Para ir a la página de configuración de los umbrales de clima, haga clic en el ícono de clima. No hay umbrales buenos ni malos, más bien la BUI proporciona un gradiente de niveles para cada estadística de actividad. Las estadísticas sobre las que se basan los íconos de clima proporcionan información *aproximada* sobre el rendimiento del dispositivo que se debe personalizar para la carga de trabajo, de la siguiente manera:

- Los diferentes entornos tienen diferentes niveles aceptables de rendimiento (latencia), de manera que no hay un único umbral que sea adecuado para todas las situaciones.
- Las estadísticas del panel de control se basan en la cantidad de operaciones/segundo y los bytes/segundo, de manera que es necesario usar hojas de trabajo de Análisis para interpretar correctamente la información sobre el rendimiento del sistema.

Panel de control de la CLI

Hay una versión de texto de la pantalla Estado > Panel de control a la que se puede acceder desde la CLI con el comando `status dashboard`:

```
hostname:> status dashboard
Data:
  pool_0:
    Used      497G bytes
    Avail     8.43T bytes
    State     online
    Compression 1x
```


▼ Ejecución continua del panel de control

Si deja la pantalla de panel de control abierta en un explorador todos los días, las 24 horas, pueden surgir problemas con la memoria del explorador. El explorador aumentará de tamaño (pérdidas de memoria) y será necesario cerrarlo y volverlo a abrir. Los exploradores administran bastante bien la memoria al navegar por diferentes sitios web (y al abrir y cerrar fichas). El problema es que la pantalla del panel de control se ejecuta constantemente y no se cierra, lo que hace que se abran y se vuelvan a abrir las imágenes de los gráficos de actividad.

Si tiene este problema al usar Firefox, desactive la caché de la memoria de la siguiente manera:

1. Abra **about:config**.
2. Filtre por **"memoria"**.
3. Configure **browser.cache.memory.enable = false**.

Configuración del panel de control de estado

La pantalla Estado > Configuración le permite personalizar el panel de control de estado, que incluye las estadísticas que aparecen y los umbrales que indican actividad mediante íconos de clima.

The screenshot shows the 'Configure Dashboard' window with the 'Layout' tab selected. On the left, there is a note: 'About: Configure the activity metrics displayed on the status dashboard. If desired, some may be configured as empty, which will reduce the network traffic required to refresh the dashboard.' The main area contains two columns of dropdown menus for selecting metrics: CPU, Network, Disk, iSCSI in the first column, and NFSv3, NFSv4, SMB2, ARC Ratio in the second column. At the top right, there are 'Layout' and 'Thresholds' tabs, and 'REVERT' and 'APPLY' buttons.

Use la ficha Diseño para seleccionar los gráficos que aparecen en el área de actividad del panel de control , como se define en la siguiente tabla.

TABLA 31 Configuración de diseño de estado

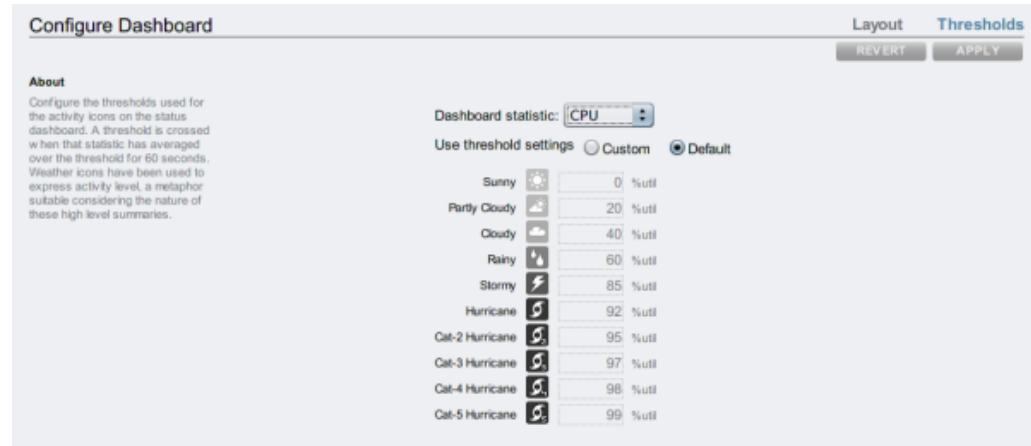
Nombre	Unidades	Descripción
<empty>	-	No se muestra ningún gráfico en esta ubicación.

Nombre	Unidades	Descripción
CPU	uso	Cantidad promedio de ciclos que las CPU del dispositivo están activas. Los ciclos de la CPU incluyen los ciclos de espera de la memoria.
Ratio de ARC	uso	Porcentaje medio de aciertos/ equivocaciones de ARC. Una caída en la tasa de aciertos indica un posible problema de rendimiento.
HTTP	operaciones por segundo	Cantidad promedio de operaciones de HTTP.
Disk	operaciones por segundo	Cantidad promedio de operaciones en los dispositivos de almacenamiento físico.
iSCSI	operaciones por segundo	Cantidad promedio de operaciones de iSCSI.
FC	operaciones por segundo	Cantidad promedio de operaciones de canal de fibra.
NDMP	bytes por segundo	Cantidad promedio de bytes de red NDMP.
NFSv2	operaciones por segundo	Cantidad promedio de operaciones de NFSv2.
NFSv3	operaciones por segundo	Cantidad promedio de operaciones de NFSv3.
NFSv4.0	operaciones por segundo	Cantidad promedio de operaciones de NFSv4.0.
NFSv4.1	operaciones por segundo	Cantidad promedio de operaciones de NFSv4.1.
Red	bytes por segundo	Cantidad promedio de bytes por segundo en todas las interfaces de red físicas.
SMB	operaciones por segundo	Cantidad promedio de operaciones de SMB.
SMB2	operaciones por segundo	Cantidad promedio de operaciones de SMB2.
SMB3	operaciones por segundo	Cantidad promedio de operaciones de SMB3.
FTP	bytes por segundo	Cantidad promedio de bytes de FTP.
SFTP	bytes por segundo	Cantidad promedio de bytes de SFTP.

Tenga en cuenta que para reducir el tráfico de red necesario para actualizar el panel de control, debe configurar algunos de los gráficos de actividad como <empty> (Vacío).

Use la pantalla Thresholds (Umbrales) para configurar los íconos de clima de la actividad del panel. Los valores predeterminados que se proporcionan se basan en cargas de trabajo intensas y tal vez no sean adecuados para su entorno.

FIGURA 14 Configuración de actividades del panel de control



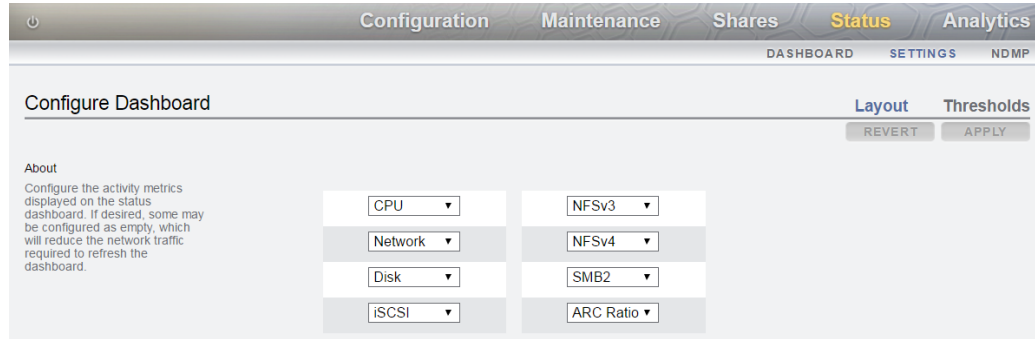
El ícono de clima que aparece en el panel de control es el más cercano a la configuración del valor de umbral para la actividad actual, medido como promedio en un período de 60 segundos. Por ejemplo, si el uso de la CPU fuera del 41%, por defecto aparecería el ícono de clima correspondiente a nublado porque el umbral es 40% (el más cercano a la actividad real). Seleccione el botón de radio Personalizados para configurar los umbrales, y asegúrese de configurarlos en el orden en el que aparecen en la pantalla.

El panel de control actualmente no se puede configurar desde la CLI. Los valores de configuración guardados en la BUI se aplican al panel de control que se visualiza desde la CLI.

▼ Modificación de las estadísticas de las actividades desplegadas

1. Vaya a la pantalla Estado > Configuración > Diseño.
2. Use los menús desplegables para elegir las estadísticas que desea desplegar en el panel de control.

3. Para guardar sus selecciones, haga clic en el botón Aplicar.



▼ Modificación de los umbrales de las actividades

1. Vaya a la pantalla Estado > Configuración > Umbrales.
2. Use el menú desplegable para elegir la estadística que desea configurar.
3. Haga clic en el botón de radio Personalizados.
4. Personalice los valores de la lista, en el orden en el que aparecen. Para algunas estadísticas hay menús desplegables con las unidades, para poder seleccionar Kilo/Mega/Giga.
5. Para guardar su configuración, haga clic en el botón Aplicar.

Estado de NDMP

Si el servicio NDMP se ha configurado y está activo, la página Estado NDMP muestra los dispositivos NDMP y la actividad reciente de los clientes. Hay un indicador verde si el dispositivo está en línea y un indicador gris si el dispositivo está sin conexión.

Para cambiar la ordenación de la lista de dispositivos NDMP, haga clic en las cabeceras de la columna Dispositivos. Para ver los detalles de un dispositivo, haga doble clic en el dispositivo.

El estado de NDMP no está disponible desde la CLI.

FIGURA 15 BUI de estado de NDMP

The screenshot shows the 'Status' tab of a BUI interface. It displays a table of NDMP devices. The table has columns for Type, Path, Vendor, Model, WWN, and Serial. There are 10 devices listed, all of which are tape drives. The 'Recent activity' section below the table shows 'No active NDMP sessions.'

TYPE	PATH	VENDOR	MODEL	WWN	SERIAL
Tape drive	/dev/rmt/14bn	STK	T1000C	50 01 04 F0 00 AC BB 27	576001000203
Tape drive	/dev/rmt/15bn	HP	Ultrium 5-SCSI	50 01 04 F0 00 79 1C 45	HU1036C6N4
Tape drive	/dev/rmt/16bn	HP	Ultrium 5-SCSI	50 01 04 F0 00 79 1C 4E	HU1036C6N2
Tape drive	/dev/rmt/17bn	HP	Ultrium 5-SCSI	50 01 04 F0 00 79 1C 51	HU1036C6MV
Tape drive	/dev/rmt/20bn	IBM	ULTRIUM-TD5	50 01 04 F0 00 79 1C 2A	1068010909
Tape drive	/dev/rmt/19bn	IBM	ULTRIUM-TD5	50 01 04 F0 00 79 1C 2D	1068011364
Tape drive	/dev/rmt/18bn	HP	Ultrium 5-SCSI	50 01 04 F0 00 AC BB 2A	HU1233PP32
Tape drive	/dev/rmt/21bn	HP	Ultrium 5-SCSI	50 01 04 F0 00 79 1C 42	HU1036C6N0
Tape drive	/dev/rmt/23bn	IBM	ULTRIUM-TD6	50 01 04 F0 00 AC BB 2D	1068000648
Tape drive	/dev/rmt/22bn	IBM	ULTRIUM-TD5	50 01 04 F0 00 AC BB 30	1068025702

TABLA 32 Estado de NDMP: dispositivos

Campo	Descripción	Ejemplos
Type	Tipo de dispositivo de NDMP.	Robot, unidad de cinta
Path	Ruta del dispositivo NDMP.	/dev/rmt/14bn
Vendor	Nombre del proveedor del dispositivo.	STK
Model	Nombre del modelo del dispositivo	T1000C
WWN	Nombre World Wide Name	50:01:04:F0:00:AC:BB:27
Serial	Número de serie del dispositivo.	576001000203

TABLA 33 Estado de NDMP: actividad reciente

Campo	Descripción	Ejemplos
ID	ID de copia de seguridad de NDMP.	49
Active	Copia de seguridad actualmente activa.	No
Remote Client	Dirección y puerto del cliente de NDMP.	192.168.1.219:4760
Authenticated	Muestra si el cliente ya completó la autenticación.	Sí, No

Campo	Descripción	Ejemplos
Data State	Ver Estado de datos.	Activo, Inactivo, ...
Mover State	Ver Estado de transferencia.	Activo, Inactivo, ...
Current Operation	Operación actual de NDMP.	Copia de seguridad, restauración, ninguno
Progress (Progreso)	Barra de progreso para esta copia de seguridad.	

Estados de NDMP

El estado de datos de NDMP muestra el estado de la operación de copia de seguridad o restauración. Los posibles valores son:

- **Active (Activo):** los datos se están grabando en la copia de seguridad o se están restaurando.
- **Idle (Inactivo):** la copia de seguridad o la restauración todavía no comenzó o ya finalizó.
- **Conectado:** se estableció la conexión, pero la copia de seguridad o la restauración todavía no comenzó.
- **Detenido:** la copia de seguridad o la restauración finalizó correctamente, generó un error o se abortó.
- **Recepción:** la operación está esperando a recibir una conexión remota.

En el estado de transferencia de NDMP se muestra el estado del subsistema de dispositivos de NDMP. Ejemplos de dispositivos de cinta:

- **Activo:** se están leyendo los datos de la cinta o se los está escribiendo en ella.
- **Inactivo:** la copia de cinta todavía no comenzó o ya finalizó.
- **En pausa:** se alcanzó el extremo de la cinta o es necesario cambiarla.
- **Halted (Detenido):** la operación de lectura/escritura finalizó correctamente, generó un error o se abortó.
- **Listen (Recepción):** la operación está esperando a recibir una conexión remota.

Configuración de una red de área de almacenamiento (SAN)

La página Configuración de SAN le permite conectar el dispositivo a una red de área de almacenamiento (SAN). Una SAN consta de tres componentes básicos:

- Un cliente que accede al almacenamiento a través de la red.
- Un dispositivo de almacenamiento que proporciona el almacenamiento mediante la red.

- Una red que enlazará al cliente con el almacenamiento.

Para configurar SAN, use las siguientes secciones:

- [Configuración de modo de los puertos FC \(BUI\)](#)
- [Detección de puertos FC \(BUI\)](#)
- [Creación de grupos de iniciadores FC \(BUI\)](#)
- [Asociación de un LUN con un grupo de iniciadores FC \(BUI\)](#)
- [Cambio de modo de los puertos FC \(CLI\)](#)
- [Detección de puertos FC \(CLI\)](#)
- [Creación de grupos de iniciadores de FC \(CLI\)](#)
- [Asociación de un LUN con un grupo de iniciadores FC \(CLI\)](#)
- [Asignación de alias a iniciadores y grupos de iniciadores mediante secuencias de comandos \(CLI\)](#)
- [Configuración de iniciadores iSCSI de SAN](#)
- [Creación de una hoja de trabajo de análisis \(BUI\)](#)
- [Agregación de un destino iSCSI con un IQN generado automáticamente \(CLI\)](#)
- [Agregación de un destino iSCSI con un IQN específico y autenticación RADIUS \(CLI\)](#)
- [Agregación de iniciador iSCSI con autenticación CHAP \(CLI\)](#)
- [Agregación de un grupo de destinos iSCSI \(CLI\)](#)
- [Agregación de un grupo de iniciadores iSCSI \(CLI\)](#)
- [Configuración de destinos SRP \(BUI\)](#)
- [Configuración de destinos SRP \(CLI\)](#)

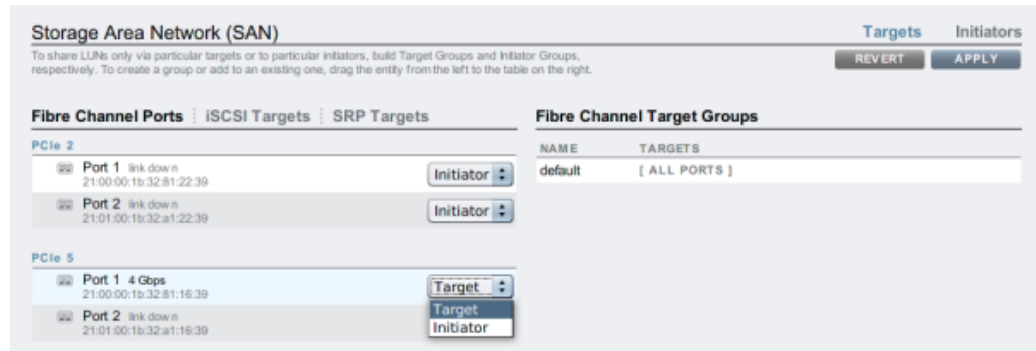
Para obtener más información sobre SAN, consulte las siguientes secciones:

- [Descripción de SAN](#)
- [Configuración de canal de fibra de SAN](#)
- [Configuración de iSCSI de SAN](#)
- [Configuración de destinos iSER de SAN](#)
- [Configuración de SRP de SAN](#)
- [Terminología de SAN](#)

▼ Configuración de modo de los puertos FC (BUI)

1. **Para usar los puertos FC, en la pantalla Configuración > SAN de la BUI, configúrelos en el modo Destino mediante el menú desplegable que se muestra**

en la siguiente imagen. Debe tener permisos de usuario `root` para realizar esta acción. Tenga en cuenta que en una configuración de cluster, los puertos de cada servidor se configuran en el modo Destino por separado.



2. Después de configurar los puertos deseados en el modo Destino, haga clic en el botón Aplicar. Aparece un mensaje de confirmación que le notifica que el dispositivo se reiniciará de inmediato. Confirme que desea reiniciarlo.
3. Cuando el dispositivo se inicia, los destinos de FC activos aparecen con el ícono , y, al pasar el puntero del mouse sobre ellos, aparece el ícono de movimiento .

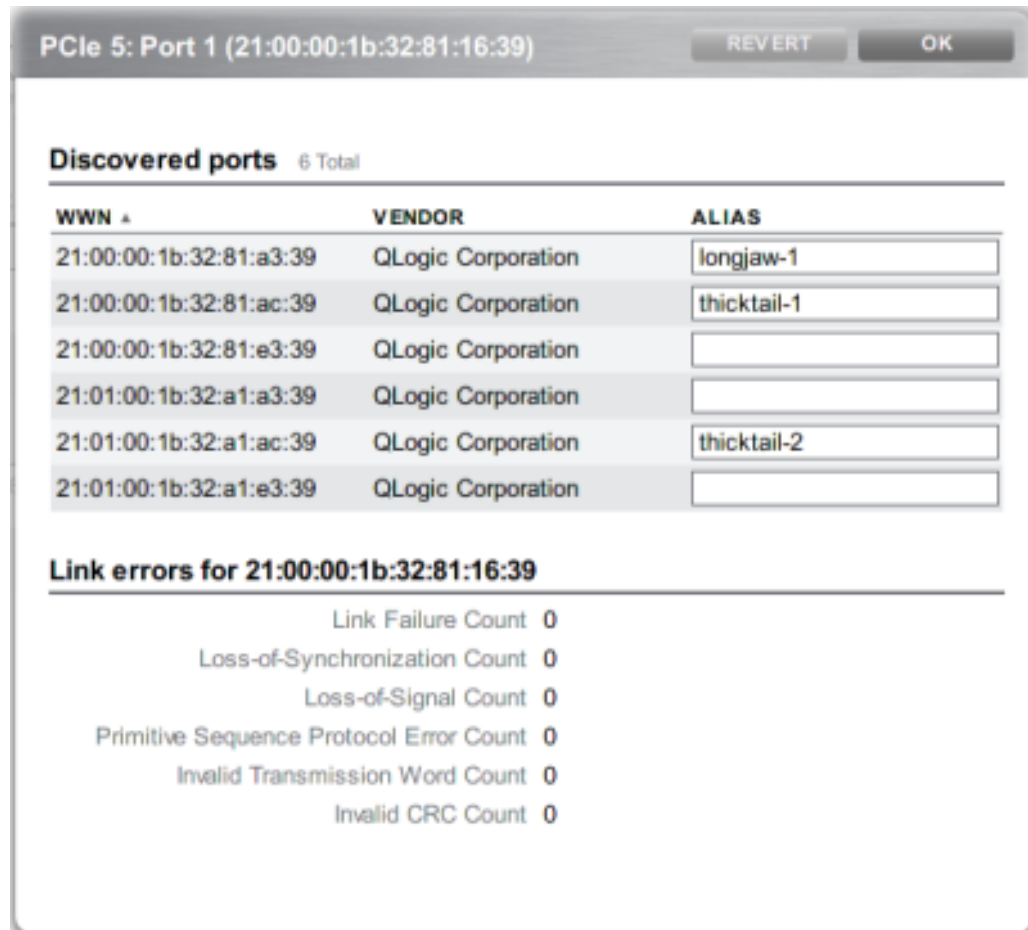
Temas relacionados

- [Descripción de SAN](#)
- [Configuración de canal de fibra de SAN](#)
- [Configuración de iSCSI de SAN](#)
- [Configuración de destinos iSER de SAN](#)
- [Configuración de SRP de SAN](#)
- [Terminología de SAN](#)

▼ Detección de puertos FC (BUI)

1. Haga clic en el ícono de información  para ver el cuadro de diálogo Puertos detectados, donde puede resolver errores de enlace. En el cuadro de diálogo

Puertos detectados, haga clic en un nombre WWN de la lista para ver los errores de enlace asociados.



- En el cuadro de diálogo Puertos detectados, haga clic en un nombre WWN de la lista para ver los errores de enlace asociados.

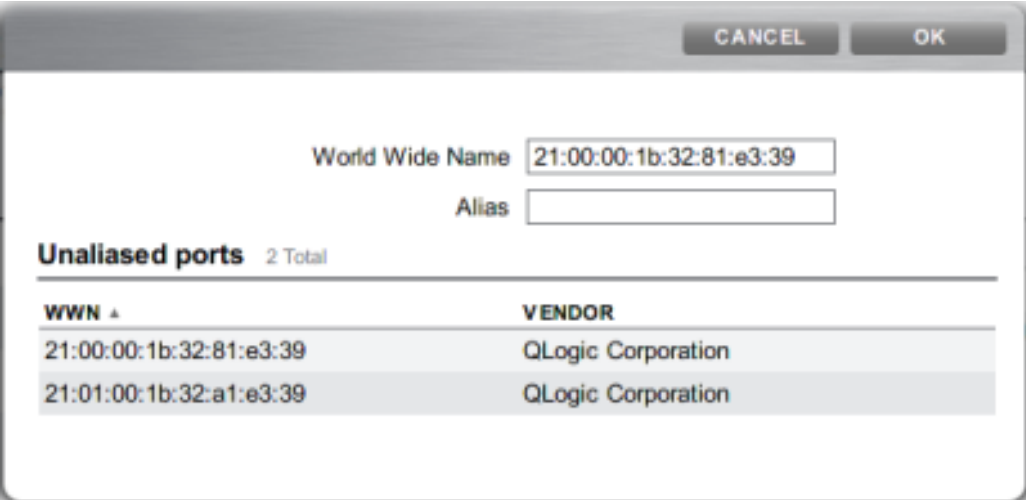
Temas relacionados

- [Descripción de SAN](#)
- [Configuración de canal de fibra de SAN](#)
- [Configuración de iSCSI de SAN](#)

- [Configuración de destinos iSER de SAN](#)
- [Configuración de SRP de SAN](#)
- [Terminología de SAN](#)

▼ Creación de grupos de iniciadores de FC (BUI)

1. Use la pantalla Iniciadores para crear y gestionar grupos de iniciadores. Haga clic en el ícono de agregación  para ver los puertos que no tienen alias. Haga clic en uno de los nombres WWN de la lista para agregar un alias relevante en el campo Alias.



WWN	VENDOR
21:00:00:1b:32:81:e3:39	QLogic Corporation
21:01:00:1b:32:a1:e3:39	QLogic Corporation

2. En la página **Initiators (Iniciadores)**, arrastre los iniciadores a la lista **Fibre Channel Initiator Groups (Grupos de iniciadores de canal de fibra)** para crear nuevos grupos o agregar iniciadores a los grupos existentes.



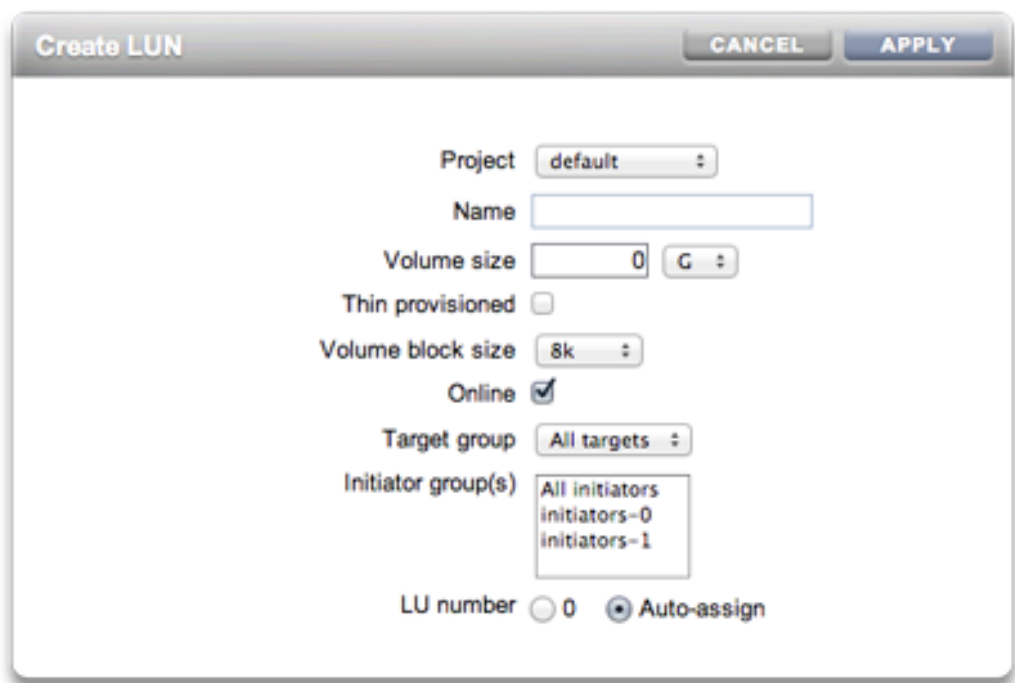
3. Haga clic en el botón **Aplicar** para confirmar el nuevo grupo de iniciadores. Ahora puede crear un LUN que tenga acceso exclusivo al grupo de iniciadores del cliente.

Temas relacionados

- [Descripción de SAN](#)
- [Configuración de canal de fibra de SAN](#)
- [Configuración de iSCSI de SAN](#)
- [Configuración de destinos iSER de SAN](#)
- [Configuración de SRP de SAN](#)
- [Terminología de SAN](#)

▼ Asociación de un LUN con un grupo de iniciadores FC (BUI)

1. Para crear el LUN, deslice el puntero del mouse sobre el grupo de iniciadores y haga clic en el ícono de agregación de LUN . Se mostrará el cuadro de diálogo Crear LUN con el grupo de iniciadores asociado seleccionado.



The image shows a 'Create LUN' dialog box with the following fields and options:

- Project:** default
- Name:** (empty text field)
- Volume size:** 0 GB
- Thin provisioned:** ☐
- Volume block size:** 8k
- Online:** ☒
- Target group:** All targets
- Initiator group(s):** A list box containing 'All initiators', 'initiators-0', and 'initiators-1'. 'All initiators' is selected.
- LU number:** ☐ 0 ☒ Auto-assign

2. Defina el nombre y el tamaño, y haga clic en Aplicar para agregar el LUN a la agrupación de almacenamiento.

Temas relacionados

- [Descripción de SAN](#)
- [Configuración de canal de fibra de SAN](#)
- [Configuración de iSCSI de SAN](#)
- [Configuración de destinos iSER de SAN](#)
- [Configuración de SRP de SAN](#)

- [Terminología de SAN](#)

▼ Cambio de modo de los puertos FC (CLI)

- Para modificar los modos de los puertos FC, use los siguientes comandos de la CLI:

```
hostname:configuration san fc targets> set targets="wwn.2101001B32A11639"
targets = wwn.2101001B32A11639 (uncommitted)
hostname:configuration san fc targets> commit
```

Temas relacionados

- [Descripción de SAN](#)
- [Configuración de canal de fibra de SAN](#)
- [Configuración de iSCSI de SAN](#)
- [Configuración de destinos iSER de SAN](#)
- [Configuración de SRP de SAN](#)
- [Terminología de SAN](#)

▼ Detección de puertos FC (CLI)

- Para descubrir los puertos FC, use los siguientes comandos de la CLI:

```
hostname:configuration san fc targets> show
Properties:
targets = wwn.2100001B32811639,wwn.2101001B32A12239

Targets:
NAME      MODE      WWN              PORT              SPEED
target-000 target    wwn.2100001B32811639  PCIe 5: Port 1    4 Gbit/s
target-001 initiator wwn.2101001B32A11639  PCIe 5: Port 2    0 Gbit/s
target-002 initiator wwn.2100001B32812239  PCIe 2: Port 1    0 Gbit/s
target-003 target    wwn.2101001B32A12239  PCIe 2: Port 2    0 Gbit/s
hostname:configuration san fc targets> select target-000
hostname:configuration san fc targets target-000> show
Properties:
wwn = wwn.2100001B32811639
port = PCIe 5: Port 1
mode = target
speed = 4 Gbit/s
discovered_ports = 6
link_failure_count = 0
loss_of_sync_count = 0
loss_of_signal_count = 0
protocol_error_count = 0
invalid_tx_word_count = 0
```

```
invalid_crc_count = 0
Ports:
PORT      WWN              ALIAS              MANUFACTURER
port-000  wwn.2100001B3281A339  longjaw-1          QLogic Corporation
port-001  wwn.2101001B32A1A339  longjaw-2          QLogic Corporation
port-002  wwn.2100001B3281AC39  thicktail-1        QLogic Corporation
port-003  wwn.2101001B32A1AC39  thicktail-2        QLogic Corporation
port-004  wwn.2100001B3281E339  <none>             QLogic Corporation
port-005  wwn.2101001B32A1E339  <none>             QLogic Corporation
```

Temas relacionados

- [Descripción de SAN](#)
- [Configuración de canal de fibra de SAN](#)
- [Configuración de iSCSI de SAN](#)
- [Configuración de destinos iSER de SAN](#)
- [Configuración de SRP de SAN](#)
- [Terminología de SAN](#)

▼ Creación de grupos de iniciadores de FC (CLI)

- **Para crear grupos de iniciadores FC, use los siguientes comandos de la CLI:**

```
hostname:configuration san fc initiators> create
hostname:configuration san fc initiators (uncommitted)> set name=lefteye
hostname:configuration san fc initiators (uncommitted)> set initiators=wwn.2101001B32A1AC39,
wwn.2100001B3281AC39
hostname:configuration san fc initiators (uncommitted)> commit
hostname:configuration san fc initiators> list
GROUP      NAME
group-001  lefteye
|
+--> INITIATORS
      wwn.2101001B32A1AC39
      wwn.2100001B3281AC39
```

Temas relacionados

- [Descripción de SAN](#)
- [Configuración de canal de fibra de SAN](#)
- [Configuración de iSCSI de SAN](#)
- [Configuración de destinos iSER de SAN](#)
- [Configuración de SRP de SAN](#)
- [Terminología de SAN](#)

▼ Asociación de un LUN con un grupo de iniciadores FC (CLI)

En el siguiente ejemplo, se muestra la creación de un LUN llamado `lefty` y su asociación con el grupo de iniciadores `fera`.

- **Para asociar un LUN con un grupo de iniciadores FC, use los siguientes comandos de la CLI:**

```
hostname:shares default> lun lefty
hostname:shares default/lefty (uncommitted)> set volsize=10
                               volsize = 10 (uncommitted)
hostname:shares default/lefty (uncommitted)> set initiatorgroup=fera
                               initiatorgroup = default (uncommitted)
hostname:shares default/lefty (uncommitted)> commit
```

Temas relacionados

- [Descripción de SAN](#)
- [Configuración de canal de fibra de SAN](#)
- [Configuración de iSCSI de SAN](#)
- [Configuración de destinos iSER de SAN](#)
- [Configuración de SRP de SAN](#)
- [Terminología de SAN](#)

▼ Asignación de alias a iniciadores y grupos de iniciadores mediante secuencias de comandos (CLI)

Consulte [Uso de la CLI](#) y [Secuencias de comandos simples de la CLI y comandos por lotes](#) para obtener información sobre cómo modificar y usar la siguiente secuencia de comandos de ejemplo.

- **Para asignar alias a iniciadores y grupos de iniciadores mediante secuencias de comandos, use los siguientes comandos de la CLI:**

```
script
/*
 * This script creates both aliases for initiators and initiator
 * groups, as specified by the below data structure. In this
 * particular example, there are five initiator groups, each of
 * which is associated with a single host (thicktail, longjaw, etc.),
 * and each initiator group consists of two initiators, each of which
 * is associated with one of the two ports on the FC HBA. (Note that
```

```

* there is nothing in the code that uses this data structure that
* assumes the number of initiators per group.)
*/
groups = {
  thicktail: {
    'thicktail-1': 'wwn.2100001b3281ac39',
    'thicktail-2': 'wwn.2101001b32a1ac39'
  },
  longjaw: {
    'longjaw-1': 'wwn.2100001b3281a339',
    'longjaw-2': 'wwn.2101001b32a1a339'
  },
  tecopa: {
    'tecopa-1': 'wwn.2100001b3281e339',
    'tecopa-2': 'wwn.2101001b32a1e339'
  },
  spinedace: {
    'spinedace-1': 'wwn.2100001b3281df39',
    'spinedace-2': 'wwn.2101001b32a1df39'
  },
  fera: {
    'fera-1': 'wwn.2100001b32817939',
    'fera-2': 'wwn.2101001b32a17939'
  }
};
for (group in groups) {
  initiators = [];
  for (initiator in groups[group]) {
    printf('Adding %s for %s ... ',
      groups[group][initiator], initiator);
    try {
      run('select alias=' + initiator);
      printf('(already exists)\n');
      run('cd ..');
    } catch (err) {
      if (err.code != EAKSH_ENTITY_BADSELECT)
        throw err;
      run('create');
      set('alias', initiator);
      set('initiator', groups[group][initiator]);
      run('commit');
      printf('done\n');
    }
    run('select alias=' + initiator);
    initiators.push(get('initiator'));
    run('cd ..');
  }
  printf('Creating group for %s ... ', group);
  run('groups');
  try {
    run('select name=' + group);
    printf('(already exists)\n');
    run('cd ..');
  } catch (err) {
    if (err.code != EAKSH_ENTITY_BADSELECT)
      throw err;
    run('create');
    set('name', group);
    run('set initiators=' + initiators);
    run('commit');
    printf('done\n');
  }
}

```

```

    }
    run('cd ..');

```

Temas relacionados

- [Descripción de SAN](#)
- [Configuración de canal de fibra de SAN](#)
- [Configuración de iSCSI de SAN](#)
- [Configuración de destinos iSER de SAN](#)
- [Configuración de SRP de SAN](#)
- [Terminología de SAN](#)

▼ Creación de una hoja de trabajo de análisis (BUI)

Para crear una hoja de trabajo de análisis que permita observar las operaciones por iniciador, realice el siguiente procedimiento:

1. **Vaya a la pantalla Análisis.**
2. **Haga clic en el ícono de agregación  a fin de agregar estadísticas. Aparece un menú de todas las estadísticas.**
3. **En la sección Protocolos del menú, seleccione Operaciones iSCSI > Desglosado por iniciador. Aparece un gráfico de las operaciones actuales por iniciador.**
4. **Para observar análisis más detallados, seleccione el iniciador del campo que se encuentra a la izquierda del gráfico y haga clic en el ícono . Aparece un menú de análisis detallados.**

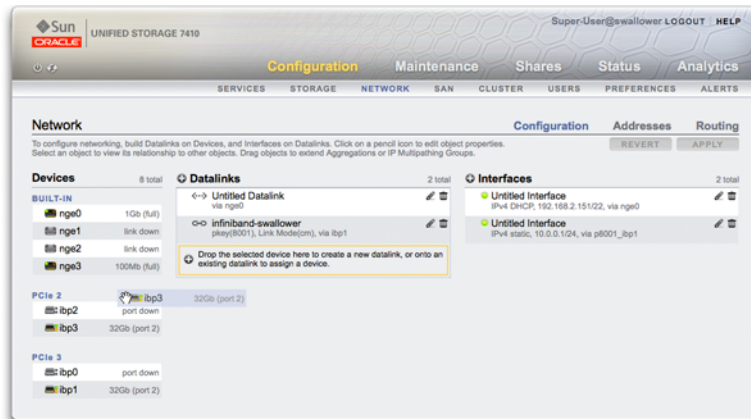
Temas relacionados

- [Descripción de SAN](#)
- [Configuración de canal de fibra de SAN](#)
- [Configuración de iSCSI de SAN](#)
- [Configuración de destinos iSER de SAN](#)
- [Configuración de SRP de SAN](#)
- [Terminología de SAN](#)

▼ Configuración de destinos iSER de SAN

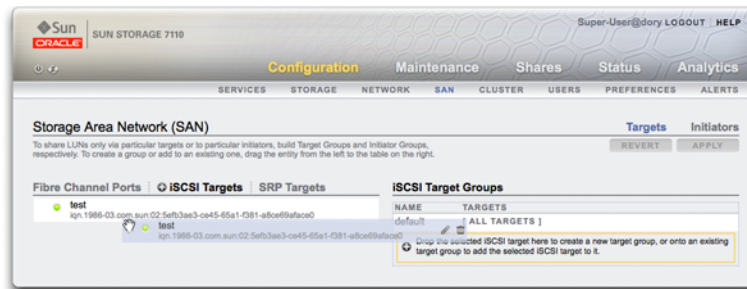
En la BUI, los destinos iSER se gestionan como destinos iSCSI en la pantalla Configuración > SAN.

1. Para configurar interfaces ibd(x), seleccione la interfaz ibd(x) (o IPMP) deseada y arrástrela hasta la lista Enlaces de datos para crear el enlace de datos en la pantalla Configuración > Red.
2. Arrastre el enlace de datos hasta la lista de interfaces para crear una nueva interfaz.

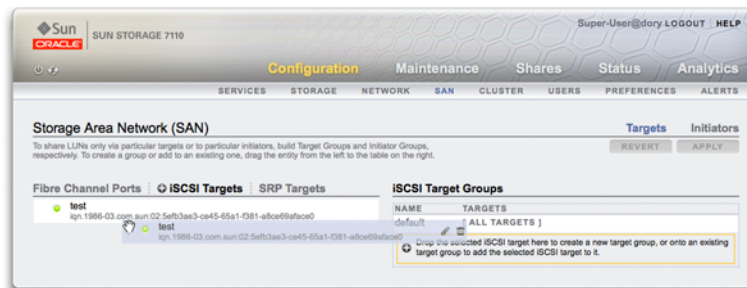


3. Para crear un destino iSER, en la página Configuración > SAN, haga clic en el enlace Destinos iSCSI.
4. Para agregar un nuevo destino iSER con un alias, haga clic en el ícono para agregar (+).

5. Para crear un grupo de destinos, arrastre el destino que acaba de crear hasta la lista Grupo de destinos iSCSI.

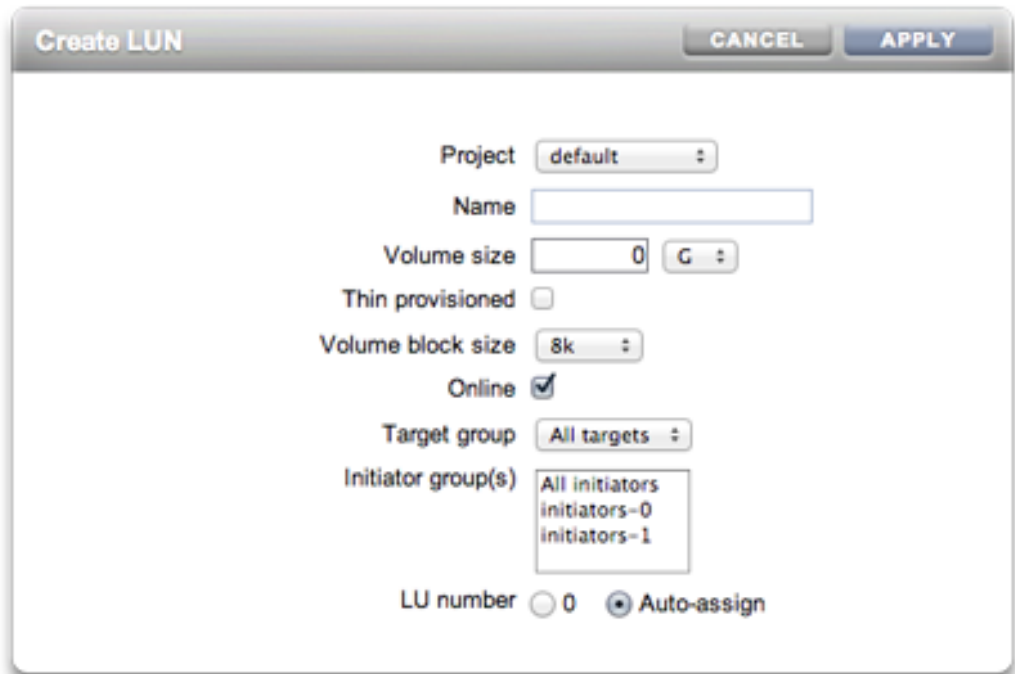


6. Para crear un iniciador, haga clic en el enlace Iniciador y, a continuación, haga clic en el enlace Iniciadores iSCSI.
7. Para agregar un nuevo iniciador, haga clic en el ícono para agregar .
8. Escriba el IQN del iniciador y un alias, y haga clic en Aceptar. La creación de un grupo de iniciadores es opcional, pero si no crea ningún grupo, el LUN asociado con el destino estará disponible para todos los iniciadores.
9. Para crear un grupo, arrastre el iniciador hasta la lista Grupos de iniciadores iSCSI.



10. Para crear un LUN, en la página Recursos compartidos, haga clic en LUN.

11. Haga clic en el ícono de agregación  y asocie el nuevo LUN con grupos de destinos o iniciadores que ya haya creado; para ello, use los menús Grupo de destinos y Grupos de iniciadores.



The image shows a 'Create LUN' dialog box with the following fields and options:

- Project:** default
- Name:** (empty text field)
- Volume size:** 0 GB
- Thin provisioned:** ☐
- Volume block size:** 8k
- Online:** ☒
- Target group:** All targets
- Initiator group(s):** All initiators, initiators-0, initiators-1
- LU number:** ☐ 0 ☒ Auto-assign

Temas relacionados

- [Descripción de SAN](#)
- [Configuración de canal de fibra de SAN](#)
- [Configuración de iSCSI de SAN](#)
- [Configuración de destinos iSER de SAN](#)
- [Configuración de SRP de SAN](#)
- [Terminología de SAN](#)

▼ Agregación de un destino iSCSI con un IQN generado automáticamente (CLI)

- Para agregar un destino iSCSI con un IQN generado automáticamente, use los siguientes comandos de la CLI:

```
hostname:configuration san iscsi targets> create
hostname:configuration san iscsi targets target (uncommitted)> set alias="Target 0"
hostname:configuration san iscsi targets target (uncommitted)> set auth=none
hostname:configuration san iscsi targets target (uncommitted)> set interfaces=igb1
hostname:configuration san iscsi targets target (uncommitted)> commit
hostname:configuration san iscsi targets> list
TARGET      ALIAS
target-000 Target 0
|
+--> IQN
      iqn.1986-03.com.sun:02:daf0161f-9f5d-e01a-b5c5-e1efa9578416
```

Temas relacionados

- [Descripción de SAN](#)
- [Configuración de canal de fibra de SAN](#)
- [Configuración de iSCSI de SAN](#)
- [Configuración de destinos iSER de SAN](#)
- [Configuración de SRP de SAN](#)
- [Terminología de SAN](#)

▼ Agregación de un destino iSCSI con un IQN específico y autenticación RADIUS (CLI)

- Para agregar un destino iSCSI con un IQN específico y autenticación RADIUS, use los siguientes comandos de la CLI:

```
hostname:configuration san iscsi targets> create
hostname:configuration san iscsi targets target (uncommitted)> set alias="Target 1"
hostname:configuration san iscsi targets target (uncommitted)> set iqn=iqn.2001-02.com.acme:12345
hostname:configuration san iscsi targets target (uncommitted)> set auth=radius
hostname:configuration san iscsi targets target (uncommitted)> set interfaces=igb1
hostname:configuration san iscsi targets target (uncommitted)> commit
hostname:configuration san iscsi targets> list
TARGET      ALIAS
target-000 Target 0
|
+--> IQN
      iqn.1986-03.com.sun:02:daf0161f-9f5d-e01a-b5c5-e1efa9578416
target-001 Target 1
```

```
|
+--> IQN
      iqn.2001-02.com.acme:12345
```

Temas relacionados

- [Descripción de SAN](#)
- [Configuración de canal de fibra de SAN](#)
- [Configuración de iSCSI de SAN](#)
- [Configuración de destinos iSER de SAN](#)
- [Configuración de SRP de SAN](#)
- [Terminología de SAN](#)

▼ Agregación de iniciador iSCSI con autenticación CHAP (CLI)

- Para agregar un iniciador iSCSI con autenticación CHAP, use los siguientes comandos de la CLI:

```
hostname:configuration san iscsi initiators> create
hostname:configuration san iscsi initiators initiator (uncommitted)> set initiator=iqn.2001-
02.com.acme:initiator12345
hostname:configuration san iscsi initiators initiator (uncommitted)> set alias="Init 0"
hostname:configuration san iscsi initiators initiator (uncommitted)> set
  chapuser=thisismychapuser
hostname:configuration san iscsi initiators initiator (uncommitted)> set
  chapsecret=123456789012abc
hostname:configuration san iscsi initiators initiator (uncommitted)> commit
hostname:configuration san iscsi initiators> list
NAME          ALIAS
initiator-000 Init 0
|
+--> INITIATOR
      iqn.2001-02.com.acme:initiator12345
```

Temas relacionados

- [Descripción de SAN](#)
- [Configuración de canal de fibra de SAN](#)
- [Configuración de iSCSI de SAN](#)
- [Configuración de destinos iSER de SAN](#)
- [Configuración de SRP de SAN](#)
- [Terminología de SAN](#)

▼ Agregación de un grupo de destinos iSCSI (CLI)

- Para agregar un grupo de destinos iSCSI, use los siguientes comandos de la CLI:

```
hostname:configuration san iscsi targets groups> create
hostname:configuration san iscsi targets group (uncommitted)> set name=tg0
hostname:configuration san iscsi targets group (uncommitted)> set targets=iqn.2001-02.com.acme:
12345,iqn.1986-03.com.sun:02:daf0161f-9f5d-e01a-b5c5-e1efa9578416
hostname:configuration san iscsi targets group (uncommitted)> commit
hostname:configuration san iscsi targets groups> list
GROUP      NAME
group-000  tg0
           |
           +-> TARGETS
                iqn.2001-02.com.acme:12345
                iqn.1986-03.com.sun:02:daf0161f-9f5d-e01a-b5c5-e1efa9578416
```

Temas relacionados

- [Descripción de SAN](#)
- [Configuración de canal de fibra de SAN](#)
- [Configuración de iSCSI de SAN](#)
- [Configuración de destinos iSER de SAN](#)
- [Configuración de SRP de SAN](#)
- [Terminología de SAN](#)

▼ Agregación de un grupo de iniciadores iSCSI (CLI)

- Para agregar un grupo de iniciadores iSCSI, use los siguientes comandos de la CLI:

```
hostname:configuration san iscsi initiators groups> create
hostname:configuration san iscsi initiators group (uncommitted)> set name=ig0
hostname:configuration san iscsi initiators group (uncommitted)> set initiators=iqn.2001-02.
com.acme:initiator12345
hostname:configuration san iscsi initiators group (uncommitted)> commit
hostname:configuration san iscsi initiators groups> list
GROUP      NAME
group-000  ig0
           |
           +-> INITIATORS
                iqn.2001-02.com.acme:initiator12345
```

Temas relacionados

- [Descripción de SAN](#)
- [Configuración de canal de fibra de SAN](#)

- [Configuración de iSCSI de SAN](#)
- [Configuración de destinos iSER de SAN](#)
- [Configuración de SRP de SAN](#)
- [Terminología de SAN](#)

▼ Configuración de destinos SRP (BUI)

En este procedimiento, se describen los pasos para configurar destinos SRP.

1. **Conecte los puertos del adaptador de canal de host (HCA) a las interfaces IB.**
2. **El dispositivo detecta automáticamente los destinos.**
3. **Para crear un grupo de destinos, vaya a la pantalla Configuration (Configuración) > SAN.**
4. **Haga clic en el enlace Destino y, a continuación, haga clic en los destinos SRP.**
5. **Aparece la página de destinos SRP.**
6. **Para crear el grupo de destinos, use el ícono de movimiento  a fin de arrastrar un destino hasta la lista Grupos de destinos.**
7. **Haga clic en APLICAR.**
8. **(Opcional) Para crear un iniciador y un grupo de iniciadores en la pantalla Iniciador, haga clic en el ícono , obtenga la GUID del iniciador, asígnele un nombre y arrástrela hasta el grupo de iniciadores.**
9. **Para crear un LUN y asociarlo con el destino SRP y los iniciadores que creó en los pasos anteriores, vaya a la pantalla Recursos compartidos.**
10. **Haga clic en el enlace LUN y, a continuación, haga clic en el ícono LUN . Use los menús Grupo de destinos y Grupo de iniciadores del cuadro de diálogo Crear LUN para seleccionar los grupos SRP que desea asociar con el LUN.**

Temas relacionados

- [Descripción de SAN](#)

- [Configuración de canal de fibra de SAN](#)
- [Configuración de iSCSI de SAN](#)
- [Configuración de destinos iSER de SAN](#)
- [Configuración de SRP de SAN](#)
- [Terminología de SAN](#)

▼ Configuración de destinos SRP (CLI)

En el siguiente ejemplo, se muestra cómo crear un grupo de destinos SRP llamado targetSRPgroup con el contexto configuration san targets srp groups de la CLI:

- **Para configurar destinos SRP, use los siguientes comandos de la CLI:**

```
hostname:configuration san targets srp groups> create
hostname:configuration san targets srp group (uncommitted)> set name=targetSRPgroup
name = targetSRPgroup (uncommitted)
hostname:configuration san targets srp group (uncommitted)> set targets=eui.0002C903000489A4
targets = eui.0002C903000489A4 (uncommitted)
hostname:configuration san targets srp group (uncommitted)> commit
hostname:configuration san targets srp groups> list
GROUP      NAME
group-000  targetSRPgroup
|
+--> TARGETS
      eui.0002C903000489A4
```

ejemplo 1 Creación de un LUN asociado con un grupo de destinos SRP mediante el uso de la CLI

En el siguiente ejemplo, se muestra cómo crear un LUN y asociarlo con el grupo targetSRPgroup usando el contexto shares de la CLI:

```
hostname:shares default> lun mylun
hostname:shares default/mylun (uncommitted)> set targetgroup=targetSRPgroup
targetgroup = targetSRPgroup (uncommitted)
hostname:shares default/mylun (uncommitted)> set volsize=10
volsize = 10 (uncommitted)
hostname:shares default/mylun (uncommitted)> commit
hostname:shares default> list
Filesystems:
NAME      SIZE      MOUNTPPOINT
test      38K       /export/test
LUNS:
NAME      SIZE      GUID
mylun     10G       600144F0E9D19FFB00004B82DF490001
```

Temas relacionados

- [Descripción de SAN](#)

- [Configuración de canal de fibra de SAN](#)
- [Configuración de iSCSI de SAN](#)
- [Configuración de destinos iSER de SAN](#)
- [Configuración de SRP de SAN](#)
- [Terminología de SAN](#)

Descripción de SAN

Estos tres componentes permanecen iguales independientemente del protocolo usado en la red. En algunos casos, la red puede incluso ser un cable entre el iniciador y el destino, pero en la mayoría de los casos, se usa algún tipo de conmutación.

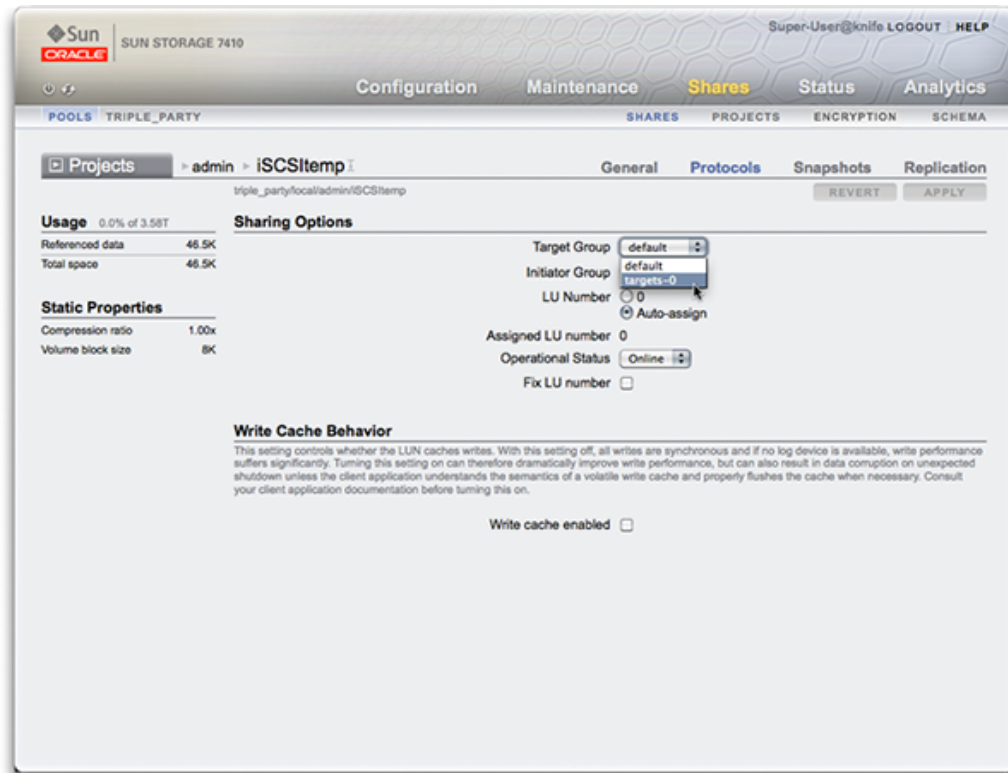
Los destinos y los iniciadores se configuran mediante protocolos. Consulte la documentación de un protocolo específico ([“Configuración de canal de fibra de SAN” \[246\]](#), [iSCSI](#) o [“Configuración de SRP” \[469\]](#)) para obtener información detallada.

Los grupos de destinos e iniciadores definen conjuntos de destinos e iniciadores que se pueden asociar con LUN. Un LUN asociado con un grupo de destinos se puede ver solamente mediante los destinos del grupo. Si el LUN no está explícitamente asociado con un grupo de destino, se encuentra en el *grupo de destino por defecto* y se podrá tener acceso a él desde todos los destinos, independientemente del protocolo. De manera similar, un LUN es visible únicamente por los iniciadores del grupo o los grupos a los que pertenece. Si el LUN no está explícitamente asociado con un grupo de iniciadores, se encuentra en el *grupo de iniciadores por defecto* y se podrá tener acceso a él desde todos los iniciadores. Si bien puede ser útil usar el grupo de iniciadores por defecto con fines de evaluación, no se recomienda utilizarlo porque puede exponer el LUN a iniciadores no deseados o en conflicto.

Para evitar posibles conflictos de LUN cuando un iniciador pertenece a varios grupos, configure iniciadores dentro de todos los grupos antes de asociar grupos a LUN.

Para configurar destinos, vaya a la página Configuración > SAN de la BUI, utilice Canal de fibra, iSCSI y SRP para navegar y, a continuación, configure los controles puertos, iniciador y grupos de destinos.

Para asociar un LUN, vaya a la página Recursos compartidos > Recursos compartidos > Protocolos y, a continuación, configure los controles Grupo de destinos y Grupo de iniciadores.

FIGURA 16 Asociación de un LUN

Use el contexto `configuration` `san` de la CLI para operar sobre destinos e iniciadores por tipo de protocolo. A continuación, use el contexto `shares` de la CLI para crear LUN y asociarlos con los grupos de destinos e iniciadores.

Temas relacionados

- Configuración de modo de los puertos FC (BUI)
- Detección de puertos FC (BUI)
- Creación de grupos de iniciadores FC (BUI)
- Asociación de un LUN con un grupo de iniciadores FC (BUI)
- Cambio de modo de los puertos FC (CLI)
- Detección de puertos FC (CLI)

- Creación de grupos de iniciadores de FC (CLI)
- Asociación de un LUN con un grupo de iniciadores FC (CLI)
- Asignación de alias a iniciadores y grupos de iniciadores mediante secuencias de comandos (CLI)
- Configuración de iniciadores iSCSI de SAN
- Creación de una hoja de trabajo de análisis (BUI)
- Agregación de un destino iSCSI con un IQN generado automáticamente (CLI)
- Agregación de un destino iSCSI con un IQN específico y autenticación RADIUS (CLI)
- Agregación de iniciador iSCSI con autenticación CHAP (CLI)
- Agregación de un grupo de destinos iSCSI (CLI)
- Agregación de un grupo de iniciadores iSCSI (CLI)
- Configuración de destinos SRP (BUI)
- Configuración de destinos SRP (CLI)

Configuración de canal de fibra de SAN

El canal de fibra (FC) es una tecnología de red con velocidad en el orden de los gigabits que se usa casi exclusivamente como transporte para SCSI. FC es uno de los varios protocolos de bloque admitidos por el dispositivo. Para compartir LUN mediante FC, el dispositivo debe contar con una o varias tarjetas FC opcionales.

Por defecto, todos los puertos FC se configuran para estar en modo de destino. Si el dispositivo se utiliza para conectarse a un SAN de cinta para realizar copias de seguridad, se deben configurar uno o más puertos en el modo de iniciador. Para configurar un puerto para el modo de iniciador, se debe restablecer el dispositivo. Es posible configurar varios puertos para el modo de iniciador simultáneamente.

Cada puerto FC tiene un nombre World Wide Name (WWN) asignado y, al igual que con otros protocolos de bloque, los destinos FC se pueden agrupar en grupos de iniciadores y destinos SAN, lo que permite que el ancho de banda de los puertos esté dedicado a LUN o grupos de LUN específicos. Una vez que un puerto FC se configura como destino, es posible examinar y verificar los puertos detectados de manera remota.

Consulte el resumen técnico *Implementación del inicio SAN de canal de fibra con Oracle ZFS Storage Appliance* en <https://www.oracle.com/technetwork/server-storage/sun-unified-storage/documentation/fc-sanboot-081412-pdf-1735984.pdf> para obtener detalles sobre soluciones de inicio SAN de canal de fibra con el dispositivo.

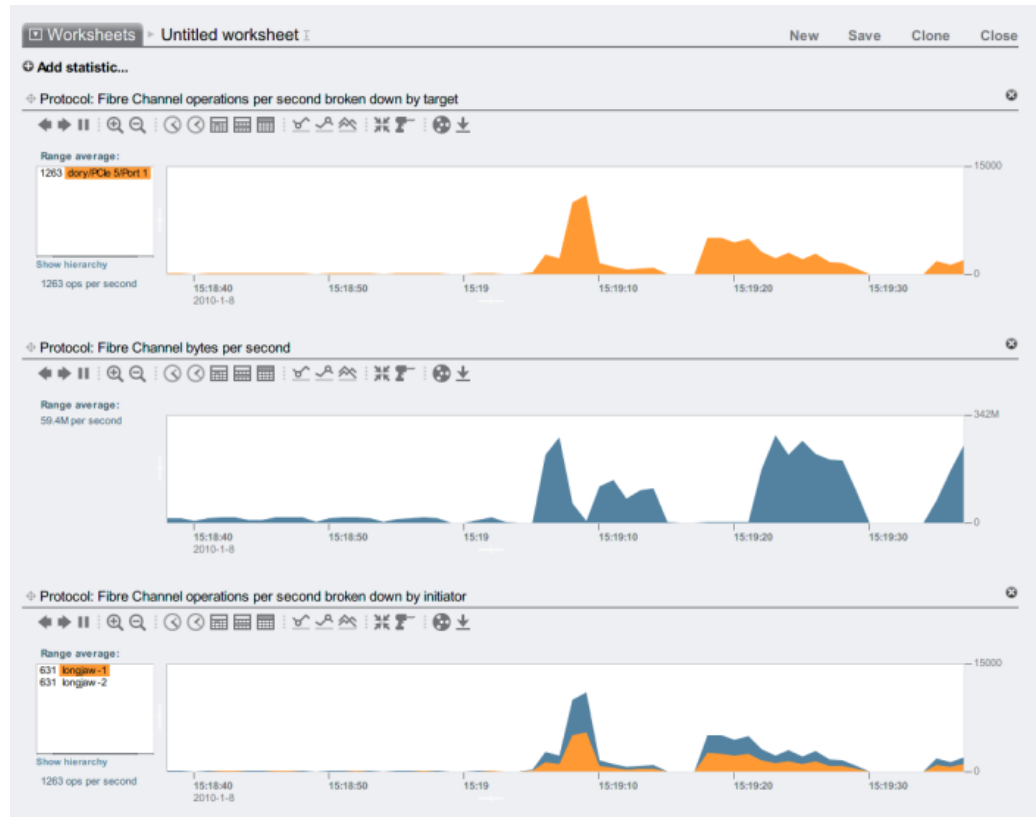
En un cluster, los iniciadores tienen dos rutas (o conjuntos de rutas) para cada LUN: una ruta (o un conjunto de rutas) corresponde al nodo principal que importó el almacenamiento asociado

con el LUN; la otra ruta (o el otro conjunto de rutas) corresponde al par en clusters de ese nodo principal. La primera ruta (o el primer conjunto de rutas) está *activa*; la segunda ruta (o el segundo conjunto de rutas) está *en espera*. Si se produce una toma de control, las rutas activas no estarán disponibles y las rutas en espera pasarán (después de un período breve) al estado activo, después de lo cual continuarán las operaciones de E/S. Este enfoque del uso de rutas múltiples se conoce como acceso asimétrico a unidad lógica (ALUA) y, junto con un iniciador capaz de reconocer ALUA, permite que la toma de control en el cluster se realice de manera transparente para las aplicaciones de nivel superior.

Los iniciadores se identifican por su nombre WWN. Al igual que con otros protocolos de bloque, se pueden crear alias para ellos. Para ayudar a crear alias para los iniciadores FC, se puede seleccionar un nombre WWN entre los nombres WWN de los puertos detectados. Además, al igual que con otros protocolos de bloque, es posible agrupar los iniciadores. Cuando se asocia un LUN con un grupo de iniciadores específicos, el LUN será visible solamente para los iniciadores del grupo. En la mayoría de las SAN FC, los LUN están siempre asociados con el grupo de iniciadores correspondiente al sistema para el que se creó el LUN.

El dispositivo es una matriz que cumple con los requisitos de ALUA. Para configurar correctamente un iniciador FC en un entorno ALUA, se necesita un controlador que sea capaz de reconocer ALUA y posiblemente un ajuste específico del iniciador. Consulte "Oracle ZFS Storage Appliance: Configuración de acceso de rutas múltiples de clientes" (ID de documento 1628999.1) para obtener más información.

El rendimiento de FC se puede observar mediante el análisis, que permite desglosar las operaciones o el rendimiento por iniciador, destino o LUN:

FIGURA 17 Rendimiento de FC

Para las operaciones, también se puede hacer un desglose por compensación, latencia, tamaño y comando SCSI, lo que permite comprender no solo *qué* es lo que hacen las operaciones de FC, sino también *cómo* lo hacen y *por qué*.

El dispositivo está diseñado para utilizar un conjunto global de recursos a fin de prestar servicios a los LUN de cada nodo principal. Por lo tanto, generalmente no es necesario restringir la profundidad de cola en los clientes, ya que los puertos FC del dispositivo pueden manejar una gran cantidad de solicitudes simultáneas. Aun así, existe la posibilidad remota de que estas colas se saturen y se generen errores en el transporte SCSI. A menudo, esta saturación de las colas está asociada con una o varias de las siguientes situaciones:

- Puertos sobrecargados del lado del usuario: demasiados hosts asociados con un puerto FC o acceso a demasiados LUN a través de un puerto FC.

- Modos operativos degradados del dispositivo, por ejemplo, una toma de control en el cluster en una configuración de cluster diseñada para ser activo-activo.

Si bien la posibilidad de saturación de las colas es remota, se puede eliminar por completo si se está dispuesto a limitar la profundidad de cola por cliente. Para determinar un límite de profundidad de cola adecuado, se debe tomar la cantidad de puertos de destino, multiplicarla por la cantidad máxima de comandos simultáneos por puerto (2.048) y dividir el producto por la cantidad de LUN provisionados. Para tener en cuenta los modos operativos degradados, se debe sumar la cantidad de LUN en todos los pares de cluster a fin de determinar la cantidad de LUN, pero como cantidad de puertos de destino se debe usar la cifra de los dos pares de cluster que sea menor. Por ejemplo, en un cluster de doble nodo principal activo-activo 7420, en el que uno de los nodos principales tiene dos puertos FC y 100 LUN, y el otro tiene cuatro puertos FC y 28 LUN, para determinar la menor profundidad de cola máxima, se deben tomar dos puertos, multiplicarlos por 2048 comandos, dividir el producto por 100 LUN más 28 LUN, o 32 comandos por LUN.

El ajuste de la profundidad de cola máxima es específico del iniciador, pero en Oracle Solaris se hace ajustando la variable global `ssd_max_throttle`.

Para resolver problemas relacionados con los enlaces, por ejemplo, una fibra óptica rota o un cable mal conectado, consulte las estadísticas de error de cada puerto FC. Si hay algún número muy diferente de cero o que va en aumento, puede significar que se han encontrado problemas en el nivel del enlace y que se deben realizar las tareas de diagnóstico en el nivel del enlace.

Temas relacionados

- [Configuración de modo de los puertos FC \(BUI\)](#)
- [Detección de puertos FC \(BUI\)](#)
- [Creación de grupos de iniciadores FC \(BUI\)](#)
- [Asociación de un LUN con un grupo de iniciadores FC \(BUI\)](#)
- [Cambio de modo de los puertos FC \(CLI\)](#)
- [Detección de puertos FC \(CLI\)](#)
- [Creación de grupos de iniciadores de FC \(CLI\)](#)
- [Asociación de un LUN con un grupo de iniciadores FC \(CLI\)](#)
- [Asignación de alias a iniciadores y grupos de iniciadores mediante secuencias de comandos \(CLI\)](#)
- [Configuración de iniciadores iSCSI de SAN](#)
- [Creación de una hoja de trabajo de análisis \(BUI\)](#)
- [Agregación de un destino iSCSI con un IQN generado automáticamente \(CLI\)](#)
- [Agregación de un destino iSCSI con un IQN específico y autenticación RADIUS \(CLI\)](#)
- [Agregación de iniciador iSCSI con autenticación CHAP \(CLI\)](#)
- [Agregación de un grupo de destinos iSCSI \(CLI\)](#)
- [Agregación de un grupo de iniciadores iSCSI \(CLI\)](#)

- [Configuración de destinos SRP \(BUI\)](#)
- [Configuración de destinos SRP \(CLI\)](#)

Configuración de iSCSI de SAN

Internet SCSI es uno de los varios protocolos de bloque admitidos por el dispositivo para compartir almacenamiento SCSI.

Cuando se usa el protocolo iSCSI, el portal de destino hace referencia a la combinación única de dirección IP y número de puerto TCP que un iniciador puede usar para establecer contacto con un destino.

Cuando se usa el protocolo iSCSI, un grupo de portales de destino es una recopilación de portales de destino. Los grupos de portales de destino se gestionan de manera transparente; cada interfaz de red tiene un grupo de portales de destino correspondiente con las direcciones activas de esa interfaz. La vinculación de un destino con una interfaz anuncia ese destino iSCSI mediante el grupo de portales asociado con esa interfaz.

Nota - No se admiten varias conexiones por sesión.

Un IQN (nombre completo iSCSI) es el identificador único de un dispositivo en una red iSCSI. iSCSI usa el formato `iqn.fecha.autoridad:ídunico` para los IQN. Por ejemplo, el dispositivo puede utilizar el IQN: `iqn.1986-03.com.sun:02:c7824a5b-f3ea-6038-c79d-ca443337d92c` para identificar uno de sus destinos iSCSI. Este nombre muestra que se trata de un dispositivo iSCSI fabricado por una empresa registrada en marzo de 1986. La autoridad de nombres es simplemente el nombre de DNS de la empresa pero invertido, en este caso, "com.sun". Todo lo que sigue es un ID único que Oracle utiliza para identificar el destino.

TABLA 34 Propiedades de destino iSCSI

Propiedad de destino	Descripción
IQN de destino	IQN de este destino. El IQN se puede especificar manualmente o se puede generar de manera automática.
Alias	Apodo en lenguaje natural para este destino.
Modo de autenticación	Puede ser Ninguno, CHAP o RADIUS.
Nombre de CHAP	Si se usa la autenticación CHAP, es el nombre de usuario de CHAP.
Secreto de CHAP	Si se usa la autenticación CHAP, es el secreto de CHAP.
Interfaces de red	Interfaces cuyos portales de destino se usan para exportar este destino.

Además de esas propiedades, la BUI indica si el destino está en línea o sin conexión:

TABLA 35 Íconos de estado de destino

Ícono	Descripción
	El destino está en línea.
	El destino está sin conexión.

En las plataformas agrupadas en cluster, los destinos que tengan al menos una interfaz activa en ese nodo de cluster estarán en línea. Tenga cuidado al asignar interfaces a los destinos; un destino puede estar configurado para usar grupos de portales en nodos principales separados. En esa situación, el destino estará en línea en los dos nodos principales, pero exportará diferentes LUN en función del almacenamiento del que cada nodo principal es responsable. Como las interfaces de red migran entre los nodos principales de cluster como parte de las operaciones de toma de control/failback o los cambios de propiedad, los destinos iSCSI estarán en línea y sin conexión mientras sus respectivas interfaces de red se importan y exportan.

Los destinos que están vinculados a una interfaz IPMP se publicarán solamente mediante las direcciones de ese grupo IPMP. Ese destino no estará disponible mediante las direcciones de prueba de ese grupo. Los destinos vinculados a interfaces incorporadas en una agregación LACP usarán la dirección de esa agregación. Si se agrega una agregación LACP a un grupo IPMP, el destino ya no podrá usar la interfaz de esa agregación, ya que la dirección pasará a ser una dirección de prueba de IPMP.

Temas relacionados

- [Configuración de modo de los puertos FC \(BUI\)](#)
- [Detección de puertos FC \(BUI\)](#)
- [Creación de grupos de iniciadores FC \(BUI\)](#)
- [Asociación de un LUN con un grupo de iniciadores FC \(BUI\)](#)
- [Cambio de modo de los puertos FC \(CLI\)](#)
- [Detección de puertos FC \(CLI\)](#)
- [Creación de grupos de iniciadores de FC \(CLI\)](#)
- [Asociación de un LUN con un grupo de iniciadores FC \(CLI\)](#)
- [Asignación de alias a iniciadores y grupos de iniciadores mediante secuencias de comandos \(CLI\)](#)
- [Configuración de iniciadores iSCSI de SAN](#)
- [Creación de una hoja de trabajo de análisis \(BUI\)](#)
- [Agregación de un destino iSCSI con un IQN generado automáticamente \(CLI\)](#)
- [Agregación de un destino iSCSI con un IQN específico y autenticación RADIUS \(CLI\)](#)
- [Agregación de iniciador iSCSI con autenticación CHAP \(CLI\)](#)
- [Agregación de un grupo de destinos iSCSI \(CLI\)](#)

- [Agregación de un grupo de iniciadores iSCSI \(CLI\)](#)
- [Configuración de destinos SRP \(BUI\)](#)
- [Configuración de destinos SRP \(CLI\)](#)

Configuración de iniciador iSCSI de SAN

Los iniciadores iSCSI tienen las siguientes propiedades configurables.

TABLA 36 Propiedades de iniciadores iSCSI de SAN

Propiedad	Descripción
Initiator IQN (IQN de iniciador)	IQN de este iniciador.
Alias	Apodo en lenguaje natural para este iniciador.
Usar CHAP	Activa o desactiva la autenticación CHAP.
Nombre de CHAP	Si se usa la autenticación CHAP, es el nombre de usuario de CHAP.
Secreto de CHAP	Si se usa la autenticación CHAP, es el secreto de CHAP.

Al planificar la configuración de clientes iSCSI, necesitará la siguiente información:

- ¿Qué iniciadores (y sus IQN) tendrán acceso a la SAN?
- Si tiene pensado usar la autenticación CHAP, ¿qué credenciales de CHAP utiliza cada iniciador?
- ¿Cuántos discos iSCSI (LUN) se necesitan? ¿De qué tamaño deben ser?
- ¿Es necesario compartir los LUN entre varios iniciadores?

Para permitir que el dispositivo realice la autenticación CHAP con RADIUS, los siguientes datos deben coincidir:

- El dispositivo debe especificar la dirección del servidor RADIUS y un secreto para usar al comunicarse con él.
- El servidor RADIUS debe tener una entrada (por ejemplo, en el archivo de clientes) en donde esté la dirección de este dispositivo y se especifique el mismo secreto que el mencionado más arriba.
- El servidor RADIUS debe tener una entrada (por ejemplo, en el archivo de usuarios) en donde esté el nombre de CHAP y el secreto de CHAP coincidente de cada iniciador.
- Si el iniciador utiliza su nombre IQN como nombre de CHAP (configuración recomendada), el dispositivo no necesita una entrada de iniciador independiente para cada cuadro de iniciador: el servidor RADIUS puede realizar todos los pasos de autenticación.
- Si el iniciador usa un nombre de CHAP independiente, el dispositivo debe tener una entrada de iniciador para ese iniciador que especifique la asignación del nombre IQN al nombre de

CHAP. NO es necesario que esta entrada de iniciador especifique el secreto de CHAP del iniciador.

Para ver consejos para la resolución de problemas de configuración comunes en iSCSI, consulte [iSCSI](#).

El rendimiento de iSCSI se puede observar mediante los análisis, que permiten desglosar las operaciones o el rendimiento por iniciador, destino o LUN.

Temas relacionados

- [Configuración de modo de los puertos FC \(BUI\)](#)
- [Detección de puertos FC \(BUI\)](#)
- [Creación de grupos de iniciadores FC \(BUI\)](#)
- [Asociación de un LUN con un grupo de iniciadores FC \(BUI\)](#)
- [Cambio de modo de los puertos FC \(CLI\)](#)
- [Detección de puertos FC \(CLI\)](#)
- [Creación de grupos de iniciadores de FC \(CLI\)](#)
- [Asociación de un LUN con un grupo de iniciadores FC \(CLI\)](#)
- [Asignación de alias a iniciadores y grupos de iniciadores mediante secuencias de comandos \(CLI\)](#)
- [Configuración de iniciadores iSCSI de SAN](#)
- [Creación de una hoja de trabajo de análisis \(BUI\)](#)
- [Agregación de un destino iSCSI con un IQN generado automáticamente \(CLI\)](#)
- [Agregación de un destino iSCSI con un IQN específico y autenticación RADIUS \(CLI\)](#)
- [Agregación de iniciador iSCSI con autenticación CHAP \(CLI\)](#)
- [Agregación de un grupo de destinos iSCSI \(CLI\)](#)
- [Agregación de un grupo de iniciadores iSCSI \(CLI\)](#)
- [Configuración de destinos SRP \(BUI\)](#)
- [Configuración de destinos SRP \(CLI\)](#)

Configuración de SRP de SAN

Protocolo RDMA SCSI, un protocolo admitido por el dispositivo para compartir almacenamiento SCSI mediante redes que proporcionan servicios RDMA (por ejemplo, InfiniBand).

Los puertos SRP se comparten con otros servicios de puertos IB, por ejemplo, IPoIB y RDMA. El servicio SRP puede funcionar solo en el modo de destino. Los destinos SRP tienen las siguientes propiedades configurables.

TABLA 37 Propiedades de destinos SRP

Propiedad	Descripción
Target EUI	Identificador único extendido (EUI) de este destino. El EUI es asignado automáticamente por el sistema y es igual al GUID del adaptador de canal de host (HCA) en el que se ejecuta el servicio del puerto SRP.
Alias	Apodo en lenguaje natural para este destino.

Además de esas propiedades, la BUI indica si el destino está en línea o sin conexión:

TABLA 38 Íconos de estado de destino de SRP

Ícono	Descripción
	El destino está en línea.
	El destino está sin conexión.

En las plataformas agrupadas en cluster, los destinos de pares se deben configurar en el mismo grupo de destinos para las configuraciones de alta disponibilidad (de rutas múltiples). La E/S de rutas múltiples de SRP es una opción de configuración del lado del iniciador.

Los iniciadores SRP tienen las siguientes propiedades configurables.

TABLA 39 Propiedades de iniciadores SRP

Propiedad	Descripción
Initiator EUI	EUI de este iniciador.
Alias	Apodo en lenguaje natural para este iniciador.

El rendimiento de SRP se puede observar mediante los análisis, que permiten desglosar las operaciones o el rendimiento por iniciador o destino.

Temas relacionados

- [Configuración de modo de los puertos FC \(BUI\)](#)
- [Detección de puertos FC \(BUI\)](#)
- [Creación de grupos de iniciadores FC \(BUI\)](#)
- [Asociación de un LUN con un grupo de iniciadores FC \(BUI\)](#)
- [Cambio de modo de los puertos FC \(CLI\)](#)
- [Detección de puertos FC \(CLI\)](#)
- [Creación de grupos de iniciadores de FC \(CLI\)](#)
- [Asociación de un LUN con un grupo de iniciadores FC \(CLI\)](#)

- Asignación de alias a iniciadores y grupos de iniciadores mediante secuencias de comandos (CLI)
- Configuración de iniciadores iSCSI de SAN
- Creación de una hoja de trabajo de análisis (BUI)
- Agregación de un destino iSCSI con un IQN generado automáticamente (CLI)
- Agregación de un destino iSCSI con un IQN específico y autenticación RADIUS (CLI)
- Agregación de iniciador iSCSI con autenticación CHAP (CLI)
- Agregación de un grupo de destinos iSCSI (CLI)
- Agregación de un grupo de iniciadores iSCSI (CLI)
- Configuración de destinos SRP (BUI)
- Configuración de destinos SRP (CLI)

Terminología de SAN

Para configurar el dispositivo a fin de utilizarlo con una SAN, debe comprender algunos términos básicos de SAN:

TABLA 40 Terminología de SAN

Término	Descripción
Destino SCSI	Un destino SCSI es un punto final de un sistema de almacenamiento que proporciona un servicio de procesamiento de comandos SCSI y solicitudes de E/S recibidas de un iniciador. El destino SCSI es creado por el administrador del sistema de almacenamiento y se lo identifica mediante métodos de asignación de direcciones únicas. El destino SCSI, una vez configurado, tiene cero o más unidades lógicas.
Iniciador SCSI	Un iniciador SCSI es un punto final de aplicación o sistema en producción que puede iniciar una sesión SCSI y enviar comandos SCSI y solicitudes de E/S. Los iniciadores SCSI también se identifican mediante métodos de asignación de direcciones únicas (consulte Destinos SCSI).
Unidad lógica	El término "unidad lógica" se utiliza para describir un componente de un sistema de almacenamiento. Tiene una numeración exclusiva; esto crea lo que se conoce como número de unidad lógica o LUN (por sus siglas en inglés). Un sistema de almacenamiento, dado que es altamente configurable, puede contener muchos LUN. Estos LUN, cuando se los asocia con uno o varios destinos SCSI, forman un dispositivo SCSI único, que es un dispositivo al que pueden acceder uno o varios iniciadores SCSI.

Término	Descripción
iSCSI	Internet SCSI, un protocolo para compartir almacenamiento SCSI mediante redes IP. El dispositivo admite la especificación de reservas persistentes SCSI-3.
iSER	Extensión iSCSI para RDMA, un protocolo que asigna el protocolo iSCSI mediante redes que proporcionan servicios RDMA (por ejemplo, InfiniBand). El subsistema iSCSI selecciona de manera transparente el protocolo iSER, en función de la presencia de hardware IB correctamente configurado. En la CLI y la BUI, todos los componentes que admiten iSER (destinos e iniciadores) se gestionan como componentes iSCSI.
FC	Canal de fibra, un protocolo para compartir almacenamiento SCSI mediante una red de área de almacenamiento (SAN). Está compuesto por cables de fibra óptica, conmutadores de canal de fibra y adaptadores bus de host (HBA). El dispositivo admite topologías de bucle arbitrado de canal de fibra (FC-AL) de 4 GB y 8 GB.
SRP	Protocolo RDMA SCSI, un protocolo para compartir almacenamiento SCSI mediante redes que proporcionan servicios RDMA (por ejemplo, InfiniBand).
IQN	Nombre completo iSCSI; es el identificador único de un dispositivo en una red iSCSI. iSCSI usa el formato <code>iqn.fecha.autoridad:ídunico</code> para los IQN. Por ejemplo, el dispositivo puede utilizar el IQN: <code>iqn.1986-03.com.sun:02:c7824a5b-f3ea-6038-c79d-ca443337d92c</code> para identificar uno de sus destinos iSCSI. Este nombre muestra que se trata de un dispositivo iSCSI fabricado por una empresa registrada en marzo de 1986. La autoridad de nombres es simplemente el nombre de DNS de la empresa pero invertido, en este caso, "com.sun". Todo lo que sigue es un identificador único que Sun utiliza para identificar el destino.
Portal de destino	Cuando se usa el protocolo iSCSI, el portal de destino hace referencia a la combinación única de dirección IP y número de puerto TCP que un iniciador puede usar para establecer contacto con un destino.
Grupo de portales de destino	Cuando se usa el protocolo iSCSI, un grupo de portales de destino es una recopilación de portales de destino. Los grupos de portales de destino se gestionan de manera transparente; cada interfaz de red tiene un grupo de portales de destino correspondiente con las direcciones activas de esa interfaz. La vinculación de un destino con una interfaz anuncia ese destino iSCSI mediante el grupo de portales asociado con esa interfaz.
CHAP	Protocolo de autenticación por desafío mutuo, es un protocolo de seguridad que puede autenticar un destino para un iniciador, un iniciador para un destino, o ambos.

Término	Descripción
RADIUS	Sistema para usar un servidor centralizado para realizar la autenticación CHAP en nombre de los nodos de almacenamiento.
Grupo de destinos	Conjunto de destinos. Los LUN se exportan a todos los destinos en un grupo de destino específico.
Grupo de iniciadores	Conjunto de iniciadores. Cuando un grupo de iniciadores se asocia con un LUN, solo los iniciadores de ese grupo pueden acceder al LUN.
Destino	Punto final de un sistema de almacenamiento que proporciona un servicio de procesamiento de comandos SCSI y solicitudes de E/S recibidas de un iniciador. El destino es creado por el administrador del sistema de almacenamiento y se lo identifica mediante métodos de asignación de direcciones únicas. El destino, una vez configurado, tiene cero o más unidades lógicas.
Iniciador	Punto final de aplicación o sistema en producción que puede iniciar una sesión SCSI y enviar comandos SCSI y solicitudes de E/S. Los iniciadores también se identifican por los métodos exclusivos de direccionamiento.

Cada LUN tiene varias propiedades que controlan el método de exportación del volumen. Consulte [Protocolos](#) para obtener más información.

Configuración de usuarios

En esta sección, se describe cómo crear usuarios del dispositivo, incluida la forma de garantizar autorizaciones para los usuarios y de usar roles para gestionar las autorizaciones.

Para configurar usuarios y roles, use las siguientes secciones:

- Adición de un administrador o usuario: [BUI](#), [CLI](#)
- Cambio de una contraseña de usuario: [BUI](#), [CLI](#)
- Edición de excepciones para un usuario: [BUI](#), [CLI](#)
- Adición de un rol: [BUI](#), [CLI](#)
- Edición de autorizaciones para un rol: [BUI](#), [CLI](#)
- Agregación de un usuario que pueda ver solamente el panel de control: [BUI](#), [CLI](#)
- [Determinación del usuario actual conectado \[272\]](#)

Para comprender conceptos de usuarios y roles, use las siguientes secciones:

- [“Descripción de usuarios y roles” \[273\]](#)
- [“Autorizaciones de usuarios” \[274\]](#)

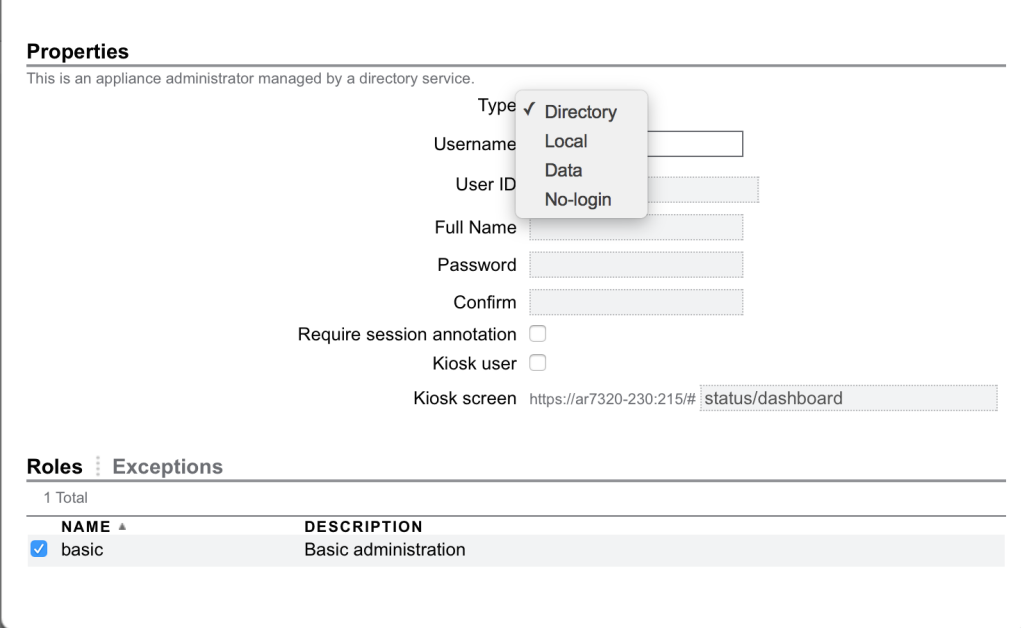
- [“Administración de propiedades de usuario” \[278\]](#)

▼ Agregación de un administrador o usuario (BUI)

Use el siguiente procedimiento para crear un usuario con o sin el rol de administrador.

1. **Vaya a Configuración > Usuarios.**
2. **Haga clic en el ícono de agregación  que se encuentra junto a Usuarios.**
A continuación de este procedimiento, consulte también "Método alternativo".
3. **En el cuadro de diálogo Agregar usuario, elija el tipo de usuario adecuado en el menú desplegable Tipo.**

Para ver las descripciones de los tipos de usuario, consulte [“Descripción de usuarios y roles” \[273\]](#).



Properties

This is an appliance administrator managed by a directory service.

Type ☒ Directory

Username

User ID

Full Name

Password

Confirm

Require session annotation ☐

Kiosk user ☐

Kiosk screen

Roles **Exceptions**

1 Total

NAME ▲	DESCRIPTION
☒ basic	Basic administration

4. **Introduzca valores para las propiedades.**

Se necesita un valor para Nombre de usuario. Si necesita ayuda para establecer el valor de Nombre de usuario, consulte [“Descripción de usuarios y roles” \[273\]](#).

- Si en el tipo de usuario seleccionó Directorio, los campos ID de usuario y Contraseña se configuran automáticamente: se usan los valores NIS, LDAP o AD.
- Si en el tipo de usuario seleccionó Local, Datos o Sin inicio de sesión, se requiere un ID de usuario. Si no establece el ID de usuario, se asignará uno automáticamente. Si necesita ayuda para establecer el valor de ID de usuario, consulte "Propiedades de usuario" en [“Administración de propiedades de usuario” \[278\]](#).
- Si en el tipo de usuario seleccionó Local o Datos, se requiere un valor para Contraseña.

Si no proporciona un valor para Nombre completo, la BUI no mostrará la identidad del usuario actual. Consulte [Determinación del usuario actual conectado \[272\]](#).

5. (Opcional) Asigne roles para los usuarios Local y Directorio.

Haga clic en el separador Roles. Los usuarios Local y Directorio tienen el rol `basic` por defecto.

Puede elegir entre los roles que aparecen en la sección Roles de Configuración > Usuarios.

Haga clic en las casillas de control de los roles que desee que tenga este usuario.

6. (Opcional) Agregue autorizaciones para los usuarios Local y Directorio.

Consulte [Tabla 43, “Ámbitos, filtros y autorizaciones disponibles para los usuarios y roles”](#).

Haga clic en el separador Excepciones. Repita los siguientes pasos hasta que haya agregado todas las autorizaciones que desee para este usuario:

a. Seleccione un ámbito.

Si hay filtros disponibles para este ámbito, aparecerán debajo del selector Ámbito.

b. Especifique los filtros para el ámbito según sea necesario.

c. Haga clic en la casilla de control correspondiente a cada autorización que desea agregar.

d. Haga clic en ADD (Agregar) en la sección Exceptions (Excepciones).

Las autorizaciones aparecen en la parte inferior de la sección Excepciones.

Tenga en cuenta que estas autorizaciones también pueden usarse para excluir aquellas que se le otorgan al usuario con este rol. Si asigna autorizaciones que tienen un ámbito más limitado (con más filtros) que las mismas autorizaciones que se le otorgan a un rol, este usuario solo tendrá las autorizaciones correspondientes al ámbito más limitado.

7. Haga clic en ADD (Agregar) en la parte superior del cuadro de diálogo.

El nuevo usuario aparece en la lista Usuarios.

Método alternativo

Para crear un nuevo usuario del mismo tipo como un usuario existente y con los mismos roles y autorizaciones asignados, mueva el cursor sobre la entrada del usuario existente y haga clic en el ícono de clonación . Complete Nombre de usuario y Nombre completo. Si el tipo de usuario que va a clonar es Local o Datos, establezca una contraseña. Haga clic en Agregar en la parte superior del cuadro de diálogo Clonar usuario.

Temas relacionados

- [“Descripción de usuarios y roles” \[273\]](#)
- [“Administración de propiedades de usuario” \[278\]](#)
- [“Autorizaciones de usuarios” \[274\]](#)
- [“Configuración de preferencias del dispositivo” \[280\]](#)

▼ Agregación de un administrador o usuario (CLI)

Use el siguiente procedimiento para crear un usuario con o sin el rol de administrador.

1. **Vaya a configuration users.**

```
hostname:> configuration users
```

2. **Introduzca un tipo de usuario seguido de un nombre de usuario.**

```
hostname:configuration users> type username
```

Para ver las descripciones de los tipos de usuario o si necesita ayuda para establecer el valor de Nombre de usuario, consulte [“Descripción de usuarios y roles” \[273\]](#).

Si especifica `directory` como tipo de usuario, el usuario se configura inmediatamente, ya que el mínimo de propiedades requeridas (UID y contraseña) proviene de NIS, LDAP o AD.

```
hostname:configuration users> directory NISorLDAPorAD-username
hostname:configuration users>
```

Si especifica `local`, `data` o `nologin` como tipo de usuario, se le pedirá que establezca propiedades.

```
hostname:configuration users> local username
hostname:configuration users username (uncommitted)>
```

3. **Establezca propiedades para los usuarios `local`, `data` y `nologin`.**

a. Introduzca `get` para mostrar las propiedades que se podrán establecer.

```
hostname:configuration users username (uncommitted)> get
Properties:
    logname = username
    type = local
    uid = (unset)
    fullname = (unset)
    initial_password = (unset)
    require_annotation = false
```

b. Establezca las propiedades requeridas.

- Para los tipos de usuario `local`, `data` y `nologin`, se requiere un ID de usuario. Si no establece `uid` de forma explícita, automáticamente se asigna `uid`. Si necesita ayuda para establecer el valor `uid`, consulte "Propiedades de usuario" en ["Administración de propiedades de usuario" \[278\]](#).
- Para los tipos de usuario `local` y `data`, debe establecer `initial_password`.

c. Introduzca el comando `commit`.

4. Introduzca `show`.

Se muestra el nuevo usuario.

5. (Opcional) Establezca preferencias y propiedades adicionales.

a. Seleccione el nuevo usuario.

b. Introduzca `show` para ver lo que puede establecer.

Ahora puede ver propiedades adicionales que podrá establecer. Para ver las descripciones de las propiedades, consulte "Propiedades de usuario" en ["Administración de propiedades de usuario" \[278\]](#).

c. Introduzca `preferences` y luego `show` para ver qué preferencias puede establecer.

Consulte ["Configuración de preferencias del dispositivo" \[280\]](#).

6. (Opcional) Para los usuarios `local` y `directory`, asigne roles adicionales.

Los usuarios de tipo `local` o `directory` tienen el rol `basic` por defecto.

Los roles que aparecen en `configuration roles` están disponibles para que los elija.

a. Introduzca el siguiente comando para agregar un rol a este usuario:

```
hostname:configuration users username> set roles=basic,additional_role
roles = basic,additional_role (uncommitted)
```

b. Introduzca el comando `commit`.

7. (Opcional) Para los usuarios `local` y `directory`, asigne autorizaciones adicionales.

Consulte [Tabla 43, “Ámbitos, filtros y autorizaciones disponibles para los usuarios y roles”](#).

a. Seleccione el nuevo usuario.

b. Introduzca `exceptions`.

```
hostname:configuration users username> exceptions
```

c. Repita los siguientes pasos hasta que haya agregado todas las autorizaciones que desee para este usuario:

i. Introduzca `create`.

ii. Introduzca `set scope=` seguido del nombre del ámbito. Use la finalización con tabulación para ver la lista.

iii. Introduzca `show` para ver los filtros y, si hay alguna, las autorizaciones disponibles.

iv. Si hay un filtro disponible, establezca un valor.

Use la finalización con tabulación para ver una lista de posibles valores de filtro.

v. Establezca en `true` todas las autorizaciones que desee que tenga este usuario.

vi. Introduzca el comando `commit`.

Tenga en cuenta que estas autorizaciones también pueden usarse para excluir aquellas que se le otorgan al usuario con este rol. Si asigna autorizaciones que tienen un ámbito más limitado (con más filtros) que las mismas autorizaciones que se le otorgan a un rol, este usuario solo tendrá las autorizaciones correspondientes al ámbito más limitado.

d. Escriba `done`.

Método alternativo

Use el comando `clone` para crear un nuevo usuario del mismo tipo como un usuario existente y con los mismos roles y autorizaciones asignados. En `configuration users`, introduzca `clone existing-user-name new-user-name`. Establezca `fullname` para el nuevo usuario. Si el tipo de usuario que va a clonar es `local` o `data`, establezca una contraseña.

Temas relacionados

- [“Descripción de usuarios y roles” \[273\]](#)
- [“Administración de propiedades de usuario” \[278\]](#)
- [“Autorizaciones de usuarios” \[274\]](#)
- [“Configuración de preferencias del dispositivo” \[280\]](#)

▼ Cambio de una contraseña de usuario (BUI)

Use el siguiente procedimiento para cambiar la contraseña de un usuario. Para cambiar la contraseña de un usuario que no sea el suyo, debe tener privilegios de superusuario (`root`) o un rol que tenga la autorización `Users changePassword`.

1. **Vaya a Configuración > Usuarios.**
2. **Mueva el cursor sobre el usuario en la lista Users (Usuarios) y haga clic en el ícono de edición .**
3. **En el cuadro de diálogo Editar usuario local, escriba una contraseña nueva y vuelva a escribirla para confirmarla.**
4. **Haga clic en Aplicar.**

Temas relacionados

- [Edición de excepciones de un usuario \(BUI\) \[264\]](#)
- [Edición de autorizaciones de un rol \(BUI\) \[269\]](#)

▼ Cambio de una contraseña de usuario (CLI)

Use el siguiente procedimiento para cambiar la contraseña de un usuario. Para cambiar la contraseña de un usuario que no sea el suyo, debe tener privilegios de superusuario (root) o un rol que tenga la autorización `user allow_changePassword`.

1. **Vaya a** `configuration users`.
2. **Introduzca** `select` **y el nombre de usuario cuya contraseña desea cambiar.**
3. **Establezca un nuevo valor para** `initial_password`.

```
hostname:configuration users username> set initial_password=new password
initial_password = (set) (uncommitted)
```

4. **Introduzca el comando** `commit`.

Temas relacionados

- [Edición de excepciones de un usuario \(CLI\) \[265\]](#)
- [Edición de autorizaciones de un rol \(CLI\) \[270\]](#)

▼ Edición de excepciones de un usuario (BUI)

Use el siguiente procedimiento para editar excepciones para un usuario.

1. **Vaya a Configuración > Usuarios.**
2. **Mueva el cursor sobre el usuario en la lista Users (Usuarios) y haga clic en el ícono de edición** .
3. **En el cuadro de diálogo Editar usuario, haga clic en Excepciones para agregar o suprimir autorizaciones.**
4. **(Opcional) Agregue autorizaciones para este usuario.**

Consulte [Tabla 43, “Ámbitos, filtros y autorizaciones disponibles para los usuarios y roles”](#).

Repita los siguientes pasos hasta que haya agregado todas las autorizaciones que desee para este usuario:

- a. **Seleccione un ámbito.**

Si hay filtros disponibles para este ámbito, aparecerán debajo del selector Ámbito.

- b. **Especifique los filtros para el ámbito según sea necesario.**
- c. **Haga clic en la casilla de control correspondiente a cada autorización que desea agregar.**
- d. **Haga clic en ADD (Agregar) en la sección Exceptions (Excepciones).**

Las autorizaciones aparecen en la parte inferior de la sección Excepciones.

5. **(Opcional) Suprima autorizaciones para este usuario.**

En la lista de autorizaciones que figuran en la parte inferior de la sección Excepciones, mueva el cursor sobre la autorización que desee suprimir y haga clic en el ícono de papelera .

6. **Haga clic en APPLY (Aplicar) en la parte superior del cuadro de diálogo.**

Temas relacionados

- [“Descripción de usuarios y roles” \[273\]](#)
- [“Autorizaciones de usuarios” \[274\]](#)
- [“Administración de propiedades de usuario” \[278\]](#)

▼ Edición de excepciones de un usuario (CLI)

Use el siguiente procedimiento para editar excepciones para un usuario.

1. **Vaya a `configuration users`.**
2. **Introduzca `select` seguido del nombre de usuario.**
3. **Introduzca `exceptions` y luego `show`.**
4. **(Opcional) Agregue autorizaciones para este usuario.**

Consulte [Tabla 43, “Ámbitos, filtros y autorizaciones disponibles para los usuarios y roles”](#).

Repita los siguientes pasos hasta que haya agregado todas las autorizaciones que desee para este usuario:

- a. **Introduzca `create`.**

- b. Introduzca `set scope=` seguido del nombre del ámbito. Use la finalización con tabulación para ver la lista.
 - c. Introduzca `show` para ver los filtros y, si hay alguna, las autorizaciones disponibles.
 - d. Si hay un filtro disponible, establezca un valor.
Use la finalización con tabulación para ver una lista de posibles valores de filtro.
 - e. Establezca en `true` todas las autorizaciones que desee agregar para este usuario.
 - f. Introduzca el comando `commit`.
5. (Opcional) Suprima autorizaciones para este usuario.
Para cada autorización que desee quitarle a este usuario, introduzca `destroy` y el nombre de la autorización.

```
hostname:configuration users username exceptions> destroy auth-001  
This will destroy "auth-001". Are you sure? (Y/N) y
```
6. Introduzca `done` y luego `done` nuevamente.

Temas relacionados

- [“Descripción de usuarios y roles” \[273\]](#)
- [“Autorizaciones de usuarios” \[274\]](#)
- [“Administración de propiedades de usuario” \[278\]](#)

▼ Agregación de un rol (BUI)

Un rol es una recopilación de autorizaciones que se pueden asignar a un usuario. Realice este procedimiento para crear un nuevo rol.

1. Vaya a **Configuración > Usuarios**.
2. Haga clic en el ícono de agregación  que se encuentra junto a Roles.
A continuación de este procedimiento, consulte también "Método alternativo".

3. **En el cuadro de diálogo Agregar rol, establezca el nombre del rol y escriba una descripción.**
4. **En la sección Autorizaciones, agregue autorizaciones para este rol.**
 Consulte [Tabla 43, “Ámbitos, filtros y autorizaciones disponibles para los usuarios y roles”](#).
 Repita los siguientes pasos hasta que haya agregado todas las autorizaciones que desee para este rol:
 - a. **Seleccione un ámbito.**
 Si hay filtros disponibles para este ámbito, aparecerán debajo del selector Ámbito.
 - b. **Especifique los filtros para el ámbito según sea necesario.**
 - c. **Haga clic en la casilla de control correspondiente a cada autorización que desea agregar.**
 - d. **Haga clic en ADD (Agregar) en la sección Authorizations (Autorizaciones).**
 Las autorizaciones aparecen en la parte inferior de la sección Autorizaciones.
5. **Haga clic en ADD (Agregar) en la parte superior del cuadro de diálogo.**
 El nuevo rol aparece en la lista Roles.

Método alternativo

Para crear un nuevo rol con las mismas autorizaciones que un rol existente, mueva el cursor sobre la entrada del rol existente y haga clic en el ícono de clonación . Escriba un nombre de rol y haga clic en Agregar en la parte superior del cuadro de diálogo Clonar rol.

Temas relacionados

- [“Descripción de usuarios y roles” \[273\]](#)
- [“Autorizaciones de usuarios” \[274\]](#)
- [“Administración de propiedades de usuario” \[278\]](#)

▼ Agregación de un rol (CLI)

Un rol es una recopilación de autorizaciones que se pueden asignar a un usuario. Realice este procedimiento para crear un nuevo rol.

1. **Vaya a `configuration roles`.**
2. **Introduzca `role` seguido del nombre del rol que desee crear.**
3. **Establezca el valor `description` del rol.**
4. **Introduzca `commit` para agregar el rol.**
5. **Seleccione el nuevo rol.**
6. **Introduzca `authorizations`.**
7. **Agregue autorizaciones para este rol.**

Consulte [Tabla 43, “Ámbitos, filtros y autorizaciones disponibles para los usuarios y roles”](#).

Repita los siguientes pasos hasta que haya agregado todas las autorizaciones que desee para este rol:

- a. **Introduzca `create`.**
 - b. **Introduzca `set scope=` seguido del nombre del ámbito. Use la finalización con tabulación para ver la lista.**
 - c. **Introduzca `show` para ver los filtros y, si hay alguna, las autorizaciones disponibles.**
 - d. **Si hay un filtro disponible, establezca un valor.**
Use la finalización con tabulación para ver una lista de posibles valores de filtro.
 - e. **Establezca en `true` todas las autorizaciones que desee incluir en este rol.**
 - f. **Introduzca el comando `commit`.**
8. **Introduzca `done` y luego `done` nuevamente.**

Temas relacionados

- [“Descripción de usuarios y roles” \[273\]](#)
- [“Autorizaciones de usuarios” \[274\]](#)
- [“Administración de propiedades de usuario” \[278\]](#)

▼ Edición de autorizaciones de un rol (BUI)

Un rol es una recopilación de autorizaciones que se pueden asignar a un usuario. Realice el siguiente procedimiento para agregar y suprimir autorizaciones de un rol.

1. **Vaya a Configuración > Usuarios.**
2. **Mueva el cursor sobre el rol en la lista Roles (Roles) y haga clic en el ícono de edición .**
3. **(Opcional) En la sección Autorizaciones del cuadro de diálogo Editar rol, agregue las autorizaciones para este rol.**
 Consulte [Tabla 43, “Ámbitos, filtros y autorizaciones disponibles para los usuarios y roles”](#).
 Repita los siguientes pasos hasta que haya agregado todas las autorizaciones que desee para este rol:
 - a. **Seleccione un ámbito.**
 Si hay filtros disponibles para este ámbito, aparecerán debajo del selector Ámbito.
 - b. **Especifique los filtros para el ámbito según sea necesario.**
 - c. **Haga clic en la casilla de control correspondiente a cada autorización que desea agregar.**
 - d. **Haga clic en ADD (Agregar) en la sección Authorizations (Autorizaciones).**
 Las autorizaciones aparecen en la parte inferior de la sección Autorizaciones.
4. **(Opcional) Suprima autorizaciones para este rol.**
 En la lista de autorizaciones que figuran en la parte inferior de la sección Autorizaciones, mueva el cursor sobre la autorización que desee suprimir y haga clic en el ícono de papelera .
5. **Haga clic en APPLY (Aplicar) en la parte superior del cuadro de diálogo.**

Temas relacionados

- [“Descripción de usuarios y roles” \[273\]](#)
- [“Autorizaciones de usuarios” \[274\]](#)
- [“Administración de propiedades de usuario” \[278\]](#)

▼ Edición de autorizaciones de un rol (CLI)

Un rol es una recopilación de autorizaciones que se pueden asignar a un usuario. Realice el siguiente procedimiento para agregar y suprimir autorizaciones de un rol.

1. **Vaya a `configuration roles`.**
2. **Introduzca `select` seguido del nombre del rol.**
3. **Introduzca `authorizations`.**
4. **(Opcional) Agregue autorizaciones para este rol.**

Consulte [Tabla 43, “Ámbitos, filtros y autorizaciones disponibles para los usuarios y roles”](#).

Repita los siguientes pasos hasta que haya agregado todas las autorizaciones que desee para este rol:

- a. **Introduzca `create`.**
- b. **Introduzca `set scope=` seguido del nombre del ámbito. Use la finalización con tabulación para ver la lista.**
- c. **Introduzca `show` para ver los filtros y, si hay alguna, las autorizaciones disponibles.**
- d. **Si hay un filtro disponible, establezca un valor.**
Use la finalización con tabulación para ver una lista de posibles valores de filtro.
- e. **Establezca en `true` todas las autorizaciones que desee incluir en este rol.**
- f. **Introduzca el comando `commit`.**
5. **(Opcional) Suprima autorizaciones para este rol.**

Para cada autorización que desee quitarle a este rol, introduzca `destroy` y el nombre de la autorización.

```
hostname:configuration roles rolename authorizations> destroy auth-001
This will destroy "auth-001". Are you sure? (Y/N) y
```

6. **Introduzca `done` y luego `done` nuevamente.**

Temas relacionados

- [“Descripción de usuarios y roles” \[273\]](#)
- [“Autorizaciones de usuarios” \[274\]](#)
- [“Administración de propiedades de usuario” \[278\]](#)

▼ Agregación de un usuario que pueda ver solamente el panel de control (BUI)

Use el siguiente procedimiento para agregar un usuario que solo pueda ver el panel de control.

1. **Vaya a Configuración > Usuarios.**
2. **Haga clic en el ícono de agregación  que se encuentra junto a Usuarios.**
3. **En el cuadro de diálogo Agregar usuario, elija Directorio o Local como Tipo de usuario.**
4. **Introduzca valores para Nombre de usuario, Nombre completo y Contraseña.**
Las propiedades Nombre de Usuario y Contraseña son obligatorias. Si necesita ayuda para establecer el valor de Nombre de usuario, consulte [“Descripción de usuarios y roles” \[273\]](#).
5. **Seleccione la casilla de control del usuario de quiosco.**
6. **Asegúrese de que la pantalla Kiosk (Quiosco) esté definida en estado o panel de control.**
7. **Haga clic en Agregar.**

Temas relacionados

- [“Descripción de usuarios y roles” \[273\]](#)
- [“Administración de propiedades de usuario” \[278\]](#)

▼ Agregación de un usuario que pueda ver solamente el panel de control (CLI)

Use el siguiente procedimiento para agregar un usuario que solo pueda ver el panel de control.

1. **Vaya a `configuration users`.**
2. **Introduzca el tipo de usuario `directory` o `local` seguido de un nombre de usuario.**
Para ver las descripciones de los tipos de usuario o si necesita ayuda para establecer el valor de Nombre de usuario, consulte [“Descripción de usuarios y roles” \[273\]](#).
3. **Establezca un valor para `initial_password`.**
4. **Introduzca el comando `commit`.**
5. **Seleccione el nuevo usuario.**
6. **Establezca `kiosk_mode` en `true`.**
7. **Asegúrese de que el valor de `kiosk_screen` sea `status/dashboard`.**
8. **Introduzca el comando `commit`.**

Temas relacionados

- [“Descripción de usuarios y roles” \[273\]](#)
- [“Administración de propiedades de usuario” \[278\]](#)

▼ Determinación del usuario actual conectado

Para ver la identidad del usuario actual conectado, consulte el nombre en la parte superior del panel de control en la BUI o use el comando `whoami` en la CLI.

1. **En la BUI, el nombre completo del usuario se muestra a la izquierda del botón **Cerrar sesión**, en la parte superior del panel de control.**

Full Name@hostname

Si no se proporcionó un nombre completo para el usuario, no se mostrará ninguna identificación del usuario:

@hostname

El nombre completo también puede aparecer en el separador del explorador.

2. **En la CLI, el comando `whoami` devuelve el nombre de inicio de sesión del usuario.**

```
hostname:> whoami
logname
```

Descripción de usuarios y roles

Un usuario es uno de los tipos que se muestran en las siguientes dos tablas. Solo a los tipos de usuario administrador se les pueden asignar autorizaciones o roles.

TABLA 41 Tipos de usuario administrador

Tipo de usuario de BUI	Tipo de usuario de CLI	Descripción
Local	local	■ Este administrador de dispositivos está definido para este dispositivo solamente. ■ El nombre de usuario debe ser un nuevo nombre de usuario de UNIX. ■ Se puede especificar un UID personalizado; de lo contrario, el sistema asignará uno. ■ Se debe especificar una contraseña. ■ A este usuario se le pueden otorgar autorizaciones directamente o mediante la asignación de roles personalizados. ■ Si bien los usuarios locales pueden utilizar servicios de datos, no se admiten grupos locales.
Directorio	directory	■ Este administrador de dispositivos está gestionado por un servicio de directorio: NIS, LDAP o Active Directory (AD). Consulte “Configuración de NIS” [429], “Configuración de LDAP” [393] y “Configuración de Active Directory” [335]. ■ El usuario debe ser un usuario de UNIX NIS/LDAP existente o un usuario de AD <i>name@domain</i>. ■ El ID de usuario y la contraseña se asignan automáticamente y no pueden establecerse. Si se configuran tanto NIS como LDAP en el dispositivo, y los servicios devuelven información diferente para un usuario determinado, el dispositivo utiliza los datos proporcionados por NIS. ■ A este usuario se le pueden otorgar autorizaciones directamente o mediante la asignación de roles personalizados.

TABLA 42 Tipos de usuario no administrador

Tipo de usuario de BUI	Tipo de usuario de CLI	Descripción
Solo datos	data	■ Un usuario de solo datos se define localmente para los datos (SMB, NFS, FTP) sin acceso de administrador. ■ El nombre de usuario debe ser un nuevo nombre de usuario de UNIX. ■ Se puede especificar un UID personalizado; de lo contrario, el sistema asignará uno. ■ Se debe especificar una contraseña.
Sin inicio de sesión	nologin	■ Un usuario sin inicio de sesión no puede iniciar sesión en el dispositivo. Se reservan un nombre de usuario y un UID con fines de asignación de identidad. ■ El nombre de usuario debe ser un nuevo nombre de usuario de UNIX.

Tipo de usuario de BUI	Tipo de usuario de CLI	Descripción
		Se puede especificar un UID personalizado; de lo contrario, el sistema asignará uno.

Un rol es una recopilación de autorizaciones que se pueden asignar a un tipo de usuario administrador. Los usuarios administradores tienen asignado el rol "básico" por defecto. El rol básico le permite al usuario iniciar sesión en la interfaz administrativa y leer la mayoría de los parámetros de configuración del sistema. El rol básico no le permite al usuario hacer cambios en el sistema. A un usuario se le pueden asignar roles adicionales y autorizaciones adicionales directamente. Es posible editar un rol para agregar o suprimir autorizaciones.

Usar roles es más seguro que proporcionar a los usuarios la contraseña de usuario raíz.

- Los roles permiten otorgar fácilmente a los usuarios solo el juego de autorizaciones que necesitan. Por ejemplo, diferentes roles pueden tener autorizaciones para modificar distintos servicios.
- Dado que los usuarios están trabajando con su propio nombre de usuario, es posible identificar fácilmente qué persona realizó una determinada acción.

Temas relacionados

- “Administración de propiedades de usuario” [278]
- “Autorizaciones de usuarios” [274]
- Adición de un administrador o usuario: [BUI](#), [CLI](#)
- Cambio de una contraseña de usuario: [BUI](#), [CLI](#)
- Edición de excepciones para un usuario: [BUI](#), [CLI](#)
- Adición de un rol: [BUI](#), [CLI](#)
- Edición de autorizaciones para un rol: [BUI](#), [CLI](#)
- Agregación de un usuario que pueda ver solamente el panel de control: [BUI](#), [CLI](#)

Autorizaciones de usuarios

Las autorizaciones permiten a los usuarios realizar tareas específicas, por ejemplo, crear recursos compartidos, reiniciar el dispositivo y actualizar el software del sistema.

Las autorizaciones se agrupan en ámbitos. Un determinado ámbito puede tener un juego de filtros para limitar el ámbito de la autorización. Por ejemplo, en lugar de otorgar una autorización para reiniciar todos los servicios, se puede usar un filtro para que la autorización permita reiniciar el servicio HTTP solamente.

En la siguiente tabla, se muestran las autorizaciones disponibles.

TABLA 43 Ámbitos, filtros y autorizaciones disponibles para los usuarios y roles

BUI de ámbito	CLI de ámbito	Filtros	Authorizations
Active Directory	ad	Nombre de dominio o grupo de trabajo	■ Unirse a un dominio de Active Directory. ■ Unirse a un grupo de trabajo
Alertas	alerta	-	■ Crear acciones de alerta personalizada o alertas de umbral ■ Publicar alertas personalizadas
Análisis	stat	Lista de detalles	■ Configurar política de consulta de nombre de host de análisis ■ Crear una estadística con este detalle ■ Leer una estadística con este detalle.
Aplicación	appliance	Nombre de dispositivo	■ Emitir una entrada de log de auditoría ■ Restaurar el dispositivo a valores de fábrica ■ Apagar el dispositivo ■ Reiniciar el dispositivo. ■ Modificar el nombre del dispositivo ■ Acceder al shell subyacente de Solaris ■ Ver certificados de sistema ■ Configurar certificados de confianza ■ Suspender todas las notificaciones
Destinos de nube	nube	Nombre del destino de nube	■ Copia de seguridad de los datos de una instantánea en la nube ■ Suprimir las instantáneas de nube ■ Restaurar las copias de seguridad en la nube en recursos compartidos locales
Agrupación en clusters	cluster	-	■ Realizar failback de recursos a un par de cluster. ■ Restablecer un dispositivo de E/S de cluster con error ■ Recuperar recursos de un par de cluster ■ Transferir recursos a un par de cluster
Conjuntos de datos	dataset	-	Configurar políticas de retención de juego de datos
Hardware	hardware	-	■ Discos en línea y sin conexión. ■ Configurar LED en discos, dispositivos y contenedores externos ■ Configurar propiedades de red para procesador de servicio ■ Eliminar una unidad como disco de reserva ■ Configurar una agrupación de almacenamiento ■ Desconfigurar una agrupación de almacenamiento

BUI de ámbito	CLI de ámbito	Filtros	Authorizations
			■ Producir fallos en disco manualmente
Almacenes de claves	keystore	Nombre de almacén de claves	■ Listar claves presentes en un almacén de claves por usuario ■ Permitir modificaciones de almacén de claves ■ Permitir acceso de lectura a valores sensibles en un almacén de claves
Red	net	-	Configurar dispositivos de red, enlaces de datos e interfaces.
Proyectos y recursos compartidos	nas	■ Agrupación de almacenamiento ■ Proyecto ■ Recurso compartido	■ Realizar copia de seguridad de datos de recursos compartidos ■ Configurar quién puede acceder a un recurso compartido ■ Cambiar propiedades generales en recurso compartido ■ Configurar propiedades específicas de protocolo ■ Cambiar cuota y reserva en recurso compartido ■ Cambiar cuotas de usuario y de grupo en recurso compartido ■ Borrar bloqueos mantenidos en representación de cliente NFS ■ Clonar una instantánea a un sistema de archivos normal ■ Crear un proyecto ■ Crear un sistema de archivos o LUN ■ Eliminar un proyecto o recurso compartido ■ Extraer una instantánea ■ Gestionar claves de cifrado para una agrupación, un proyecto o un recurso compartido ■ Promover clon ■ Renombrar un proyecto o recurso compartido ■ Cambiar nombre a instantánea ■ Restaurar datos en el recurso compartido ■ Revertir un sistema de archivos a una instantánea anterior ■ Configurar la replicación de datos en otros dispositivos ■ Gestionar datos replicados desde otros dispositivos ■ Configurar un programa recurrente de instantáneas

BUI de ámbito	CLI de ámbito	Filtros	Authorizations
			■ Verificar si existen errores en una agrupación de almacenamiento ■ Gestionar la migración shadow en un recurso compartido ■ Realizar una instantánea manual
Roles	rol	Nombre de rol	■ Configurar autorizaciones para un rol. ■ Cambiar una descripción de un rol ■ Crear rol ■ Destruir rol
SAN	stmf	-	Configurar destinos y hosts de SAN
Servicios	svc	Nombre de servicio	■ Activar o desactivar servicio ■ Configurar propiedades y configuraciones de servicio ■ Reiniciar servicio
Esquema de propiedades de recursos compartidos	schema	-	Modificar esquema de propiedades.
Actualizar	update	-	■ Suprimir software del sistema ■ Actualizar software del sistema. ■ Cargar actualizaciones del sistema
Usuarios	user	Nombre de usuario	■ Configurar autorizaciones para un usuario ■ Cambiar una contraseña. ■ Configurar preferencias para un usuario ■ Configurar propiedades para un usuario ■ Configurar roles para un usuario ■ Crear un usuario ■ Destruir un usuario
Flujo de trabajo	workflow	■ Propietario ■ Name	■ Suprimir flujo de trabajo ■ Ejecutar flujo de trabajo
Hoja de trabajo	worksheet	■ Propietario ■ Name	■ Modificar hoja de trabajo ■ Leer hoja de trabajo

Temas relacionados

- Adición de un administrador o usuario: [BUI](#), [CLI](#)
- Edición de excepciones para un usuario: [BUI](#), [CLI](#)
- Adición de un rol: [BUI](#), [CLI](#)
- Edición de autorizaciones para un rol: [BUI](#), [CLI](#)

Administración de propiedades de usuario

En la página Configuración > Usuarios, se muestran los usuarios y los roles. Mueva el cursor sobre una entrada a fin de ver los botones para clonar, editar y destruir que corresponden al usuario o rol. Haga doble clic en un usuario o rol, o haga clic en el ícono de edición , para ver el cuadro de diálogo Editar usuario o Editar rol. En la siguiente tabla, se describen los botones de esta página.

TABLA 44 Botones de la página Usuarios de la BUI

Botón	Descripción
	Permite agregar un usuario o rol nuevos. Se visualiza un nuevo cuadro de diálogo Agregar usuario o Agregar rol, donde puede introducir los valores de las propiedades.
	Permite abrir un cuadro de búsqueda. Escriba una cadena de búsqueda para ver solamente entradas de usuario o de rol donde aparezca ese texto de búsqueda. Haga clic nuevamente en el botón de búsqueda o en Mostrar todo en la parte superior de la lista para ver la lista completa.
	Permite clonar un usuario o un rol. Agregue un nuevo usuario o rol con las mismas autorizaciones que el usuario o rol clonados.
	Permite editar un usuario o un rol.
	Permite eliminar un usuario, un rol o una autorización.

Según el tipo de usuario, todas las siguientes propiedades se pueden configurar cuando se agrega un usuario. Puede configurar un subconjunto de estas propiedades al editar un usuario.

TABLA 45 Propiedades de usuario

Propiedad de la BUI	Propiedad de la CLI	Descripción
Tipo	type	Para obtener una descripción de los tipos de usuario, consulte “Descripción de usuarios y roles” [273] .
Nombre de usuario	logname	Nombre de inicio de sesión único del usuario.
ID usuario	uid	Activado para usuarios locales, de datos y sin inicio de sesión. Puede especificar el ID de usuario o permitir que el sistema lo asigne. Si usted especifica el ID de usuario, este no podrá ser menor que 100 ni mayor que 2147483646, y no podrá ser igual a 60001, 60002 o 65534. Esos UID están reservados por el proveedor del sistema operativo para el uso en aplicaciones futuras. Los usuarios finales del sistema y los proveedores de productos en capas no pueden utilizarlos ya que, si lo hicieran, se podrían producir problemas de seguridad con otras aplicaciones.
Nombre completo	fullname	Nombre completo o nombre real del usuario. En la BUI, el nombre completo se muestra a la izquierda del botón Cerrar sesión, en la

Propiedad de la BUI	Propiedad de la CLI	Descripción
		parte superior del panel de control, y también puede aparecer en la ficha del explorador.
Password/Confirm	initial_password	Para usuarios locales y de datos, escriba la contraseña inicial en estos campos.
Require session annotation (Requerir anotación de sesión)	require_annotation	Si está activado: ■ BUI: el usuario debe introducir un comando antes de visualizar la página de BUI inicial. ■ CLI: el usuario debe introducir un comando antes de visualizar el símbolo del sistema de la CLI. ■ REST: se produce un error en las solicitudes por falta de autorización. El comentario aparece en el log de auditoría. Esta anotación se puede usar para describir el propósito del inicio de sesión. Puede usarse un número de ticket para efectuar el seguimiento del trabajo de un proyecto en particular.
Kiosk user (Usuario de quiosco)	kiosk_mode	Cuando está activado, este usuario es de tipo quiosco. ■ BUI: el usuario solo puede visualizar la pantalla con el valor de la propiedad "Pantalla de quiosco". ■ CLI: se produce un error en el inicio de sesión. ■ REST: se produce un error en las solicitudes por falta de autorización.
Kiosk screen (Pantalla de quiosco)	kiosk_screen	Pantalla a la que está restringido este usuario si se activa el usuario de quiosco o si la propiedad kiosk_mode es true. Por defecto: status/dashboard
Roles	roles	Roles asignados a un usuario de directorio o local.
Excepciones	exceptions	Autorizaciones adicionales asignadas a un usuario de directorio o local, o las limitaciones en las autorizaciones asignadas a un rol.
-	preferences	Preferencias del entorno de usuario, como la configuración regional, la página de inicio de la BUI, los tiempos de espera excedidos, las claves públicas SSH y los tokens de inicio de sesión en REST. Consulte “Configuración de preferencias del dispositivo” [280] .

Las siguientes propiedades se pueden configurar cuando se crea o se edita un rol.

TABLA 46 Propiedades de roles

Propiedad de la BUI	Propiedad de la CLI	Descripción
Nombre	name	Nombre del rol como aparecerá en las listas.
Descripción	description	Descripción detallada del rol.
Authorizations	authorizations	Autorizaciones para este rol.

Temas relacionados

- Adición de un administrador o usuario: [BUI](#), [CLI](#)
- Cambio de una contraseña de usuario: [BUI](#), [CLI](#)
- Edición de excepciones para un usuario: [BUI](#), [CLI](#)
- Adición de un rol: [BUI](#), [CLI](#)
- Edición de autorizaciones para un rol: [BUI](#), [CLI](#)
- Agregación de un usuario que pueda ver solamente el panel de control: [BUI](#), [CLI](#)

Configuración de preferencias del dispositivo

En esta sección, se describe la forma de configurar las preferencias de usuario, como la localidad, las propiedades de sesión, los análisis avanzados y las claves SSH.

- La BUI solo permite establecer las preferencias del usuario con el que se inició la sesión actual.
- La CLI permite establecer las preferencias de cualquier usuario para el que se tenga la autorización apropiada.

Para configurar las preferencias de usuario, use las siguientes secciones:

- Definición de preferencias: [BUI](#), [CLI](#)
- Configuración de claves SSH públicas: [BUI](#), [CLI](#)
- “[Propiedades de preferencias](#)” [285]

▼ Definición de preferencias (BUI)

Utilice este procedimiento para establecer las preferencias del usuario con el que inició la sesión actual.

Para cambiar las preferencias de un usuario distinto al que usó para iniciar sesión, consulte [Establecimiento de preferencias \(CLI\)](#) [281].

1. Vaya a Configuración > Preferencias.

General

Initial login screen `https://ar7320-230:215/#status/dashboard`

Locality `C`

Session timeout `15` minutes

Current session annotation [Edit..](#)

Make available advanced analytics statistics ☐

2. Establezca los valores de las preferencias.

Consulte [“Propiedades de preferencias” \[285\]](#) para ver las descripciones.

Por defecto, el explorador cierra automáticamente la sesión de la BUI después de 15 minutos de inactividad del usuario. Para definir otro límite, especifique un entero positivo diferente en Timeout de sesión.

Por defecto, no existe un límite para el tiempo que la CLI puede estar inactiva (*infinite*). Para definir un límite sobre la cantidad de tiempo que la CLI puede estar inactiva, introduzca un entero positivo para el timeout de inactividad de la CLI y seleccione la unidad de tiempo en el menú. Al alcanzar el límite de timeout, se cierra la CLI.

Para obtener más información sobre las claves SSH públicas, consulte [Configuración de claves SSH públicas \(BUI\) \[283\]](#).

3. Haga clic en Aplicar.

Temas relacionados

- [Agregación de un administrador o usuario \(BUI\) \[258\]](#)
- [Establecimiento de preferencias \(CLI\) \[281\]](#)
- [“Propiedades de preferencias” \[285\]](#)
- [Configuración de claves SSH públicas \(BUI\) \[283\]](#)

▼ Establecimiento de preferencias (CLI)

Utilice este procedimiento para establecer las preferencias del usuario que usó para iniciar la sesión actual o de cualquier usuario para el que se tenga la autorización `changePreferences`.

Consulte [“Autorizaciones de usuarios” \[274\]](#) y Edición de excepciones para un usuario (BUI, CLI) para obtener información sobre cómo adquirir la autorización `changePreferences`.

1. Vaya a `configuration users`.

```
hostname:> configuration users
```

2. Seleccione el usuario para el que desea editar las preferencias.

a. Introduzca `show` para ver los usuarios.

A fin de editar las preferencias de un usuario distinto al que usó para iniciar la sesión actual, debe tener la autorización `changePreferences` para ese usuario.

b. Utilice el nombre en la columna **NOMBRE DE USUARIO:**

```
hostname:configuration users> select username
```

3. Introduzca `preferences y, a continuación, show` para ver las preferencias.

Tenga en cuenta que la propiedad `session_annotation` solamente se muestra para el usuario con el que se inició la sesión actual.

```
hostname:configuration users username> preferences
hostname:configuration users username preferences> show
Properties:
    locale = C
    login_screen = status/dashboard
    session_timeout = 15
    cli_idle_timeout = infinite (default)
    session_annotation =
    advanced_analytics = false
```

Children:

```
    keys => Manage SSH public keys
    tokens => Manage REST tokens
```

4. Establezca los valores de las preferencias.

Consulte [“Propiedades de preferencias” \[285\]](#) para ver las descripciones.

Por defecto, el explorador cierra automáticamente la sesión de la BUI después de 15 minutos de inactividad del usuario. Para definir otro límite, especifique un entero positivo diferente en `session_timeout`.

Por defecto, no existe un límite para el tiempo que la CLI puede estar inactiva (`infinite`). Para definir un límite sobre la cantidad de tiempo que la CLI puede estar inactiva, establezca un valor como 15 minutos o 1 hora en `cli_idle_timeout`. Las unidades de tiempo por defecto son segundos, así que, si introduce un valor de 1800 (sin especificar una unidad), el valor de `timeout` es 1800 segundos o 30 minutos. Al alcanzar el límite de `timeout`, se cierra la CLI. Para desactivar el `timeout`, defina el valor de `cli_idle_timeout` en `infinite` o especifique el siguiente comando:

```
hostname:configuration preferences> unset cli_idle_timeout
cli_idle_timeout = infinite (default, uncommitted)
```

Para obtener más información sobre keys, consulte [Configuración de claves SSH públicas \(CLI\) \[284\]](#).

5. **Introduzca el comando** `commit`.
6. **Escriba** `done`.
7. **(Opcional) Como alternativa, puede usar** `configuration preferences`.
Este método solamente permite establecer las preferencias del usuario con el que se inició la sesión actual.
 - a. **Vaya a** `configuration preferences`.
 - b. **Introduzca** `show`.
 - c. **Establezca los valores de las preferencias, introduzca** `commit` **e introduzca** `done`.

Temas relacionados

- [Agregación de un administrador o usuario \(CLI\) \[260\]](#)
- [“Propiedades de preferencias” \[285\]](#)
- [Configuración de claves SSH públicas \(CLI\) \[284\]](#)

▼ Configuración de claves SSH públicas (BUI)

Las claves SSH públicas se pueden usar para permitir conexiones SSH sin usar contraseñas. Esta función es útil para la comodidad del administrador y para la ejecución automatizada de secuencias de comandos.

Utilice este procedimiento para establecer las claves SSH públicas del usuario con el que inició la sesión actual.

Para definir las claves de un usuario distinto al que usó para iniciar la sesión actual, consulte [Configuración de claves SSH públicas \(CLI\) \[284\]](#).

1. **Vaya a Configuración > Preferencias.**

2. Haga clic en el ícono de agregación  que se encuentra junto a Claves SSH públicas.
3. Seleccione un valor para Tipo y, a continuación, escriba la clave SSH pública y un comentario de clave.
4. Haga clic en Agregar.

Temas relacionados

- [Definición de preferencias \(BUI\) \[280\]](#)
- [Configuración de claves SSH públicas \(CLI\) \[284\]](#)
- [“Propiedades de preferencias” \[285\]](#)
- [“Configuración de SSH” \[469\]](#)

▼ Configuración de claves SSH públicas (CLI)

Las claves SSH públicas se pueden usar para permitir conexiones SSH sin usar contraseñas. Esta función es útil para la comodidad del administrador y para la ejecución automatizada de secuencias de comandos.

Utilice este procedimiento para establecer las claves SSH públicas del usuario que usó para iniciar la sesión actual o de cualquier usuario para el que se tenga la autorización `changePreferences`. Consulte [“Autorizaciones de usuarios” \[274\]](#) y Edición de excepciones para un usuario ([BUI](#), [CLI](#)) para obtener información sobre cómo adquirir la autorización `changePreferences`.

1. **Vaya a `configuration users`.**
2. **Seleccione el usuario para el que desea editar las preferencias.**

```
hostname:configuration users> select username
```
3. **Introduzca `preferences keys` y, a continuación, `show` para ver las claves SSH existentes.**

```
hostname:configuration users username> preferences keys  
hostname:configuration users username preferences keys> show
```
4. **Configure una clave SSH.**
Introduzca `create` para crear una clave SSH nueva.

Establezca los valores de `type` (DSA o RSA), `key` y (opcionalmente) `comment` para definir el propósito de esta clave.

5. Introduzca el comando `commit`.

Introduzca `show` para ver la clave nueva.

6. Escriba `done`.

7. (Opcional) Como alternativa, puede usar `configuration preferences`.

Este método solamente permite crear claves SSH para el usuario con el que se inició la sesión actual.

a. **Vaya a `configuration preferences keys`.**

b. **Introduzca `create`.**

c. **Establezca los valores de `type`, `key` y (opcionalmente) `comment`.**

d. **Introduzca `commit`, `show` y `done`.**

Temas relacionados

- [Establecimiento de preferencias \(CLI\) \[281\]](#)
- [“Propiedades de preferencias” \[285\]](#)
- [“Configuración de SSH” \[469\]](#)

Propiedades de preferencias

En la siguiente tabla, se describen las propiedades para configurar las preferencias de usuario.

TABLA 47 Propiedades de preferencias

Propiedad de la BUI	Propiedad de la CLI	Descripción
Pantalla de inicio de sesión inicial	<code>login_screen</code>	La página de la BUI que se presenta después de iniciar sesión correctamente si no se especifica una página en la URL. Por defecto, esta página es el panel de control de estado (<code>status/dashboard</code>). La pantalla que se presenta antes de iniciar sesión contiene una petición de datos de inicio de sesión del sistema y un mensaje opcional del

Propiedad de la BUI	Propiedad de la CLI	Descripción
		sistema. Consulte “Mensaje de inicio de sesión del sistema” en “ Propiedades y logs de la identidad del sistema ” [476].
Localidad	locale	Por defecto, es C. Las localidades C y POSIX admiten solo caracteres ASCII o texto sin formato. ISO 8859-1 admite los siguientes idiomas: afrikáans, euskera, catalán, danés, holandés, inglés, feroés, finlandés, francés, gallego, alemán, islandés, irlandés, italiano, noruego, portugués, español y sueco.
Timeout de sesión	session_timeout	La cantidad de minutos hasta que el explorador cierra automáticamente la sesión después de que el usuario sale de la BUI.
Timeout de inactividad de la CLI	cli_idle_timeout	La cantidad de tiempo que la CLI puede estar inactiva antes de que se detenga la sesión. El valor por defecto, <i>infinite</i> , implica que la CLI no se cerrará automáticamente cuando esté inactiva.
Anotación de sesión actual	session_annotation	Texto de anotación agregado a los logs de auditoría.
Estadísticas de análisis avanzado	advanced_analytics	Se muestran estadísticas adicionales en Análisis.
Claves SSH públicas	keys	Claves RSA/DSA públicas. Es posible asociar comentarios de texto con las claves para ayudar a los administradores a llevar un control del motivo por el que se agregaron.
Tokens de REST	tokens	Los tokens persistentes y no persistentes de inicio de sesión en REST. Defina el token name, establezca preserve en verdadero o falso, y establezca el token expiration en segundos.

Configuración de alertas

Los eventos importantes del dispositivo, como los fallos de hardware y software, disparan alertas. Las alertas aparecen en los logs de alertas.

En esta sección, se describe cómo realizar las siguientes tareas:

- [Agregación de acciones de alerta](#)
 - Configure acciones de alerta adicionales (respuestas a eventos de alerta) para los eventos del sistema especificados.
 - Configure acciones de alerta para los eventos definidos en un flujo de trabajo. Además de las mismas acciones de alerta que puede especificar para eventos del sistema, estas acciones de alerta permiten proporcionar información que el sistema brinda para eventos del sistema, por ejemplo, el efecto que este evento tiene en el sistema y la acción recomendada que debe realizar el administrador.

- Agregue una acción de alerta para alertas de umbral en eventos de estadística específicos.
- [Agregación de alertas de umbral](#)
Cree alertas de umbral para estadísticas de análisis específicas.

Agregación de acciones de alerta

Una acción de alerta es una respuesta a un evento de alerta. Los procedimientos en esta sección describen cómo seleccionar uno o varios eventos y especificar respuestas a alertas para esos eventos. Algunos ejemplos de respuestas a alertas son enviar un correo electrónico, reanudar un juego de datos o ejecutar un flujo de trabajo. Puede especificarse más de una acción de alerta para cualquier alerta de evento en particular.

Para crear acciones de alerta, utilice los siguientes temas:

- Agregación de una acción de alerta: [BUI](#), [CLI](#)
- Agregación de una acción de alerta para un evento definido en un flujo de trabajo: [BUI](#), [CLI](#)
- Agregación de una acción para una alerta de umbral específica: [BUI](#), [CLI](#)
- “Categorías de eventos de alerta” [297]
- “Tipos de acciones de alerta” [298]

▼ Agregación de una acción de alerta (BUI)

Seleccione uno o varios eventos y, a continuación, seleccione respuestas a alertas para esos eventos. Puede especificarse más de una acción de alerta para una alerta de evento en particular.

1. **Navegue hasta Configuración > Alertas.**
2. **Haga clic en el ícono  de agregación en el título del separador Acciones de alerta.**

3. **En la sección Eventos del cuadro de diálogo, seleccione el evento Categoría.**

Al seleccionar la categoría, se mostrarán los eventos incluidos en esa categoría, a excepción de Personalizado. Seleccione uno de estos procedimientos:

- **Todos los eventos.**

Seleccione Todo (Todos los eventos) o Subjuego. Si selecciona Subjuego, alterne entre las distintas casillas de control de los eventos a fin de que queden marcados solo los tipos de

eventos (como alertas de servicios o fallos de hardware) para los que desee realizar esta acción de alerta.

■ **Una categoría específica, como Eventos de hardware o Servicios.**

Seleccione Todo (Todos los eventos de esta categoría) o Subjuego. Si selecciona Subjuego, alterne entre las distintas casillas de control de los eventos para que queden marcados solo los eventos para los que desee realizar esta acción de alerta.

La categoría Análisis permite seleccionar eventos de alto nivel, como advertencia de suspensión automática de juegos de datos, memoria total excedida y uso excedido. Para definir una alerta de una condición de umbral para una estadística específica, consulte [Agregación de una alerta de umbral \(BUI\) \[300\]](#).

La categoría Umbrales no permite especificar eventos de umbral para una estadística específica. La categoría Umbrales permite seleccionar eventos de alto nivel, como un umbral de estadística infringido. La configuración de acciones de alerta para estos eventos de umbral de alto nivel puede ser adecuada para no tener que configurar una acción de alerta por separado para cada alerta de evento de umbral de estadística específica que defina. Para definir una acción de alerta específica de un evento de umbral de estadística específico, agregue una acción de alerta de umbral en [Agregación de una acción para una alerta de umbral específica \(BUI\) \[294\]](#).

■ **Personalizado.**

Esta selección permite especificar una acción de alerta para un evento que se define en un flujo de trabajo. Consulte [Agregación de una acción de alerta para un evento definido en un flujo de trabajo \(BUI\) \[291\]](#).

4. En la sección Acciones de alerta del cuadro de diálogo, seleccione la acción que debe realizarse al enviar esta alerta de evento.

La mayoría de las acciones tienen argumentos. Por ejemplo, es posible que deba especificar un destinatario de correo electrónico o seleccionar un juego de datos o un flujo de trabajo.

5. (Opcional) Seleccione el botón Probar para crear una alerta de prueba y ejecutar esta acción de alerta.

Una prueba puede ser útil para comprobar si el correo electrónico o el servicio SNMP están configurados correctamente, por ejemplo.

6. (Opcional) Para especificar acciones adicionales para esta alerta de evento, haga clic en el ícono de agregación en el título de la sección Acciones de alerta.

Seleccione la acción y especifique los argumentos.

7. Haga clic en el botón Agregar en la parte superior derecha del cuadro de diálogo.

Pasos siguientes

Para modificar una acción de alerta, haga doble clic o desplácese sobre ella, haga clic en el ícono de edición , realice los cambios y haga clic en el botón Aplicar.

Para suprimir una acción de alerta, desplácese sobre ella, haga clic en el ícono para suprimir  y confirme que desea suprimir esta acción de alerta.

Temas relacionados

- [“Categorías de eventos de alerta” \[297\]](#)
- [“Tipos de acciones de alerta” \[298\]](#)
- [Agregación de una alerta de umbral \(BUI\) \[300\]](#)
- [Agregación de una acción para una alerta de umbral específica \(BUI\) \[294\]](#)
- [“Creación y publicación de alertas personalizadas dentro de un flujo de trabajo” \[853\]](#)

▼ Agregación de una acción de alerta (CLI)

Especifique uno o varios eventos y, a continuación, especifique respuestas a alertas para esos eventos. Puede especificarse más de una acción de alerta para una alerta de evento en particular.

1. **Vaya a `configuration alerts actions` e introduzca el comando `create`.**

```
hostname:configuration alerts actions> create
```

2. **Defina la propiedad `category`.**

Consulte [Tabla 48, “Categorías de eventos de acciones de alerta”](#) o introduzca el comando `set category=` seguido del carácter de tabulación para ver la lista de categorías de eventos disponibles.

Especifique una de las siguientes opciones:

- **La categoría `a11`.**

Introduzca `show` para ver la lista de eventos en esta categoría. Por defecto, todos los eventos están definidos como `true`, por lo que la acción de alerta se realizará para todos los eventos de la categoría. Si esta acción de alerta debe realizarse solo para un subjuego de eventos, defina en `false` los eventos que no deben disparar esta acción de alerta.

- **Una categoría específica, como `hardware_faults` o `smf`.**

Introduzca `show` para ver la lista de eventos en esta categoría. Por defecto, todos los eventos están definidos como `true`, por lo que la acción de alerta se realizará para todos los eventos

de la categoría. Si la acción de alerta debe realizarse solo para un subjuego de eventos, defina en `false` los eventos que no deben disparar esta acción de alerta.

La categoría `analytics` permite seleccionar eventos de alto nivel, como juegos de datos de advertencias suspendidas automáticamente, memoria total excedida y uso excedido. Para definir una alerta de una condición de umbral para una estadística específica, consulte [Agregación de una alerta de umbral \(CLI\) \[302\]](#).

La categoría `thresholds` *no* permite especificar eventos de umbral. La categoría `thresholds` requiere la especificación de una alerta de evento de umbral existente. Para definir una alerta de una condición de umbral para una estadística específica, consulte [Agregación de una alerta de umbral \(CLI\) \[302\]](#). Para definir una acción de alerta específica para un evento de umbral de estadística específico, agregue una acción de alerta de umbral en [Agregación de una acción para una alerta de umbral específica \(CLI\) \[295\]](#). Para definir una acción de alerta para eventos de umbral de alto nivel, como la infracción de un umbral de estadística, utilice la categoría `Umbrales` en el procedimiento de la BUI [Agregación de una acción de alerta \(BUI\) \[287\]](#).

■ La categoría `custom`.

La categoría `custom` permite definir una acción de alerta para un evento que se define en un flujo de trabajo. Consulte [Agregación de una acción de alerta para un evento definido en un flujo de trabajo \(CLI\) \[293\]](#).

3. **Introduzca el comando `commit`.**
4. **Introduzca el comando `list` para ver la lista de todas las acciones de alerta configuradas.**

La nueva acción de alerta debe estar en la parte inferior de la lista y debe tener un nombre (`actions-###`) y una categoría, pero no una acción ni un controlador.

5. **Seleccione la nueva acción de alerta.**

```
hostname:configuration alerts actions> select actions-001
hostname:configuration alerts actions-001>
```

6. **Configure el controlador de la alerta.**

Introduzca `action` y, a continuación, introduzca `get`.

```
hostname:configuration alerts actions-001> action
hostname:configuration alerts actions-001 action (uncommitted)> get
      handler = email
      address = (unset)
      subject = (unset)
```

El controlador por defecto es `email`. Si quiere utilizar otro controlador, introduzca el comando `set handler=` seguido de un carácter de tabulación para ver la lista de posibles controladores.

7. Defina valores para todos los argumentos del controlador.

Introduzca nuevamente el comando `get` para ver la lista de argumentos, si los hay, para el controlador especificado.

La mayoría de las acciones tienen argumentos. Por ejemplo, es posible que deba especificar un destinatario de correo electrónico, un juego de datos o un flujo de trabajo.

8. Introduzca el comando `commit`.

Introduzca el comando `list` para confirmar que la acción es correcta.

9. Escriba `done`.

Introduzca el comando `list` para ver la lista de acciones.

Pasos siguientes

Para cambiar los eventos incluidos en esta acción de alerta, introduzca el comando `select actions-###`, defina los eventos en `true` o `false`, e introduzca el comando `commit`.

Para especificar acciones adicionales en esta acción de alerta, introduzca el comando `select actions-###` y repita los pasos 6 a 9. Las acciones adicionales se muestran en líneas individuales para las instancias de `actions-###` especificadas.

Para suprimir una acción de alerta, introduzca el comando `destroy actions-###` y luego `y` para confirmar.

Temas relacionados

- [“Categorías de eventos de alerta” \[297\]](#)
- [“Tipos de acciones de alerta” \[298\]](#)
- [Agregación de una alerta de umbral \(CLI\) \[302\]](#)
- [Agregación de una acción para una alerta de umbral específica \(CLI\) \[295\]](#)
- [“Creación y publicación de alertas personalizadas dentro de un flujo de trabajo” \[853\]](#)

▼ Agregación de una acción de alerta para un evento definido en un flujo de trabajo (BUI)

Esta acción de alerta se realiza cuando se invoca la función `postalert` en un flujo de trabajo y se especifica el UUID de esta acción de alerta. Para obtener más información, consulte [“Creación y publicación de alertas personalizadas dentro de un flujo de trabajo” \[853\]](#).

Antes de empezar Para realizar este procedimiento, debe tener la autorización `configure` de la opción `Alertas`.

1. **Navegue hasta Configuración > Alertas.**
2. **Haga clic en el ícono  de agregación en el título del separador Acciones de alerta.**
3. **En la sección Eventos del cuadro de diálogo, seleccione la categoría de evento Personalizado.**
4. **Seleccione la gravedad del evento que precipitó esta acción de alerta: menor, grave o crítico.**
5. **Introduzca una breve descripción del evento que precipitó esta acción de alerta.**
6. **(Opcional) Complete los campos Respuesta, Impacto y Acción recomendada.**

Respuesta	Cadena que describe las acciones que realizará el sistema para mitigar los efectos de este evento.
Impacto	Cadena que describe el efecto que este evento tiene sobre el dispositivo.
Acción recomendada	Cadena que describe las acciones que debe realizar el administrador para mitigar los efectos de este evento.

7. **En la sección Acciones de alerta del cuadro de diálogo, seleccione la acción que debe realizarse al enviar esta alerta de evento.**

La mayoría de las acciones tienen argumentos. Por ejemplo, es posible que deba especificar un destinatario de correo electrónico o seleccionar un juego de datos o un flujo de trabajo.
8. **(Opcional) Para especificar acciones adicionales para esta alerta de evento, haga clic en el ícono de agregación en el título de la sección Acciones de alerta.**

Seleccione la acción y especifique los argumentos.
9. **Haga clic en el botón Agregar en la parte superior derecha del cuadro de diálogo.**

Temas relacionados

- [Agregación de una acción de alerta \(BUI\) \[287\]](#)
- [“Categorías de eventos de alerta” \[297\]](#)
- [“Tipos de acciones de alerta” \[298\]](#)

▼ Agregación de una acción de alerta para un evento definido en un flujo de trabajo (CLI)

Esta acción de alerta se realiza cuando se invoca la función `postalert` en un flujo de trabajo y se especifica el UUID de esta acción de alerta. Para obtener más información, consulte [“Creación y publicación de alertas personalizadas dentro de un flujo de trabajo” \[853\]](#).

Antes de empezar Para realizar este procedimiento, debe tener la autorización `alert allow_configure`.

1. **Vaya a `configuration alerts actions` e introduzca el comando `create`.**
2. **Defina la propiedad `category` con el valor `custom`.**
3. **Defina la propiedad `severity` del evento que precipitó esta acción de alerta: `Critical`, `Major` o `Minor`.**
4. **En `description`, agregue una breve descripción del evento que precipitó esta acción de alerta.**
5. **(Opcional) Defina los campos `response`, `impact` y `recommended_action`.**

`response` Cadena que describe las acciones que realizará el sistema para mitigar los efectos de este evento.

`impact` Cadena que describe el efecto que este evento tiene sobre el dispositivo.

`recommended_action` Cadena que describe las acciones que debe realizar el administrador para mitigar los efectos de este evento.

6. **Introduzca el comando `commit`.**
7. **Introduzca el comando `list` para ver la lista de todas las acciones de alerta configuradas.**
La nueva acción de alerta debe estar en la parte inferior de la lista y debe tener un nombre (`actions-###`) y una categoría, pero no una acción ni un controlador.
8. **Seleccione la nueva acción de alerta.**
9. **Configure el controlador de la alerta.**

Introduzca `action` y, a continuación, introduzca `get`.

El controlador por defecto es `email`. Si quiere utilizar otro controlador, introduzca el comando `set handler=` seguido de un carácter de tabulación para ver la lista de posibles controladores.

10. Defina valores para todos los argumentos del controlador.

Introduzca nuevamente el comando `get` para ver la lista de argumentos, si los hay, para el controlador especificado.

La mayoría de las acciones tienen argumentos. Por ejemplo, es posible que deba especificar un destinatario de correo electrónico, un juego de datos o un flujo de trabajo.

11. Introduzca el comando `commit`.

Introduzca el comando `list` para confirmar que la acción es correcta.

12. Escriba `done`.

Introduzca el comando `list` para ver la lista de acciones.

Temas relacionados

- [Agregación de una acción de alerta \(CLI\) \[289\]](#)
- [“Categorías de eventos de alerta” \[297\]](#)
- [“Tipos de acciones de alerta” \[298\]](#)

▼ **Agregación de una acción para una alerta de umbral específica (BUI)**

Este procedimiento describe cómo agregar una acción de alerta para alertas de umbral en eventos de estadística específicos.

Si la alerta de umbral específica no requiere una respuesta única, puede utilizar la categoría Umbrales en el procedimiento [Agregación de una acción de alerta \(BUI\) \[287\]](#) para especificar acciones de alerta que se ejecutan para eventos de umbral de alto nivel, como la infracción de un umbral de estadística.

1. Navegue hasta Configuración > Alertas.

2. Haga clic en el separador Alertas de umbral.

Si la alerta de evento de umbral para la cual desea agregar una acción de alerta aún no existe, utilice el procedimiento [Agregación de una alerta de umbral \(BUI\) \[300\]](#) para agregar la alerta de umbral. Puede agregar acciones de alerta al crear la alerta de umbral y luego omitir el resto de los pasos de este procedimiento.

3. Seleccione la alerta de umbral para la cual desea agregar una acción de alerta.

Haga doble clic o desplácese sobre la alerta y haga clic en el ícono de edición .

4. **En la sección Acciones de alerta del cuadro de diálogo, seleccione la acción que debe realizarse al enviar esta alerta de umbral.**

La mayoría de las acciones tienen argumentos. Por ejemplo, es posible que deba especificar un destinatario de correo electrónico o seleccionar un juego de datos o un flujo de trabajo.

5. **(Opcional) Seleccione el botón Probar para crear una alerta de prueba y ejecutar esta acción de alerta.**

Una prueba puede ser útil para comprobar si el correo electrónico o el servicio SNMP están configurados correctamente, por ejemplo.

6. **(Opcional) Para especificar acciones adicionales para esta alerta de evento de umbral, haga clic en el ícono de agregación en el título de la sección Acciones de alerta.**

Seleccione la acción y especifique los argumentos.

7. **Haga clic en el botón Aplicar en la parte superior derecha del cuadro de diálogo.**

Temas relacionados

- [Agregación de una alerta de umbral \(BUI\) \[300\]](#)

▼ Agregación de una acción para una alerta de umbral específica (CLI)

Este procedimiento describe cómo agregar una acción de alerta para alertas de umbral en eventos de estadística específicos. La categoría `thresholds` requiere la especificación de una alerta de evento de umbral existente.

Si la alerta de umbral específica no requiere una respuesta única, puede utilizar la categoría Umbral en el procedimiento [Agregación de una acción de alerta \(BUI\) \[287\]](#) para especificar acciones de alerta que se ejecutan para eventos de umbral de alto nivel, como la infracción de un umbral de estadística.

1. **Obtenga el UUID de la alerta de umbral.**

- a. **Vaya a `configuration alerts thresholds` e introduzca el comando `list`.**

Si la alerta de evento de umbral para la cual desea agregar una acción de alerta aún no existe, utilice el procedimiento [Agregación de una alerta de umbral \(CLI\) \[302\]](#) para agregar la alerta de umbral.

- b. **Introduzca el comando `select threshold-###` para la alerta de umbral en la cual desea agregar una acción de alerta.**

- c. **Introduzca** `get uuid`, **copie ese UUID de alerta de umbral e introduzca el comando** `done`.
2. **Vaya a** `configuration alerts actions` **e introduzca el comando** `list`.

Haga lo siguiente si aún *no* existe una acción de alerta que posea un UUID que coincida con el UUID del paso 1.

 - a. **Introduzca** `create`.
 - b. **Introduzca** `set category=thresholds`.
 - c. **Introduzca el comando** `set thresholdid=uuid`, **donde** *uuid* **es el UUID copiado en el paso 1.**
 - d. **Introduzca el comando** `commit`.

Si ya existe una acción de alerta con el mismo UUID del paso 1, puede especificar una acción adicional para esta alerta.
3. **Seleccione la acción de alerta que tenga el mismo UUID del paso 1.**
4. **Configure el controlador de la alerta.**

Introduzca `action` y, a continuación, introduzca `get`.

El controlador por defecto es `email`. Si quiere utilizar otro controlador, introduzca el comando `set handler=` seguido de un carácter de tabulación para ver la lista de posibles controladores.
5. **Defina valores para todos los argumentos del controlador.**

Introduzca nuevamente el comando `get` para ver la lista de argumentos, si los hay, para el controlador especificado.

La mayoría de las acciones tienen argumentos. Por ejemplo, es posible que deba especificar un destinatario de correo electrónico, un juego de datos o un flujo de trabajo.
6. **Introduzca el comando** `commit`.

Introduzca el comando `list` para confirmar que la acción es correcta.
7. **Escriba** `done`.

Introduzca el comando `list` para ver la lista de acciones.

Temas relacionados

- [Agregación de una alerta de umbral \(CLI\) \[302\]](#)

Categorías de eventos de alerta

En la siguiente tabla, se describen las categorías de eventos de alerta disponibles. Las categorías de eventos de BUI se muestran en el menú Categoría, en la sección Evento del cuadro de diálogo Agregar acción. Los eventos dentro de cada categoría se muestran al seleccionar la categoría correspondiente. Las categorías de eventos de la CLI son valores de la propiedad `category`, que se muestran al introducir el comando `set category=` seguido de un carácter de tabulación. Los eventos dentro de cada categoría aparecen al especificar la categoría y luego emitir el comando `show`.

TABLA 48 Categorías de eventos de acciones de alerta

Categoría de BUI	Categoría de CLI	Descripción
Active Directory	ad	Autenticación degradada del cliente de Active Directory o SMB Kerberos.
Todos los eventos	all	Eventos de alto nivel, como todas las alertas o los defectos, las alertas de servicio y los fallos de hardware.
Análisis	analytics	Eventos de alto nivel, como advertencia de suspensión automática de juegos de datos, memoria total excedida y uso excedido.
Software del dispositivo	appliance_software	Eventos que evitan actualizaciones de software o provocan un aviso grave del núcleo.
Instantánea de nube	cloud	Operaciones en la nube, entre ellas, copias de seguridad y restauraciones de instantáneas de recursos compartidos en la nube.
Cluster	cluster	Eventos de cluster, incluidos fallos de enlace y errores de pares.
Propiedades personalizadas	custom	Una acción de alerta para un evento definido por el usuario, que se especifica en un flujo de trabajo. Consulte “Creación y publicación de alertas personalizadas dentro de un flujo de trabajo” [853] .
Eventos de hardware	hardware	Cambios en la configuración del hardware e inicio del dispositivo.
Fallos de hardware	hardware_faults	Cualquier fallo de hardware.
Operaciones NDMP	ndmp	Eventos iniciados y finalizados de restauración y copia de seguridad TAR/DUMP de NDMP.
NDMP: solo copias de seguridad	backup	
NDMP: solo restauraciones	restore	

Categoría de BUI	Categoría de CLI	Descripción
Red	network	Eventos y fallos de puertos de red, enlaces de datos e interfaces IP.
Asistencia técnica remota	scrk	Eventos de carga de paquetes de asistencia.
Replicación remota	replication	Eventos y fallos de envío y recepción.
Replicación remota: solo origen	replication_source	
Replicación remota: solo destino	replication_target	
Servicios	smf	Eventos de fallo de servicios de software.
Eventos de migración shadow	shadow	Errores de migración o migración finalizada.
Umbrales	thresholds	En la BUI, los eventos de umbral son <code>Stat threshold error</code>, <code>Stat threshold normal</code> y <code>Stat threshold violated</code>. En la CLI, <code>thresholds</code> permite agregar una acción a una alerta de evento de umbral existente, según se describe en Agregación de una acción para una alerta de umbral específica (CLI) [295].
Agrupación ZFS	zfs_pool	Eventos de agrupación de almacenamiento, incluida la limpieza y la activación de discos de reserva.

Tipos de acciones de alerta

En la siguiente tabla, se describen los tipos de acciones de alerta disponibles. Los tipos de acciones de la BUI se enumeran en un menú, en la sección Acciones de alerta del cuadro de diálogo Agregar acción. Los tipos de acciones de la CLI son valores de la propiedad `handler` que se muestran al introducir el comando `set handler=` seguido de un carácter de tabulación.

TABLA 49 Tipos de acciones de alerta

Tipo de acción de la BUI	Tipo de acción de la CLI	Descripción del tipo de acción
Enviar correo electrónico	email	Envía un correo electrónico con el asunto especificado al destinatario especificado.
Introduzca valores para Enviar a y Asunto	Defina las propiedades <code>address</code> y <code>subject</code> .	Introduzca un solo destinatario, no una lista de destinatarios. Para enviar a varios destinatarios individuales, debe crear acciones de alerta individuales para esta alerta de evento. Utilice el servicio SMTP para configurar la forma en que se envía el correo electrónico. ■ BUI: Configuración > Servicios > SMTP ■ CLI: <code>configuration services smtp</code>

Tipo de acción de la BUI	Tipo de acción de la CLI	Descripción del tipo de acción
Envío de captura SNMP	snmp_trap	Envía una captura SNMP que contiene detalles de la alerta. Utiliza el servicio SNMP para configurar un destino para la captura SNMP. ■ BUI: Configuración > Servicios > SNMP ■ CLI: configuration services snmp
Enviar mensaje de syslog	syslog	Envía un mensaje de sistema que contiene detalles de la alerta a uno o varios sistemas remotos. Utiliza el servicio de syslog para configurar los destinos de syslog. ■ BUI: Configuración > Servicios > Syslog ■ CLI: configuration services syslog Para obtener más información acerca del envío de mensajes de syslog, consulte “Configuración de Syslog” [470].
Reanudar juego de datos Seleccione el juego de datos en el menú.	resume_dataset Defina dataset.	Reanuda un juego de datos de análisis. Reanudar y suspender juegos de datos puede ser útil para diagnosticar problemas de rendimiento intermitentes y para otros casos donde no es deseable mantener continuamente activado un juego de datos. Para obtener más información, consulte “Acerca de los juegos de datos de análisis” de Guía de análisis de Oracle® ZFS Storage Appliance versión OS8.8.x.
Suspender juego de datos Seleccione el juego de datos en el menú.	suspend_dataset Defina dataset.	Suspende un juego de datos de análisis.
Reanudar hoja de trabajo Seleccione la hoja de trabajo en el menú.	resume_worksheet Defina worksheet.	Reanuda una hoja de trabajo de análisis. Reanudar y suspender hojas de trabajo puede ser útil por los mismos motivos que reanudar y suspender juegos de datos. Una hoja de trabajo puede contener numerosos juegos de datos. Para obtener más información, consulte “Gráficos y diagramas de hojas de trabajo” de Guía de análisis de Oracle® ZFS Storage Appliance versión OS8.8.x.
Suspender hoja de trabajo Seleccione la hoja de trabajo en el menú.	suspend_worksheet Defina worksheet.	Suspende una hoja de trabajo de análisis.
Ejecutar flujo de trabajo	execute_workflow Defina workflow.	Ejecuta el flujo de trabajo especificado. Para activar un flujo de trabajo que sea elegible como acción de alerta, la acción <code>alert</code> del flujo de trabajo debe definirse con el valor <code>true</code>, como se describe en “Uso de los flujos de trabajo para acciones de alerta” [852].

Tipo de acción de la BUI	Tipo de acción de la CLI	Descripción del tipo de acción
Seleccione el flujo de trabajo en el menú.		Nota - El flujo de trabajo ejecutado no puede publicar una alerta. Consulte “Creación y publicación de alertas personalizadas dentro de un flujo de trabajo” [853] .

Agregación de alertas de umbral

Una alerta de umbral es una alerta personalizada en la cual se define un umbral para una estadística de análisis en particular, y la acción de alerta se ejecuta cuando el valor de la estadística está fuera de ese umbral. Consulte también [Guía de análisis de Oracle® ZFS Storage Appliance versión OS8.8.x](#).

Para crear alertas de umbral de estadísticas de análisis personalizadas, consulte los siguientes temas:

- Agregación de una alerta de umbral: [BUI](#), [CLI](#)
- [“Propiedades de alertas de umbral” \[303\]](#)

▼ Agregación de una alerta de umbral (BUI)

Utilice este procedimiento para especificar una alerta en un evento de umbral de estadística de análisis específico y para especificar una acción (respuesta) para la alerta.

Antes de empezar Para realizar este procedimiento, debe tener la autorización configure de la opción Alertas.

1. **Navegue hasta Configuración > Alertas.**
2. **Haga clic en el separador Alertas de umbral.**
3. **Haga clic en el ícono  de agregación en el título del separador Alertas de umbral.**
4. **En la sección Umbral del cuadro de diálogo, especifique el evento de umbral.**
 - a. **Seleccione una estadística en el menú desplegable.**
 - b. **Seleccione el tipo de evento: excede o está por debajo.**
 - c. **Especifique el porcentaje o la cantidad de bytes, operaciones, accesos o solicitudes.**

5. **En la sección Calendario del cuadro de diálogo, especifique en qué momento debe enviarse esta alerta de evento de umbral.**
Puede especificar que la alerta se envíe solo cuando el evento se produce en determinados días o en determinados intervalos de tiempo, o si el evento se prolonga durante un período específico. Puede especificar varios de estos parámetros de calendario.
6. **En la sección Acciones de alerta del cuadro de diálogo, seleccione la acción que debe realizarse al enviar esta alerta de evento de umbral.**
La mayoría de las acciones tienen argumentos. Por ejemplo, es posible que deba especificar un destinatario de correo electrónico o seleccionar un juego de datos o un flujo de trabajo.
Si esta alerta de umbral no requiere una respuesta única, puede dejar vacía la sección Acciones de alerta y, en su lugar, utilizar la categoría Umbrales en el procedimiento [Agregación de una acción de alerta \(BUI\) \[287\]](#) para especificar acciones de alerta que se ejecutan para eventos de umbral de alto nivel, como la infracción de un umbral de estadística.
7. **(Opcional) Seleccione el botón Probar para crear una alerta de prueba y ejecutar esta acción de alerta.**
Una prueba puede ser útil para comprobar si el correo electrónico o el servicio SNMP están configurados correctamente, por ejemplo.
8. **(Opcional) Para especificar acciones adicionales para esta alerta de evento de umbral, haga clic en el ícono de agregación en el título de la sección Acciones de alerta.**
Seleccione la acción y especifique los argumentos.
9. **Haga clic en el botón Aplicar en la parte superior derecha del cuadro de diálogo.**

Pasos siguientes

Para modificar una alerta de umbral, haga doble clic o desplácese sobre ella y haga clic en el ícono de edición , realice los cambios y haga clic en el botón Aplicar.

Para suprimir una alerta de umbral, desplácese sobre ella, haga clic en el ícono para suprimir  y confirme que desea suprimir esta alerta.

Temas relacionados

- [“Propiedades de alertas de umbral” \[303\]](#)
- [“Tipos de acciones de alerta” \[298\]](#)

▼ Agregación de una alerta de umbral (CLI)

Utilice este procedimiento para especificar una alerta en un evento de umbral de estadística de análisis específico.

Antes de empezar Para realizar este procedimiento, debe tener la autorización `alert allow_configure`.

1. **Vaya a `configuration alerts thresholds` e introduzca el comando `create`.**

```
hostname:configuration alerts thresholds> create
```

2. **Introduzca `get` para ver la lista de propiedades de la alerta de umbral.**

3. **Defina las propiedades de la alerta de umbral.**

Debe definir al menos `statname` y `limit`. El resto de las propiedades que deben definirse tienen valores por defecto.

Para ver la lista de estadísticas para las cuales puede definir alertas de umbral, introduzca `set statname=` seguido de un carácter de tabulación.

4. **Introduzca el comando `commit`.**
5. **Copie el UUID en el mensaje de confirmación.**
6. **Cree una acción de alerta para esta alerta de umbral.**

Siga el procedimiento [Agregación de una acción para una alerta de umbral específica \(CLI\) \[295\]](#) a partir del paso 2.

Pasos siguientes

Para modificar una alerta de umbral, introduzca el comando `select threshold-###`, defina la alerta de umbral e introduzca `commit`.

Si desea especificar acciones adicionales para esta alerta de evento, siga el procedimiento [Agregación de una acción para una alerta de umbral específica \(CLI\) \[295\]](#).

Para suprimir una alerta de umbral, introduzca el comando `destroy threshold-###` y luego y para confirmar.

Temas relacionados

- [“Propiedades de alertas de umbral” \[303\]](#)
- [“Tipos de acciones de alerta” \[298\]](#)
- [Agregación de una acción para una alerta de umbral específica \(CLI\) \[295\]](#)

Propiedades de alertas de umbral

Utilice las siguientes propiedades para especificar la estadística, definir el umbral y establecer en qué momento se ejecutarán las acciones de alerta para las alertas de umbral.

TABLA 50 Propiedades de alertas de umbral

Propiedad de la BUI	Propiedad de la CLI	Descripción
nombre de estadística	statname	La estadística que desea supervisar.
excede	type=normal	Cómo comparar el valor de umbral con el valor de la estadística actual.
está por debajo	type=inverted	
porcentaje	limit	El porcentaje (en números enteros) o la cantidad de bytes, operaciones, accesos o solicitudes.
durante al menos Seleccione la unidad de tiempo.	minpost La unidad de tiempo es segundos.	Cantidad de tiempo (en números enteros) en que el valor de la estadística debe permanecer en la condición de umbral antes de ejecutar la acción de alerta.
solo entre	window_start window_end	La ventana de tiempo durante la cual debe ejecutarse esta acción de alerta. Seleccione horarios entre 00:00 y 23:30 UTC. Para ejecutar esta acción de alerta en cualquier momento en que se cumplan las condiciones, especifique none como hora de inicio u hora de finalización.
solo durante	days	Qué días se deben enviar estas alertas. Las opciones son días, días de semana o fines de semana.
Volver a publicar la alerta cada... mientras continúe este problema. Seleccione la unidad de tiempo.	frequency La unidad de tiempo es segundos.	Cantidad de tiempo (en números enteros) entre ejecuciones de la acción de alerta cuando el valor de la estadística permanece en la condición de umbral.
Publicar alerta también cuando se solucione la condición durante al menos... Seleccione la unidad de tiempo.	minclear La unidad de tiempo es segundos.	Cantidad de tiempo (en números enteros) que el valor de la estadística debe permanecer fuera de la condición de umbral antes de ejecutar una acción de seguimiento de alerta.

Configuración de certificados

En esta sección, se describe el uso de certificados de clave pública. Los certificados de clave pública y las cadenas de confianza proporcionan un mecanismo para identificar digitalmente un sistema sin tener que intercambiar información secreta de manera manual.

Un certificado de clave pública es un blob de datos que codifica un valor de clave pública; información sobre la generación del certificado, por ejemplo, un nombre o quién lo firmó; un hash o un total de control del certificado; y una firma digital del hash. En conjunto, estos valores componen el certificado. La firma digital garantiza que el certificado no se modificó.

El dispositivo admite certificados que sean propiedad del cliente. El ciclo de vida de un certificado comienza con la generación de una solicitud de firma de certificado (CSR). A continuación, la CSR se envía a la autoridad de certificación (CA) para la firma. Cuando la CA devuelve el certificado firmado, se lo puede instalar en el dispositivo. Si un certificado está firmado por una CA que no es raíz, debe obtener también certificados de las CA de segundo nivel y de niveles superiores.

Puede gestionar los siguientes dos tipos de certificados:

- Los certificados de sistema identifican el sistema actual.
- Los certificados de confianza identifican sistemas remotos.

Para gestionar certificados de sistema, realice las siguientes tareas:

- Creación de un certificado de sistema nuevo: [BUI](#), [CLI](#)
- Carga de certificados de CA que no son raíz: [BUI](#), [CLI](#)
- Visualización de detalles de certificados de sistema y CSR: [BUI](#), [CLI](#)
- Destrucción de una CSR o un certificado de sistema: [BUI](#), [CLI](#)
- Configuración del certificado del sistema por defecto o del dispositivo: [BUI](#), [CLI](#)

Para gestionar certificados de confianza, realice las siguientes tareas:

- Carga de un certificado de confianza: [BUI](#), [CLI](#)
- Visualización de detalles de certificado de confianza: [BUI](#), [CLI](#)
- Destrucción de un certificado de confianza: [BUI](#), [CLI](#)
- Asignación de un certificado a un servicio: [BUI](#), [CLI](#)

Para usar la política HTTP con seguridad de transporte estricta (HSTS) junto con los certificados, consulte el siguiente tema:

- [“HTTP con seguridad de transporte estricta” \[316\]](#)

▼ Creación de un certificado de servidor nuevo (BUI)

Siga este procedimiento para crear un nuevo certificado de servidor.

1. **Vaya a Configuración > Valores de configuración > Certificados y haga clic en el separador Sistema.**
2. **Cree una nueva CSR.**

Agregue una nueva CSR o copie una existente.

- Para agregar una nueva CSR, haga clic en el ícono de agregación de elemento .
- Para crear una nueva CSR basada en una CSR o un certificado existentes, mueva el cursor sobre la entrada existente y haga clic en el ícono de copia .

3. Complete los campos en el cuadro de diálogo Nueva solicitud de certificado.

4. Haga clic en Crear.

5. Guarde la nueva CSR.

Quando se le solicite abrir la CSR o guardarla, podrá guardarla en ese momento o más adelante.

- Para guardar la CSR ahora, seleccione Guardar archivo y haga clic en Aceptar.
- Para guardarla más adelante, haga lo siguiente:
 - a. En el cuadro de diálogo para abrir o guardar, haga clic en Cancelar.
 - b. Mueva el cursor sobre la entrada en la tabla y haga clic en el ícono de descarga .

6. Transfiera la CSR a la CA de la manera indicada.

7. Cargue el certificado firmado.

Después de recibir el certificado firmado de la autoridad de certificación, haga lo siguiente:

- a. Vaya a Configuración > Valores de configuración > Certificados y haga clic en el separador Sistema.
- b. Haga clic en el ícono de carga .
- c. Navegue hasta la ubicación del certificado firmado y selecciónelo.
- d. Haga clic en Cargar.

▼ Creación de un certificado de servidor nuevo (CLI)

Siga este procedimiento para crear un nuevo certificado de servidor.

1. **Vaya a configuration settings certificates system.**
2. **Cree una nueva CSR.**
Agregue una nueva CSR o copie una existente.
 - **Para agregar una nueva CSR, introduzca el comando `create`.**
 - **Para crear una nueva CSR en función de un certificado o una CSR existentes, haga lo siguiente:**
 - a. **Introduzca el comando `list` para ver la tabla de certificados.**
 - b. **Introduzca el comando `clone cert`, en el que `cert` es un valor de la columna CERT de la tabla.**

```
hostname:configuration settings certificates system> clone cert-001
```

3. **Complete el formulario de la CSR.**

```
hostname:configuration settings certificates system (uncommitted)> get
  subject_commonname = hostname.us.example.com
  subject_organizationname = (unset)
subject_organizationalunitname = (unset)
  subject_localityname = (unset)
  subject_stateorprovincename = (unset)
  subject_countryname = (unset)
  subject_emailaddress = (unset)
      dns = hostname.us.example.com
      ip = ip-addr
      uri = (unset)
      dirname = (unset)
      comment = (unset)
hostname:configuration settings certificates system (uncommitted)> set comment="test"
  comment = test (uncommitted)
hostname:configuration settings certificates system (uncommitted)> commit
```

4. **Ahora puede ver la CSR.**

- a. **Introduzca el comando `list` para ver la nueva CSR en la tabla.**

```
hostname:configuration settings certificates system> list
CERT   TYPE SUBJECT COMMON NAME      ISSUER COMMON NAME      NOT AFTER
cert-002 req  hostname.us.example.com
cert-001 cert  hostname.us.example.com  CA                        2023-1-25
cert-000 cert  3ebff8d2-58f6-4de4-a2c... 3ebff8d2-58f6-4de4-a2c... 2038-1-19
```

- b. Introduzca el comando `dump cert`, en el que `cert` es su nuevo CSR de la tabla.

```
hostname:configuration settings certificates system> dump cert-002
-----BEGIN CERTIFICATE REQUEST-----
...
-----END CERTIFICATE REQUEST-----
```

5. Copie la CSR y transfírela a la CA de la manera indicada.

6. Importe el certificado firmado.

Después de recibir el certificado firmado de la autoridad de certificación, haga lo siguiente:

- a. Vaya a `configuration settings certificates system`.

- b. Introduzca el comando `import`.

- c. Cuando se le solicite, pegue el certificado firmado.

```
hostname:configuration settings certificates system> import
("." to end)> -----BEGIN CERTIFICATE-----
...
("." to end)> -----END CERTIFICATE-----
("." to end)> .
```

7. Verifique el certificado importado.

- a. Introduzca el comando `list` para ver el nuevo certificado firmado en la tabla.

- b. Introduzca `select cert` y, luego, introduzca `get` para ver las propiedades del certificado.

- c. Introduzca `done` y, luego, introduzca `dump cert` para ver el certificado.

▼ Carga de certificados de CA que no son raíz (BUI)

Si el certificado de servidor está firmado por una autoridad de certificación que no es de tipo raíz, debe obtener también certificados para las autoridades de certificación de segundo nivel y niveles superiores. Después de obtener estos certificados de las autoridades de certificación, realice el siguiente procedimiento para cargarlos.

1. Vaya a **Configuración > Valores de configuración > Certificados** y haga clic en el separador **Sistema**.

2. Haga clic en el ícono de carga .
3. Navegue hasta la ubicación del certificado firmado y selecciónelo.
4. Haga clic en Cargar.
5. Repita los pasos 3 y 4 para cada certificado firmado.

▼ Carga de certificados de CA que no son raíz (CLI)

Si el certificado de servidor está firmado por una autoridad de certificación que no es de tipo raíz, también debe obtener certificados para las autoridades de certificación de segundo nivel y niveles superiores. Después de obtener estos certificados de las autoridades de certificación, realice el siguiente procedimiento para cargarlos.

1. **Vaya a `configuration settings certificates system`.**
2. **Introduzca el comando `import`.**
 Cuando se le solicite, pegue el certificado firmado.

```
hostname:configuration settings certificates system> import
("." to end)> -----BEGIN CERTIFICATE-----
...
("." to end)> -----END CERTIFICATE-----
("." to end)> .
```
3. **Repita el paso 2 para cada certificado firmado.**
4. **Si desea comprobar los certificados importados, use el comando `list` para ver la tabla de certificados.**

```
hostname:configuration settings certificates system> list
CERT      TYPE SUBJECT COMMON NAME      ISSUER COMMON NAME      NOT AFTER
cert-002 cert hostname.us.example.com  CA                      2023-1-25
cert-001 cert 3ebff8d2-58f6-4de4-a2c... 3ebff8d2-58f6-4de4-a2c... 2038-1-19
```

▼ Visualización de detalles de certificados y CSR (BUI)

Realice este procedimiento para visualizar los detalles de la CSR y del certificado.

Un certificado del sistema puede ser un certificado basado en dirección IP o dominio generado automáticamente, un certificado basado en ASN generado automáticamente o un certificado firmado por una autoridad de certificación (CA).

1. **Vaya a Configuración > Valores de configuración > Certificados y haga clic en el separador Sistema.**

Si no los suprimió, debería ver al menos un certificado generado automáticamente basado en dominio o dirección IP y exactamente un certificado generado automáticamente basado en el identificador exclusivo universal (UUID) del número de serie de dispositivo (ASN).

2. **Mueva el cursor sobre una entrada existente y haga clic en el ícono de información .**

Los valores de Subject Common Name (Nombre común de asunto), Issuer Common Name (Nombre común de emisor) y DirName (Nombre dir) (nombre distintivo) son el UUID de ASN. Para un cluster, DirName (Nombre dir) incluye el UUID de ASN de cada par.

3. **Cuando finalice, haga clic en Aceptar para cerrar la ventana Detalles.**

▼ Visualización de detalles de certificados y CSR (CLI)

Realice este procedimiento para visualizar los detalles de la CSR y del certificado.

Un certificado del sistema puede ser un certificado basado en dirección IP o dominio generado automáticamente, un certificado basado en ASN generado automáticamente o un certificado firmado por una autoridad de certificación (CA).

1. **Vaya a `configuration settings certificates system`.**

2. **Introduzca el comando `list`.**

Si no los suprimió, debería ver al menos un certificado generado automáticamente basado en dominio o dirección IP y exactamente un certificado generado automáticamente basado en el identificador exclusivo universal (UUID) del número de serie de dispositivo (ASN).

```
hostname:configuration settings certificates system> list
CERT      TYPE SUBJECT COMMON NAME    ISSUER COMMON NAME    NOT AFTER
cert-002 cert alice.example.com...  alice.example.com...  2038-1-19
cert-001 cert 17f5fdce-6d64-4736...  17f5fdce-6d64-4736... 2038-1-19
```

3. **Use el comando `get` para ver los detalles de una solicitud de firma de certificado (CSR) o un certificado.**

- **El siguiente es un ejemplo de un certificado generado automáticamente basado en ASN.**

En el siguiente ejemplo, los valores de `subject_commonname`, `issuer_commonname` y `dirname` (nombre distintivo) son el UUID de ASN. Para un cluster, `dirname` incluye el UUID de ASN de cada par.

```
hostname:configuration settings certificates system> select cert-001
hostname:configuration settings certificates system cert-002> get
      uuid = uuid
subject_commonname = 17f5fdce-6d64-4736-882c-bff99680bce6
  issuer_commonname = 17f5fdce-6d64-4736-882c-bff99680bce6
        dirname = 17f5fdce-6d64-4736-882c-bff99680bce6,a040a259-53b0-4967-8b71-
f65e7fbd8bed
      comment = Automatically generated
    notbefore = 2006-2-15 18:00
    notafter = 2038-1-19 03:14:07
  serialnumber = 5D:DD:79:C5:00:00:00:03
a1fingerprint = 60:AF:B4:EB:63:B3:E4:76:E0:90:C6:DD:93:7C:F8:61:71:E4:67:68
```

- **El siguiente es un ejemplo de un certificado generado automáticamente convencional.**

```
hostname:configuration settings certificates system> select cert-002
hostname:configuration settings certificates system cert-002> get
      uuid = uuid
subject_commonname = alice.example.com
  issuer_commonname = alice.example.com
        dns = alice.example.com,alice,ip-addr
        ip = ip-addr
        uri = https://alice.example.com:215,https://alice:215,https://ip-addr
      comment = Automatically generated
    notbefore = 2006-2-15 18:00
    notafter = 2038-1-19 03:14:07
  serialnumber = 59:8A:73:7B:00:00:00:27
sha1fingerprint = 0A:14:26:ED:C7:43:0D:30:33:98:87:24:C5:9B:A2:52:55:FE:B1:D7
```

- **El siguiente es un ejemplo de una CSR.**

```
      uuid = uuid
subject_commonname = alice.example.com
subject_organizationname = Example Corp, Inc
subject_localityname = Exampleton
subject_stateorprovincename = CA
subject_countryname = US
        dns = alice.example.com
        ip = ip-addr
```

- **El siguiente es el certificado firmado por CA que se obtiene como resultado de la CSR anterior.**

```
      uuid = uuid
subject_commonname = alice.example.com
subject_organizationname = Example Corp, Inc
subject_localityname = Exampleton
```

```

subject_stateorprovincename = CA
subject_countrynname = US
issuer_commonname = Most Trusted Certificate
issuer_organizationname = Totally Trustworthy Certificates, Inc
issuer_localityname = Trustville
issuer_stateorprovincename = AK
issuer_countrynname = US
    dns = alice.example.com
    ip = ip-addr
    notbefore = 2021-3-16 17:51:19
    notafter = 2022-3-16 17:51:19
    serialnumber = 4F
    sha1fingerprint = 62:FB:29:84:8C:3E:0E:C6:D2:49:88:38:F2:53:12:8D:A5:F9:
96:88

```

▼ Dstrucción de una CSR o un certificado (BUI)

Realice este procedimiento para destruir una CSR o un certificado.

Nota - Al destruir la CSR, se destruye también la clave privada asociada. Por lo tanto, no será posible importar certificados derivados de esa CSR. Al destruir un certificado, se destruye también la clave privada asociada. Por lo tanto, no se podrá volver a importar ese certificado.

Después de que se destruye un certificado basado en ASN, se genera automáticamente un nuevo certificado basado en ASN sin reiniciar el software del dispositivo.

1. **Vaya a Configuración > Valores de configuración > Certificados y haga clic en el separador Sistema.**
2. **Mueva el cursor sobre una entrada existente y haga clic en el ícono de papelera .**
3. **Haga clic en Destruir.**

▼ Dstrucción de una CSR o un certificado (CLI)

Realice este procedimiento para destruir una CSR o un certificado.

Nota - Al destruir la CSR, se destruye también la clave privada asociada. Por lo tanto, no será posible importar certificados derivados de esa CSR. Al destruir un certificado, se destruye también la clave privada asociada. Por lo tanto, no se podrá volver a importar ese certificado.

Después de que se destruye un certificado basado en ASN, se genera automáticamente un nuevo certificado basado en ASN sin reiniciar el software del dispositivo.

1. **Para ver todas las entradas de certificados, vaya al contexto `configuration settings certificates system` e introduzca el comando `list`.**

2. **Para destruir una CSR o un certificado, utilice el comando `destroy`.**

```
hostname:configuration settings certificates system> destroy cert-002
Caution: Destroying a certificate issued by a certificate authority also
destroys the associated private key. Re-importing the certificate will not be possible.
Destroy appliance certificate? (Y/N) y
```

▼ Configuración del certificado por defecto del dispositivo (BUI)

Use este procedimiento para configurar el certificado por defecto de este dispositivo.

1. **Vaya a Configuración > Valores de configuración > Certificados y haga clic en el separador Sistema.**
2. **En el menú "Certificado predeterminado de sistema", seleccione el certificado que desea establecer como el certificado por defecto para este dispositivo.**
3. **Haga clic en Aplicar.**

▼ Configuración del certificado por defecto del dispositivo (CLI)

Use este procedimiento para configurar el certificado por defecto de este dispositivo.

1. **Para ver todas las entradas de certificados, vaya al contexto `configuration settings certificates system` e introduzca el comando `list`.**

2. **Para definir un certificado por defecto, use el comando `default`.**

```
hostname:configuration settings certificates system> set default=cert-002
default= cert-002 (uncommitted)
hostname:configuration settings certificates system> commit
```

▼ Carga de certificados de confianza (BUI)

Realice este procedimiento para cargar un certificado de confianza.

1. **Vaya a Configuración > Valores de configuración > Certificados y haga clic en la ficha De confianza.**
2. **Haga clic en el ícono de carga**  **.**
3. **Navegue hasta la ubicación del certificado firmado y selecciónelo.**
4. **Haga clic en Cargar.**
5. **Repita los pasos 3 y 4 para cada certificado firmado.**
6. **Compruebe los certificados importados.**

Consulte [Visualización de detalles de certificados de confianza \(BUI\) \[314\]](#).

▼ Carga de certificados de confianza (CLI)

Realice este procedimiento para cargar un certificado de confianza.

1. **Vaya a configuration settings certificates trusted.**
2. **Introduzca el comando import.**

Cuando se le solicite, pegue el certificado firmado.

```
hostname:configuration settings certificates system> import
("." to end)> -----BEGIN CERTIFICATE-----
...
("." to end)> -----END CERTIFICATE-----
("." to end)> .
```

3. **Repita el paso 2 para cada certificado firmado.**
4. **Compruebe los certificados importados.**

Consulte [Visualización de detalles de certificados de confianza \(CLI\) \[314\]](#).

▼ Visualización de detalles de certificados de confianza (BUI)

Realice este procedimiento para visualizar los detalles del certificado de confianza.

Un certificado de confianza puede ser un certificado basado en dirección IP o dominio generado automáticamente, un certificado basado en ASN generado automáticamente o un certificado firmado por una autoridad de certificación (CA).

1. **Vaya a Configuración > Valores de configuración > Certificados y haga clic en la ficha De confianza.**

Si no los suprimió, debería ver al menos un certificado generado automáticamente basado en dominio o dirección IP y exactamente un certificado generado automáticamente basado en el identificador exclusivo universal (UUID) del número de serie de dispositivo (ASN).

2. **Mueva el cursor sobre una entrada existente y haga clic en el ícono de información .**

Los valores de Subject Common Name (Nombre común de asunto), Issuer Common Name (Nombre común de emisor) y DirName (Nombre dir) (nombre distintivo) son el UUID de ASN. Para un cluster, DirName (Nombre dir) incluye el UUID de ASN de cada par.

3. **Cuando finalice, haga clic en Aceptar para cerrar la ventana Detalles.**

▼ Visualización de detalles de certificados de confianza (CLI)

Realice este procedimiento para visualizar los detalles del certificado de confianza.

Un certificado de confianza puede ser un certificado basado en dirección IP o dominio generado automáticamente, un certificado basado en ASN generado automáticamente o un certificado firmado por una autoridad de certificación (CA).

1. **Vaya a `configuration settings certificates trusted`.**
2. **Muestre la lista de certificados.**

Si no los suprimió, debería ver al menos un certificado generado automáticamente basado en dominio o dirección IP y exactamente un certificado generado automáticamente basado en el identificador exclusivo universal (UUID) del número de serie de dispositivo (ASN).

```
hostname:configuration settings certificates trusted> list
CERT      TYPE SUBJECT COMMON NAME    ISSUER COMMON NAME    NOT AFTER
cert-002  cert  cd9dfcfe-b0d3-600f-... cd9dfcfe-b0d3-600f-... 2038-1-19
cert-001  cert  3638ef45-ae8c-ec31-... 3638ef45-ae8c-ec31-... 2038-1-19
```

3. **Para ver los detalles de un certificado, seleccione el certificado y use el comando `get`.**

▼ Dstrucción de un certificado de confianza (BUI)

Realice este procedimiento para destruir un certificado de confianza.

Después de que se destruye un certificado basado en ASN, se genera automáticamente un nuevo certificado basado en ASN sin reiniciar el software del dispositivo.

1. **Vaya a Configuración > Valores de configuración > Certificados y haga clic en la ficha De confianza.**
2. **Mueva el cursor sobre una entrada existente y haga clic en el ícono de papelera .**
3. **Haga clic en Destruir.**

▼ Dstrucción de un certificado de confianza (CLI)

Realice este procedimiento para destruir un certificado de confianza.

Después de que se destruye un certificado basado en ASN, se genera automáticamente un nuevo certificado basado en ASN sin reiniciar el software del dispositivo.

1. **Para ver todas las entradas de certificados, vaya al contexto `configuration settings certificates trusted` e introduzca el comando `list`.**
2. **Para destruir un certificado, use los siguientes comandos.**

```
hostname:configuration settings certificates system> destroy cert-001
Caution: Destroying a certificate issued by a certificate authority also
destroys the associated private key. Re-importing the certificate will not be possible.
Destroy appliance certificate? (Y/N) y
```

▼ Asignación de un certificado a un servicio (BUI)

Realice este procedimiento para asignar un certificado a un servicio, como LDAP.

1. **Vaya a Configuración > Valores de configuración > Certificados y haga clic en la ficha De confianza.**
2. **En el menú desplegable de los certificados de sistema, seleccione el certificado que desea asignar.**
3. **Haga clic en el ícono de edición .**
4. **Seleccione el servicio, como `ldap`, de la lista de servicios en la parte inferior de la página.**

▼ Asignación de un certificado a un servicio (CLI)

Realice este procedimiento para asignar un certificado a un servicio, como LDAP.

1. **Para ver todas las entradas de certificados, vaya al contexto `configuration settings certificates trusted` e introduzca el comando `list`.**
2. **Seleccione el certificado al cual desea asignar el servicio y establezca el nombre del servicio.**

```
hostname:configuration settings certificates trusted> select cert-001
hostname:configuration settings certificates trusted cert-001> set services=ldap
services= ldap (uncommitted)
hostname:configuration settings certificates trusted cert-001> commit
```

HTTP con seguridad de transporte estricta

La política HTTP con seguridad de transporte estricta (HSTS) solo permite conexiones HTTPS seguras, y no conexiones HTTP, por un período determinado. Antes de usar HSTS, deberá familiarizarse con sus requisitos previos, comprender el comportamiento del explorador con la política HSTS activada e instalar un certificado firmado por una autoridad de certificación.

Nota - Si no se puede conservar un certificado válido y adecuado, se podrían denegar las ventajas de seguridad de HSTS o podría suceder que el explorador no se conecte con el dispositivo.

Para activar HSTS, use los procedimientos siguientes:

- Activación de HTTP con seguridad de transporte estricta: [BUI](#), [CLI](#)

▼ Activación de HTTP con seguridad de transporte estricta (BUI)

Realice este procedimiento para activar la política HSTS en este dispositivo.

1. **Vaya a Configuración > Valores de configuración > Certificados.**
2. **En Configuración de seguridad, seleccione la casilla de control para activar HSTS.**
3. **(Opcional) Defina el tiempo máximo durante el que HSTS permanecerá activado.**
Actualice el valor de HSTS Max Age (Duración máxima de HSTS), incluidas las unidades.
4. **Haga clic en Aplicar.**

▼ Activación de HTTP con seguridad de transporte estricta (CLI)

Realice este procedimiento para activar la política HSTS en este dispositivo.

1. **Vaya a `configuration settings certificates security`.**
2. **Introduzca el comando `get` para ver las propiedades de seguridad.**

```
hostname:configuration settings certificates security> get
      hsts_enable = false
      hsts_max_age = 730 days
```
3. **Configure la propiedad para activar HSTS en `true`.**

```
hostname:configuration settings certificates security> set hsts_enable=true
      hsts_enable = true (uncommitted)
```
4. **(Opcional) Defina el tiempo máximo durante el que HSTS permanecerá activado.**
Actualice el valor de `hsts_max_age`, incluidas las unidades. Las unidades pueden ser `seconds`, `minutes`, `hours`, `days`, `weeks` o `months`.

5. Confirme los cambios.

Configuración de cifrados y versiones de SSL/TLS

En esta sección, se describe cómo configurar los cifrados y las versiones del protocolo SSL/TLS que Oracle ZFS Storage Appliance usa para comunicarse con dispositivos pares.

Un cifrado es un algoritmo para realizar operaciones de cifrado y descifrado. El dispositivo usa cifrados para distintas tareas, como el cifrado y descifrado de datos durante la replicación de datos. Configure los cifrados y las versiones de SSL/TLS según los requisitos de seguridad del sitio. Para la replicación remota, asegúrese de que los dispositivos de origen y de destino estén configurados para admitir los mismos valores.

No cambie los cifrados ni las versiones de SSL/TLS, a menos que el cluster esté en pleno funcionamiento. Si la configuración se cambia de modo que los dos controladores no usen configuraciones compatibles, el segundo controlador no podrá volver a unirse al cluster. Si esto ocurre, restablezca la configuración de modo que sean compatibles.

Es posible que los sistemas Oracle ZFS Storage Appliance que ejecutan una versión de firmware anterior no admitan los cifrados que se ofrecen en las versiones de TLS más recientes. Debido a que las versiones y al menos uno de los cifrados deben ser idénticos en los dispositivos que se comunican entre sí, si uno de los dispositivos admite solo cifrados TLSv1.0, todos los dispositivos se deben configurar para admitir los cifrados y la versión TLSv1.0.

Para configurar SSL/TLS, realice las siguientes tareas:

- [Configuración de SSL/TLS \(BUI\) \[318\]](#)
- [Configuración de SSL/TLS \(CLI\) \[319\]](#)

▼ Configuración de SSL/TLS (BUI)

Para configurar los cifrados y las versiones de SSL/TLS, siga los pasos que se indican a continuación. Las versiones y al menos uno de los cifrados deben ser idénticos en todos los dispositivos que se comunican entre sí.

- 1. Vaya a Configuración > Valores de configuración > Par.**
- 2. Haga clic en Editar junto a Cifrados y versiones de SSL/TLS.**
- 3. Configure las versiones y los cifrados, y haga clic en Aceptar.**

La lista de cifrados varía en función de las versiones seleccionadas.

▼ Configuración de SSL/TLS (CLI)

Para configurar los cifrados y las versiones de SSL/TLS, siga los pasos que se indican a continuación. Las versiones y al menos uno de los cifrados deben ser idénticos en todos los dispositivos que se comunican entre sí.

1. **Vaya a `configuration settings peer` e introduzca `ls` para mostrar los cifrados y las versiones de SSL/TLS.**

La lista de cifrados varía en función de las versiones seleccionadas.

2. **Para introducir las versiones de SSL/TLS, use el comando `set tls_version` y el nombre de la versión.**

```
hostname:configuration settings peer> set tls_version=TLSv1.2
      tls_version = TLSv1.2 (uncommitted)
```

3. **Para introducir los cifrados, use el comando `set ciphers` y los nombres de los cifrados, separados por comas.**

```
hostname:configuration settings peer> set
ciphers=AES128-GCM-SHA256,ECDH-ECDSA-AES128-GCM-SHA256
      ciphers =
AES128-GCM-SHA256,ECDH-ECDSA-AES128-GCM-SHA256 (uncommitted)
```

4. **Introduzca `commit`. Para ver las versiones y los cifrados, introduzca `show`.**

```
hostname:configuration settings peer> commit
hostname:configuration settings peer> show
Properties:
      tls_version = TLSv1.2
      ciphers =
AES128-GCM-SHA256:ECDH-ECDSA-AES128-GCM-SHA256
hostname:configuration settings peer>
```

Configuración de la complejidad de contraseña

Un usuario administrativo con privilegios suficientes puede configurar reglas de complejidad de contraseña para todos los usuarios locales. Posteriormente, cuando los usuarios locales configuren o cambien sus contraseñas, estas reglas de complejidad los limitarán; las contraseñas existentes no se verán afectadas.

Para configurar la complejidad de contraseña en los usuarios locales, consulte las siguientes secciones:

- Configuración de la complejidad de contraseña: [BUI](#), [CLI](#)
- “Propiedades de la complejidad de contraseña” [321]

Para obtener información sobre la configuración de los usuarios, incluidos roles, autorizaciones y excepciones, consulte [“Configuración de usuarios” \[257\]](#).

▼ Configuración de la complejidad de contraseña (BUI)

Utilice el siguiente procedimiento para configurar la complejidad de contraseña en los usuarios locales.

Antes de empezar Para las excepciones o el rol de un usuario administrativo, si no existe ningún servicio autorizado en el ámbito de los servicios, agregue la autorización "configurar" al servicio de contraseña.

1. **Vaya a Configuración > Valores de configuración > Contraseñas.**
2. **Modifique las propiedades con los valores que se describen en [“Propiedades de la complejidad de contraseña” \[321\]](#).**
3. **Haga clic en APLICAR.**

Temas relacionados

- [“Propiedades de la complejidad de contraseña” \[321\]](#)
- [“Configuración de usuarios” \[257\]](#)

▼ Configuración de la complejidad de contraseña (CLI)

Utilice el siguiente procedimiento para configurar la complejidad de contraseña en los usuarios locales.

Antes de empezar Para las excepciones o el rol de un usuario administrativo, si no existe ningún servicio autorizado en el ámbito de los servicios, agregue la autorización "configurar" al servicio de contraseña.

1. **Vaya a `configuration settings passwords`.**
2. **Introduzca `show` para ver las propiedades y sus valores.**

3. Configure las propiedades con los valores que se describen en [“Propiedades de la complejidad de contraseña” \[321\]](#).
4. Introduzca el comando `commit`.

Temas relacionados

- [“Propiedades de la complejidad de contraseña” \[321\]](#)
- [“Configuración de usuarios” \[257\]](#)

Propiedades de la complejidad de contraseña

En la siguiente tabla, se describen las propiedades para configurar la complejidad de contraseña en los usuarios locales.

TABLA 51 Propiedades de la complejidad de contraseña

Nombre de la BUI	Nombre de la CLI	Descripción
Longitud mínima	passlength	Longitud mínima de caracteres de la contraseña. Debe ser un entero positivo. Valor por defecto: 8.
Número mínimo de letras	min_letters	Cantidad mínima de caracteres alfabéticos. Valor por defecto: 0.
Número mínimo de letras en mayúscula	min_upper	Cantidad mínima de caracteres alfabéticos en mayúscula. Valor por defecto: 0.
Número mínimo de letras en minúscula	min_lower	Cantidad mínima de caracteres alfabéticos en minúscula. Valor por defecto: 0.
Número mínimo de dígitos	min_digit	Cantidad mínima de caracteres numéricos. Valor por defecto: 0.
Número mínimo de signos de puntuación	min_punctuation	Cantidad mínima de signos de puntuación. Tenga en cuenta que algunas versiones de Oracle ILOM no admiten los dos puntos ni los espacios en la contraseña de usuario root. Valor por defecto: 0.
Número máximo de caracteres repetidos consecutivos	max_repeats	Cantidad máxima de caracteres repetidos consecutivos. Valor por defecto: 0.
La contraseña no debe contener el nombre de usuario en orden circular	namecheck	Controla si la contraseña puede basarse en el nombre de usuario. Valor por defecto: verdadero.

Servicios de dispositivos

Los servicios de los dispositivos se gestionan con facilidad desde la pantalla Configuración > Servicios de la BUI o el contexto `configuration services` de la CLI.

Use las siguientes tareas para ver y gestionar los servicios del dispositivo:

- [Visualización de un servicio en la BUI \[324\]](#)
- [Selección de un servicio en la CLI \[325\]](#)
- Activación de un servicio: [BUI](#), [CLI](#)
- Desactivación de un servicio: [BUI](#), [CLI](#)
- [Visualización de los estados de los servicios en la CLI \[327\]](#)
- [Visualización de la ayuda de un servicio en la CLI \[328\]](#)
- Configuración de las propiedades de los servicios: [BUI](#), [CLI](#)
- Visualización de logs de servicio: [BUI](#), [CLI](#)
- [“Lista de servicios de dispositivo disponibles” \[332\]](#)
- [“Puertos de servicio necesarios” \[334\]](#)

Para obtener información acerca de cómo configurar un servicio individual, seleccione uno de los servicios de la siguiente tabla:

Servicios de datos	Servicios de directorio	Configuración del sistema	Acceso remoto
NFS	NIS	DNS	SSH
iSCSI	LDAP	IPMP	API de RESTful
SMB	Active Directory	NTP	HTTPS
FTP	Asignación de identidad	Asistencia técnica remota	
HTTP		Enrutamiento dinámico	
NDMP		Etiquetas de servicio	
Replicación remota		SMTP	
Migración shadow		SNMP	
SFTP		Syslog	
SRP		Identidad de sistema	
TFTP		Kerberos	

Servicios de datos	Servicios de directorio	Configuración del sistema	Acceso remoto
Análisis de virus			
Nube			

Gestión de servicios

Para obtener información acerca de la gestión de los servicios del dispositivo, consulte las siguientes tareas:

- [Visualización de un servicio en la BUI \[324\]](#)
- [Selección de un servicio en la CLI \[325\]](#)
- Activación de un servicio: [BUI](#), [CLI](#)
- Desactivación de un servicio: [BUI](#), [CLI](#)
- [Visualización de los estados de los servicios en la CLI \[327\]](#)
- [Visualización de la ayuda de un servicio en la CLI \[328\]](#)
- Configuración de las propiedades de los servicios: [BUI](#), [CLI](#)
- Visualización de logs de servicio: [BUI](#), [CLI](#)
- [“Lista de servicios de dispositivo disponibles” \[332\]](#)
- [“Puertos de servicio necesarios” \[334\]](#)

▼ Visualización de un servicio en la BUI

1. Vaya a **Configuración > Servicios**.
2. Para ver o editar las propiedades de un servicio específico, mueva el cursor sobre el ícono de estado del servicio que se encuentra a la izquierda del nombre del servicio.

El ícono de estado se convierte en un ícono de flecha .

3. Haga clic en el ícono de flecha  para visualizar la pantalla de propiedades para el servicio seleccionado.
4. En cualquiera de las pantallas de los servicios, puede hacer clic en el ícono de la flecha pequeña que se encuentra a la izquierda del título **Servicios** (cerca de la parte superior izquierda de cada pantalla) para mostrar un panel lateral de todos los servicios. Haga clic en este ícono nuevamente para ocultar la lista.

Temas relacionados

- [Activación de un servicio \(BUI\) \[325\]](#)
- [Configuración de las propiedades de los servicios \(BUI\) \[328\]](#)
- [“Lista de servicios de dispositivo disponibles” \[332\]](#)
- [“Puertos de servicio necesarios” \[334\]](#)

▼ Selección de un servicio en la CLI

Después de haber seleccionado un servicio, puede ver el estado, activarlo, desactivarlo y configurar las propiedades.

1. **Vaya a `configuration services`.**
2. **Para seleccionar un servicio, escriba el nombre del servicio. Por ejemplo, introduzca `nis`:**

```
hostname:configuration services> nis
hostname:configuration services nis>
```

Temas relacionados

- [Activación de un servicio \(CLI\) \[326\]](#)
- [Configuración de las propiedades de los servicios \(CLI\) \[329\]](#)
- [“Lista de servicios de dispositivo disponibles” \[332\]](#)
- [“Puertos de servicio necesarios” \[334\]](#)

▼ Activación de un servicio (BUI)

Utilice el siguiente procedimiento para activar un servicio que no está en línea.

1. **Vaya a `Configuración > Servicios`.**
2. **Haga clic en el ícono de encendido  para pasar el servicio al modo en línea .**

Temas relacionados

- [Desactivación de un servicio \(BUI\) \[326\]](#)

- [Configuración de las propiedades de los servicios \(BUI\) \[328\]](#)
- [“Lista de servicios de dispositivo disponibles” \[332\]](#)
- [“Puertos de servicio necesarios” \[334\]](#)

▼ Activación de un servicio (CLI)

Utilice el siguiente procedimiento para activar un servicio que no está en línea.

1. **Vaya a configuration services.**
2. **Seleccione un servicio, luego, introduzca el comando `enable` para activar un servicio.**

```
hostname:configuration services> nis
hostname:configuration services nis> enable
```

Temas relacionados

- [Desactivación de un servicio \(CLI\) \[327\]](#)
- [Configuración de las propiedades de los servicios \(CLI\) \[329\]](#)
- [“Lista de servicios de dispositivo disponibles” \[332\]](#)
- [“Puertos de servicio necesarios” \[334\]](#)

▼ Desactivación de un servicio (BUI)

Utilice el siguiente procedimiento para desactivar un servicio que está en línea.

1. **Vaya a Configuración > Servicios.**
2. **Haga clic en el ícono de encendido  para pasar el servicio al modo fuera de línea .**

Temas relacionados

- [Activación de un servicio \(BUI\) \[325\]](#)
- [“Lista de servicios de dispositivo disponibles” \[332\]](#)
- [“Puertos de servicio necesarios” \[334\]](#)

▼ Desactivación de un servicio (CLI)

Utilice el siguiente procedimiento para desactivar un servicio que está en línea.

1. **Vaya a `configuration services`.**
2. **Seleccione el servicio, luego, introduzca el comando `disable` para desactivarlo.**

```
hostname:configuration services> nis
hostname:configuration services nis> disable
```

Temas relacionados

- [Activación de un servicio \(CLI\) \[326\]](#)
- [“Lista de servicios de dispositivo disponibles” \[332\]](#)
- [“Puertos de servicio necesarios” \[334\]](#)

▼ Visualización de los estados de los servicios en la CLI

Use el siguiente procedimiento para ver los estados del servicio.

1. **Vaya a `configuration services`.**
2. **Introduzca el comando `show` para enumerar el estado actual de todos los servicios.**
3. **Para ver el estado de un servicio individual, seleccione el servicio y, luego, introduzca `show`.**

```
hostname:configuration services> nis
hostname:configuration services nis> show
Properties:
    <status> = online
    domain = fishworks
    broadcast = true
    ypservers =
```

Temas relacionados

- [Activación de un servicio \(CLI\) \[326\]](#)
- [Configuración de las propiedades de los servicios \(CLI\) \[329\]](#)
- [“Lista de servicios de dispositivo disponibles” \[332\]](#)
- [“Puertos de servicio necesarios” \[334\]](#)

▼ Visualización de la ayuda de un servicio en la CLI

Use el siguiente procedimiento para visualizar los comandos disponibles para un servicio.

1. **Vaya a configuration services.**
2. **Seleccione el servicio e introduzca `help`.**

```
hostname:configuration services> nis
hostname:configuration services nis> help
Subcommands that are valid in this context:

help [topic]          => Get context-sensitive help. If [topic] is specified,
                        it must be one of "builtins", "commands", "general",
                        "help", "script" or "properties".

show                  => Show information pertinent to the current context

commit                => Commit current state, including any changes

done                  => Finish operating on "nis"

enable                => Enable the nis service

disable               => Disable the nis service

get [prop]            => Get value for property [prop]. ("help properties"
                        for valid properties.) If [prop] is not specified,
                        returns values for all properties.

set [prop]            => Set property [prop] to [value]. ("help properties"
                        for valid properties.) For properties taking list
                        values, [value] should be a comma-separated list of
                        values.
```

Temas relacionados

- [Configuración de las propiedades de los servicios \(CLI\) \[329\]](#)
- [“Lista de servicios de dispositivo disponibles” \[332\]](#)
- [“Puertos de servicio necesarios” \[334\]](#)

▼ Configuración de las propiedades de los servicios (BUI)

Las pantallas Configuration (Configuración) > Services (Servicios) le permiten ver y modificar los servicios. En la siguiente tabla, se describen los íconos y los botones de las pantallas de servicios.

Ícono	Descripción
	Vaya a la pantalla de servicios para configurar propiedades y ver logs. Este botón aparece al mover el cursor sobre un servicio.
	El servicio está activado y funciona normalmente.
	El servicio está fuera de línea o desactivado.
	El servicio tiene un problema y se necesita la intervención del operador.
	Activa o desactiva el servicio.
	Reinicia el servicio.
	No se puede activar ni desactivar el servicio.
	Reinicia el servicio no disponible actualmente. Debe activar el servicio antes.

1. **Vaya a Configuración > Servicios.**
2. **Haga doble clic en un servicio.**
3. **Cambie las propiedades y, a continuación, haga clic en Aplicar.**
Para restablecer las propiedades, haga clic en Revertir.

Temas relacionados

- [Activación de un servicio \(BUI\) \[325\]](#)
- [“Lista de servicios de dispositivo disponibles” \[332\]](#)
- [“Puertos de servicio necesarios” \[334\]](#)

▼ Configuración de las propiedades de los servicios (CLI)

Utilice el siguiente procedimiento para definir las propiedades de un servicio. Los nombres de las propiedades son similares a los nombres correspondientes en la BUI, pero los nombres de la CLI normalmente son más cortos y a veces están abreviados.

1. **Vaya a `configuration services`.**

2. **Seleccione un servicio e introduzca `show` para ver la lista de propiedades que puede configurar para ese servicio, junto con sus valores actuales.**

```
hostname:configuration services> nis
hostname:configuration services nis> show
Properties:
    <status> = online
    domain =
    broadcast = true
    ypservers =
```

3. **Use el comando `set` para configurar las propiedades.**

```
hostname:configuration services nis> set domain="mydomain"
domain = mydomain (uncommitted)
```

4. **Después de configurar las propiedades, introduzca `commit` para guardar y activar la nueva configuración.**

```
hostname:configuration services nis> commit
hostname:configuration services nis> show
Properties:
    <status> = online
    domain = mydomain
    broadcast = true
    ypservers =
```

Temas relacionados

- [Activación de un servicio \(CLI\) \[326\]](#)
- [“Lista de servicios de dispositivo disponibles” \[332\]](#)
- [“Puertos de servicio necesarios” \[334\]](#)

▼ Visualización de logs de servicio (BUI)

Algunos servicios proporcionan logs de servicio que brindan información que ayuda a diagnosticar problemas con los servicios. Si el botón Logs aparece en la parte superior de la pantalla del servicio, significa que ese servicio proporciona un log. Los logs de servicio pueden proporcionar información acerca de la hora en la que cambió el estado de un servicio y los mensajes de error del servicio. El contenido de los logs es específico para cada servicio individual y puede cambiar.

1. **Vaya a **Configuration (Configuración) > Services (Servicios)** y haga doble clic en un servicio.**
2. **Haga clic en el botón Logs en la parte superior derecha de una pantalla de servicios.**

Los siguientes son ejemplos de mensajes comunes:

Mensaje de log de ejemplo	Descripción
Ejecutando método de inicio	El servicio se está iniciando.
Method "start" exited with status 0 (Se salió del método de inicio con estado)	El servicio informó que el inicio se realizó correctamente (0 == éxito).
Method "refresh" exited with status 0 (Se salió del método de actualización con estado)	El servicio actualizó correctamente la configuración en función de los parámetros del servicio.
Ejecutando método de detención	El servicio se está cerrando.
Enabled	Se comprobó el estado del servicio para ver si se lo debía iniciar (por ejemplo, durante el inicio del sistema) y se encontró que el servicio estaba activado.
Desactivado	Se comprobó el estado del servicio para ver si se lo debía iniciar (por ejemplo, durante el inicio del sistema) y se encontró que el servicio estaba desactivado.

El siguiente ejemplo de log es del servicio NTP:

```
[ Oct 15 21:05:31 Enabled. ]
[ Oct 15 21:07:37 Executing start method (...). ]
[ Oct 15 21:13:38 Method "start" exited with status 0. ]
```

El primer evento del log en este ejemplo muestra que el sistema se inició a las 21:05. La segunda entrada, a las 21:07:37, registra que el servicio comenzó a iniciarse y completó el inicio a las 21:13:38. Debido a la naturaleza de NTP y al ajuste del reloj del sistema, este servicio puede tardar varios minutos para completar el inicio, como se muestra en el log.

Temas relacionados

- [“Lista de servicios de dispositivo disponibles” \[332\]](#)
- [“Puertos de servicio necesarios” \[334\]](#)

▼ Visualización de logs de servicio (CLI)

- No es posible ver los registros de los servicios desde la CLI. Use la BUI como se describe en [Visualización de logs de servicio \(BUI\) \[330\]](#).

Lista de servicios de dispositivo disponibles

En esta sección se muestran los servicios del dispositivo disponibles junto con descripciones breves e información sobre el puerto. Ciertos servicios siempre están activados y no se los puede desactivar, tal como se describe en la tabla siguiente.

TABLA 52 Servicios de datos

Servicio	Descripción	Puertos usados
NFS	Acceso al sistema de archivos mediante los protocolos NFSv3, NFSv4.0 y NFS v4.1	111 y 2049
iSCSI	Acceso al LUN mediante el protocolo iSCSI	3260 y 3205
SMB	Acceso al sistema de archivos mediante el protocolo SMB	SMB mediante NetBIOS 139 SMB mediante TCP 445 Datagrama NetBIOS 138 Servicio de nombres NetBIOS 137
FTP	Acceso al sistema de archivos mediante el protocolo FTP	21
HTTP	Acceso al sistema de archivos mediante el protocolo HTTP	80
NDMP	Servicio de host NDMP	10000
Replicación remota	Replicación remota	216 y 217
Migración shadow	Migración shadow de datos	
SFTP	Acceso al sistema de archivos mediante el protocolo SFTP	218
SRP	Acceso de bloque mediante el protocolo SRP	
TFTP	Acceso al sistema de archivos mediante el protocolo TFTP	
Análisis de virus	Análisis de virus del sistema de archivos	
Nube	Servicio de datos en la nube para copias de seguridad de nube	

Nota - Los UID y los GID de 0 a 99 están reservados por el proveedor del sistema operativo para uso en aplicaciones futuras. Los usuarios finales del sistema y los proveedores de productos en capas no pueden utilizarlos ya que, si lo hicieran, se podrían producir problemas de seguridad con aplicaciones futuras.

TABLA 53 Servicios de directorio

Servicio	Descripción	Puertos usados
NIS	Autenticación de usuarios y grupos desde un servicio NIS.	
LDAP	Autenticación de usuarios y grupos desde un directorio LDAP.	389
Active Directory	Autenticación de usuarios con un servidor Active Directory de Microsoft. Nota - Una vez activado, este se convierte en un servicio que siempre está activado y no se puede desactivar.	
Asignación de identidad	Asignación entre entidades de Windows e ID de UNIX. Nota - Un servicio que está siempre activado, no se puede desactivar.	

TABLA 54 Valores del servicio

Servicio	Descripción	Puertos usados
DNS	Cliente de servicio de nombres de dominio Nota - Un servicio que está siempre activado, no se puede desactivar.	53
Enrutamiento dinámico	Protocolos de enrutamiento dinámico RIP y RIPng	
IPMP	Rutas múltiples de red IP para failover de IP Nota - Un servicio que está siempre activado, no se puede desactivar.	
Kerberos	Autenticación Kerberos	88
NTP	Cliente de protocolo de tiempo de red	
Asistencia técnica remota	Registro del producto y configuración de asistencia técnica	8000 (depende del puerto que se haya abierto en el proxy)
Service Tags	Asistencia para inventario del producto	6481
SMTP	Configuración del servidor de correo saliente Nota - Un servicio que está siempre activado, no se puede desactivar.	
SNMP	SNMP para enviar capturas sobre alertas y proporcionar información de estado del dispositivo	
Syslog	Relé Syslog para enviar mensajes Syslog sobre alertas y reenviar mensajes Syslog de servicios	
System Identity	Nombre y ubicación del sistema	

Servicio	Descripción	Puertos usados
	Nota - Un servicio que está siempre activado, no se puede desactivar.	

TABLA 55 Servicios de acceso remoto

Servicio	Descripción	Puertos usados
SSH	SSH para acceso desde la CLI	22
REST	API de RESTful Nota - Un servicio que está siempre activado, no se puede desactivar.	

Puertos de servicio necesarios

Para proporcionar seguridad en una red, puede implementar firewalls en la arquitectura de la red. Los números de puerto se usan para crear reglas de firewall e identificar de manera unívoca una transacción realizada por la red mediante la especificación del host y del servicio.

En la siguiente lista, se muestra la cantidad mínima de puertos necesarios para crear reglas de firewall que permitan utilizar todas las funciones del dispositivo:

Puertos de entrada

- icmp/0-65535 (PING)
- tcp/1920 (EM)
- tcp/215 (BUI)
- tcp/22 (SSH)
- udp/161 (SNMP)

Puertos de salida

- tcp/80 (WEB)
- tcp/443 (SSL WEB)

Nota - Un puerto de salida de tcp/443 se usa para enviar mensajes de asistencia técnica remota, cargar paquetes de asistencia y actualizar notificaciones. Para la replicación, de ser posible, use túneles GRE (Generic Routing Encapsulation, encapsulado de enrutamiento genérico). De esta manera, el tráfico circula por las interfaces de back end y se evita el firewall, que podría ralentizar el tráfico. Si no hay túneles GRE disponibles en el núcleo NFS, debe ejecutar la replicación por la interfaz de front end. En este caso, el puerto 216 y el puerto 217 también deben estar abiertos.

Configurando servicios

Para obtener información acerca de cómo configurar un servicio, seleccione uno de los servicios de la siguiente tabla:

Servicios de datos	Servicios de directorio	Configuración del sistema	Acceso remoto
NFS	NIS	DNS	SSH
iSCSI	LDAP	IPMP	API de RESTful
SMB	Active Directory	NTP	HTTPS
FTP	Asignación de identidad	Asistencia técnica remota	
HTTP		Enrutamiento dinámico	
NDMP		Etiquetas de servicio	
Replicación remota		SMTP	
Migración shadow		SNMP	
SFTP		Syslog	
SRP		Identidad de sistema	
TFTP		Kerberos	
Análisis de virus			
Nube			

Temas relacionados

- [“Lista de servicios de dispositivo disponibles” \[332\]](#)

Configuración de Active Directory

El servicio Active Directory (AD) proporciona acceso a la base de datos de Active Directory de Microsoft, que almacena información sobre usuarios, grupos, recursos compartidos y otros objetos compartidos.

Este servicio AD tiene dos modos: modo de dominio y modo de grupo de trabajo. Estos modos determinan cómo se autentican los usuarios de SMB. Al operar en modo de dominio, los clientes SMB se autentican por medio del controlador de dominios de AD. En el modo de grupo de trabajo, los clientes SMB se autentican localmente como usuarios locales. Consulte [“Configuración de usuarios” \[257\]](#) para obtener más información sobre usuarios locales.

Puede agregar un usuario de AD como administrador del dispositivo. Para obtener más información, consulte [“Configuración de usuarios” \[257\]](#).

Utilice uno de los siguientes métodos para la integración con AD:

- Apunte la configuración LDAP a AD.
AD debe incluir datos de UNIX, y el servicio AD debe usar nombres de tipo UNIX.
- Únase a un dominio de AD.
Use un nombre de usuario de AD *name@domain*. No es necesario configurar LDAP ni agregar datos de UNIX a AD.

Para configurar Active Directory, consulte las siguientes secciones:

- [Unión a un dominio AD \(BUI\) \[336\]](#)
- [Unión a un grupo de trabajo AD \(BUI\) \[337\]](#)
- [Configuración de Active Directory \(CLI\) \[337\]](#)
- [“Unión a un dominio de Active Directory” \[339\]](#)
- [“Dominios y grupos de trabajo de Active Directory” \[339\]](#)
- [“Compatibilidad de Active Directory con Windows” \[340\]](#)

▼ Unión a un dominio AD (BUI)

1. **(Opcional) Configure un sitio de Active Directory en el contexto de SMB.**
2. **(Opcional) Configure un controlador de dominios preferido en el contexto de SMB.**
3. **Active el NTP o asegúrese de que el reloj del dispositivo y el del controlador de dominio estén sincronizados con una diferencia de cinco minutos como máximo.**
4. **Asegúrese de que la infraestructura de DNS se delegue correctamente al dominio de Active Directory o establezca la dirección IP del controlador de dominios como servidor de nombres de DNS.**
Puede especificar hasta tres de sus controladores de dominios redundantes como servidores de nombres de DNS.
5. **Vaya a Configuration (Configuración) > Services (Servicios) > Active Directory y haga clic en Join Domain (Unirse a dominio).**
6. **Configure el dominio, el nombre de usuario administrativo y la contraseña administrativa de Active Directory.**
7. **Haga clic en APPLY (Aplicar) para confirmar la configuración.**

Temas relacionados

- [Unión a un grupo de trabajo AD \(BUI\) \[337\]](#)
- [Configuración de Active Directory \(CLI\) \[337\]](#)
- [“Unión a un dominio de Active Directory” \[339\]](#)
- [“Dominios y grupos de trabajo de Active Directory” \[339\]](#)
- [“Compatibilidad de Active Directory con Windows” \[340\]](#)

▼ Unión a un grupo de trabajo AD (BUI)

1. **Vaya a Configuration (Configuración) > Services (Servicios) > Active Directory y haga clic en Join Workgroup (Unirse a grupo de trabajo).**
2. **Introduzca el nombre del grupo de trabajo de Windows.**
3. **Haga clic en APPLY (Aplicar) para confirmar la configuración.**

Temas relacionados

- [Unión a un dominio AD \(BUI\) \[336\]](#)
- [Configuración de Active Directory \(CLI\) \[337\]](#)
- [“Unión a un dominio de Active Directory” \[339\]](#)
- [“Dominios y grupos de trabajo de Active Directory” \[339\]](#)
- [“Compatibilidad de Active Directory con Windows” \[340\]](#)

▼ Configuración de Active Directory (CLI)

1. **Vaya a configuration services ad.**

```
hostname:> configuration services ad
```

2. **Para ver una configuración existente, introduzca show.**

```
hostname:configuration services ad> show
Properties:
    <status> = online
    mode = domain
    domain = eng.test.com
```

```
Children:
    domain => Join an Active Directory domain
    workgroup => Join a Windows workgroup
```

Observe que el dispositivo actualmente funciona en el dominio eng.test.com.

3. Para salir del modo de dominio y unirse a un grupo de trabajo de Windows, introduzca los siguientes comandos:

```
hostname:configuration services ad> workgroup
hostname:configuration services ad workgroup> set workgroup=WORKGROUP
hostname:configuration services ad workgroup> commit
hostname:configuration services ad workgroup> done
hostname:configuration services ad> show
Properties:
    <status> = disabled
    mode = workgroup
    workgroup = WORKGROUP
```

4. Para configurar el sitio y el controlador de dominios preferido en preparación para unir otro dominio, introduzca los comandos siguientes:

```
hostname:configuration services ad> done
hostname:> configuration services smb
hostname:configuration services smb> set ads_site=sf
hostname:configuration services smb> set pdc=192.0.2.21
hostname:configuration services smb> commit
hostname:configuration services smb> show
Properties:
    <status> = online
    lmauth_level = 4
    pdc = 192.168.3.21
    ads_site = sf
hostname:configuration services smb> done
```

5. Para unir el dominio nuevo una vez configuradas las propiedades, introduzca los comandos siguientes.

Al unirse a un dominio de AD, debe establecer el usuario y la contraseña cada vez que confirme el nodo.

```
hostname:> configuration services ad
hostname:configuration services ad> domain
hostname:configuration services ad domain> set domain=example.com
hostname:configuration services ad domain> set user=Administrator
hostname:configuration services ad domain> set password=(set)
hostname:configuration services ad domain> commit
hostname:configuration services ad domain> done
hostname:configuration services ad> show
Properties:
    <status> = online
    mode = domain
    domain = example.com
```

Temas relacionados

- [Unión a un dominio AD \(BUI\) \[336\]](#)
- [Unión a un grupo de trabajo AD \(BUI\) \[337\]](#)
- [“Unión a un dominio de Active Directory” \[339\]](#)
- [“Dominios y grupos de trabajo de Active Directory” \[339\]](#)
- [“Compatibilidad de Active Directory con Windows” \[340\]](#)

Unión a un dominio de Active Directory

Si la cuenta todavía no existe por defecto en Active Directory, se crea automáticamente una cuenta de confianza de la máquina para el sistema en el contenedor por defecto para las cuentas de computadoras (cn=Computers) como parte de la operación para unirse al dominio. Los siguientes usuarios tienen permitido realizar operaciones de unión al dominio:

- **Administrador del dominio:** puede unir la cantidad de sistemas que desee al dominio; las cuentas de confianza de los equipos pueden estar en cualquier contenedor.
- **Administrador delegado con autoridad sobre una o varias unidades organizativas:** puede unir la cantidad de sistemas que desee al dominio; las cuentas de los equipos deben encontrarse en las unidades organizativas por las que es responsable.
- **Usuario normal con cuentas de equipo preprocesadas por el administrador:** puede unir sistemas al dominio si cuenta con la autorización previa del administrador.
- **Usuario normal:** normalmente está autorizado a unir una cantidad limitada de sistemas.

Las siguientes son las propiedades disponibles para las operaciones de unión a dominios de Active Directory:

- **Dominio de Active Directory:** nombre completo o nombre de NetBIOS de un dominio de Active Directory.
- **Usuario:** usuario de AD que tiene credenciales para crear una cuenta en Active Directory.
- **Contraseña:** contraseña del usuario administrativo.
- **Unidad organizativa:** especifica una unidad organizativa alternativa en la que se creará la cuenta de confianza de equipo del sistema. La unidad organizativa se especifica como lista separada por comas de uno o varios pares de valores de nombre que usan el formato de nombre distintivo correspondiente al dominio, por ejemplo, ou=innerOU,ou=outerOU.
- **Usar cuenta creada con anterioridad:** si la cuenta del sistema ya existe y la unidad organizativa especificada no es la unidad en la que se encuentra la cuenta, use la cuenta creada con anterioridad.

Temas relacionados

- [Unión a un dominio AD \(BUI\) \[336\]](#)
- [Unión a un grupo de trabajo AD \(BUI\) \[337\]](#)
- [Configuración de Active Directory \(CLI\) \[337\]](#)
- [“Dominios y grupos de trabajo de Active Directory” \[339\]](#)
- [“Compatibilidad de Active Directory con Windows” \[340\]](#)

Dominios y grupos de trabajo de Active Directory

La propiedad configurable para unirse a un grupo de trabajo es Windows Workgroup.

En lugar de activar y desactivar el servicio directamente, se modifica el servicio mediante la unión a un dominio o un grupo de trabajo. La unión a un dominio implica la creación de una cuenta para el dispositivo en el dominio de Active Directory determinado. El nombre de la cuenta puede tener un máximo de 15 caracteres y debe ser único con respecto a los demás nombres registrados en el dominio de Active Directory. De no ser así, se pueden producir conflictos con dispositivos que tengan nombres similares, lo que a su vez generaría problemas de funcionalidad. Después de haber establecido la cuenta del equipo, el dispositivo puede hacer consultas de manera segura en la base de datos para buscar información sobre usuarios, grupos y recursos compartidos.

Al unirse a un grupo de trabajo, se abandona de manera implícita un dominio de Active Directory, y los clientes SMB que se almacenan en la base de datos de Active Directory no pueden conectarse a los recursos compartidos.

Firmas de LDAP de Active Directory

No hay una opción de configuración para firmas de LDAP, ya que esa opción se negocia automáticamente al comunicarse con el controlador del dominio. Las firmas de LDAP se aplican a las comunicaciones entre el dispositivo de almacenamiento y el controlador de dominios, mientras que las firmas de SMB se aplican a las comunicaciones entre los clientes SMB y el dispositivo de almacenamiento.

Temas relacionados

- [Unión a un dominio AD \(BUI\) \[336\]](#)
- [Unión a un grupo de trabajo AD \(BUI\) \[337\]](#)
- [Configuración de Active Directory \(CLI\) \[337\]](#)
- [“Unión a un dominio de Active Directory” \[339\]](#)
- [“Compatibilidad de Active Directory con Windows” \[340\]](#)

Compatibilidad de Active Directory con Windows

Compatibilidad de Active Directory con Windows Server

La versión OS8.8.x del software Oracle ZFS Storage Appliance admite todas las versiones de servidor de Active Directory.

Compatibilidad de Active Directory con clientes Windows

A partir de Windows 10, los clientes pueden activar la autenticación Kerberos con nombres de principal de servicio (SPN) basados en direcciones IP. Para ello, deben crear una entrada de registro TryIPSPN. Para obtener más información, consulte [Configuración de Kerberos](#)

[para direcciones IP](#). No obstante, Oracle ZFS Storage Appliance no admite SPN basados en direcciones IP.

Al igual que Windows, Oracle ZFS Storage Appliance no registra los SPN basados en direcciones IP como parte de la unión al dominio de AD. Microsoft advierte los siguientes potenciales problemas con los SPN basados en direcciones IP: normalmente, no se usan direcciones IP en lugar de nombres de host, ya que las direcciones IP a menudo son temporarias. El uso de direcciones IP puede provocar conflictos y fallos en la autenticación, ya que los permisos de direcciones caducan y se renuevan. Por lo tanto, el registro de un SPN basado en direcciones IP es un proceso manual y solo debe usarse cuando no sea posible cambiar a un nombre de host basado en DNS.

Una vez activada la configuración del registro TryIPSPN, los clientes Windows 10 pueden acceder a los recursos compartidos de SMB que exporta el dispositivo mediante NTLMSSP. Si el administrador del dominio agregó manualmente SPN `cifs\appliance-IP-address` al atributo ServicePrincipalName del objeto de computadora de AD correspondiente al dispositivo, el KDC de Windows podrá emitir tickets de servicio del CIFS para el dispositivo mediante los SPN basados en direcciones IP. Sin embargo, si el cliente posteriormente presenta un ticket de servicio del CIFS que usa SPN basados en direcciones IP para acceder a recursos de SMB en el dispositivo, el subsistema Kerberos del dispositivo rechazará el contexto de seguridad. Esto se debe a la falta de compatibilidad con los SPN basados en direcciones IP. Como consecuencia, `debug.sys` presenta los siguientes mensajes de aviso:

```
krbssp: user authentication failed (GSS major error): No credentials were
supplied, or the credentials were unavailable or inaccessible
krbssp: user authentication failed (GSS minor error): No principal in keytab
('FILE:/var/krb5/krb5.keytab') matches desired name cifs/appliance-IP-address@AD-realm
```

Para evitar este problema, los SPN basados en direcciones IP no deben publicarse en un servidor de AD.

Temas relacionados

- [Unión a un dominio AD \(BUI\) \[336\]](#)
- [Unión a un grupo de trabajo AD \(BUI\) \[337\]](#)
- [Configuración de Active Directory \(CLI\) \[337\]](#)
- [“Unión a un dominio de Active Directory” \[339\]](#)
- [“Dominios y grupos de trabajo de Active Directory” \[339\]](#)

Configuración de DNS

El cliente DNS (servicio de nombres de dominio) proporciona la capacidad de resolver direcciones IP como nombres de host, y viceversa, y se puede activar o desactivar. De manera opcional, si se configura y activa la resolución secundaria de nombres de host mediante NIS

y/o LDAP, se la puede solicitar para nombres de host y direcciones que no se pueden resolver con DNS. La resolución de nombres de host se utiliza en todas las interfaces de usuario del dispositivo, incluso en Logs, para indicar la ubicación desde la cual un usuario realizó una acción auditable, y en Análisis, para proporcionar estadísticas por cliente.

Para configurar y gestionar DNS, realice estos procedimientos:

- Configuración de DNS: [BUI](#), [CLI](#)
- Uso de la herramienta de comprobación del sistema de DNS: [BUI](#), [CLI](#)
- “Prueba de resolución de nombres de host (CLI)” [346]
- Agregación de servidores DNS: [BUI](#), [CLI](#)
- Visualización del estado del servidor DNS: [BUI](#), [CLI](#)

Para comprender el uso de DNS para el dispositivo, lea los siguientes temas:

- “Propiedades y logs de DNS” [349]
- “Active Directory y DNS” [350]
- “Resolución no DNS” [350]
- “Operación sin DNS” [351]

▼ Configuración de DNS (BUI)

DNS normalmente se configura durante la configuración inicial, como se describe en “Configuración inicial (BUI)” en la *Guía de instalación de Oracle ZFS Storage Appliance*. Para cambiar la configuración de DNS después de la configuración inicial, realice el siguiente procedimiento.

1. Vaya a Configuración > Servicios > DNS.

2. En Configuración general, defina las siguientes propiedades:

Para obtener más información acerca de las propiedades de DNS, consulte “Propiedades y logs de DNS” [349].

- **Dominio DNS:** introduzca un nombre de dominio.
- **Dominios de búsqueda de DNS:** haga clic en el ícono de agregación  para agregar dominios de búsqueda. Para eliminar un dominio, haga clic en el ícono de eliminación  que está junto al dominio que desea eliminar.
- **Permitir resolución no DNS IPv4:** seleccione esta casilla para activar la resolución no DNS de direcciones IPv4. Consulte “Resolución no DNS” [350].
- **Permitir resolución no DNS IPv6:** seleccione esta casilla para activar la resolución no DNS de direcciones IPv6. Consulte “Resolución no DNS” [350].

3. Haga clic en Aplicar.

Temas relacionados

- [Agregación de un servidor DNS \(BUI\) \[346\]](#)
- [“Comprobación del sistema de DNS” \[344\]](#)

▼ Configuración de DNS (CLI)

DNS normalmente se configura durante la configuración inicial, como se describe en [“Configuración inicial \(CLI\)” en la Guía de instalación de Oracle ZFS Storage Appliance](#). Para cambiar la configuración de DNS después de la configuración inicial, realice el siguiente procedimiento.

1. Vaya a `configuration services dns` e introduzca `show`.

```
hostname:> configuration services dns
hostname:configuration services dns> show
Properties:
    <status> = online
    domain = example.com
    servers = IP-address
    search =
    allow_alternate_v4 = false
    allow_alternate_v6 = false
```

2. Establezca el dominio, los servidores y el dominio de búsqueda y active o desactive la resolución no DNS.

Para obtener más información, consulte [“Propiedades y logs de DNS” \[349\]](#) y [“Resolución no DNS” \[350\]](#).

```
hostname:configuration services dns> set domain=example.com
    domain = example.com (uncommitted)
hostname:configuration services dns> set servers=IP-address
    servers = IP-address (uncommitted)
hostname:configuration services dns> set search=example.com
    search = example.com (uncommitted)
hostname:configuration services dns> set allow_alternate_v4=true
    allow_alternate_v4 = true (uncommitted)
```

3. Introduzca el comando `commit`.

```
hostname:configuration services dns> commit
```

Temas relacionados

- [Agregación de un servidor DNS \(CLI\) \[347\]](#)
- [“Comprobación del sistema de DNS” \[344\]](#)

Comprobación del sistema de DNS

La herramienta de comprobación del sistema de DNS verifica la validez de su configuración de DNS. Si un dispositivo tiene un problema y la configuración de DNS es dudosa, esta herramienta puede ayudar a identificar el problema o eliminar la configuración de DNS que contribuyó al problema.

Además de comprobar el dispositivo donde se ejecuta la herramienta, puede especificar otro nombre de host o dirección IP para comprobar.

La herramienta de comprobación del sistema de DNS identifica configuraciones cuestionables como las siguientes:

- Datos de DNS faltantes o incoherentes, como la falta de registros A o PTR, o la falta de coincidencia del nombre de los registros A y PTR.
- Problemas con la búsqueda de nombres públicos de Internet.
- Problemas con la búsqueda de direcciones inexistentes.
- Problemas de rendimiento de las consultas.

La herramienta de comprobación del sistema de DNS detecta los posibles problemas de configuración y los informa como advertencias, en lugar de errores, ya que la configuración podría ser adecuada para una situación específica. Asegúrese de comprender la advertencia y la situación específica del sistema que se está evaluando.

Los siguientes son ejemplos de problemas de configuración que la herramienta de comprobación del sistema de DNS podría no identificar:

- La herramienta no puede detectar alias y, por lo tanto, no puede detectar un problema como el siguiente:
 - Referencias de cliente mediante registros CNAME.
 - Nombres con registros A que hacen referencia al sistema cuando estos nombres no aparecen en los registros PTR.
- Configuración de DNS específica de Active Directory (AD); por ejemplo, los registros SRV que se usan para ubicar los controladores de dominios.

Además de producir las advertencias, el informe que genera la herramienta de comprobación del sistema de DNS incluye los pasos detallados que se realizaron para detectar cada advertencia de configuración. Por ejemplo, si las direcciones de interfaz configuradas del sistema incluyen una dirección cuyo registro PTR se refiere a otro nombre, el informe mostrará una descripción como la siguiente:

```
WARN: 1.2.3.4 is b.example.com, expected a.example.com
      interfaces -> 1.2.3.4
```

PTR 1.2.3.4 -> b.example.com

Puede mostrar todas las operaciones de búsqueda que den como resultado una advertencia informada. Puede mostrar todos los pasos realizados por la herramienta de comprobación del sistema de DNS y no solo los pasos que den como resultado una advertencia informada.

▼ Uso de la herramienta de comprobación del sistema de DNS (BUI)

1. **Vaya a Configuración > Servicios > DNS.**
2. **Haga clic en la ficha Estado.**
3. **(Opcional) En la sección Prueba, especifique el sistema donde ejecutará la comprobación del sistema de DNS.**
 Por defecto, está seleccionado el sistema actual.
 Para especificar otro sistema:
 - a. **Seleccione el botón de radio "Otro sistema".**
 - b. **En el campo de texto, introduzca el nombre de host o la dirección IP del sistema que se comprobará.**
4. **Haga clic en el botón Ejecutar.**
5. **En la sección Resultados, examine la salida de la comprobación del sistema de DNS.**
 Por defecto, está seleccionada la ficha Advertencias, que muestra solo las advertencias de configuración.
 - Para mostrar todos los pasos de la prueba, incluidos los que no dan como resultado una advertencia, seleccione la ficha Mostrar todo.
 - Para mostrar todas las operaciones de búsqueda que dan como resultado un mensaje determinado, haga doble clic en cualquier parte del mensaje y, luego, en el ícono de información  ubicado a la derecha del mensaje. La siguiente información adicional aparece en una ventana emergente por separado.

Temas relacionados

- [Configuración de DNS \(BUI\) \[342\]](#)
- ["Comprobación del sistema de DNS" \[344\]](#)

▼ Uso de la herramienta de comprobación del sistema de DNS (CLI)

1. **Vaya a `configuration services dns`.**
2. **Use el comando `health` para ejecutar la herramienta de comprobación del sistema de DNS en el sistema actual o en otro sistema.**

Con el comando `health`, se pueden especificar las opciones siguientes:

- a Muestra todos los pasos, incluidos los que no dan como resultado una advertencia.
- v Muestra todas las operaciones de búsqueda que dan como resultado un mensaje determinado.

- **Para ejecutar la herramienta en este sistema, introduzca `health`.**
- **Para ejecutar la herramienta en otro sistema, introduzca uno de los siguientes comandos:**

```
health hostname  
health IP-address
```

Temas relacionados

- [Configuración de DNS \(CLI\) \[343\]](#)
- [“Comprobación del sistema de DNS” \[344\]](#)

Prueba de resolución de nombres de host (CLI)

Los valores incorporados devueltos por la CLI `nslookup` y `getent hosts` se pueden comparar para probar si la resolución de nombres de host está funcionando:

```
hostname:> nslookup hostname  
IP-address    hostname.com  
hostname:> getent hosts hostname  
IP-address    hostname.com
```

▼ Agregación de un servidor DNS (BUI)

1. **Vaya a Configuración > Servicios > DNS.**
2. **Haga clic en el ícono de agregación  que está junto a Servidores DNS.**
3. **En el cuadro de diálogo Servidor DNS nuevo, introduzca la dirección IP del servidor.**

4. Haga clic en Agregar.

Se envía una consulta a los servidores DNS afectados para validar los cambios. Si no se recibe una respuesta válida, aparece un mensaje para confirmar la configuración. Puede confirmar los cambios independientemente de si el servidor es válido o no.

Temas relacionados

- [Visualización del estado del servidor DNS \(BUI\) \[348\]](#)

▼ Agregación de un servidor DNS (CLI)

1. Vaya a `configuration services dns` e introduzca `create`.

```
hostname:> configuration services dns
hostname:configuration services dns> create
```

2. Introduzca `show`.

```
hostname:configuration services server (uncommitted)> show
Properties:
    address = (unset)
    status = unavailable
    rtt = unavailable
    err_msg =
```

3. Introduzca `set address=` y la dirección del servidor.

```
hostname:configuration services server (uncommitted)> set address=192.0.2.254
address = 192.0.2.254 (uncommitted)
```

4. Introduzca `show`.

```
hostname:configuration services server (uncommitted)> show
Properties:
    address = 192.0.2.254
    status = online
    rtt = 1.812ms
    err_msg =
```

5. Introduzca el comando `commit`.

Se envía una consulta a los servidores DNS afectados para validar los cambios. Si no se recibe una respuesta válida, aparece un mensaje para confirmar la configuración. Puede confirmar los cambios independientemente de si el servidor es válido o no.

```
hostname:configuration services server (uncommitted)> commit
```

Temas relacionados

- [Visualización del estado del servidor DNS \(CLI\) \[348\]](#)

▼ Visualización del estado del servidor DNS (BUI)

Los detalles de los servidores DNS se muestran junto a cada entrada en la BUI. Un indicador de estado muestra si el estado del servidor es en línea, fuera de línea o desconocido. La columna RTT indica el tiempo de ida y vuelta, en milisegundos, para recibir una respuesta válida.

1. **Vaya a Configuración > Servicios > DNS.**
2. **En Servidores DNS, compruebe el indicador de estado que está junto a cada entrada de servidor:**

- **Ícono verde**  : en línea
- **Ícono ámbar**  : fuera de línea
- **Ícono gris**  : desconocido

▼ Visualización del estado del servidor DNS (CLI)

Seleccione un servidor DNS para ver sus propiedades. La propiedad `status` indica si el estado del servidor es en línea, fuera de línea o desconocido. La propiedad `rtt` indica el tiempo de ida y vuelta, en milisegundos, para recibir una respuesta válida. Si el estado del servidor es fuera de línea, la propiedad `err_msg` muestra el motivo, por ejemplo, `connection timed out`.

1. **Vaya a `configuration services dns` e introduzca `show`.**

```
hostname:> configuration services dns
hostname:configuration services dns> show
SERVER      STATUS      ADDRESS
server-000  online      198.51.100.1
server-001  offline     198.51.100.2
```

2. **Seleccione el servidor cuyo estado desea ver.**

```
hostname:configuration services dns> select server-000
```

3. **Introduzca `show`.**

```
hostname:configuration services server-000> show
Properties:
    address = 198.51.100.1
    status = online
    rtt = 1.768ms
    err_msg =
```


Propiedades y logs de DNS

Las propiedades configurables del cliente DNS incluyen un nombre de dominio base y una lista de servidores, especificados por dirección IP. Debe proporcionar un nombre de dominio y al menos una dirección de servidor; el servidor debe poder devolver un registro de NS (NameServer) para el dominio que especifica, aunque no es necesario que sea autoritativo para ese dominio.

TABLA 56 Propiedades de DNS

Propiedad	Descripción
Dominio DNS	Nombre de dominio en el que se busca primero al realizar búsquedas de nombres de host parciales..
Servidores DNS	Uno o varios servidores DNS. Se deben usar direcciones IP.
Dominio(s) de búsqueda de DNS	Lista de hasta cuatro dominios en los que se puede buscar el dominio de Active Directory, el dominio de búsqueda de Active Directory anticuado y el dominio de DNS especificado.
Permitir resolución no DNS IPv4	Las direcciones IPv4 se pueden resolver como nombres de host, y viceversa, mediante NIS y/o LDAP si se configuran y activan.
Permitir resolución no DNS IPv6	Las direcciones IPv4 e IPv6 se pueden resolver como nombres de host, y viceversa, mediante NIS y/o LDAP si se configuran y activan.

Los cambios realizados en las propiedades de los servicios se documentan en las secciones [Configuración de las propiedades de los servicios \(BUI\) \[328\]](#) y [Configuración de las propiedades de los servicios \(CLI\) \[329\]](#). Los nombres de propiedades de la CLI son versiones más abreviadas que las mencionadas anteriormente.

TABLA 57 Logs de DNS

Log	Descripción
network-dns-client:default	Registra los eventos del servicio DNS

Temas relacionados

- [“Active Directory y DNS” \[350\]](#)

Active Directory y DNS

Si tiene pensado utilizar Active Directory, los servidores deben poder resolver registros de servidores y nombres de host en la parte de Active Directory del espacio de nombres del dominio. Por ejemplo, si el dispositivo reside en el dominio example.com y la porción de Active Directory del espacio de nombres es redmond.example.com, los servidores de nombres deben poder alcanzar un servidor autoritativo para example.com y deben proporcionar delegación para el dominio redmond.example.com a uno o varios servidores Active Directory que sirvan ese dominio. Estos requisitos son impuestos por Active Directory, no por el dispositivo. Si no se los cumple, no podrá unirse a dominios de Active Directory.

Nota - Con OS8.6.0 y posteriores, si el sufijo del dominio DNS principal no coincide con el nombre de DNS de Active Directory, la configuración `d` como resultado un espacio de nombres separado. Si no desea un espacio de nombres separado, asegúrese de que el dominio DNS y el dominio de Active Directory sean iguales.

Temas relacionados

- [“Configuración de DNS” \[341\]](#)
- [“Configuración de Active Directory” \[335\]](#)

Resolución no DNS

DNS es un mecanismo estándar, de nivel empresarial, altamente escalable y confiable para realizar asignaciones entre nombres de host y direcciones IP. El uso de servidores DNS es una práctica recomendada que, por lo general, genera los mejores resultados. En algunos entornos, puede haber un subconjunto de hosts que se pueden resolver solo mediante asignaciones NIS o LDAP. Si esto es así en su entorno, active la resolución de hosts no DNS y configure los servicios de directorios apropiados. Si se usa LDAP para la resolución de hosts, la asignación de hosts debe encontrarse en el DN estándar de la base de datos: `ou=Hosts,(Base DN)` y debe utilizar el esquema estándar. Cuando se usa este modo con uso compartido de NFS mediante grupos de redes, puede ser necesario que los sistemas cliente utilicen el mismo mecanismo de resolución de nombres de host que el que está configurado en el dispositivo porque, de no hacerlo, las excepciones de uso compartido de NFS podrían no funcionar correctamente.

Cuando se activa la resolución de hosts no DNS, igual se usa DNS. Se usan NIS (si está activado) y LDAP (si está activado) para resolver el nombre o la dirección solo si una dirección o un nombre de host no se puede resolver con DNS. Esto puede tener resultados confusos y aparentemente incoherentes. Puede validar los resultados de resolución de hosts con el comando `getent` de la CLI que se describió más arriba.

Se desalienta el uso de estas opciones.

Operación sin DNS

Si el dispositivo no puede acceder a ninguno de los servidores DNS desde la ubicación de instalación en la red, puede elegir operar sin DNS. Para ello, debe proporcionar la dirección de servidor 127.0.0.1. Para operar sin DNS:

- **BUI:** Vaya a Configuración > Servicios > DNS. En el campo Servidores de DNS, introduzca `127.0.0.1`.
- **CLI:** Vaya a `configuration services dns` e introduzca `show`. Introduzca `set servers=127.0.0.1` y, a continuación, introduzca `commit`.

No se recomienda el uso de este modo, ya que hay varias funciones que no se ejecutarán correctamente, por ejemplo:

- En Análisis, no se podrán resolver direcciones de cliente como nombres de host.
- La función de Active Directory no funcionará (no podrá unirse a dominios).
- El uso de LDAP protegido por SSL no funcionará correctamente con certificados que contengan nombres de host.
- Las acciones de umbral y alerta que requieren el envío de mensajes de correo electrónico solamente se pueden enviar a servidores de correo que se encuentran en una subred conectada, y todas las direcciones se deben especificar con la dirección IP del servidor de correo.
- Algunas operaciones pueden tardar más de lo normal debido a los tiempos de espera para la resolución de los nombres de host.

Estas limitaciones pueden mitigarse parcialmente mediante el uso de un servicio de resolución de hosts alternativo; consulte [“Resolución no DNS” \[350\]](#).

Temas relacionados

- Activación de un servicio [BUI](#), [CLI](#)
- Desactivación de un servicio [BUI](#), [CLI](#)

Configuración de enrutamiento dinámico

El protocolo de información de enrutamiento (RIP) es un protocolo de enrutamiento dinámico de distancia-vector utilizado por el dispositivo para configurar de manera automática las rutas óptimas en función de los mensajes recibidos de otros hosts en enlaces con RIP activado (normalmente enrutadores). El dispositivo admite RIPv1 y RIPv2 para IPv4, y RIPng para IPv6.

Las rutas que se configuran mediante estos protocolos se marcan con el tipo "dinámico" en la tabla de enrutamiento. RIP y RIPng escuchan en los puertos UDP 520 y 521, respectivamente.

TABLA 58 Enrutamiento dinámico

Log	Descripción
network-routing-route:default	Registra eventos del servicio RIP.
network-routing-ripng:quagga	Registra eventos del servicio RIPng.

Configuración de FTP

El servicio FTP (protocolo de transferencia de archivos) permite tener acceso al sistema de archivos desde clientes FTP. No se permite el inicio de sesión anónimo; los usuarios deben autenticarse con el servicio de nombres que está configurado en Servicios.

El FTP se puede usar en combinación con la autenticación Kerberos. Para obtener información acerca del servicio Kerberos del dispositivo, consulte [“Configuración de Kerberos” \[377\]](#). Para una mayor seguridad al configurar FTP, puede especificar los cifrados y las versiones de SSL/TLS, como se describe en [“Propiedades de FTP” \[353\]](#).

En un entorno en cluster, solo es posible acceder a un recurso compartido en el controlador que lo gestiona. Si el parámetro `default_root` hace referencia a un recurso compartido, el acceso a FTP será posible solo desde el controlador que actualmente es propietario de ese recurso compartido. Si el parámetro `user_home` hace referencia a un recurso compartido, el cambio automático al directorio del usuario solo será posible desde el controlador que actualmente es propietario del recurso compartido.

Para configurar el FTP, consulte las siguientes secciones:

- [Agregación de acceso FTP a un recurso compartido \(BUI\) \[352\]](#)
- [“Propiedades de FTP” \[353\]](#)
- [“Logs de FTP” \[355\]](#)

▼ Agregación de acceso FTP a un recurso compartido (BUI)

1. **Vaya a Configuración > Servicios.**
2. **Asegúrese de que el servicio FTP esté activado y en línea. De no ser así, actívelo.**
3. **Seleccione o agregue un recurso compartido en la pantalla Recursos compartidos.**
4. **Haga clic en el separador Protocols (Protocolos) y compruebe que esté activado el acceso FTP.**

5. (Opcional) Configure el acceso de modo de recurso compartido en solo lectura o lectura/escritura.

Temas relacionados

- [“Propiedades de FTP” \[353\]](#)
- [“Logs de FTP” \[355\]](#)

Propiedades de FTP

TABLA 59 Propiedades generales de FTP

Propiedad	Descripción
Puerto para conexiones entrantes	Puerto mediante el cual el servicio FTP escucha. El valor por defecto es 21.
Cantidad máxima de conexiones ("0" es ilimitada)	La cantidad máxima de conexiones FTP simultáneas. Configure este valor de manera de cubrir la cantidad prevista de usuarios simultáneos. El valor por defecto es 30, porque cada conexión crea un proceso de sistema, y si se permiten demasiadas (miles), se podría producir un ataque de DoS.
Activar motor de retraso para prevenir ataques de temporización	Esta opción inserta pequeñas demoras durante la autenticación para frustrar, mediante mediciones de tiempo, intentos de adivinar nombres de usuario. Si se activa, mejora la seguridad.
Inicio de sesión root por defecto	La ubicación por defecto del inicio de sesión de FTP que puede configurarse de modo que todos los usuarios de FTP tengan un directorio FTP por defecto. ■ Si este valor es /, los usuarios de FTP ven todos los recursos compartidos. ■ Si este valor es cualquier otro (/export 0 /export/ftp), los usuarios de FTP solo pueden ver los recursos compartidos de FTP en ese directorio. ■ Si se proporciona una ruta de acceso válida en el campo Directorios principales del usuario, todos los usuarios de FTP que tengan un directorio en user_home tendrán su directorio de inicio de sesión por defecto configurado en /export al iniciar sesión.
Directorios principales del usuario	La ubicación de los directorios principales del usuario de FTP, en relación con el inicio de sesión root por defecto. ■ En el inicio de sesión, si un usuario tiene un directorio en esta ubicación, iniciará sesión en ese directorio después de autenticarse correctamente en el servicio FTP. ■ Si el usuario no tiene un directorio de inicio, iniciará sesión en la ubicación por defecto.

Propiedad	Descripción
	Deje esta propiedad vacía para desactivar los directorios principales de usuarios de FTP y que todos los usuarios inicien sesión en la ubicación de inicio de sesión por defecto.
Nivel de registro	El nivel de detalle del log <code>proftpd</code> .
Permisos para enmascarar desde archivos y directorios creados recientemente	Permisos de archivo para eliminar al crear archivos. El permiso de escritura de grupos y mundial está enmascarado por defecto para evitar que cualquiera pueda escribir en cargas recientes.

TABLA 60 Propiedades de seguridad de FTP

Propiedad	Descripción
Activar SSL/TLS	Permite conexiones FTP cifradas SSL/TLS. Con esta opción, se garantiza que la transacción FTP esté cifrada. Por defecto está desactivado.
Cifrados y versiones de SSL/TLS	Cifrados y versiones del protocolo SSL/TLS para conexiones FTP. Los valores por defecto son TLSv1.1, TLSv1.2 y los cifrados asociados. TLSv1.0 no está activado por defecto por cuestiones de seguridad, pero se puede activar para una compatibilidad con versiones anteriores. La lista de cifrados disponibles cambia en función de las versiones seleccionadas. Algunos cifrados o versiones del protocolo SSL/TLS seleccionados se eliminan después de una actualización de software si ya no se admiten. Para evitar la falta de disponibilidad del servicio, conserve la configuración por defecto, a menos que necesite cambiarla o que el soporte de Oracle le indique lo contrario.
Puerto para conexiones SSL/TLS entrantes	Puerto por el que el servicio FTP cifrado SSL/TLS escucha. El valor por defecto es 21.
Permitir inicio de sesión root	Permite al usuario root iniciar sesiones FTP. Desactivado por defecto, porque la autenticación FTP es de texto sin formato, lo que representa un riesgo de seguridad por ataques de examen de red.
Cantidad máxima de intentos de inicio de sesión permitidos	Cantidad de intentos de inicio de sesión incorrectos antes de que se desconecte la conexión FTP y el usuario tenga que volver a conectarse para intentarlo de nuevo. El valor por defecto es 3.
Permitir direcciones de conexión de datos externas	Permite que las conexiones FTP externas activen la transferencia directa de archivos entre servidores FTP. Esta propiedad está desactivada por defecto.

Temas relacionados

- [Agregación de acceso FTP a un recurso compartido \(BUI\) \[352\]](#)

- [“Logs de FTP” \[355\]](#)

Logs de FTP

TABLA 61 Logs de FTP

Log	Descripción
proftpd	Registra eventos de FTP, incluidos los inicios de sesión correctos y los intentos de inicio de sesión fallidos.
proftpd_xfer	Log de transferencia de archivos.
proftpd_tls	Registra eventos de FTP relacionados con el cifrado SSL/TLS.

Temas relacionados

- [Agregación de acceso FTP a un recurso compartido \(BUI\) \[352\]](#)
- [“Propiedades de FTP” \[353\]](#)

Configuración de HTTP

El servicio HTTP proporciona acceso a sistemas de archivos mediante el protocolo WebDAV (sistema distribuido de creación y control de versiones web) de HTTP. Este servicio permite a los clientes acceder a los sistemas de archivos compartidos mediante un explorador web o como sistema de archivos local si el software del cliente lo admite. La URL para acceder a estos recursos compartidos de HTTP tiene el siguiente formato:

- `http://hostname/shares/mountpoint/share_name`

HTTP se puede usar junto con la autenticación Kerberos. Para obtener información acerca del servicio Kerberos del dispositivo, consulte [“Configuración de Kerberos” \[377\]](#).

Para agregar seguridad al configurar HTTP, puede especificar los cifrados y las versiones de SSL/TLS, como se describe en [“Propiedades y logs de HTTP” \[356\]](#).

Para configurar el HTTP, consulte las siguientes secciones:

- [Agregación de acceso HTTP a un recurso compartido \(BUI\) \[356\]](#)
- [“Propiedades y logs de HTTP” \[356\]](#)
- [“Autenticación y control de acceso de HTTP” \[359\]](#)
- [“Configuración de la API de objeto” \[360\]](#)
- [Cómo trabajar con un servidor de Keystone \[361\]](#)

▼ Agregación de acceso HTTP a un recurso compartido (BUI)

1. Vaya a **Configuration (Configuración) > Services (Servicios)**.
2. Compruebe que el servicio HTTP esté activado y en línea. De no ser así, actívelo.
3. Seleccione o agregue un recurso compartido en la pantalla **Recursos compartidos**.
4. Haga clic en el separador **Protocols (Protocolos)** y compruebe que esté activado el acceso HTTP.
5. (Opcional) Configure el acceso de modo de recurso compartido en solo lectura o lectura/escritura.

Para la API de objetos HTTP, configure el acceso en Lectura y escritura.

Temas relacionados

- [“Propiedades y logs de HTTP” \[356\]](#)
- [“Autenticación y control de acceso de HTTP” \[359\]](#)
- [“Configuración de la API de objeto” \[360\]](#)
- [Cómo trabajar con un servidor de Keystone \[361\]](#)

Propiedades y logs de HTTP

TABLA 62 Propiedades generales de HTTP

Etiqueta de BUI	Propiedad de la CLI	Descripción
N/D	status	Propiedad de solo lectura que muestra el estado del servicio HTTP.
Protocolos	protocols	Seleccione los métodos de acceso que se admiten: HTTP, HTTPS o ambos.
Puerto HTTP (para conexiones entrantes)	listen_port	Puerto HTTP. El valor por defecto es 80.
Puerto HTTPS (para conexiones entrantes seguras)	https_port	Puerto HTTP seguro. El valor por defecto es 443.

TABLA 63 Propiedades de seguridad de HTTP

Etiqueta de BUI	Propiedad de la CLI	Descripción
Versiones de SSL/TLS	tls_version	Versiones del protocolo SSL/TLS para conexiones HTTP. Las versiones de TLS por defecto son TLSv1.1, TLSv1.2 y

Etiqueta de BUI	Propiedad de la CLI	Descripción
		los cifrados asociados. TLSv1.0 no está activado por defecto por cuestiones de seguridad, pero se puede activar para una compatibilidad con versiones anteriores. La lista de cifrados disponibles cambia en función de las versiones seleccionadas. Algunos cifrados o versiones del protocolo SSL/TLS seleccionados se eliminan después de una actualización de software si ya no se admiten. Para evitar la falta de disponibilidad del servicio, conserve la configuración por defecto, a menos que necesite cambiarla o que el soporte de Oracle le indique lo contrario.
Lista de cifrados	cifrados	Lista de cifrados para conexiones HTTP. La lista de cifrados disponibles cambia en función de las versiones seleccionadas. Algunos cifrados SSL/TLS seleccionados se eliminan después de una actualización de software si ya no se admiten. Para evitar la falta de disponibilidad del servicio, conserve la configuración por defecto, a menos que necesite cambiarla o que el soporte de Oracle le indique lo contrario.

TABLA 64 Propiedades de WebDAV de HTTP

Etiqueta de BUI	Propiedad de la CLI	Descripción
Activar WebDAV	webdav_enabled	Cuando se selecciona, permite activar la función WebDAV de HTTP.
Requerir inicio de sesión de cliente	require_login	Los clientes deben autenticarse antes de que se permita el acceso a los recursos compartidos y sean propietarios de los archivos que creen. Si no se configura esta propiedad, el propietario de los archivos creados será el servicio HTTP, con usuario nobody. Consulte “Autenticación y control de acceso de HTTP” [359] .

TABLA 65 Propiedades de servicio de la API de objetos Swift de HTTP

Etiqueta de BUI	Propiedad de la CLI	Descripción
Enable Swift (Activar Swift)	swift_enabled	Cuando se selecciona, se activa el servicio de la API de objetos Swift de HTTP.
Ruta por defecto	swift_default_path	Permite establecer la ubicación usada cuando el usuario no la configura.
Usar servicio de identidad de OpenStack	swift_ids_on	Cuando se selecciona, se habilitan las propiedades requeridas para la comunicación

Etiqueta de BUI	Propiedad de la CLI	Descripción
		con un servidor de Keystone: URI de autenticación, Rol, Cliente, Usuario, Contraseña.
URI de autenticación	swift_ids_auth_server	URI de servicio de identidad, por ejemplo: <code>http://keystone:5000/V2.0</code> .
Rol	swift_ids_role	Tipo de servicio de identidad de OpenStack.
Cliente	swift_ids_tenant	Nombre del cliente del servicio de identidad de OpenStack.
Usuario	swift_ids_user	Nombre del usuario del servicio de identidad de OpenStack.
Contraseña	swift_ids_password	Contraseña del usuario del servicio de identidad de OpenStack.

Nota - El servicio de la API de objetos no admite el cambio de propietario del recurso compartido. Si se cambia el propietario del recurso compartido, no se cambiará el propietario de la cuenta en el repositorio de objetos y pueden producirse fallos en las solicitudes de autenticación subsiguientes.

TABLA 66 Propiedades de servicio de la API de objetos Amazon S3 de HTTP

Etiqueta de BUI	Propiedad de la CLI	Descripción
Enable S3 (Activar S3)	s3_enabled	Cuando se selecciona, se activa el servicio de la API de objetos Amazon S3 de HTTP.
Ruta por defecto	s3_default_path	Permite establecer la ubicación usada cuando el usuario no la configura.
Frase de contraseña maestra	master_passphrase	Establece la contraseña maestra para el servicio de la API de objetos Amazon S3.
Confirmar frase de contraseña maestra		Confirma la frase de contraseña maestra.

Nota - El servicio de la API de objetos no admite el cambio de propietario del recurso compartido. Si se cambia el propietario del recurso compartido, no se cambiará el propietario de la cuenta en el repositorio de objetos y pueden producirse fallos en las solicitudes de autenticación subsiguientes.

TABLA 67 Propiedades del servicio de API de HTTP Oracle Cloud Infrastructure Object Storage

Etiqueta de BUI	Propiedad de la CLI	Descripción
Activar OCI	oci_enabled	Cuando se selecciona, permite activar el servicio de API de HTTP Oracle Cloud Infrastructure Object Storage.

Etiqueta de BUI	Propiedad de la CLI	Descripción
Ruta por defecto	<code>oci_default_path</code>	Permite establecer la ubicación usada cuando el usuario no la configura.
Clave	nodo <code>keys</code>	En la BUI, configure un nombre de usuario válido en el dispositivo. También puede introducir un comentario y la clave pública RSA en formato PEM para el servicio de API de Oracle Cloud Infrastructure Object Storage. En la CLI, configure un nombre de <code>user</code> válido en el dispositivo. También puede introducir un valor para <code>comment</code> y usar el comando <code>setkey</code> para introducir de forma interactiva la clave pública RSA en formato PEM para el servicio de API de Oracle Cloud Infrastructure Object Storage.

Nota - El servicio de la API de objetos no admite el cambio de propietario del recurso compartido. Si se cambia el propietario del recurso compartido, no se cambiará el propietario de la cuenta en el repositorio de objetos y pueden producirse fallos en las solicitudes de autenticación subsiguientes.

Logs de HTTP

El log del servicio HTTP se almacena en `network-http:apache24`.

Temas relacionados

- [Agregación de acceso HTTP a un recurso compartido \(BUI\) \[356\]](#)
- [“Autenticación y control de acceso de HTTP” \[359\]](#)
- [“Configuración de la API de objeto” \[360\]](#)
- [Cómo trabajar con un servidor de Keystone \[361\]](#)

Autenticación y control de acceso de HTTP

Si la opción "Require client login" (Requerir inicio de sesión de cliente) está activada, el dispositivo denegará el acceso a los clientes que no proporcionen credenciales de autenticación válidas correspondientes a un usuario local, un usuario de NIS o un usuario de LDAP. No se admite la autenticación de Active Directory.

Solo se admite la autenticación HTTP básica. Tenga en cuenta que, a menos que se esté usando HTTPS, durante esta operación se transmiten el nombre de usuario y la contraseña sin cifrar, lo que posiblemente no sea apropiado para todos los entornos.

Normalmente, los usuarios autenticados tienen los mismos permisos con HTTP que tendrían con NFS o FTP. Los archivos y los directorios creados por un usuario autenticado serán propiedad de ese usuario a la vista de los demás protocolos. Los usuarios con privilegios (los que tienen un UID menor que 100) serán tratados como *nobody* para el control de acceso. El propietario de los archivos creados por los usuarios con privilegios será *nobody*.

Si la opción "Require client login" (Requerir inicio de sesión de cliente) está desactivada, el dispositivo no intentará autenticar los clientes (aunque los clientes proporcionen credenciales). El propietario de los archivos de creación reciente es *nobody*, y todos los usuarios se consideran como *nobody* para el control de acceso.

Independientemente de la autenticación, no hay ningún permiso enmascarado en los archivos y los directorios creados. Los archivos creados tienen permisos 666 de Unix (lectura y escritura para todos), mientras que los directorios creados tienen permisos 777 de Unix (lectura, escritura y ejecución para todos).

Temas relacionados

- [Agregación de acceso HTTP a un recurso compartido \(BUI\) \[356\]](#)
- [“Propiedades y logs de HTTP” \[356\]](#)
- [“Configuración de la API de objeto” \[360\]](#)
- [Cómo trabajar con un servidor de Keystone \[361\]](#)

Configuración de la API de objeto

El servicio de API de objeto permite que un dispositivo guarde datos como objetos de almacenamiento en el sistema de archivos Oracle ZFS mediante el protocolo HTTP y la API OpenStack Object Storage (Swift), la API Amazon S3 (Simple Storage Service) o la API Oracle Cloud Infrastructure Object Storage.

Después de activar y configurar el servicio de la API de objetos, vaya a `Shares > Filesystems` para activar la característica en sistemas de archivos individuales. Haga doble clic en un sistema de archivos para ver los detalles correspondientes y, a continuación, seleccione el separador `Protocols`. En la sección `HTTP` correspondiente a la opción `Modo de almacén de objetos`, seleccione `Lectura y escritura` para activar la característica para el sistema de archivos.

Activación del servicio de la API de objetos

Para activar el servicio de API de objeto, vaya a `Configuration > Services > HTTP` y seleccione `Swift`, `S3` u `OCI`. Luego, según corresponda, seleccione la casilla de control `Activar Swift`, `Activar S3` o `Activar OCI`, y complete las propiedades usando las descripciones que figuran en [“Propiedades y logs de HTTP” \[356\]](#). Para finalizar, haga clic en `APLICAR`.

Configuración de propiedades de la API de objetos

Después de haber activado el servicio de la API de objetos, puede configurarlo con las propiedades de la API de objetos, como se muestra en [“Propiedades y logs de HTTP” \[356\]](#).

Si se seleccionó la opción del servicio de identidad de OpenStack al aplicar los cambios para el servicio HTTP, se establece una conexión de prueba con el servidor especificado con la información de las propiedades proporcionadas. Si la conexión falla, se abre un cuadro de diálogo que le permite aplicar o cancelar todos los cambios hechos en el servicio HTTP.

Temas relacionados

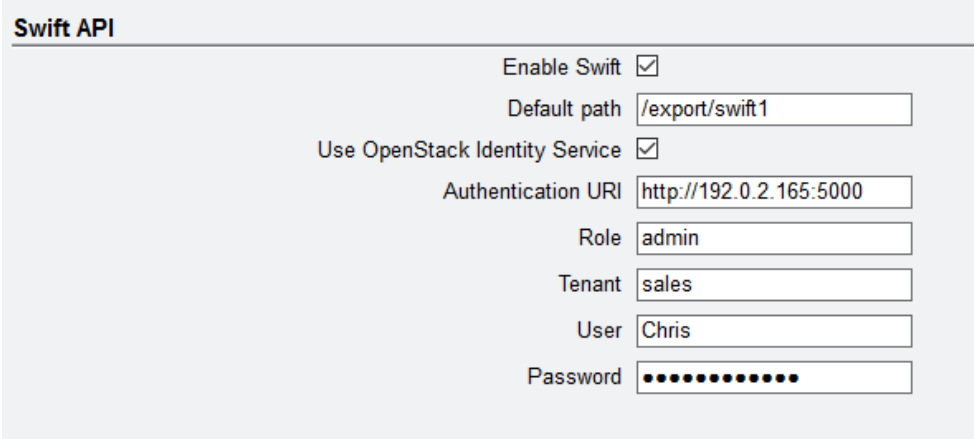
- [Agregación de acceso HTTP a un recurso compartido \(BUI\) \[356\]](#)
- [“Propiedades y logs de HTTP” \[356\]](#)
- [“Autenticación y control de acceso de HTTP” \[359\]](#)
- [Cómo trabajar con un servidor de Keystone \[361\]](#)

▼ Cómo trabajar con un servidor de Keystone

Antes de empezar Debería estar familiarizado con OpenStack y el servicio de Keystone. Para usar un servidor de Keystone para autenticación, el servidor debe estar instalado y activo. Además, se debe configurar un usuario con el rol de administrador para el servicio de la API de objetos Swift en el servidor de Keystone. El dispositivo incluye una cuenta preconfigurada denominada `swift`.

1. Si no usa el usuario `swift` preconfigurado, cree una cuenta de usuario para acceder a los datos del repositorio del almacén de objetos.
2. Use este nombre de usuario para crear proyectos que usen el repositorio.
3. Vaya a `Servicios > HTTP > Swift`.
 - a. Seleccione la casilla de control `Enable Swift` e introduzca una ruta por defecto.
 - b. Seleccione la casilla de control `Use OpenStack Identity Service`.

c. Especifique las credenciales de inicio de sesión para este usuario.



The screenshot shows a configuration window titled "Swift API". It contains several settings:

- Enable Swift**: A checkbox that is checked.
- Default path**: A text input field containing the value `/export/swift1`.
- Use OpenStack Identity Service**: A checkbox that is checked.
- Authentication URI**: A text input field containing the value `http://192.0.2.165:5000`.
- Role**: A text input field containing the value `admin`.
- Tenant**: A text input field containing the value `sales`.
- User**: A text input field containing the value `Chris`.
- Password**: A text input field filled with 12 dots, indicating a masked password.

Temas relacionados

- [Agregación de acceso HTTP a un recurso compartido \(BUI\) \[356\]](#)
- [“Propiedades y logs de HTTP” \[356\]](#)
- [“Autenticación y control de acceso de HTTP” \[359\]](#)
- [“Configuración de la API de objeto” \[360\]](#)

Configuración de HTTPS

El servicio HTTPS permite gestionar el dispositivo mediante el protocolo HTTPS. Este servicio permite que los clientes gestionen la conexión al servicio de la API de RESTful y la BUI del dispositivo.

Para una mayor seguridad al configurar HTTPS, puede especificar los cifrados y las versiones de SSL/TLS, como se describe en [“Propiedades y logs de HTTPS” \[363\]](#).

Propiedades y logs de HTTPS

TABLA 68 Propiedades de seguridad de HTTPS

Propiedad	Descripción
Cifrados y versiones de SSL/TLS	Cifrados y versiones del protocolo SSL/TLS para las conexiones HTTPS al servicio de la API de RESTful y la BUI del dispositivo. Los valores por defecto son TLSv1.1, TLSv1.2 y los cifrados asociados. TLSv1.0 no está activado por defecto por cuestiones de seguridad, pero se puede activar para una compatibilidad con versiones anteriores. La lista de cifrados disponibles cambia en función de las versiones seleccionadas. Algunos cifrados o versiones del protocolo SSL/TLS seleccionados se eliminan después de las actualizaciones de software si ya no se admiten. Para evitar la falta de disponibilidad del servicio, conserve la configuración por defecto, a menos que necesite cambiarla o que el soporte de Oracle le indique lo contrario.

TABLA 69 Logs de HTTPS

Log	Descripción
appliance-kit-http:default	Log del servicio HTTPS.

Configuración de asignación de identidades

La asignación de identidades permite asociar identidades de Windows y UNIX, lo que a su vez permite que un cliente SMB y un cliente NFS accedan al mismo juego de archivos. El servicio de asignación de identidades gestiona simultáneamente las identidades de los usuarios de Windows y UNIX mediante la creación y el mantenimiento de una base de datos de asignaciones entre identificadores de usuario (UID) e identificadores de grupos (GID) de UNIX por un lado e identificadores de seguridad (SID) de Windows por el otro.

Para gestionar la asignación de identidades, realice estas tareas:

- Configuración de asignación de identidades: [BUI](#), [CLI](#)
- Creación de reglas de asignación: [BUI](#), [CLI](#)
- [Visualización de una asignación \(BUI\) \[370\]](#)
- Vaciado de asignaciones de la caché: [BUI](#), [CLI](#)

Para comprender la asignación de identidades, consulte estos temas:

- [“Prácticas recomendadas de asignación de identidad” \[372\]](#)
- [“Conceptos de asignación de identidad” \[372\]](#)

- [“Asignaciones almacenadas en caché y asignaciones efímeras” \[373\]](#)
- [“Distinción entre mayúsculas y minúsculas en la asignación de identidades” \[374\]](#)
- [“Símbolos de dirección de reglas de asignación” \[375\]](#)

▼ Configuración de asignación de identidades (BUI)

Use el siguiente procedimiento para configurar la asignación de identidades.

Antes de empezar Asegúrese de estar unido al menos a un dominio de Active Directory. Para obtener más información sobre directorios activos, consulte [“Configuración de Active Directory” \[335\]](#).

1. **Vaya a Configuración > Servicios > Asignación de identidad > Propiedades.**
2. **Seleccione uno de los siguientes modos de asignación.**
 - **Basada en reglas**
 - **Basada en directorios:** configure todos los siguientes atributos.
 - **Atributo de AD - Nombre de usuario de UNIX:** nombre incluido en la base de datos de Active Directory para el nombre de usuario de UNIX equivalente
 - **Atributo de AD - Nombre de grupo de UNIX:** nombre incluido en la base de datos de Active Directory para el nombre de grupo de UNIX equivalente
 - **Atributo nativo de LDAP - Nombre de usuario de Windows:** nombre incluido en la base de datos de LDAP para la identidad de Windows equivalente
 - **IDMU**
3. **Para guardar la configuración, haga clic en Aplicar. Para borrar los valores de configuración, haga clic en Revertir.**

Temas relacionados

- Para obtener información acerca de los distintos modos de asignación, consulte [“Conceptos de asignación de identidad” \[372\]](#).
- Para crear una regla para permitir o denegar asignaciones, consulte [Creación de reglas de asignación \(BUI\) \[366\]](#).

▼ Configuración de asignación de identidades (CLI)

Use el siguiente procedimiento para configurar la asignación de identidades.

Antes de empezar Asegúrese de estar unido al menos a un dominio de Active Directory.

1. **Vaya a configuration services idmap.**

2. **Introduzca get para ver las propiedades de asignación de identidades.**

```
hostname:configuration services idmap> get
```

```
<status> = online
ad_unixuser_attr =
ad_unixgroup_attr =
nldap_winname_attr =
directory_based_mapping = none
```

The three *_attr properties correspond to the three fields on C>S>Identity Mapping>Properties.

3. **Establezca directory_based_mapping en uno de los siguientes modos de asignación.**

- **Para usar la asignación basada en reglas, configure directory_based_mapping con el valor none.**

```
hostname:configuration services idmap> set directory_based_mapping=none
hostname:configuration services idmap>
```

- **Para usar la asignación basada en directorios, configure directory_based_mapping con el valor name y asigne cada uno de los siguientes atributos.**

- **ad_unixuser_attr:** nombre incluido en la base de datos de Active Directory para el nombre de usuario de UNIX equivalente
- **ad_unixgroup_attr:** nombre incluido en la base de datos de Active Directory para el nombre de grupo de UNIX equivalente
- **nldap_winname_attr:** nombre incluido en la base de datos de LDAP para la identidad de Windows equivalente

```
hostname:configuration services idmap> set directory_based_mapping=name
hostname:configuration services idmap> set ad_unixuser_attr=demo_unixuser
hostname:configuration services idmap> set ad_unixgroup_attr=demo_group
hostname:configuration services idmap> set nldap_winname_attr=demo_winuser
```

- **Para usar Gestión de identidades para UNIX (IDMU), configure directory_based_mapping con el valor idmu.**

```
hostname:configuration services idmap> set directory_based_mapping=idmu
hostname:configuration services idmap>
```

Temas relacionados

- Para obtener información acerca de los distintos modos de asignación, consulte [“Conceptos de asignación de identidad” \[372\]](#).

- Para crear una regla para permitir o denegar asignaciones, consulte [Creación de reglas de asignación \(CLI\) \[367\]](#).

▼ Creación de reglas de asignación (BUI)

Use el siguiente procedimiento para otorgar o denegar credenciales para usuarios específicos mediante el servicio de asignación de identidades. Una regla de asignación de autorización otorga credenciales de identidad de Windows a partir de una identidad de UNIX o viceversa. Una regla de asignación de denegación bloquea una identidad de Windows para evitar que reciba las credenciales de una identidad de UNIX o viceversa.

Nota - Si crea una regla de asignación que bloquea a un usuario en particular y después el nombre de ese usuario se modifica, la asignación deja de bloquearlo.

Antes de empezar Configure la asignación basada en reglas como se describe en [Configuración de asignación de identidades \(BUI\) \[364\]](#).

1. **Vaya a Configuración > Servicios > Asignación de identidad > Reglas.**
2. **Haga clic en el ícono de agregación de elemento  que se encuentra junto a Rules (Reglas).**
3. **En el cuadro de diálogo Agregar regla de asignación, seleccione **Allow (Permitir)** o **Deny (Denegar)** como tipo de asignación.**
4. **Rellene los campos restantes en función del tipo de asignación seleccionado.**
 - **Asignación de autorización:**
 - **Dirección de asignación:** seleccione una dirección.
 - **Dominio de Windows:** escriba el dominio de Active Directory de la identidad de Windows o seleccione Todos.
 - **Identidad de Windows:** escriba el nombre de la identidad de Windows.
 - **Identidad de Unix:** escriba el nombre de la identidad de UNIX.
 - **Tipo de identidad de Unix:** seleccione **user** (Usuario) o **group** (Grupo).
 - **Asignación de denegación:**
 - a. **Para Dirección de asignación, seleccione una de dos opciones.**

- **Bloquear asignación de identidad de Windows:** impide que una identidad de Windows obtenga las credenciales de una identidad de UNIX
- **Bloquear asignación de identidad de Unix:** impide que una identidad de UNIX obtenga las credenciales de una identidad de Windows

b. **Introduzca la información de identidad de Windows o UNIX.**

- Si seleccionó `Block Windows identity mapping` (**Bloquear asignación de identidad de Windows**), escriba el dominio de Windows y la identidad que desea bloquear.
- Si seleccionó `Block UNIX identity mapping` (**Bloquear asignación de identidad de UNIX**), escriba la identidad y el tipo de identidad de UNIX que desea bloquear.

5. **Haga clic en Agregar.**

La nueva asignación aparece en la lista Reglas.

Temas relacionados

- [“Símbolos de dirección de reglas de asignación” \[375\]](#)

▼ Creación de reglas de asignación (CLI)

Use el siguiente procedimiento para otorgar o denegar credenciales para usuarios específicos mediante el servicio de asignación de identidades. Una regla de asignación de autorización otorga credenciales de identidad de Windows a partir de una identidad de UNIX o viceversa. Una regla de asignación de denegación bloquea una identidad de Windows para evitar que reciba las credenciales de una identidad de UNIX o viceversa.

Nota - Si crea una regla de asignación que bloquea a un usuario en particular y después el nombre de ese usuario se modifica, la asignación deja de bloquearlo.

Antes de empezar Configure la asignación basada en reglas como se describe en [Configuración de asignación de identidades \(CLI\) \[364\]](#).

1. **Vaya a** `configuration services idmap`.

2. **Introduzca** `create`.

```
hostname:configuration services idmap> create
```

```
hostname:configuration services idmap (uncommitted)>
```

3. Configure las propiedades según corresponda.

Puede utilizar el comando `list` para ver una lista de las propiedades disponibles.

```
hostname:configuration services idmap (uncommitted)> list
Properties:
    windomain = (unset)
    winname = (unset)
    direction = (unset)
    unixname = (unset)
    unixtype = (unset)
```

- a. **windomain:** dominio de Active Directory de la identidad de Windows.
- b. **winname:** configure esta propiedad con una de las siguientes opciones.
 - **Para crear una asignación de autorización, configure `winname` con el nombre de la identidad de Windows.**
Introduzca `*` para indicar todos los usuarios del dominio especificado.
 - **Para crear una asignación de denegación que impida que una identidad de UNIX reciba las credenciales de una identidad de Windows, configure el nombre de la identidad de Windows.**
 - **Para crear una asignación de denegación que impida que una identidad de Windows reciba las credenciales de una identidad de UNIX, no configure `winname`.**
- c. **direction:** configure esta propiedad con la dirección de la asignación.
 - **win2unix:** asignación de Windows a UNIX
 - **unix2win:** asignación de UNIX a Windows
 - **bi:** asignación bidireccional
- d. **unixname:** configure esta propiedad con una de las siguientes opciones.
 - **Para crear una asignación de autorización, configure el nombre de la identidad de UNIX o introduzca `*` para indicar todos los usuarios del tipo especificado.**
 - **Para crear una asignación de denegación que impida que una identidad de Windows reciba las credenciales de una identidad de UNIX, configure el nombre de la identidad de UNIX.**

- Para crear una asignación de denegación que impida que una identidad de UNIX reciba las credenciales de una identidad de Windows, no configure `unixname`.

- e. `unixtype`: configure esta propiedad con el valor `user` o `group` para definir el tipo de identidad de UNIX.

```
hostname:configuration services idmap (uncommitted)> set windomain=demo.domain.com
hostname:configuration services idmap (uncommitted)> set winname=*
hostname:configuration services idmap (uncommitted)> set direction=win2unix
hostname:configuration services idmap (uncommitted)> set unixname=
hostname:configuration services idmap (uncommitted)> set unixtype=user
```

4. Introduzca `commit` para confirmar los cambios y crear la regla de asignación.

```
hostname:configuration services idmap (uncommitted)> commit
hostname:configuration services idmap>
```

Puede usar el comando `list` para ver la nueva regla en la lista Reglas.

```
hostname:configuration services idmap> list
```

MAPPING	WINDOWS ENTITY	DIRECTION	UNIX ENTITY
idmap-000	Alice@demo.domain.com	(U) ==	wdp (U)
idmap-001	*@demo.domain.com	(U) => ""	(U)

ejemplo 2 Creación de asignaciones bidireccionales (CLI)

En este ejemplo, se crea una asignación bidireccional basada en nombres entre un usuario de Windows y un usuario de UNIX.

```
hostname:> configuration services idmap
hostname:configuration services idmap> create
hostname:configuration services idmap (uncommitted)> set
    windomain=eng.fishworks.com
hostname:configuration services idmap (uncommitted)> set winname=Bill
hostname:configuration services idmap (uncommitted)> set direction=bi
hostname:configuration services idmap (uncommitted)> set unixname=wdp
hostname:configuration services idmap (uncommitted)> set unixtype=user
hostname:configuration services idmap (uncommitted)> commit
hostname:configuration services idmap> list
```

MAPPING	WINDOWS ENTITY	DIRECTION	UNIX ENTITY
idmap-000	Bill@eng.fishworks.com	(U) ==	wdp (U)

ejemplo 3 Creación de asignaciones de denegación (CLI)

En este ejemplo, se crea una asignación de denegación para impedir que todos los usuarios de Windows de un dominio obtengan credenciales.

```
hostname:configuration services idmap> create
hostname:configuration services idmap (uncommitted)> list
Properties:
    windomain = (unset)
```

```
winname = (unset)
direction = (unset)
unixname = (unset)
unixtype = (unset)

hostname:configuration services idmap (uncommitted)> set
  windomain=guest.fishworks.com
hostname:configuration services idmap (uncommitted)> set winname=*
hostname:configuration services idmap (uncommitted)> set direction=win2unix
hostname:configuration services idmap (uncommitted)> set unixname=
hostname:configuration services idmap (uncommitted)> set unixtype=user
hostname:configuration services idmap (uncommitted)> commit
hostname:configuration services idmap> list
MAPPING      WINDOWS ENTITY      DIRECTION      UNIX ENTITY
idmap-000    Bill@eng.fishworks.com      (U) ==          wdp (U)
idmap-001    *@guest.fishworks.com      (U) =>          "" (U)
```

▼ Visualización de una asignación (BUI)

Use el siguiente procedimiento para ver una asignación existente.

1. **Vaya a Configuración > Servicios > Asignación de identidad > Mostrar asignaciones.**
2. **Seleccione `Windows` o `UNIX` como plataforma desde la que se asigna la identidad.**
3. **Introduzca la información de identidad de Windows o UNIX.**
 - Si seleccionó `Windows`, escriba el dominio de Windows y el nombre de usuario.
 - Si seleccionó `UNIX`, seleccione `User` (Usuario) o `Group` (Grupo) como tipo y escriba el nombre de la entidad.
4. **Haga clic en Mostrar asignación.**

Se muestran las propiedades de identidad del usuario o del grupo. También se muestran el origen de la asignación y el origen de backend:

Origen

- **Nueva asignación:** la asignación se creó de cero, es decir, no se recuperó de la memoria caché ni estaba predefinida.
- **Asignación de caché:** la asignación se recuperó de la memoria caché, que almacena asignaciones durante 10 minutos después de que se las solicita.
- **Asignación de codificación fija:** la asignación está predefinida y es fija en el dispositivo. Estas asignaciones se crearon para las identidades predeterminadas de UNIX y Windows.
- **Asignación algorítmica:** no se pudo asignar un UID o un GID no efímero de UNIX por nombre, por lo que se lo asignó a un SID generado algorítmicamente.

Backend

- **Directorio de AD:** asignación basada en directorios que se creó usando anotaciones en Active Directory.
- **Directorio nativo de LDAP:** asignación basada en directorios que se creó usando anotaciones en el directorio LDAP.
- **IDMU:** la asignación se creó usando la función Gestión de identidades para UNIX de Windows.
- **Regla de nombre:** la asignación se creó usando una regla de nombre.
- **Efímera:** como no había una identidad equivalente en el momento de crear la asignación, el sistema creó una temporal con un UID o un GID efímero.
- **Local SID:** no se pudo asignar un UID o un GID no efímero de UNIX por nombre, por lo que se lo asignó a un SID local generado algorítmicamente.
- **Asignación conocida:** la asignación usa un SID conocido. Estos SID de Windows identifican usuarios genéricos o grupos genéricos. Los valores son constantes en todos los sistemas operativos.

▼ Vaciado de asignaciones de la caché (BUI)

Use el siguiente procedimiento para vaciar o hacer caducar todas las asignaciones de la caché.

Después de proporcionada una asignación solicitada, se almacena en la caché durante 10 minutos y luego expira. Puede hacer caducar inmediatamente una asignación mediante la función de vaciado, que hace caducar todas las asignaciones almacenadas en caché.

1. **Vaya a Configuración > Servicios > Asignación de identidad > Mostrar asignaciones.**
2. **Haga clic en Vaciar caché de asignación.**
Se expiran todas las asignaciones almacenadas en la caché.

▼ Vaciado de asignaciones de la caché (CLI)

Use el siguiente procedimiento para vaciar o hacer caducar todas las asignaciones de la caché.

Después de proporcionada una asignación solicitada, se almacena en la caché durante 10 minutos y luego expira. Puede hacer caducar inmediatamente una asignación mediante la función de vaciado, que hace caducar todas las asignaciones almacenadas en caché.

1. **Vaya a `configuration services idmap`.**

2. Introduzca `flush`.

```
hostname:configuration services idmap> flush
hostname:configuration services idmap>
```

Se expiran todas las asignaciones almacenadas en la caché.

Prácticas recomendadas de asignación de identidad

- Configure reglas de asignación de identidad específicas de usuario si desea que un usuario tenga acceso a juegos de archivos comunes por medio de clientes NFS y SMB. Si los clientes NFS y SMB obtienen acceso a sistemas de archivos separados, no hay necesidad de configurar ninguna regla de asignación de identidad.
- La reconfiguración del servicio de asignación de identidad no afecta las sesiones activas de SMB. Los usuarios conectados siguen conectados y las asignaciones de nombres previas quedan disponibles para autorizar el acceso a recursos compartidos adicionales durante 10 minutos como máximo. Para evitar el acceso no autorizado, configure las asignaciones antes de exportar los recursos compartidos.
- La seguridad que proporcionan las asignaciones de identidades es solamente tan eficaz como la sincronización que tienen con los servicios de directorio. Por ejemplo, si crea una asignación basada en nombres que deniega el acceso a un usuario en particular y el nombre de usuario cambia, la asignación ya no deniega el acceso a ese usuario.
- Puede haber solo una asignación bidireccional para cada dominio de Windows que asigne todos los usuarios del dominio de Windows a todas las identidades de UNIX. Si desea crear varias reglas para todo el dominio, asegúrese de especificar que esas reglas asignen *solo* de Windows a UNIX.
- Cuando sea posible, use el modo de asignación IDMU en lugar del modo de asignación basada en directorios.

Conceptos de asignación de identidad

El servicio SMB usa el servicio de asignación de identidad para asociar identidades de Windows y UNIX. Cuando el servicio SMB autentica a un usuario, utiliza el servicio de asignación de identidad para asignar la identidad de Windows del usuario a la identidad apropiada de UNIX. Si no existe una identidad de UNIX para un usuario de Windows, el servicio genera una identidad temporal con un UID y un GID efímeros. Estas asignaciones permiten exportar recursos compartidos y tener acceso a ellos de manera concurrente mediante clientes SMB y NFS. Mediante la asociación de las identidades de Windows y UNIX, los clientes NFS y SMB pueden compartir la misma identidad y así tener acceso al mismo juego de archivos.

En el sistema operativo Windows, un token de acceso contiene la información de seguridad para el inicio de sesión e identifica al usuario, los grupos del usuario y los privilegios del usuario. Los administradores definen usuarios y grupos de Windows en un grupo de trabajo o en una base de datos de SAM, que se gestiona en un controlador de dominio de Active Directory. Cada usuario y cada grupo tiene un SID que lo identifica de manera exclusiva, tanto en el host como en el dominio local, así como en todos los dominios posibles de Windows.

UNIX crea credenciales de usuario basadas en la autenticación de usuario y los permisos de archivos. Los administradores definen usuarios y grupos de UNIX en archivos de grupos y contraseñas locales o en un servicio de nombres o directorio, como, por ejemplo, NIS o LDAP. Cada usuario y cada grupo de UNIX tiene un UID y un GID. Normalmente, el UID o el GID identifican de manera exclusiva el usuario o el grupo en un único dominio de UNIX. Sin embargo, estos valores no son exclusivos en diferentes dominios.

Las siguientes opciones están disponibles al seleccionar un modo de asignación:

- **Asignación basada en reglas:** se usa para crear diversas reglas que asignan identidades por nombre, lo que establece equivalencias entre identidades de Windows y UNIX. Las reglas de asignación son útiles si se desea que un usuario tenga acceso al mismo juego de archivos por medio de clientes SMB y NFS.
- **Asignación basada en directorios:** se usa para agregar anotaciones a un objeto de LDAP o Active Directory con información acerca de la manera en la que la identidad del objeto se asigna a una identidad equivalente en la plataforma opuesta.
- **Asignación basada en IDMU:** Gestión de identidades para UNIX (IDMU) es una función que Microsoft ofrece para Windows Server 2003, que viene incluida con Windows Server 2003 R2 y posteriores. IDMU admite Windows como servidor de NIS/NFS mediante la agregación de un panel "Atributos de UNIX" a la interfaz de usuario Usuarios y computadoras de Active Directory. Esto permite a los administradores especificar un número de parámetros relacionados con UNIX, incluidos UID, GID, shell de inicio de sesión y directorio de inicio. Estos parámetros están disponibles mediante Active Directory con un esquema similar (pero no igual) al de RFC 2307 y mediante el servicio NIS. Cuando se selecciona el modo de asignación IDMU, el servicio de asignación de identidad consume estos atributos de UNIX para establecer asignaciones entre identidades de Windows y UNIX. Este enfoque es muy similar al de la asignación basada en directorios, con la diferencia de que el servicio de asignación de identidad consulta el esquema de propiedades establecido por el software IDMU en lugar de permitir un esquema personalizado. Cuando se utiliza este enfoque, no se puede utilizar ningún otro método de asignación basada en directorios.

Asignaciones almacenadas en caché y asignaciones efímeras

Cuando el servicio de asignación de identidad proporciona una asignación de nombre, la almacena en caché durante 10 minutos. Una vez transcurrido ese lapso, la asignación caduca.

En ese lapso de 10 minutos, la asignación persiste aunque el servicio de asignación de identidad se reinicie. Los cambios realizados en las asignaciones o los directorios del servicio de nombres no afectan las conexiones existentes durante el período de 10 minutos de vida de la asignación. El servicio evalúa las asignaciones solamente cuando el cliente intenta conectarse a un recurso compartido y no hay una asignación vigente. Por ejemplo, si el servidor SMB solicita una asignación para el usuario después de que la primera asignación caduca, el servicio la vuelve a evaluar.

Si no hay ninguna regla de asignación basada en nombres que pueda aplicarse a un usuario en particular, ese usuario recibe credenciales temporales mediante una asignación efímera, a menos que esté bloqueado por otra asignación. Cuando un usuario de Windows que tiene un nombre de UNIX efímero crea un archivo en el sistema, los clientes de Windows que acceden al archivo mediante SMB ven que el propietario de ese archivo es la identidad de Windows. Sin embargo, los clientes NFS ven que el archivo es propiedad de “nobody” (nadie).

Distinción entre mayúsculas y minúsculas en la asignación de identidades

Los nombres de Windows no distinguen entre mayúsculas y minúsculas, pero los de UNIX sí. Los nombres de usuario JSMITH, JSmith y jsmith son equivalentes en Windows, pero son tres nombres diferentes en UNIX. La distinción entre mayúsculas y minúsculas afecta las asignaciones de nombres de manera diferente en función de la dirección de la asignación.

- Para que una asignación de Windows a UNIX genere una coincidencia, el uso de mayúsculas y minúsculas del nombre de usuario de Windows debe coincidir con el uso de mayúsculas y minúsculas del nombre de usuario de UNIX. Por ejemplo, solo el nombre de usuario "jsmith" de Windows coincide con el nombre de usuario "jsmith" de UNIX. El nombre de usuario Jsmith de Windows no coincide.
- Cuando la asignación usa el carácter comodín "*" para asignar varios nombres de usuario, se produce una excepción del requisito de coincidencia de uso de mayúsculas y minúsculas para las asignaciones de Windows a UNIX.

Si el servicio de asignación de identidad encuentra una asignación que asigna el usuario de Windows *@some.domain al usuario de UNIX "*", primero busca un nombre de UNIX que coincida exactamente con el nombre de Windows. Si no encuentra ninguno, el servicio convierte todo el nombre de Windows a minúsculas y vuelve a buscar un nombre de UNIX que coincida. Por ejemplo, el nombre de usuario "JSmith@some.domain" de Windows se asigna al nombre de usuario "jsmith" de UNIX. Si el servicio no encuentra una coincidencia después de usar minúsculas para el nombre de usuario de Windows, el usuario no obtiene una asignación.

Puede crear una regla para establecer coincidencias entre cadenas que difieren solo en el uso de mayúsculas y minúsculas. Por ejemplo, puede crear una asignación específica de usuario que asigne el usuario "JSmith@some.domain" de Windows al usuario "jSmith" de

UNIX. En todos los demás casos, el servicio asigna un identificador efímero al usuario de Windows.

- Para que se obtenga una coincidencia en una asignación de UNIX a Windows, no es necesario que coincida el uso de mayúsculas y minúsculas. Por ejemplo, el nombre de usuario "jsmith" de UNIX coincide con cualquier nombre de usuario de Windows que tenga las letras "JSMITH", sin importar si son mayúsculas o minúsculas.

Símbolos de dirección de reglas de asignación

Después de crear una asignación basada en nombres, los siguientes símbolos indican la semántica de cada regla.

- : asigna identidades de Windows a identidades de UNIX, e identidades de UNIX a identidades de Windows
- : asigna identidades de Windows a identidades de UNIX
- : asigna identidades de UNIX a identidades de Windows
- : impide que las identidades de Windows obtengan credenciales
- : impide que las identidades de UNIX obtengan credenciales

Si el ícono es gris en lugar de negro, la regla corresponde a una identidad de UNIX que no se puede resolver.

Configuración de IPMP

IPMP (rutas múltiples de red de protocolo de Internet) permite agrupar varias interfaces de red como si fueran una sola, lo que mejora el ancho de banda y la fiabilidad (redundancia de interfaz) de la red. En esta sección, se pueden configurar algunas propiedades. Para la configuración de las interfaces de red en los grupos IPMP, consulte [“Configuración de red” \[96\]](#).

TABLA 70 Propiedades de IPMP

Propiedad	Descripción
Failure detection latency (Latencia de detección de fallos)	Tiempo que necesita IPMP para declarar que una interfaz de red ha fallado y conmutar por error sus direcciones IP.
Activar failback	Permite al servicio reanudar las conexiones con una interfaz reparada.

Los cambios realizados en las propiedades de los servicios se documentan en las secciones [Configuración de las propiedades de los servicios \(BUI\) \[328\]](#) y [Configuración de las](#)

[propiedades de los servicios \(CLI\)](#) [329]. Los nombres de propiedades de la CLI son versiones más abreviadas que las mencionadas anteriormente.

TABLA 71 Logs de IPMP

Log	Descripción
network-initial:default	Registra el proceso de configuración de red.

Configuración de iSCSI

Al configurar un LUN en el dispositivo, puede exportar ese volumen por medio de un destino de interfaz estándar de equipos pequeños de Internet (iSCSI). El servicio iSCSI permite a los iniciadores iSCSI utilizar el protocolo iSCSI para tener acceso a los destinos deseados.

El servicio admite tareas de detección, gestión y configuración con el protocolo iSNS. El servicio iSCSI admite autenticación unidireccional (el destino autentica al iniciador) y bidireccional (el destino y el iniciador se autentican mutuamente) con CHAP. Asimismo, el servicio admite la gestión de datos de autenticación de CHAP en una base de datos RADIUS.

El sistema realiza primero la autenticación y después la autorización, en dos pasos independientes.

Nota - Para ver ejemplos de configuración de destinos e iniciadores iSCSI, consulte [“Configuración de una red de área de almacenamiento \(SAN\)”](#) [224].

TABLA 72 Propiedades del servicio iSCSI

Propiedad	Descripción
Use iSNS (Usar iSNS)	Indica si la detección iSNS está activada
iSNS Server (Servidor iSNS)	Servidor iSNS
Use RADIUS (Usar RADIUS)	Indica si RADIUS está activado
RADIUS Server (Servidor RADIUS)	Un servidor RADIUS
RADIUS Server Secret (Secreto de servidor RADIUS)	El secreto del servidor RADIUS

Si el iniciador local tiene un nombre CHAP y un secreto CHAP, el sistema realiza la autenticación. Si el iniciador local no tiene propiedades CHAP, el sistema no realiza ninguna autenticación y, por lo tanto, todos los iniciadores son elegibles para autorización.

El servicio iSCSI le permite especificar una lista global de iniciadores que se pueden utilizar en grupos de iniciadores.

Si el iniciador no se puede conectar con el destino:

- Asegúrese de que el IQN del iniciador coincida con el IQN identificado en la lista de iniciadores.
- Compruebe que la dirección IP del servidor iSNS sea correcta y que el servidor iSNS esté configurado.
- Compruebe que la dirección IP del destino sea correcta del lado del iniciador.
- Compruebe que los nombres y los secretos CHAP del iniciador coincidan de ambos lados.
- Asegúrese de que el nombre y el secreto CHAP del destino no sean iguales a los de ninguno de los iniciadores.
- Compruebe que la dirección IP y el secreto del servidor RADIUS sean correctos, y que el servidor RADIUS esté configurado.
- Compruebe que el iniciador que está accediendo al LUN pertenezca al grupo de iniciadores de ese LUN.
- Compruebe que los destinos que exportan ese LUN estén en línea.
- Compruebe que el estado operativo del LUN sea en línea.
- Compruebe el número de unidad lógica de cada LUN.

Si, durante los failover failback, no sobreviven las E/S de copia reducida de iSER provenientes del cliente Red Hat, modifique el parámetro `node.session.timeo.replacement_timeout` en el archivo `/etc/iscsi/iscsid.conf` a 300sec.

Temas relacionados

- Configuración de las propiedades de servicio [BUI](#), [CLI](#)

Configuración de Kerberos

Kerberos es un protocolo de red que usa cifrado de clave secreta para autenticar la comunicación entre un cliente y una máquina host o un servicio. Usa un servidor del Centro de distribución de claves (KDC) para emitir tickets con registro de hora. Puede usar el dispositivo para importar los principales de Kerberos y las claves creadas en el KDC o puede usar el dispositivo para configurar los principales para el KDC, y las claves se crean automáticamente. Si bien puede usar ambos métodos, la importación es la práctica recomendada y es de uso más común. Todas las claves se cifran usando la contraseña de Kerberos y se las almacena en el archivo de tabla de claves del dispositivo.

Tanto Kerberos como Active Directory pueden estar activados al mismo tiempo porque tienen reinos y claves diferentes. Cuando ambos están activos, el reino Kerberos es el que se usa por defecto.

El dispositivo puede usar Kerberos para autenticar usuarios para el inicio de sesión administrativo y para el acceso a servicios, incluidos NFS, HTTP, FTP, SFTP y SSH. Los usuarios del dispositivo deben tener un principal de Kerberos con el mismo nombre para poder usar la autenticación de Kerberos para estos servicios. Kerberos también se puede usar para configurar valores de seguridad para recursos compartidos individuales que usan el protocolo NFS, como se describe en “[Configuración de reinos Kerberos para NFS](#)” [425]. Dado que el servicio Kerberos usa registros de hora, configure primero el servicio NTP del dispositivo.

Para configurar Kerberos, consulte las siguientes secciones:

- Creación de un reino Kerberos: [BUI](#), [CLI](#)
- Importación de claves de Kerberos: [BUI](#), [CLI](#)
- Creación de principales y claves de Kerberos: [BUI](#), [CLI](#)
- Supresión de principales y claves de Kerberos: [BUI](#), [CLI](#)
- Destrucción de un reino Kerberos: [BUI](#), [CLI](#)
- “[Kerberos Service Properties](#)” [391]
- “[Propiedades y logs de Kerberos](#)” [392]
- “[Configuración de reinos Kerberos para NFS](#)” [425]

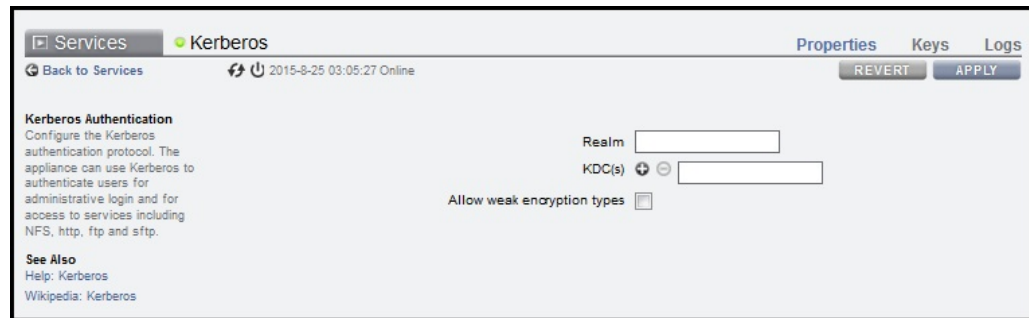
▼ Creación de un reino Kerberos (BUI)

Use el siguiente procedimiento para crear un reino Kerberos, configurar los KDC y seleccionar tipos de cifrado débiles o de alta seguridad. Las descripciones de cada propiedad están en “[Kerberos Service Properties](#)” [391].

Antes de empezar Asegúrese de haber configurado el servicio [servicio NTP](#).

1. **Vaya a Configuración > Servicios.**
2. **Para activar el servicio Kerberos, haga clic en el ícono de activación  para Kerberos.**
3. **Haga clic en Kerberos.**
4. **En el campo Realm (Reino Kerberos), escriba el reino Kerberos.**

Por cuestiones de simplicidad, el nombre de reino Kerberos puede ser el mismo que el nombre de dominio DNS, excepto que el nombre de reino Kerberos está en mayúscula.



5. **En el campo KDC(s) (KDC), escriba el nombre de host del servidor administrativo de KDC.**

Si la configuración de Kerberos incluye compatibilidad con DNS para consultas de KDC, deje este campo en blanco.

6. **Si tiene otro KDC, haga clic en el ícono de agregación  que está junto a KDC (s) (KDC) y escriba el nombre de host correspondiente. Repita esta acción para cada KDC adicional.**

Si la configuración incluye compatibilidad con DNS, no realice este paso.

7. **Para permitir el uso de tipos de cifrado débiles, como DES y Exportable ArcFour con HMAC/md5, seleccione Allow weak encryption types (Permitir tipos de cifrado débiles).**

De manera predeterminada, no se permite el uso de tipos de cifrado débiles.

8. **Haga clic en APPLY (Aplicar).**

Para restablecer los valores originales de las propiedades, haga clic en REVERT (Revertir).

Pasos siguientes

Elija una de las siguientes opciones:

- [Importación de claves de Kerberos \(BUI\) \[381\]](#)
- [Creación de principales y claves de Kerberos \(BUI\) \[384\]](#)

▼ Creación de un reino Kerberos (CLI)

Use el siguiente procedimiento para crear un reino Kerberos, configurar los KDC y seleccionar tipos de cifrado débiles o de alta seguridad. Las descripciones de cada propiedad están en [“Kerberos Service Properties” \[391\]](#) y [“Propiedades y logs de Kerberos” \[392\]](#).

Antes de empezar Asegúrese de haber configurado el servicio [servicio NTP](#).

1. **Vaya a `configuration services kerberos` e introduzca `show`.**

```
hostname:configuration services kerberos> show
Properties:
    <status> = disabled
    allow_weak_crypto = false
```

2. **Para activar el servicio Kerberos, introduzca `enable` y, a continuación, introduzca `commit`.**

3. **Para permitir el uso de tipos de cifrado débiles, como DES y Exportable ArcFour con HMAC/md5, introduzca `set allow_weak_crypto=true` y, a continuación, introduzca `commit`.**

De manera predeterminada, no se permite el uso de tipos de cifrado débiles.

4. **Para crear un reino Kerberos, introduzca `create` y el nombre del reino Kerberos y, a continuación, introduzca `commit`.**

Por cuestiones de simplicidad, el nombre de reino Kerberos puede ser el mismo que el nombre de dominio DNS, excepto que el nombre de reino Kerberos está en mayúscula.

```
hostname:configuration services kerberos> create TEST.NET
hostname:configuration services kerberos TEST.NET (uncommitted)> commit
```

5. **Escriba `done`.**

6. **Para ver todos los reinos Kerberos, introduzca `list`.**

```
hostname:configuration services kerberos> list
REALM          KDC
TEST.NET
```

7. **Seleccione el reino Kerberos.**

```
hostname:configuration services kerberos> select TEST.NET
hostname:configuration services kerberos TEST.NET>
```

8. **Para configurar los servidores KDC, introduzca `set kdc=` y el nombre de host del servidor administrativo de KDC. Si tiene KDC adicionales, agréguelos en la misma línea, separados por comas. A continuación, introduzca `commit`.**

Si la configuración de Kerberos incluye compatibilidad con DNS para consultas de KDC, no realice este paso.


```
hostname:configuration services kerberos TEST.NET> set kdc=kdc1.us.oracle.com,kdc2.us.oracle.com
kdc = kdc1.us.oracle.com,kdc2.us.oracle.com (uncommitted)
hostname:configuration services kerberos TEST.NET> commit
```

Pasos siguientes

Elija una de las siguientes opciones:

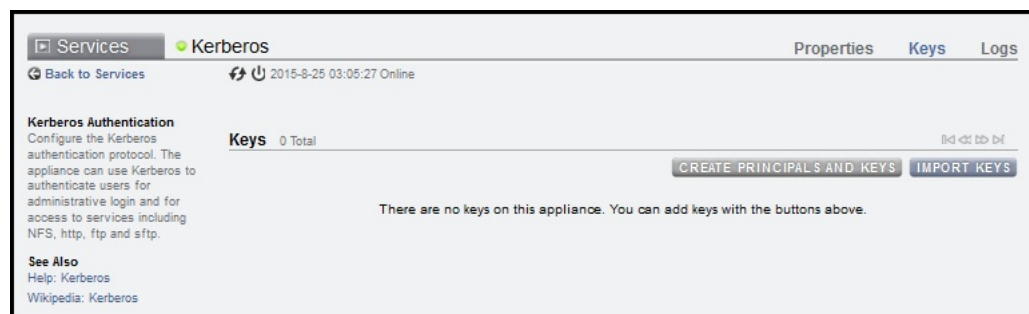
- [Importación de claves de Kerberos \(CLI\) \[382\]](#)
- [Creación de principales y claves de Kerberos \(CLI\) \[386\]](#)

▼ Importación de claves de Kerberos (BUI)

Use el siguiente procedimiento para importar claves de Kerberos creadas en KDC. Las claves se almacenan en la tabla de claves del dispositivo. Para esta tarea no se requieren credenciales de inicio de sesión para KDC. Las descripciones de cada propiedad están en [“Kerberos Service Properties” \[391\]](#).

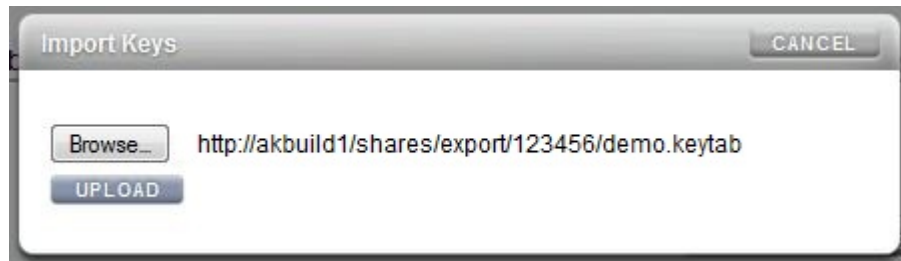
Antes de empezar Asegúrese de haber activado el servicio Kerberos, configurado el reino Kerberos e identificado los KDC como se describe en [Creación de un reino Kerberos \(BUI\) \[378\]](#).

1. **Vaya a Configuración > Servicios.**
2. **Haga clic en Kerberos.**
3. **Haga clic en Keys (Claves) y, luego, en IMPORT KEYS (Importar claves).**



4. **En el cuadro de diálogo Import Keys (Importar claves), haga clic en Browse (Examinar) y seleccione el archivo de tabla de claves de Kerberos.**

5. Haga clic en Cargar.



Se muestra la lista de claves.

Keys 16 Total				1-16	
				CREATE PRINCIPALS AND KEYS	IMPORT KEYS
KVNO	PRINCIPAL	ENCRYPTION TYPE	TYPE #		
2	nfs/ar7320-220.us.oracle.com@TEST.NET	ArcFour with HMAC/md5	23		
2	nfs/ar7320-220.us.oracle.com@TEST.NET	Triple DES cbc mode with HMAC/sha1	16		
2	nfs/ar7320-220.us.oracle.com@TEST.NET	AES-128 CTS mode with 96-bit SHA-1 HMAC	17		
2	nfs/ar7320-220.us.oracle.com@TEST.NET	AES-256 CTS mode with 96-bit SHA-1 HMAC	18		
2	host/ar7320-220.us.oracle.com@TEST.NET	ArcFour with HMAC/md5	23		
2	host/ar7320-220.us.oracle.com@TEST.NET	Triple DES cbc mode with HMAC/sha1	16		
2	host/ar7320-220.us.oracle.com@TEST.NET	AES-128 CTS mode with 96-bit SHA-1 HMAC	17		
2	host/ar7320-220.us.oracle.com@TEST.NET	AES-256 CTS mode with 96-bit SHA-1 HMAC	18		
2	nfs/ar7320-230.us.oracle.com@TEST.NET	ArcFour with HMAC/md5	23		
2	nfs/ar7320-230.us.oracle.com@TEST.NET	Triple DES cbc mode with HMAC/sha1	16		
2	nfs/ar7320-230.us.oracle.com@TEST.NET	AES-128 CTS mode with 96-bit SHA-1 HMAC	17		
2	nfs/ar7320-230.us.oracle.com@TEST.NET	AES-256 CTS mode with 96-bit SHA-1 HMAC	18		
2	host/ar7320-230.us.oracle.com@TEST.NET	ArcFour with HMAC/md5	23		
2	host/ar7320-230.us.oracle.com@TEST.NET	Triple DES cbc mode with HMAC/sha1	16		
2	host/ar7320-230.us.oracle.com@TEST.NET	AES-128 CTS mode with 96-bit SHA-1 HMAC	17		
2	host/ar7320-230.us.oracle.com@TEST.NET	AES-256 CTS mode with 96-bit SHA-1 HMAC	18		

▼ Importación de claves de Kerberos (CLI)

Use el siguiente procedimiento para importar claves de Kerberos creadas en KDC. Las claves se almacenan en la tabla de claves del dispositivo. Para esta tarea no se requieren credenciales

de inicio de sesión para KDC. Las descripciones de cada propiedad están en [“Kerberos Service Properties” \[391\]](#) y [“Propiedades y logs de Kerberos” \[392\]](#).

Antes de empezar Asegúrese de haber activado el servicio Kerberos, configurado el reino Kerberos e identificado los KDC como se describe en [Creación de un reino Kerberos \(CLI\) \[380\]](#).

1. **Vaya a `configuration services kerberos importkeytab` e introduzca `show` para ver las propiedades.**

```
hostname:configuration services kerberos importkeytab (uncommitted)> show
Properties:
    url = (unset)
    user = (unset)
    password = (unset)
```

2. **Introduzca `set url=` y la dirección URL del archivo de tabla de claves de Kerberos.**

```
hostname:configuration services kerberos importkeytab (uncommitted)> set url=http://akbuild1/
shares/export/123456/demo.keytab
url = http://akbuild1/shares/export/123456/demo.keytab
```

3. **Introduzca `set user=` y el nombre de usuario para el acceso URL.**

```
hostname:configuration services kerberos importkeytab (uncommitted)> set user=myusername
user = myusername
```

4. **Introduzca `set password=` y la contraseña para el acceso URL y, a continuación, introduzca `commit`.**

```
hostname:configuration services kerberos importkeytab (uncommitted)> set password=letmein
password = (set)
hostname:configuration services kerberos importkeytab (uncommitted)> commit
Transferred 718 of 718 (100%) . . . done
Imported 8 keys.
```

5. **Introduzca `show` para ver los reinos Kerberos y los KDC.**

```
hostname:configuration services kerberos> show
Properties:
    <status> = online
    allow_weak_crypto = true

Realms:
REALM          KDC
TEST.NET       kdc1.us.oracle.com
```

6. **Para ver los principales correspondientes a un reino Kerberos, seleccione el reino Kerberos e introduzca `show`.**

```
hostname:configuration services kerberos> select TEST.NET
hostname:configuration services kerberos TEST.NET> show
Properties:
    kdcs = kdc1.us.oracle.com

Keytab entries:
NAME          KEYS  PRINCIPAL
principal-000 4      host/hostname.us.oracle.com@TEST.NET
principal-001 4      nfs/hostname.us.oracle.com@TEST.NET
```

7. Para ver las claves correspondientes a un principal, seleccione el principal e introduzca `show`.

```
hostname:configuration services kerberos TEST.NET> select principal-001
hostname:configuration services kerberos principal-001> show
Properties:
    name = nfs/hostname.us.oracle.com@TEST.NET
Keys:
KEY      KVNO  ENCTYPENO  ENCTYPE
key-000  28    18         AES-256 CTS mode with 96-bit SHA-1 HMAC
key-001  28    17         AES-128 CTS mode with 96-bit SHA-1 HMAC
key-002  28    16         Triple DES cbc mode with HMAC/sha1
key-003  28    23         ArcFour with HMAC/md5
key-004  28    24         Exportable ArcFour with HMAC/md5
key-005  28    3          DES cbc mode with RSA-MD5
key-006  28    1          DES cbc mode with CRC-32
```

Leyenda de cabeceras de columna:

- KEY = Nombre de clave
- KVNO = Número de versión de clave
- ENCTYPENO = Número de tipo de cifrado
- ENCTYPE = Tipo de cifrado

8. Para ver las propiedades de una clave, seleccione la clave e introduzca `show`.

```
hostname:configuration services kerberos principal-001> select key-003
hostname:configuration services kerberos principal-001 key-003> show
Properties:
    principal = nfs/hostname.us.oracle.com@TEST.NET
    kvno = 28
    enctype = ArcFour with HMAC/md5
    enctypeno = 23
```

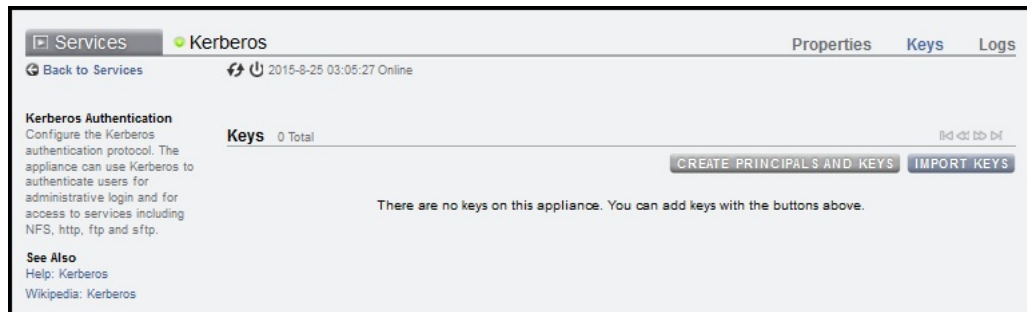
▼ Creación de principales y claves de Kerberos (BUI)

Use el siguiente procedimiento para crear principales de Kerberos en el servidor administrativo de KDC con el dispositivo. Se generan claves para cada principal y se las almacena en la tabla de claves del dispositivo. Las descripciones de cada propiedad están en [“Kerberos Service Properties” \[391\]](#).

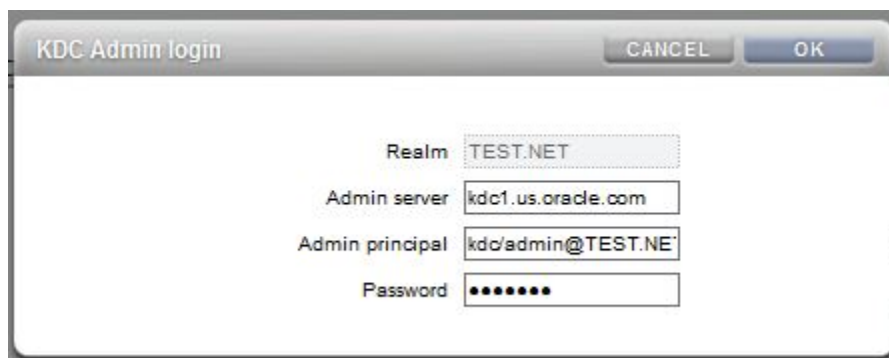
- Antes de empezar**
- Asegúrese de haber activado el servicio Kerberos, configurado el reino Kerberos e identificado los KDC como se describe en [Creación de un reino Kerberos \(BUI\) \[378\]](#).
 - Asegúrese de tener credenciales de inicio de sesión para KDC.

1. **Vaya a Configuración > Servicios.**
2. **Haga clic en Kerberos.**

3. Haga clic en **Keys (Claves)** y, luego, en **CREATE PRINCIPALS AND KEYS (Crear principales y claves)**.



4. En el cuadro de diálogo de inicio de sesión de administrador de KDC, complete los siguientes campos:
 - **Reino Kerberos:** este campo se rellena de manera automática y no se puede modificar.
 - **Servidor de administración:** nombre de host del servidor administrativo de KDC. Este campo se rellena automáticamente, pero se puede modificar.
 - **Principal de administrador:** nombre del administrador de KDC para el reino Kerberos.
 - **Contraseña:** contraseña del administrador de KDC.



5. Haga clic en **Aceptar**.
6. En el cuadro de confirmación, haga clic en **OK (Aceptar)**.

Aparece la lista de principales y claves.

KVNO	PRINCIPAL	ENCRYPTION TYPE	TYPE #
2	nfs/ar7320-220.us.oracle.com@TEST.NET	ArcFour with HMAC/md5	23
2	nfs/ar7320-220.us.oracle.com@TEST.NET	Triple DES cbc mode with HMAC/sha1	16
2	nfs/ar7320-220.us.oracle.com@TEST.NET	AES-128 CTS mode with 96-bit SHA-1 HMAC	17
2	nfs/ar7320-220.us.oracle.com@TEST.NET	AES-256 CTS mode with 96-bit SHA-1 HMAC	18
2	host/ar7320-220.us.oracle.com@TEST.NET	ArcFour with HMAC/md5	23
2	host/ar7320-220.us.oracle.com@TEST.NET	Triple DES cbc mode with HMAC/sha1	16
2	host/ar7320-220.us.oracle.com@TEST.NET	AES-128 CTS mode with 96-bit SHA-1 HMAC	17
2	host/ar7320-220.us.oracle.com@TEST.NET	AES-256 CTS mode with 96-bit SHA-1 HMAC	18
2	nfs/ar7320-230.us.oracle.com@TEST.NET	ArcFour with HMAC/md5	23
2	nfs/ar7320-230.us.oracle.com@TEST.NET	Triple DES cbc mode with HMAC/sha1	16
2	nfs/ar7320-230.us.oracle.com@TEST.NET	AES-128 CTS mode with 96-bit SHA-1 HMAC	17
2	nfs/ar7320-230.us.oracle.com@TEST.NET	AES-256 CTS mode with 96-bit SHA-1 HMAC	18
2	host/ar7320-230.us.oracle.com@TEST.NET	ArcFour with HMAC/md5	23
2	host/ar7320-230.us.oracle.com@TEST.NET	Triple DES cbc mode with HMAC/sha1	16
2	host/ar7320-230.us.oracle.com@TEST.NET	AES-128 CTS mode with 96-bit SHA-1 HMAC	17
2	host/ar7320-230.us.oracle.com@TEST.NET	AES-256 CTS mode with 96-bit SHA-1 HMAC	18

▼ Creación de principales y claves de Kerberos (CLI)

Use el siguiente procedimiento para crear principales de Kerberos en el servidor administrativo de KDC con el dispositivo. Se generan claves para cada principal y se las almacena en la tabla de claves del dispositivo. Las descripciones de cada propiedad están en [“Kerberos Service Properties” \[391\]](#) y [“Propiedades y logs de Kerberos” \[392\]](#).

- Antes de empezar**
- Asegúrese de haber activado el servicio Kerberos, configurado el reino Kerberos e identificado los KDC como se describe en [Creación de un reino Kerberos \(CLI\) \[380\]](#).
 - Asegúrese de tener credenciales de inicio de sesión para KDC.

1. Vaya a `configuration services kerberos` e introduzca `list`.

```
hostname:configuration services kerberos> list
REALM          KDC
TEST.NET
```

2. Seleccione el reino Kerberos.

```
hostname:configuration services kerberos> select TEST.NET
hostname:configuration services kerberos TEST.NET>
```

3. **Para crear los principales, introduzca `principals` y, a continuación, introduzca `show` para ver las propiedades.**

```
hostname:configuration services kerberos TEST.NET> principals
hostname:configuration services kerberos TEST.NET principals (uncommitted)> show
Properties:
    realm = TEST.NET
    server = kdc1.us.oracle.com
    admin = (unset)
    password = (unset)
```

4. **(Opcional) Para cambiar el servidor KDC, introduzca `set kdc=` y el nombre de host del servidor KDC. A continuación, introduzca `commit`.**

```
hostname:configuration services kerberos TEST.NET> set kdc=kdc2.us.oracle.com
    kdc = kdc2.us.oracle.com (uncommitted)
hostname:configuration services kerberos TEST.NET> commit
```

5. **Introduzca `set admin=` y el nombre de administrador de KDC para el reino Kerberos.**

```
hostname:configuration services kerberos TEST.NET principals (uncommitted)> set admin=kdc/
admin
```

6. **Introduzca `set password=` y la contraseña de administrador de KDC y, a continuación, introduzca `commit`.**

```
hostname:configuration services kerberos TEST.NET principals (uncommitted)> set
password=test123
    password = (set)
hostname:configuration services kerberos TEST.NET principals (uncommitted)> commit
```

7. **Introduzca `show` para ver los principales correspondientes a KDC.**

```
hostname:configuration services kerberos TEST.NET> show
Properties:
    kdc = kdc1.us.oracle.com
Keytab entries:
NAME KEYS PRINCIPAL
principal-000 4 host/hostname.us.oracle.com@TEST.NET
principal-001 4 nfs/hostname.us.oracle.com@TEST.NET
```

8. **Para ver las claves correspondientes a un principal, seleccione el principal e introduzca `show`.**

```
hostname:configuration services kerberos TEST.NET> select principal-001
hostname:configuration services kerberos principal-001> show
Properties:
    name = nfs/hostname.us.oracle.com@TEST.NET
Keys:
KEY KVNO ENCTYPENO ENCTYPE
key-000 28 18 AES-256 CTS mode with 96-bit SHA-1 HMAC
```

key-001	28	17	AES-128 CTS mode with 96-bit SHA-1 HMAC
key-002	28	16	Triple DES cbc mode with HMAC/sha1
key-003	28	23	ArcFour with HMAC/md5
key-004	28	24	Exportable ArcFour with HMAC/md5
key-005	28	3	DES cbc mode with RSA-MD5
key-006	28	1	DES cbc mode with CRC-32

Leyenda de cabeceras de columna:

- KEY = Nombre de clave
- KVNO = Número de versión de clave
- ENCTYPENO = Número de tipo de cifrado
- ENCTYPE = Tipo de cifrado

9. Para ver las propiedades de una clave, seleccione la clave e introduzca `show`.

```
hostname:configuration services kerberos principal-001> select key-003
hostname:configuration services kerberos principal-001 key-003> show
Properties:
    principal = nfs/hostname.us.oracle.com@TEST.NET
    kvno = 28
    enctype = ArcFour with HMAC/md5
    enctypeno = 23
```

▼ Supresión de principales y claves de Kerberos (BUI)

Use el siguiente procedimiento para suprimir claves individuales.

- 1. Vaya a Configuración > Servicios.**
- 2. Haga clic en Kerberos.**
- 3. Haga clic en Keys (Claves).**

Aparece la lista de principales y claves.

Keys 16 Total				1-16	
				CREATE PRINCIPALS AND KEYS	
				IMPORT KEYS	
KVNO	PRINCIPAL	ENCRYPTION TYPE	TYPE #		
2	nfs/ar7320-220.us.oracle.com@TEST.NET	ArcFour with HMAC/md5	23		
2	nfs/ar7320-220.us.oracle.com@TEST.NET	Triple DES cbc mode with HMAC/sha1	16		
2	nfs/ar7320-220.us.oracle.com@TEST.NET	AES-128 CTS mode with 96-bit SHA-1 HMAC	17		
2	nfs/ar7320-220.us.oracle.com@TEST.NET	AES-256 CTS mode with 96-bit SHA-1 HMAC	18		
2	host/ar7320-220.us.oracle.com@TEST.NET	ArcFour with HMAC/md5	23		
2	host/ar7320-220.us.oracle.com@TEST.NET	Triple DES cbc mode with HMAC/sha1	16		
2	host/ar7320-220.us.oracle.com@TEST.NET	AES-128 CTS mode with 96-bit SHA-1 HMAC	17		
2	host/ar7320-220.us.oracle.com@TEST.NET	AES-256 CTS mode with 96-bit SHA-1 HMAC	18		
2	nfs/ar7320-230.us.oracle.com@TEST.NET	ArcFour with HMAC/md5	23		
2	nfs/ar7320-230.us.oracle.com@TEST.NET	Triple DES cbc mode with HMAC/sha1	16		
2	nfs/ar7320-230.us.oracle.com@TEST.NET	AES-128 CTS mode with 96-bit SHA-1 HMAC	17		
2	nfs/ar7320-230.us.oracle.com@TEST.NET	AES-256 CTS mode with 96-bit SHA-1 HMAC	18		
2	host/ar7320-230.us.oracle.com@TEST.NET	ArcFour with HMAC/md5	23		
2	host/ar7320-230.us.oracle.com@TEST.NET	Triple DES cbc mode with HMAC/sha1	16		
2	host/ar7320-230.us.oracle.com@TEST.NET	AES-128 CTS mode with 96-bit SHA-1 HMAC	17		
2	host/ar7320-230.us.oracle.com@TEST.NET	AES-256 CTS mode with 96-bit SHA-1 HMAC	18		

- (Opcional) Para ordenar la vista por columna, como PRINCIPAL, haga clic en la cabecera de la columna.
- Para suprimir una clave individual, mueva el cursor del mouse sobre la fila correspondiente, haga clic en el ícono de la papelera  y confirme la acción.
Si suprime todas las claves de un principal, se suprime el principal del dispositivo.

▼ Supresión de principales y claves de Kerberos (CLI)

Use el siguiente procedimiento para suprimir claves individuales o suprimir todas las claves de un principal.

- Vaya a `configuration services kerberos` e introduzca `list`.

```
hostname:configuration services kerberos> list
REALM                                KDC
TEST.NET
```

2. Seleccione el reino Kerberos.

```
hostname:configuration services kerberos> select TEST.NET
hostname:configuration services kerberos TEST.NET>
```

3. Introduzca show para ver los principales correspondientes a KDC.

```
hostname:configuration services kerberos TEST.NET> show
Properties:
    kdc = kdc1.us.oracle.com
Keytab entries:
NAME      KEYS  PRINCIPAL
principal-000  4    host/hostname.us.oracle.com@TEST.NET
principal-001  4    nfs/hostname.us.oracle.com@TEST.NET
```

4. Para suprimir todas las claves de un principal, introduzca destroy y el nombre del principal y, a continuación, confirme la acción.

Para suprimir una clave individual, consulte el siguiente paso.

```
hostname:configuration services kerberos TEST.NET> destroy principal-000
This will delete all keys for "principal-000". Are you sure? (Y/N) Y
```

5. Para suprimir una clave individual de un principal, seleccione primero el principal e introduzca show para ver la lista de claves.

```
hostname:configuration services kerberos TEST.NET> select principal-001
hostname:configuration services kerberos principal-001> show
Properties:
    name = nfs/hostname.us.oracle.com@TEST.NET
Keys:
KEY      KVNO  ENCTYPENO  ENCTYPE
key-000  28    18         AES-256 CTS mode with 96-bit SHA-1 HMAC
key-001  28    17         AES-128 CTS mode with 96-bit SHA-1 HMAC
key-002  28    16         Triple DES cbc mode with HMAC/sha1
key-003  28    23         ArcFour with HMAC/md5
key-004  28    24         Exportable ArcFour with HMAC/md5
key-005  28    3          DES cbc mode with RSA-MD5
key-006  28    1          DES cbc mode with CRC-32
```

Leyenda de cabeceras de columna:

- KEY = Nombre de clave
- KVNO = Número de versión de clave
- ENCTYPENO = Número de tipo de cifrado
- ENCTYPE = Tipo de cifrado

6. Para ver las propiedades de una clave, seleccione la clave e introduzca show.

```
hostname:configuration services kerberos principal-001> select key-003
hostname:configuration services kerberos principal-001 key-003> show
Properties:
    principal = nfs/hostname.us.oracle.com@TEST.NET
    kvno = 28
    enctype = ArcFour with HMAC/md5
    encyteno = 23
```

7. **Para suprimir una clave o ver otra clave, introduzca `done` para regresar al contexto del principal.**

```
hostname:configuration services kerberos principal-001 key-003> done
hostname:configuration services kerberos principal-001>
```

8. **Para suprimir la clave, introduzca `destroy` y el nombre de la clave y, a continuación, confirme la acción.**

```
hostname:configuration services kerberos principal-001> destroy key-003
This will delete key "key-003". Are you sure? (Y/N) Y
```

▼ Destrucción de un reino Kerberos (BUI)

Quando se destruye un reino Kerberos, también se destruyen las claves correspondientes.

1. **Vaya a Configuración > Servicios.**
2. **Haga clic en Kerberos.**
3. **Borre el contenido del campo Reino Kerberos, haga clic en Aplicar y confirme la acción.**

▼ Destrucción de un reino Kerberos (CLI)

Quando se destruye un reino Kerberos, también se destruyen las claves correspondientes.

1. **Vaya a `configuration services kerberos`.**
2. **Introduzca `destroy` y el nombre del reino Kerberos y, a continuación, confirme la acción.**

```
hostname:configuration services kerberos> destroy TEST.NET
This will destroy "TEST.NET". Are you sure? (Y/N) Y
```

Kerberos Service Properties

Las siguientes propiedades están disponibles para el servicio Kerberos.

- **Reino Kerberos:** cadena; nombre del reino Kerberos.
- **KDC:** lista de cero o más nombres de host; centros de distribución de claves del reino Kerberos. Se considera que el primer centro de distribución de claves (KDC) de la lista es el servidor de administración, lo que es relevante si se crean principales en el KDC desde el dispositivo, pero no al importar claves. La lista puede estar vacía si se publica por lo menos un KDC para el reino Kerberos en DNS.

- **Permitir tipos de cifrado débiles:** valor booleano. Activa o desactiva la compatibilidad con los tipos de cifrado débil anticuados (des-cbc-crc, des-cbc-md5 y arcfour-hmac-exp). Esta propiedad está desactivada por defecto.
- **Administrador:** cadena; nombre del principal de administración de Kerberos (administrador). Por convención, el nombre de un principal se divide en tres componentes: el primario, la instancia y el reino Kerberos. Puede especificar un principal como joe, joe/admin o joe/admin@ENG.EXAMPLE.COM. Esta propiedad se usa solo si se crean principales de servicio, pero no se los conserva.
- **Contraseña:** contraseña de administración de Kerberos. Cadena; contraseña del administrador. Esta propiedad se usa solo si se crean principales de servicio, pero no se los conserva.

Los cambios realizados en las propiedades de los servicios se documentan en las secciones [Configuración de las propiedades de los servicios \(BUI\) \[328\]](#) y [Configuración de las propiedades de los servicios \(CLI\) \[329\]](#).

Propiedades y logs de Kerberos

En la siguiente tabla, se describe la asignación entre las propiedades de la CLI de Kerberos y las descripciones de propiedades de la BUI correspondientes.

Nota - Las propiedades más antiguas de Kerberos asociadas con el servicio NFS quedaron anticuadas, pero seguirán funcionando en secuencias de comandos y flujos de trabajo.

TABLA 73 Propiedades de Kerberos

Propiedad de la CLI	Propiedad de la BUI
realm	Realm (Reino Kerberos)
kdc	KDC(s) (KDC)
allow_weak_crypto	Permitir tipos de cifrado débiles. Uso de tipos de cifrado débil en Kerberos (arcfour-hmac-md5-exp, des-cbc-md5 y des-cbc-crc).
principals	Kerberos administrator principal (Principal de administrador de Kerberos)
principals - server	Admin server - KDC host name (Servidor de administración: nombre de host de KDC)
principals - admin	Admin principal - Administrator login name on KDC (Principal de administrador: nombre de inicio de sesión del administrador en KDC)
principals - password	Password - Administrator login password on KDC (Contraseña: contraseña de inicio de sesión del administrador en KDC)

Propiedad de la CLI	Propiedad de la BUI
importkeytab	Import Keys - Imports keys in a keytab file from the KDC (Importar claves: importa claves en un archivo de tabla de claves de KDC)
importkeytab - url	URL of keytab file (URL del archivo de tabla de claves)
importkeytab - user	User name for URL access (Nombre de usuario para el acceso URL)
importkeytab - password	Password for URL access (Contraseña para el acceso URL)

El siguiente log está disponible para el servicio Kerberos.

TABLA 74 Logs disponibles para el servicio Kerberos

Log	Descripción
appliance-kit-kerberos:default	Log de eventos del servicio Kerberos en el dispositivo

Configuración de LDAP

El protocolo de acceso a directorios ligero (LDAP) es un servicio de directorio para centralizar la gestión de usuarios, grupos, nombres de host y otros recursos (denominados objetos). El dispositivo puede actuar como un cliente LDAP con las siguientes características:

- Los usuarios de LDAP pueden iniciar sesión en los servicios de FTP y HTTP.
- Se puedan usar los nombres de usuario de LDAP (en lugar de identificadores numéricos) para configurar listas ACL del directorio raíz en los recursos compartidos.

Nota - El dispositivo no usa información de autorización de LDAP. Toda la información de autorización es local.

- El certificado del servidor LDAP puede ser autofirmado.
- Puede suministrar una lista de los certificados de autoridad de certificación de confianza.

Para configurar LDAP, establezca los valores del esquema, la configuración de seguridad y los servidores LDAP, tal como se describe en las siguientes secciones:

- [“Propiedades de LDAP” \[394\]](#)
- [“Asignaciones personalizadas de LDAP” \[396\]](#)
- Configuración de valores de esquema de LDAP: [BUI](#), [CLI](#)
- [“Configuración de seguridad de LDAP” \[402\]](#)

- Configuración de valores de seguridad de LDAP: [BUI](#), [CLI](#)
- Configuración de la lista de servidores LDAP: [BUI](#), [CLI](#)
- “Configuración de certificados de servidor LDAP” [407]
- Supervisión del estado de servidores LDAP: [BUI](#), [CLI](#)

Una vez completada la configuración de LDAP, puede configurar un usuario de LDAP existente como usuario del dispositivo. Consulte “[Agregación de un usuario de LDAP al dispositivo](#)” [411].

Propiedades de LDAP

Consulte la configuración apropiada para su entorno con el administrador del servidor LDAP.

En las tablas de esta sección, se describen las propiedades del esquema LDAP, las propiedades de seguridad y las propiedades del servidor.

TABLA 75 Propiedades del esquema LDAP

Propiedad de la BUI	Propiedad de la CLI	Descripción
Nombre distintivo de búsqueda base	base_dn	Nombre distintivo del objeto base, que es el punto inicial para las búsquedas de directorio. Este nombre distintivo de búsqueda base está precedido automáticamente por una especificación de subárbol por defecto: ou=people para búsquedas de usuarios, ou=group para búsquedas de grupos y ou=netgroup para búsquedas de grupos de red. Para sustituir este comportamiento por defecto, use las propiedades del descriptor de búsqueda que aparecen a continuación y se describen en “ Asignaciones personalizadas de LDAP ” [396].
Ámbito de búsqueda ■ Un nivel (no recursivo) ■ Subárbol (recursivo)	search_scope ■ one ■ sub	Objetos del directorio LDAP que se buscan, en relación con el objeto base. Para un ámbito no recursivo, o para one, los resultados de búsqueda se limitan solo a los objetos que están directamente por debajo del objeto de búsqueda base. Este es el valor por defecto. Para un ámbito recursivo, o para sub, los resultados de búsqueda pueden incluir cualquier objeto que esté por debajo del objeto de búsqueda base.
Definición de esquema para Usuarios, Grupos y Grupos de red ■ Descriptor de búsqueda ■ Asignaciones de atributos	■ user_search, group_search, netgroup_search ■ user_mapattr, group_mapattr, netgroup_mapattr	El esquema usado por el dispositivo. Use estas propiedades para anular el descriptor de búsqueda predeterminado (el nombre distintivo base más una especificación de subárbol por defecto), las asignaciones de atributos y las asignaciones de clases de objetos para usuarios, grupos y grupos de red. Para obtener más

Propiedad de la BUI	Propiedad de la CLI	Descripción
■ Asignaciones de clases de objetos	■ user_mapobjclass, group_mapobjclass, netgroup_mapobjclass	información, consulte “Asignaciones personalizadas de LDAP” [396] .

Temas relacionados

- [“Asignaciones personalizadas de LDAP” \[396\]](#)
- Configuración de valores de esquema de LDAP: [BUI](#), [CLI](#)

TABLA 76 Propiedades de seguridad de LDAP

Propiedad de la BUI	Propiedad de la CLI	Descripción
Autenticar como ■ Anónimos ■ Automático ■ Proxy (usuario específico)	cred_level ■ anonymous ■ self ■ proxy	Credenciales usadas para autenticar el dispositivo ante el servidor LDAP. Consulte “Configuración de seguridad de LDAP” [402] para ver las descripciones de estas opciones.
Activar SSL/TLS	use_tls	Alterne TLS (seguridad de capa de transporte, descendiente de SSL) para establecer conexiones seguras con el servidor LDAP. Si se usa el método Automático para autenticar, esta opción no está disponible porque este método usa el cifrado de Kerberos. Si especifica el puerto 636 al agregar un servidor LDAP, el sistema configura LDAP y TLS sin procesar. Si especifica cualquier otro puerto al agregar un servidor LDAP (generalmente, el puerto 389), el sistema configura LDAP y StartTLS. Al usar TLS sin procesar, se utiliza un puerto dedicado por separado para la conexión TLS segura. Con StartTLS, el servidor LDAP no requiere un puerto dedicado para establecer la conexión LDAP cifrada. El servidor LDAP usa el mismo puerto 389 para una conexión TLS.
Método de autenticación ■ Simple (RFC 4513) ■ SASL/DIGEST-MD5	auth_method ■ simple ■ sasl/DIGEST-MD5 ■ sasl/GSSAPI ■ none	Método usado para autenticar el dispositivo ante el servidor LDAP. Si se autentica como Proxy, seleccione el método de autenticación Simple o SASL/DIGEST-MD5, y establezca el nombre distintivo y una contraseña. En la CLI, establezca auth_method en sasl/GSSAPI si usa el método de autenticación self. Establezca auth_method en none si usa el método de autenticación anonymous.
Nombre distintivo	proxy_dn	El nombre distintivo de la cuenta que se usará para la autenticación del proxy.
Contraseña	proxy_password	La contraseña de la cuenta de nombre distintivo del proxy.

Temas relacionados

- [“Configuración de seguridad de LDAP” \[402\]](#)
- Configuración de valores de seguridad de LDAP: [BUI](#), [CLI](#)

TABLA 77 Propiedades del servidor LDAP

Propiedad de la BUI	Propiedad de la CLI	Descripción
■ Usar orden de servidores ■ Ignorar el orden de los servidores	use_server_order	Consulte la descripción de la propiedad del servidor para obtener una explicación del efecto que produce configurar el orden de servidores en una lista de servidores.
Camarero	servers	La lista de servidores LDAP que se utilizan. ■ Si se especifica un solo servidor, el dispositivo usa ese único servidor. Si ese servidor falla, los servicios LDAP no estarán disponibles. ■ Si se especifican varios servidores y se selecciona Ignorar el orden de los servidores en la BUI o si use_server_order es false, el servidor de la lista que esté en funcionamiento podrá usarse en cualquier momento sin preferencias en particular. Si alguno de los servidores falla, se usa otro de los servidores de la lista. Los servicios LDAP siguen estando disponibles, a menos que fallen todos los servidores especificados. ■ Si se especifican varios servidores y se selecciona Usar orden de servidores en la BUI o si use_server_order es true, los servicios LDAP usarán el primer servidor de la lista que esté disponible. Se selecciona el primer servidor de la lista; si falla, se selecciona el próximo servidor de la lista. Los servicios LDAP siguen estando disponibles, a menos que fallen todos los servidores especificados.

Temas relacionados

- [“Configuración de certificados de servidor LDAP” \[407\]](#)
- Configuración de la lista de servidores LDAP: [BUI](#), [CLI](#)
- Supervisión del estado de servidores LDAP: [BUI](#), [CLI](#)

Asignaciones personalizadas de LDAP

Para buscar en el directorio LDAP, el dispositivo usa un descriptor de búsqueda que es el nombre distintivo de búsqueda base, precedido por una especificación de subárbol por defecto. El dispositivo también utiliza nombres de clase de objeto por defecto y nombres de atributo por defecto para buscar las propiedades necesarias.

El dispositivo tiene el siguiente comportamiento de búsqueda en LDAP, de acuerdo con el formato RFC 2307:

- Búsquedas de usuarios: se antepone `ou=people` al nombre distintivo de búsqueda base, se utilizan la clase de objeto `posixAccount` y los nombres de atributos que se muestran en [Atributos del tipo de datos de usuarios](#).
- Búsquedas de grupos: se antepone `ou=group` al nombre distintivo de búsqueda base, se utilizan la clase de objeto `posixGroup` y los nombres de atributos que se muestran en [Atributos del tipo de datos de grupos](#).
- Búsquedas de grupos de red: se antepone `ou=netgroup` al nombre distintivo de búsqueda base y se utiliza la clase de objeto `nisNetgroup`.

Si estos valores por defecto no funcionan en su entorno, use las propiedades que se muestran en [Propiedades del esquema LDAP](#) para personalizar el descriptor de búsqueda, los nombres de clases de objetos y nombres de atributos como se muestra en Configuración de valores de esquema de LDAP: [BUI](#), [CLI](#). Para personalizar un descriptor de búsqueda, introduzca el nombre distintivo completo, incluido el nombre distintivo de búsqueda base y el ámbito de búsqueda. El dispositivo usará este valor personalizado sin modificar y no tendrá en cuenta los valores definidos para las propiedades Nombre distintivo de búsqueda base y Ámbito de búsqueda. Para personalizar nombres de clases de objetos y nombres de atributos, use la sintaxis *default=new*, donde *default* es el valor por defecto y *new* es el valor que desea utilizar.

En la siguiente tabla, se muestran los nombres de atributos por defecto que se utilizan para buscar información sobre los usuarios.

TABLA 78 Atributos de tipo de datos de usuarios

Nombre del atributo por defecto	Descripción del valor del atributo
<code>uid</code>	Nombre de usuario. Por ejemplo: <code>f1astname</code>
<code>uidNumber</code>	ID de usuario numérico
<code>gidNumber</code>	ID de grupo principal numérico
<code>gecos</code>	Nombre mostrado. Por ejemplo: <i>"Firstname, Lastname"</i>

En la siguiente tabla, se muestran los nombres de atributos por defecto que se utilizan para buscar información sobre los grupos.

TABLA 79 Atributos de tipo de datos de grupos

Nombre del atributo por defecto	Descripción del valor del atributo
<code>cn</code>	Nombre de grupo
<code>gidNumber</code>	ID de grupo numérico
<code>memberUid</code>	Lista de nombres de usuarios de miembros

Temas relacionados

- [Propiedades del esquema LDAP](#)

- Configuración de valores de esquema de LDAP: [BUI](#), [CLI](#)

▼ Configuración de valores de esquema de LDAP (BUI)

1. Vaya a Configuración > Servicios.

2. En Servicios de directorio, seleccione LDAP.

En el separador Propiedades, vaya a la sección Esquema de la página.

3. Introduzca un valor para el nombre distintivo de búsqueda base.

Por ejemplo, introduzca:

```
dc=example,dc=com
```

Este nombre distintivo de búsqueda base está precedido automáticamente con `ou=people` en las búsquedas de usuarios, `ou=group` en las búsquedas de grupos y `ou=netgroup` para búsquedas de grupos de red. Si estos valores no funcionan en su entorno, establezca diferentes valores para el descriptor de búsqueda en la definición del esquema de este tipo de búsqueda. El valor del nombre distintivo de búsqueda base se ignora si proporciona un valor para el descriptor de búsqueda en la definición del esquema.

4. Seleccione un ámbito de búsqueda recursivo o no recursivo.

Esta selección es aplicable a todas las búsquedas. Si desea anular esta selección para tipos específicos de búsquedas, proporcione un valor para el descriptor de búsqueda en la definición del esquema de este tipo de búsqueda. El valor del ámbito de búsqueda se ignora si proporciona un valor para el descriptor de búsqueda en la definición del esquema.

5. Haga clic en Editar, junto a la cabecera de definición del esquema.

Se abrirá el cuadro de diálogo Editar definición de esquema LDAP. El cuadro de diálogo tiene tres separadores: Usuarios, Grupos y Grupos de red. Cada uno tiene tres campos de propiedades: Descriptor de búsqueda, Asignaciones de atributos y Asignaciones de clases de objetos.

6. Edite los campos del descriptor de búsqueda.

El descriptor de búsqueda por defecto que se utiliza para las búsquedas de usuarios es `ou=people,base-search-DN`. El descriptor de búsqueda por defecto que se utiliza para las búsquedas de grupos es `ou=group,base-search-DN`. El descriptor de búsqueda por defecto que se utiliza para las búsquedas de grupos de red es `ou=netgroup,base-search-DN`. Si la base de datos LDAP no tiene subárboles denominados `people`, `group` o `netgroup`, las búsquedas en la base de datos se considerarán por error objetos no encontrados.

Edite los campos del descriptor de búsqueda en cada separador e introduzca los subárboles correctos para buscar usuarios, grupos y grupos de red. Por ejemplo, en el separador Usuarios, puede introducir lo siguiente en el descriptor de búsqueda:

```
ou=employees,dc=example,dc=com
```

Si la base de datos LDAP no tiene subárboles de usuarios y grupos, use este campo del descriptor de búsqueda y vuelva a introducir el nombre distintivo de búsqueda base para impedir que `ou=people` o `ou=group` se antepongan automáticamente. Por ejemplo, introduzca lo siguiente en los campos Usuarios o Grupos del descriptor de búsqueda:

```
dc=example,dc=com
```

Debe incluir el nombre distintivo de búsqueda base completo en el valor del descriptor de búsqueda. También elija un ámbito. Tanto el nombre distintivo de búsqueda base como la selección de ámbito se ignorarán y, en su lugar, se usará el valor del descriptor de búsqueda. El ejemplo del párrafo anterior especifica una búsqueda no recursiva. Para especificar una búsqueda recursiva, cambie el ejemplo de este modo:

```
dc=example,dc=com?sub
```

7. Edite los campos de asignaciones de atributos.

Los atributos por defecto que se utilizan para búsquedas de usuarios se muestran en [Atributos del tipo de datos de usuarios](#). Los atributos por defecto que se utilizan para búsquedas de grupos se muestran en [Atributos del tipo de datos de grupos](#).

Si su organización almacena estos datos en diferentes atributos, use el campo de asignaciones de atributos para especificar el atributo que usará a fin de recuperar los datos proporcionados. Por ejemplo, para usar `employeename` en lugar de `uid` como atributo para los nombres de usuarios, introduzca `uid=employeename` en el campo de asignaciones de atributos en el separador Usuarios.

Para especificar cambios de atributos adicionales en un tipo de datos determinado, haga clic en el ícono de agregación  ubicado a la derecha del campo de asignaciones de atributos.

8. Edite los campos de asignaciones de clases de objetos.

La clase de objeto por defecto que se utiliza para las búsquedas de usuarios es `posixAccount`. La clase de objeto por defecto que se utiliza para las búsquedas de grupos es `posixGroup`. La clase de objeto por defecto que se utiliza para las búsquedas de grupos de red es `nisNetgroup`.

Si en su entorno se utiliza otra clase de objeto, use el campo de asignaciones de clases de objetos para especificar el nombre de la clase que usará. Por ejemplo, para usar `unixaccount` en lugar de `posixAccount` como clase de objeto del usuario, introduzca `posixAccount=unixaccount` en el campo de asignaciones de clases de objetos en el separador Usuarios.

Para especificar cambios de clases de objetos adicionales, haga clic en el ícono de agregación  ubicado a la derecha del campo de asignaciones de clases de objetos.

9. Haga clic en **Guardar** en el cuadro de diálogo **Editar definición de esquema LDAP**.
10. Haga clic en **Aplicar** en la parte superior de la página LDAP.

Temas relacionados

- [Propiedades del esquema LDAP](#)
- [Atributos del tipo de datos de usuarios](#)
- [Atributos del tipo de datos de grupos](#)

▼ Configuración de valores de esquema de LDAP (CLI)

1. Vaya a `configuration services ldap` e introduzca el comando `show`.
2. Introduzca un valor para el nombre distintivo de búsqueda base.

Encierre el valor entre comillas para conservar los símbolos de igual y la coma incrustados. Por ejemplo, introduzca:

```
hostname:configuration services ldap> set base_dn="dc=example,dc=com"
```

Este nombre distintivo de búsqueda base está precedido automáticamente con `ou=people` en las búsquedas de usuarios, `ou=group` en las búsquedas de grupos y `ou=netgroup` para búsquedas de grupos de red. Si estos valores no funcionan en su entorno, establezca valores distintos para `user_search`, `group_search` o `netgroup_search`. El valor de `base_dn` se ignora si proporciona un valor para `user_search`, `group_search` o `netgroup_search`.

3. Especifique un ámbito recursivo o no recursivo.

Para una búsqueda recursiva, establezca `search_scope` en `sub`. Para una búsqueda no recursiva, establezca `search_scope` en `one`.

El valor de `search_scope` se aplica a todas las búsquedas. Si desea sustituir `search_scope` para tipos específicos de búsquedas, proporcione un valor en `user_search`, `group_search` o `netgroup_search`.

4. Configure las propiedades del descriptor de búsqueda.

Las propiedades del descriptor de búsqueda son `user_search`, `group_search` y `netgroup_search`.

Por defecto, `ou=people` se antepone al valor de `base_dn` en las búsquedas de usuarios, `ou=group` se antepone al valor de `base_dn` en las búsquedas de grupos y `ou=netgroup` se antepone al valor de `base_dn` en las búsquedas de grupos de red. Si la base de datos LDAP no tiene subárboles denominados `people`, `group` o `netgroup`, las búsquedas en la base de datos se considerarán por error objetos no encontrados.

Configure los valores de las propiedades del descriptor de búsqueda para especificar los subárboles correctos para la búsqueda de usuarios, grupos y grupos de red. Encierre el valor entre comillas para conservar los símbolos de igual y las comas incrustados. Por ejemplo, puede introducir lo siguiente en el descriptor de búsqueda de usuarios:

```
hostname:configuration services ldap> set user_search="ou=employees,dc=example,dc=com"
```

Si la base de datos LDAP no tiene subárboles de usuarios y grupos, use las propiedades del descriptor de búsqueda y vuelva a introducir el nombre distintivo de búsqueda base para que ni `ou=people` ni `ou=group` se antepongan automáticamente, tal como se muestra en el siguiente ejemplo:

```
hostname:configuration services ldap> set group_search="dc=example,dc=com"
```

Debe incluir el valor de `base_dn` en el descriptor de búsqueda. También elija un ámbito. Tanto `base_dn` como `search_scope` se ignorarán y, en cambio, se usará el valor del descriptor de búsqueda. El ejemplo del párrafo anterior especifica una búsqueda no recursiva. Para especificar una búsqueda recursiva, cambie el ejemplo de este modo:

```
hostname:configuration services ldap> set group_search="dc=example,dc=com?sub"
```

5. Configure las propiedades de asignación de atributos.

Los atributos por defecto que se utilizan para búsquedas de usuarios se muestran en [Atributos del tipo de datos de usuarios](#). Los atributos por defecto que se utilizan para búsquedas de grupos se muestran en [Atributos del tipo de datos de grupos](#).

Si en su entorno se almacenan estos datos en diferentes atributos, use las propiedades `user_mapattr`, `group_mapattr` y `netgroup_mapattr` para especificar el atributo que usará a fin de recuperar los datos proporcionados. Por ejemplo, para usar `employeename` en lugar de `uid` como atributo para los nombres de usuarios, introduzca el siguiente comando:

```
hostname:configuration services ldap> set user_mapattr="uid=employeename"
```

Encierre la asignación entre comillas para conservar el símbolo de igual en la asignación.

Para especificar varios cambios de atributos, introduzca una lista de asignaciones con cada asignación entre comillas, tal como se muestra en el siguiente ejemplo:

```
hostname:configuration services ldap> set user_mapattr="uid=employeename", "
uidNumber=employeenumber"
```

6. Configure las propiedades de asignación de objetos.

La clase de objeto por defecto que se utiliza para las búsquedas de usuarios es `posixAccount`. La clase de objeto por defecto que se utiliza para las búsquedas de grupos es `posixGroup`. La clase de objeto por defecto que se utiliza para las búsquedas de grupos de red es `nisNetgroup`.

Si en su entorno se usa otra clase de objetos, use las propiedades `user_mapobjclass`, `group_mapobjclass` y `netgroup_mapobjclass` para especificar el nombre de la clase de objeto que

se usará. Por ejemplo, para usar `unixaccount` en lugar de `posixAccount` como clase de objeto del usuario, introduzca el siguiente comando:

```
hostname:configuration services ldap> set user_mapobjclass="posixAccount=unixaccount"
```

7. Confirme el cambio en la configuración de las propiedades.

Introduzca `show`, revise la configuración de las propiedades e introduzca `commit`.

Temas relacionados

- [Propiedades del esquema LDAP](#)
- [Atributos del tipo de datos de usuarios](#)
- [Atributos del tipo de datos de grupos](#)

Configuración de seguridad de LDAP



Atención - Para reducir los riesgos de seguridad, siempre configure LDAP con SSL/TLS o Kerberos.

Para configurar los valores de seguridad del dispositivo LDAP, primero especifique las credenciales que se usarán para autenticar el dispositivo en el servidor LDAP. A continuación, especifique otras propiedades, según se necesite, para respaldar la elección de credenciales.

El dispositivo puede autenticarse mediante uno de los siguientes juegos de credenciales:

Anónimo

El método de autenticación Anónimo restringe el acceso a datos del dispositivo solamente a los datos que están disponibles para todos.

Puede optar por activar el protocolo TLS (antes conocido como SSL). Se recomienda firmemente activar TLS para que la información crítica se envíe de forma segura.

Automático

El método de autenticación Automático usa la identidad y las credenciales del usuario para autenticar el dispositivo. La autenticación automática utiliza el cifrado de Kerberos y el método de autenticación SASL/GSSAPI.

Proxy (usuario específico)

El método de autenticación Proxy usa un proxy para una cuenta de usuario específica.

Puede optar por activar el protocolo TLS (antes conocido como SSL). Se recomienda firmemente activar TLS para que la información crítica se envíe de forma segura.

Debe seleccionar el método de autenticación: Simple (RFC 4513) o SASL/DIGEST-MD5.

Debe especificar el nombre distintivo del proxy y la contraseña de proxy. El nombre distintivo de proxy es el nombre distintivo que corresponde a la cuenta que se usará para la autenticación del proxy. La contraseña de proxy es la contraseña que corresponde a la cuenta del nombre distintivo de proxy.

Si especifica el puerto 636 al agregar un servidor LDAP, el sistema configura LDAP y TLS sin procesar. Si especifica cualquier otro puerto al agregar un servidor LDAP (generalmente, el puerto 389), el sistema configura LDAP y StartTLS. Para obtener información sobre StartTLS, consulte [Propiedades de seguridad de LDAP](#).

▼ Configuración de valores de seguridad de LDAP (BUI)

1. Vaya a Configuración > Servicios.

2. En Servicios de directorio, seleccione LDAP.

En el separador Propiedades, vaya a la sección Configuración de seguridad de la página.

3. Especifique las credenciales que se usarán para autenticar el dispositivo en el servidor LDAP.

Para la opción Autenticar como, seleccione Anónimo, Automático o Proxy (usuario específico).

4. Active SSL/TLS.

Si seleccionó el valor Anónimo o Proxy para Autenticar como, puede optar por activar SSL/TLS. Se recomienda firmemente activar TLS para que la información crítica se envíe de forma segura.

5. Especifique un método de autenticación.

Si seleccionó Proxy en la opción Autenticar como, seleccione Simple (RFC 4513) o SASL/DIGEST-MD5 en el menú Método de autenticación. A continuación, especifique el nombre distintivo y la contraseña.

6. Haga clic en Aplicar.

Se valida la configuración del servidor LDAP. Si el nombre distintivo de proxy o la contraseña de proxy genera un fallo o un timeout, aparece una advertencia.

Temas relacionados

- [Propiedades de seguridad de LDAP](#)
- [“Configuración de seguridad de LDAP” \[402\]](#)

▼ Configuración de valores de seguridad de LDAP (CLI)

1. **Para ver las propiedades, vaya a `configuration services ldap` e introduzca `show`.**

En la siguiente tabla, se muestran combinaciones de valores de propiedades que son válidas para los restantes pasos de este procedimiento.

cred_level	auth_method	use_tls
anonymous	none	true
anonymous	none	false
self	sasl/GSSAPI	false
proxy	simple	true
proxy	simple	false Nota - Esta configuración está permitida, pero no se recomienda, ya que el nombre distintivo (DN) y la contraseña del usuario se enviarán en texto sin formato.
proxy	sasl/DIGEST-MD5	true
proxy	sasl/DIGEST-MD5	false

2. **Especifique las credenciales que se usarán para autenticar el dispositivo en el servidor LDAP.**

Defina `cred_level` en `anonymous`, `self` o `proxy`.

```
hostname:configuration services ldap> set cred_level=proxy
```

3. **Especifique un método de autenticación.**

Defina `auth_method` en una de las siguientes opciones:

- `none`: ninguno (utilizar `conanonymous`)
- `sasl/GSSAPI`: SASL/GSSAPI (utilizar con `self`)
- `simple`: simple, RFC 4513 (utilizar con `proxy`)
- `sasl/DIGEST-MD5`: SASL/DIGEST-MD5 (utilizar con `proxy`)

```
hostname:configuration services ldap> set auth_method=sasl/DIGEST-MD5
```

4. **Defina propiedades adicionales para las credenciales de proxy.**

Si `cred_level` está configurado en `proxy`, defina el nombre y la contraseña de la cuenta de proxy.

```
hostname:configuration services ldap> set proxy_dn=ProxyName
hostname:configuration services ldap> set proxy_password=MyPassword5
```

5. **Active SSL/TLS.**

Si especificó `anonymous` o `proxy` para `cred_level`, puede optar por activar SSL/TLS. Se recomienda firmemente activar TLS para que la información crítica se envíe de forma segura.

```
hostname:configuration services ldap> set use_tls=true
```

6. Introduzca el comando `commit`.

Los cambios en la configuración del servidor LDAP se validan cuando se los confirma. Si la validación de `proxy_dn` o `proxy_password` genera un fallo o un timeout, aparece un mensaje de advertencia.

Temas relacionados

- [Propiedades de seguridad de LDAP](#)
- [“Configuración de seguridad de LDAP” \[402\]](#)

▼ Configuración de la lista de servidores LDAP (BUI)

1. Vaya a Configuración > Servicios.

2. En Servicios de directorio, seleccione LDAP.

En el separador Propiedades, desplácese hasta la sección Servidores LDAP de la página.

3. Configure la lista.

- **Si tiene pensado incluir más de un servidor en la lista, decida si los servidores se probarán en algún orden en particular.**

Si los servidores van a probarse en el orden en que aparecen en la lista, seleccione el botón "Usar orden de servidores" en la parte superior de la lista. Por defecto, se selecciona "Ignorar el orden de los servidores". Para obtener más información sobre el uso de servidores, consulte [Propiedades del servidor LDAP](#).

- **Para agregar un servidor a la lista, haga clic en el ícono de agregación  ubicado a la izquierda del título de la sección Servidores LDAP.**

En el cuadro de diálogo Servidor LDAP nuevo, introduzca el nombre del servidor, como `hostname.example.com` y, opcionalmente, el puerto.

LDAP Servers			☒ Use server order	☐ Ignore server order
SERVER	LAST SEEN	RTT		
 ldap-server1.us.example.com:636	4s	796.968ms		
    ldap-server2.us.example.com:484	4s	48.454ms		

- **Para cambiar el orden de los servidores en la lista, use las herramientas que aparecen a la izquierda de la fila.**

Estas herramientas solo están disponibles si se selecciona y se aplica "Usar orden de servidores".

Haga clic en la fila del servidor que desea mover y realice una de las siguientes acciones:

- **Haga clic en las flechas arriba o abajo que aparecen a la izquierda de la fila.**
- **Haga clic y mantenga presionado el ícono de movimiento que aparece en el extremo izquierdo de la fila. Luego, arrastre la entrada del servidor hacia arriba o abajo en la lista.**
- **Para cambiar el nombre de un servidor de la lista, haga clic en la fila del servidor que desea modificar y, a continuación, en el ícono de edición  ubicado a la derecha de la fila.**
- **Para quitar un servidor de la lista, haga clic en la fila del servidor que desea quitar y, a continuación, en el ícono de papelera  ubicado a la derecha de la fila.**

4. Haga clic en el botón Aplicar que se encuentra en la parte superior de la página.

Temas relacionados

- [Propiedades del servidor LDAP](#)
- [“Configuración de certificados de servidor LDAP” \[407\]](#)
- [Supervisión del estado de servidores LDAP \(BUI\) \[410\]](#)

▼ Configuración de la lista de servidores LDAP (CLI)

1. Vaya a `configuration services ldap`.
2. Introduzca el comando `list` para mostrar los servidores LDAP existentes.
3. Configure la lista.
 - Si tiene pensado incluir más de un servidor en la lista, decida si los servidores se probarán en algún orden en particular.
 Si los servidores deben probarse en el orden en que aparecen especificados en la propiedad `servers`, establezca la propiedad `use_server_order` en `true`. El valor por defecto de la propiedad `use_server_order` es `false`. Para obtener más información sobre el uso de servidores, consulte [Propiedades del servidor LDAP](#).
 - Confirme el valor de la propiedad `servers`.

```
hostname:configuration services ldap> get servers
servers = ldap-server2.us.example.com:484,ldap-server1.us.example.com:636
```
 - Para agregar, quitar o reordenar los servidores en la lista, restablezca el valor de la propiedad `servers`.
 En el siguiente ejemplo, se reordena la lista:

```
hostname:configuration services ldap> set servers=ldap-server1.us.example.com:636,ldap-server2.us.example.com:484
```
4. Introduzca el comando `commit`.

Temas relacionados

- [Propiedades del servidor LDAP](#)
- [“Configuración de certificados de servidor LDAP” \[407\]](#)
- [Supervisión del estado de servidores LDAP \(CLI\) \[410\]](#)

Configuración de certificados de servidor LDAP

Un certificado del servidor LDAP puede ser autofirmado o estar firmado por una autoridad de certificación. En esta sección, se describe cómo configurar certificados inicialmente y cómo gestionar un nuevo certificado cuando caduca el anterior.

Configuración inicial de certificados de servidor LDAP

Para obtener más información sobre los certificados de confianza, consulte las secciones al respecto en [“Configuración de certificados” \[303\]](#).

Puede suministrar una lista de los certificados de autoridad de certificación de confianza. Los certificados de servidor LDAP emitidos por estas autoridades de certificación de confianza no requieren una gestión especial.

Si un certificado del servidor LDAP no fue emitido por una autoridad de certificación de confianza (es decir, es autofirmado o lo emitió una autoridad de certificación regular), se le pedirá a usted que revise y apruebe el certificado. El cuadro de diálogo Aceptar certificado de servidor LDAP muestra información sobre el certificado y le solicita que acepte o rechace el certificado. Si lo acepta, el certificado se agrega a la lista de certificados de confianza.

Gestión de certificados de servidor LDAP nuevos y caducados

Si aceptó un certificado individualmente (ya sea un certificado autofirmado o firmado por una autoridad de certificación), cuando el certificado del servidor LDAP caduque, usted deberá aprobar el certificado nuevo. Seleccione el servidor, pruebe la conexión, examine el certificado nuevo y apruébelo. Consulte Aprobación de un nuevo certificado de servidor LDAP: [BUI](#), [CLI](#).

Si suministra certificados de una autoridad de certificación, los cambios en cada certificado del servidor se harán automáticamente. Cuando el servidor cambie los certificados de una autoridad de certificación, asegúrese de que el nuevo certificado de la autoridad de certificación se haya agregado al dispositivo antes de que el servidor LDAP empiece a utilizarlo. Si el servidor empieza a usar el nuevo certificado de una autoridad de certificación antes de que usted lo haya agregado al dispositivo, el servicio LDAP se interrumpirá.

▼ Aprobación de un nuevo certificado de servidor LDAP (BUI)

Siga este procedimiento para aceptar un nuevo certificado después de que caduque el certificado anterior.

Antes de empezar TLS debe estar activado. Asegúrese de que esté activada la casilla Activar SSL/TLS.

1. **Vaya a Configuración > Servicios.**
2. **En Servicios de directorio, seleccione LDAP.**
En el separador Propiedades, desplácese hasta la sección Servidores LDAP de la página.
3. **En la tabla, haga clic en el ícono de edición  del servidor que tiene el nuevo certificado.**

4. **Haga clic en el botón Probar conexión en el cuadro de diálogo Editar servidor LDAP para probar la conexión de TLS.**

En un cuadro de diálogo nuevo, se informa si el certificado nuevo es de confianza.

5. **En el cuadro de diálogo del certificado de confianza, haga clic en el botón Aceptar.**

Si en este cuadro de diálogo se informó que el certificado no es de confianza, se abrirá el cuadro de diálogo Aceptar certificado de servidor LDAP. Allí verá información sobre el certificado y los botones Rechazar y Aceptar.

6. **Revise la información del certificado y haga clic en el botón Aceptar.**

El certificado se agrega a la lista de certificados de confianza.

Temas relacionados

- [Visualización de detalles de certificados de confianza \(BUI\) \[314\]](#)

▼ Aprobación de un nuevo certificado de servidor LDAP (CLI)

Siga este procedimiento para aceptar un nuevo certificado después de que caduque el certificado anterior.

Antes de empezar TLS debe estar activado. Asegúrese de que la propiedad `use_tls` esté establecida en `true`.

1. **Vaya a `configuration services ldap`.**
2. **Introduzca el comando `list` para mostrar la lista de servidores LDAP.**
3. **Seleccione un servidor.**
4. **Introduzca el comando `test` para probar la conexión de TLS.**

Se muestra información sobre el certificado nuevo.

5. **Examine y apruebe el certificado nuevo.**

El certificado se agrega a la lista de certificados de confianza. Si vuelve a introducir el comando `test`, aparece el mensaje "El certificado es de confianza".

Temas relacionados

- [Visualización de detalles de certificados de confianza \(CLI\) \[314\]](#)

▼ Supervisión del estado de servidores LDAP (BUI)

1. **Vaya a Configuración > Servicios.**

2. **En Servicios de directorio, seleccione LDAP.**

3. **Consulte el estado del servidor.**

En el separador Propiedades, desplácese hasta la sección Servidores LDAP de la página.

Para cada servidor, se muestra el siguiente estado:

- **Ícono de estado:** indicador que representa el estado del servidor. El ícono de indicador está en línea  o no disponible .
- **Última visualización:** tiempo total transcurrido desde que se recibió la última respuesta de cada servidor LDAP.
- **RTT:** tiempo de ida y vuelta para recibir la respuesta del servidor.

4. **Consulte los logs del servidor LDAP.**

a. **Haga clic en el separador Logs en la parte superior de la página LDAP.**

b. **Seleccione un servidor LDAP en el menú desplegable.**

Las entradas del log incluyen una hora y una descripción para alertas de servidores LDAP específicos.

c. **Consulte otros logs.**

Use los botones de flechas ubicados a la derecha del menú del servidor para ver logs anteriores o posteriores sobre el servidor seleccionado.

Temas relacionados

- [Propiedades del servidor LDAP](#)
- [Configuración de la lista de servidores LDAP \(BUI\) \[405\]](#)

▼ Supervisión del estado de servidores LDAP (CLI)

1. **Vaya a `configuration services ldap`.**

2. **Introduzca el comando `list` para mostrar el estado de los servidores LDAP.**

```
hostname:configuration services ldap> list
SERVER          STATUS          LDAP SERVER
```

```
server-000  unavailable  ldap-server1.us.example.com:636
server-001  online       ldap-server2.us.example.com:484
```

Temas relacionados

- [Propiedades del servidor LDAP](#)
- [Configuración de la lista de servidores LDAP \(CLI\) \[407\]](#)

Agregación de un usuario de LDAP al dispositivo

Después de completar la configuración de LDAP, puede configurar que los usuarios de LDAP existentes puedan iniciar sesión en el dispositivo mediante su nombre de host y contraseña de LDAP.

Nota - El ID de usuario de LDAP existente no puede ser menor que 100 ni mayor que 2147483646; tampoco puede ser igual que 60001, 60002 o 65534. Esos UID están reservados por el proveedor del sistema operativo para el uso en aplicaciones futuras. Los usuarios finales del sistema y los proveedores de productos en capas no pueden utilizarlos ya que, si lo hicieran, se podrían producir problemas de seguridad con otras aplicaciones.

En la BUI, siga el procedimiento [Agregación de un administrador o usuario \(BUI\) \[258\]](#) utilizando los siguientes valores de propiedades:

1. Seleccione Directorio en el menú desplegable Tipo.
2. En Nombre de usuario, especifique el nombre de usuario de LDAP existente del usuario.

En la CLI, siga el procedimiento [Agregación de un administrador o usuario \(CLI\) \[260\]](#) mediante el tipo de usuario `directory` y el nombre de usuario de LDAP existente del usuario.

```
hostname:configuration users> directory LDAPusername
```

Los campos ID de usuario (`uid`) y Contraseña (`initial_password`) se configuran automáticamente: Se utilizan los valores de LDAP o, si se configuró NIS, los valores de NIS.

Nota - Si se configuran tanto NIS como LDAP en el dispositivo, y los servicios devuelven información diferente para un usuario determinado, el dispositivo utiliza los datos proporcionados por NIS.

Configuración de NDMP

El servicio de protocolo simple de administración de redes (NDMP) permite al sistema participar en operaciones de copia de seguridad y restauración basadas en NDMP controladas

por un cliente remoto de NDMP denominado Aplicación de gestión de datos (DMA). Con NDMP, los datos almacenados en recursos compartidos creados por el administrador en el dispositivo se pueden incluir en copias de seguridad y se pueden restaurar tanto con dispositivos de cinta conectados localmente o con sistemas remotos. Los dispositivos de cinta conectados localmente también se pueden exponer a DMA para operaciones de copia de seguridad y restauración de sistemas remotos.

NDMP no se puede usar para realizar copias de seguridad ni restaurar datos de configuración del sistema. En cambio, use la función de restauración y copia de seguridad de configuración (consulte [“Copia de seguridad de la configuración”](#) en el *Manual de servicio del cliente de Oracle ZFS Storage Appliance*).

Para configurar el NDMP, consulte las siguientes secciones:

- [“Configuraciones locales y remotas de NDMP”](#) [412]
- [“Formatos y tipos de copia de seguridad de NDMP”](#) [413]
- [“Copia de seguridad de NDMP con los tipos "dump" y "tar"”](#) [413]
- [“Copia de seguridad de NDMP con el tipo zfs”](#) [415]
- [“Copias de seguridad incrementales de NDMP”](#) [417]
- [“Copias de seguridad de réplicas”](#) [419]
- [“Propiedades y logs de NDMP”](#) [421]

Configuraciones locales y remotas de NDMP

El dispositivo admite operaciones de copia de seguridad y restauración tanto con configuraciones *locales*, en las que las unidades de cinta están físicamente conectadas al dispositivo, como con configuraciones *remotas*, en las que los datos se transmiten por secuencias a otro sistema de la misma red. En ambos casos, la copia de seguridad debe ser gestionada por una DMA admitida.

En las configuraciones locales, los dispositivos de cinta admitidos, incluidos las unidades y los cambiadores (robots), están conectados físicamente al sistema mediante una tarjeta de canal de fibra (FC) o SCSI admitida configurada en el modo Iniciador. Estos dispositivos se pueden ver en la pantalla Estado de NDMP. El servicio NDMP presenta estos dispositivos a DMA cuando DMA hace búsquedas de dispositivos. Una vez que se configuraron en la DMA, estos dispositivos están disponibles para hacer una copia de seguridad y restauración del dispositivo u otros sistemas en la misma red. Después de agregar unidades o cambiadores de cinta al sistema, o extraerlos del sistema, puede ser necesario reiniciar para que el servicio NDMP reconozca los cambios. Después de eso, posiblemente sea necesario volver a configurar la DMA porque los nombres de los dispositivos de cinta pueden haber cambiado.

En configuraciones remotas, los dispositivos de cinta no están conectados físicamente al sistema cuya copia de seguridad o restauración se está realizando (el servidor de datos), sino

que están conectados al sistema que ejecuta la DMA o un sistema independiente (el servidor de cintas). Estas configuraciones se conocen normalmente como "configuraciones de 3 niveles" porque la DMA controla otros dos sistemas. En estas configuraciones, el flujo de datos se transmite entre el servidor de datos y el servidor de cinta por medio de una red IP.

Formatos y tipos de copia de seguridad de NDMP

El protocolo NDMP no especifica un formato de datos de copia de seguridad. El dispositivo admite tres tipos de copia de seguridad que corresponden a diferentes implementaciones y formatos de cinta. Las DMA pueden usar los siguientes valores de la variable TYPE del entorno de NDMP para seleccionar un tipo de copia de seguridad:

TABLA 80 Formatos y tipos de copia de seguridad de NDMP

Tipo de copia de seguridad	Detalles
dump	Basado en archivos para sistemas de archivos solamente. Admite historial de archivos y recuperación de acceso directo (DAR).
tar	Basado en archivos para sistemas de archivos solamente. Admite historial de archivos y recuperación de acceso directo (DAR).
zfs	Basado en recursos compartidos para sistemas de archivos y volúmenes. No admite historial de archivos ni recuperación de acceso directo (DAR), pero puede ser más rápido para algunos juegos de datos. Solo admitido con NDMPv4.

No hay un formato estándar de flujo de datos de NDMP, de manera que los flujos de copia de seguridad generados en el dispositivo se pueden restaurar solamente en sistemas Oracle ZFS Storage Appliance que ejecutan software compatible. Las versiones futuras del software de dispositivo por lo general pueden restaurar flujos cuya copia de seguridad se generó con versiones anteriores del software, pero no necesariamente a la inversa. Por ejemplo, el tipo de copia de seguridad "zfs" es nuevo en 2010.Q3; por lo tanto, los sistemas que ejecutan 2010.Q1 (o versiones anteriores) no pueden restaurar flujos de copia de seguridad creados con el tipo "zfs" en 2010.Q3.

Copia de seguridad de NDMP con los tipos "dump" y "tar"

Al hacer copias de seguridad con los tipos "dump" y "tar", los administradores usan una ruta del sistema de archivos para especificar los datos que se deben incluir en la copia de seguridad; esta ruta se llama *ruta de copia de seguridad*. Por ejemplo, si el administrador configura la copia

de seguridad de `/export/home`, entonces se hace una copia de seguridad del recurso compartido montado en esa ruta. De manera similar, si se restaura un flujo de copia de seguridad en `/export/code`, aquí se restauran los archivos, aunque al hacer la copia de seguridad se encontraran en otra ruta.

Para hacer copias de seguridad, se pueden especificar solamente rutas que sean puntos de montaje de recursos compartidos existentes o que estén contenidas en recursos compartidos existentes. Si la ruta de la copia de seguridad coincide con el punto de montaje de un recurso compartido, solo ese recurso compartido se incluye en la copia de seguridad. De lo contrario, la ruta debe estar dentro de un recurso compartido, en cuyo caso únicamente la parte de ese recurso compartido se incluye en la copia de seguridad. En ambos casos, los demás recursos compartidos que están montados dentro del recurso compartido especificado bajo la ruta de copia de seguridad no se incluyen en la copia de seguridad; para que se los incluya en la copia de seguridad, se deben especificar por separado.

Instantáneas: si la ruta de copia de seguridad especifica un sistema de archivos activo (por ejemplo, `/export/code`) o una ruta incluida en un sistema de archivos activo (por ejemplo, `/export/code/src`), el dispositivo genera de inmediato una instantánea nueva y, luego, hace una copia de seguridad de la ruta determinada a partir de esa instantánea. Cuando se completa la copia de seguridad, se destruye la instantánea. Si la ruta de acceso de copia de seguridad especifica una instantánea (por ejemplo, `/export/code/.zfs/snapshot/mysnap`), no se genera una instantánea nueva, y el sistema hace la copia de seguridad a partir de la instantánea especificada.

Metadatos de recursos compartidos: para simplificar las operaciones de copia de seguridad y restauración de configuraciones complejas de recursos compartidos, las copias de seguridad "dump" y "tar" incluyen los metadatos de recursos compartidos correspondientes a los proyectos y los recursos compartidos asociados con la ruta de copia de seguridad. Estos metadatos describen la configuración de recursos compartidos en el dispositivo, incluidas las propiedades de uso compartido de protocolos, las propiedades de cuotas y otras propiedades configuradas en la pantalla Recursos compartidos. No se deben confundir con los metadatos del sistema de archivos, como la estructura de directorio y los permisos de archivos, que también se incluyen en las operaciones de copia de seguridad y restauración con NDMP.

Por ejemplo, si hace una copia de seguridad de `/export/proj`, se incluirán en la copia de seguridad los metadatos de todos los recursos compartidos cuyos puntos de montaje comiencen con `/export/proj`, así como los metadatos de recursos compartidos de los proyectos principales. De manera similar, si hace una copia de seguridad de `/export/someshare/somedir` y hay un recurso compartido montado en `/export/someshare`, se incluyen los metadatos de recursos compartidos de ese recurso compartido y su proyecto.

Al realizar una restauración, si el destino de la ruta de restauración no se encuentra en un recurso compartido existente, los proyectos y los recursos compartidos del flujo de la copia de seguridad se vuelven a crear en caso de ser necesario con las propiedades originales como están almacenadas en la copia de seguridad. Por ejemplo, si hace una copia de seguridad de `/export/`

foo, que contiene el proyecto `proj1` y los recursos compartidos `share1` y `share2`, y luego destruye el proyecto y lo restaura a partir de la copia de seguridad, los dos recursos compartidos y el proyecto se vuelven a crear con las propiedades que tienen en la copia de seguridad como parte de la operación de restauración.

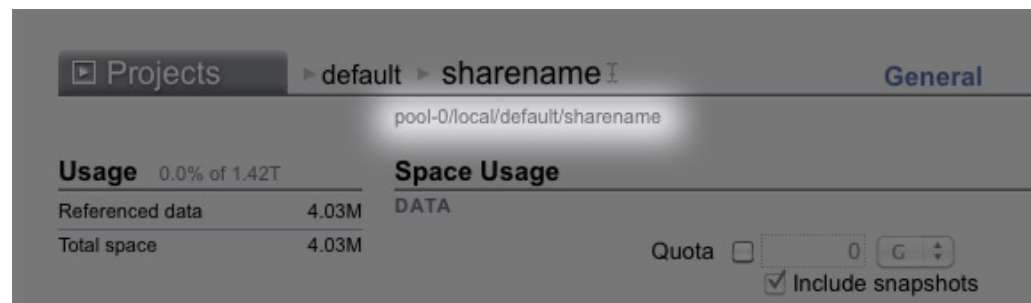
Durante una restauración, si ya existe un proyecto que se hubiese vuelto a crear automáticamente, se usa el proyecto existente en lugar de crearlo automáticamente. Si ya existe un recurso compartido que se hubiese vuelto a crear y si el punto de montaje del recurso coincide con lo que espera el dispositivo en función de la ruta de copia de seguridad original y el destino de la restauración, se usa el recurso compartido existente en lugar de crearlo automáticamente. En todos los demás casos, se crea automáticamente un nuevo recurso compartido a partir de los metadatos incluidos en la copia de seguridad. Si ya existe un recurso compartido que tiene el mismo nombre (pero un punto de montaje diferente), el recurso compartido creado recibirá un nombre único que comience con `ndmp-` y con el punto de montaje correcto.

Se recomienda restaurar un flujo cuyos juegos de datos ya no existan en el dispositivo, lo que permitirá al dispositivo volver a crear los juegos de datos como se especifica en el flujo de la copia de seguridad o crear previamente un recurso compartido de destino para las restauraciones. Cualquiera de estas dos prácticas evita resultados sorpresa relacionados con la creación automática de un recurso compartido como se describió anteriormente.

Copia de seguridad de NDMP con el tipo `zfs`

Al hacer copias de seguridad con el tipo "`zfs`", los administradores utilizan el nombre canónico presente en el dispositivo para especificar los datos que se deben incluir en la copia de seguridad. En la BUI, se encuentra debajo del nombre del recurso compartido:

FIGURA 18 Nombre de recursos compartidos de NDMP



mientras que en la CLI aparece como el valor de la propiedad `canonical_name`. Los nombres canónicos no comienzan con el carácter "/", pero, al configurar la ruta de acceso de copia de seguridad, se les debe agregar este carácter como prefijo.

Se pueden especificar tanto proyectos como recursos compartidos para hacer copias de seguridad del tipo "zfs". Si el nombre canónico se especifica tal cual está, se crea una nueva instantánea y se la utiliza para hacer la copia de seguridad. Se puede usar el sufijo `@snapshot` para especificar una instantánea específica para hacer la copia de seguridad, en cuyo caso no se crea una instantánea nueva y se hace la copia de seguridad de la instantánea especificada. Por ejemplo:

TABLA 81 Copias de seguridad de nombres canónicos y recursos compartidos

Nombre canónico.	Recursos compartidos que se incluyen en la copia de seguridad
<code>pool-0/local/default</code>	Instantánea nueva del proyecto local denominado <code>default</code> y todos sus recursos compartidos.
<code>pool-0/local/default@yesterday</code>	Instantánea denominada <code>yesterday</code> del proyecto local <code>default</code> y todos sus recursos compartidos que tienen la instantánea <code>yesterday</code> .
<code>pool-0/local/default/code</code>	Instantánea nueva de <code>code</code> en el proyecto local <code>default</code> . <code>code</code> puede ser un sistema de archivos o un volumen.
<code>pool-0/local/default/code@yesterday</code>	Instantánea denominada <code>yesterday</code> del recurso compartido <code>code</code> en el proyecto local <code>default</code> . <code>code</code> puede ser un sistema de archivos o un volumen.

Como las copias de seguridad incrementales basadas en niveles con el tipo "zfs" requieren una instantánea de base proveniente de la copia de seguridad incremental anterior, el comportamiento por defecto para las copias de seguridad por niveles para las que se crea una nueva instantánea es conservar la nueva instantánea para que se la pueda utilizar para las copias de seguridad incrementales subsiguientes. Si la DMA indica que la copia de seguridad no se utilizará para las copias de seguridad incrementales subsiguientes (mediante la configuración de `UPDATE=n`), la instantánea recientemente creada se destruye después de hacer la copia de seguridad. Las instantáneas de usuarios existentes nunca se destruyen después de una copia de seguridad. Para obtener información detallada, consulte [“Copias de seguridad incrementales de NDMP” \[417\]](#).

Metadatos de recursos compartidos: los metadatos de recursos compartidos (es decir, la configuración del recurso compartido) siempre se incluyen en las copias de seguridad "zfs". Al restaurar una copia de seguridad completa de tipo "zfs", el proyecto o el recurso compartido de destino no debe existir. Se lo vuelve a crear a partir de los metadatos del flujo de la copia de seguridad. Al restaurar una copia de seguridad incremental de tipo "zfs", el proyecto o el recurso compartido de destino debe existir. Las propiedades correspondientes se actualizan a partir de los metadatos del flujo de la copia de seguridad. Para obtener información detallada, consulte [“Copias de seguridad incrementales de NDMP” \[417\]](#).

Copias de seguridad incrementales de NDMP

El dispositivo admite copias de seguridad incrementales basadas en niveles para todos los tipos de copia de seguridad mencionados. Para especificar un nivel de copia de seguridad, las DMA normalmente especifican las siguientes tres variables de entorno:

Variable	Detalles
LEVEL	Número entero del 0 al 9 que identifica el nivel de la copia de seguridad.
DMP_NAME	Especifica un conjunto de copias de seguridad incrementales en particular. Es posible usar simultáneamente varios conjuntos de copias de seguridad incrementales por niveles especificando diferentes valores para DMP_NAME.
UPDATE	Indica si esta copia de seguridad se puede usar como base para copias de seguridad incrementales subsiguientes.

Por definición, una copia de seguridad de nivel N incluye todos los archivos cambiados desde la copia de seguridad previa del mismo conjunto de copias de seguridad (especificado por "DMP_NAME") del mismo recurso compartido cuyo NIVEL sea menor que N. Las copias de seguridad de nivel 0 siempre incluyen todos los archivos. Si UPDATE (Actualización) tiene el valor "y" (predeterminado), la copia de seguridad actual se registra de manera tal que las copias de seguridad futuras con un nivel mayor que N usen esta copia de seguridad como base. Estas variables normalmente son gestionadas por la DMA, y los administradores no necesitan configurarlas directamente.

A continuación, se presenta un ejemplo de programación de copia de seguridad incremental:

TABLA 82 Modelo de programa de copia de seguridad incremental

Día	Detalles
Primero del mes	Copia de seguridad de nivel 0. La copia de seguridad contiene todos los archivos del recurso compartido.
Cada día 7, 14, 21 del mes	Copia de seguridad de nivel -1. La copia de seguridad contiene todos los archivos cambiados desde la última copia de seguridad completa (mensual).
Cada día	Copia de seguridad de nivel -2. La copia de seguridad contiene todos los archivos cambiados desde la última copia de seguridad de nivel 1.

Para recuperar el estado de un sistema de archivos como se encontraba el día 24 del mes, un administrador normalmente restaura la copia de seguridad de nivel 0 del primero de mes en un

nuevo recurso compartido, después restaura la copia de seguridad de nivel 1 del 21 del mes y después restaura la copia de seguridad de nivel 2 del 24 del mes.

Para implementar copias de seguridad incrementales basadas en niveles, el dispositivo debe llevar un control del historial de copias de seguridad de cada recurso compartido. Para las copias de seguridad "tar" y "dump", el historial de copias de seguridad por niveles se mantiene en los metadatos del recurso compartido. Las copias de seguridad incrementales recorren el sistema de archivos e incluyen los archivos modificados desde el momento de la copia de seguridad del nivel previo. En el momento de la restauración, el sistema simplemente restaura todos los archivos del flujo de la copia de seguridad. En el ejemplo anterior, por lo tanto, sería posible restaurar la copia de seguridad de nivel 2 a partir del día 24 en cualquier sistema de archivos, y los archivos incluidos en el flujo de la copia de seguridad se restaurarían aunque el sistema de archivos de destino no coincidiera con el sistema de archivos a partir del cual se hizo la copia de seguridad de los archivos. Sin embargo, la práctica recomendada sugiere utilizar un procedimiento como el anterior, que comienza con un árbol vacío y restaura las copias de seguridad de los niveles previos para recuperar el estado del sistema de archivos original.

Para implementar copias de seguridad incrementales basadas en niveles para el tipo "zfs" de manera efectiva, el sistema utiliza un enfoque diferente. Las copias de seguridad que son parte de un conjunto incremental no destruyen la instantánea utilizada para la copia de seguridad, sino que la dejan en el sistema. Las copias de seguridad incrementales subsiguientes usan esta instantánea como base para identificar con rapidez los bloques del sistema de archivos que han cambiado y generar el flujo de copia de seguridad. Como consecuencia, no se deben destruir las instantáneas que deja el servicio NDMP después de hacer una copia de seguridad si desea crear copias de seguridad incrementales subsiguientes.

Otra consecuencia importante de este comportamiento es que, para restaurar un flujo incremental, el estado del sistema de archivos debe coincidir exactamente con el estado correspondiente de la instantánea base del flujo incremental. En otras palabras, para restaurar una copia de seguridad de nivel 2, el sistema de archivos debe tener exactamente el mismo aspecto que tenía cuando se completó la copia de seguridad de nivel 1. Tenga en cuenta que el procedimiento anterior, comúnmente utilizado, garantiza que sea así porque al restaurar el flujo de copia de seguridad de nivel 2 a partir de la copia de seguridad del día 24, el sistema está exactamente como estaba cuando se completó la copia de seguridad de nivel 1 del día 21 porque esa copia de seguridad acaba de ser restaurada.

El servicio NDMP genera un error si se intenta restaurar un flujo de copia de seguridad "zfs" incremental en un sistema de archivos cuya instantánea más reciente no coincide con la instantánea de base del flujo incremental o si el sistema de archivos se modificó desde esa instantánea. Puede configurar el servicio NDMP para revertir a la instantánea de base justo antes de comenzar la restauración. Para ello, configure la variable de entorno de NDMP "ZFS_FORCE" con el valor "y" o configure la propiedad "Rollback datasets" (Revertir juegos de datos) del servicio NDMP (consulte ["Propiedades y logs de NDMP" \[421\]](#)).

Copias de seguridad de réplicas

El producto Oracle ZFS Storage Appliance admite la copia de seguridad directa de réplicas e instantáneas de réplicas con el tipo de copia de seguridad "zfs". No es necesario clonar antes un juego de datos de réplica (proyecto o recurso compartido) para hacer la copia de seguridad correspondiente.

Nota - Dado que la copia de seguridad es de una réplica, en la copia de seguridad se incluyen las propiedades del juego de datos de origen en lugar de las del juego de datos de destino.

Activación de la copia de seguridad de réplicas

- Para activar la copia de seguridad de réplicas, aplique la actualización diferida correspondiente. Para obtener más información, consulte [“Deferred Updates” in Oracle ZFS Storage Appliance Customer Service Manual](#).
- Para la copia de seguridad de réplicas se requiere la versión 2011.1.0 o posterior del software en el origen.
- Si la copia de seguridad de una réplica se restaurará en el origen con el juego de datos replicado original, el origen debe ejecutar la versión 2013.1.4 o posterior del software.

Sintaxis de copia de seguridad de réplicas

Para hacer una copia de seguridad de un proyecto o un recurso compartido replicado, introduzca en la DMA el nombre del juego de datos ZFS sin la extensión de la instantánea. `ndmpd` usa el software del dispositivo para determinar cuál es la instantánea más reciente y completa de la réplica para hacer la copia de seguridad. Para especificar un juego de datos de réplica para hacer una copia de seguridad, use la función de copiar y pegar para evitar escribir mal los nombres de los juegos de datos de la réplica, que son largos y pueden incluir un UUID.

Si se incluye una extensión de instantánea generada por el usuario, `ndmpd` hace la copia de seguridad de la instantánea indicada por el usuario. Si se incluye una extensión generada por el sistema (comienza con `.rr`), se produce un error en la copia de seguridad y se genera un mensaje que se registra en la consola de DMA.

Retenciones persistentes de copias de seguridad de réplicas

Las retenciones persistentes se aplican sobre instantáneas incluidas en copias de seguridad cuando las copias de seguridad en cuestión finalizan. Esto es necesario para las copias de seguridad incrementales futuras, que usan las instantáneas actuales como base. Si esto no se

hiciera, el subsistema de replicación podría suprimir las instantáneas de réplicas que ya no necesita. Las retenciones son liberadas por `ndmpd` cuando las instantáneas ya no se necesitan.

Las retenciones persistentes se pueden liberar manualmente. Al suprimir una instantánea de una réplica que tiene una retención, aparece un mensaje para solicitar confirmación que advierte acerca del efecto potencial en las copias de seguridad actuales o futuras de NDMP. Las instantáneas requeridas por el subsistema de replicación no se pueden suprimir.

Si no es necesario hacer copias de seguridad incrementales, configure el parámetro `UPDATE` de DMA con el valor `no` (`UPDATE=n`) para evitar que se apliquen retenciones persistentes. El modo por defecto es `UPDATE=y`. Para obtener más información sobre la variable de entorno de NDMP `UPDATE`, consulte el resumen técnico [NDMP Implementation Guide for the Oracle ZFS Storage Appliance](https://www.oracle.com/storage/technologies/nas-unified-storage-documentation.html) (<https://www.oracle.com/storage/technologies/nas-unified-storage-documentation.html>).

Copias de seguridad incrementales de réplicas

La continuación (el incremento) de una serie de copias de seguridad en una reversión o un corte de replicación no es posible; en cambio, puede iniciar una nueva serie de copias de seguridad. Use una copia de seguridad completa (nivel 0) para la primera copia de seguridad después de que se haya producido un cambio de estado de replicación, por ejemplo, en un nuevo origen después de que se ha realizado una reversión o un corte.

Las extensiones de instantáneas estáticas que no cambian por nivel `NO` se pueden usar para las instantáneas de réplicas generadas por el usuario (instantáneas que no comienzan con `.rr`). Esto evita que se produzcan colisiones de nombres, lo que generaría un error y podría resultar en un error de replicación.

Algunas DMA no admiten las operaciones de copia de seguridad y restauración incrementales de réplicas del tipo `zfs` para cambios de nombre de extensión de instantánea por nivel. Para conservar espacio en el dispositivo y asegurarse de que dichas instantáneas no se preserven para copias de seguridad incrementales futuras, configure `UPDATE=n` en el momento de realizar la copia de seguridad de la réplica. Las instantáneas generadas por el usuario se pueden eliminar manualmente.

Aunque no haya habido cambios en los datos del usuario de un juego de datos restaurado, el cambio de los metadatos puede generar errores en la restauración de réplicas incrementales. Para evitar esto, siempre realice el `rollback` a la instantánea base antes de restaurar réplicas incrementales; para ello, configure el parámetro `ZFS rollback before restore` con el valor `Always`.

En el caso de copias de seguridad de réplicas no incrementales, por ejemplo, de copias de seguridad únicas, defina `UPDATE=n` para que las instantáneas futuras no se guarden ni consuman espacio. Algunas instantáneas de réplicas antiguas preservadas para copias de seguridad incrementales futuras, por ejemplo, las creadas al configurar `UPDATE=y`, pueden ya no ser

necesarias y ocupar espacio de manera innecesaria. Es seguro destruir manualmente estas instantáneas. Las instantáneas requeridas por el subsistema de replicación no se pueden suprimir. Las instantáneas que no se necesitan se pueden suprimir después de confirmar el mensaje de advertencia acerca del efecto posible en copias de seguridad en curso o futuras de NDMP si la instantánea se suprime.

Propiedades y logs de NDMP

La configuración del servicio NDMP tiene las siguientes propiedades y logs:

TABLA 83 Propiedades de NDMP

Propiedad	Descripción
Versión	Versión de NDMP admitida por la DMA.
Puerto TCP (solo v4)	El puerto de conexión por defecto de NDMP es 10000. NDMPv3 usa siempre este puerto. NDMPv4 permite utilizar un puerto diferente de ser necesario.
Omitir cambios de solo metadatos	Indica al sistema que incluya en la copia de seguridad solamente los archivos cuyo contenido haya cambiado y que omita los archivos en los que hayan cambiado solo los metadatos, por ejemplo, permisos o propietarios. Esta opción se aplica solamente a las copias de seguridad "tar" y "dump" incrementales y está desactivada por defecto.
Agrupaciones de restauración de destino	Al hacer una restauración completa con los tipos "tar" o "dump", el sistema vuelve a crear los juegos de datos si todavía no hay un recurso compartido montado en el destino. Como el protocolo NDMP especifica solamente el punto de montaje, el sistema elige una agrupación en donde volver a crear los proyectos y los recursos compartidos. En un sistema que tiene varias agrupaciones, esta propiedad permite especificar una o varias agrupaciones. Solo es necesario especificar varias agrupaciones si el cluster tiene agrupaciones activas en cada nodo principal. Debe asegurarse de que esta lista esté sincronizada con los cambios de configuración de almacenamiento. Si ninguna de las agrupaciones existe o está en línea, el sistema selecciona una agrupación por defecto de manera aleatoria.
Permitir copia de seguridad basada en token	Activa o desactiva el método basado en token para la copia de seguridad ZFS. Esta propiedad está desactivada por defecto.
Revertir ZFS antes de la restauración (solo v4)	Se aplica solamente a las copias de seguridad de tipo "zfs". Determina si, al restaurar una copia de seguridad incremental, el sistema revierte el proyecto y los recursos compartidos de destino con la información de la instantánea usada como base para la restauración incremental. Si se revierten el proyecto y los recursos compartidos, se pierden los cambios realizados a partir

Propiedad	Descripción
	de esa instantánea. Esta configuración normalmente es controlada por la DMA mediante la variable de entorno "ZFS_FORCE", pero esta propiedad se puede usar para anular la configuración de la DMA y revertir siempre estos juegos de datos o nunca revertirlos. Para obtener información detallada, consulte “Copias de seguridad incrementales de NDMP” [417] . Si no se los revierte, la restauración generará un error a menos que ya se hayan revertido manualmente. Esta propiedad debe utilizarse con DMA que no permiten a los administradores configurar variables de entorno personalizadas, como "ZFS_FORCE".
Permitir recuperación de acceso directo	Activa el sistema para localizar archivos por posición en lugar de hacer búsquedas secuenciales durante las operaciones de restauración. Si se activa esta opción, se reduce el tiempo necesario para recuperar una cantidad pequeña de archivos de varias cintas. Debe especificar esta opción al realizar la copia de seguridad para poder recuperar archivos individuales más adelante.
Restaurar rutas absolutas (solo v3)	Especifica que cuando se restaura un archivo, también se restaura la ruta absoluta completa de ese archivo (en lugar de restaurar solamente el archivo). Esta opción está desactivada por defecto.
Creación de recursos compartidos al restaurar	Permite configurar la operación de restauración para crear un nuevo recurso compartido en función del tipo de copia de seguridad: ■ Todos: permite que todos los tipos de copia de seguridad creen recursos compartidos nuevos al restaurar. ■ Tar_Dump: permite que los tipos de copia de seguridad "tar" y "dump" creen recursos compartidos nuevos al restaurar. ■ ZFS: permite que el tipo de copia de seguridad "zfs" cree recursos compartidos nuevos al restaurar. ■ Ninguno: no permite que ningún tipo de copia de seguridad cree recursos compartidos nuevos al restaurar.
Modo de cinta de DMA (para unidades conectadas localmente)	Especifica si la DMA espera una semántica System V o BSD. La opción por defecto es System V, que es la recomendada para la mayoría de las DMA. Esta opción se aplica solo para las unidades de cinta conectadas localmente exportadas mediante NDMP. Consulte la documentación de la DMA para determinar cuál es el modo que espera su DMA. Si se cambia esta opción, solo se modifican los dispositivos que se exportan cuando la DMA busca dispositivos, de manera que tendrá que reconfigurar los dispositivos de cinta en la DMA después de cambiar esta configuración.

Propiedad	Descripción
Nombre de usuario y contraseña de DMA	Se utiliza para autenticar DMA. El sistema usa MD5 para la autenticación de usuarios.

TABLA 84 Logs de NDMP

Log	Descripción
system-ndmpd:default	Log del servicio NDMP.

Configuración de NFS

Sistema de archivos de red (NFS) es un protocolo estándar del sector utilizado para compartir archivos por medio de una red. Oracle ZFS Storage Appliance admite las versiones 2, 3, 4.0 y 4.1 de NFS. Para obtener más información acerca de cómo se construye el espacio de nombres del sistema de archivos, consulte [“Trabajo con espacio de nombres del sistema de archivos” \[544\]](#). Para obtener información acerca de NFS con usuarios locales, consulte [“Configuración de usuarios” \[257\]](#).



Atención - Para evitar la pérdida del servicio NFS, además de la pérdida de datos, no monte sistemas de archivos NFS mediante interfaces privadas.

Para configurar el NFS, consulte las siguientes secciones:

- [“Propiedades del servicio NFS” \[423\]](#)
- [“Configuración de reinos Kerberos para NFS” \[425\]](#)
- [“Logs y análisis de NFS” \[426\]](#)
- [“Propiedades de NFS” \[426\]](#)
- [“Dependencias del servicio de nombres de NFS” \[427\]](#)
- [Uso compartido de un sistema de archivos por medio de NFS \[428\]](#)

Propiedades del servicio NFS

Las siguientes propiedades del servicio NFS están disponibles en Configuración > Servicios. Tenga en cuenta que NFSv4 también se conoce como NFSv4.0.

- **Versión mínima admitida:** Use esta lista desplegable para controlar las versiones de NFS que admite el dispositivo.
- **Versión máxima admitida:** Use esta lista desplegable para controlar las versiones de NFS que admite el dispositivo.

Nota - La configuración de la versión mínima y la versión máxima de NFS con el mismo valor hace que el dispositivo se comuniquen solamente con clientes que usan esa versión. Esto puede resultar útil si se está teniendo algún problema con una de las versiones de NFS (por ejemplo, las características de rendimiento de una versión de NFS con la carga de trabajo) y desea forzar a los clientes a usar solo la versión que funciona mejor.

- **Número máximo de threads de servidor:** Define la cantidad máxima de solicitudes simultáneas de NFS (de 20 a 3000). Debe cubrir al menos la cantidad de clientes NFS simultáneos que anticipa tener. El valor por defecto es 1500.
- **Período de gracia:** Define la cantidad de segundos que tienen todos los clientes para recuperar el estado de bloqueo después del reinicio de un dispositivo (de 15 a 600 segundos) a partir de una interrupción no planificada. Esta propiedad afecta solo a clientes NFSv4.0 y NFSv4.1 (NFSv3 no tiene estado, por lo que no hay ningún estado que reclamar). Durante este período, el servicio NFS procesa solamente reclamos del estado de bloqueo antiguos. No se procesa ninguna otra solicitud de servicio hasta que finaliza el período de gracia. El período de gracia predeterminado es de 90 segundos. Al reducir el período de gracia, los clientes NFS pueden reanudar la operación con mayor rapidez después de un reinicio de servidor, pero también aumenta la probabilidad de que un cliente no pueda recuperar todo el estado de bloqueo. Oracle ZFS Storage Appliance ofrece una recuperación del estado de bloqueo sin período de gracia para clientes NFSv4.0 y NFSv4.1 durante interrupciones planificadas. Las interrupciones planificadas se producen durante eventos como las actualizaciones o el reinicio del dispositivo con el comando `maintenance system reboot` de la CLI o el ícono de encendido  de la BUI. Para las interrupciones planificadas, el servicio NFS procesa todas las solicitudes de servicio sin que se produzcan demoras en el período de gracia.
- **Dominio de identidades NFSv4 personalizado:** use esta propiedad para definir el dominio para asignar identidades de usuarios y grupos de NFSv4.0 y NFSv4.1. Si no configura esta propiedad, los dispositivos utilizan DNS para obtener el dominio de identidades: primero buscan un registro de recursos DNS `_nfsv4idmapdomain` y, a continuación, regresan al dominio DNS en sí.
- **Usar cadenas de ID numéricas de NFSv4:** use esta propiedad para permitir que los clientes NFSv4.0 y NFSv4.1 usen cadenas numéricas para los ID de usuarios y grupos. Si no configura esta propiedad, los ID de usuarios y grupos se intercambian en la forma de `usuario@dominio`, que es el valor por defecto. Esta propiedad es aplicable solo si el tipo de autenticación es `AUTH_SYS`. La propiedad de la CLI es `use_numeric_ids`.
- **Activar delegación NFSv4:** seleccione esta propiedad para permitir a los clientes almacenar localmente archivos en la caché y hacer modificaciones sin contactar al servidor. Esta opción está activada de forma predeterminada y, generalmente, mejora el rendimiento, pero en raras circunstancias puede causar problemas. Debe desactivar este parámetro solamente después de realizar mediciones detalladas del rendimiento de su carga de trabajo

particular y después de validar que la configuración tiene un beneficio de rendimiento mensurable. Esta opción solo afecta a montajes NFSv4.0 y NFSv4.1.

- **Visibilidad de montaje:** esta propiedad permite limitar la disponibilidad de información acerca de las listas de acceso de recursos compartidos y los montajes remotos proveniente de los clientes NFS. La opción Full permite acceso total. La opción Restricted restringe el acceso de manera que los clientes puedan ver solo los recursos compartidos a los que tienen permitido el acceso. Los clientes no pueden ver las listas de acceso de los recursos compartidos definidas en el servidor ni puntos de montaje remoto con respecto al servidor generadas por otros clientes. De forma predeterminada, la propiedad está configurada con el valor Full (Total).
- **Oracle Intelligent Storage Protocol** (Protocolo de almacenamiento inteligente de Oracle): los servicios de NFSv4.0 y NFSv4.1 incluyen compatibilidad con el protocolo de almacenamiento inteligente de Oracle, que permite que los clientes NFSv4.0 y NFSv4.1 de Oracle Database transmitan información de optimización al servidor NFSv4.0 y NFSv4.1 de Oracle ZFS Storage Appliance. Para obtener más información, consulte [“Configuración de Oracle ZFS Storage Appliance para clientes de Oracle Database” \[869\]](#).

Temas relacionados

- [“Propiedades de NFS” \[426\]](#)
- Configuración de las propiedades de servicio [BUI](#), [CLI](#).

Configuración de reinos Kerberos para NFS

La configuración de un reino Kerberos crea ciertos principales de servicio y agrega las claves necesarias al keytab local del sistema. Se debe configurar el NTP service antes de configurar NFS con Kerberos. Los siguientes principales de servicio se crean y se actualizan para permitir el uso de NFS con Kerberos:

```
host/node1.example.com@EXAMPLE.COM
nfs/node1.example.com@EXAMPLE.COM
```

Si los dispositivos están agrupados en clusters, los principales y las claves se generan para cada nodo de cluster:

```
host/node1.example.com@EXAMPLE.COM
nfs/node1.example.com@EXAMPLE.COM
host/node2.example.com@EXAMPLE.COM
nfs/node2.example.com@EXAMPLE.COM
```

Si ya se crearon los principales, la configuración del dominio Kerberos restablece la contraseña de cada uno de ellos.

Para obtener información sobre cómo configurar KDC y clientes protegido por Kerberos, consulte la <https://docs.oracle.com/en/operating-systems/solaris.html>. Para obtener información acerca del servicio Kerberos del dispositivo, consulte [“Configuración de Kerberos” \[377\]](#). Después de configurar Kerberos, cambie el modo de seguridad en la

pantalla Recursos compartidos ->; Sistema de archivos ->; Protocolos a un modo que use Kerberos.

Nota - Los clientes NFS con Kerberos deben acceder al dispositivo mediante una dirección IP que se convierta en un FQDN para esos principales. Por ejemplo, si un dispositivo está configurado con varias direcciones IP, los clientes NFS con Kerberos únicamente pueden usar la dirección IP que se convierte en el FQDN del dispositivo.

Logs y análisis de NFS

Estos registros están disponibles para el servicio NFS:

TABLA 85 Logs disponibles para NFS

Log	Descripción
network-nfs-server:default	Log de servidor NFS maestro
appliance-kit-nfsconf:default	Log de eventos de configuración de NFS del dispositivo
network-nfs-cbd:default	Log del daemon de devolución de llamadas de NFSv4.0 y NFSv4.1
network-nfs-mapid:default	Log del daemon mapid de NFSv4.0 y NFSv4.1, que asigna credenciales de usuarios y grupos de NFSv4.0 y NFSv4.1
network-nfs-status:default	Log del daemon statd de NFS, que ayuda a las funciones de bloqueo y recuperación para bloqueos de NFS
network-nfs-nlockmgr:default	Log del daemon lockd de NFS, que posibilita operaciones de bloqueo de registros para archivos

Puede supervisar la actividad NFS en la sección Análisis. Esto incluye:

- Operaciones de NFS por segundo
- ... por tipo de operación (lectura/escritura/...)
- ... por nombre de recurso compartido
- ... por nombre de host de cliente
- ... por nombre de archivo que se accede
- ... por latencia de acceso

Propiedades de NFS

En la siguiente tabla, se describe la asignación entre las propiedades de la CLI y las descripciones de propiedades de la BUI antes mencionadas.



Atención - Para evitar la pérdida del servicio NFS, además de la pérdida de datos, no monte sistemas de archivos NFS mediante interfaces privadas.

TABLA 86 Propiedades de NFS

Propiedad de la CLI	Propiedad de la BUI
version_min	Versión mínima admitida
version_max	Versión máxima admitida
nfsd_servers	Cantidad máxima de subprocesos de servidor
grace_period	Período de gracia
mapid_domain	Dominio de identidades personalizado de NFSv4 y NFSv4.1
use_numeric_ids	Uso de ID de cadena numérica en NFSv4 y NFSv4.1
enable_delegation	Activación de delegación en NFSv4 y NFSv4.1
mount_visibility	Nivel de restricción de información de recursos compartidos de clientes

Dependencias del servicio de nombres de NFS

El dispositivo usa servicios de nombres, como DNS, NIS y LDAP, para solucionar los nombres de host y las direcciones IP correspondientes, las identidades de usuario y las estadísticas de análisis. En este tema, se describen las dependencias del servicio de nombres de NFS y los problemas que se generan si no se configuran servicios de nombres para el dispositivo.

NFS depende de la información de cada uno de los siguientes servicios de nombres:

TABLA 87 Dependencias del servicio de nombres de NFS

Descripción	Servicio
Dirección IP y nombre de host correspondiente de los clientes y servidores de NFS	DNS
Número de identidad de usuario y nombre de usuario correspondiente	NIS/LDAP
Número de identidad de grupo y nombre de grupo correspondiente	NIS/LDAP
Clientes pertenecientes a grupos de red	NIS/LDAP

Si el dispositivo no puede acceder a ninguno de los servidores de red DNS o las asignaciones de DNS no están completas, se pueden producir los siguientes problemas:

- Fallo de montaje del sistema de archivos

- Una vez que el sistema de archivos se montó correctamente, se deniega el acceso del cliente a recursos compartidos de NFS.
- El cliente recibe errores de "autenticación débil"
- El servidor NFS no responde
- Fallos en la búsqueda de grupos y usuarios, usando NFSv3 o NFSv4, como se muestra en la siguiente tabla.

Versión de NFS	Problema	Configuración
NFSv3 o NFSv4	No se puede acceder a archivos y directorios cuando el usuario es miembro de 16 grupos o más.	
NFSv4	No se puede recuperar la información de propiedad (los usuarios y grupos pueden mostrarse como nobody).	Establezca la opción "Usar cadenas de ID numéricas de NFSv4".
NFSv4	No se puede cambiar la propiedad de los archivos.	En el cliente, establezca el equivalente de la opción "Usar cadenas de ID numéricas de NFSv4".
NFSv4	No se puede recuperar la información de ACL.	Establezca la opción "Usar cadenas de ID numéricas de NFSv4".
NFSv4	No se pueden cambiar los ACL, incluida la incapacidad de cambiar las entradas no relacionadas con las entradas afectadas.	Establezca la opción "Usar cadenas de ID numéricas de NFSv4". En el cliente, establezca el equivalente de la opción "Usar cadenas de ID numéricas de NFSv4".

Temas relacionados

- [“Configuración de DNS” \[341\]](#)
- [“Operación sin DNS” \[351\]](#)

▼ Uso compartido de un sistema de archivos por medio de NFS

1. **Vaya a Configuración > Servicios.**
2. **Compruebe que el servicio NFS esté activado y en línea. De no ser así, actívelo.**



Atención - Para evitar la pérdida del servicio NFS, además de la pérdida de datos, no monte sistemas de archivos NFS mediante interfaces privadas.

3. **Vaya a la pantalla Recursos compartidos y edite un recurso compartido existente o cree uno nuevo.**
4. **Haga clic en la ficha Protocolos del recurso compartido que está editando y compruebe que esté activado el uso compartido por medio de NFS.**
En esta pantalla, también puede configurar el modo de uso compartido de NFS (lectura/lectura + escritura).

Configuración de NIS

El servicio de información de red (NIS) es un servicio de nombres para la gestión centralizada. El dispositivo puede actuar como un cliente NIS para usuarios y grupos, con las siguientes características:

- Los usuarios de NIS pueden iniciar sesión en los servicios de FTP y HTTP.
- Los usuarios de NIS puedan recibir privilegios para la administración del dispositivo. El dispositivo complementa la información de NIS con su propia configuración de privilegios.

Para configurar el NIS, consulte las siguientes secciones:

- [“Propiedades y logs de NIS” \[429\]](#)
- [“Agregación de un usuario de NIS al dispositivo” \[430\]](#)

Propiedades y logs de NIS

TABLA 88 Propiedades de NIS

Propiedad de la BUI	Propiedad de la CLI	Descripción
Dominio	domain	El dominio de NIS que se utiliza.
Servidores: buscar mediante difusión	broadcast	Envíe una difusión de NIS a fin de localizar servidores NIS para ese dominio específico.
Servidores: usar servidores de la lista	ypservers	Especifique una lista de nombres de host o direcciones IP de los servidores NIS.

El dispositivo se conecta con el primer servidor NIS de la lista o con un servidor encontrado mediante difusión, y pasa al siguiente si el servidor actual deja de responder.

TABLA 89 Logs de NIS

Log	Descripción
network-nis-client:default	Log del servicio de clientes NIS.

Log	Descripción
appliance-kit-nsswitch:default	Log del servicio de nombres del dispositivo, por medio del cual se hacen las consultas de NIS.
system-identity:domain	Log del configurador de nombre de dominio del dispositivo.

Temas relacionados

- [“Agregación de un usuario de NIS al dispositivo” \[430\]](#)

Agregación de un usuario de NIS al dispositivo

Después de completar la configuración de NIS, puede configurar que los usuarios de NIS existentes puedan iniciar sesión en el dispositivo mediante su nombre de host y contraseña de NIS.

Nota - El ID de usuario de NIS existente no puede ser menor que 100 ni mayor que 2147483646; tampoco puede ser igual que 60001, 60002 o 65534. Los UID de 0 a 99 inclusive están reservados por el proveedor del sistema operativo para uso en aplicaciones futuras. Los usuarios finales del sistema y los proveedores de productos en capas no pueden utilizarlos ya que, si lo hicieran, se podrían producir problemas de seguridad con otras aplicaciones.

En la BUI, siga el procedimiento [Agregación de un administrador o usuario \(BUI\) \[258\]](#) utilizando los siguientes valores de propiedades:

1. Seleccione Directorio en el menú desplegable Tipo.
2. En Nombre de usuario, especifique el nombre de usuario de NIS existente del usuario.

En la CLI, siga el procedimiento [Agregación de un administrador o usuario \(CLI\) \[260\]](#) mediante el tipo de usuario `directory` y el nombre de usuario de NIS existente del usuario.

```
hostname:configuration users> directory NISusername
```

Los campos ID de usuario (`uid`) y Contraseña (`initial_password`) se configuran automáticamente: se usan valores de NIS.

Configuración de NTP

El servicio de protocolo de tiempo de red (NTP) se puede usar para mantener la precisión del reloj del dispositivo. Es importante para mantener registros de hora exactos en el sistema de

archivos y para la autenticación de protocolos. El dispositivo registra la hora con la zona horaria UTC. Las horas que aparecen en la BUI usan el desplazamiento de zona horaria del explorador.

A la derecha de la pantalla de la BUI, aparece la hora del dispositivo (hora del servidor) y el explorador (hora del cliente). Si el servicio NTP no está en línea, se puede hacer clic en el botón SYNC (Sincronizar) para hacer que la hora del dispositivo coincida con la hora del explorador del cliente.

Si comparte sistemas de archivos con SMB, los relojes de los clientes deben estar sincronizados con una diferencia de cinco minutos como máximo con respecto al reloj del dispositivo para evitar errores de autenticación de usuarios. Una manera de garantizar la sincronización del reloj es configurar el dispositivo y los clientes SMB para usar el mismo servidor NTP.

TABLA 90 Sincronización del reloj de NTP

Log	Descripción
network-ntp:default	Log del servicio NTP.

Para configurar el NTP, consulte las siguientes secciones:

- [Configuración de la sincronización del reloj \(BUI\) \[431\]](#)
- [Configuración de NTP \(CLI\) \[431\]](#)
- [“Propiedades de NTP” \[433\]](#)

▼ Configuración de la sincronización del reloj (BUI)

Esta tarea permite configurar la hora del dispositivo para que coincida con la hora del explorador.

1. **Vaya a Configuration (Configuración) > Services (Servicios) > NTP.**
2. **Desactive el servicio NTP.**
3. **Haga clic en SYNC (Sincronizar).**

▼ Configuración de NTP (CLI)

1. **En `configuration services ntp`, edite las autorizaciones con el comando `authkey`:**

```
hostname:configuration services ntp> authkey
hostname:configuration services ntp authkey>
```

2. Desde este contexto, se pueden agregar nuevas claves con el comando `create`:

```
hostname:configuration services ntp authkey> create
hostname:configuration services ntp authkey-000 (uncommitted)> get
    keyno = (unset)
    type = (unset)
    key = (unset)
hostname:configuration services ntp authkey-000 (uncommitted)> set keyno=1
    keyno = 1 (uncommitted)
hostname:configuration services ntp authkey-000 (uncommitted)> set type=A
    type = A (uncommitted)
hostname:configuration services ntp authkey-000 (uncommitted)> set key=coconuts
    key = (set) (uncommitted)
hostname:configuration services ntp authkey-000 (uncommitted)> commit
hostname:configuration services ntp authkey>
```

3. Para asociar claves de autenticación con servidores mediante la CLI, la propiedad `serverkeys` se debe configurar con una lista de valores en la que cada valor es una clave que se asociará con el servidor correspondiente en la propiedad `servers`.

Si un servidor no usa ninguna autenticación, la clave de servidor correspondiente se debe configurar con el valor 0. Por ejemplo, haga lo siguiente para usar la clave creada más arriba con el fin de autenticar los servidores "server1" y "server2":

```
hostname:configuration services ntp> set servers=server1,server2
    servers = server1,server2 (uncommitted)
hostname:configuration services ntp> set serverkeys=1,1
    serverkeys = 1,1 (uncommitted)
hostname:configuration services ntp> commit
hostname:configuration services ntp>
```

4. Para asociar claves de autenticación con servidores, configure la propiedad `serverkeys` con una lista de valores en la que cada valor sea una clave que se asociará con el servidor correspondiente en la propiedad `servers`.

Si un servidor no usa ninguna autenticación, la clave de servidor correspondiente se debe configurar con el valor 0. Por ejemplo, para usar la clave creada más arriba a fin de autenticar los servidores "server1" y "server2":

```
hostname:configuration services ntp> set servers=server1,server2
    servers = server1,server2 (uncommitted)
hostname:configuration services ntp> set serverkeys=1,1
    serverkeys = 1,1 (uncommitted)
hostname:configuration services ntp> commit
hostname:configuration services ntp>
```

5. Para autenticar el servidor "server1" con la clave 1, el servidor "server2" con la clave 2 y el servidor "server3" con la clave 3:

```
hostname:configuration services ntp> set servers=server1,server2,server3
    servers = server1,server2,server3 (uncommitted)
hostname:configuration services ntp> set serverkeys=1,2,3
    serverkeys = 1,2,3 (uncommitted)
hostname:configuration services ntp> commit
hostname:configuration services ntp>
```

6. Para autenticar los servidores "server1" y "server2" con la clave 1 y tener, además, un servidor NTP no autenticado "server3":

```
hostname:configuration services ntp> set servers=server1,server2,server3
      servers = server1,server2,server3 (uncommitted)
hostname:configuration services ntp> set serverkeys=1,1,0
      serverkeys = 1,1,0 (uncommitted)
hostname:configuration services ntp> commit
hostname:configuration services ntp>
```

Propiedades de NTP

Las siguientes propiedades de NTP están disponibles en Configuration (Configuración) > Services (Servicios) > NTP:

TABLA 91 Propiedades de NTP

Propiedad	Descripción	Ejemplos
Detectar servidor NTP mediante direcciones de multidifusión	Escriba una dirección de multidifusión para localizar automáticamente un servidor NTP.	224.0.1.1
Especificar servidores NTP de manera manual	Escriba uno o varios servidores NTP (y las claves de autenticación correspondientes, si las hay) para que el dispositivo establezca contacto directamente.	0.pool.ntp.org
Claves de autenticación NTP	Escriba una o varias claves de autenticación de NTP para que use el dispositivo al autenticar la validez de los servidores NTP. Consulte Tabla 92, “Claves privadas y números enteros de NTP” .	Clave de autenticación: 10, tipo: ASCII, clave privada: SUN7000

Validación: si se proporciona una configuración no válida, aparece una advertencia y no se confirma la configuración. Esto sucede si:

- Se usa una dirección de multidifusión, pero no se encuentra una respuesta de NTP.
- Se usa una dirección de un servidor NTP, pero ese servidor no responde correctamente a NTP.

Autenticación: para prevenir ataques de suplantación de identidad de NTP provenientes de servidores no autorizados, NTP tiene un esquema de cifrado de claves privadas mediante el cual los servidores NTP se asocian con una clave privada que es utilizada por el cliente para verificar la identidad del servidor. Estas claves no se usan para cifrar tráfico ni para autenticar el cliente; solo las utiliza el cliente NTP (es decir, el dispositivo) para autenticar el servidor NTP. Para asociar una clave privada con un servidor NTP, se debe especificar primero la clave privada.

Cada clave privada tiene un número entero exclusivo asociado a ella, junto con un tipo y una clave. El tipo debe ser uno de los siguientes:

TABLA 92 Claves privadas y números enteros de NTP

Tipo	Descripción	Ejemplo
DES	Número hexadecimal de 64 bits en formato DES.	0101010101010101
NTP	Número hexadecimal de 64 bits en formato NTP.	8080808080808080
ASCII	Cadena ASCII de 1 a 8 caracteres.	topsecret
MD5	Cadena ASCII de 1 a 8 caracteres que usa el esquema de autenticación MD5.	md5secret

Después de haber especificado las claves, se puede asociar el servidor NTP con una clave privada en particular. Para una clave dada, los valores de número de clave, tipo de clave y clave privada del cliente y el servidor deben coincidir para que se autentique el servidor NTP.

Configuración de la asistencia técnica remota

La pantalla del servicio de asistencia técnica remota se usa para gestionar el registro del dispositivo y el servicio de asistencia técnica remota.

La operación de registro conecta el dispositivo con [Oracle Auto Service Request \(https://www.oracle.com/support/premier/auto-service-request.html\)](https://www.oracle.com/support/premier/auto-service-request.html). La función ASR de Oracle abre automáticamente las solicitudes de servicio (SR) de problemas específicos informados por el dispositivo. La operación de registro también conecta el dispositivo con My Oracle Support para detectar notificaciones de actualización.

El servicio de asistencia técnica remota se comunica con el servicio de asistencia técnica de Oracle para proporcionar lo siguiente:

- **Informe de fallos:** el sistema informa los problemas activos a Oracle para generar una respuesta de servicio automatizada. En función de la naturaleza del fallo, se puede abrir un caso de asistencia técnica. Los detalles de estos eventos se pueden ver en la pantalla Problema activo. Para obtener más información, consulte [“Cómo trabajar con los problemas” en el Manual de servicio del cliente de Oracle ZFS Storage Appliance](#).
- **Latidos:** se envían mensajes diarios de latidos a Oracle para indicar que el sistema esté en funcionamiento. El servicio de asistencia técnica de Oracle puede notificar al contacto técnico de una cuenta cuando uno de los sistemas activados tarda mucho en enviar un latido.

- **Configuración del sistema:** se envían mensajes periódicos a Oracle en los que se describen la configuración y las versiones actuales de software y hardware, y la configuración del almacenamiento. En estos mensajes, no se transmiten metadatos ni datos de usuario.
- **Paquetes de asistencia:** para poder cargar paquetes de asistencia en el servicio de asistencia técnica de Oracle, primero se debe haber activado el servicio de asistencia técnica remota. Para obtener más información, consulte “[Cómo trabajar con paquetes de soporte](#)” en el *Manual de servicio del cliente de Oracle ZFS Storage Appliance*.
- **Notificaciones de actualización:** se crea una alerta cuando hay actualizaciones de software disponibles en My Oracle Support (MOS). Para obtener más información, consulte “[Cómo trabajar con notificaciones y actualizaciones de software](#)” en el *Manual de servicio del cliente de Oracle ZFS Storage Appliance*.

Debe registrarse para usar el servicio de asistencia técnica remota.

Para poder usar las funciones de informe de fallos y latidos del servicio de asistencia técnica remota, debe tener un nombre de usuario y una contraseña válidos para una cuenta de inicio de sesión único de Oracle. Vaya a [My Oracle Support \(http://support.oracle.com\)](http://support.oracle.com) y haga clic en Registrarse para crear su cuenta.

Para configurar la asistencia técnica remota, consulte las siguientes secciones:

- Registro del dispositivo [BUI](#), [CLI](#)
- [Cambio de la información de la cuenta \(BUI\) \[436\]](#)
- [“Propiedades de la asistencia técnica remota” \[437\]](#)

▼ Registro del dispositivo (BUI)

1. **Vaya a Configuration (Configuración) > Services (Servicios) > Phone Home (Asistencia técnica remota).**
2. **Escriba el nombre de usuario y la contraseña de la cuenta de inicio de sesión único de Oracle.**
Haga clic en Privacy Statement (Declaración de privacidad) para obtener información sobre la política de privacidad. Se puede visualizar en cualquier momento tanto en la BUI como en la CLI.
3. **Haga clic en APPLY (Aplicar) para confirmar los cambios.**
4. **Use [My Oracle Support \(http://support.oracle.com/\)](http://support.oracle.com/) para completar la activación de Auto Service Request (ASR) (<https://www.oracle.com/support/premier/auto-service-request.html>).**

Consulte "Cómo gestionar y aprobar activos pendientes de ASR en My Oracle Support" (ID de documento 1329200.1).

▼ Registro del dispositivo (CLI)

1. **Vaya a `configuration services scrk`.**
2. **Configure `soa_id` y `soa_password` con el nombre de usuario y la contraseña de su cuenta de inicio de sesión único de Oracle, respectivamente.**
3. **Confirme los cambios.**
4. **Use [My Oracle Support \(http://support.oracle.com/\)](http://support.oracle.com/) para completar la activación de [Auto Service Request \(ASR\) \(https://www.oracle.com/support/premier/auto-service-request.html\)](https://www.oracle.com/support/premier/auto-service-request.html).**

Consulte "Cómo gestionar y aprobar activos pendientes de ASR en My Oracle Support" (ID de documento 1329200.1).

ejemplo 4 Registro mediante CLI

```
hostname:> configuration services scrk
hostname:configuration services scrk>set soa_id=myuser
soa_id = myuser(uncommitted)
hostname:configuration services scrk> set soa_password=mypass
soa_password = (set) (uncommitted)
hostname:configuration services scrk> commit
```

▼ Cambio de la información de la cuenta (BUI)

1. **Vaya a `Configuration (Configuración) > Services (Servicios) > Phone Home (Asistencia técnica remota)`.**
2. **Haga clic en "Cambiar cuenta..." para cambiar la cuenta de inicio de sesión único de Oracle que utiliza el dispositivo.**
3. **Confirme los cambios.**
4. **Use [My Oracle Support](http://support.oracle.com/) para completar la activación de [Auto Service Request \(ASR\)](https://www.oracle.com/support/premier/auto-service-request.html).**

Consulte "Cómo gestionar y aprobar activos pendientes de ASR en My Oracle Support" (ID de documento 1329200.1).

Propiedades de la asistencia técnica remota

Si el dispositivo no está conectado directamente a Internet, tal vez deba configurar un proxy HTTP mediante el cual el servicio de asistencia técnica remota pueda comunicarse con Oracle. Esta configuración de proxy se usará también para cargar paquetes de asistencia. Para obtener más detalles sobre paquetes de soporte, consulte [“Cómo trabajar con paquetes de soporte” en el Manual de servicio del cliente de Oracle ZFS Storage Appliance](#).

TABLA 93 Configuración del proxy web del servicio de asistencia técnica remota

Propiedad	Descripción
Use proxy web	Conexión mediante un proxy web.
Host: puerto	Nombre de host o dirección IP del proxy web, y puerto.
Nombre de usuario	Nombre de usuario del proxy web.
Password (Contraseña)	Contraseña del proxy web.

TABLA 94 Estado del servicio de asistencia técnica remota

Propiedad	Descripción
Last heartbeat sent at (Hora de último latido enviado)	Hora a la que se envió el último latido al servicio de asistencia técnica de Oracle.

Si el servicio de asistencia técnica remota se activa antes de haber proporcionado una cuenta de inicio de sesión único de Oracle válida, aparecerá en el estado de mantenimiento. Debe proporcionar una cuenta de inicio de sesión único de Oracle válida para poder usar el servicio de asistencia técnica remota.

En Mantenimiento > Logs > Asistencia técnica remota, hay un log de eventos del servicio de asistencia técnica remota.

Configuración de la API de RESTful

La API de RESTful de Oracle ZFS Storage Appliance permite gestionar el dispositivo mediante solicitudes simples, por ejemplo, GET, PUT, POST y DELETE HTTP combinadas con las direcciones URL de los recursos gestionados.

La arquitectura basada en RESTful del dispositivo está definida como un modelo cliente-servidor por capas. Una de las ventajas de este modelo es que los servicios se pueden redireccionar de manera transparente a través de concentradores, enrutadores y otros sistemas de red estándar sin necesidad de configuración de los clientes. Esta arquitectura admite el

almacenamiento de información en caché y es útil cuando muchos clientes solicitan los mismos recursos estáticos.

Para consultar la documentación completa de la API de RESTful del dispositivo Oracle ZFS Storage Appliance, consulte la [Guía de la API de RESTful del dispositivo Oracle ZFS Storage Appliance](#).

Configuración de etiquetas de servicio

Las etiquetas de servicio se usan para facilitar el inventario de productos y la asistencia técnica. Estas etiquetas permiten que se hagan consultas de datos al dispositivo, por ejemplo:

- Número de serie del sistema
- Tipo de sistema
- Números de versión de software

Puede registrar las etiquetas de servicio con el servicio de asistencia técnica de Oracle, lo que le permite llevar un control de sus equipos Oracle con facilidad, además de acelerar las llamadas de servicio. Las etiquetas de servicio están activadas de forma predeterminada.

TABLA 95 Propiedades de puertos UDP/TCP

Propiedad	Descripción
Discovery Port (Puerto de detección)	Puerto UDP usado para la detección de etiquetas de servicio. El valor predeterminado es 6481.
Listener Port (Puerto de listener)	Puerto TCP usado para hacer consultas de datos de etiquetas de servicio. El valor predeterminado es 6481.

Configuración de SFTP

El servicio SFTP (protocolo de transferencia de archivos SSH) permite tener acceso al sistema de archivos desde clientes SFTP. No se permite el inicio de sesión anónimo; los usuarios deben autenticarse con el servicio de nombres que está configurado en Servicios.

El SFTP se puede usar en combinación con la autenticación Kerberos. Para obtener información acerca del servicio Kerberos del dispositivo, consulte [“Configuración de Kerberos” \[377\]](#).

Para una mayor seguridad al configurar SFTP, puede especificar los cifrados y MAC, como se describe en [“Propiedades, puertos y logs de SFTP” \[441\]](#).

Para configurar el SFTP, consulte las siguientes secciones:

- [Agregación de acceso SFTP a un recurso compartido \(BUI\) \[439\]](#)
- [Configuración de SFTP para acceso remoto \(CLI\) \[439\]](#)
- [“Propiedades, puertos y logs de SFTP” \[441\]](#)

▼ Agregación de acceso SFTP a un recurso compartido (BUI)

1. Vaya a **Configuration (Configuración) > Services (Servicios)**.
2. Compruebe que el servicio SFTP esté activado y en línea. De no ser así, actívelo.
3. Vaya a **Shares (Recursos compartidos) > Shares (Recursos compartidos)** y seleccione o agregue un recurso compartido.
4. Vaya al separador **Protocolos (Protocolos)** y compruebe que el acceso SFTP esté activado.
5. (Opcional) Configure el acceso de modo de recurso compartido en solo lectura o lectura/escritura.

Temas relacionados

- [Configuración de SFTP para acceso remoto \(CLI\) \[439\]](#)
- [“Propiedades, puertos y logs de SFTP” \[441\]](#)

▼ Configuración de SFTP para acceso remoto (CLI)

1. Cree un usuario local o un usuario de red (LDAP o NIS) con el rol de administrador apropiado. (Consulte [“Configuración de usuarios” \[257\]](#)).
2. Use el comando `ssh-keygen -t dsa` en el host o el cliente de Oracle Solaris para generar una clave de autenticación SSH.
3. Introduzca un nombre de archivo en donde almacenar la clave.
4. Si es necesario, introduzca una frase de contraseña o deje este campo en blanco para iniciar sesión directamente en el recurso compartido de SFTP.

Se muestra la ubicación de la clave. La clave presenta un aspecto similar al siguiente:

```
ssh-dss AAAAB3NzaC1kc3MAAACBAPMms5h8UWk1NPf/VJDDEo00AwT+s6iZxkCmmrgAmLFTX9izWk+
bsvNld01XN/6EgkusLjo/+UaEt5+704vMHC1Raq3A1VHLS5tVjeX3iCs+fDo0qwXZg3Brh8QBAawk3
ywr2osuII1tHh4v/HwEAHZq5mVWxav0p03bgmx10/+VAAAFQDIJxnm52DfyEdQQMTY+jRVvzGwMQA
AAIAhTP6Ey+2gGFICKkvUofsc04d8pbqH8duE9P6Y88s0+opuj52GkAdRut2fRrdM9Cf3h41IOc8Bw9
```

```
bZIBzrCKBNWBudZG56tsfLdi1w6vS6gxKrmL2v7fSp9wYPsxZGh0LfU29zw4n2WVcVHbGyFEoVe+taq
aq+AYJaWoHnjZL1/LpQAAAIAlc8+uc3hD0cK3pAkYdg8b2rYIG0AZU4py0rq24D6PeVHd5h5jbe4p
WDM70uYqGCOPYi0KeEoMnJpczRX5qjI+BfoUY4sH24WwWsKkT8XX9PUAa0WT+7axEqg2N6Ye1aTJ95J
vMaj6E7HkAIra2Sj2H/LSDktL42UL+j1Wx5A==username sunray
```

5. **Vaya a Configuración ->Servicios > SFTP. En Claves, haga clic en el signo más (+).**
6. **En la ventana Nueva clave, seleccione DSA.**
7. **Copie solo la porción de la clave (en el ejemplo anterior, comienza con AAAA y termina con Wx5A==) y péguela en el campo Clave.**

Nota - La clave no debe incluir espacios en blanco.

8. **Introduzca el nombre de usuario y agregue un comentario como recordatorio.**
9. **Vaya a Shares (Recursos compartidos) > Shares (Recursos compartidos) y haga clic en el ícono de agregación de elemento  para crear un sistema de archivos.**
10. **En la ventana Create Filesystem (Crear sistema de archivos), introduzca el nombre del sistema de archivos (por ejemplo, sftp), cambie los permisos a Read/Write (Lectura y escritura) para el recurso compartido y haga clic en APPLY (Aplicar).**
11. **Haga clic en el ícono de edición  para configurar las propiedades del recurso compartido. (Consulte [“Propiedades de sistema de archivos” \[525\]](#)).**
12. **Para acceder al recurso compartido, use el comando `sftp` como se muestra en estos ejemplos:**

```
sftp -o "port=218" username 10.x.x.151:/export/sftp
Connecting to 10.x.xx.151...
Changing to: /export/sftp
sftp>
```

Ejemplo con la opción -v:

```
sftp -v -o "IdentityFile=/home/username/.ssh/id_dsa" -o "port=218"
root 10.x.xx.151:/export/sftp
```

Temas relacionados

- [Agregación de acceso SFTP a un recurso compartido \(BUI\) \[439\]](#)
- [“Propiedades, puertos y logs de SFTP” \[441\]](#)

Propiedades, puertos y logs de SFTP

Propiedades de SFTP

TABLA 96 Propiedades de SFTP

Propiedad	Descripción
Puerto (para conexiones entrantes)	Puerto por el que el servicio SFTP escucha. El valor por defecto es 218.
Permitir inicio de sesión root	Permite al usuario root iniciar sesiones SFTP. Esta propiedad está desactivada por defecto.
Nivel de inicio de sesión	Nivel de detalle de los mensajes de log de SFTP.
Timeout de Sesión Inactiva	Timeout de inactividad en segundos para la sesión del cliente. Si no se registra ninguna actividad una vez que se alcanza el valor de timeout, se cierra la sesión del usuario. Por defecto, el valor está configurado en <i>Infinite</i> .
Claves	Claves RSA/DSA públicas para la autenticación SFTP. Es posible asociar comentarios de texto con las claves para ayudar a los administradores a llevar un control del motivo por el que se agregaron. A partir de la versión 2011.1 del software, la gestión de claves para SFTP se modificó para aumentar la seguridad. Al crear una clave SFTP, se debe incluir la propiedad <i>user</i> con una asignación de usuario válida. Las claves SFTP se agrupan por usuario y se autentican mediante SFTP con el nombre del usuario. Se recomienda volver a crear las claves SFTP existentes que no incluyan la propiedad de usuario, aunque si no la incluyen igual servirán para la autenticación.

TABLA 97 Propiedades de seguridad de SFTP

Propiedad	Descripción
Cifrados	Cifrados para conexiones SFTP.
MAC	Códigos de autenticación de mensajes (MAC) para conexiones SFTP.

Puertos SFTP

El servicio SFTP usa un número de puerto no estándar para las conexiones con el dispositivo. Esto es así para evitar conflictos con conexiones SSH administrativas al puerto 22. Por defecto, el puerto SFTP es el 218 y se debe especificar en el cliente SFTP antes de establecer la conexión. Por ejemplo, un cliente de Oracle Solaris que use SFTP se conectaría con el siguiente comando:

```
manta# sftp -o "Port 218" root@hostname
```

Logs de SFTP

network-sftp:default: registra los eventos del servicio SFTP

Temas relacionados

- [Agregación de acceso SFTP a un recurso compartido \(BUI\) \[439\]](#)
- [Configuración de SFTP para acceso remoto \(CLI\) \[439\]](#)

Configuración de la migración shadow

El servicio de migración shadow permite la migración automática de datos desde fuentes externas o internas. Esta funcionalidad se describe en detalle en la documentación de [Migración shadow \[575\]](#). El servicio en sí mismo solo controla la migración automática en segundo plano. Independientemente de si el servicio está activado o no, los datos se migrarán sincrónicamente para solicitudes en banda.

Este servicio solo se debe desactivar con fines de prueba, o si la carga del sistema es demasiado grande debido a la migración shadow. Si está desactivado, el sistema de archivos no finalizará la migración. La finalidad principal de este servicio consiste en permitir el ajuste de la cantidad de subprocesos dedicados a la migración en segundo plano.

Propiedad Number of Threads (Número de threads): número de threads que se dedicarán a la migración de datos en segundo plano. Estos subprocesos son globales en toda la máquina y, al aumentar la cantidad, se puede aumentar la concurrencia y velocidad general de migración a expensas de un mayor consumo de recursos (red, E/S y CPU).

Configuración de SMB

El servicio SMB proporciona acceso a sistemas de archivos mediante el protocolo SMB. Las versiones admitidas de SMB son SMB 1, SMB 2.0, SMB 2.1, SMB 3.0 y SMB 3.1. Para compartir sistemas de archivos por SMB, configure el sistema de archivos como se describe en [“Propiedades de sistema de archivos” \[525\]](#). En las siguientes tablas, se muestran las funciones admitidas y no admitidas de SMB 3.1, SMB 3.0 y SMB 2.1.

Es muy recomendable actualizar a los clientes de SMB 1 a, por lo menos, SMB 2.0 porque SMB 1 tiene problemas conocidos de seguridad y rendimiento que se resolvieron en versiones posteriores de SMB.

TABLA 98 Funciones admitidas y no admitidas de SMB 3.1

Funciones admitidas	Funciones no admitidas
Integridad previa a la autenticación	

Funciones admitidas	Funciones no admitidas
Mejoras en el cifrado: se agregó AES-128-GCM.	

TABLA 99 Funciones admitidas y no admitidas de SMB 3.0

Funciones admitidas	Funciones no admitidas
Conmutación por error transparente (recursos compartidos con disponibilidad continua)	SMB sobre Acceso directo a memoria remoto (RDMA)
Multicanal	Servicio de instantáneas de volumen (VSS) para sistemas de archivos SMB
Cifrado	Cesión de directorio

TABLA 100 Funciones admitidas y no admitidas de SMB 2.1

Funciones admitidas	Funciones no admitidas
Arrendamiento	Caché de rama
Solicitud de negociación de varios protocolos	Manipulación flexible
Operaciones individuales de escritura directa	
Operaciones de créditos múltiples	

Los identificadores de usuario y las cuentas locales se asignan a identificadores de usuario de Windows. Tenga en cuenta que la cuenta *huésped* es una cuenta especial de solo lectura y no se puede configurar para operaciones de lectura/escritura en el dispositivo.

Para configurar el SMB, consulte las siguientes secciones:

- [“Propiedades del servicio SMB” \[444\]](#)
- [“Configuración de propiedades para exportar recursos compartidos mediante SMB” \[446\]](#)
- [“Interoperabilidad NFS/SMB” \[447\]](#)
- [“Espacios de nombres de DFS de SMB” \[447\]](#)
- [“Matriz de compatibilidad de herramientas de gestión de espacios de nombres de DFS independientes de Microsoft para SMB” \[448\]](#)
- [Agregación de espacios de nombres de DFS a un grupo SMB local \[450\]](#)
- [“Directorio raíz automático de SMB” \[450\]](#)
- [Agregación de reglas de directorio raíz automático de SMB \(CLI\) \[451\]](#)
- [Agregación de usuarios a grupos locales de SMB \[452\]](#)
- [“Integración de MMC con SMB” \[453\]](#)
- [“Gestión de recursos compartidos de SMB” \[454\]](#)
- [“Usuarios, grupos y conexiones de SMB” \[456\]](#)
- [“Visualización de servicios de SMB” \[458\]](#)

- [Configuración de SMB \(BUI\) \[460\]](#)
- [Configuración de Active Directory de SMB \(BUI\) \[462\]](#)
- [Configuración de recursos compartidos y proyectos SMB \(BUI\) \[462\]](#)
- [Configuración del servicio de datos de SMB \(BUI\) \[463\]](#)

Propiedades del servicio SMB

Los cambios realizados en las propiedades de los servicios se documentan en las secciones [Configuración de las propiedades de los servicios \(BUI\) \[328\]](#) y [Configuración de las propiedades de los servicios \(CLI\) \[329\]](#).

- **Versión mínima admitida:** elija la versión mínima de SMB que el dispositivo admite.
- **Versión máxima admitida:** elija la versión máxima de SMB que el dispositivo admite.
- **Comentario de sistema:** cadena de texto significativa.
- **Timeout de sesión inactiva:** configuración del timeout para la inactividad de la sesión.
- **Controlador de dominio preferido:** controlador de dominio preferido para utilizar al unir un dominio de Active Directory. Si este controlador no está disponible, Active Directory utiliza los registros de DNS SRV y el sitio de Active Directory para localizar un controlador de dominio apropiado. Para obtener más información, consulte [“Configuración de Active Directory” \[335\]](#).
- **Sitio de Active Directory:** sitio que se utiliza para unirse a un dominio de Active Directory. Un sitio es una recopilación lógica de equipos que están conectados mediante enlaces de red de ancho de banda elevado y baja latencia. Si se configura esta propiedad pero no se especifica el controlador de dominio preferido, para unirse a un dominio de Active Directory, se preferirán los controladores de dominio de este sitio por sobre los controladores de dominio externos.
- **Número máximo de threads de servidor:** cantidad máxima de subprocesos de servidor simultáneos (trabajadores). El valor por defecto es 1024.
- **Activar DNS dinámico:** elija si el dispositivo utilizará DNS dinámico para actualizar los registros de DNS en el dominio de Active Directory. La opción está desactivada por defecto.
- **Activar bloqueos oportunistas:** elija si el dispositivo otorgará bloqueos oportunistas a los clientes SMB. Esto mejora el rendimiento de la mayoría de los clientes. La opción está activada por defecto. El servidor SMB otorga un bloqueo oportunista a un proceso de un cliente para que el cliente pueda almacenar en la caché los datos mientras el bloqueo está vigente. Cuando el servidor revoca el bloqueo oportunista, el cliente alinea con el servidor los datos almacenados en la caché.
- **Restringir el acceso anónimo a la lista de recursos compartidos:** si se activa esta opción, los clientes deben autenticarse en el servicio SMB antes de recibir una lista de recursos compartidos. Si la opción está desactivada, los clientes anónimos pueden acceder a la lista de recursos compartidos.

- **Servidor WINS principal:** dirección WINS principal configurada en TCP/IP.
- **Servidor WINS secundario:** dirección WINS secundaria configurada en TCP/IP.
- **Direcciones IP excluidas de WINS:** Direcciones IP excluidas del registro con WINS.
- **Nivel de compatibilidad del gestor de LAN:** modos de autenticación admitidos (LM, NTLM, LMv2, NTLMv2). Para obtener más información acerca de los modos de autenticación admitidos en cada nivel de compatibilidad, consulte la biblioteca de información de Oracle Solaris para *smb*. NTLMv2 es el nivel mínimo recomendado para evitar vulnerabilidades de seguridad conocidas públicamente.
- **Firma de SMB activada:** permite la interoperabilidad con clientes SMB mediante la función de firma de SMB. Si se firmó un paquete, se verifica la firma. Si el paquete no se firmó, se lo acepta sin verificación de firma (si no es obligatorio el uso de firmas de SMB, como se describe a continuación).
- **Firma de SMB requerida:** cuando se requiere el uso de firmas de SMB, todos los paquetes de SMB deben estar firmados o se los rechazará y los clientes que no admitan el uso de firmas no podrán conectarse con el servidor.
- **No tener en cuenta solicitudes de cero circuitos virtuales:** Cuando un cliente SMB establece una nueva conexión, puede solicitar que el dispositivo elimine todas las conexiones y todos los bloqueos de archivos previos provenientes de este cliente, para lo que especifica una cantidad de cero circuitos virtuales (en inglés, VC). Sin embargo, este artefacto del protocolo no respeta la traducción de direcciones de red (NAT) para los clientes o varias entradas de DNS asignadas para el mismo host. En combinación, las solicitudes de cero circuitos virtuales entre ubicaciones enmascaradas o redundantes puede hacer que se restablezcan conexiones activas no relacionadas. Por defecto, se respetan las solicitudes de cero circuitos virtuales para evitar bloqueos obsoletos de archivos, pero si se observa que las sesiones de SMB se desconectan por error, no tener en cuenta las solicitudes de cero circuitos virtuales puede solucionar el problema.
- **Visibilidad de recursos compartidos:** use esta propiedad para establecer la política de enumeración basada en el acceso (ABE) para la visibilidad de los recursos compartidos disponibles para los clientes. Los valores válidos son "Completa" y "Restringida". Mientras que el valor "Completa" permite acceso total, el valor "Restringida" limita el acceso solo a los recursos compartidos que el cliente está autorizado para ver. El acceso a los recursos compartidos está determinado por las excepciones de SMB y la ACL del recurso compartido. Por defecto, esta propiedad está configurada con el valor "Completa".
- **Activación de NetBIOS:** permite activar o desactivar todos los servicios de NetBIOS. Un valor "true" (valor por defecto) activa los servicios de nombre de NetBIOS (puerto UDP 137), datagrama (puerto UDP 138) y sesión (puerto TCP 139); asimismo, permite localizar el controlador de dominios mediante una detección basada en NetBIOS, mientras que un valor "false" los desactiva todos.
- **Cifrar el acceso a datos:** permite que el servidor SMB exija a los clientes cifrar los datos de todas las sesiones nuevas. Es posible omitir esta imposición si el servidor permite el acceso no cifrado. Se configura el cifrado de SMB en el nivel global; el valor por defecto es `false`. Consulte también "Rechazar el acceso sin cifrar".

- **Rechazar el acceso sin cifrar:** rechaza el acceso sin cifrar cuando se activa el cifrado en el nivel global o el cifrado en el nivel de recurso compartido. El valor predeterminado es `true`. Cuando se establece en `false`, no se permite el acceso sin cifrar. No establezca esta propiedad en `false` a menos que haya comprendido las consecuencias para la seguridad. El acceso sin cifrar puede aceptarse y permitirse cuando el escenario de despliegue requiere soporte para los clientes de nivel inferior que no son compatibles con el cifrado.
- **Activar varios canales:** se activa o se desactiva la compatibilidad con varios niveles de SMB3. Cuando está establecido en el valor por defecto `true`, el servidor SMB acepta rutas de acceso de varios canales entre el cliente y el servidor SMB. En algunas configuraciones de firewall, puede ser útil desactivar la compatibilidad con varios niveles.

Configuración de propiedades para exportar recursos compartidos mediante SMB

Se deben configurar varias propiedades de recursos compartidos al exportar un recurso mediante SMB.

TABLA 101 Propiedades de recursos compartidos de SMB

Propiedad	Descripción
Distinción entre mayúsculas y minúsculas	Los clientes SMB no diferencian mayúsculas de minúsculas, de manera que esta propiedad debe configurarse como "combinado" o "indistinto". Consulte "Propiedades estáticas" [513] .
Rechazar codificación que no sea UTF-8	Si en un sistema de archivos se permite el uso de nombres de archivo que no tengan codificación UTF-8, los clientes SMB pueden funcionar incorrectamente. Consulte "Propiedades estáticas" [513] .
Bloqueo no bloqueante obligatorio	Esta propiedad se debe activar para permitir que el bloqueo de rango de bytes funcione correctamente. Consulte "Propiedades estáticas" [513] .
Nombre de recurso	Nombre que utilizan los clientes para hacer referencia al recurso compartido. Para obtener información acerca de cómo se hereda este nombre desde un proyecto, consulte "Protocolos de recursos compartidos y proyectos" [547] .
ACL en el nivel de recurso compartido	Lista de control de acceso (ACL) que agrega otra capa de control de acceso más allá de las ACL almacenadas en el sistema de archivos. Para obtener más información acerca de esta propiedad, consulte "Listas de control de acceso para sistemas de archivos" [564] .

Las propiedades de distinción entre mayúsculas y minúsculas y rechazo de codificación que no sea UTF-8 se pueden configurar solamente al crear el recurso compartido.

No puede haber dos recursos compartidos SMB en el mismo sistema que compartan el mismo nombre de recurso. Los nombres de recursos que se hayan heredado de los proyectos tienen un comportamiento especial. Para obtener información detallada, consulte [Recursos compartidos y proyectos](#) [483]. Los nombres de recursos deben tener menos de 80 caracteres y pueden contener cualquier carácter alfanumérico además de los siguientes caracteres:

" / \ [] : | < > + ; , ? * =

Cuando está activada la enumeración basada en el acceso, los clientes pueden ver entradas de directorios para los archivos que ellos no pueden abrir. Las entradas de directorio solo se filtran cuando el cliente no tiene acceso a ese archivo. Por ejemplo, si un cliente intenta abrir un archivo para obtener acceso de lectura y escritura, pero la ACL otorga acceso de solo lectura, se producirá un error en esa solicitud abierta, pero el archivo aún será incluido en la lista de entradas.

Interoperabilidad NFS/SMB

El dispositivo admite el acceso concurrente de clientes NFS y SMB a los mismos recursos compartidos. Para configurar correctamente el dispositivo para interoperabilidad NFS/SMB, debe configurar los siguientes componentes:

- Configure el servicio de Active Directory. Consulte [“Configuración de Active Directory”](#) [335].
- Establezca una estrategia de servicio de asignación de identidades y configure el servicio. Consulte [“Configuración de asignación de identidades”](#) [363].
- Configure SMB. Consulte [“Configuración de SMB”](#) [442].
- Configure el control de acceso, las entradas de la ACL y los valores heredados de la ACL en los recursos compartidos.

SMB y NFSv3 no usan el mismo modelo de control de acceso. Para obtener los mejores resultados, configure la ACL en el directorio raíz desde un cliente SMB, ya que el modelo de control de acceso de SMB es más detallado. Para obtener información acerca de las entradas heredables triviales de ACL, consulte [“Listas de control de acceso para sistemas de archivos”](#) [564].

Espacios de nombres de DFS de SMB

El sistema de archivos distribuidos (DFS, Distributed File System) es una tecnología de virtualización que se entrega mediante los protocolos SMB y MSRPC. DFS permite a los administradores agrupar carpetas compartidas que se encuentran en diferentes servidores conectándolas de manera transparente con uno o varios espacios de nombres de DFS. Un espacio de nombres de DFS es una vista virtual de carpetas compartidas en una organización. El administrador puede seleccionar las carpetas compartidas que desea presentar en el espacio

de nombres, diseñar la jerarquía en la que aparecen esas carpetas y determinar los nombres que muestran las carpetas compartidas en el espacio de nombres. Cuando un usuario visualiza el espacio de nombres, las carpetas parecen residir en un único sistema de archivos de gran capacidad. Los usuarios pueden navegar por las carpetas del espacio de nombres sin necesidad de saber los nombres de los servidores o las carpetas compartidas que alojan los datos.

Se puede aprovisionar solo un recurso compartido por sistema como espacio de nombres de DFS independiente. No se admiten los espacios de nombres de DFS basados en dominios. Tenga en cuenta que se puede aprovisionar un espacio de nombres de DFS por cluster, aunque cada nodo de cluster tenga una agrupación de almacenamiento independiente. Para aprovisionar un recurso compartido de SMB como espacio de nombres de DFS, use el complemento de MMC de gestión de DFS para crear un espacio de nombres independiente.

Cuando el dispositivo no está unido a un dominio de Active Directory, es necesario realizar una configuración adicional para que los usuarios del grupo de trabajo puedan modificar los espacios de nombres de DFS. Para que un usuario local de SMB pueda crear o suprimir un espacio de nombres de DFS, ese usuario debe tener una cuenta local independiente creada en el servidor. Para obtener información sobre los pasos para permitir que el usuario local de SMB `dfsadmin` manipule los nombres de espacios de DFS, consulte [Agregación de espacios de nombres de DFS a un grupo SMB local \[450\]](#).

Matriz de compatibilidad de herramientas de gestión de espacios de nombres de DFS independientes de Microsoft para SMB

En la siguiente tabla se enumeran las operaciones (subcomandos y opciones) de las herramientas de DFS de Microsoft en diversas versiones de sistemas operativos de Windows. Identifica cuáles de estas versiones son admitidas por el servicio DFS en el dispositivo para gestionar un espacio de nombres DFS independiente en el dispositivo.

- **y**: admitido
- **n**: no admitido
- **NA**: no se aplica

Microsoft Windows systems	XP	2003	2003	Vista	2008	2008	Win7
			R2			R2	
	SP3	SP2	SP2	SP2	SP2	SP1	SP1
dfscmd CLI:							
/map [comment] [/restore]	y	y	y	y	y	y	y
/unmap	y	y	y	y	y	y	y
/add [/restore]	y	y	y	y	y	y	y
/remove	y	y	y	y	y	y	y
/view [/partial /full]	y	y	y	y	y	y	y

dfsutil CLI (old format):							
/addstdroot [/comment]	y	y	y	n	n	y	y
/remstdroot	y	y	y	n	n	y	y
/root:<DfsName> /view	n	n	n	y	y	y	y
/addlink [/comment]	NA	NA	NA	y	y	y	y
/removelink	NA	NA	NA	y	y	y	y
/state /display	NA	NA	NA	y	y	y	y
/state /enable	NA	NA	NA	y	y	y	y
/state /disable	NA	NA	NA	y	y	y	y
/ttl /display	NA	NA	NA	y	y	y	y
/ttl /set	NA	NA	NA	y	y	y	y
/server:<MachineName> /view	y	y	y	y	y	y	y
dfsutil CLI (new format):							
root addstd [comment]	NA	NA	NA	n	n	y	y
root remove	NA	NA	NA	n	n	y	y
root (view namespace)	NA	NA	NA	y	y	y	y
link add [comment]	NA	NA	NA	y	y	y	y
link remove	NA	NA	NA	y	y	y	y
link (view)	NA	NA	NA	y	y	y	y
target add	NA	NA	NA	y	y	y	y
target remove	NA	NA	NA	y	y	y	y
target (view)	NA	NA	NA	y	y	y	y
property comment (view)	NA	NA	NA	y	y	y	y
property comment set	NA	NA	NA	y	y	y	y
property ttl (view)	NA	NA	NA	y	y	y	y
property ttl set	NA	NA	NA	y	y	y	y
property state (view)	NA	NA	NA	y	y	y	y
property state offline	NA	NA	NA	y	y	y	y
property state online	NA	NA	NA	y	y	y	y
DFS GUI:							
add standalone root	y	y	y	n	n	n	n
remove standalone root	y	y	y	n	n	n	n
change root comment	y	y	y	n	n	n	n
change root timeout	y	y	y	n	n	n	n
add link	y	y	y	n	n	n	n
remove link	y	y	y	n	n	n	n
change link comment	y	y	y	n	n	n	n
change link timeout	y	y	y	n	n	n	n
add link's target	y	y	y	n	n	n	n
remove link's target	y	y	y	n	n	n	n
enable link's referral (target)	y	y	y	n	n	n	n
disable link's referral (target)	y	y	y	n	n	n	n
hide root	y	y	y	y	y	y	y
show root	y	y	y	y	y	y	y
display links	y	y	y	n	n	n	n
display targets	y	y	y	n	n	n	n
	XP	2003	2003	Vista	2008	2008	Win7
			R2			R2	
	SP3	SP2	SP2	SP2	SP2	SP1	SP1

Tenga en cuenta lo siguiente:

- Oracle Solaris no verifica el destino de enlace de DFS.

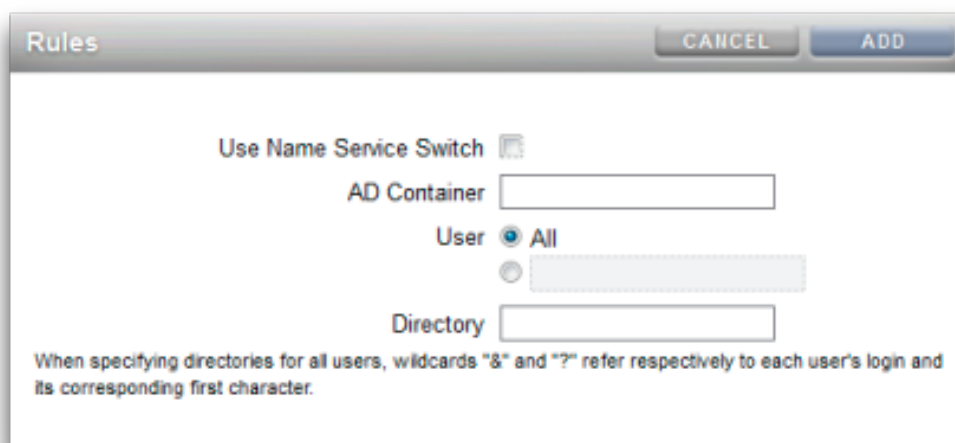
- Los comandos de la CLI para modificar y visualizar comentarios y tiempo de espera (TTL) se usan tanto para la raíz como para el enlace.
- Los comandos de la CLI para visualizar el estado se aplican a la raíz, el destino de la raíz, el enlace y el destino del enlace.
- Los comandos de la CLI para modificar el estado se usan solamente para el enlace y el destino del enlace.

▼ Agregación de espacios de nombres de DFS a un grupo SMB local

1. Cree una cuenta de usuario local en el servidor para el usuario `dfsadmin`. Asegúrese de usar la misma contraseña que cuando se creó el usuario local en el equipo con Windows.
2. Agregue `dfsadmin` al grupo local de administradores de SMB.
3. Inicie sesión como `dfsadmin` en el equipo con Windows desde el cual se modificará el espacio de nombres de DFS.

Directorio raíz automático de SMB

Para el uso compartido de archivos de Windows, el directorio raíz automático proporciona acceso a los sistemas de archivos mediante el protocolo SMB. El directorio raíz automático define y mantiene los recursos compartidos del directorio raíz para los usuarios que acceden al sistema a través de SMB. Las reglas de directorio raíz automático asignan los clientes SMB a directorios raíz.

FIGURA 19 Configuración de las reglas del directorio raíz automático

- **Usar conmutador de servicios de nombres:** activa o desactiva el servicio NSS (conmutador de servicios de nombres). No se puede crear simultáneamente una regla de NSS y una regla para todos los usuarios.
- **AD Container** (Contenedor de Active Directory): define el contenedor de Active Directory, por ejemplo: dc=com,dc=fishworks,ou=Engineering,CN=myhome.
- **Usuario:** define la regla de directorio raíz automático para todos los usuarios o el usuario que se especifique. Si se especifica un usuario, los comodines "&" y "?" hacen referencia al inicio de sesión del usuario y el primer carácter correspondiente.
- **Directorio:** define el directorio para la regla, por ejemplo: /export/wdp.

▼ Agregación de reglas de directorio raíz automático de SMB (CLI)

1. **Vaya a `configuration services smb`.**
2. **Use el comando `create` para agregar reglas de directorio principal automático y el comando `list` para enumerar las reglas existentes.**

En este ejemplo, se agrega una regla para el usuario "Bill" y después se enumeran las reglas:

```

hostname:> configuration services smb
hostname:configuration services smb> create
hostname:configuration services rule (uncommitted)> set use_nss=false
hostname:configuration services rule (uncommitted)> set user=Bill
hostname:configuration services rule (uncommitted)> set directory=/export/wdp
hostname:configuration services rule (uncommitted)> set container="dc=com,dc=fishworks,
ou=Engineering,CN=myhome"
hostname:configuration services rule (uncommitted)> commit
hostname:configuration services smb> list
RULE      NSS      USER      DIRECTORY      CONTAINER
rule-000  false   Bill      /export/wdp    dc=com,dc=fishworks,
ou=Engineering,CN=myhome

```

3. Cree reglas de directorio raíz automático mediante el uso de comodines.

El carácter & coincide con el nombre de usuario de los usuarios, mientras que el carácter ? coincide con la primera letra del nombre de usuario del usuario. En el siguiente ejemplo, se usan comodines para que haya coincidencia con todos los usuarios:

```

hostname:configuration services smb> create
hostname:configuration services rule (uncommitted)> set use_nss=false
hostname:configuration services rule (uncommitted)> set user=*
hostname:configuration services rule (uncommitted)> set directory=/export/??/&
hostname:configuration services rule (uncommitted)> set container="dc=com,dc=fishworks,
ou=Engineering,CN=myhome"
hostname:configuration services rule (uncommitted)> commit
hostname:configuration services smb> list
RULE      NSS      USER      DIRECTORY      CONTAINER
rule-000  false   Bill      /export/wdp    dc=com,dc=fishworks,
ou=Engineering,CN=myhome

```

4. El conmutador de servicio de nombres también se puede usar para crear reglas de directorio raíz automático:

```

hostname:configuration services smb> create
hostname:configuration services rule (uncommitted)> set use_nss=true
hostname:configuration services rule (uncommitted)> set container="dc=com,dc=fishworks,
ou=Engineering,CN=myhome"
hostname:configuration services rule (uncommitted)> commit
hostname:configuration services smb> list
RULE      NSS      USER      DIRECTORY      CONTAINER
rule-000  true    Bill      /export/wdp    dc=com,dc=fishworks,
ou=Engineering,CN=myhome

```

▼ Agregación de usuarios a grupos locales de SMB

Los grupos locales son grupos de usuarios del dominio o locales que confieren privilegios adicionales a esos usuarios.

Grupos locales de SMB:

- **Administradores:** los administradores pueden pasar por alto permisos de archivos para cambiar la propiedad de los archivos.

- **Operadores de copia de seguridad:** los operadores de copia de seguridad pueden pasar por alto los controles de acceso de archivos para hacer copias de seguridad de los archivos y restaurarlos.

1. Vaya a configuration services smb groups.

```
hostname:configuration services smb> groups
```

2. Introduzca create.

```
hostname:configuration services smb groups> create
```

3. Especifique el usuario que desea agregar al grupo:

```
hostname:configuration services smb member (uncommitted)> set user=Bill
```

4. Introduzca el nombre de grupo y, luego, confirme el cambio:

```
hostname:configuration services smb member (uncommitted)> set group="Backup Operators"
hostname:configuration services smb member (uncommitted)> commit
```

5. Introduzca list para confirmar que el usuario fue agregado al grupo especificado:

```
hostname:configuration services smb groups> list
MEMBER      USER      GROUP
member-000  WINDOMAIN\Bill      Backup Operators
```

Integración de MMC con SMB

Microsoft Management Console (MMC) es una estructura extensible de componentes registrados, conocidos como complementos, que proporcionan funciones de gestión integrales tanto para el sistema local como para los sistemas remotos de la red. Administración de equipos es una recopilación de herramientas de Microsoft Management Console que se puede utilizar para configurar, supervisar y gestionar servicios y recursos locales y remotos.

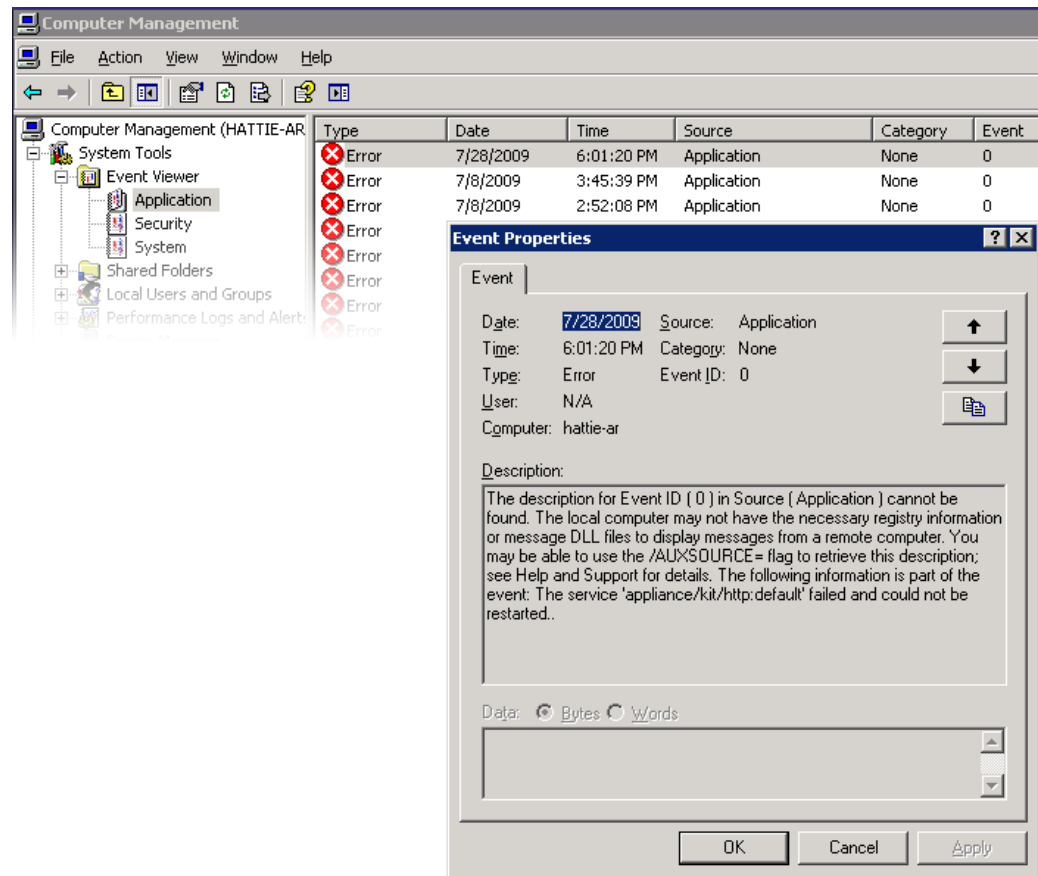
Para usar las funciones de MMC en el dispositivo en el modo de grupo de trabajo, asegúrese de agregar el administrador de Windows que utilizará la consola de administración al grupo local de administradores del dispositivo. De lo contrario, puede aparecer el error `Access is denied` (Acceso denegado), o uno similar, en el cliente de administración al intentar conectarse con el dispositivo mediante MMC.

El dispositivo admite las siguientes características de administración de equipos:

El complemento Visor de eventos de MMC muestra el log de aplicación, el log de seguridad y el log de sistema. Estos logs muestran el contenido de los logs de alertas, auditoría y sistema del dispositivo.

En la siguiente pantalla, se muestra un ejemplo del log de aplicación y del cuadro de diálogo de propiedades de un evento de error.

FIGURA 20 Visor de eventos de SMB



Gestión de recursos compartidos de SMB

La gestión de recursos compartidos permite hacer lo siguiente:

- Enumerar recursos compartidos

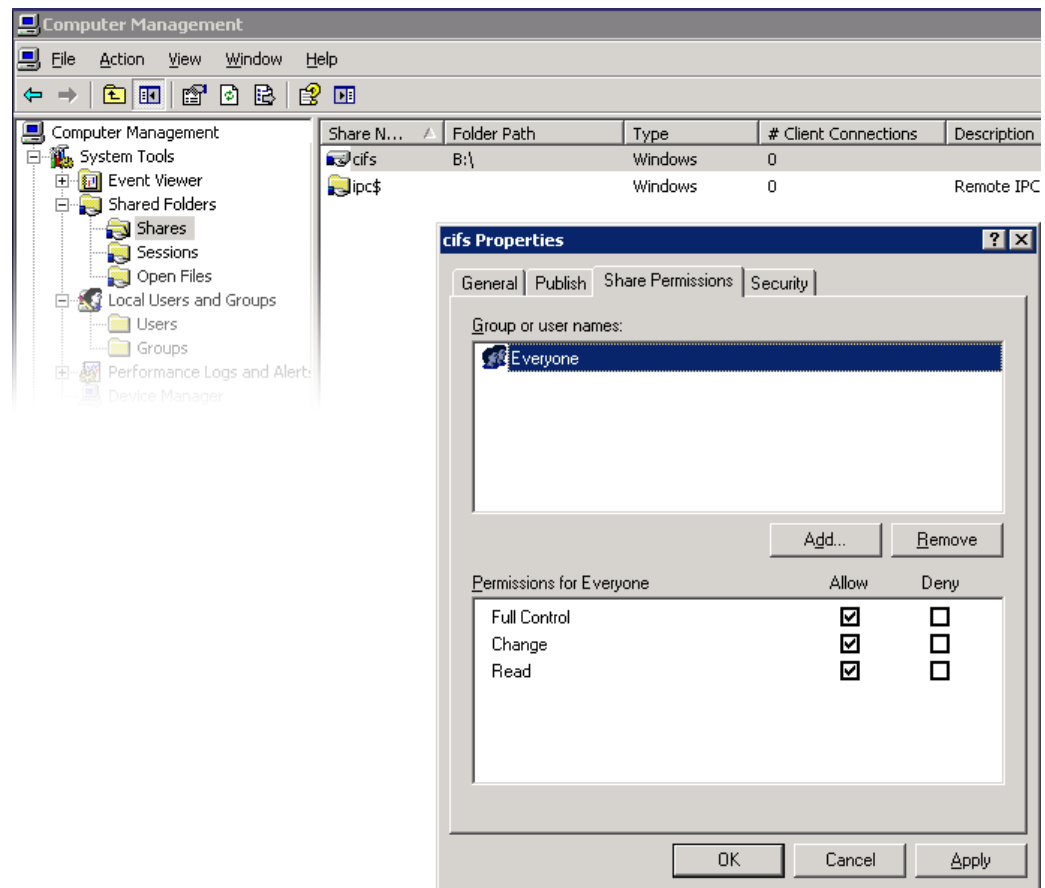
- Configurar listas ACL en recursos compartidos
- Cambiar permisos de recursos compartidos
- Definir la descripción de un recurso compartido

Las funciones que actualmente no se pueden realizar con MMC incluyen:

- Agregar o suprimir recursos compartidos
- Configurar la propiedad de almacenamiento en caché del lado del cliente
- Configurar la propiedad de cantidad máxima o permitida de usuarios

En la siguiente pantalla se muestra un ejemplo de las propiedades de permiso de un recurso compartido.

FIGURA 21 Propiedades de permisos de recursos compartidos de SMB



Usuarios, grupos y conexiones de SMB

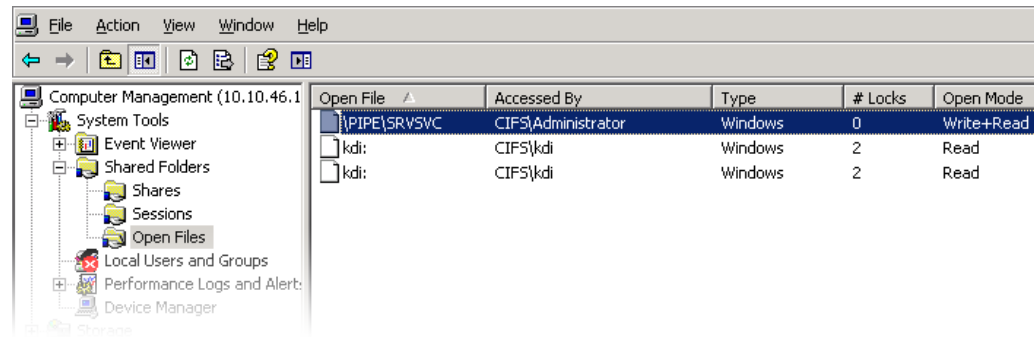
Se admiten las siguientes funciones:

- Visualizar usuarios y grupos locales de SMB
- Generar listas de conexiones de usuarios, incluida una lista de la cantidad de archivos abiertos por conexión
- Cerrar conexiones de usuarios

- Generar listas de archivos abiertos, incluida una lista de la cantidad de bloqueos que hay en el archivo y el modo de apertura del archivo
- Cerrar archivos abiertos

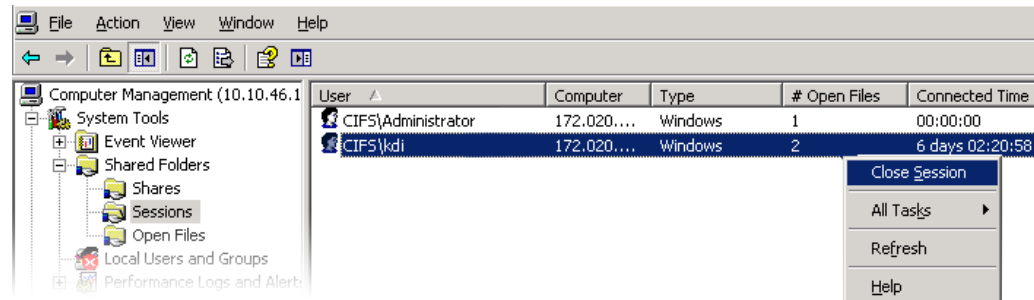
En la siguiente pantalla se muestra un ejemplo de archivos abiertos por conexión.

FIGURA 22 Archivos abiertos por conexión



En la siguiente pantalla se muestra un ejemplo de sesiones abiertas.

FIGURA 23 Sesiones abiertas

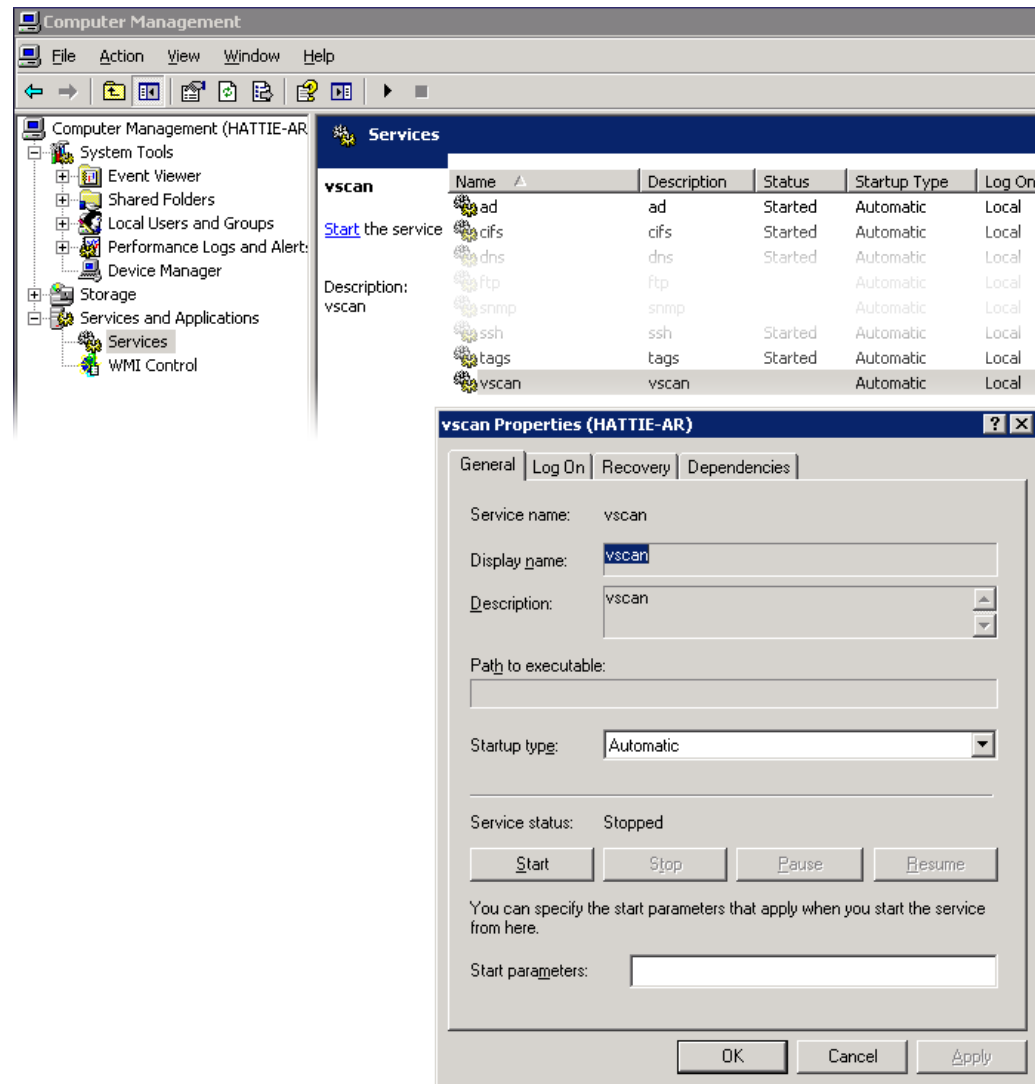


Visualización de servicios de SMB

La lista de servicios del dispositivo es compatible con la aplicación de MMC. Sin embargo, no puede activar o desactivar servicios con la aplicación de MMC. Permite generar listas de servicios del dispositivo. No se pueden activar ni desactivar servicios con la aplicación Administración de equipos de MMC.

En la siguiente pantalla se muestra un ejemplo de las propiedades generales para el servicio vscan.

FIGURA 24 Propiedades de vscan



Para garantizar que solo los usuarios apropiados tengan acceso a las operaciones administrativas, existen algunas restricciones de acceso para las operaciones que se realizan de manera remota mediante MMC.

TABLA 102 Usuarios y operaciones permitidas

Usuario	Operaciones permitidas
Usuarios comunes	Enumerar recursos compartidos.
Miembros de los grupos de administradores o usuarios avanzados	Gestionar recursos compartidos, generar listas de conexiones de usuarios.
Miembros del grupo de administradores	Generar listas de archivos abiertos, cerrar archivos, desconectar conexiones de usuarios, ver log de servicios y eventos.

▼ Configuración de SMB (BUI)

La configuración inicial del dispositivo se puede completar con la BUI o la CLI, y debería llevar menos de 20 minutos. La instalación inicial también se puede volver a realizar en otro momento desde los contextos Mantenimiento > Sistema de la BUI o la CLI. La configuración inicial lo llevará a los pasos siguientes:

1. **Configure dispositivos de red, enlaces de datos e interfaces.**
 - a. Cree interfaces con los íconos de agregación de enlace de datos o interfaz  o mediante la función de arrastrar y soltar dispositivos en las listas de enlaces de datos o interfaces.
 - b. Configure las propiedades deseadas y haga clic en el botón Aplicar para agregarlas a la lista.
 - c. Configure cada interfaz como activa o en espera, según corresponda.
 - d. Haga clic en APPLY (Aplicar) en la parte superior de la página para confirmar los cambios.
2. **Configurar el DNS.**
 - a. Proporcione el nombre del dominio base.
 - b. Proporcione la dirección IP de al menos un servidor que pueda resolver el nombre de host y los registros del servidor en la porción de Active Directory del espacio de nombres del dominio.
3. **Configure las claves de autenticación de NTP para garantizar la sincronización del reloj.**

- a. Haga clic en el ícono  para agregar una nueva clave.
 - b. Especifique el número, el tipo y el valor privado de la nueva clave, y aplique los cambios.

La clave aparece como opción al lado de cada servidor NTP especificado.
 - c. Asocie la clave con el servidor NTP apropiado y aplique los cambios. Para garantizar la sincronización del reloj, configure el dispositivo y los clientes SMB para usar el mismo servidor NTP.
4. Especifique Active Directory como servicio de directorio para los usuarios y los grupos.
 - a. Configure el dominio del directorio.
 - b. Haga clic en APPLY (Aplicar) para confirmar los cambios.
5. Configure una agrupación de almacenamiento.
 - a. Haga clic en el ícono  para agregar una nueva agrupación.
 - b. Establezca el nombre de la agrupación.
 - c. En la pantalla Allocate and verify storage (Asignar y verificar almacenamiento), configure la asignación de estante de discos para la agrupación de almacenamiento.

Si no se detecta ningún estante de discos, compruebe el cableado y la alimentación de energía.
 - d. Haga clic en COMMIT (Confirmar) para avanzar a la siguiente pantalla.
 - e. En la pantalla Configure Added Storage (Configurar almacenamiento agregado), seleccione el perfil de datos deseado.

Se los califica en términos de disponibilidad, rendimiento y capacidad. Use estas calificaciones a fin de determinar la mejor configuración para sus necesidades empresariales.
 - f. Haga clic en COMMIT (Confirmar) para activar la configuración.

6. Configure la asistencia técnica remota.

- a. **Si el dispositivo no está conectado directamente a Internet, configure un proxy HTTP mediante el cual el servicio de asistencia técnica remota pueda comunicarse con Oracle.**
- b. **Escriba el nombre de usuario y la contraseña de la cuenta en línea.**
Aparece una declaración de privacidad para que lea.
- c. **Elija con cuál de los equipos de inventario desea registrarse.**
El equipo por defecto para cada cuenta es igual al nombre de usuario de la cuenta con "\$" como prefijo.
- d. **Confirme los cambios de configuración inicial.**

▼ **Configuración de Active Directory de SMB (BUI)**

1. **Cree una cuenta para el dispositivo en el dominio de Active Directory.**
Para obtener instrucciones detalladas, consulte [“Configuración de Active Directory” \[335\]](#).
2. **En la pantalla Configuración > Servicios > Active Directory, haga clic en el botón Unirse a dominio.**
3. **Especifique el dominio, el usuario administrativo y la contraseña administrativa de Active Directory.**
4. **Haga clic en APPLY (Aplicar) para confirmar los cambios.**

▼ **Configuración de recursos compartidos y proyectos SMB (BUI)**

1. **Vaya a Recursos compartidos > Recursos compartidos.**
2. **Cree un proyecto.**
 - a. **En la pantalla Shares (Recursos compartidos), haga clic en el ícono de panel abierto  para ampliar el panel Projects (Proyectos).**
 - b. **Haga clic en el ícono de agregación  para agregar un nuevo proyecto.**

- c. Especifique el nombre del proyecto y haga clic en **APPLY** (Aplicar).
3. Seleccione un nuevo proyecto del panel Proyectos.
4. Haga clic en el ícono de agregación de elemento  para agregar un sistema de archivos.
5. Haga clic en el ícono de edición  del sistema de archivos.
6. Haga clic en el separador General y anule la selección de la casilla de control Inherit from project (Heredar del proyecto).
7. En /export, elija un punto de montaje, aunque el acceso a los recursos compartidos de SMB sea por nombre de recurso, y haga clic en **APPLY** (Aplicar).
8. Haga clic en el separador Protocols (Protocolos) del proyecto y configure el nombre del recurso de SMB en activado.
9. Active sharesmb y la ACL de nivel de recurso compartido para el proyecto.
10. Haga clic en **APPLY** (Aplicar) para activar la configuración.

▼ Configuración del servicio de datos de SMB (BUI)

1. Vaya a Configuration (Configuración) > Services (Servicios) > SMB y haga clic en el ícono de encendido  para activar el servicio.
2. Configure las propiedades de SMB y haga clic en **APPLY** (Aplicar) para activar la configuración. Consulte [“Propiedades del servicio SMB” \[444\]](#).
3. Haga clic en el separador Autohome (Directorio raíz automático) en la pantalla Configuration (Configuración) > Services (Servicios) > SMB para definir las reglas del directorio raíz automático para asignar clientes SMB en directorios raíz tal como se describe en [“Directorio raíz automático de SMB” \[450\]](#). Haga clic en **APPLY** (Aplicar) para activar la configuración.
4. En la pantalla Configuración > Servicios > SMB, haga clic en el separador Grupos locales y use el ícono de agregación de elemento  para agregar usuarios administradores u operadores de copia de seguridad a los grupos locales, tal como se describe en [Agregación de usuarios a grupos locales de SMB \[452\]](#). Haga clic en **APPLY** (Aplicar) para activar la configuración.

Configuración de SMTP

El servicio SMTP envía todos los mensajes generados por el dispositivo, normalmente en respuesta a las alertas configuradas en la pantalla Alertas. El servicio SMTP no acepta correo externo, solo envía correo generado automáticamente por el dispositivo.

Por defecto, el servicio SMTP usa DNS (registros MX) para determinar dónde se deben enviar los mensajes. Si el DNS no está configurado para el dominio del dispositivo o si el dominio de destino para correo saliente no tiene bien configurados los registros MX de DNS, el dispositivo se puede configurar para que reenvíe todos los mensajes de correo mediante un servidor de correo saliente, normalmente denominado host inteligente.

TABLA 103 Propiedades SMTP

Propiedad	Descripción
Send mail through smarthost (Enviar correo mediante host inteligente)	Si está activada, todos los mensajes de correo se envían por medio del servidor de correo saliente especificado. De lo contrario, el DNS se usa para determinar dónde se deben enviar los mensajes de correo para cada dominio en particular.
Smarthost hostname (Nombre de host del host inteligente)	Nombre de host del servidor de correo saliente.
Allow customized from address (Permitir remitente personalizado)	Si está activada, el remitente para correo electrónico se establece en la propiedad de remitente personalizado. Es posible que se desee personalizarla si el remitente predeterminado se identifica como correo no deseado, por ejemplo.
Custom from address (Remitente personalizado)	Remitente que se debe usar para los mensajes de correo electrónico salientes.

Al cambiar las propiedades, puede usar Alertas para enviar un mensaje de correo electrónico de prueba y comprobar que las propiedades sean correctas. Un motivo común por el que no se entregan los mensajes de correo electrónico es una configuración errónea del DNS, lo que impide que el dispositivo pueda determinar a qué servidor de correo debe entregar los mensajes. Como se describió anteriormente, se puede usar un host inteligente si no se puede configurar el DNS.

TABLA 104 Logs de SMTP

Log	Descripción
network-smtp:sendmail	Registra los eventos del servicio SMTP.
mail	Log de la actividad de SMTP (incluidos los mensajes enviados).

Configuración de SNMP

El servicio Protocolo Simple de Administración de Redes (SNMP) proporciona dos funciones diferentes en el dispositivo:

- La información de estado del dispositivo puede ser proporcionada mediante SNMP.
- Es posible configurar alertas para enviar capturas SNMP. Consulte [“Configuración de alertas” \[286\]](#).

Cuando este servicio está activado, las versiones v1, v2c y v3 de SNMP están disponibles. El dispositivo admite un máximo de 128 interfaces de red físicas y lógicas. La presencia de más de 128 interfaces de red podría provocar retrasos en la conexión en el caso de comandos como `snmpwalk` y `snmpget`. Si necesita más de 128 interfaces de red, póngase en contacto con la asistencia técnica de Oracle.

Para configurar el SNMP, consulte las siguientes secciones:

- [Configuración de SNMP para proporcionar información de estado del dispositivo \(BUI\) \[465\]](#)
- [Configuración de SNMP para enviar capturas \(BUI\) \[465\]](#)
- [“Propiedades de SNMP” \[466\]](#)
- [“MIB de SNMP” \[467\]](#)
- [“MIB de Sun FM.” \[467\]](#)
- [“MIB de Sun AK” \[468\]](#)

▼ Configuración de SNMP para proporcionar información de estado del dispositivo (BUI)

1. Vaya a **Configuration (Configuración) > Services (Servicios) > SNMP**.
2. Configure el nombre de comunidad, la red autorizada y la cadena de contacto.
3. (Opcional) Configure el destino de captura con un host SNMP remoto o establezca el valor 127.0.0.1.
4. Haga clic en **APPLY (Aplicar)** para confirmar la configuración.

▼ Configuración de SNMP para enviar capturas (BUI)

1. Vaya a **Configuration (Configuración) > Services (Servicios) > SNMP**.

2. **Configure el nombre de comunidad, la cadena de contacto y los destinos de las capturas.**
3. **(Opcional) Configure la red autorizada para permitir el acceso de clientes SNMP o establezca el valor 127.0.0.1/8.**
4. **Haga clic en APPLY (Aplicar) para confirmar la configuración.**
5. **Debe configurar alertas para enviar las capturas que desea recibir.**
Para obtener más información acerca de las alertas, consulte [“Configuración de alertas” \[286\]](#).

Temas relacionados

- [“Propiedades de SNMP” \[466\]](#)

Propiedades de SNMP

TABLA 105 Propiedades de SNMP

Propiedad	Descripción
Versión	Alterna entre v1/2c y v3.
Nombre de comunidad	Alterna entre público e introducido por el usuario. Si selecciona Introducido por el usuario, también debe introducir un nombre de comunidad. Si selecciona v3, esta propiedad no está disponible.
Red y subred autorizadas	Introduzca una dirección IPv4 y una subred apropiadas (números enteros de 0 a 32). Si selecciona v3, esta propiedad no está disponible.
Contacto de dispositivo	Introduzca un contacto apropiado para el dispositivo.
Nombre de usuario/contraseña	Introduzca un nombre de usuario (máximo de 501 caracteres) y una contraseña (de 8 a 501 caracteres) que sean válidos. Si selecciona v1/2c, esta propiedad no está disponible.
Autenticación	Alterna entre los algoritmos de autenticación MD5 y SHA. Si selecciona v1/2c, esta propiedad no está disponible. Tenga en cuenta que ya no se recomienda el uso de MD5, que podría eliminarse en una futura versión.
Privacy (Privacidad)	Alterna entre Ninguna y los algoritmos de cifrado DES y AES. Si selecciona v1/2c, esta propiedad no está disponible. Tenga en cuenta que ya no se recomienda el uso de DES, que podría eliminarse en una futura versión.
Engine ID (ID de motor)	Valor de identificador del motor procesado con un algoritmo hash por snmpd. Si no se activó SNMP, la etiqueta indica “0x000”.
Destinos de capturas	Permite agregar direcciones IPv4. Use los botones “+” y “-” para agregar o quitar direcciones.

El servicio SNMP también proporciona la cadena de ubicación MIB-II. Esta propiedad se obtiene de la configuración de [Identidad de sistema](#).

MIB de SNMP

Si el servicio SNMP está en línea, las redes autorizadas tendrán acceso a las siguientes MIB (bases de datos de información de administración):

TABLA 106 MIB de SNMP

MIB	Objetivo
.1.3.6.1.2.1.1	Sistema MIB-II: información genérica del sistema, que incluye nombre de host, contacto y ubicación.
.1.3.6.1.2.1.2	Interfaces MIB-II: estadísticas de la interfaz de red.
.1.3.6.1.2.1.4	IP MIB-II: información del protocolo de Internet, incluidas las direcciones IP y la tabla de rutas.
.1.3.6.1.2.1.31	MIB-II ifMIB: extensiones para la estructura de interfaces genéricas
.1.3.6.1.4.1.42	MIB de Sun Enterprise (SUN-MIB.mib.txt).
.1.3.6.1.4.1.42.2.195	FM de Sun: estadísticas de gestión de fallos (SUN-FM-MIB.mib.txt)
.1.3.6.1.4.1.42.2.225	AK de Sun: información y estadísticas del dispositivo (SUN-AK-MIB.mib.txt)

Nota - Los archivos MIB de SNMP de Sun están disponibles en <https://your IP address or host name:215/help/docs/snmp/SUN-MIB.mib.txt>.

MIB de Sun FM.

La MIB de Sun FM (SUN-FM-MIB.mib) proporciona acceso a información del gestor de fallos de SUN, por ejemplo:

- Problemas activos en el sistema
- Eventos del gestor de fallos
- Información de configuración del gestor de fallos

Hay cuatro tablas principales para leer:

TABLA 107 MIB de Sun FM

OID	Tabla de contenidos
.1.3.6.1.4.1.42.2.195.1.1	Problemas de la gestión de fallos
.1.3.6.1.4.1.42.2.195.1.2	Eventos de fallo de la gestión de fallos
.1.3.6.1.4.1.42.2.195.1.3	Configuración del módulo de gestión de fallos

OID	Tabla de contenidos
.1.3.6.1.4.1.42.2.195.1.5	Recursos defectuosos de la gestión de fallos

Consulte el archivo de la MIB para obtener descripciones completas.

Nota - Los archivos MIB de FM de Sun están disponibles en <https://your IP address or host name:215/help/docs/snmp/SUN-FM-MIB.mib.txt>.

MIB de Sun AK

La MIB de Sun AK (SUN-AK-MIB.mib) proporciona la siguiente información:

- Número de referencia y cadena de descripción del producto
- Versión de software del dispositivo
- Números de serie del dispositivo y el chasis
- Horas de instalación, actualización e inicio
- Estado del cluster, incluido el nodo par
- Estado de los recursos compartidos para sistemas de archivos y LUN (nombre de agrupación, nombre de proyecto, nombre de recurso compartido, tamaño, gigabytes y bytes usados y disponibles, punto de montaje del sistema de archivos)
- Estado de los recursos compartidos de réplica (nombre de agrupación, nombre de proyecto, nombre de recurso compartido, tamaño, bytes usados y disponibles, nombre de origen del recurso compartido de réplica, punto de montaje del sistema de archivos)
- Estado de la agrupación (nombre, perfil, estado, tamaño total, tamaño disponible, tamaño usado por tipo, compresión de datos y ratios de deduplicación de datos)
- Estado del hardware para los discos (nombre de componente, defectuoso, presente, nombre de chasis contenedor, proveedor, modelo, número de serie, velocidad, tipo)

Hay seis tablas principales para leer:

TABLA 108 MIB de Sun AK

OID	Tabla de contenidos
.1.3.6.1.4.1.42.2.225.1.4	Información general del dispositivo
.1.3.6.1.4.1.42.2.225.1.5	Estado del cluster
.1.3.6.1.4.1.42.2.225.1.6	Estado de los recursos compartidos
.1.3.6.1.4.1.42.2.225.1.7	Estado del recurso compartido de réplica
.1.3.6.1.4.1.42.2.225.1.8	Estado de agrupación
.1.3.6.1.4.1.42.2.225.1.9	Estado de hardware

Consulte el archivo de la MIB para obtener descripciones completas.

Nota - Los archivos MB de AK de Sun están disponibles en <https://your IP address or host name:215/help/docs/snmp/SUN-AK-MIB.mib.txt>.

Configuración de SRP

Al configurar un LUN en el dispositivo, puede exportar ese volumen por medio de un destino de protocolo remoto SCSI (SRP). El servicio SRP permite a los iniciadores utilizar el protocolo SRP para tener acceso a los destinos.

Para obtener información acerca de destinos e iniciadores SRP, consulte [“Configuración de una red de área de almacenamiento \(SAN\)” \[224\]](#).

Configuración de SSH

El servicio SSH (Shell seguro) permite a los usuarios iniciar sesión en la CLI del dispositivo y realizar la mayoría de las mismas acciones administrativas que se pueden realizar en la BUI. El servicio SSH también se puede usar como medio para ejecutar secuencias de comandos automatizadas desde un host remoto; por ejemplo, para recuperar logs diarios o estadísticas de Analytics (Análisis).

Las claves SSH se pueden configurar para cuentas individuales mediante la función de preferencias que se describe en [“Configuración de preferencias del dispositivo” \[280\]](#).

SSH también se puede usar en combinación con la autenticación Kerberos. Para obtener información acerca del servicio Kerberos del dispositivo, consulte [“Configuración de Kerberos” \[377\]](#).

Para una mayor seguridad al configurar SSH, puede especificar los cifrados y MAC, como se describe en [“Propiedades y logs de SSH” \[470\]](#).

Para configurar SSH, consulte las siguientes secciones:

- [Desactivación de acceso SSH para root \(CLI\) \[469\]](#)
- [“Propiedades y logs de SSH” \[470\]](#)

▼ Desactivación de acceso SSH para root (CLI)

1. **Vaya a** `configuration services ssh`.

2. **Establezca el permiso de inicio de sesión root en false.**
3. **Confirme la configuración.**

Propiedades y logs de SSH

TABLA 109 Propiedades de SSH

Propiedad	Descripción	Ejemplos
Período de gracia de inicio de sesión	La conexión SSH se desconecta después de esta cantidad de segundos si el cliente no logró autenticarse.	120
Permitir inicio de sesión root	Permite al usuario root iniciar sesión con SSH.	sí
Puerto (para las conexiones entrantes)	El puerto designado para conexiones entrantes.	22

TABLA 110 Propiedades de seguridad de SSH

Propiedad	Descripción
Cifrados	Cifrados para conexiones SSH.
MAC	Códigos de autenticación de mensajes (MAC) para conexiones SSH.

TABLA 111 Logs de SSH

Log	Descripción
network-ssh:default	Log de eventos y errores del servicio SSH.

Configuración de Syslog

El servicio Relé Syslog ofrece dos funciones diferentes en el dispositivo:

- Se pueden configurar alertas para enviar mensajes Syslog a uno o varios sistemas remotos. Consulte [“Configuración de alertas” \[286\]](#).
- En el caso de los servicios del dispositivo capaces de utilizar Syslog, se reenviarán sus propios mensajes Syslog a sistemas remotos.

El *mensaje de Syslog* es un mensaje de evento pequeño que se transmite del dispositivo a uno o varios sistemas remotos (o como nos gusta llamarlo: intercontinental printf). El mensaje contiene los siguientes elementos:

- Una utilidad que describe el tipo del componente del sistema que emitió el mensaje..

- Una gravedad que describe la gravedad de la condición relacionada con el mensaje.
- Un registro de hora que describe la hora del evento asociado en UTC.
- Un nombre de host que describe el nombre canónico del dispositivo.
- Una etiqueta que describe el nombre del componente del sistema que emitió el mensaje. Consulte [“Formato de los mensajes de alerta de Syslog” \[473\]](#) para obtener detalles del formato del mensaje.
- Un mensaje que describe el evento en sí mismo. Consulte [“Formato de los mensajes de alerta de Syslog” \[473\]](#) para obtener detalles del formato del mensaje.

Los receptores Syslog se proporcionan con la mayoría de los sistemas operativos, incluidos Oracle Solaris y Linux. Existen diversos paquetes de software de gestión de terceros y de código abierto que también admiten Syslog. Los receptores Syslog permiten a los administradores agregar mensajes de diversos sistemas a un único sistema de gestión e incorporarlos a un único conjunto de archivos log.

El Relé Syslog se puede configurar para utilizar el formato de salida "clásico" descrito por RFC 3164, o el formato de salida nuevo, con versión, descrito por RFC 5424. Los mensajes Syslog se transmiten como datagramas de UDP. Por lo tanto, es posible que sean rechazados por la red o que no puedan ser enviados, si el sistema de envíos no tiene suficiente memoria o la red está suficientemente congestionada. Por consiguiente, los administradores deben asumir que, en caso de fallos complejos en la red, es posible que se pierdan o se rechacen algunos mensajes.

Propiedades de Syslog

- **Versión de protocolo:** versión del protocolo Syslog que se utilizará, ya sea Syslog clásico (RFC 3164) o Syslog actualizado (RFC 5424).
- **Destinos:** la lista de direcciones IPv4, IPv6 y FQDN de destino hacia donde se transmiten los mensajes.

Para configurar Syslog, consulte las siguientes secciones:

- [“Syslog clásico: RFC 3164” \[471\]](#)
- [“Syslog actualizado: RFC 5424” \[472\]](#)
- [“Formato de los mensajes de SYSLOG” \[472\]](#)
- [“Formato de los mensajes de alerta de Syslog” \[473\]](#)
- [“Ejemplo de configuración de un receptor Oracle Solaris \(CLI\)” \[475\]](#)
- [“Ejemplo de configuración de un receptor Linux \(CLI\)” \[475\]](#)

Syslog clásico: RFC 3164

El protocolo Syslog clásico incluye los valores de utilidad y nivel codificados como una prioridad de número entero único, el registro de hora, un nombre de host, una etiqueta y el cuerpo del mensaje.

La etiqueta es una de las que se describen en [“Formato de los mensajes de SYSLOG” \[472\]](#).

El nombre de host será el nombre canónico del dispositivo según se define en la configuración de Identidad de sistema. Para obtener más información, consulte [“Configuración de identidad del sistema” \[476\]](#).

Syslog actualizado: RFC 5424

El protocolo Syslog clásico incluye los valores de utilidad y nivel codificados como una prioridad de número entero único, un campo de versión (1), el registro de hora, un nombre de host, el nombre de una aplicación y el cuerpo del mensaje. Los mensajes de syslog transmitidos por los sistemas de almacenamiento definirán los campos procid, msgid y structured-data de RFC 5424 con un valor nulo (-) para indicar que estos campos no contienen datos.

El nombre de la aplicación es uno de los que se describen en [“Formato de los mensajes de SYSLOG” \[472\]](#).

El nombre de host será el nombre canónico del dispositivo según se define en la configuración de Identidad de sistema. Para obtener más información, consulte [“Configuración de identidad del sistema” \[476\]](#).

Formato de los mensajes de SYSLOG

El protocolo Syslog en sí mismo no define el formato de la carga útil del mensaje y deja a cargo del remitente la inclusión de cualquier tipo de datos estructurados o cadenas en lenguaje natural no estructuradas que sea adecuado. Los sistemas Oracle ZFS Storage Appliance utilizan la etiqueta del subsistema de syslog ak para indicar una carga útil del mensaje estructurada y analizable, que se describe a continuación. Otras etiquetas del subsistema indican texto arbitrario en formato legible para el ojo humano; sin embargo, los administradores deben tener en cuenta estas formas de cadenas *inestables* y sujetas a cambios sin aviso, o su eliminación en futuras versiones del software de almacenamiento.

TABLA 112 Formatos de los mensajes de SYSLOG

Utilidad	Nombre de la etiqueta	Descripción
daemon	ak	Etiqueta genérica para subsistemas del dispositivo. Todas las alertas se etiquetarán como ak, lo que indicará que continúa un SUNW-MSG-ID.
daemon	idmap	Servicio de asignación de identidad para conversión de identidad de POSIX y Windows. Consulte

Utilidad	Nombre de la etiqueta	Descripción
		“Configuración de asignación de identidades” [363] .
daemon	smbd	Protocolo de datos SMA para acceder a recursos compartidos. Consulte “Configuración de SMB” [442] .

Formato de los mensajes de alerta de Syslog

Si se configura una alerta con la acción Enviar mensaje Syslog, se generará una carga útil de mensaje Syslog que contendrá texto localizado compuesto por los siguientes campos estándar. Cada campo tendrá un prefijo con el nombre de campo en letras MAYÚSCULAS seguido de dos puntos y un carácter de espacio en blanco.

TABLA 113 Formatos de los mensajes de alerta de Syslog

Nombre de campo	Descripción
SUNW-MSG-ID	El identificador de mensaje de error de Sun estable asociado con la alerta. A cada condición del sistema y diagnóstico de error que genera la alerta del administrador se le asigna un identificador único y persistente en el catálogo de mensajes de error de Sun. Estos identificadores se pueden leer con facilidad por teléfono o se pueden anotar en una computadora portátil, con un enlace al artículo de conocimientos correspondiente que se encuentra en My Oracle Support (https://support.oracle.com/) "Predictive Self-Healing" (Reparación automática predictiva) (ID del documento 1154428.1).
TYPE	Tipo de condición. Esta será una de las etiquetas: Fallo, que indica un error en el conector o componente de hardware, Defecto, que indica un problema de configuración o defecto de software, Alerta, que indica una condición no asociada a un error o defecto, como la finalización de una actividad de copia de seguridad o replicación remota.
VER	Versión de este formato de codificación. La descripción corresponde a la versión "1" del formato SUNW-MSG-ID. Si hay un "1" presente en el campo VER, el código de análisis puede suponer que estarán presentes todos los campos posteriores. Se debe escribir un código de análisis para manejar o ignorar campos adicionales si se especifica un número entero decimal mayor que uno.
SEVERITY	Gravedad de la condición asociada con el problema que activó la alerta. A continuación, se muestra la lista de gravedades.

Nombre de campo	Descripción
EVENT-TIME	Hora correspondiente al evento. La hora tendrá el formato "Day Mon DD HH:MM:SS YYYY" (Día Mes DD HH:MM:SS AAAA) en UTC. Por ejemplo: Wed Aug 14 21:34:22 2019.
PLATFORM	Identificador de plataforma del dispositivo. Este campo es de uso exclusivo del servicio de asistencia de Oracle.
CSN	El número de serie del chasis del dispositivo.
HOSTNAME	Nombre canónico del dispositivo según se define en la configuración de System Identity. Consulte System Identity .
SOURCE	Subsistema dentro del software del dispositivo que emitió el evento. Este campo es de uso exclusivo del servicio de asistencia de Oracle.
REV	Revisión interna del subsistema. Este campo es de uso exclusivo del servicio de asistencia de Oracle.
EVENT-ID	Identificador único universal (UUID) asociado con este evento. El sistema de gestión de fallos de Oracle asocia el UUID con cada alerta y diagnóstico de error, de manera tal que los administradores puedan recopilar y correlacionar múltiples mensajes asociados con una única condición y puedan detectar mensajes duplicados. El personal del servicio de asistencia de Oracle puede utilizar EVENT-ID para recuperar información post mortem adicional asociada con el problema, lo cual puede ayudar a Oracle a encontrar una respuesta para el problema.
DESC	Descripción de la condición asociada con el evento.
AUTO-RESPONSE	Respuesta automática al problema, si la hubiera, proporcionada por el software de gestión de fallos incluido en el sistema. Las respuestas automáticas incluyen capacidades, como la de desconectar discos con errores, chips de memoria de DRAM y núcleos centrales de procesador de manera preventiva.
REC-ACTION	Acción de servicio recomendada. Comprende un breve resumen de la acción recomendada; sin embargo, los administradores deben consultar el artículo informativo y esta documentación para obtener información sobre todo el procedimiento de reparación.

El campo SEVERITY se configurará con uno de los siguientes valores:

TABLA 114 Campos de gravedad de Syslog

Gravedad	Nivel de Syslog	Descripción
Minor (Menor)	LOG_WARNING	Se produjo un inconveniente que en la actualidad no afecta el servicio,

Gravedad	Nivel de Syslog	Descripción
		pero el problema se debe corregir antes de que se torne más grave.
Mayor (Grave)	LOG_ERR	Se produjo un problema que afecta el servicio, pero no seriamente.
Crítico	LOG_CRIT	Se produjo un problema que afecta seriamente el servicio y requiere corrección inmediata.

Ejemplo de configuración de un receptor Oracle Solaris (CLI)

La mayoría de los sistemas operativos incluyen un receptor Syslog, pero es posible que se requieran algunos pasos de configuración para activarlo. Para obtener información específica sobre la configuración del receptor Syslog, consulte la documentación del sistema operativo o del software de gestión.

Oracle Solaris incluye un `syslogd` que puede actuar como receptor Syslog, pero la capacidad de recepción remota está desactivada por defecto. Para activar Oracle Solaris para recibir tráfico de Syslog, utilice `svccfg` y `svcadm` para modificar la configuración de Syslog de la siguiente manera:

```
# svccfg -s system/system-log setprop config/log_from_remote = true
# svcadm restart system/system-log
```

Oracle Solaris `syslogd` solo comprende el protocolo Syslog clásico. Consulte la página del comando `man syslog.conf(4)` de Oracle Solaris para obtener información sobre cómo configurar el filtrado y el registro de los mensajes recibidos.

Por defecto, Oracle Solaris `syslogd` registra mensajes en `/var/adm/messages` y se registra una alerta de prueba de la siguiente manera:

```
Aug 14 21:34:22 poptart.example.us.com poptart ak: SUNW-MSG-ID: AK-8000-LM, \
TYPE: alert, VER: 1, SEVERITY: Minor\nEVENT-TIME: Wed Aug 14 21:34:22 2019\n\
PLATFORM: i86pc, CSN: 12345678, HOSTNAME: poptart\n\
SOURCE: jsui.359, REV: 1.0\n\
EVENT-ID: 92dfeb39-6e15-e2d5-a7d9-dc3e221becea\n\
DESC: A test alert has been posted.\n\
AUTO-RESPONSE: None.\nIMPACT: None.\nREC-ACTION: None.
```

Ejemplo de configuración de un receptor Linux (CLI)

La mayoría de los sistemas operativos incluyen un receptor Syslog, pero es posible que se requieran algunos pasos de configuración para activarlo. Para obtener información específica sobre la configuración del receptor Syslog, consulte la documentación del sistema operativo o del software de gestión.

La mayoría de las distribuciones de Linux incluyen un daemon syslogd(8) que puede actuar como receptor Syslog, pero la capacidad de recepción remota está desactivada por defecto. Para activar Linux para recibir tráfico de Syslog, edite el archivo de configuración `/etc/sysconfig/syslog` de manera tal que se incluya la opción `-r` (activa el registro remoto):

```
SYSLOGD_OPTIONS="-r -m 0"
```

Luego, reinicie el servicio de registro:

```
# /etc/init.d/syslog stop
# /etc/init.d/syslog start
```

Algunas distribuciones de Linux tienen un filtro de paquetes `ipfilter` que rechazará paquetes UDP de Syslog UDP por defecto y que se debe modificar para permitirlos. En estas distribuciones, utilice un comando similar al siguiente para agregar una regla INPUT para aceptar los paquetes UDP de Syslog:

```
# iptables -I INPUT 1 -p udp --sport 514 --dport 514 -j ACCEPT
```

Por defecto, Linux `syslogd` registra mensajes en `/var/log/messages` y se registra una alerta de prueba de la siguiente manera:

```
Aug 12 22:03:15 192.168.1.105 poptart ak: SUNW-MSG-ID: AK-8000-LM, \
TYPE: alert, VER: 1, SEVERITY: Minor EVENT-TIME: Mon Aug 12 22:03:14 2019 \
PLATFORM: i86pc, CSN: 12345678, HOSTNAME: poptart SOURCE: jsui.3775, REV: 1.0 \
EVENT-ID: 9d40db07-8078-4b21-e64e-86e5cac90912 \
DESC: A test alert has been posted. AUTO-RESPONSE: None. IMPACT: None. \
REC-ACTION: None.
```

Configuración de identidad del sistema

Este servicio ofrece configuración para el nombre del sistema y su ubicación, y un mensaje de inicio de sesión del sistema opcional que aparece al iniciar sesión. Posiblemente deba cambiar estos valores si el dispositivo se traslada a otra ubicación de la red o se utiliza con un propósito diferente. Para cambiar estos datos en la BUI, vaya a Configuración > Servicio > Identidad de sistema. Para acceder a los mismos datos en la CLI, vaya al contexto `configuration service identity`.

Propiedades y logs de la identidad del sistema

Las propiedades de Identidad de sistema se describen en la siguiente tabla.

TABLA 115 Propiedades de identidad del sistema

Texto de la BUI	Propiedad de la CLI	Descripción
Nombre de sistema	<code>nodename</code>	Nombre canónico único que identifica el dispositivo y aparece en la interfaz de usuario. Este nombre es independiente de los nombres

Texto de la BUI	Propiedad de la CLI	Descripción
		DNS que se usan para conectarse al sistema (que se configurarían en los servidores DNS remotos). Este nombre se puede cambiar en cualquier momento.
Ubicación de sistema	syslocation	Cadena de texto que describe la ubicación física del dispositivo. Si SNMP está activado, se exporta como la cadena <i>syslocation</i> en MIB-II.
Mensaje de inicio de sesión del sistema	loginmessage	El mensaje de inicio de sesión del sistema opcional puede configurarse en cualquier momento. El mensaje aparece tanto en la BUI como en la CLI. En la BUI, el mensaje aparece en la esquina superior izquierda de la pantalla principal de inicio de sesión. Los usuarios deben hacer clic en el botón Continuar para iniciar sesión. En la CLI, el mensaje aparece inmediatamente arriba del indicador después de iniciar sesión.

Los cambios realizados en las propiedades de los servicios se documentan en las secciones [Configuración de las propiedades de los servicios \(BUI\) \[328\]](#) y [Configuración de las propiedades de los servicios \(CLI\) \[329\]](#). Los nombres de propiedades de la CLI son versiones más abreviadas que las mencionadas anteriormente.

TABLA 116 Logs de identidad del sistema

Log	Descripción
system-identity:node	Registra los eventos y los errores del servicio de identidad del sistema.

Para ver los logs de servicio, consulte [“Uso de logs” en el Manual de servicio del cliente de Oracle ZFS Storage Appliance Customer](#).

Configuración de TFTP

El protocolo trivial de transferencia de archivos (TFTP) es un protocolo simple para transferir archivos. TFTP está diseñado para ser pequeño y fácil de implementar; por lo tanto, carece de la mayoría de las funciones de un FTP regular. TFTP únicamente lee y escribe archivos (o correo) desde/hacia un servidor remoto. No puede mostrar directorios y, en la actualidad, no ofrece la autenticación de usuarios.

TABLA 117 Propiedades de TFTP

Propiedad	Descripción
Directorio raíz por defecto	Ubicación del inicio de sesión de TFTP. El valor por defecto es <code>/export</code> y corresponde al elemento superior de

Propiedad	Descripción
	la jerarquía de recursos compartidos. Todos los usuarios serán direccionados a esta ubicación cuando inicien sesión después de autenticarse correctamente con el servicio TFTP.

Para usar TFTP con un recurso compartido, consulte [Agregación de acceso TFTP a un recurso compartido \(BUI\) \[478\]](#).

▼ Agregación de acceso TFTP a un recurso compartido (BUI)

1. **Vaya a Configuración > Servicios.**
2. **Compruebe que el servicio TFTP esté activado y en línea. De no ser así, actívelo.**
3. **Vaya a Shares (Recursos compartidos) > Shares (Recursos compartidos) y seleccione o agregue un recurso compartido.**
4. **Vaya al separador Protocolos (Protocolos) y compruebe que el acceso TFTP esté activado.**
5. **(Opcional) Configure el acceso de modo de recurso compartido en solo lectura o lectura/escritura.**

Configuración de análisis de virus

El servicio de análisis de virus analiza el sistema de archivos para determinar la presencia de virus. Cuando se accede a un archivo desde algún protocolo, el servicio de análisis de virus primero analiza el archivo y, si encuentra algún virus, deniega el acceso y pone el archivo en cuarentena. Una vez que el archivo ha sido analizado con las definiciones de virus más recientes, no se lo vuelve a analizar hasta la siguiente modificación. Es posible que los archivos a los que se accede mediante clientes NFS que tienen datos de archivos almacenados en caché o a los que el servidor NFSv4.0 o NFSv4.1 han delegado privilegios de lectura no se pasen de inmediato a cuarentena.

Para configurar el análisis de virus, consulte las siguientes secciones:

- [Configuración de análisis de virus para un recurso compartido \(BUI\) \[479\]](#)
- [“Propiedades y logs de análisis de virus” \[479\]](#)
- [“Extensiones de archivo de análisis de virus” \[480\]](#)

- [“Motores de análisis” \[481\]](#)

▼ Configuración de análisis de virus para un recurso compartido (BUI)

1. Vaya a Configuration (Configuración) > Services (Servicios) > Virus Scan (Análisis de virus).
2. Active el servicio.
3. Configure las propiedades adecuadas.
4. Haga clic en APPLY (Aplicar) para confirmar la configuración.
5. Vaya a Shares (Recursos compartidos).
6. Edite un sistema de archivos o un proyecto.
7. Seleccione el separador General.
8. Active la opción Virus scan (Análisis de virus).

Temas relacionados

- [“Propiedades y logs de análisis de virus” \[479\]](#)
- [“Extensiones de archivo de análisis de virus” \[480\]](#)
- [“Motores de análisis” \[481\]](#)

Propiedades y logs de análisis de virus

TABLA 118 Propiedades de los análisis de virus

Propiedad	Descripción
Tamaño máximo de archivo para analizar	Los archivos con un tamaño mayor que el especificado no se analizan para evitar que el rendimiento se vea afectado de manera significativa. Es poco probable que estos archivos grandes sean ejecutables (por ejemplo, archivos de bases de datos), de manera que es menos probable que representen un riesgo para los clientes vulnerables. El valor por defecto es 1 GB.
Permitir acceso a archivos que exceden el tamaño de archivo máximo	Esta opción está activada por defecto y permite el acceso a los archivos cuyo tamaño es mayor que el

Propiedad	Descripción
	tamaño máximo de análisis (y que, por lo tanto, no se analizan antes de devolverlos a los clientes). Los administradores de un sitio que tienen requisitos de seguridad más estrictos pueden decidir desactivar esta opción y aumentar el tamaño máximo de los archivos que se analizan, de manera que todos los archivos accesibles se analicen para comprobar que no tienen virus.

TABLA 119 Logs de análisis de virus

Log	Descripción
vscan	Log del servicio de análisis de virus..

Temas relacionados

- [Configuración de análisis de virus para un recurso compartido \(BUI\) \[479\]](#)
- [“Extensiones de archivo de análisis de virus” \[480\]](#)
- [“Motores de análisis” \[481\]](#)

Extensiones de archivo de análisis de virus

En esta sección, se describe cómo controlar qué archivos se analizan. Con el valor por defecto, " * ", se analizan todos los archivos. El análisis de todos los archivos puede afectar el rendimiento, por lo tanto, puede designar un subconjunto de archivos para analizar.

Por ejemplo, para analizar únicamente los archivos de alto riesgo, incluidos los archivos zip, pero no los archivos cuyos nombres tienen el patrón "data-archive*.zip", puede configurar los siguientes parámetros:

TABLA 120 Extensiones de archivo de análisis de virus

Acción	Patrón
Explorar	exe
Explorar	com
Explorar	bat
Explorar	doc
Explorar	zip
No analizar	data-archive*.zip
No analizar	*

Nota - Debe usar "Don't Scan *" (No analizar *) para excluir todos los tipos de archivos que no se incluyeron explícitamente en la lista de análisis. Un archivo con el nombre `file.name.exe.bat.jpg123` *no* se analizaría, ya que solamente la parte "jpg123" del nombre, la extensión, se compararía con las reglas.

No use los parámetros de exclusión antes de los parámetros de inclusión. Por ejemplo, no use el parámetro "Don't Scan *" (No analizar *) antes de los parámetros de inclusión, ya que de esa forma se excluirán todos los tipos de archivos que siguen.

TABLA 121 Acciones de análisis de virus

Acción	Patrón
No analizar	*
Explorar	exe
Explorar	com
Explorar	bat
Explorar	doc
Explorar	zip
No analizar	data-archive*.zip

Temas relacionados

- [Configuración de análisis de virus para un recurso compartido \(BUI\) \[479\]](#)
- [“Propiedades y logs de análisis de virus” \[479\]](#)
- [“Motores de análisis” \[481\]](#)

Motores de análisis

En esta sección, se especifican los motores de análisis que se deben utilizar. Un motor de análisis es un servidor de análisis de virus externo proporcionado por un tercero con el que el dispositivo se conecta mediante ICAP (protocolo de adaptación de contenidos de Internet, RFC 3507) para analizar los archivos en busca de virus.

TABLA 122 Propiedades de los motores de análisis

Propiedad	Descripción
Activar	Se usa este motor de análisis.
Host	Nombre de host o dirección IP del servidor del motor de análisis.

Propiedad	Descripción
Conexiones máximas	Cantidad máxima de conexiones simultáneas. Algunos motores de análisis funcionan mejor si la cantidad de conexiones se limita a 8.
Puerto	Puerto para el motor de análisis.

Temas relacionados

- [Configuración de análisis de virus para un recurso compartido \(BUI\) \[479\]](#)
- [“Propiedades y logs de análisis de virus” \[479\]](#)
- [“Extensiones de archivo de análisis de virus” \[480\]](#)

Recursos compartidos y proyectos

El producto Oracle ZFS Storage Appliance usa agrupaciones de almacenamiento, proyectos y recursos compartidos para organizar los datos. Los recursos compartidos son los sistemas de archivos y LUN exportados mediante protocolos de datos admitidos a los clientes del dispositivo. Todos los recursos compartidos de un proyecto pueden compartir valores de configuración en común, y se pueden aplicar cuotas en el nivel del proyecto además del nivel de recursos compartidos. Para obtener más información sobre cómo el dispositivo organiza los datos, consulte [“Acerca de las agrupaciones de almacenamiento, los proyectos y los recursos compartidos” \[500\]](#).

Para crear y modificar proyectos, realice las siguientes tareas:

- Creación de un proyecto: [BUI](#), [CLI](#)
- Edición de un proyecto: [BUI](#), [CLI](#)
- Cambio de nombre de un proyecto: [BUI](#), [CLI](#)
- Supresión de un proyecto: [BUI](#), [CLI](#)

Para crear y modificar sistemas de archivos y LUN, realice las siguientes tareas:

- Creación de un sistema de archivos o un LUN en un proyecto: [BUI](#), [CLI](#)
- Edición de un sistema de archivos o un LUN: [BUI](#), [CLI](#)
- Cambio de nombre de un sistema de archivos o un LUN: [BUI](#), [CLI](#)
- Movimiento de un sistema de archivos o un LUN a otro proyecto: [BUI](#), [CLI](#)
- Supresión de un sistema de archivos o un LUN: [BUI](#), [CLI](#)
- Configuración de cuotas de usuarios o grupos: [BUI](#), [CLI](#)

Para obtener más información acerca de la manera en que el dispositivo organiza el almacenamiento, consulte los siguientes temas:

- [“Acerca de las agrupaciones de almacenamiento, los proyectos y los recursos compartidos” \[500\]](#)
- [“Gestión de espacio de recursos compartidos” \[539\]](#)
- [“Propiedades de proyectos y recursos compartidos” \[502\]](#)
- [“Trabajo con espacio de nombres del sistema de archivos” \[544\]](#)
- [“Estadísticas de uso del recurso compartido” \[546\]](#)

- [“Protocolos de recursos compartidos y proyectos” \[547\]](#)
- [“Listas de control de acceso para sistemas de archivos” \[564\]](#)
- [“Trabajo con esquemas” \[571\]](#)
- [Instantáneas y clones \[589\]](#)
- [Replicación remota \[623\]](#)

▼ Creación de un proyecto (BUI)

Los proyectos heredan las propiedades de la agrupación principal. Los proyectos heredan las propiedades del proyecto principal. Para ver una lista de las propiedades que se pueden heredar, consulte [“Propiedades heredadas” \[503\]](#).

Un proyecto creado en una agrupación cifrada se cifra automáticamente. No se puede crear un proyecto no cifrado en una agrupación cifrada.

Utilice este procedimiento para crear un proyecto no cifrado. Para crear un proyecto cifrado, ya sea en una agrupación cifrada o en una no cifrada, consulte [Creación de un proyecto cifrado \(BUI\) \[816\]](#).

1. **Vaya a Recursos compartidos > Proyectos.**
2. **Haga clic en el ícono de agregación  que se encuentra junto a Proyectos o en el panel Proyectos expandido. Para expandir el panel Proyectos, haga clic en el ícono de la flecha.**
3. **En el cuadro de diálogo Crear proyecto, introduzca un nombre para el proyecto nuevo.**

El nombre debe tener entre 1 y 64 caracteres de longitud. El nombre no puede comenzar con un punto (.) ni puede incluir espacios. Los caracteres permitidos son los alfanuméricos y los siguientes caracteres especiales:

_ - . :
4. **Establezca las propiedades correspondientes a este proyecto.**

Las propiedades de los proyectos se describen en [“Propiedades de proyecto” \[517\]](#).
5. **Haga clic en APLICAR.**

El proyecto nuevo se agrega a la lista Proyectos.

Temas relacionados

- [“Propiedades de proyecto” \[517\]](#)

- [Creación de un proyecto cifrado \(BUI\) \[816\]](#)

▼ Creación de un proyecto (CLI)

Los proyectos heredan las propiedades de la agrupación principal. Los proyectos heredan las propiedades del proyecto principal. Para ver una lista de las propiedades que se pueden heredar, consulte [“Propiedades heredadas” \[503\]](#).

Un proyecto creado en una agrupación cifrada se cifra automáticamente. No se puede crear un proyecto no cifrado en una agrupación cifrada.

Utilice este procedimiento para crear un proyecto no cifrado. Para crear un proyecto cifrado, ya sea en una agrupación cifrada o en una no cifrada, consulte [Creación de un proyecto cifrado \(CLI\) \[817\]](#).

1. Vaya a shares.

```
hostname:> shares
```

2. Introduzca el comando `project` y un nombre para el proyecto.

El nombre debe tener entre 1 y 64 caracteres de longitud. El nombre no puede comenzar con un punto (.) ni puede incluir espacios. Los caracteres permitidos son los alfanuméricos y los siguientes caracteres especiales:

```
_ - . : 
```

```
hostname:shares> project home
```

3. Utilice los comandos `get` y `set` para establecer las propiedades correspondientes a este proyecto.

Las propiedades de los proyectos se describen en [“Propiedades de proyecto” \[517\]](#).

4. Introduzca el comando `commit`.

```
hostname:shares home> commit
```

Temas relacionados

- [“Propiedades de proyecto” \[517\]](#)
- [Creación de un proyecto cifrado \(CLI\) \[817\]](#)

▼ Edición de un proyecto (BUI)

Para modificar las propiedades de un proyecto, siga estos pasos.

1. **Vaya a Recursos compartidos > Proyectos.**
2. **Seleccione un proyecto de una de las siguientes formas:**
 - Mueva el cursor sobre el proyecto deseado y haga clic en el ícono de edición .
 - Haga doble clic en el nombre del proyecto
 - Haga clic en el ícono de flecha que se encuentra junto a Proyectos para expandir el panel y, a continuación, haga clic en el nombre del proyecto.

Se selecciona el proyecto y aparecen separadores para editar las propiedades.
3. **Haga clic en uno de los separadores para editar las propiedades del proyecto.**
4. **Modifique las propiedades del proyecto según sea necesario.**

Las propiedades de los proyectos se describen en [“Propiedades de proyecto” \[517\]](#).

Temas relacionados

- [Instantáneas y clones \[589\]](#)
- [Replicación remota \[623\]](#)

▼ Edición de un proyecto (CLI)

Para modificar las propiedades de un proyecto, siga estos pasos.

1. **Vaya a shares.**
`hostname:> shares`
2. **Introduzca `select` y un nombre de proyecto.**
`hostname:shares> select home`
3. **Para que se muestren las propiedades del proyecto, use el comando `get`.**
4. **Para modificar las propiedades del proyecto, use el comando `set`. Las propiedades y los valores de los proyectos se describen en [“Propiedades de proyecto” \[517\]](#).**

Por ejemplo, para activar `vscan` para este proyecto, introduzca el siguiente comando:

`hostname:shares home >set vscan=true`
5. **Escriba `commit`.**
`hostname:shares home> commit`

▼ Cambio de nombre de un proyecto (BUI)



Atención - El cambio de nombre del proyecto interrumpe las operaciones de E/S del cliente que estén activas.

1. **Desconecte los clientes activos que estén conectados al proyecto.**
2. **Vaya a Recursos compartidos > Proyectos.**
3. **En la lista Proyectos, haga clic en el nombre del proyecto.**
4. **Introduzca el nombre nuevo para el proyecto.**

El nombre debe tener entre 1 y 64 caracteres de longitud. El nombre no puede comenzar con un punto (.) ni puede incluir espacios. Los caracteres permitidos son los alfanuméricos y los siguientes caracteres especiales:

_ - . :

5. **Pulse Intro.**
6. **Haga clic en Aceptar para confirmar.**

▼ Cambio de nombre de un proyecto (CLI)



Atención - El cambio de nombre del proyecto interrumpe las operaciones de E/S del cliente que estén activas.

1. **Desconecte los clientes activos que estén conectados al proyecto.**
2. **Vaya a shares.**
3. **Para ver los proyectos, use el comando `list`.**

```
hostname:shares> list
default
home
```

4. **Introduzca `rename`, el nombre actual del proyecto y el nombre nuevo del proyecto.**

El nombre debe tener entre 1 y 64 caracteres de longitud. El nombre no puede comenzar con un punto (.) ni puede incluir espacios. Los caracteres permitidos son los alfanuméricos y los siguientes caracteres especiales:

```
_ _ _ :  
hostname:shares> rename home project1
```

5. **Para confirmar que se haya cambiado el nombre del proyecto, use el comando `list`.**

```
hostname:shares> list  
default  
project1
```

Temas relacionados

- [“Propiedades de proyecto” \[517\]](#)

▼ Supresión de un proyecto (BUI)



Atención - La supresión de un proyecto destruye todos los datos incluidos en el proyecto, ya que se suprimen los sistemas de archivos y los LUN.

1. **Vaya a Recursos compartidos > Proyectos.**
2. **Pase el cursor del mouse sobre el proyecto que desea suprimir y haga clic en el ícono de destrucción .**
3. **Haga clic en Aceptar.**
4. **Para supervisar la cantidad de espacio que se debe reclamar en la agrupación de almacenamiento si se aceptó la actualización diferida de supresión asíncrona de juego de datos (OS8.7.0), vaya a Configuración > Almacenamiento, seleccione la agrupación de almacenamiento apropiada y tome nota de la cantidad de espacio en el campo Asynchronous Dataset Destroy (Destrucción asíncrona de juego de datos).**

Una vez que finaliza la operación, no se muestra Asynchronous Dataset Destroy (Destrucción asíncrona de juego de datos).

▼ Supresión de un proyecto (CLI)



Atención - La supresión de un proyecto destruye todos los datos incluidos en el proyecto, ya que se suprimen los sistemas de archivos y los LUN.

1. Vaya a shares.

```
hostname:> shares
```

2. Escriba `destroy` y un nombre de proyecto.

```
hostname:shares> destroy home
```

3. Introduzca `y`.

```
This will destroy all data in "home"! Are you sure? (Y/N)
hostname:shares> y
```

4. Para supervisar la cantidad de espacio que se debe reclamar en la agrupación de almacenamiento si se aceptó la actualización diferida de supresión asíncrona de juego de datos (OS8.7.0), introduzca `cd ..` para volver al contexto raíz. Introduzca `configuration storage` y `ls` para mostrar las propiedades de la agrupación de almacenamiento. Para la agrupación apropiada, tome nota de la cantidad de espacio para la propiedad `async_destroy_reclaim_space`.

Una vez que finaliza la operación, se muestra 0 (cero).

▼ Creación de un sistema de archivos o un LUN en un proyecto (BUI)

Los sistemas de archivos y los LUN que se crean dentro de un proyecto heredan las propiedades del proyecto principal. Para ver una lista de las propiedades que se pueden heredar, consulte [“Propiedades heredadas” \[503\]](#).

Un sistema de archivos o LUN creado dentro de un proyecto cifrado se cifra automáticamente. No se puede crear un recurso compartido no cifrado en un proyecto cifrado.

Utilice este procedimiento para crear un recurso compartido no cifrado. Para crear un recurso compartido cifrado, ya sea en un proyecto cifrado o en uno no cifrado, consulte [Creación de sistemas de archivos o LUN cifrados \(BUI\) \[821\]](#).

Antes de empezar Si está agregando un sistema de archivos o un LUN a un proyecto que no es el proyecto predeterminado, el proyecto en cuestión ya debe existir. Para crear un proyecto nuevo, consulte [Creación de un proyecto \(BUI\) \[484\]](#).

1. Vaya a Recursos compartidos > Recursos compartidos.**2. Seleccione Sistemas de archivos o LUN.****3. Haga clic en el ícono de agregación .**

4. Complete los campos del cuadro de diálogo Crear sistema de archivos o Crear LUN.

- En el caso de los sistemas de archivos, seleccione un proyecto e introduzca un nombre.
- En el caso de los LUN, seleccione un proyecto, introduzca un nombre y especifique el tamaño del volumen.

El nombre debe tener entre 1 y 64 caracteres de longitud. El nombre no puede comenzar con un punto (.) ni puede incluir espacios. Los caracteres permitidos son los alfanuméricos y los siguientes caracteres especiales:

_ - . :

5. Configure otras propiedades.

Las propiedades del recurso compartido se describen en [“Propiedades de sistema de archivos” \[525\]](#) y [“Propiedades de LUN” \[534\]](#).

6. Haga clic en APLICAR.

Temas relacionados

- [“Propiedades de proyectos y recursos compartidos” \[502\]](#)
- [Creación de sistemas de archivos o LUN cifrados \(BUI\) \[821\]](#)

▼ Creación de un sistema de archivos o un LUN en un proyecto (CLI)

Los sistemas de archivos y los LUN que se crean dentro de un proyecto heredan las propiedades del proyecto principal. Para ver una lista de las propiedades que se pueden heredar, consulte [“Propiedades heredadas” \[503\]](#).

Un sistema de archivos o LUN creado dentro de un proyecto cifrado se cifra automáticamente. No se puede crear un recurso compartido no cifrado en un proyecto cifrado.

Utilice este procedimiento para crear un recurso compartido no cifrado. Para crear un recurso compartido cifrado, ya sea en un proyecto cifrado o en uno no cifrado, consulte [Creación de sistemas de archivos o LUN cifrados \(CLI\) \[823\]](#).

Si está agregando un sistema de archivos o un LUN a un proyecto que no es el proyecto predeterminado, el proyecto en cuestión ya debe existir. Para crear un proyecto nuevo, consulte [Creación de un proyecto \(CLI\) \[485\]](#).

1. Vaya a `shares`.

2. Seleccione el proyecto.

Si el proyecto que está seleccionado no es el que desea, use el comando `select project-name` para seleccionar uno distinto.

3. Cree el sistema de archivos o LUN.

Introduzca `filesystem filesystem-name` O `lun lun-name`.

El nombre debe tener entre 1 y 64 caracteres de longitud. El nombre no puede comenzar con un punto (.) ni puede incluir espacios. Los caracteres permitidos son los alfanuméricos y los siguientes caracteres especiales:

_ - . :

En el ejemplo siguiente, se crea un sistema de archivos llamado `fs-1` en el proyecto `default`.

```
hostname:shares default> filesystem fs-1
hostname:shares default/fs-1 (uncommitted)>
```

4. Si está creando un LUN, introduzca `set volsize=` y el tamaño del volumen.

```
hostname:shares default/lun1 (uncommitted)> set volsize=2G
volsize = 2G (uncommitted)
```

5. Introduzca el comando `commit`.

```
hostname:shares default/fs-1 (uncommitted)> commit
```

6. Seleccione el sistema de archivos o LUN.

Introduzca `select filesystem-name` O `select lun-name`.

```
hostname:shares default> select fs-1
```

7. Utilice los comandos `get` y `set` para establecer las propiedades correspondientes a este sistema de archivos o LUN.

Las propiedades del recurso compartido se describen en [“Propiedades de sistema de archivos” \[525\]](#) y [“Propiedades de LUN” \[534\]](#).

8. Introduzca el comando `commit`.**Temas relacionados**

- [“Propiedades de proyectos y recursos compartidos” \[502\]](#)
- [Creación de sistemas de archivos o LUN cifrados \(CLI\) \[823\]](#)

▼ Edición de un sistema de archivos o un LUN (BUI)

Para modificar las propiedades de un sistema de archivos o un LUN individuales, siga estos pasos:

1. **Vaya a Recursos compartidos > Recursos compartidos.**
2. **Seleccione Sistemas de archivos o LUN.**
3. **Edite el sistema de archivos o LUN.**
 - Pase el cursor del mouse sobre el sistema de archivos o el LUN y haga clic en el ícono de edición .
 - Haga doble clic en el sistema de archivos o LUN que desee editar.

Se muestran las propiedades generales del sistema de archivos o el LUN.
4. **Haga clic en uno de los separadores: Protocolos, Acceso, Instantáneas o Replicación.**
5. **Modifique las propiedades del sistema de archivos o LUN.**

Las propiedades del recurso compartido se describen en [“Propiedades de sistema de archivos” \[525\]](#) y [“Propiedades de LUN” \[534\]](#).
6. **Haga clic en APLICAR.**

Temas relacionados

- [“Propiedades de proyectos y recursos compartidos” \[502\]](#)

▼ Edición de un sistema de archivos o un LUN (CLI)

Para modificar las propiedades de un sistema de archivos o un LUN individuales, siga estos pasos:

1. **Seleccione el sistema de archivos o LUN que desee cambiar.**
 - a. **Vaya a shares.**
 - b. **Seleccione el proyecto.**

Si el proyecto que está seleccionado no es el que desea, use el comando `select project-name` para seleccionar uno distinto.

c. Seleccione el sistema de archivos o LUN.

Introduzca `select filesystem-name` O `select lun-name`.

2. Use el comando `get` para ver las propiedades del recurso compartido.
3. Utilice el comando `set` para modificar las propiedades del sistema de archivos o LUN.

Las propiedades del recurso compartido se describen en [“Propiedades de sistema de archivos” \[525\]](#) y [“Propiedades de LUN” \[534\]](#).

4. Introduzca el comando `commit`.

Temas relacionados

- [“Propiedades de proyectos y recursos compartidos” \[502\]](#)

▼ Cambio de nombre de un sistema de archivos o un LUN (BUI)



Atención - El cambio de nombre del recurso compartido interrumpe las operaciones de E/S del cliente que estén activas.

1. Desconecte todos los clientes activos que estén conectados al sistema de archivos o el LUN cuyo nombre desea cambiar.
2. Vaya a **Recursos compartidos > Recursos compartidos**.
3. Seleccione **Sistemas de archivos o LUN**.
4. Haga clic en el nombre del sistema de archivos o del LUN en la lista.
5. Introduzca el nombre nuevo para el sistema de archivos o el LUN.

El nombre debe tener entre 1 y 64 caracteres de longitud. El nombre no puede comenzar con un punto (.) ni puede incluir espacios. Los caracteres permitidos son los alfanuméricos y los siguientes caracteres especiales:

_ - . :

6. **Pulse Intro.**
7. **Haga clic en Aceptar para confirmar.**

Temas relacionados

- [“Propiedades de sistema de archivos” \[525\]](#)
- [“Propiedades de LUN” \[534\]](#)

▼ Cambio de nombre de un sistema de archivos o un LUN (CLI)



Atención - El cambio de nombre del recurso compartido interrumpe las operaciones de E/S del cliente que estén activas.

1. **Desconecte todos los clientes activos que estén conectados al sistema de archivos o al LUN.**
2. **Vaya a `shares`.**

```
hostname:> shares
```
3. **Para ver los proyectos, use el comando `list`.**

```
hostname:shares> list
default
home
```
4. **Introduzca `select` y el nombre del proyecto que contiene el sistema de archivos o el LUN cuyo nombre desea cambiar.**

```
hostname:shares> select default
```

5. **Introduzca `rename`, el nombre actual del sistema de archivos o del LUN y el nombre nuevo del sistema de archivos o del LUN.**

El nombre debe tener entre 1 y 64 caracteres de longitud. El nombre no puede comenzar con un punto (.) ni puede incluir espacios. Los caracteres permitidos son los alfanuméricos y los siguientes caracteres especiales:

_ - . :

```
hostname:shares default> rename fs-1 fs-2
```

Temas relacionados

- [“Propiedades de sistema de archivos” \[525\]](#)
- [“Propiedades de LUN” \[534\]](#)

▼ Movimiento de un sistema de archivos o un LUN a otro proyecto (BUI)

Los sistemas de archivos y los LUN que se encuentran dentro de un proyecto heredan las propiedades del proyecto.

1. **Vaya a Recursos compartidos > Recursos compartidos.**
2. **Seleccione Sistemas de archivos o LUN.**
3. **Pase el cursor del mouse sobre el sistema de archivos o el LUN y haga clic en el ícono de movimiento .**
4. **Arrastre el sistema de archivos o el LUN al otro proyecto debajo de Proyectos.**
Si el panel del proyecto no está expandido, se expandirá automáticamente hasta que se coloque el recurso compartido en un proyecto.

Temas relacionados

- [“Propiedades de sistema de archivos” \[525\]](#)
- [“Propiedades de LUN” \[534\]](#)

▼ Movimiento de un sistema de archivos o un LUN a otro proyecto (CLI)

Los sistemas de archivos y los LUN que se encuentran dentro de un proyecto heredan las propiedades del proyecto.

1. **Vaya a `shares` y seleccione el proyecto que contenga el sistema de archivos o el LUN que desee mover.**
En este ejemplo, el proyecto `default` contiene el sistema de archivos o el LUN que se desea mover.

```
hostname> shares  
hostname:shares> select default
```

2. **Introduzca `move`, el nombre del sistema de archivos o del LUN que desea mover y el nombre del proyecto de destino.**

```
hostname:shares default> move foo home
```

Temas relacionados

- [“Propiedades de sistema de archivos” \[525\]](#)
- [“Propiedades de LUN” \[534\]](#)

▼ Supresión de un sistema de archivos o un LUN (BUI)



Atención - La supresión de un sistema de archivos o un LUN destruye todos los datos que se encuentran en el recurso compartido. Esta operación no se puede deshacer.

1. **Vaya a Recursos compartidos > Recursos compartidos.**
2. **Seleccione Sistemas de archivos o LUN.**
3. **Pase el cursor del mouse sobre el sistema de archivos o el LUN que desea suprimir y haga clic en el ícono de destrucción .**
4. **Haga clic en Aceptar.**
5. **Para supervisar la cantidad de espacio que se debe reclamar en la agrupación de almacenamiento si se aceptó la actualización diferida de supresión asíncrona de juego de datos (OS8.7.0), vaya a Configuración > Almacenamiento, seleccione la agrupación de almacenamiento apropiada y tome nota de la cantidad de espacio en el campo Asynchronous Dataset Destroy (Destrucción asíncrona de juego de datos).**

Una vez que finaliza la operación, no se muestra Asynchronous Dataset Destroy (Destrucción asíncrona de juego de datos).

Temas relacionados

- [“Propiedades de sistema de archivos” \[525\]](#)
- [“Propiedades de LUN” \[534\]](#)

▼ Supresión de un sistema de archivos o un LUN (CLI)



Atención - La supresión de un sistema de archivos o un LUN destruye todos los datos que se encuentran en el recurso compartido. Esta operación no se puede deshacer.

1. Vaya a shares.

```
hostname> shares
```

2. Introduzca `select` y el nombre del proyecto que contiene el sistema de archivos o el LUN.

```
hostname:shares> select default
```

3. Introduzca `select` y el nombre del sistema de archivos o del LUN.

```
hostname:shares default>select fs-1
```

4. Introduzca `destroy`.

```
hostname:shares default/fs-1> destroy
This will destroy all data in "fs-1"! Are you sure? (Y/N)
```

5. Introduzca `Y`.

```
hostname:shares default> y
```

6. Para supervisar la cantidad de espacio que se debe reclamar en la agrupación de almacenamiento si se aceptó la actualización diferida de supresión asíncrona de juego de datos (OS8.7.0), introduzca `cd ../../` para volver al contexto raíz. Introduzca `configuration storage` y `ls` para mostrar las propiedades de la agrupación de almacenamiento. Para la agrupación apropiada, tome nota de la cantidad de espacio para la propiedad `async_destroy_reclaim_space`.

Una vez que finaliza la operación, se muestra 0 (cero).

Temas relacionados

- [“Propiedades de sistema de archivos” \[525\]](#)
- [“Propiedades de LUN” \[534\]](#)

▼ Configuración de cuotas de usuarios o grupos (BUI)

Se pueden configurar cuotas para un usuario o un grupo en el nivel del proyecto o el sistema de archivos.

1. **Vaya a Recursos compartidos > Recursos compartidos y seleccione un proyecto o un recurso compartido.**
2. **Haga clic en el separador General.**
3. **En la sección Uso de espacio - Usuarios y grupos, seleccione Usuario, Grupo o Usuario o grupo en el menú desplegable.**

Nota - Los usuarios que no consuman espacio en el sistema de archivos y no tengan cuotas configuradas no aparecen en la lista de usuarios activos.

4. **Para establecer una cuota en el nivel del proyecto, seleccione una de tres opciones:**
 - Ninguna: no se define ninguna cuota para este sistema de archivos.
 - Por defecto: se establece la cuota por defecto en el nivel del proyecto. Si no se definió una cuota por defecto, no se aplica ninguna cuota para este sistema de archivos.
 - Haga clic en el botón de radio, introduzca una cuota en el campo del tamaño y seleccione una medida.

5. **Haga clic en APLICAR.**

Las propiedades de cuotas de usuario y grupo se validan aparte de las demás propiedades. Sin embargo, tal vez solo vea un error de validación si se introduce un usuario o un grupo no válidos y alguna otra propiedad no válida. Cuando se corrige un error y se aplican los cambios, se muestran los mensajes de error restantes.

Si aparece un mensaje de error que indica que se introdujo una propiedad no válida, puede tratarse de un usuario o un grupo no válidos, otra propiedad no válida en la página, o ambos. Cuando se corrige una propiedad no válida y se aplican los cambios, se muestran los mensajes de error restantes.

Temas relacionados

- [“Configuración de cuotas de usuarios o grupos” \[542\]](#)

▼ **Configuración de cuotas de usuarios o grupos (CLI)**

Se pueden configurar cuotas para un usuario o un grupo en el nivel del proyecto o el sistema de archivos.

1. **Vaya a `shares`, seleccione un proyecto y, a continuación, seleccione un recurso compartido, como se muestra en este ejemplo:**

```
hostname:> shares select default select eschrock
```

2. Introduzca `users` y, a continuación, `list` para ver los usuarios actuales.

```
hostname:shares default/eschrock> users
hostname:shares default/eschrock users> list
USER      NAME      USAGE  QUOTA  SOURCE
user-000   root      321K   -      -
user-001   ahl       9.94K  -      -
user-002   eschrock  20.0G  -      -
```

Nota - Los usuarios que no consuman espacio en el sistema de archivos y no tengan cuotas configuradas no aparecen en la lista de usuarios activos.

3. Introduzca `select` y el valor `name=` del usuario.

```
hostname:shares default/eschrock users> select name=eschrock
hostname:shares default/eschrock user-002> get
      name = eschrock
      unixname = eschrock
      unixid = 132651
      winname = (unset)
      winid = (unset)
      usage = 20.0G
      quota = (unset)
      source = (unset)
```

4. Introduzca `quota=` y un valor. Introduzca `commit` y `done`.

Nota - Para borrar una cuota, configúrela con el valor `0`.

```
hostname:shares default/eschrock user-002> set quota=100G
      quota = 100G (uncommitted)
hostname:shares default/eschrock user-002> commit
hostname:shares default/eschrock user-002> done
```

5. Para definir una cuota para dicho usuario o grupo, utilice el comando `quota`. Después de este comando, se pueden configurar el nombre y la cuota.

La columna Origen muestra `local` si la cuota se estableció en el nivel del sistema de archivos, `default` si se estableció en el nivel de proyecto o `-` si no se estableció ninguna cuota. En el siguiente ejemplo, la cuota por defecto del usuario establecida en el nivel de usuario es de 50 GB.

Si se estableció una cuota por defecto de usuario o grupo en el nivel de proyecto, este procedimiento sustituye ese valor.

```
hostname:shares default/eschrock users> quota
hostname:shares default/eschrock users quota (uncommitted)> set name=bmc
      name = bmc (uncommitted)
hostname:shares default/eschrock users quota (uncommitted)> set quota=default
      quota = default (uncommitted)
```

```
hostname:shares default/eschrock users quota (uncommitted)> commit
hostname:shares default/eschrock users> list
USER      NAME      USAGE  QUOTA  SOURCE
user-000   root      321K   -      -
user-001   ahl       9.94K  -      -
user-002   eschrock  20.0G  100G   local
user-003   bmc       -      50G    default
```

Temas relacionados

- [“Configuración de cuotas de usuarios o grupos” \[542\]](#)

Acerca de las agrupaciones de almacenamiento, los proyectos y los recursos compartidos

El producto Oracle ZFS Storage Appliance gestiona el almacenamiento físico mediante un modelo de almacenamiento agrupado en el que los sistemas de archivos y los LUN comparten un espacio común. En este tema, se describe cómo se organiza el almacenamiento mediante agrupaciones de almacenamiento, proyectos y recursos compartidos.

Agrupaciones de almacenamiento

El dispositivo se basa en el sistema de archivos ZFS, que coloca a los dispositivos de almacenamiento subyacentes en agrupaciones. Los sistemas de archivos y los LUN, denominados "recursos compartidos" en su juego, se asignan desde esta agrupación de almacenamiento según sea necesario. Antes de crear sistemas de archivos o LUN, primero, debe configurar el almacenamiento en el dispositivo. Una vez que se configura una agrupación de almacenamiento, no es necesario asignar un tamaño estático a los sistemas de archivos, aunque este comportamiento se puede lograr mediante la utilización de cuotas y reservas.

Cuando se admiten varias agrupaciones de almacenamiento, generalmente, no se recomienda este tipo de configuración porque ofrece desventajas significativas, como se describe en la sección [“Configuración del almacenamiento” \[127\]](#). Solo se deben utilizar varias agrupaciones cuando las características de fiabilidad o rendimiento de dos perfiles distintos son considerablemente diferentes, como la agrupación reflejada para bases de datos y una agrupación RAID-Z para cargas de trabajo de transmisión.

Cuando hay varias agrupaciones activas en un único host, la BUI muestra una lista desplegable en la barra de menús que se puede utilizar para pasar de una agrupación a otra. En la CLI, se mostrará el nombre de la agrupación actual entre paréntesis, el cual se podrá cambiar mediante la configuración de la propiedad `pool`. Si existe solo una agrupación configurada, se ocultan estos controles. Cuando se seleccionan varias agrupaciones, la agrupación por defecto elegida por la interfaz de usuario es arbitraria; por lo tanto, cualquier operación de secuencia de

comandos deberá definir el nombre de la agrupación de manera explícita antes de manipular recursos compartidos.

Proyectos

Todos los sistemas de archivos y LUN se agrupan en proyectos. Un proyecto se puede considerar como un grupo de coherencia que define un punto de control administrativo común para la gestión de recursos compartidos. Todos los recursos compartidos de un proyecto pueden compartir configuraciones en común, y se pueden aplicar cuotas tanto en el nivel del proyecto como en el nivel del recurso compartido. Los proyectos también se pueden utilizar únicamente para agrupar recursos compartidos lógicamente relacionados entre sí, de manera que se pueda acceder a sus atributos en común (por ejemplo, espacio acumulado) desde un único punto.

El dispositivo genera un único proyecto por defecto cuando se configura por primera vez una agrupación de almacenamiento. Es posible generar todos los recursos compartidos dentro de este proyecto por defecto, aunque en el caso de entornos de tamaño razonable, se recomienda generar proyectos adicionales, aunque solo sea con fines organizativos.

Recursos compartidos

Los recursos compartidos son los sistemas de archivos y LUN exportados mediante protocolos de datos admitidos a los clientes del dispositivo. Se puede acceder a los sistemas de archivos exportados por medio de SMB, NFS, HTTP/WebDav y FTP. Los LUN exportan volúmenes basados en bloques y se puede acceder a ellos mediante iSCSI o canal de fibra.

La combinación de proyecto y recurso compartido es un identificador único de un recurso compartido dentro de una agrupación. Los proyectos de una agrupación no pueden incluir recursos compartidos que tengan el mismo nombre. Si intenta usar un nombre ya existente para un recurso compartido o cambiar el nombre de un recurso compartido por un nombre que ya está en uso, se produce un error de punto de montaje.

Además de las propiedades por defecto, puede configurar recursos compartidos y proyectos con cualquier número de propiedades adicionales. A estas propiedades se les asignan tipos básicos con fines de validación y se heredan como la mayoría de las otras propiedades estándar. Los valores nunca son consumidos por el software de ninguna manera, y solamente existen para el consumo del usuario final. El esquema de propiedades es global para el sistema, abarca todas las agrupaciones y está sincronizado entre pares de cluster.

Temas relacionados

- [“Gestión de espacio de recursos compartidos” \[539\]](#)
- [“Propiedades de proyectos y recursos compartidos” \[502\]](#)
- [Instantáneas y clones \[589\]](#)

Propiedades de proyectos y recursos compartidos

Todos los proyectos y los recursos compartidos tienen un número de propiedades asociadas que se pueden configurar mediante la BUI o la CLI. Para ver una lista de los nombres y las descripciones de las propiedades, seleccione uno de estos enlaces:

- [“Propiedades heredadas” \[503\]](#)
- [“Propiedades de proyecto” \[517\]](#)
- [“Propiedades de sistema de archivos” \[525\]](#)
- [“Propiedades de LUN” \[534\]](#)

Las propiedades de los proyectos y los recursos compartidos pueden ser de uno de los siguientes tipos:

TABLA 123 Tipos de propiedades de proyectos y recursos compartidos

Tipo de propiedad	Descripción
Heredadas	Las propiedades heredadas, el tipo más común de propiedad, representa la mayoría de las propiedades de recursos compartidos y proyectos configurables. Los recursos compartidos que forman parte de un proyecto pueden tener configuraciones locales para las propiedades o pueden heredar las configuraciones del proyecto principal. De manera predeterminada, los recursos compartidos heredan todas las propiedades del proyecto. Si se cambia una propiedad en un proyecto, todos los recursos compartidos que heredan esa propiedad se actualizan para reflejar el nuevo valor. Cuando se heredan, todas las propiedades tienen el mismo valor que el proyecto principal, excepto las propiedades de SMB y punto de montaje. Cuando se heredan, estas propiedades conectan la configuración del proyecto con su propio nombre de recurso compartido.
Solo lectura	Las propiedades de solo lectura representan estadísticas relacionadas con el proyecto y los recursos compartidos, y no se pueden cambiar. Las propiedades más comunes de este tipo son las estadísticas de uso de espacio.
Gestión de espacio	Las propiedades de gestión de espacio (cuota y reserva) se aplican a los recursos compartidos y a los proyectos, pero no se heredan. Se aplicará un proyecto con una cuota de 100G en todos los recursos compartidos, pero cada recurso compartido individual no tendrá una cuota, salvo que esta se defina explícitamente.
Estáticas (momento de creación)	Las propiedades estáticas se especifican en el momento de creación del sistema de archivos o el LUN, pero no se pueden cambiar después de crear el recurso compartido. Estas propiedades controlan las estructuras de datos en disco y comprenden configuraciones de internacionalización, distinción entre mayúsculas y minúsculas, y tamaño del bloque de volumen.
Predeterminada de proyecto	Las propiedades predeterminadas del proyecto se configuran en el proyecto, pero no lo afectan. Se utilizan para completar la configuración inicial al crear un sistema de archivos o LUN, y pueden resultar útiles cuando los recursos compartidos tienen un juego común de propiedades no heredables. El cambio

Tipo de propiedad	Descripción
	de estas propiedades no afecta los recursos compartidos existentes y las propiedades se pueden cambiar antes o después de la creación del recurso compartido.
Local de sistema de archivos	Las propiedades locales del sistema de archivos solo se aplican a los sistemas de archivos y son propiedades de conveniencia para gestionar el directorio raíz del sistema de archivos. No se pueden configurar en los proyectos. Estas propiedades de control de acceso también pueden ser configuradas por las operaciones de protocolo en banda.
Local de LUN	Las propiedades locales de LUN solo se aplican a los LUN y no se heredan. No se pueden configurar en los proyectos.
Personalizadas	Las propiedades personalizadas son propiedades definidas por el usuario.

Propiedades heredadas

Las propiedades heredadas son las que heredan el valor de su principal. Los proyectos pueden heredar propiedades de su agrupación principal y los recursos compartidos pueden heredarlas de su proyecto principal. Normalmente, las propiedades heredables se pueden configurar de manera explícita en un proyecto o recurso compartido. Cuando un valor se configura de manera explícita para una propiedad inicialmente heredada, esa propiedad es una propiedad local.

La BUI solo permite heredar todas las propiedades a la vez, mientras que la CLI permite heredar propiedades individuales.

Por defecto, los recursos compartidos heredan todas las propiedades de su proyecto principal. Si se cambia una propiedad en un proyecto, todos los recursos compartidos que heredan esa propiedad (esa propiedad no se configuró de forma local) se actualizan para reflejar el nuevo valor. Cuando se heredan, todas las propiedades tienen el mismo valor que el proyecto principal, excepto las propiedades de SMB y punto de montaje. Cuando se heredan, las propiedades de SMB y punto de montaje conectan la configuración del proyecto con su propio nombre de recurso compartido.

Además de las propiedades descritas en las siguientes secciones, se heredan las propiedades de cifrado. Si se cifra una agrupación, todos los proyectos creados en ella heredan la configuración de cifrado de esa agrupación. Si se cifra un proyecto, todos los recursos compartidos creados en él heredan la configuración de cifrado de ese proyecto. Consulte [“Propiedades de cifrado” \[832\]](#). Creación de un proyecto cifrado ([BUI](#), [CLI](#)) y Creación de sistemas de archivos o LUN cifrados ([BUI](#), [CLI](#)).

Para obtener una descripción de la forma en que una restauración de una copia de seguridad puede cambiar la configuración de las propiedades heredadas y la manera de evitar eso, consulte [“Configuración de la propiedad heredada después de la restauración de la copia de seguridad” \[839\]](#).

Punto de montaje

La propiedad Punto de montaje es la ubicación en la que se monta el sistema de archivos. Esta propiedad solo es válida para los sistemas de archivos.

Las siguientes restricciones se aplican a la propiedad de punto de montaje:

- Debe estar en /export
- No puede entrar en conflicto con otro recurso compartido
- No puede entrar en conflicto con otro recurso compartido en un par de cluster para permitir un failover adecuado

Cuando se hereda la propiedad de punto de montaje, el nombre del juego de datos actual se agrega a la configuración de punto de montaje del proyecto y se une mediante una barra inclinada (/). Por ejemplo, si el proyecto `home` tuviera la configuración de punto de montaje `/export/home`, `home/bob` heredaría el punto de montaje `/export/home/bob`.

Los recursos compartidos de SMB se exportan mediante el nombre del recurso, y el punto de montaje no es visible en el protocolo. Sin embargo, incluso los recursos compartidos solo de SMB deben tener un único punto de montaje válido en el dispositivo.

Los puntos de montaje se pueden anidar debajo de los puntos de montaje de otros recursos compartidos, aunque con algunas limitaciones. Para obtener más información, consulte [“Trabajo con espacio de nombres del sistema de archivos” \[544\]](#).

Solo lectura

La propiedad Solo lectura controla si el contenido del sistema de archivos es de solo lectura. Esta propiedad solo es válida para los sistemas de archivos.

Independientemente de la configuración de protocolo, el contenido de un sistema de archivos de solo lectura no se puede modificar. Esta configuración no afecta la capacidad para cambiar el nombre ni las propiedades del sistema de archivos ni para destruirlo. Además, cuando un sistema de archivos es de solo lectura, las propiedades de control de acceso no se pueden modificar, ya que para ello es necesario cambiar los atributos del directorio raíz del sistema de archivos.

Actualización de hora de acceso en el momento de la lectura

La propiedad Actualización de hora de acceso en momento de lectura controla si la hora de acceso a los archivos está actualizada en el momento de la lectura. Esta propiedad solo es válida para los sistemas de archivos.

Según los estándares POSIX, la hora de acceso a un archivo debe reflejar correctamente la última vez que este fue leído. Para ello, se deben enviar datos escritos al sistema de archivos subyacente, incluso para una carga de trabajo que mayormente es de solo lectura. En el caso de los juegos de trabajo compuestos principalmente por lecturas de una gran cantidad de archivos, la desactivación de esta propiedad podría generar mejoras en el rendimiento a costa del cumplimiento de las normas. Estas actualizaciones se producen de manera asíncrona y se agrupan entre sí; por lo tanto, el efecto no debe ser visible, excepto en caso de carga pesada.

Bloqueo no bloqueante obligatorio

La propiedad Bloqueo no bloqueante obligatorio controla si la semántica de bloqueo de SMB tiene prioridad sobre la semántica de POSIX. Esta propiedad solo es válida para los sistemas de archivos.

De forma predeterminada, los sistemas de archivos implementan el comportamiento de los archivos conforme a los estándares POSIX. Estos estándares son fundamentalmente incompatibles con el comportamiento requerido por el protocolo SMB. En los recursos compartidos en los que SMB es el protocolo principal, esta opción siempre debe estar activada. Para cambiar esta propiedad, todos los clientes se deben desconectar y volver a conectar.

Desduplicación de datos

La propiedad Desduplicación de datos controla si se eliminan las copias de datos duplicadas. La desduplicación es un proceso síncrono, de toda la agrupación, basado en bloques y que se puede activar por proyecto o por recurso compartido.

Antes de que se pueda activar la desduplicación en un proyecto o recurso compartido, debe configurar la agrupación de almacenamiento con metadispositivos. Los metadispositivos son dispositivos de caché designados que se utilizan para almacenar tipos específicos de metadatos para optimizar los casos de uso como la desduplicación.

La desduplicación solo está disponible en juegos de datos con un tamaño de registro de 128 KB o superior.

Para activar la desduplicación, seleccione la casilla de control Desduplicación de datos en la pantalla de propiedades generales para proyectos o recursos compartidos. El tamaño de los datos con duplicación anulada, así como la relación de desduplicación, se muestra en el área de uso del panel de control de estado. Los datos escritos con la desduplicación activada se introducen en la tabla de desduplicación indexada por el total de control de datos. La desduplicación fuerza el uso del total de control SHA-256 criptográficamente fuerte. Los datos escritos posteriormente identificarán datos duplicados y solo mantendrán la copia existente en el disco. La desduplicación solo se produce entre bloques del mismo tamaño y con datos escritos

con el mismo tamaño de registro. Para obtener mejores resultados, configure el tamaño del registro con el tamaño de la aplicación que utiliza los datos, y en el caso de cargas de trabajo de transmisión, utilice un tamaño de registro grande.

Nota - A partir de la actualización diferida de deduplicación de datos en OS8.7, si se configura la replicación para un proyecto o un recurso compartido de deduplicación, se ejecutará una prueba de compatibilidad para determinar si el destino de replicación tiene el software y el metadispositivo requeridos para recibir actualizaciones de deduplicación. Si el destino ejecuta OS8.6 o anterior, las actualizaciones de replicación con deduplicación activada generarán un error y se publicará una alerta para indicar que se debe desactivar la deduplicación de datos en el origen. Si el destino ejecuta OS8.7 pero no tiene el metadispositivo requerido, el destino ignorará la propiedad de deduplicación de datos entrante y se publicará una alerta para indicar que el sistema de destino ignorará deliberadamente la configuración de deduplicación durante la recepción de la replicación.

Si un origen que ejecuta OS8.6 o anterior se replica en un destino con deduplicación activada, la prueba de compatibilidad comprobará en el destino la presencia de un metadispositivo o recurso compartido con deduplicación en el paquete. Si la prueba de compatibilidad encuentra alguno de estos elementos, el destino conservará la configuración de deduplicación al recibir actualizaciones de replicación.

Si los datos no contienen duplicados, al activar la opción de deduplicación de datos, se agregará más sobrecarga (un total de control más intenso en la CPU y entradas de tabla de deduplicación en el disco) sin proporcionar beneficios. Si los datos contienen duplicados, la activación de la opción de deduplicación de datos ahorrará espacio ya que almacenará solo una copia de un bloque determinado independientemente de la cantidad de veces que ocurra. La deduplicación puede afectar el rendimiento, ya que el total de control es más costoso para calcular y se debe acceder a los metadatos de la tabla de deduplicación y mantenerlos.

Recuerde que la deduplicación no afecta el tamaño calculado de un recurso compartido ni tampoco afecta la cantidad de espacio utilizada para la agrupación. Por ejemplo, si dos recursos compartidos contienen el mismo archivo de 512 GB, cada uno parecerá tener 512 GB de tamaño, pero el total de la agrupación será de solo 512 GB y la deduplicación se informará como 512 G (x2). Si tres recursos compartidos contienen el mismo archivo de 512 GB, cada uno parecerá tener 512 GB de tamaño, el total para la agrupación será 512 GB y la deduplicación será 512 G (x3).

Para supervisar el rendimiento de la deduplicación, se usan tres juegos de análisis:

- **ZFS DMU operations (by DMU object type)** (Operaciones de DMU de ZFS [por tipo de objeto de DMU]): este análisis muestra el número de operaciones que se están ejecutando según la tabla de deduplicación de datos en comparación con otras operaciones de ZFS.
- **Meta device bytes used (by pool)** (Bytes de metadispositivos utilizados [por agrupación]): cantidad de espacio usado en los dispositivos de metadatos.

Esta estadística permanecerá en blanco hasta que se use al menos el 1 % de la capacidad de los metadispositivos.

- **Meta device percent used (by pool)** (Porcentaje de metadispositivos utilizado [por agrupación]): cantidad de espacio usado en los dispositivos de metadatos.

Esta estadística permanecerá en blanco hasta que se use al menos el 1 % de la capacidad de los metadispositivos.

Para usar la función de deduplicación con cifrado, recuerde que solo el AES con el modo de cifrado CCM es compatible con la deduplicación. Para obtener más información, consulte [“Gestión de claves de cifrado” \[833\]](#).

Compresión de datos

La propiedad Compresión de datos controla si los datos están comprimidos antes de escribirlos en el disco. De manera opcional, los recursos compartidos pueden comprimir datos antes de realizar operaciones de escritura en la agrupación de almacenamiento. Esto permite una utilización de almacenamiento mucho mayor a expensas de una mayor utilización de la CPU. De forma predeterminada, no se realizan compresiones. Si la compresión no proporciona un ahorro mínimo de espacio, no se confirma en el disco para evitar la descompresión innecesaria al volver a leer los datos. Antes de elegir un algoritmo de compresión, se recomienda llevar a cabo las pruebas de rendimiento necesarias y medir la relación de compresión obtenida.

Valor de la BUI	Valor de la CLI	Descripción
Desactivada	off	No se realiza ninguna compresión..
LZ4	lz4	Algoritmo que normalmente consume menos CPU que GZIP-2, pero comprime mejor que LZJB, según los datos que se compriman.
LZJB (la más rápida)	lzjb	Codificación simple a lo largo de la ejecución que solo funciona con entradas lo suficientemente simples, pero no consume mucha CPU.
GZIP-2 (rápida)	gzip-2	Versión liviana del algoritmo de compresión gzip.
GZIP (valor predeterminado)	gzip	Algoritmo de compresión gzip estándar.
GZIP-9 (mejor compresión)	gzip-9	La mayor compresión posible mediante gzip. Consume una cantidad significativa de la CPU y, a menudo, puede proporcionar solo utilidad marginal.

Total de control

La propiedad Total de control verifica el total de control utilizado para los bloques de datos. En el dispositivo, se realiza el total de control de todos los datos en el disco, de manera de evitar las tradicionales dificultades (en particular, datos de lectura y escritura fantasma). Permite al sistema detectar datos no válidos devueltos de los dispositivos. El total de control por defecto (fletcher4) es suficiente para el funcionamiento normal, pero los usuarios pueden aumentar la solidez de la suma de comprobación a expensas de carga de CPU adicional. Siempre se realiza el total de control de los metadatos con el mismo algoritmo, por lo tanto, esto solo afecta los datos del usuario(bloques de LUN o archivos).

Valor de la BUI	Valor de la CLI	Descripción
Fletcher 2 (heredado)	fletcher2	Suma de comprobación fletcher de 16 bits.
Fletcher 4 (estándar)	fletcher4	Suma de comprobación fletcher de 32 bits.
SHA-256 (extra sólido)	sha256	Suma de comprobación de SHA-256.
SHA-256-MAC	sha256mac	

Uso del dispositivo de caché

La propiedad Uso de dispositivo de caché controla si se usan dispositivos de caché para el recurso compartido. Por defecto, todos los juegos de datos utilizan dispositivos de caché en el sistema. Los dispositivos de caché están configurados como parte de la agrupación de almacenamiento y proporcionan una capa adicional de almacenamiento en caché para obtener acceso más veloz organizado en niveles. Para obtener más información acerca de los dispositivos de caché, consulte [“Configuración del almacenamiento” \[127\]](#). Esta propiedad es independiente de la existencia de dispositivos de caché actualmente configurados en la agrupación de almacenamiento. Por ejemplo, es posible tener esta propiedad configurada como `all` aunque no haya dispositivos de caché presentes. Si en el futuro se agregan dichos dispositivos, el recurso compartido automáticamente aprovechará el rendimiento adicional. Esta propiedad no afecta el uso de la caché principal (DRAM).

Valor de la BUI	Valor de la CLI	Descripción
Todos los datos y metadatos	all	Todos los datos de LUN o archivos normales se almacenan en la caché, al igual que los metadatos.
Solo metadatos	metadata	Solo se guardan metadatos en los dispositivos de caché. Esto permite el recorrido rápido de las estructuras del directorio, pero podría ser necesario leer los dispositivos de datos para recuperar el contenido de los archivos.
No utilizar dispositivos de la caché	none	Ningún dato de este recurso compartido está almacenado en caché en el dispositivo de caché. Los datos solo se

Valor de la BUI	Valor de la CLI	Descripción
		almacenan en la caché principal o se almacenan en dispositivos de datos.

Desviación de escritura síncrona

La propiedad Desviación de escritura síncrona controla el comportamiento al realizar trabajos de mantenimiento de escrituras síncronas. De forma predeterminada, el sistema optimiza las escrituras síncronas para latencia, que aprovecha los dispositivos de log para proporcionar tiempos de respuesta más rápidos. En un sistema con varios sistemas de archivos discontinuos, esto puede generar disputa de dispositivos de log, lo cual puede aumentar la latencia de todos los consumidores. Aun cuando existen varios sistemas de archivos que solicitan semántica síncrona, podría suceder que algunos sistemas de archivos sean más sensibles a la latencia que otros.

Un caso común es una base de datos con un log separado. El log es extremadamente sensible a la latencia y, si bien la base de datos en sí misma requiere semántica síncrona, tiene un ancho de banda más pesado y no es sensible a la latencia. En este entorno, se pueden obtener mejoras de rendimiento significativas si esta propiedad se configura en `throughput` en la base de datos principal mientras se deja el sistema de archivos log en `latency`. Esta configuración cambiará el comportamiento aun cuando no haya dispositivos de log presentes, aunque los efectos pueden ser menos dramáticos.

El protocolo de almacenamiento inteligente de Oracle puede omitir la configuración de desviación de escritura síncrona. En lugar de usar la desviación de escritura definida en el sistema de archivos, Oracle Intelligent Storage Protocol puede usar el valor de la desviación de escritura proporcionado por el cliente NFSv4.0 o NFSv4.1 de Oracle Database. El valor de la desviación de escritura enviado por el cliente NFSv4.0 o NFSv4.1 de Oracle Database se utiliza únicamente para esa solicitud de cliente.

Valor de la BUI	Valor de la CLI	Descripción
Latencia	latency	Las escrituras síncronas se optimizan para la latencia y, de esta manera, aprovechan los dispositivos de log dedicados, si corresponde.
Rendimiento	rendimiento	Las escrituras síncronas se optimizan para el rendimiento. Los datos se escriben en los discos de datos principales en lugar de los dispositivos de log, y las escrituras se llevan a cabo de tal manera que se optimiza el ancho de banda total del sistema. Los dispositivos de log se usan para cantidades pequeñas de metadatos asociados con las escrituras de datos.

Tamaño de registro de la base de datos

La propiedad Tamaño de registro de base de datos especifica un tamaño de bloque sugerido para los archivos del sistema de archivos. Esta propiedad es válida solo para sistemas de archivos y está diseñada para utilizarse con cargas de trabajo de la base de datos que acceden a los archivos en registros de tamaño fijo. El sistema ajusta automáticamente el tamaño de los bloques de acuerdo con algoritmos internos optimizados para los patrones de acceso habituales. En cuanto a las bases de datos que crean archivos muy grandes pero que acceden a ellos en pequeños bloques aleatorios, estos algoritmos quizá funcionen por debajo de su nivel habitual. Si se especifica un tamaño de registro mayor o igual que el tamaño de grabación de la base de datos, el rendimiento puede mejorar considerablemente. El uso de esta propiedad se desaconseja de manera especial en los sistemas de archivos de finalidad general; puede afectar negativamente al rendimiento.

El tamaño de registro por defecto es 128 KB. El tamaño especificado debe ser una potencia de dos mayor o igual que 512 y menor o igual que 1 MB. Si se modifica el tamaño de registro del sistema de archivos, se ven afectados solo los archivos que se creen después del cambio; los archivos existentes y los datos recibidos no sufren cambios. Si se usan tamaños de bloques mayores que 128 KB para los proyectos o los recursos compartidos, no será posible replicar esos proyectos o recursos compartidos en sistemas que no admitan bloques de gran tamaño.

El protocolo de almacenamiento inteligente de Oracle puede omitir la configuración del tamaño de registro de la base de datos. En lugar de usar el tamaño de registro definido en el sistema de archivos, Oracle Intelligent Storage Protocol puede usar el valor del tamaño del bloque proporcionado por el cliente NFSv4.0 o NFSv4.1 de Oracle Database. El tamaño del bloque proporcionado por el cliente NFSv4.0 o NFSv4.1 de Oracle Database únicamente puede aplicarse al crear nuevos archivos o tablas en una base de datos. Los tamaños de bloque de tablas y archivos existentes no se modificarán. Para obtener más información, consulte [“Configuración de Oracle ZFS Storage Appliance para clientes de Oracle Database” \[869\]](#).

Replicación adicional

La propiedad Replicación adicional controla el número de copias almacenadas en cada bloque, más allá de la redundancia de la agrupación de almacenamiento. Los metadatos siempre se almacenan con copias múltiples, pero esta propiedad permite que se aplique el mismo comportamiento a los bloques de datos. La agrupación de almacenamiento intenta almacenar estos bloques adicionales en dispositivos diferentes, pero no está garantizado. Además, no se puede importar una agrupación de almacenamiento si se pierde un dispositivo lógico completo (segmento RAID, par reflejado, etc.). Esta propiedad no reemplaza la replicación adecuada en la agrupación de almacenamiento, pero puede tranquilizar a los administradores.

Exploración de virus

La propiedad Análisis de virus controla si se analiza la presencia de virus en el sistema de archivos. Esta propiedad solo es válida para los sistemas de archivos. Esta configuración de propiedad es independiente del estado del servicio de análisis de virus. Aunque el servicio de análisis de virus esté activado, se debe activar específicamente el análisis del sistema de archivos mediante esta propiedad. Del mismo modo, el análisis de virus se puede activar para un recurso compartido en particular aunque el servicio en sí mismo esté desactivado. Para obtener más información sobre la configuración del análisis de virus, consulte [Análisis de virus](#).

Prevención de destrucción

Cuando está configurada esta opción, no se puede destruir el recurso compartido o proyecto. Esto incluye destruir un recurso compartido mediante clones dependientes, destruir un recurso compartido dentro de un proyecto o destruir un paquete de replicación. Sin embargo, esta característica no afecta los recursos compartidos destruidos mediante actualizaciones de replicación. Si se destruye un recurso compartido en un dispositivo que es la fuente de replicación, se destruirá el recurso compartido correspondiente en el destino, incluso si está configurada esta propiedad. Para destruir el recurso compartido, primero se debe desactivar la propiedad de manera explícita como un paso aparte. Esta propiedad está desactivada de forma predeterminada.

Restringir cambio de propiedad

De forma predeterminada, nadie puede cambiar la propiedad de los archivos, excepto el usuario root (en un cliente adecuado con una exportación activada por root). Esta propiedad se puede desactivar por sistema de archivos o por proyecto. Cuando está desactivada, el propietario del archivo o directorio puede cambiar la propiedad del archivo, para permitir a los usuarios "ceder" sus propios archivos de manera eficaz. Cuando se cambia la propiedad, se segmentan los bits setgid o setuid, y se evita que los usuarios escalen privilegios mediante esta operación.

Propiedades locales del LUN

Estas propiedades solo se aplican a los LUN y no se heredan. No se pueden configurar en los proyectos.

Tamaño del volumen

La propiedad Tamaño del volumen es el tamaño lógico del LUN exportado mediante iSCSI. Esta propiedad controla el tamaño del LUN. De forma predeterminada, los LUN reservan suficiente espacio para llenar el volumen por completo. El cambio del tamaño del LUN mientras se exporta activamente a los clientes podría arrojar resultados indefinidos. Podría ser necesario que los clientes deban volver a realizar la conexión o generar daños en los datos en el sistema de archivos sobre el LUN. Consulte las mejores prácticas para el cliente iSCSI determinado antes de intentar realizar esta operación.

Aprovisionamiento fino

La propiedad Aprovisionamiento fino controla si el espacio está reservado para el volumen. De forma predeterminada, el LUN reserva el espacio suficiente exacto para llenar el volumen por completo. Esto garantiza que los clientes no obtengan errores de falta de espacio en momentos inoportunos. Esta propiedad permite que el tamaño del volumen supere la cantidad de espacio disponible. Cuando se configura, el LUN consume solo el espacio que se ha escrito en el LUN. Si bien esto permite el aprovisionamiento fino de los LUN, la mayoría de los sistemas de archivos no esperan quedarse "sin espacio" en los dispositivos subyacentes, y si el recurso compartido se queda sin espacio, se puede generar inestabilidad o daño de datos en los clientes.

Cuando no se configura, el tamaño del volumen se comporta como una reserva que no incluye las instantáneas. Por lo tanto, tiene las mismas patologías, incluida la imposibilidad de tomar instantáneas si la instantánea en teoría puede desviarse al punto de superar la cantidad de espacio disponible. Para obtener más información, consulte la propiedad Reservation (Reserva) en [“Gestión de espacio de sistemas de archivos y proyectos” \[541\]](#).

Tamaño de bloque de volumen

La propiedad Tamaño de bloque de volumen determina el tamaño del bloque nativo para los LUN. Puede tener cualquier potencia de 2 desde 512 bytes hasta 1M; el valor predeterminado es 8K. Esta propiedad es estática; se la define cuando se crea el LUN y no se la puede cambiar.

Nota - Los LUN cuyo tamaño de bloque de volumen es menor que 4K pueden causar una degradación del rendimiento.

Otras propiedades

Están disponibles las siguientes propiedades: Valor por defecto del proyecto, Local de sistema de archivos, Gestión de espacio, Solo lectura y Personalizada.

Valor por defecto del proyecto

Las propiedades predeterminadas del proyecto se configuran en el proyecto, pero no lo afectan. Se utilizan para completar la configuración inicial al crear un sistema de archivos o LUN, y pueden resultar útiles cuando los recursos compartidos tienen un juego común de propiedades no heredables. El cambio de estas propiedades no afecta los recursos compartidos existentes y las propiedades se pueden cambiar antes o después de la creación del recurso compartido.

Sistema de archivos local

Las propiedades locales del sistema de archivos solo se aplican a los sistemas de archivos y son propiedades de conveniencia para gestionar el directorio raíz del sistema de archivos. No se heredan y no se pueden configurar en los proyectos. Estas propiedades de control de acceso también pueden ser configuradas por las operaciones de protocolo en banda.

Gestión de espacio

Las propiedades de gestión de espacio (cuota y reserva) se aplican a los recursos compartidos y a los proyectos, pero no se heredan. Se aplicará un proyecto con una cuota de 100G en todos los recursos compartidos, pero cada recurso compartido individual no tendrá una cuota, salvo que esta se defina explícitamente.

Solo lectura

Las propiedades de solo lectura representan estadísticas relacionadas con el proyecto y los recursos compartidos, y no se pueden cambiar. Las propiedades más comunes de este tipo son las estadísticas de uso de espacio.

Propiedades personalizadas

Las propiedades personalizadas son propiedades definidas por el usuario mediante un esquema. Para obtener más información, consulte [“Trabajo con esquemas” \[571\]](#).

Propiedades estáticas

Las propiedades estáticas (momento de creación) se especifican en la creación del sistema de archivos o el LUN, pero no se pueden cambiar después de crear el recurso compartido. Estas propiedades controlan las estructuras de datos en disco y comprenden configuraciones

de internacionalización, distinción entre mayúsculas y minúsculas, y tamaño del bloque de volumen.

En la BUI, las propiedades estáticas se pueden ver en el lado izquierdo de la interfaz al editar un sistema de archivos o un LUN.

TABLA 124 Propiedades estáticas de sistemas de archivos y LUN

Nombre de la BUI	Nombre de la CLI	Descripción
Fecha de creación	creation	Indica la fecha de creación.
Ratio de compresión	compressratio	Ratio de compresión actual del sistema de archivos o el LUN, que es producto del algoritmo de compresión. Para obtener más información, consulte “Ratio de compresión” [514] .
Distinción entre mayúsculas y minúsculas	casesensitivity	La propiedad Distinción entre mayúsculas y minúsculas controla si las consultas de directorio distinguen entre mayúsculas y minúsculas. Para obtener más información, consulte “Distinción entre mayúsculas y minúsculas” [515] .
Rechazar codificación que no sea UTF-8	utf8only	Esta propiedad aplica la codificación UTF-8 para todos los archivos y directorios. Para obtener más información, consulte “Rechazar codificación que no sea UTF-8” [516] .
Normalización	normalization	La propiedad Normalización controla la normalización de unicode que se lleva a cabo (si corresponde) en sistemas de archivos y directorios. Unicode admite la posibilidad de que el mismo nombre lógico esté representado por codificaciones diferentes. Para obtener más información, consulte “Normalización” [516] .
Tamaño de bloque de volumen (solo LUN)	volblocksize	La propiedad Tamaño de bloque de volumen determina el tamaño del bloque nativo para los LUN. Para obtener más información, consulte “Tamaño de bloque de volumen” [517] .
Origen	origin	Muestra el nombre de la instantánea a partir de la que se clonó. Para obtener más información, consulte “Origen” [517] .
Origen de migración de datos (solo sistemas de archivos)	shadow	Ubicación del origen si el sistema de archivos refleja activamente un sistema de archivos existente, ya sea de manera local o mediante NFS. Para obtener más información, consulte “Origen de migración de datos” [517] .

Ratio de compresión

Si la compresión está activada, esta propiedad muestra el ratio de compresión obtenido actualmente para el recurso compartido. Esto se expresa como multiplicador. Por ejemplo,

una compresión de 2x significa que los datos consumen la mitad del espacio que el contenido sin comprimir. Para obtener más información acerca de la selección de un algoritmo de compresión, consulte "Compresión de datos" en ["Propiedades heredadas" \[503\]](#).

Distinción entre mayúsculas y minúsculas

La propiedad Distinción entre mayúsculas y minúsculas controla si las consultas de directorio distinguen entre mayúsculas y minúsculas. Admite las siguientes opciones:

Valor de la BUI	Valor de la CLI	Descripción
Mixto	mixed	La distinción entre mayúsculas y minúsculas depende del protocolo que se utilice. En el caso de NFS, FTP y HTTP, las consultas distinguen entre mayúsculas y minúsculas. En el caso de SMB, las consultas no distinguen entre mayúsculas y minúsculas. Este es el valor predeterminado y prioriza el cumplimiento de los diversos protocolos sobre la coherencia entre los protocolos. Cuando se utiliza este modo, es posible crear archivos diferentes mediante protocolos que distinguen entre mayúsculas y minúsculas, pero que no son compatibles cuando se accede mediante SMB. En este caso, el servidor SMB creará una versión "alterada" de los conflictos que identifican el nombre de archivos de manera única.
Sin distinción entre mayúsculas y minúsculas	insensitive	Las consultas no distinguen entre mayúsculas y minúsculas, incluso mediante protocolos (como NFS) que tradicionalmente distinguen entre mayúsculas y minúsculas. Esto puede generar confusión para los clientes de estos protocolos, pero evita que los clientes creen conflictos de nombres lo cual derivaría en el uso de nombres alterados mediante SMB. Esta configuración solo se debe utilizar donde SMB es el protocolo principal y los protocolos alternativos se consideran de segunda clase, donde el cumplimiento de los estándares esperados no constituye un problema.
Con distinción entre mayúsculas y minúsculas	sensitive	Las consultas distinguen entre mayúsculas y minúsculas, incluso mediante SMB donde las consultas tradicionalmente no distinguen entre mayúsculas y minúsculas. En general, no se debe utilizar esta configuración porque el servidor SMB puede tratar los conflictos de nombres mediante los nombres alterados, y podría generar un comportamiento extraño en las aplicaciones de Windows.

Rechazar codificación que no sea UTF-8

Esta propiedad aplica la codificación UTF-8 para todos los archivos y directorios. Cuando se configura, se produce un error si se intenta crear un archivo o directorio con una codificación UTF-8 no válida. Esto solo afecta a NFSv3, donde la codificación no está definida por el estándar. NFSv4.0 y NFSv4.1 utilizan siempre UTF-8 y SMB negocia la codificación adecuada. Generalmente, esta configuración debe tener el valor `on`; de lo contrario, SMB (que debe conocer la codificación para realizar comparaciones con distinción entre mayúsculas y minúsculas, entre otras cosas) no podrá decodificar los nombres de archivos creados con una codificación UTF-8 no válida. Esta configuración solo debe tener el valor `off` en los despliegues NFSv3 preexistentes, donde los clientes se configuraron para utilizar codificaciones diferentes. La activación de SMB, NFSv4.0 o NFSv4.1 cuando esta propiedad se establece en `off` puede generar resultados indefinidos si un cliente NFSv3 crea un archivo o directorio que no tiene una codificación de UTF-8 válida. Se debe establecer esta propiedad en `on` si la propiedad de normalización se define en un valor distinto de `none`.

Normalización

La propiedad Normalización controla la normalización de unicode que se lleva a cabo (si corresponde) en sistemas de archivos y directorios. Unicode admite la posibilidad de que el mismo nombre lógico esté representado por codificaciones diferentes. Sin la normalización, el nombre almacenado en el disco será diferente y las consultas que utilizan una de las formas alternativas arrojarán errores según el formato de creación del archivo y la manera de acceder a él. Si se establece esta propiedad en un valor distinto de `none` (el valor por defecto), la propiedad "Rechazar codificación que no sea UTF-8" también se debe establecer en `on`.

Valor de la BUI	Valor de la CLI	Descripción
Ninguno	<code>none</code>	No se lleva a cabo ninguna normalización.
Formulario C	<code>formC</code>	<i>Composición canónica del formulario de normalización (NFC, Normalization Form Canonical Composition):</i> los caracteres se descomponen y, luego, se recomponen mediante equivalencia canónica.
Formulario D	<code>formD</code>	<i>Descomposición canónica del formulario de normalización (NFC, Normalization Form Canonical Decomposition):</i> los caracteres se descomponen mediante equivalencia canónica.
Formulario KC	<code>formKC</code>	<i>Composición de compatibilidad del formulario de normalización (NFKC, Normalization Form Compatibility Composition):</i> los caracteres se descomponen por equivalencia de compatibilidad y, luego, se recomponen mediante equivalencia canónica.
Formulario KD	<code>formKD</code>	<i>Descomposición de compatibilidad del formulario de normalización (NFKC, Normalization Form</i>

Valor de la BUI	Valor de la CLI	Descripción
		<i>Compatibility Decomposition</i>): los caracteres se descomponen mediante equivalencia de compatibilidad.

Tamaño de bloque de volumen

La propiedad Tamaño de bloque de volumen determina el tamaño del bloque nativo para los LUN. Puede tener cualquier potencia de 2 desde 512 bytes hasta 1M; el valor predeterminado es 8K.

Nota - Los LUN cuyo tamaño de bloque de volumen es menor que 4K pueden causar una degradación del rendimiento.

Origen

Si se trata de un clon, se refiere al nombre de la instantánea desde la cual se clonó.

Origen de migración de datos

Si está configurado, el sistema de archivos refleja activamente un sistema de archivos existente, ya sea de manera local o mediante NFS. Para obtener más información sobre la migración de datos, consulte [Migración shadow \[575\]](#).

Propiedades de proyecto

Nota - En la CLI, use el comando `get` para ver una lista de todas las propiedades. Utilice el comando `list` para mostrar una lista de todos los elementos secundarios.

TABLA 125 Propiedades de proyecto

Ubicación de la BUI	Nombre de la BUI	Nombre de la CLI	Tipo de propiedad	Descripción
Crear proyecto	Nombre	project	Estática	Define el nombre del proyecto.
	Cifrado	encryption	Heredada	Define el tipo de cifrado. Para obtener más información, consulte “Gestión de claves de cifrado” [833] .

Ubicación de la BUI	Nombre de la BUI	Nombre de la CLI	Tipo de propiedad	Descripción
	Heredar clave	--	--	Si se selecciona, esta opción indica que la clave de cifrado se hereda de la agrupación principal.
	Clave	key	Heredada	Establece una clave de cifrado específica que se usa cuando la clave no se hereda de la agrupación principal.
	Nombre de clave	keyname	Estática	Identifica la clave.
General - Uso de espacio - Datos	Cuota	quota	Gestión de espacio	Establece un límite sobre la cantidad de espacio que puede consumir cualquier entidad en particular.
	Reserva	reservation	Gestión de espacio	Representa una garantía de espacio que puede consumir cualquier entidad en particular.
General - Uso de espacio - Usuarios y grupos	Cuota por defecto de usuario	defaultuserquota	Gestión de espacio	Establece un límite para la cantidad de espacio que puede consumir el usuario.
	Cuota predeterminada de grupo	defaultgroupquota	Gestión de espacio	Establece un límite para la cantidad de espacio que puede consumir el grupo.
	Usuario y grupo	usuarios / grupos	--	Especifica usuarios o grupos.
	Uso	--	Gestión de espacio	Muestra la cantidad de datos que usan los usuarios o los grupos.
General - Propiedades heredadas	Punto de montaje	mountpoint	Heredada	Controla la ruta de acceso usada para exportar sistemas de archivos. Para obtener más información, consulte “Punto de montaje” [504] .
	Solo lectura	readonly	Heredada	Controla si el contenido del sistema de archivos es de solo lectura. Para obtener más información, consulte “Solo lectura” [504] .

Ubicación de la BUI	Nombre de la BUI	Nombre de la CLI	Tipo de propiedad	Descripción
	Actualización de hora de acceso en el momento de la lectura	atime	Heredada	Controla si la hora de acceso a los archivos está actualizada en el momento de la lectura. Para obtener más información, consulte “Actualización de hora de acceso en el momento de la lectura” [504] .
	Bloqueo no bloqueante obligatorio	nbmand	heredado	Controla si la semántica de bloqueo de SMB tiene prioridad sobre la semántica de POSIX. Para obtener más información, consulte “Bloqueo no bloqueante obligatorio” [505] .
	Desduplicación de datos	dedup	Heredada	Controla si las copias duplicadas de los datos se eliminan. Para obtener más información, consulte “Desduplicación de datos” [505] .
	Compresión de datos	compression	Heredada	Controla si los datos están comprimidos antes de escribirlos en el disco. Para obtener más información, consulte “Compresión de datos” [507] .
	Total de control	checksum	Heredada	Controla el total de control utilizado para los bloques de datos. Para obtener más información, consulte “Total de control” [508] .
	Uso del dispositivo de caché	secondarycache	Heredada	Controla si los dispositivos de caché se utilizan para el recurso compartido. Para obtener más información, consulte “Uso del dispositivo de caché” [508] .
	Desviación de escritura síncrona	logbias	Heredada	Controla el comportamiento al realizar trabajos de mantenimiento de escrituras síncronas. Para obtener más

Ubicación de la BUI	Nombre de la BUI	Nombre de la CLI	Tipo de propiedad	Descripción
				información, consulte “Desviación de escritura síncrona” [509] .
	Tamaño de registro de la base de datos	recordsize	Heredada	Especifica un tamaño de bloque sugerido para los archivos del sistema de archivos. Para obtener más información, consulte “Tamaño de registro de la base de datos” [510] .
	Replicación adicional	copies	Heredada	Controla la cantidad de copias almacenadas en cada bloque, más allá de la redundancia de la agrupación de almacenamiento. Para obtener más información, consulte “Replicación adicional” [510] .
	Exploración de virus	vscan	Heredada	Controla si se analiza la presencia de virus en un sistema de archivos. Para obtener más información, consulte “Exploración de virus” [511] .
	Prevención de destrucción	nodestroy	Heredada	Cuando se la configura, evita que se destruyan recursos compartidos o proyectos. Para obtener más información, consulte “Prevención de destrucción” [511] .
	Restringir cambio de propiedad	rstchown	Heredada	Controla la propiedad y se puede desactivar en sistemas de archivos o proyectos individuales. Para obtener más información, consulte “Restringir cambio de propiedad” [511] .
General - Propiedades personalizadas	Esquema	custom	--	Se pueden agregar según sea necesario para anexar etiquetas definidas por el usuario a proyectos y recursos compartidos. Para obtener más información, consulte “Propiedades de esquema” [573] .

Ubicación de la BUI	Nombre de la BUI	Nombre de la CLI	Tipo de propiedad	Descripción
General - Valores de configuración por defecto - Sistemas de archivos	Usuario	default_user	Valor predeterminado de creación	Especifica un ID de usuario o un nombre de usuario.
	Grupo	default_group	Valor predeterminado de creación	Especifica un ID de grupo o un nombre de grupo.
	Permisos	default_permissions	Valor predeterminado de creación	Define los permisos por defecto para el sistema de archivos.
General - Valores de configuración por defecto - LUNs LUN	Tamaño del volumen	default_volsize	Solo para LUN, valor predeterminado de creación	Muestra el tamaño de volumen máximo y la unidad de medida. Para obtener más información, consulte “Tamaño del volumen” [512] .
	Aprovisionamiento fino	default_sparse	Solo para LUN, valor predeterminado de creación	Cuando se la selecciona, indica solo la cantidad de espacio consumido físicamente por los datos. Para obtener más información, consulte “Aprovisionamiento fino” [512] .
	Tamaño de bloque de volumen	default_volblocksize	Valor predeterminado de creación	Muestra el tamaño de bloque nativo para los LUN; puede ser un valor de 512 B a 1 MB (el valor por defecto es 8 KB). Para obtener más información, consulte “Tamaño de bloque de volumen” [512] .
Propiedades de ancho de banda	Límite de lectura	readlimit	--	Define la cantidad máxima de bytes por segundo que se pueden leer desde un recurso compartido. m indica megabytes y g indica gigabytes. La configuración por defecto es ilimitado, lo que impide la limitación de E/S.
	Límite de escritura	writelimit	--	Define la cantidad máxima de bytes por segundo que se pueden escribir en un recurso compartido. m indica megabytes y g

Propiedades de proyecto

Ubicación de la BUI	Nombre de la BUI	Nombre de la CLI	Tipo de propiedad	Descripción
				indica gigabytes. La configuración por defecto es ilimitado, lo que impide la limitación de E/S.
	Límite de lectura efectivo	effectivewritelimit	--	Propiedad de solo lectura que informa el límite inferior de lectura para un recurso compartido.
	Límite de escritura efectivo	effectivewritelimit	--	Propiedad de solo lectura que informa el límite inferior de escritura para un recurso compartido.
Protocolos - NFS	NFS	sharenfs	Heredada	La configuración y los valores de la propiedad NFS Protocol (Protocolo NFS) se describen en “Propiedades del protocolo NFS” [548] .
Protocolos - Excepciones de NFS	Es posible definir excepciones para los modos de uso compartido general para los clientes o las recopilaciones de clientes. Para obtener más información, consulte “Excepciones del modo de recurso compartido de NFS” [549] .			
Protocolos - SMB	SMB	sharesmb	Heredada	La configuración y los valores de la propiedad Protocolo SMB se describen en “Propiedades de protocolo SMB” [555] .
Protocolos - Excepciones de SMB	Es posible definir excepciones para los modos de uso compartido general para los clientes o las recopilaciones de clientes. Consulte “Excepciones de modo de recurso compartido del protocolo SMB” [559] .			
Protocolos - HTTP (Inherit from project [Heredar de proyecto])	Modo de recurso compartido	sharedav	Heredada	Determina si el recurso compartido está disponible solo para lectura, para lectura y escritura, o para ninguna de estas opciones. En la CLI, on es un alias para rw.
Protocolos - FTP (Heredar de proyecto)	Modo de recurso compartido	shareftp	Heredada	Determina si el recurso compartido está disponible solo para lectura, para lectura y escritura, o para ninguna de estas opciones. En la CLI, on es un alias para rw.
Protocolos: SFTP (Heredar de proyecto)	Modo de recurso compartido	sharesftp	Heredada	Determina si el recurso compartido está

Ubicación de la BUI	Nombre de la BUI	Nombre de la CLI	Tipo de propiedad	Descripción
				disponible solo para lectura, para lectura y escritura, o para ninguna de estas opciones. En la CLI, <code>on</code> es un alias para <code>rw</code> .
Protocolos: TFTP (Heredar de proyecto)	Modo de recurso compartido	shareftp	Heredada	Determina si el recurso compartido está disponible solo para lectura, para lectura y escritura, o para ninguna de estas opciones. En la CLI, <code>on</code> es un alias para <code>rw</code> .
Acceso	Comportamiento de la ACL en cambio de modo	aclmode	Heredada	Controla cómo interactúan las solicitudes de cambio de modo con la ACL existente.
	Comportamiento de valores heredados de ACL	aclinherit	Heredada	Controla cómo los archivos o los directorios nuevos heredan la configuración existente de ACL del directorio principal.
Instantáneas: Propiedades	visibilidad de <code>.zfs/snapshot</code>	snapdir	Heredada	Controla si se puede acceder a instantáneas del sistema de archivos mediante los protocolos de datos de <code>.zfs/snapshot</code> que se encuentran en el directorio raíz del sistema de archivos.
	Etiqueta de instantánea programada	snaplabel	Heredada	Agrega una etiqueta definida por el usuario a cada instantánea programada y aparece en blanco de forma predeterminada.
Instantáneas - Instantáneas	Nombre	snapshot name	--	Especifica el nombre de la instantánea.
	Creación	creation	--	Especifica la fecha y la hora de creación de la instantánea.
	Único	space_unique	--	Indica la cantidad de espacio único utilizado por la instantánea.

Propiedades de proyecto

Ubicación de la BUI	Nombre de la BUI	Nombre de la CLI	Tipo de propiedad	Descripción
	Total	space_data	--	Indica la cantidad total de espacio al que hace referencia la instantánea.
Instantáneas - Programas	Frecuencia	frequency	Hora de creación	Indica con qué frecuencia se toma la instantánea.
	Mantener al máximo	keep	Hora de creación	Controla la política de retención de las instantáneas.
Replicación (Heredar de proyecto)/Crear nuevas acciones	Destino	target	Heredada	Identifica el sistema de destino de replicación.
	Agrupación	pool	Heredada	Especifica la agrupación de almacenamiento en el destino donde se replicará este proyecto.
	Ruta de exportación de datos	export_path	Heredada	Indica la ruta de exportación de los datos.
	Limite de ancho de banda	max_bandwidth	Heredada	Especifica una velocidad máxima para esta actualización de replicación (en términos de cantidad de datos transferidos por la red por segundo).
	Activar cifrado SSL	use_ssl	Heredada	Controla si se deben cifrar datos por cable mediante SSL.
	Desactivar compresión	--	Heredada	Controla si la compresión está activada o desactivada.
	Incluir instantáneas	include_snaps	Heredada	Controla si las actualizaciones de replicación incluyen instantáneas de no replicación.
	Retener instantáneas de usuario en destino	retain_user_snaps_on_target	Heredada	Cuando se la configura, las instantáneas generadas por el usuario se conservan en el destino de la replicación. Las instantáneas se conservan en el destino hasta que se desactive la opción.
	Incluir origen de clon como datos	include_clone_origin_as_data	Heredada	Permite controlar la replicación de cada recurso compartido que se clonó a partir de un

Ubicación de la BUI	Nombre de la BUI	Nombre de la CLI	Tipo de propiedad	Descripción
				recurso compartido que es externo al paquete de replicación en el destino.
	Objetivo de punto de recuperación	recovery_point_objective	Heredada	Especifica la cantidad máxima tolerable de pérdida de datos en caso de desastre o una interrupción de servicio importante.
	Alerta de advertencia de demora de réplica	replica_lag_warning_alert	Heredada	Especifica un límite, representado como porcentaje del RPO, cuando se genera una alerta menor.
	Alerta de error de demora de réplica	replica_lag_error_alert	Heredada	Especifica un límite, representado como porcentaje del RPO, cuando se genera una alerta mayor.
	Frecuencia de actualización	continuous	Heredada	Controla si la acción se replica continuamente o en intervalos manuales o programados.

Propiedades de sistema de archivos

Nota - En la CLI, use el comando `get` para ver una lista de todas las propiedades.

TABLA 126 Propiedades de sistema de archivos

Ubicación de la BUI	Nombre de la BUI	Nombre de la CLI	Tipo de propiedad	Descripción
Crear sistema de archivos	Proyecto	select project_name	--	Define el proyecto que usa el sistema de archivos para heredar la configuración de parámetros. También se puede seleccionar el proyecto por defecto.
	Nombre	filesystem	--	Define el nombre del sistema de archivos.
	Origen de migración de datos	shadow	Hora de creación	Muestra la ubicación del origen si está migrando datos.

Ubicación de la BUI	Nombre de la BUI	Nombre de la CLI	Tipo de propiedad	Descripción
	Usuario	root-user	Sistema de archivos local	Especifica el propietario del directorio raíz.
	Grupo	root_group	Sistema de archivos local	Especifica el grupo del directorio raíz.
	Permisos o Usar permisos por defecto de Windows	root_permission	Sistema de archivos local	Especifica los permisos estándar de UNIX para el directorio raíz o los permisos por defecto de Windows.
	Heredar punto de montaje	--	--	Indica que se hereda el punto de montaje si está seleccionada.
	Punto de montaje	mountpoint	Heredada	Controla la ruta de acceso usada para exportar sistemas de archivos. Para obtener más información, consulte “Punto de montaje” [504] .
	Rechazar codificación que no sea UTF-8	utf8only	Hora de creación	Aplica la codificación UTF-8 para todos los sistemas de archivos y directorios. Para obtener más información, consulte “Rechazar codificación que no sea UTF-8” [516] .
	Distinción entre mayúsculas y minúsculas	casesensitivity	Hora de creación	Controla si en las consultas del directorio se distingue entre mayúsculas y minúsculas, si no se distingue o si se usa una combinación. Para obtener más información, consulte “Distinción entre mayúsculas y minúsculas” [515] .
	Normalización	normalization	Hora de creación	Controla la normalización de unicode que se lleva a cabo (si existe alguna) en sistemas de archivos y directorios. Para obtener más información, consulte “Normalización” [516] .
	Cifrado	encryption	Heredada	Define el tipo de cifrado. Para obtener más información, consulte

Ubicación de la BUI	Nombre de la BUI	Nombre de la CLI	Tipo de propiedad	Descripción
				“Gestión de claves de cifrado” [833] .
	Heredar clave	--	--	Si se selecciona, esta opción indica que la clave de cifrado se hereda del proyecto principal.
	Clave	key	Heredada	Establece una clave de cifrado específica que se usa cuando la clave no se hereda del proyecto principal.
	Nombre de clave	keyname	Estática	Identifica la clave.
General - Uso de espacio - Datos	Cuota	quota	Gestión de espacio	Establece un límite sobre la cantidad de espacio que puede consumir cualquier entidad en particular.
	Cuota/Incluir instantáneas	quota_snap	Gestión de espacio	Establece un límite sobre la cantidad de espacio que puede consumir cualquier entidad en particular, incluidas las instantáneas.
	Reserva	reservation	Gestión de espacio	Representa una garantía de espacio que puede consumir cualquier entidad en particular.
	Reserva/Incluir instantáneas	reservation_snap	Gestión de espacio	Representa una garantía de espacio que puede consumir cualquier entidad en particular, incluidas las instantáneas.
General - Uso de espacio - Usuarios y grupos	Usuarios y grupos	--	--	Especifica los usuarios o los grupos.
	Uso	--	--	Muestra la cantidad de datos que usan los usuarios o los grupos.
	Cuota	quota	Gestión de espacio	Establece un límite sobre la cantidad de espacio que puede consumir cualquier entidad en particular.
General - Propiedades (Heredar de proyecto)	Punto de montaje	mountpoint	Heredada	Controla la ruta de acceso usada para exportar sistemas de archivos. Para obtener más información,

Ubicación de la BUI	Nombre de la BUI	Nombre de la CLI	Tipo de propiedad	Descripción
				consulte “Punto de montaje” [504] .
	Solo lectura	readonly	Heredada	Controla si el contenido del sistema de archivos es de solo lectura. Para obtener más información, consulte “Solo lectura” [504] .
	Actualización de hora de acceso en el momento de la lectura	atime	Heredada	Controla si la hora de acceso a los archivos está actualizada en el momento de la lectura. Para obtener más información, consulte “Actualización de hora de acceso en el momento de la lectura” [504] .
	Bloqueo no bloqueante obligatorio	nbmand	heredado	Controla si la semántica de bloqueo de SMB tiene prioridad sobre la semántica de POSIX. Para obtener más información, consulte “Bloqueo no bloqueante obligatorio” [505] .
	Desduplicación de datos (advertencia)	dedup	Heredada	Controla si las copias duplicadas de los datos se eliminan. Para obtener más información, consulte “Desduplicación de datos” [505] .
	Compresión de datos	compression	Heredada	Controla si los datos están comprimidos antes de escribirlos en el disco. Para obtener más información, consulte “Compresión de datos” [507] .
	Total de control	checksum	Heredada	Controla el total de control utilizado para los bloques de datos. Para obtener más información, consulte “Total de control” [508] .
	Uso del dispositivo de caché	secondarycache	Heredada	Controla si los dispositivos de caché se utilizan para el recurso compartido. Para obtener más información, consulte

Ubicación de la BUI	Nombre de la BUI	Nombre de la CLI	Tipo de propiedad	Descripción
				“Uso del dispositivo de caché” [508] .
	Desviación de escritura síncrona	logbias	Heredada	Controla el comportamiento al realizar trabajos de mantenimiento de escrituras síncronas. Para obtener más información, consulte “Desviación de escritura síncrona” [509] .
	Tamaño de registro de la base de datos	recordsize	Heredada	Especifica un tamaño de bloque sugerido para los archivos del sistema de archivos. Para obtener más información, consulte “Tamaño de registro de la base de datos” [510] .
	Replicación adicional	copies	Heredada	Controla la cantidad de copias almacenadas en cada bloque, más allá de la redundancia de la agrupación de almacenamiento. Para obtener más información, consulte “Replicación adicional” [510] .
	Exploración de virus	vscan	Heredada	Controla si se analiza la presencia de virus en un sistema de archivos. Para obtener más información, consulte “Exploración de virus” [511] .
	Prevención de destrucción	nodestroy	Heredada	Cuando se la configura, evita que se destruyan recursos compartidos o proyectos. Para obtener más información, consulte “Prevención de destrucción” [511] .
	Restringir cambio de propiedad	rstchown	Heredada	Controla la propiedad y se puede desactivar en sistemas de archivos o proyectos individuales. Para obtener más información, consulte “Restringir cambio de propiedad” [511] .

Propiedades de sistema de archivos

Ubicación de la BUI	Nombre de la BUI	Nombre de la CLI	Tipo de propiedad	Descripción
General - Custom Properties (Inherit from Project) (Propiedades personalizadas [Heredar de proyecto])	--	custom	--	Se pueden agregar propiedades personalizadas según sea necesario para anexar etiquetas definidas por el usuario a proyectos y recursos compartidos.
Protocolos - NFS	NFS	share nfs	Heredada	La configuración y los valores de la propiedad NFS Protocol (Protocolo NFS) se describen en “Propiedades del protocolo NFS” [548] .
Protocolos - Excepciones de NFS	Es posible definir excepciones para los modos de uso compartido general para los clientes o las recopilaciones de clientes. Para obtener más información, consulte “Excepciones del modo de recurso compartido de NFS” [549] .			
Protocolos - SMB	SMB	share smb	Heredada	La configuración y los valores de la propiedad Protocolo SMB se describen en “Propiedades de protocolo SMB” [555] .
Protocolos - Excepciones de SMB	Es posible definir excepciones para los modos de uso compartido general para los clientes o las recopilaciones de clientes. Consulte “Excepciones de modo de recurso compartido del protocolo SMB” [559] .			
Protocolos - ACL de nivel de recurso compartido	Tipo	--	--	Indica el tipo de la ACL.
	Destino	--	--	Indica el destino de la ACL.
	Acceso	--	--	Indica si se permite o se bloquea el acceso a la ACL.
	Permisos: Herencia	--	--	Especifica los permisos UNIX estándar para la ACL.
Protocolos - HTTP (Heredar de proyecto)	Modo de recurso compartido	share dav	Heredada	Determina si el recurso compartido está disponible solo para lectura, para lectura y escritura, o para ninguna de estas opciones. En la CLI, on es un alias para rw.
Protocolos - FTP (Heredar de proyecto)	Modo de recurso compartido	share ftp	Heredada	Determina si el recurso compartido está disponible solo para lectura, para lectura y escritura, o para ninguna de estas opciones. En la

Ubicación de la BUI	Nombre de la BUI	Nombre de la CLI	Tipo de propiedad	Descripción
				CLI, <code>on</code> es un alias para <code>rw</code> .
Protocolos: SFTP (Heredar de proyecto)	Modo de recurso compartido	sharesftp	Heredada	Determina si el recurso compartido está disponible solo para lectura, para lectura y escritura, o para ninguna de estas opciones. En la CLI, <code>on</code> es un alias para <code>rw</code> .
Protocolos: TFTP (Heredar de proyecto)	Modo de recurso compartido	shareftp	Heredada	Determina si el recurso compartido está disponible solo para lectura, para lectura y escritura, o para ninguna de estas opciones. En la CLI, <code>on</code> es un alias para <code>rw</code> .
Acceso - Acceso a directorio raíz	Usuario	root_user	Sistema de archivos local	Especifica el propietario del directorio raíz.
	Grupo	root_group	Sistema de archivos local	Especifica el grupo del directorio raíz.
	Permisos	root_permissions	Sistema de archivos local	Especifica los permisos UNIX estándar para el directorio raíz.
Acceso - Comportamiento de ACL (Heredar de proyecto)	Comportamiento de la ACL en cambio de modo	aclmode	Heredada	Controla cómo interactúan las solicitudes de cambio de modo con la ACL existente.
	Comportamiento de valores heredados de ACL	aclinherit	Heredada	Controla cómo los archivos o los directorios nuevos heredan la configuración existente de ACL del directorio principal.
Acceso - ACL de directorio raíz	Tipo	--	--	Indica el tipo de la ACL.
	Destino	--	--	Indica el destino de la ACL.
	Acceso	--	--	Indica si se permite o se bloquea el acceso a la ACL.
	Permisos: Herencia	--	--	Especifica los permisos UNIX estándar para la ACL.
Instantáneas - Propiedades (Heredar de proyecto)	visibilidad de .zfs/snapshot	snapdir	Heredada	Controla si se puede acceder a instantáneas del sistema de archivos

Ubicación de la BUI	Nombre de la BUI	Nombre de la CLI	Tipo de propiedad	Descripción
				mediante los protocolos de datos de .zfs/snapshot que se encuentran en el directorio raíz del sistema de archivos.
	Etiqueta de instantánea programada	snaplabel	Heredada	Agrega una etiqueta definida por el usuario a cada instantánea programada y aparece en blanco de forma predeterminada.
Instantáneas - Instantáneas	Nombre	--	--	Especifica el nombre de la instantánea.
	Creación	--	--	Especifica la fecha y la hora de creación de la instantánea.
	Unique (Único)	--	--	Indica la cantidad de espacio único utilizado por la instantánea.
	Total	--	--	Indica la cantidad total de espacio al que hace referencia la instantánea. Representa el tamaño del sistema de archivos en el momento en que se tomó la instantánea; en teoría, cualquier instantánea puede abarcar una cantidad de espacio igual al tamaño total a medida que se sobrescriben los bloques de datos.
	Clones	--	--	Muestra la cantidad de clones de la instantánea.
Instantáneas - Programas	Frecuencia	frequency	Hora de creación	Indica con qué frecuencia se toma la instantánea.
	Mantener al máximo	keep	Hora de creación	Controla la política de retención de las instantáneas.
Replicación (Heredar de proyecto)/Crear nuevas acciones	Destino	target	Heredada	Identifica el sistema de destino de replicación.
	Agrupación	pool	Heredada	Especifica la agrupación de almacenamiento en el destino donde se replicará este proyecto.
	Ruta de exportación de datos	export_path	Heredada	Indica la ruta de exportación de los datos.

Ubicación de la BUI	Nombre de la BUI	Nombre de la CLI	Tipo de propiedad	Descripción
	Limite de ancho de banda	max_bandwidth	Heredada	Especifica una velocidad máxima para esta actualización de replicación (en términos de cantidad de datos transferidos por la red por segundo).
	Activar cifrado SSL	use_ssl	Heredada	Controla si se deben cifrar datos por cable mediante SSL.
	Disable compression (Desactivar compresión)	compression	Heredada	Controla si la compresión está activada o desactivada.
	Incluir instantáneas	include_snaps	Heredada	Controla si las actualizaciones de replicación incluyen instantáneas de no replicación.
	Retener instantáneas de usuario en destino	retain_user_snaps_on_target	Heredada	Cuando se la configura, las instantáneas generadas por el usuario se conservan en el destino de la replicación. Las instantáneas se conservan en el destino hasta que se desactive la opción.
	Incluir origen de clon como datos	include_clone_origin_as_data	Heredada	Permite controlar la replicación de cada recurso compartido que se clonó a partir de un recurso compartido que es externo al paquete de replicación en el destino.
	Objetivo de punto de recuperación	recovery_point_objective	Heredada	Especifica la cantidad máxima tolerable de pérdida de datos en caso de desastre o una interrupción de servicio importante.
	Alerta de advertencia de demora de réplica	replica_lag_warning_alert	Heredada	Especifica un límite, representado como porcentaje del RPO, cuando se genera una alerta menor.
	Alerta de error de demora de réplica	replica_lag_error_alert	Heredada	Especifica un límite, representado como porcentaje del RPO,

Propiedades de LUN

Ubicación de la BUI	Nombre de la BUI	Nombre de la CLI	Tipo de propiedad	Descripción
				cuando se genera una alerta mayor.
	Frecuencia de actualización	continuous	Heredada	Controla si la acción se replica continuamente o en intervalos manuales o programados.
Uso	Datos con referencia	space_data	Solo lectura	Muestra la cantidad total del espacio al que hace referencia el recurso compartido activo, independiente de las instantáneas.
	Reserva sin uso	space_unused_res	Solo lectura	Muestra la cantidad de espacio restante que está reservado para el sistema de archivos.
	Datos de instantáneas	space_snapshots	Solo lectura	Muestra la cantidad total de datos que en la actualidad tienen todas las instantáneas del recurso compartido.
	Datos disponibles	space_available	Solo lectura	Muestra las cuotas del recurso compartido o del proyecto, o la capacidad absoluta de la agrupación.
	Espacio total	space_total	Solo lectura	Muestra la suma de los datos de referencia, los datos de instantáneas y la reserva sin uso.

Propiedades de LUN

Nota - En la CLI, use el comando `get` para ver una lista de todas las propiedades.

TABLA 127 Propiedades de LUN

Ubicación de la BUI	Nombre de la BUI	Nombre de la CLI	Tipo de propiedad	Descripción
Crear LUN	Proyecto	--	--	Define el proyecto que usa el LUN para heredar la configuración de parámetros.
	Nombre	--	--	Define el nombre del LUN.

Ubicación de la BUI	Nombre de la BUI	Nombre de la CLI	Tipo de propiedad	Descripción
	Tamaño del volumen	volsize	LUN local	Define el tamaño de volumen máximo y la unidad de medida. Para obtener más información, consulte “Tamaño del volumen” [512] .
	Aprovisionamiento fino	sparse	LUN local	Cuando se la selecciona, indica solo la cantidad de espacio consumido físicamente por los datos. Para obtener más información, consulte “Aprovisionamiento fino” [512] .
	Tamaño de bloque de volumen	volblocksize	Hora de creación	Tamaño de bloque nativo para los LUN; cualquier potencia de 2 desde 512 B hasta 1 MB, el valor predeterminado es 8 KB.
	En línea	status	LUN local	Indica si está en línea o no.
	Grupo de destinos	targetgroup	LUN local	Muestra grupos de destinos usados al exportar un LUN.
	Grupo(s) de iniciadores	initiatorgroup	LUN local	Muestra grupos de iniciadores que tienen acceso al LUN.
	Punto de montaje	mountpoint	Heredada	Controla la ruta de acceso usada para exportar sistemas de archivos. Para obtener más información, consulte “Punto de montaje” [504] .
	Número de LU	lunumber	LUN local	Establece el número de unidades lógicas en cero o asigna el número automáticamente.
	Cifrado	encryption	Heredada	Define el tipo de cifrado. Para obtener más información, consulte “Gestión de claves de cifrado” [833] .
	Heredar clave	--	--	Si se selecciona, esta opción indica que la clave de cifrado se hereda del proyecto principal.

Propiedades de LUN

Ubicación de la BUI	Nombre de la BUI	Nombre de la CLI	Tipo de propiedad	Descripción
	Clave	key	Heredada	Establece una clave de cifrado específica que se usa cuando la clave no se hereda del proyecto principal.
	Nombre de clave	keyname	Estática	Identifica la clave.
	GUID	lunguid	Solo lectura, local de LUN	Identificador globalmente único, de solo lectura que identifica al dispositivo SCSI.
General - Uso de espacio - Datos	Tamaño del volumen	volsize	LUN local	Define el tamaño de volumen máximo y la unidad de medida. Para obtener más información, consulte “Tamaño del volumen” [512] .
	Aprovisionamiento fino	sparse	LUN local	Cuando se la selecciona, indica solo la cantidad de espacio consumido físicamente por los datos. Para obtener más información, consulte “Aprovisionamiento fino” [512] .
General - Propiedades (Heredar de proyecto)	Desduplicación de datos (advertencia)	dedup	Heredada	Controla si las copias duplicadas de los datos se eliminan. Para obtener más información, consulte “Desduplicación de datos” [505] .
	Compresión de datos	compression	Heredada	Controla si los datos están comprimidos antes de escribirlos en el disco. Para obtener más información, consulte “Compresión de datos” [507] .
	Total de control	checksum	Heredada	Controla el total de control utilizado para los bloques de datos. Para obtener más información, consulte “Total de control” [508] .
	Replicación adicional	copies	Heredada	Controla la cantidad de copias almacenadas en cada bloque, más allá de la redundancia de la agrupación de almacenamiento. Para

Ubicación de la BUI	Nombre de la BUI	Nombre de la CLI	Tipo de propiedad	Descripción
				obtener más información, consulte “Replicación adicional” [510].
	Uso del dispositivo de caché	secondarycache	Heredada	Controla si los dispositivos de caché se utilizan para el recurso compartido. Para obtener más información, consulte “Uso del dispositivo de caché” [508].
	Desviación de escritura síncrona	logbias	Heredada	Controla el comportamiento al realizar trabajos de mantenimiento de escrituras síncronas. Para obtener más información, consulte “Desviación de escritura síncrona” [509].
	Prevención de destrucción	nodestroy	Heredada	Cuando se la configura, evita que se destruyan recursos compartidos o proyectos. Para obtener más información, consulte “Prevención de destrucción” [511].
Propiedades personalizadas (Heredar de proyecto)	Esquema	schema	--	Se pueden agregar según sea necesario para anexas etiquetas definidas por el usuario a proyectos y recursos compartidos. Para obtener más información, consulte “Trabajo con esquemas” [571].
Protocolos - Opciones de uso compartido	En línea	status	LUN local	Indica si está en línea o no.
	Grupo de destinos	targetgroup	LUN local	Muestra grupos de destinos usados al exportar un LUN.
	Grupo(s) de iniciadores: LU number (LUN)	initiatorgroup	LUN local	Muestra grupos de iniciadores que tienen acceso al LUN.
Protocolos - Comportamiento de caché de escritura	Escritura en caché activada	writetocache	LUN local	Controla si la caché del LUN realiza operaciones de escritura.

Propiedades de LUN

Ubicación de la BUI	Nombre de la BUI	Nombre de la CLI	Tipo de propiedad	Descripción
Instantáneas - Propiedades (Heredar de proyecto)	Etiqueta de instantánea programada	snaplabel	Heredada	Agrega una etiqueta definida por el usuario a cada instantánea programada y aparece en blanco de forma predeterminada.
Instantáneas - Instantáneas	Nombre	--	--	Especifica el nombre de la instantánea.
	Creación	--	--	Especifica la fecha y la hora de creación de la instantánea.
	Unique (Único)	--	--	Indica la cantidad de espacio único utilizado por la instantánea.
	Total	--	--	Indica la cantidad total de espacio al que hace referencia la instantánea.
	Clones	--	--	Muestra la cantidad de clones de la instantánea.
Instantáneas - Programas	Frecuencia	frequency	Hora de creación	Indica con qué frecuencia se toma la instantánea.
	Mantener al máximo	keep	Hora de creación	Controla la política de retención de las instantáneas.
Replicación (Heredar de proyecto)/Crear nuevas acciones	Destino	target	Heredada	Identifica el sistema de destino de replicación.
	Agrupación	pool	Heredada	Especifica la agrupación de almacenamiento en el destino donde se replicará este proyecto.
	Ruta de exportación de datos	export_path	Heredada	Indica la ruta de exportación de los datos.
	Limite de ancho de banda	max_bandwidth	Heredada	Especifica una velocidad máxima para esta actualización de replicación (en términos de cantidad de datos transferidos por la red por segundo).
	Activar cifrado SSL	use_ssl	Heredada	Controla si se deben cifrar datos por cable mediante SSL.
	Disable compression (Desactivar compresión)	compression	Heredada	Controla si la compresión está activada o desactivada.

Ubicación de la BUI	Nombre de la BUI	Nombre de la CLI	Tipo de propiedad	Descripción
Uso	Incluir instantáneas	include_snaps	Heredada	Controla si las actualizaciones de replicación incluyen instantáneas de no replicación.
	Retener instantáneas de usuario en destino	retain_user_snaps_on_target	Heredada	Cuando se la configura, las instantáneas generadas por el usuario se conservan en el destino de la replicación.
	Frecuencia de actualización	continuous	Heredada	Controla si la acción se replica continuamente o en intervalos manuales o programados.
	Datos con referencia	space_data	Solo lectura	Muestra la cantidad total del espacio al que hace referencia el recurso compartido activo, independiente de las instantáneas.
	Datos de instantáneas	space_snapshots	Solo lectura	Muestra la cantidad total de datos que en la actualidad tienen todas las instantáneas del recurso compartido.
	Datos disponibles	space_available	Solo lectura	Muestra las cuotas del recurso compartido o del proyecto, o la capacidad absoluta de la agrupación.
	Espacio total	space_total	Solo lectura	Muestra la suma de los datos de referencia, los datos de instantáneas y la reserva sin uso.

Gestión de espacio de recursos compartidos

El dispositivo gestiona el almacenamiento físico mediante un modelo de almacenamiento en agrupaciones en el que los sistemas de archivos y los LUN comparten un espacio común. Los sistemas de archivos nunca tienen un tamaño específico asignado a ellos y solo ocupan la cantidad de espacio que necesitan. Los LUN reservan suficiente espacio físico para escribir todo el contenido del dispositivo, a menos que tengan aprovisionamiento fino, en cuyo caso se comportan como sistemas de archivos y utilizan solo la cantidad de espacio físicamente consumido por los datos.

Este sistema proporciona máxima flexibilidad y simplicidad de gestión en un entorno cuando a los usuarios generalmente se les confía hacer lo correcto. Un entorno más estricto, donde se supervisa o se restringe el uso de datos por parte del usuario, requiere una gestión más cuidadosa.

En estos temas se define la terminología y el modo de gestión del uso del espacio, ya sea por recurso compartido o por usuario, mediante el uso de cuotas y reservas.

- [“Terminología de recursos compartidos” \[540\]](#)
- [“Gestión de espacio de sistemas de archivos y proyectos” \[541\]](#)
- [“Configuración de cuotas de usuarios o grupos” \[542\]](#)
- [“Trabajo con gestión de identidad” \[543\]](#)
- [“Estadísticas de uso del recurso compartido” \[546\]](#)

Terminología de recursos compartidos

Antes de entrar en detalles, es importante comprender algunos términos básicos que se utilizan cuando se habla del uso del espacio en el dispositivo.

- **Datos físicos:** tamaño de los datos almacenados físicamente en el disco. Normalmente, equivale al tamaño lógico de los datos correspondientes, pero puede ser diferente en la fase de compresión o debido a otros factores. Esto incluye el espacio del recurso compartido activo y de todas las instantáneas. El recuento de espacio generalmente se aplica y se gestiona según el espacio físico.
- **Datos lógicos:** cantidad de espacio consumida lógicamente por un sistema de archivos. No se toma en cuenta la compresión, y se puede visualizar como un límite superior teórico sobre la cantidad de espacio consumido por el sistema de archivos. La copia del sistema de archivos a otro dispositivo con un algoritmo de compresión diferente no consumirá más que esta cantidad. Esta estadística no se exporta explícitamente y, por lo general, solo se puede computar tomando la cantidad de espacio físico consumido y multiplicándola por la relación de compresión actual.
- **Datos de referencia:** representa la cantidad total del espacio al que hace referencia el recurso compartido activo, independiente de las instantáneas. Cantidad de espacio que el recurso compartido consumiría si se destruyeran todas las instantáneas. También se refiere a la cantidad de datos que puede gestionar directamente el usuario mediante los protocolos de datos.
- **Datos de instantánea:** representa la cantidad total de datos que en la actualidad tienen todas las instantáneas del recurso compartido. Se trata de la cantidad de espacio que quedaría libre si se destruyeran todas las instantáneas.

- **Cuota:** una cuota representa el límite de la cantidad de espacio que puede consumir cualquier entidad en particular. Se puede basar en el sistema de archivos, el proyecto, el usuario o el grupo, y es independiente de cualquier uso de espacio actual.
- **Reserva:** una reserva representa una garantía de espacio para un sistema de archivos o proyecto en particular. Aparta el espacio disponible del resto de la agrupación sin aumentar el espacio real consumido por el sistema de archivos. Esta configuración no se puede aplicar a usuarios ni grupos. Se puede crear la noción tradicional de un sistema de archivos de tamaño estático configurando la cuota y la reserva con el mismo valor.

Gestión de espacio de sistemas de archivos y proyectos

La manera más simple de aplicar cuotas y reservas es por proyecto o por sistema de archivos. Las cuotas y reservas no se aplican a los LUN, aunque su uso se toma en cuenta para las reservas o cuotas totales del proyecto.

Cuotas de datos: una cuota de datos aplica un límite a la cantidad de espacio que puede utilizar un proyecto o sistema de archivos. De forma predeterminada, incluye los datos del sistema de archivos y todas las instantáneas. Los clientes que intenten escribir nuevos datos obtendrán un error cuando el sistema esté completo, ya sea debido a una cuota o a que la agrupación de almacenamiento no tiene espacio. Según se describe en [“Gestión del espacio de instantáneas” \[591\]](#), es posible que este comportamiento no sea intuitivo en todas las situaciones, en particular cuando hay instantáneas presentes. La eliminación de un archivo podría provocar que el sistema de archivos escriba nuevos datos si una instantánea hace referencia a los bloques de datos; por lo tanto, podría ocurrir que la única manera de reducir el uso del espacio sea destruir las instantáneas existentes.

Si no se configuró la propiedad "incluir instantáneas", la cuota solo se aplica a los datos inmediatos a los que hace referencia el sistema de archivos, no a las instantáneas. El espacio utilizado por las instantáneas es aplicado por la cuota de nivel de proyecto, pero no se aplica de otra manera. En este caso, la eliminación de un archivo al que hace referencia una instantánea reducirá los datos de referencia del sistema de archivos, aunque el sistema en su totalidad utilice más espacio. Si la agrupación de almacenamiento está llena (en contraposición al sistema de archivos que alcanza una cuota predeterminada), la única manera de liberar espacio sería destruir las instantáneas.

Las cuotas de datos se aplican de manera estricta, lo que significa que a medida que el uso del espacio se acerca al límite, se debe regular la cantidad de datos que se pueden escribir ya que la cantidad exacta de datos que se van a escribir se desconoce hasta que se confirma la escritura. Esto puede afectar el rendimiento durante la operación en la cuota o cerca de ella. Por consiguiente, en general es conveniente mantenerse por debajo de la cuota durante los procedimientos de funcionamiento normal.

Las cuotas se gestionan mediante la BUI en Recursos compartidos > General > Uso de espacio > Datos. Se gestionan en la CLI como las propiedades `quota` y `quota_snap`.

Reservas de datos: la reserva de datos se utiliza para asegurarse de que un sistema de archivos o un proyecto tenga al menos una determinada cantidad de espacio disponible, aunque otros recursos compartidos del sistema intenten utilizar más espacio. Esta reserva sin uso se considera parte del sistema de archivos; por lo tanto, si el resto de la agrupación (o proyecto) alcanza su capacidad, el sistema de archivos aún puede escribir datos nuevos aunque haya otros recursos compartidos sin espacio.

De forma predeterminada, una reserva incluye todas las instantáneas de un sistema de archivos. Si no se configuró la propiedad "incluir instantáneas", la reserva solo se aplica a los datos inmediatos del sistema de archivos. El comportamiento al tomar instantáneas puede no ser siempre intuitivo. Si existe una reserva activa de datos del sistema de archivos (pero no de instantáneas), cada vez que se tome una instantánea, el sistema deberá reservar suficiente espacio para que esa instantánea se desvíe por completo, aunque esto nunca ocurra. Por ejemplo, si un sistema de archivos de 50 G tiene una reserva de 100 G sin instantáneas, al tomar la primera instantánea se reservarán 50 G adicionales de espacio y el sistema de archivos finalmente reservará 150 G de espacio total. Si hay espacio insuficiente para garantizar el desvío completo de los datos, se producirá un error al tomar la instantánea.

Las reservas se gestionan mediante la BUI en Recursos compartidos > General > Uso de espacio > Datos. Se gestionan en la CLI como las propiedades `reservation` y `reservation_snap`.

Gestión de espacio para replicación de LUN: al crear un LUN, se reserva todo el espacio físico que se configura para el LUN, de manera que los demás sistemas de archivos no pueden utilizarlo (a menos que se use aprovisionamiento fino). Para la replicación, cuando se genera una instantánea de un LUN de cualquier tamaño dado, también se reserva hasta dos veces el tamaño del LUN, en función de la cantidad de espacio del LUN que se haya usado.

En la siguiente lista se muestra el espacio adicional máximo requerido para replicar un LUN:

- Hasta 100 % en el origen entre actualizaciones
- Hasta 200 % en el origen durante una actualización
- Hasta 200 % en el destino

Configuración de cuotas de usuarios o grupos

Se pueden configurar cuotas en un usuario o grupo tanto en el nivel del sistema de archivos como del proyecto. Estas aplican el uso de datos físicos en función de la identidad POSIX o Windows del propietario o grupo del archivo o directorio. Existen diferencias significativas

entre las cuotas de usuario y de grupo, y las cuotas de datos de proyecto y de sistema de archivos:

- Las cuotas de grupos y usuarios se pueden aplicar a los sistemas de archivos y a los proyectos.
- Las cuotas predeterminadas pueden configurarse en el nivel de proyecto y pueden ser heredadas por los sistemas de archivos del proyecto.
- Las cuotas predeterminadas configuradas en el nivel de proyecto se pueden modificar en el nivel de sistema de archivos.
- Las cuotas predeterminadas se pueden recuperar y modificar con el protocolo SMB.
- Las cuotas de grupos y usuarios se implementan mediante la *aplicación demorada*. Eso significa que los usuarios podrán superar la cuota por un breve período antes de que se escriban los datos en el disco. Una vez que se hayan colocado los datos en el disco, el usuario recibirá un mensaje de error sobre los nuevos datos escritos, al igual que sucede con la cuota de nivel del sistema de archivos.
- Las cuotas de grupos y usuarios siempre se aplican respecto de los datos de referencia. Eso significa que las instantáneas no afectan las cuotas y un clon de una instantánea consumirá la misma cantidad de cuota efectiva, aunque se compartan los bloques subyacentes.
- No se admiten reservas de usuarios y grupos.
- Las cuotas de grupos y usuarios, a diferencia de las cuotas de datos, se almacenan con los datos del sistema de archivos regular. Esto significa que si el sistema de archivos se queda sin espacio, no podrá realizar cambios en las cuotas de grupos y usuarios. En primer lugar, debe tener espacio adicional disponible antes de modificar las cuotas de grupos y usuarios.
- Las cuotas de grupos y usuarios se envían como parte de cualquier replicación remota. El administrador debe garantizar que los entornos de servicios de nombres sean idénticos en el origen y el destino.
- La copia de seguridad y restauración NDMP de todo un recurso compartido incluirá las cuotas de cualquier usuario o grupo. Las restauraciones en un recurso compartido existente no afectarán las cuotas actuales.

Trabajo con gestión de identidad

Las cuotas de usuario y grupo aprovechan el servicio de asignación de identidad en el dispositivo. Esto permite a los usuarios y grupos ser especificados como identidades UNIX o Windows, según el entorno. Al igual que la titularidad de archivos, estas identidades se rastrean de las siguientes maneras:

- Si no existe una asignación UNIX, se almacena una referencia al ID de Windows.
- Si existe una asignación UNIX, se almacena el ID de UNIX.

Eso significa que el formato canónico de la identidad es el ID de UNIX. Si más tarde se cambia la asignación, se aplicará la nueva asignación en función de la nueva ID de UNIX. Si un usuario de Windows crea un archivo cuando no existe asignación y, posteriormente, se crea dicha asignación, los nuevos archivos se tratarán como un propietario diferente para los fines de formato de uso y control de acceso. Esto además implica que si se vuelve a utilizar una ID de usuario (es decir, se crea una nueva asociación de nombre de usuario), las cuotas o los archivos existentes aparecerán como propiedad del nuevo nombre de usuario.

Se recomienda determinar reglas de asignación de identidad antes de intentar utilizar sistemas de archivos de manera activa. De lo contrario, cualquier cambio en la asignación en ocasiones puede tener resultados sorprendentes.

Trabajo con espacio de nombres del sistema de archivos

A cada sistema de archivos del dispositivo, se le debe asignar un único punto de montaje que actúe como punto de acceso para los datos del sistema de archivos. Se pueden asignar puntos de montaje a los proyectos, pero estos solo actuarán como herramienta para gestionar el espacio de nombres mediante propiedades heredadas. Los proyectos nunca se montan y no exportan datos mediante ningún protocolo.

Todos los recursos compartidos se deben montar en `/export`. Si bien es posible crear un sistema de archivos montado en `/export`, no es necesario hacerlo. Si no existe dicho recurso compartido, los directorios se crearán dinámicamente según sea necesario debajo de esta parte de la jerarquía. Cada punto de montaje debe ser único dentro de un cluster.

- **Puntos de montaje anidados del espacio de nombres:** Es posible crear sistemas de archivos con puntos de montaje debajo de los puntos de montaje de los demás sistemas de archivos. En este caso, los sistemas de archivos principales se montan antes que los secundarios y viceversa. Se deben considerar los siguientes casos al utilizar puntos de montaje anidados:
 - Si no existe un punto de montaje, se creará uno, de propiedad de root y modo 0755. Este punto de montaje se puede eliminar, o no, al cambiar el nombre, destruir o mover el sistema de archivos, según el caso. Para mayor seguridad, los puntos de montaje se deben crear dentro del recurso compartido principal antes de crear el sistema de archivos secundario.
 - Si el directorio principal es de solo lectura y el punto de montaje no existe, se producirá un error en el montaje del sistema de archivos. Esto puede ocurrir sincrónicamente al crear un sistema de archivos, pero también puede ocurrir asincrónicamente al realizar un cambio a gran escala, por ejemplo, el cambio del nombre de los sistemas de archivos con puntos de montaje heredados.
 - Cuando se cambia el nombre de un sistema de archivos o se cambia su punto de montaje, todos los sistemas secundarios debajo del punto de montaje actual, además del

nuevo punto de montaje (si fuera diferente) se desmontan y se vuelven a montar una vez aplicado el cambio. Esto interrumpirá los servicios de datos que en la actualidad acceden al recurso compartido.

- La capacidad de recorrer automáticamente puntos de montaje anidados depende del protocolo, según se describe a continuación.
- **Espacio de nombre NFSv2, NFSv3 NFSv4.0 y NFSv4.1:** Según NFS, cada sistema de archivos es una exportación única que se hace visible mediante el protocolo MOUNT. NFSv2 y NFSv3 no tienen manera de recorrer los sistemas de archivos anidados, y se debe acceder a cada sistema de archivos mediante su ruta completa. Si bien los puntos de montaje anidados aún funcionan, los intentos por cruzar un punto de montaje anidado generarán un directorio vacío en el cliente. Si bien esto se puede mitigar mediante el uso de montajes automáticos, la compatibilidad transparente con puntos de montaje anidados en un entorno dinámico requiere NFSv4.0 o NFSv4.1.

NFSv4.0 y NFSv4.1 tienen varias mejoras en comparación con NFSv3 en lo que respecta a los puntos de montaje. En primer lugar, se pueden montar los directorios principales, aun cuando no existe un recurso compartido disponible en ese punto de la jerarquía. Por ejemplo, si se compartiera `/export/home`, sería posible montar `/export` en el cliente y recorrer las exportaciones reales de manera transparente. Aún más importante, algunos clientes de NFSv4.0 y NFSv4.1 (incluido Linux) admiten montajes automáticos en el lado del cliente, denominados ocasionalmente "montajes duplicados". Con dicho cliente, cuando un usuario recorre un punto de montaje, el sistema de archivos secundario se monta automáticamente en el punto de montaje local adecuado y se elimina cuando el sistema de archivos se desmonta en el cliente. Desde la perspectiva del servidor, se trata de solicitudes de montaje separadas, pero están unidas con el cliente para formar un espacio de nombres del sistema de archivos sin problemas.

- **Espacio de nombres en SMB:** El protocolo SMB no utiliza puntos de montaje, ya que cada recurso compartido está disponible por nombre de recurso. Sin embargo, cada sistema de archivos debe tener un punto de montaje único. En la actualidad no se admiten puntos de montaje anidados (múltiples sistemas de archivos dentro de un recurso) y cualquier intento de recorrer un punto de montaje resultará en un directorio vacío.
- **Espacio de nombres en FTP, FTPS y SFTP:** Los sistemas de archivos se exportan mediante su punto de montaje estándar. Los puntos de montaje anidados se admiten plenamente y son transparentes para el usuario. Sin embargo, no es posible dejar de compartir un sistema de archivos anidado cuando se comparte el principal. Si se comparte un punto de montaje principal, también se compartirán los puntos de montaje secundarios.
- **Espacio de nombres en HTTP y HTTPS:** Los sistemas de archivos se exportan en el directorio `/shares`, de manera que un sistema de archivos en `/export/home` aparecerá en `/shares/export/home` mediante HTTP/HTTPS. Los puntos de montaje anidados se admiten plenamente y son transparentes para el usuario. El mismo comportamiento relacionado con opciones de recursos compartidos conflictivos descrito en la sección del protocolo de FTP también se aplica al HTTP.

Estadísticas de uso del recurso compartido

A la izquierda de la vista (debajo del panel del proyecto contraído), hay una tabla en la que se explican las estadísticas de uso del espacio actual. Estas estadísticas se utilizan para un recurso en particular (al editar un recurso compartido) o para la agrupación en general (al observar la lista de recursos compartidos). Si hay propiedades con el valor cero, se excluyen de la tabla.

Algunas de las estadísticas de uso también se muestran en el contexto de la CLI `shares show`.

En la siguiente tabla, se describen las propiedades de uso de la BUI y la CLI.

Nombre de la BUI	Nombre de la CLI	Descripción
Espacio disponible	--	Esta estadística se muestra de manera implícita como capacidad en términos de porcentaje de capacidad en el título. El espacio disponible refleja las cuotas del recurso compartido o del proyecto, o la capacidad absoluta de la agrupación. El número que se muestra aquí representa la suma del espacio total utilizado y la cantidad de espacio disponible.
Datos con referencia	usage_data	La cantidad de datos a que hacen referencia los datos. Esto incluye todos los datos del sistema de archivos o bloques LUN, además de los metadatos requeridos. Gracias a la compresión, este valor puede ser muy inferior al tamaño lógico de los datos incluidos en el recurso compartido. Si el recurso compartido es un clon de una instantánea, este valor puede ser inferior al almacenamiento físico que podría incluir en teoría, y puede ser cero.
Datos de instantáneas	usage_snapshots	Cantidad de espacio utilizado por todas las instantáneas del recurso compartido, incluidas las instantáneas del proyecto. Este tamaño no es igual a la suma del espacio único consumido por todas las instantáneas. Los bloques a los que hacen referencia varias instantáneas no están incluidos en las estadísticas de uso por instantánea, pero aparecerán en el total de datos de la instantánea del recurso compartido.
Reserva sin uso	--	Si un sistema de archivos tiene un juego de reserva, este valor indica la cantidad de espacio restante reservada para el sistema de archivos. Este valor no está configurado para los LUN. El dispositivo impide que otros recursos compartidos consuman este espacio, lo que garantiza una cantidad de espacio suficiente para el sistema de archivos. Si la reserva no incluye instantáneas, debe haber espacio suficiente al tomar una instantánea para que se sobrescriba toda la instantánea. Para obtener más información acerca de las reservas, consulte “Propiedades de sistema de archivos” [525] .

Nombre de la BUI	Nombre de la CLI	Descripción
Espacio total	usage_total	La suma de los datos de referencia, los datos de instantáneas y la reserva sin uso.

Protocolos de recursos compartidos y proyectos

Cada recurso compartido tiene propiedades específicas del protocolo que definen el comportamiento de protocolos diferentes para ese recurso compartido. Estas propiedades pueden ser definidas para cada recurso compartido o heredadas del proyecto del recurso compartido.

En el caso de iSCSI, los iniciadores pueden detectar el destino mediante uno de los mecanismos descritos en [“Configuración de una red de área de almacenamiento \(SAN\)” \[224\]](#).

Para obtener información acerca de las propiedades de protocolo admitidas, consulte las secciones siguientes:

- [“Protocolo NFS” \[547\]](#)
- [“Protocolo SMB” \[555\]](#)
- [“Protocolo HTTP” \[563\]](#)
- [“Protocolo FTP” \[563\]](#)
- [“Protocolo SFTP” \[563\]](#)
- [“Protocolo TFTP” \[564\]](#)

Temas relacionados

- [“Configuración de NFS” \[423\]](#)
- [“Configuración de SMB” \[442\]](#)

Protocolo NFS

En esta sección, se incluyen los siguientes temas:

- [“Propiedades del protocolo NFS” \[548\]](#)
- [“Excepciones del modo de recurso compartido de NFS” \[549\]](#)
- [“Codificaciones de juegos de caracteres de protocolos NFS” \[553\]](#)
- [“Modos de seguridad del protocolo NFS” \[554\]](#)

Para obtener más información acerca del protocolo NFS, utilice estos temas:

- “Configuración de NFS” [423]
- “Propiedades de sistema de archivos” [525]
- “Propiedades de proyecto” [517]
- NFSv2 and NFSv3 Security (RFC 2623) (<http://www.ietf.org/rfc/rfc2623.txt>)
- NFSv4 Protocol (RFC 7530) (<http://www.ietf.org/rfc/rfc7530.txt>)
- NFSv4.1 Protocol (RFC 5661) (<https://tools.ietf.org/html/rfc5661>)

Para obtener información acerca de otros protocolos admitidos, consulte las secciones siguientes:

- “Protocolo SMB” [555]
- “Protocolo HTTP” [563]
- “Protocolo FTP” [563]
- “Protocolo SFTP” [563]
- “Protocolo TFTP” [564]

Propiedades del protocolo NFS

Cada recurso compartido tiene propiedades específicas del protocolo que definen el comportamiento de protocolos diferentes para ese recurso compartido. Estas propiedades pueden ser definidas para cada recurso compartido o heredadas del proyecto del recurso compartido. En la siguiente tabla, se muestran las propiedades del protocolo NFS y los valores posibles.

TABLA 128 Propiedades del protocolo NFS

Propiedad	Valores de la CLI	Tipo de propiedad	Descripción
Modo de recurso compartido	off rw ro	Heredada	Determina si el recurso compartido está disponible solo para lectura, para lectura y escritura, o para ninguna de estas opciones. Consulte “Protocolos de recursos compartidos y proyectos” [547].
Desactivar creación del archivo setuid/setgid	nosuid	Heredada	Si está seleccionada, los clientes no podrán crear archivos con bits setuid (S_ISUID) y setgid (S_ISGID) configurados, ni activar estos bits en los archivos existentes mediante la llamada del sistema chmod(2).
Evitar que los clientes monten subdirectorios	nosub	Heredada	Si está seleccionada, los clientes no podrán montar subdirectorios directamente. Se les obligará a montar la raíz del recurso

Propiedad	Valores de la CLI	Tipo de propiedad	Descripción
			compartido. Nota: Esto es aplicable solo a los protocolos NFSv2 y NFSv3, no a NFSv4.0 ni NFSv4.1.
Asignación de usuarios anónimos	anon	Heredada	A menos que la opción root esté vigente para un cliente en particular, el usuario root de ese cliente se trata como un usuario desconocido, y todos los intentos de dicho usuario por acceder a los archivos del recurso compartido serán considerados intentos de un usuario con este uid. Las ACL y los bits de acceso de este archivo se evaluarán normalmente.
Juego de caracteres	Consulte los valores posibles en Codificaciones de juegos de caracteres .	Heredada	Configura el juego de caracteres por defecto para todos los clientes.
Modo de seguridad	sec= Consulte una lista de valores posibles en Modos de seguridad .	Heredada	Configura el modo de seguridad de todos los clientes.
Enforce reserved ports for system authentication (Forzar puertos reservados para autenticación del sistema)	resvport	Heredada	Cuando se configura en un recurso compartido o un proyecto en combinación con el modo de seguridad de autenticación del sistema, los clientes NFS deben usar puertos TCP con números bajos ("reservados"). Algunos clientes NFS, como Oracle Solaris y Linux, usan puertos TCP con números bajos por defecto. Otros clientes, como Windows, tal vez requieran configuración.

Excepciones del modo de recurso compartido de NFS

Es posible definir excepciones para el modo de recurso compartido global para clientes o juegos de clientes. Para ello, se deben definir modos de recurso compartido específicos para el cliente o *excepciones*. Para restringir el acceso a determinados clientes, defina el modo de recurso compartido global en none y otorgue cada vez más acceso a grupos más pequeños. Por ejemplo, puede crear un recurso compartido con el modo de recurso compartido global definido en none, el cual deniega el acceso a todos los clientes y, luego, otorgar acceso de solo lectura a un subjuego de los clientes. Además, puede otorgar acceso de lectura/escritura a un subjuego aún más pequeño de los clientes y, finalmente, solo los host de confianza tendrán acceso root y de lectura/escritura.

Los modos de recurso compartido específicos del cliente tienen prioridad por sobre el modo de recurso compartido global. El cliente tiene permitido el acceso en función del modo de recurso

compartido específico del cliente que se especifique en una excepción. Si no hay excepciones, el cliente recibe acceso en función del modo de recurso compartido global.

TABLA 129 Tipos de clientes

Tipo	Prefijo de la CLI	Descripción	Ejemplo
Host(FQDN) o grupo de red	none	Un único cliente cuya dirección IP se convierte en el nombre totalmente cualificado especificado o un grupo de red que contiene los nombres totalmente cualificados en los cuales se convierte la dirección IP del cliente.	hostname.sf.example.com
Dominio DNS	.	Todos los clientes con direcciones IP que se convierten en un nombre totalmente cualificado que termina con este sufijo.	sf.example.com
Subred IPv4	@	Todos los clientes con direcciones IP que se encuentran dentro de la subred IPv4 especificada, expresada en la notación CIDR..	192.0.2.254/22
Subred IPv6	@	Todos los clientes con direcciones IP que se encuentran dentro de la subred IPv6 especificada, expresada en la notación CIDR..	2001:db8:410:d43::/64

Para cada cliente o juego de clientes, debe especificar si el cliente tiene acceso de solo lectura o acceso de lectura y escritura al recurso compartido. Si está configurando una excepción de NFS, también debe especificar si el cliente tiene privilegios de usuario root o si se lo debe considerar como un usuario sin acceso root.

Gestión de grupos de red

Los grupos de red se pueden usar para controlar el acceso de las exportaciones del NFS. Sin embargo, gestionar grupos de red puede ser complejo. En su lugar, considere usar reglas de subred de IP o reglas de dominio DNS.

Si se usan grupos de red, se resolverán desde NIS o LDAP, según qué servicio esté activado. Si se usa LDAP, cada grupo de red se debe encontrar en la ubicación por defecto, ou=Netgroup, (DN de base), y se debe usar un esquema estándar.

El componente de nombre de usuario de una entrada de grupo de red generalmente no afecta el NFS; solo el nombre del host resulta significativo. Los nombres de host incluidos en grupos de red deben ser canónicos y, si se resuelven mediante DNS, deben ser completos. Es decir, el subsistema NFS intentará verificar que la dirección IP del cliente solicitante se convierta en un nombre de host canónico que coincida con el FQDN especificado o con uno de los miembros

de uno de los grupos de red especificados. Esta coincidencia debe ser exacta, incluidos todos los componentes del dominio; de lo contrario, la excepción no coincidirá y se intentará la excepción siguiente. Para obtener más información sobre la resolución de nombres de hosts, consulte [DNS](#).

A partir de la versión de software 2013.1.0, los usuarios del cliente UNIX pueden pertenecer a un máximo de 1024 grupos sin una degradación del rendimiento. Las versiones anteriores admitían hasta 16 grupos por usuario del cliente UNIX.

Modos de recurso compartido de NFS y opciones de excepciones

En la CLI, todas las excepciones y los modos de recursos compartidos de NFS se especifican mediante una única cadena de opciones para la propiedad `sharenfs`. Esta cadena es una lista de valores separados por comas. Debe comenzar con `ro`, `rw`, `on` u `off`, como analogía de los modos de recursos compartidos globales descritos para la BUI.

TABLA 130 Valores de modos de recurso compartido de NFS (BUI y CLI)

Valores de modos de recurso compartido de la BUI	Valores de modos de recurso compartido de la CLI	Descripción	Ejemplo
Ninguno	<code>off</code>	El modo de recurso compartido está desactivado.	<code>sharenfs=off</code>
	<code>on</code>	El nombre del recurso compartido es el nombre del juego de datos y está disponible para lectura y escritura o solo para lectura si las excepciones de NFS <code>rw</code> o <code>ro</code> están definidas. El modo de recurso compartido está desactivado para todos los otros clientes.	<code>sharenfs="on, ro=sf.example.com"</code>
	<code>resource_name</code>	El nombre del recurso compartido es el nombre del recurso y está disponible para lectura y escritura o solo para lectura si las excepciones de NFS <code>rw</code> o <code>ro</code> están definidas. El modo de recurso compartido está desactivado para todos los otros clientes.	<code>sharenfs="myshare, ro=sf.example.com"</code>
Lectura y escritura	<code>on</code>	El nombre del recurso compartido es el nombre del juego de datos y está disponible para lectura y escritura para todos los clientes si no hay excepciones de NFS.	<code>sharenfs=on</code>
	<code>rw</code>	El nombre del recurso compartido es el nombre del juego de datos y está disponible para lectura y escritura para todos los clientes excepto para los que se definió la excepción <code>ro</code> .	<code>sharenfs=rw 0</code> <code>sharenfs="rw, ro=sf.example.com"</code>

Valores de modos de recurso compartido de la BUI	Valores de modos de recurso compartido de la CLI	Descripción	Ejemplo
	<i>resource_name</i>	El nombre del recurso compartido es el nombre del recurso y está disponible para lectura y escritura para todos los clientes si no hay excepciones de NFS.	sharenfs=myshare
	<i>resource_name, rw</i>	El nombre del recurso compartido es el nombre del recurso y está disponible para lectura y escritura para todos los clientes excepto para los que se definió la excepción ro. Las excepciones de NFS pueden o no estar definidas.	sharenfs="myshare, rw" O sharenfs="myshare, rw, ro=sf.example.com"
Solo lectura	ro	El nombre del recurso compartido es el nombre del juego de datos y está disponible solo para lectura para todos los host excepto para los que se definió la excepción rw.	sharenfs="ro, rw=sf.example.com"
	<i>resource_name, ro</i>	El nombre del recurso compartido es el nombre del recurso y está disponible solo para lectura para todos los clientes excepto para los que se definió la excepción rw. Las excepciones de NFS pueden o no estar definidas.	sharenfs="myshare, ro" O sharenfs="myshare, ro, rw=sf.example.com"

En el ejemplo siguiente, se configura el modo de recurso compartido para todos los clientes en solo lectura. Los usuarios root de todos los clientes tendrán acceso a los archivos del recurso compartido como si fueran el usuario genérico nobody.

```
set sharenfs=ro
```

También se podrá agregar cualquiera de las opciones `nosuid` y `anon`, o ambas. Por lo tanto, para definir la asignación de todos los usuarios desconocidos con el UID 153762, debería especificar lo siguiente:

```
set sharenfs="ro,anon=153762"
```

Nota - Los valores de las propiedades de la CLI que contienen el carácter = deben estar entre comillas.

Se pueden especificar excepciones adicionales de NFS si se anexa texto con el formato *option=collection*, donde *option* equivale a `ro`, `rw` o `root`, y define el tipo de acceso que se otorgará a la recopilación de clientes. La recopilación es especificada por el carácter de prefijo de la tabla Tipos de cliente y un nombre de dominio/nombre de host DNS o número de red CIDR. Por ejemplo, para otorgar acceso de lectura y escritura a todos los hosts del dominio `sf.example.com` y acceso root a los de la red `192.168.44.0/24`, puede utilizar:

```
set sharenfs="ro,anon=153762,rw=.sf.example.com,root=@192.168.44.0/24"
```

Nota - Este ejemplo es aplicable solo a excepciones de NFS.

Los nombres de grupos de red se pueden utilizar en cualquier lugar donde se puede utilizar un nombre de host completo. Por ejemplo, puede permitir el acceso de lectura y escritura al grupo de red `engineering` de la siguiente manera:

```
set sharenfs="ro,rw=engineering"
```

Codificaciones de juegos de caracteres de protocolos NFS

En general, no se especifica la codificación del juego de caracteres utilizada para el nombre de archivos. Los protocolos NFSv3 y NFSv2 no especifican el juego de caracteres. NFSv4.0 y NFSv4.1 deberían usar UTF-8, pero no todos los clientes lo hacen y el servidor no aplica esta restricción. Si la opción de solo UTF-8 está desactivada para un recurso compartido, estos nombres de archivos se escriben literalmente en el sistema de archivos sin tener información de su codificación. Eso significa que solo pueden ser interpretados por los clientes que utilizan la misma codificación. Sin embargo, SMB exige el almacenamiento de nombres de archivos como UTF-8 para que puedan ser interpretados por el servidor. De esta manera, resulta imposible admitir codificaciones arbitrarias de clientes y, al mismo tiempo, se permite el acceso mediante SMB.

A fin de admitir dichas configuraciones, la codificación del juego de caracteres se puede configurar para todos los recursos compartidos o por cliente. Se admiten las siguientes codificaciones de juegos de caracteres:

cp932	euc-tw	iso8859-7	koi8-r
euc-cn	iso8859-1	iso8859-8	shift_jis
euc-jp	iso8859-2	iso8859-9	
euc-jpms	iso8859-5	iso8859-13	
euc-kr	iso8859-6	iso8859-15	

El comportamiento por defecto consiste en dejar la codificación del juego de caracteres sin especificar (pasarla por alto). La BUI permite elegir del juego de caracteres mediante el mecanismo de listas de excepciones estándar. En la CLI, cada juego de caracteres se convierte en una opción con uno o varios hosts; * indica la configuración de la totalidad del recurso compartido. Por ejemplo:

```
hostname:shares default> set sharenfs="rw,euc-kr=*
```

Compartirá el sistema de archivos con `euc-kr` como la codificación por defecto. Por ejemplo:

```
hostname:shares default> set sharenfs="rw,euc-kr=host1.domain.com,euc-jp=host2.domain.com"
```

Utilice la codificación por defecto para todos los clientes excepto `host1` y `host2`, los cuales utilizarán `euc-kr` y `euc-jp`, respectivamente. El formato de las listas del `host` es igual al de otras opciones de CLI NFS.

Recuerde que algunos clientes NFS no admiten correctamente configuraciones locales alternativas. Para obtener más información, consulte la documentación del cliente NFS.

Modos de seguridad del protocolo NFS

Los modos de seguridad se configuran por recurso compartido. En la siguiente lista, se describe la configuración de seguridad de Kerberos:

- **krb:** autenticación de usuario final mediante Kerberos V5.
- **krb5i:** krb5 más protección de integridad (los paquetes de datos están protegidos contra alteraciones).
- **krb5p:** krb5i más protección de privacidad (los paquetes de datos están protegidos contra alteraciones y cifrados).

Los modos de seguridad se especifican cuando se anexa texto con el formato `option=mode`, donde `option` equivale a `sec` y `mode` es la configuración de seguridad. Por ejemplo:

```
hostname: shares default> set sharenfs="sec=krb5"
```

Nota - Los valores de las propiedades de la CLI que contienen el carácter = deben estar entre comillas.

Al definir modos de seguridad, se pueden especificar combinaciones de varios tipos de Kerberos. La combinación de modos de seguridad permite el montaje de clientes con cualquiera de los tipos de Kerberos indicados en la lista, como se muestra en la siguiente tabla.

TABLA 131 Combinaciones de tipos de Kerberos

Configuración	Descripción
sys	Autenticación del sistema
krb5	Kerberos v5 únicamente; los clientes deben realizar el montaje con esta configuración.
krb5:krb5i	Kerberos v5, con integridad; los clientes pueden realizar el montaje con cualquiera de las configuraciones enumeradas.
krb5i	Kerberos v5 con integridad únicamente; los clientes deben realizar el montaje con esta configuración.
krb5:krb5i:krb5p	Kerberos v5, con integridad o privacidad; los clientes pueden realizar el montaje con cualquiera de las configuraciones enumeradas.
krb5p	Kerberos v5 con privacidad únicamente; los clientes pueden realizar el montaje con esta configuración.

Puertos reservados

Para configurar puertos reservados para la autenticación del sistema, use `resvport` como se muestra en el siguiente ejemplo:

```
set sharenfs="sec=sys,rw,resvport"
```

Tenga en cuenta que `resvport` solo se puede usar con el modo de seguridad de autenticación de sistema `sec=sys`.

Protocolo SMB

En esta sección, se incluyen los siguientes temas:

- [“Propiedades de protocolo SMB” \[555\]](#)
- [“Propiedad de almacenamiento en caché de lado de cliente” \[557\]](#)
- [“Propiedad de bloqueos oportunistas” \[558\]](#)
- [“Excepciones de modo de recurso compartido del protocolo SMB” \[559\]](#)
- [“ACL en el nivel de recurso compartido” \[562\]](#)

Para obtener más información acerca del protocolo SMB, consulte estos temas:

- [“Configuración de SMB” \[442\]](#)
- [“Propiedades de sistema de archivos” \[525\]](#)
- [“Propiedades de proyecto” \[517\]](#)

Para obtener información acerca de otros protocolos admitidos, consulte las secciones siguientes:

- [“Protocolo NFS” \[547\]](#)
- [“Protocolo HTTP” \[563\]](#)
- [“Protocolo FTP” \[563\]](#)
- [“Protocolo SFTP” \[563\]](#)
- [“Protocolo TFTP” \[564\]](#)

Propiedades de protocolo SMB

Cada recurso compartido tiene propiedades específicas del protocolo que definen el comportamiento de protocolos diferentes para ese recurso compartido. Estas propiedades pueden ser definidas para cada recurso compartido o heredadas del proyecto del recurso compartido.

TABLA 132 Propiedades de protocolo SMB

Propiedad de la BUI	Propiedad de la CLI	Tipo de propiedad	Descripción
Modo de recurso compartido	<code>off rw ro</code>	Heredada	Especifica si el recurso compartido está disponible solo para lectura, para lectura y escritura, o para ninguna de estas opciones. Consulte Tabla 134, “Valores de modos de recurso compartido de SMB (BUI y CLI)” en “Excepciones de modo de recurso compartido del protocolo SMB” [559].
Nombre de recurso	<code>resource_name</code>	Heredada	El nombre que utilizan los clientes SMB para hacer referencia a este recurso compartido. Es posible especificar excepciones de modo de recurso compartido para este recurso. Consulte Tabla 134, “Valores de modos de recurso compartido de SMB (BUI y CLI)” en “Excepciones de modo de recurso compartido del protocolo SMB” [559].
Activar enumeración basada en el acceso	<code>abe</code>	Heredada	Especifica si se debe realizar una enumeración basada en el acceso.
Activar acceso de invitado	<code>guestok</code>	Heredada	Especifica si se debe otorgar acceso de invitado. Esta propiedad está desactivada por defecto.
Es un espacio de nombres de DFS	<code>dfsroot</code>	Heredada	Especifica si este recurso compartido se aprovisiona como espacio de nombres de DFS independiente.
Política de almacenamiento en caché de lado de cliente	<code>csc</code>	Heredada	Las opciones de configuración por recurso compartido proporcionadas para permitir el almacenamiento en caché en el lado del cliente. Para obtener más información, consulte “ Propiedad de almacenamiento en caché de lado de cliente ” [557].
Política de bloqueo oportunista	<code>oplocks</code>	Heredada	Especifica si se deben activar los bloqueos oportunistas en el nivel de recurso compartido. Para obtener más información, consulte “ Propiedad de bloqueos oportunistas ” [558].
Activar disponibilidad continua	<code>cont_avail</code>	Heredada	Especifica si los clientes SMB3 pueden solicitar manejadores de archivos persistentes para el recurso compartido. Cuando se activa esta opción, el dispositivo puede almacenar el estado asociado con un manejador de archivos persistente en almacenamiento estable persistente. El estado se puede almacenar de manera transparente en caso de un fallo de controlador, como una operación de toma de control y failback en controladores en cluster. Los recursos compartidos SMB con disponibilidad continua no se pueden compartir por medio de NFS ni usar en

Propiedad de la BUI	Propiedad de la CLI	Tipo de propiedad	Descripción
			cargas de trabajo como las de directorio raíz, que tienen un número muy alto de aperturas y cierres. Los recursos compartidos SMB con disponibilidad continua solo se recomiendan para aplicaciones empresariales que tengan un número limitado de aperturas y cierres.
Cifrar acceso a datos	encrypt	Heredada	Especifica si se debe activar el cifrado SMB3 en el nivel de recurso compartido. Cuando se activa esta opción, el servidor SMB exige que los clientes cifren las solicitudes para acceder al recurso compartido. Es posible omitir esta imposición si el servidor permite el acceso no cifrado. Esta propiedad está desactivada por defecto. Para conocer las propiedades de cifrado SMB a nivel global, consulte "Cifrado de acceso a datos" y "Rechazo de acceso no cifrado" en "Propiedades del servicio SMB" [444] .
Omitir control de desvío	bypassstraverse	Heredada	Especifica si se debe omitir el control de desvío para el recurso compartido. Esta propiedad está desactivada por defecto. Cuando se desactiva esta opción, se utiliza la semántica de UNIX: siempre forzar los permisos de desvío de las carpetas durante el desplazamiento hacia un objeto en este recurso compartido. Cuando se activa esta opción, se utiliza la semántica de Windows: el acceso a un objeto de este recurso compartido depende de los derechos del usuario sobre ese objeto; se ignoran los permisos de desvío de las carpetas.

Propiedad de almacenamiento en caché de lado de cliente

La propiedad de almacenamiento en caché de lado de cliente (`csc`) controla si los archivos y los programas del recurso compartido se almacenan en caché en el cliente local para usarlos fuera de línea cuando no hay conexión con el dispositivo.

Valor de la BUI	Valor de la CLI	Descripción
Sin almacenamiento en caché	none	Desactiva el almacenamiento en caché de lado de cliente para el recurso compartido. Los archivos y programas del recurso compartido no están disponibles fuera de línea. Esta opción bloquea los archivos fuera de línea de la computadora cliente e impide que se hagan copias de

Valor de la BUI	Valor de la CLI	Descripción
		los archivos y los programas en la carpeta del recurso compartido.
Almacenamiento en caché manual	<code>manual</code>	Solo los archivos y los programas especificados se almacenan en caché en el cliente local y están disponibles fuera de línea. Esta es la opción por defecto en la configuración inicial de los recursos compartidos. Si se usa esta opción, por defecto no hay ningún archivo ni programa disponible fuera de línea. Puede controlar cuáles son los archivos y los programas a los que accede cuando no está conectado a la red.
Almacenamiento en caché automático de documentos	<code>documents</code>	Todos los archivos a los que se accede desde el recurso compartido se almacenan en caché en el cliente local y están disponibles fuera de línea. Los archivos se reintegran automáticamente cuando el cliente local vuelve a estar en línea. Los programas a los que se accede desde el recurso compartido no están disponibles fuera de línea a menos que se hayan almacenado en caché con anterioridad.
Almacenamiento en caché automático de programas	<code>programs</code>	Todos los programas a los que se accede desde el recurso compartido se almacenan en caché en el cliente local y están disponibles fuera de línea. Cuando está en línea, los programas se ejecutan desde el cliente local. Asimismo, todos los archivos a los que se accede desde el recurso compartido se almacenan en caché en el cliente local y están disponibles fuera de línea. Los archivos se reintegran automáticamente cuando el cliente local vuelve a estar en línea.

Propiedad de bloqueos oportunistas

Los bloqueos oportunistas son un mecanismo de almacenamiento en caché de clientes que facilita el almacenamiento en caché local para reducir el tráfico de red y mejorar el rendimiento. La propiedad (`oplocks`) controla si el servidor otorga o deniega los bloqueos oportunistas en el nivel del recurso compartido y se aplica tanto a bloqueos oportunistas de concesión (SMB 2.1 y posteriores) y heredados (SMB 2.0 y anteriores).

El cliente solicita un bloqueo oportunista sobre un archivo dentro de un recurso compartido y esa solicitud se otorga o deniega en función de la configuración del servidor y el estado actual del archivo. Si el cliente intenta acceder a un archivo de manera incongruente con los bloqueos oportunistas que ya se han otorgado para ese archivo, se produce un conflicto. En estos casos, el servidor inicia un proceso para romper los bloqueos oportunistas existentes antes de continuar con la operación que genera el conflicto.

La activación de los bloqueos oportunistas mejora el rendimiento cuando hay solo un cliente que accede a los archivos que están en un recurso compartido. Sin embargo, en algunas situaciones, como cuando varios clientes acceden simultáneamente al mismo archivo, puede

introducir una sobrecarga innecesaria. Así, los bloqueos oportunistas se pueden activar o desactivar por recurso compartido, en lugar de hacerlo de manera generalizada, en función del patrón de cargas de trabajo esperadas.

Si no se define una propiedad de bloqueos oportunistas en el nivel del recurso compartido, la configuración por defecto es la propiedad de bloqueos oportunistas globales en el nivel del servicio. Para obtener más información, consulte "Activar bloqueos oportunistas" en la sección [“Propiedades del servicio SMB” \[444\]](#).

Valor de la BUI	Valor de la CLI	Descripción	Ejemplo
Enabled	enabled	Activa los bloqueos oportunistas para un recurso compartido	set sharesmb="myshare, oplocks=enabled, abe=off, dfsroot=false"
Desactivado	disabled	Desactiva los bloqueos oportunistas para un recurso compartido	set sharesmb="myshare, oplocks=disabled, abe=off, dfsroot=false"
empty	--	La propiedad de bloqueos oportunistas no está activada ni desactivada. Utiliza la propiedad de bloqueos oportunistas globales cuando no está configurada la propiedad en el nivel del recurso compartido.	set sharesmb="myshare, abe=off, dfsroot=false"

Excepciones de modo de recurso compartido del protocolo SMB

Es posible definir excepciones para el modo de recurso compartido global para clientes o juegos de clientes. Para ello, se deben definir modos de recurso compartido específicos para el cliente o *excepciones*. Para restringir el acceso a determinados clientes, defina el modo de recurso compartido global en *none* y otorgue cada vez más acceso a grupos más pequeños. Por ejemplo, puede crear un recurso compartido con el modo de recurso compartido global definido en *none*, el cual deniega el acceso a todos los clientes y, luego, otorgar acceso de solo lectura a un subjuego de los clientes. Además, puede otorgar acceso de lectura/escritura a un subjuego aún más pequeño de los clientes y, finalmente, solo los host de confianza tendrán acceso de lectura/escritura.

TABLA 133 Tipos de clientes

Tipo	Prefijo de la CLI	Descripción	Ejemplo
Host(FQDN) o grupo de red	none	Un único cliente cuya dirección IP se convierte en el nombre totalmente cualificado especificado o un grupo de red que contiene los nombres	hostname.sf.example.com

Tipo	Prefijo de la CLI	Descripción	Ejemplo
		totalmente cualificados en los cuales se convierte la dirección IP del cliente.	
Dominio DNS	.	Todos los clientes con direcciones IP que se convierten en un nombre totalmente cualificado que termina con este sufijo.	sf.example.com
Subred IPv4	@	Todos los clientes con direcciones IP que se encuentran dentro de la subred IPv4 especificada, expresada en la notación CIDR..	192.0.2.254/22
Subred IPv6	@	Todos los clientes con direcciones IP que se encuentran dentro de la subred IPv6 especificada, expresada en la notación CIDR..	2001:db8:410:d43::/64

Para cada cliente o juego de clientes, debe especificar si el cliente tiene acceso de solo lectura o acceso de lectura y escritura al recurso compartido.

Gestión de grupos de red: los grupos de red se pueden usar para controlar el acceso de las exportaciones de SMB. Sin embargo, gestionar grupos de red puede ser complejo. En su lugar, considere usar reglas de subred de IP o reglas de dominio DNS.

Si se usan grupos de red, se resolverán desde NIS o LDAP, según qué servicio esté activado. Si se usa LDAP, cada grupo de red se debe encontrar en la ubicación por defecto, `ou=Netgroup`, (DN de base), y se debe usar un esquema estándar.

El componente de nombre de usuario de una entrada de grupo de red generalmente no afecta el SMB; solo el nombre del host resulta significativo. Los nombres de host incluidos en grupos de red deben ser canónicos y, si se resuelven mediante DNS, deben ser completos. Es decir, el subsistema de SMB intentará verificar que la dirección IP del cliente solicitante se convierta en un nombre de host canónico que coincida con el FQDN especificado o con uno de los miembros de uno de los grupos de red especificados. Esta coincidencia debe ser exacta, incluidos todos los componentes del dominio; de lo contrario, la excepción no coincidirá y se intentará la excepción siguiente. Para obtener más información sobre la resolución de nombres de hosts, consulte [DNS](#).

A partir de la versión de software 2013.1.0, los usuarios del cliente UNIX pueden pertenecer a un máximo de 1024 grupos sin una degradación del rendimiento. Las versiones anteriores admitían hasta 16 grupos por usuario del cliente UNIX.

Modos de recurso compartido de SMB y opciones de excepciones

En la CLI, todas las excepciones y los modos de recursos compartidos de SMB se especifican mediante una única cadena de opciones para la propiedad `sharesmb`. Esta cadena es una lista de

valores separados por comas. Debe comenzar con `ro`, `rw`, `on` u `off`, como analogía de los modos de recursos compartidos globales descritos para la BUI.

TABLA 134 Valores de modos de recurso compartido de SMB (BUI y CLI)

Valores de modos de recurso compartido de la BUI	Valores de modos de recurso compartido de la CLI	Descripción	Ejemplo
Ninguno	<code>off</code>	El modo de recurso compartido está desactivado.	<code>sharesmb=off</code>
	<code>on</code>	El nombre del recurso compartido es el nombre del juego de datos y está disponible para lectura y escritura o solo para lectura si las excepciones de SMB <code>rw</code> o <code>ro</code> están definidas. El modo de recurso compartido está desactivado para todos los otros clientes.	<code>sharesmb="on, ro=sf.example.com"</code>
	<code>resource_name</code>	El nombre del recurso compartido es el nombre del recurso y está disponible para lectura y escritura o solo para lectura si las excepciones de SMB <code>rw</code> o <code>ro</code> están definidas. El modo de recurso compartido está desactivado para todos los otros clientes.	<code>sharesmb="myshare, ro=sf.example.com"</code>
Lectura y escritura	<code>on</code>	El nombre del recurso compartido es el nombre del juego de datos y está disponible para lectura y escritura para todos los clientes si no hay excepciones de SMB.	<code>sharesmb=on</code>
	<code>rw</code>	El nombre del recurso compartido es el nombre del juego de datos y está disponible para lectura y escritura para todos los clientes excepto para los que se definió la excepción <code>ro</code> .	<code>sharesmb=rw 0</code> <code>sharesmb="rw, ro=sf.example.com"</code>
	<code>resource_name</code>	El nombre del recurso compartido es el nombre del recurso y está disponible para lectura y escritura para todos los clientes si no hay excepciones de SMB.	<code>sharesmb=myshare</code>
	<code>resource_name, rw</code>	El nombre del recurso compartido es el nombre del recurso y está disponible para lectura y escritura para todos los clientes excepto para los que se definió la excepción <code>ro</code> . Las excepciones de SMB pueden o no estar definidas.	<code>sharesmb="myshare, rw" 0</code> <code>sharesmb="myshare, rw, ro=sf.example.com"</code>
Solo lectura	<code>ro</code>	El nombre del recurso compartido es el nombre del juego de datos y está disponible solo para lectura para todos los host excepto para los que se definió la excepción <code>rw</code> .	<code>sharesmb="ro, rw=sf.example.com"</code>
	<code>resource_name, ro</code>	El nombre del recurso compartido es el nombre del recurso y está disponible solo para lectura para todos los clientes excepto para los que se definió la excepción <code>rw</code> . Las	<code>sharesmb="myshare, ro" 0</code> <code>sharesmb="myshare, ro, rw=sf.example.com"</code>

Valores de modos de recurso compartido de la BUI	Valores de modos de recurso compartido de la CLI	Descripción	Ejemplo
		excepciones de SMB pueden o no estar definidas.	

En el ejemplo siguiente, se configura el modo de recurso compartido para todos los clientes en solo lectura.

```
set sharesmb=ro
```

Es posible especificar excepciones de SMB adicionales si se anexa texto con el formato *option=collection*, donde *option* equivale a *ro* o *rw*. No se puede otorgar acceso root con excepciones de SMB. La recopilación es especificada por el carácter de prefijo de la tabla 114 y un nombre de dominio/nombre de host DNS o número de red CIDR.

Por ejemplo, para otorgar acceso de lectura y escritura a todos los hosts del dominio sf.example.com:

```
set sharesmb="ro,rw=.sf.example.com"
```

En este ejemplo, se otorga acceso de solo lectura a los clientes con las direcciones IP 2001:db8:410:d43::/64 y 192.0.2.254/22:

```
set sharesmb="on,ro=@[2001:db8:410:d43::/64]:@192.0.2.254/22"
```

Los nombres de grupos de red se pueden utilizar en cualquier lugar donde se puede utilizar un nombre de host completo. Por ejemplo, puede permitir el acceso de lectura y escritura al grupo de red engineering de la siguiente manera:

```
set sharesmb="ro,rw=engineering"
```

ACL en el nivel de recurso compartido

Una lista de control de acceso (ACL) de nivel de recurso compartido, cuando se la combina con la ACL de un archivo o un directorio en el recurso compartido, determina los permisos vigentes para ese archivo. Por defecto, esta ACL otorga control total a todos. Esta ACL proporciona otra capa de control de acceso superior a las ACL de archivos y permite realizar configuraciones de control de acceso más sofisticadas. Esta propiedad solo se puede determinar después de exportar el sistema de archivos mediante la configuración del nombre de recurso de SMB. Si el sistema de archivos no se exporta mediante el protocolo SMB, la configuración de la ACL de nivel de recurso compartido no se aplicará.

Cuando está activada la enumeración basada en el acceso, los clientes pueden ver entradas de directorios para los archivos que ellos no pueden abrir. Las entradas de directorio solo se filtran cuando el cliente no tiene acceso a ese archivo. Por ejemplo, si un cliente intenta abrir un archivo para obtener acceso de lectura y escritura, pero la ACL otorga acceso de solo lectura,

se producirá un error en esa solicitud abierta, pero el archivo aún será incluido en la lista de entradas.

Para obtener más información acerca de las ACL, consulte [“Listas de control de acceso para sistemas de archivos” \[564\]](#).

Protocolo HTTP

Cada recurso compartido tiene propiedades específicas del protocolo que definen el comportamiento de protocolos diferentes para ese recurso compartido. Estas propiedades pueden ser definidas para cada recurso compartido o heredadas del proyecto del recurso compartido. Para el protocolo HTTP (`sharedav`) y para un almacén de objetos, los usuarios pueden configurar el modo de recurso compartido para determinar si el sistema de archivos está disponible solo para lectura (`ro`), para lectura y escritura (`rw o on`) o para ninguna de las dos opciones (`off`).

Temas relacionados

- [“Propiedades de proyecto” \[517\]](#)
- [“Propiedades de sistema de archivos” \[525\]](#)

Protocolo FTP

Cada recurso compartido tiene propiedades específicas del protocolo que definen el comportamiento de protocolos diferentes para ese recurso compartido. Estas propiedades pueden ser definidas para cada recurso compartido o heredadas del proyecto del recurso compartido. Para el protocolo FTP (`shareftp`), los usuarios pueden configurar el modo de recurso compartido para determinar si el sistema de archivo está disponible solo para lectura (`ro`), para lectura y escritura (`rw o on`) o para ninguna de las dos opciones (`off`).

Temas relacionados

- [“Propiedades de proyecto” \[517\]](#)
- [“Propiedades de sistema de archivos” \[525\]](#)

Protocolo SFTP

Cada recurso compartido tiene propiedades específicas del protocolo que definen el comportamiento de protocolos diferentes para ese recurso compartido. Estas propiedades pueden ser definidas para cada recurso compartido o heredadas del proyecto del recurso compartido. Para el protocolo SFTP (`sharesftp`), los usuarios pueden configurar el modo de

recurso compartido para determinar si el sistema de archivo está disponible solo para lectura (`ro`), para lectura y escritura (`rw o on`) o para ninguna de las dos opciones (`off`).

Temas relacionados

- [“Propiedades de proyecto” \[517\]](#)
- [“Propiedades de sistema de archivos” \[525\]](#)

Protocolo TFTP

Cada recurso compartido tiene propiedades específicas del protocolo que definen el comportamiento de protocolos diferentes para ese recurso compartido. Estas propiedades pueden ser definidas para cada recurso compartido o heredadas del proyecto del recurso compartido. Para el protocolo TFTP (`sharetftp`), los usuarios pueden configurar el modo de recurso compartido para determinar si el sistema de archivo está disponible solo para lectura (`ro`), para lectura y escritura (`rw o on`) o para ninguna de las dos opciones (`off`).

Temas relacionados

- [“Propiedades de proyecto” \[517\]](#)
- [“Propiedades de sistema de archivos” \[525\]](#)

Listas de control de acceso para sistemas de archivos

Es posible configurar opciones para controlar el comportamiento de la ACL, además de controlar el acceso al directorio raíz del sistema de archivos.

Nota - Las ACL están disponibles solo para los sistemas de archivos.

Para obtener más información acerca de las ACL, consulte los siguientes temas:

- [“Acceso a directorio raíz” \[564\]](#)
- [“Comportamiento de la ACL en cambio de modo” \[566\]](#)
- [“Comportamiento de valores heredados de ACL” \[566\]](#)
- [“ACL de directorio raíz” \[568\]](#)

Acceso a directorio raíz

Para establecer un control de acceso básico para el directorio raíz del sistema de archivos, vaya a Recursos compartidos > Recursos compartidos > *Sistema de archivos* > Acceso. Estas

configuraciones se pueden gestionar en banda mediante cualquier protocolo que se utilice, pero también se pueden especificar aquí para su comodidad. Estas propiedades no se pueden cambiar en un sistema de archivos de solo lectura, ya que requieren el cambio de metadatos del directorio raíz del sistema de archivos.

- **Usuario:** el propietario del directorio raíz. Esto se puede especificar como ID de usuario o nombre de usuario. Para obtener más información sobre la asignación de usuarios de UNIX y Windows, consulte [Asignación de identidades](#). En el caso del acceso a NFS basado en UNIX, esto se puede cambiar desde el cliente con el comando `chown`.
- **Grupo:** el grupo del directorio raíz. Esto se puede especificar como ID de grupo o nombre de grupo. Para obtener más información sobre la asignación de grupos de UNIX y Windows, consulte [Asignación de identidades](#). En el caso del acceso a NFS basado en UNIX, esto se puede cambiar desde el cliente con el comando `chgrp`.
- **Permisos:** permisos UNIX estándar para el directorio raíz. En el caso del acceso a NFS basado en UNIX, esto se puede cambiar desde el cliente con el comando `chmod`. Los permisos se dividen en tres tipos.

Tipo de acceso	Descripción
Usuario	Usuario que es el propietario actual del directorio.
Grupo	Grupo que es el grupo actual del directorio.
Otros	Los demás accesos.

Para cada tipo de acceso, se pueden otorgar los siguientes permisos.

Tipo		Descripción
Lectura	R	Permiso para mostrar el contenido del directorio.
Escritura	W	Permiso para crear archivos en el directorio.*
Ejecución	X	Permiso para consultar entradas en el directorio. Si los usuarios tienen permisos de ejecución, pero no tienen permisos de lectura, pueden acceder a los archivos de manera explícita por nombre, pero no pueden mostrar el contenido del directorio.

Temas relacionados

- [“Comportamiento de la ACL en cambio de modo” \[566\]](#)
- [“Comportamiento de valores heredados de ACL” \[566\]](#)

- [“ACL de directorio raíz” \[568\]](#)

Comportamiento de la ACL en cambio de modo

Cuando se modifica una ACL mediante `chmod(2)` con los permisos user/group/other de UNIX estándar, la solicitud de cambio de modo simplificado interactuará con la ACL existente de diferentes maneras, según la configuración de esta propiedad. Para editar el comportamiento de ACL con respecto al cambio de modo, consulte Edición de un proyecto [BUI](#), [CLI](#).

TABLA 135 Valores de cambio de modo

Valor de la BUI	Valor de la CLI	Descripción
Descartar ACL	<code>discard</code>	Se descartan todas las entradas de la ACL que no representan el modo del directorio o del archivo. Este es el comportamiento por defecto.
Enmascarar ACL con el modo	<code>mask</code>	Se reducen los permisos de manera que no superen los bits de permisos de grupos, excepto que se trate de una entrada de usuario con el mismo UID que el propietario del archivo o directorio. En este caso, se reducen los permisos de la ACL de manera que no superen los bits de permisos de los propietarios. El valor de la máscara también conserva la ACL tras los cambios de modo, siempre que no se haya llevado a cabo una operación explícita de configuración de la ACL.
No cambiar ACL	<code>passthrough</code>	No se efectúan cambios en la ACL aparte de la generación de las entradas de la ACL necesarias para representar el nuevo modo del archivo o directorio.

Temas relacionados

- [“ACL de directorio raíz” \[568\]](#)
- [“Comportamiento de valores heredados de ACL” \[566\]](#)
- [“ACL de directorio raíz” \[568\]](#)

Comportamiento de valores heredados de ACL

Cuando se crea un nuevo archivo o directorio, es posible heredar la configuración de la ACL existente del directorio principal. Esta propiedad controla la manera en que funciona esta herencia. La configuración de esta propiedad generalmente solo afecta las entradas de la ACL indicadas como heredables (las demás entradas no se propagarán independientemente de la configuración de esta propiedad). Sin embargo, todas las entradas de las ACL triviales se

pueden heredar cuando se utilizan con SMB. Una ACL trivial representa las entradas UNIX tradicionales `owner/group/other`. Para editar el comportamiento de valores heredados de ACL, consulte Edición de un proyecto [BUI](#), [CLI](#).

TABLA 136 Valores de comportamiento heredados de ACL

Valor de la BUI	Valor de la CLI	Descripción
No heredar entradas	<code>discard</code>	No se heredan entradas de la ACL. El archivo o directorio se crea según el cliente y el protocolo que se utiliza.
Solo heredar entradas de denegación	<code>noallow</code>	Solo se heredan las entradas de ACL que especifican permisos <code>deny</code> .
Heredar todo excepto "escribir ACL" y "cambiar propietario"	<code>restricted</code>	Elimina los permisos <code>write_acl</code> y <code>write_owner</code> cuando se hereda la entrada de ACL, pero deja intactas las entradas de ACL heredables en caso contrario. Este es el valor por defecto.
Heredar todas las entradas	<code>passthrough</code>	Se heredan todas las entradas de ACL heredables. Generalmente, se utiliza el modo <code>passthrough</code> para crear todos los archivos <code>data</code> con el mismo modo en un árbol de directorio. El administrador configura la herencia de la ACL para crear todos los archivos con un modo, por ejemplo, <code>0664</code> o <code>0666</code> .
Heredar todo menos el permiso de "ejecución" cuando no está especificado	<code>passthrough-x</code>	Igual que <code>passthrough</code> , excepto que las entradas de ACL de propietario, grupo y todos heredan el permiso de ejecución solo si el modo de creación de archivos también solicita el bit de ejecución. La configuración <code>passthrough</code> funciona como se espera para los archivos de datos, pero se recomienda incluir de manera opcional el bit de ejecución del modo de creación de archivos en la ACL heredada. Un ejemplo es un archivo de salida que se genera desde las herramientas, como <code>cc</code> o <code>gcc</code> . Si la ACL heredada no incluye el bit de ejecución, el archivo de salida ejecutable del compilador no se podrá ejecutar hasta que se utilice <code>chmod(1)</code> para cambiar los permisos del archivo.
Heredar todo, pero preservar modo de cliente	<code>passthrough-mode-preserve</code>	Las entradas heredables de la ACL se heredan y, a la vez, preservan el modo de creación especificado por la aplicación. Esto conserva los bits de herencia de modo que SMB crea ACL que interoperan correctamente con los recursos compartidos a los que se accede mediante NFS y SMB simultáneamente. Esta configuración de la propiedad solo está disponible después de aplicar la actualización diferida para Passthrough de ACL con preservación de modo. Para obtener más información, consulte “Deferred Updates” in Oracle ZFS Storage Appliance Customer Service Manual .

Cuando se utiliza SMB para crear un archivo en un directorio con una ACL trivial, se heredan todas las entradas de la ACL. Como resultado, se genera el siguiente comportamiento:

- Los bits de herencia se muestran de manera diferente cuando se los visualiza en SMB o NFS. Cuando se visualiza el directorio de ACL en SMB, se muestran los bits de herencia. Los bits de herencia no se muestran en NFS.
- Cuando se crea un archivo en un directorio con SMB, las entradas de ACL se muestran como heredadas; sin embargo, cuando se visualiza mediante NFS, el directorio no tiene entradas de ACL heredables.
- Si se cambia la ACL para que deje de ser trivial, por ejemplo, al agregar una entrada de control de acceso (ACE), no se produce este comportamiento.
- Si se modifica la ACL mediante SMB, los bits de herencia sintéticos anteriores se convertirán en bits de herencia reales en la ACL resultante.

Temas relacionados

- [“Propiedades de proyecto” \[517\]](#)

ACL de directorio raíz

El acceso específico en archivos y directorios se gestiona mediante una lista de control de acceso (ACL, Access Control List). Una ACL describe los permisos otorgados, si existen, a grupos o usuarios específicos. El dispositivo admite ACL de estilo NFSv4.0 y NFSv4.1, a las que también se puede acceder mediante SMB. No se admiten ACL de borrador POSIX (utilizadas por NFSv3). Se pueden representar algunas ACL triviales mediante NFSv3, pero si se realizan cambios complicados en la ACL, se puede producir un comportamiento indefinido cuando se accede mediante NFSv3.

Al igual que el acceso al directorio raíz, esta propiedad solo afecta el directorio raíz del sistema de archivos. Las ACL se pueden controlar mediante la gestión de protocolos en banda, pero la BUI y la CLI ofrecen una manera de configurar la ACL solo para el directorio raíz del sistema de archivos. Puede utilizar herramientas de gestión en banda si la BUI no es una opción. El cambio de esta ACL no afecta los directorios y archivos existentes en el sistema de archivos. Según el comportamiento de herencia de la ACL, estas configuraciones pueden o no ser heredadas por los directorios y archivos recientemente creados. Sin embargo, cuando se utiliza SMB para crear un archivo en un directorio con una ACL trivial, se heredan todas las entradas de la ACL.

Una ACL se compone de una cantidad no específica de entradas de control de acceso (ACE, Access Control Entries). En cada ACE, se describe un tipo/destino, un juego de permisos, indicadores de herencia y un modo. Las ACE se aplican en orden, desde el comienzo de la ACL, para determinar si se debe permitir una acción determinada. Para obtener información sobre las ACL de configuración en banda mediante protocolos de datos, consulte la documentación del cliente adecuada. Aquí se describe la interfaz de la BUI para gestionar las ACL y el efecto sobre el directorio raíz.

TABLA 137 Recursos compartidos: tipos de ACL

Tipo	Descripción
Propietario	Propietario actual del directorio. Si se cambia el propietario, esta ACE se aplicará al nuevo propietario.
Grupo	Grupo actual del directorio. Si se cambia el grupo, esta ACE se aplicará al nuevo grupo.
Todos	Cualquier usuario.
Usuario designado	Usuario con el nombre designado en el campo <i>target</i> . El usuario se puede especificar como un ID de usuario o un nombre que se puede resolver mediante la configuración de servicio de nombres actual.
Grupo nombrado	Grupo con el nombre designado en el campo <i>target</i> . El grupo se puede especificar como un ID de grupo o un nombre que se puede resolver mediante la configuración de servicio de nombres actual.

TABLA 138 Recursos compartidos: modos de ACL

Modo	Descripción
 Permitir	Los permisos se otorgan de manera explícita al destino de la ACE.
 Denegar	Los permisos se deniegan de manera explícita al destino de la ACE.

TABLA 139 Recursos compartidos: permisos de ACL

	Permiso	Descripción
	Lectura	
(r)	Leer datos/Mostrar directorio	Permiso para mostrar el contenido de un directorio. Cuando es heredado por un archivo, comprende el permiso para leer los datos del archivo.
(x)	Ejecutar archivo/Recorrer directorio	Permiso para recorrer (consultar) las entradas de un directorio. Cuando es heredado por un archivo, comprende el permiso para ejecutar el archivo.
(a)	Leer atributos	Permiso para leer atributos básicos (sin ACL) de un archivo. Los atributos básicos se consideran los atributos de nivel de estadística y la admisión de este permiso significa que el usuario puede ejecutar los equivalentes a <i>ls</i> y <i>stat</i> .
(R)	Leer atributos extendidos	Permiso para leer los atributos extendidos de un archivo o realizar una consulta en el directorio de atributos extendidos.
	Escritura	
(w)	Escribir datos/Agregar archivo	Permiso para agregar un nuevo archivo a un directorio. Cuando es heredado por un archivo, comprende el permiso para modificar los datos de un archivo en cualquier lugar del rango de desplazamiento del archivo.

	Permiso	Descripción
		Comprende la capacidad de aumentar el archivo o escribir en cualquier desplazamiento arbitrario.
(p)	Anexar datos/Agregar subdirectorio	Permiso para crear un subdirectorio dentro de un directorio. Cuando es heredado por un archivo, comprende el permiso para modificar los datos del archivo, pero solo a partir del final del archivo. En la actualidad, no se admite este permiso (cuando se aplica a archivos).
(d)	Suprimir	Permiso para suprimir un archivo.
(D)	Suprimir elemento secundario	Permiso para suprimir un archivo dentro de un directorio. A partir de la versión de software 2011.1, si está configurado el indicador sticky bit, solo el propietario del archivo puede suprimir el archivo secundario.
(A)	Write Attributes (Escribir atributos)	Permiso para cambiar los horarios asociados con un archivo o directorio.
(W)	Write Extended Attributes (Escribir atributos extendidos)	Permiso para crear atributos extendidos o escribir en el directorio de atributos extendidos.
	Admin	
(c)	Read ACL/Permissions (Leer ACL/permisos)	Permiso para leer la ACL.
(C)	Write ACL/Permissions (Escribir ACL/permisos)	Permiso para escribir la ACL o cambiar los modos de acceso básico.
(o)	Cambiar propietario	Permiso para cambiar el propietario.
	Herencia	
(f)	Aplicar a archivos	Permite heredar en los archivos creados recientemente en un directorio.
(d)	Aplicar a directorios	Permite heredar en todos los directorios creados recientemente en un directorio.
(i)	No aplicar a sí mismo	La ACE actual no se aplica al directorio actual, pero sí se aplica a los elementos secundarios. Este indicador requiere la configuración de una de las siguientes opciones: Aplicar a archivos o Aplicar a directorios.
(n)	No aplicar elementos secundarios pasados	La ACE actual solo debe heredar un nivel de los tres hacia los elementos secundarios inmediatos. Este indicador requiere la configuración de una de las siguientes opciones: Aplicar a archivos o Aplicar a directorios.

Cuando la opción de utilizar los permisos predeterminados de Windows se usa en el momento de la creación del recurso compartido, se crea una ACL con las siguientes tres entradas para el directorio raíz del recurso compartido:

TABLA 140 Entidades de directorio raíz de recursos compartidos

Tipo	Acción	Acceso
Propietario	Permitir	Control completo
Grupo	Permitir	Leer y ejecutar
Todos	Permitir	Leer y ejecutar

En la CLI, configure las propiedades de ACL de directorio raíz después de desplazarse hasta el contexto `shares` y seleccionar un proyecto y un sistema de archivos. Use comas para separar las propiedades ACE y separe las entradas ACE múltiples con comas. Los campos `target` e `inheritance` son opcionales. Para establecer las propiedades, introduzca `set root_acl=ace1,ace2,ace3,...`, donde `acen` es:

```
type:[target:]permissions:[inheritance:]mode
```

Ejemplos:

```
set root_acl=owner@:r:allow
```

```
set root_acl=everyone@:rwx:fd:allow
```

```
set root_acl=user:root:r:allow
```

Trabajo con esquemas

Además de las propiedades estándar integradas, puede configurar cualquier cantidad de propiedades adicionales disponibles en todos los proyectos y recursos compartidos. A estas propiedades se les asignan tipos básicos con fines de validación y se heredan como la mayoría de las otras propiedades estándar. Los valores nunca son consumidos por el software de ninguna manera, y solamente existen para el consumo del usuario final. El esquema de propiedades es global para el sistema, abarca todas las agrupaciones y está sincronizado entre pares de cluster.

Para trabajar con esquemas, consulte las siguientes secciones:

- [Creación de esquemas \(BUI\) \[571\]](#)
- [Creación de esquemas \(CLI\) \[572\]](#)
- [“Propiedades de esquema” \[573\]](#)

▼ Creación de esquemas (BUI)

1. **Vaya a Recursos compartidos > Esquema.**

2. Haga clic en el ícono + para agregar una nueva propiedad a la lista de propiedades del esquema.
3. Introduzca el nombre de la propiedad (`contact`).
4. Introduzca una descripción de la propiedad ("Contacto del propietario").
5. Elija un tipo para la nueva propiedad (Dirección de correo electrónico).
6. Haga clic en la opción para aplicar.
7. Navegue hasta el proyecto o el recurso compartido existente.
8. Cambie la propiedad Contacto del propietario en la sección Propiedades personalizadas.

▼ Creación de esquemas (CLI)

1. Vaya hasta el contexto del esquema (`shares schema`).
2. Cree una nueva propiedad denominada `contact` (`create contact`).
3. Configure la descripción de la propiedad (`set description="Owner Contact"`).
4. Configure el tipo de propiedad (`set type=EmailAddress`).
5. Confirme los cambios (`commit`).
6. Vaya hasta un proyecto o recurso compartido existente.
7. Establezca la propiedad `custom:contact`.

ejemplo 5 Ejemplo de esquema

El contexto del esquema se encuentra en Recursos compartidos > Esquema.

```
carp:> shares schema
carp:shares schema> show
Properties:
```

NAME	TYPE	DESCRIPTION
owner	EmailAddress	Owner Contact

Cada propiedad es un elemento secundario del contexto del esquema, que utiliza el nombre de la propiedad como token. Para crear una propiedad, utilice el comando `create`:

```
carp:shares schema> create department
carp:shares schema department (uncommitted)> get
                                type = String
                                description = department
carp:shares schema department (uncommitted)> set description="Department Code"
                                description = Department Code (uncommitted)
carp:shares schema department (uncommitted)> commit
carp:shares schema>
```

Dentro del contexto de una propiedad en particular, los campos se pueden configurar con los comandos de la CLI estándar:

```
carp:shares schema> select owner
carp:shares schema owner> get
                                type = EmailAddress
                                description = Owner Contact
carp:shares schema owner> set description="Owner Contact Email"
                                description = Owner Contact Email (uncommitted)
carp:shares schema owner> commit
```

Una vez definidas las propiedades personalizadas, es posible acceder a estas como cualquier otra propiedad bajo el nombre `custom:property_name`:

```
carp:shares default> get
...
        custom:department = 123-45-6789
        custom:owner =
...
carp:shares default> set custom:owner=bob@corp
        custom:owner = bob@corp (uncommitted)
carp:shares default> commit
```

Propiedades de esquema

Para definir propiedades personalizadas, acceda al elemento de navegación Recursos compartidos > Esquema. El esquema actual se muestra como una lista y se pueden agregar o quitar entradas, según sea necesario. Cada propiedad tiene los siguientes campos:

TABLA 141 Campos de propiedades de esquemas

Campo	Descripción
NAME (Nombre)	El nombre de la CLI para esta propiedad. Debe contener solo caracteres alfanuméricos o los caracteres <code>._:\</code> .
DESCRIPTION (Descripción)	El nombre de la BUI para esta propiedad. Puede contener caracteres arbitrarios y se utiliza en la sección de ayuda de la CLI.

Campo	Descripción
TYPE	El tipo de propiedad, con fines de validación. Debe ser uno de los tipos que se describen a continuación.

Los tipos válidos de propiedades son:

TABLA 142 Tipos válidos para las propiedades

Tipo de BUI	Tipo de CLI	Descripción
Cadena	String	Datos de cadenas arbitrarias. Es el equivalente de la falta de validación.
Número entero	Integer	Un número entero positivo o negativo.
Número entero positivo	PositiveInteger	Un número entero positivo.
Booleana	Booleana	Un valor verdadero/falso. En la BUI, esto se presenta como una casilla de control, mientras que en la CLI debe ser uno de los valores <code>true</code> o <code>false</code> .
Email Address (Dirección de correo electrónico)	EmailAddress	Una dirección de correo electrónico. Solo se realiza una validación sintáctica mínima.
Nombre de host o IP	Host	Una dirección IP (v4 o v6) o un nombre de host DNS válido.

Una vez definidas, las propiedades están disponibles en la ficha de propiedades general, mediante la descripción proporcionada en la tabla de propiedades. Las propiedades se identifican por su nombre de CLI; por lo tanto, el cambio de nombre de una propiedad eliminará todas las configuraciones existentes en el sistema. Una propiedad que se suprime y, luego, se le vuelve a asignar el nombre original aún hará referencia a los valores configurados anteriormente. El cambio de tipo de propiedad, si bien está admitido, tendrá resultados indefinidos sobre las propiedades existentes del sistema. Las propiedades existentes conservarán su configuración actual, incluso si no fueran válidas según el nuevo tipo de propiedad.

Migración shadow

Una tarea común de los administradores consiste en mover datos de una ubicación a otra. En el sentido más abstracto, este problema comprende una gran cantidad de casos de uso, desde la replicación de datos entre servidores hasta el mantenimiento de los datos del usuario en equipos portátiles sincronizados con los servidores. Existen diversas herramientas externas disponibles para ello; sin embargo, el dispositivo tiene dos soluciones integradas para migrar los datos relacionados con los casos de uso más comunes. La primera, la replicación, tiene como finalidad replicar datos entre uno o varios dispositivos, y se trata por separado; consulte [Replicación remota \[623\]](#). La segunda, la migración shadow, se describe en este documento.

La migración shadow es un proceso para migrar datos desde fuentes NAS externas con la finalidad de reemplazar o retirar la original una vez finalizada la migración. Generalmente, se utiliza cuando se introduce un dispositivo nuevo en un entorno existente para tomar el control de las tareas de uso compartido de archivos de otro servidor, pero es posible darle otros usos novedosos.

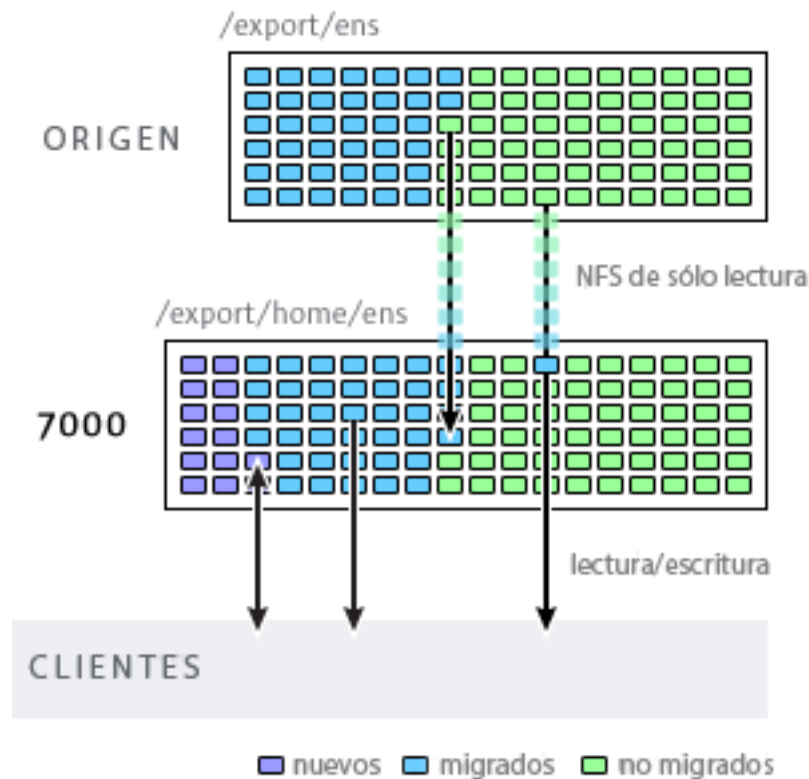
Para usar la migración shadow, consulte las siguientes secciones:

- [“Descripción de migración shadow” \[576\]](#)
- [“Creación de un sistema de archivos shadow” \[579\]](#)
- [“Gestión de la migración en segundo plano” \[579\]](#)
- [“Tratamiento de errores de migración” \[580\]](#)
- [“Seguimiento de una migración en curso” \[580\]](#)
- [“Cancelación de migración” \[583\]](#)
- [“Toma de instantáneas de sistemas de archivos shadow” \[584\]](#)
- [“Copias de seguridad de sistemas de archivos shadow” \[584\]](#)
- [“Replicación de sistemas de archivos shadow” \[584\]](#)
- [“Migración de sistemas de archivos locales” \[585\]](#)
- [“Uso de análisis de migración shadow” \[585\]](#)
- [Prueba de una posible migración shadow con la CLI \[586\]](#)
- [Migración de datos desde un servidor NFS activo con la CLI \[586\]](#)

Descripción de migración shadow

La migración shadow utiliza la interposición, pero está integrada al dispositivo y no requiere una máquina física aparte. Cuando se generan sistemas de archivos, existe la opción de realizar una migración "shadow" de un directorio existente, ya sea de manera local o mediante NFS. En este caso, el tiempo de inactividad se programa una vez, donde el dispositivo de origen X se coloca en modo de solo lectura, se genera un recurso compartido con la propiedad shadow configurada, y los clientes se actualizan para apuntar al nuevo recurso compartido del dispositivo. A continuación, los clientes pueden acceder al dispositivo en modo lectura y escritura.

FIGURA 25 Migración shadow



Una vez que está configurada la propiedad shadow, los datos se migran de manera transparente en segundo plano desde el dispositivo de origen de manera local. Si una solicitud proviene de un cliente para un archivo que aún no se ha migrado, el dispositivo migrará automáticamente este archivo al servidor local antes de responder la solicitud. Esto puede generar latencia inicial en algunas solicitudes de clientes, pero una vez que se haya migrado un archivo, todos los accesos serán locales para el dispositivo y tendrán rendimiento nativo. A menudo sucede que el conjunto de trabajo actual para un sistema de archivos es mucho más pequeño que el tamaño total; por lo tanto, una vez que se ha migrado este conjunto de trabajo, no se percibirán cambios en el rendimiento, independientemente del tamaño nativo total en el origen.

La desventaja de la migración shadow es que requiere una confirmación antes de que finalice la migración de datos, aunque esto sucede con cualquier método de interposición. Durante la migración, partes de los datos se encuentran en dos ubicaciones, lo que significa que las copias de seguridad son más complicadas y las instantáneas pueden estar incompletas o existir solo en un host. Por lo tanto, es extremadamente importante que antes de realizar cualquier migración entre dos hosts esta se pruebe cuidadosamente, para asegurarse de que la gestión de identidad y los controles de acceso estén configurados correctamente. Para esto no es necesario probar toda la migración de datos, pero se debe verificar que los archivos o directorios que no se leen a nivel mundial migren correctamente, que se conserven las ACL (si hubiera) y que las identidades estén representadas correctamente en el nuevo sistema.

La migración shadow se implementa con datos en el disco dentro del sistema de archivos; por lo tanto, no existe una base de datos externa ni datos almacenados localmente fuera de la agrupación de almacenamiento. Si se produce un failover de una agrupación de un cluster, o si se produce un error en los dos discos de sistema y se necesita un nuevo nodo principal, todos los datos necesarios para continuar con la migración shadow sin interrupciones se mantendrán en la agrupación de almacenamiento.

A continuación se describen las restricciones del origen shadow:

- Para migrar datos correctamente, el directorio o sistema de archivos de origen *debe ser de solo lectura*. Los cambios realizados en el origen de archivos pueden (o no) propagarse en función del tiempo, y los cambios de la estructura de directorio pueden provocar errores irreversibles en el dispositivo.
- La migración shadow admite la migración solo de orígenes NFS. Los sistemas de archivos NFSv4.0 y NFSv4.1 proporcionarán los mejores resultados. Es posible llevar a cabo la migración de NFSv2 y NFSv3; sin embargo, las ACL se perderán en el proceso y los archivos demasiado grandes para NFSv2 no se podrán migrar mediante ese protocolo. No se admite la migración desde orígenes SMB.
- No se admite la migración shadow de LUN.

Durante la migración, si un cliente accede a un archivo o directorio que aún no se ha migrado, se produce un efecto observable sobre el comportamiento. A continuación se describe la semántica del sistema de archivos shadow:

- En el caso de directorios, las solicitudes del cliente se bloquean hasta que se genera la infraestructura de metadatos en el destino de la migración para los directorios participantes para los que no aún no se estableció una infraestructura. En el caso de los archivos, solo se migra la parte del archivo que se solicita y diversos clientes pueden migrar diferentes partes de un archivo al mismo tiempo.
- Se puede eliminar y sobrescribir los archivos y directorios, o cambiar su nombre, de manera arbitraria en el sistema de archivos shadow sin afectar el proceso de migración.
- En el caso de archivos que son enlaces físicos, es posible que el recuento de enlaces físicos no coincida con el origen hasta la finalización de la migración.
- La mayoría de los atributos de los archivos se migran cuando se crea el directorio, pero el tamaño en disco (`st_nblocks` en la estructura estática UNIX) no está disponible hasta que se realiza una operación de lectura o escritura en el archivo. El tamaño lógico será correcto, pero el comando `du(1)`, u otro, informará un tamaño cero hasta que se migre realmente el contenido de los archivos.
- Si se reinicia el dispositivo, la migración retomará desde donde se detuvo originalmente. Si bien el dispositivo no deberá volver a migrar datos, es posible que deba recorrer algunas partes ya migradas del sistema de archivos local, lo cual puede afectar el tiempo total de migración debido a la interrupción.
- La migración de datos utiliza atributos extendidos privados en los archivos. En general, no son observables, excepto en el directorio raíz del sistema de archivos o mediante instantáneas. La agregación, la modificación o la eliminación de cualquier atributo extendido que comience con `SUNWshadow` ejercerá efectos indefinidos en el proceso de migración y generará un estado de daño o incompleto. Además, el estado de todo el sistema de archivos se almacena en el directorio `.SUNWshadow` en la raíz del sistema de archivos. Cualquier modificación que se realice en este contenido tendrá un efecto similar.
- Una vez que el sistema de archivos haya finalizado la migración, se publicará una alerta y se eliminará el atributo `shadow`, junto con los metadatos aplicables. Después de esto, el sistema de archivos no se podrá distinguir de un sistema de archivos normal.
- Los datos se pueden migrar desde varios sistemas de archivos a un único sistema de archivos, mediante el uso de montajes de clientes automáticos NFSv4.0 y NFSv4.1 (en ocasiones denominados montajes duplicados) o montajes locales anidados.

Use las siguientes reglas para migrar correctamente la información de identidad de los archivos, incluidas las ACL:

- Los dispositivos de origen y de destino de la migración deben tener la misma configuración de servicio de nombres.
- El origen de migración y el dispositivo de destino deben tener el mismo dominio `mapid` NFSv4.0 o NFSv4.1
- El origen de migración debe admitir NFSv4.0 y NFSv4.1. Es posible utilizar NFSv3, pero se perderá una parte de la información. Se conservarán los permisos de POSIX y la información de identidad básica (propietario y grupo), pero se perderán las ACL.

- Se debe exportar el origen de la migración con permisos root al dispositivo.

Si observa archivos o directorios cuyo propietario es "nobody" (nadie), probablemente signifique que el dispositivo no tiene servicios de nombres configurados correctamente, o que el dominio mapid NFSv4.0 y NFSv4.1 es diferente. Si obtiene errores de 'permiso denegado' cuando recorre sistemas de archivos a los que el cliente debería tener acceso, el problema más probable radica en la imposibilidad de exportar el origen de la migración con permisos root.

Creación de un sistema de archivos shadow

El origen de la migración shadow solo se puede configurar cuando se crea un sistema de archivos. En la BUI, se encuentra disponible en el cuadro de diálogo de creación del sistema de archivos. En el caso de la CLI, está disponible como propiedad `shadow`. La propiedad adquiere uno de los siguientes formatos:

- **Local:** `file:///<path>`
- **NFS:** `nfs://<host>/<path>`

La BUI también permite la forma alternativa `<host>:/<path>` para montajes de NFS, que coincide con la sintaxis utilizada en los sistemas UNIX. La BUI además determina la parte del protocolo de la configuración (`file://` o `nfs://`) mediante el uso de un menú desplegable. Cuando se crea un sistema de archivos, el servidor verifica que la ruta existe y que se puede montar.

Gestión de la migración en segundo plano

Cuando se crea un recurso compartido, este automáticamente comienza a migrar en segundo plano, además de responder las solicitudes en línea. Esta migración se controla mediante el servicio de migración shadow. Existe un único valor ajustable global, que es la cantidad de subprocesos dedicados a esta tarea. Al aumentar la cantidad de subprocesos, se obtendrá un mayor paralelismo a expensas de recursos adicionales.

El servicio de migración shadow se puede desactivar, pero esto solo se debe realizar con fines de prueba, o cuando la activación de la migración shadow supere la capacidad del sistema hasta el punto en el cual este necesite detenerse temporalmente. Cuando se desactiva el servicio de migración shadow, las solicitudes síncronas aún se migran según sea necesario, pero no se produce ninguna migración en segundo plano. Cuando el servicio está desactivado, no se completa ninguna migración shadow, aunque se lea manualmente todo el contenido del sistema de archivos. Se recomienda dejar siempre el servicio activado.

Tratamiento de errores de migración

Dado que la migración shadow necesita la confirmación de las nuevas modificaciones realizadas en el servidor antes de completar la migración, es muy importante probar la migración y supervisar los errores. Los errores detectados durante la migración en segundo plano se mantienen y se muestran en la BUI como parte del estado de migración shadow. Los errores detectados durante otras migraciones síncronas no se rastrean, pero se registrarán cuando el proceso en segundo plano acceda al archivo afectado. Para cada archivo, se mantienen el nombre de archivo remoto y el error específico. Esta lista detallada aparecerá al hacer clic en el ícono de información ubicado junto al recuento de errores. La lista de errores no se actualiza a medida que se corrigen los errores, sino que simplemente se vacía cuando la migración finaliza con éxito.

La migración shadow no finalizará hasta que todos los archivos se migren con éxito. Si existen errores, la migración en segundo plano volverá a intentar continuamente la migración hasta que tenga éxito. Esto permite al administrador corregir los errores (como los problemas de permisos), permitir la finalización de la migración y garantizar el éxito. Si no se puede finalizar la migración debido a errores persistentes, se podrá cancelar la migración y dejar el sistema de archivos local con los datos que se pudieron migrar. Esto solo se debe realizar como último recurso, ya que una vez que la migración se cancela, no se puede reanudar.

Seguimiento de una migración en curso

Para hacer un seguimiento del progreso de migración shadow, el dispositivo proporciona las siguientes estadísticas:

- tamaño de datos transferidos hasta el momento,
- tamaño estimado que falta migrar,
- tiempo de migración hasta el momento,
- Tiempo de migración restante
- Errores de migración

Al principio de la migración, el dispositivo obtiene las estadísticas del sistema de archivos de origen y calcula su tamaño. Utiliza estos valores para proporcionar una representación visual relativamente precisa del progreso de migración y una estimación de los datos que faltan migrar. Se debe tener en cuenta que los bytes faltantes son una estimación basada en la suposición de que se está migrando un sistema de archivos completo. Si solo se está migrando parte del sistema de archivos, la estimación de los bytes faltantes es incorrecta. Si el sistema de archivos de origen tiene sistemas de archivos anidados, se recalcula el tamaño total del sistema de archivos cuando se descubre el punto de montaje anidado durante la migración y se vuelven a estimar los bytes restantes según el nuevo total calculado. La estimación de los bytes restantes

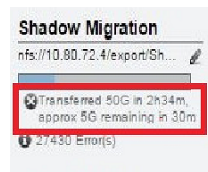
puede ser inexacta si el sistema de archivos de origen usa compresión. Estos valores están disponibles en la BUI y la CLI mediante las propiedades del sistema de archivos estándar y las propiedades del nodo de migración shadow (o panel de la interfaz de usuario).

Nota - Cuando se migra un archivo disperso (un archivo que tiene bloques vacíos), el archivo de destino será más pequeño que el archivo de origen. La migración shadow no escribe los bloques vacíos en el archivo de destino, por lo que el espacio utilizado es menor.

En las siguientes tareas, se describe cómo supervisar el progreso de la migración shadow y ver los errores resultantes. Para ver los errores de migración shadow mediante la API de RESTful, consulte [“Operaciones del sistema de archivos” de Guía de la API de RESTful de Oracle® ZFS Storage Appliance \(versión OS8.8.x\)](#).

▼ Supervisión del progreso y de los errores de migración (BUI)

1. Vaya a **Recursos compartidos > Recursos compartidos** y seleccione un sistema de archivos con origen de migración shadow.
2. En **Migración shadow**, examine la barra de progreso y el estado de la migración shadow.



3. Para ver los errores de migración shadow, haga clic en el ícono .

▼ Supervisión del progreso y de los errores de migración (CLI)

1. Vaya a un sistema de archivos con origen de migración shadow, introduzca `shadow y`, luego, introduzca `list`.

```

hostname:shares default/file_sys1> shadow
hostname:shares default/file_sys1 shadow> list
Properties:
    source = nfs://zfs0000-15/sm/errors
    transferred = (unset)
    remaining = 1.37G
    elapsed = 0h3m
    errors = 23
    complete = true
    time = (unset)

Children:
    errors => Shadow Migration Errors
hostname:shares default/file_sys1 shadow>

```

Nota - Si no hay un origen de migración shadow definido (shadow=none), el comando shadow no es válido para el sistema de archivos:

```

hostname:shares default/xyz_1> shadow
error: invalid command "shadow"

```

2. Para ver los errores de migración shadow, introduzca el nodo secundario `errors` e introduzca `help` para ver una lista de subcomandos.

```

hostname:shares default/file_sys1 shadow> errors

hostname:shares default/file_sys1 shadow errors> help

Subcommands that are valid in this context:

    help [topic]          => Get context-sensitive help. If [topic] is specified,
                           it must be one of "builtins", "commands", "general",
                           "help" or "script".

    show                  => Show information pertinent to the current context

    done                  => Finish operating on "errors"

    select [entry]        => Select the specified entry to get its properties,
                           set its properties, or run a subcommand

    list                  => Lists up to the first 100 errors. The "-a" option may be
                           used to list all the errors if there are more than 100
                           errors. The "-number" option may be used to list the first
                           (number) of errors. Format: list -a or list -xx

```

3. Introduzca `show` para ver errores de migración individuales en el contexto actual.

```

hostname:shares default/file_sys1 shadow errors> show
Errors:

PATH                                REASON
ak-2013-dev-on-clone.tar.gz        Permission denied
test_dir/CREDITS.html               Permission denied
test_dir/CREDITS_ja.html            Permission denied
test_dir/CREDITS_pt_BR.html         Permission denied
test_dir/CREDITS_zh_CN.html         Permission denied

```

```

test_dir/DISTRIBUTION.txt      Permission denied
test_dir/LEGALNOTICE.txt      Permission denied
test_dir/LICENSE.txt          Permission denied
test_dir/README.html          Permission denied
test_dir/README_ja.html       Permission denied
test_dir/README_pt_BR.html    Permission denied
test_dir/README_zh_CN.html    Permission denied
test_dir/THIRDPARTYLICENSE.txt Permission denied
test_dir/bin                   Permission denied
test_dir/cnd2                  Permission denied
test_dir/etc                   Permission denied
test_dir/gsf1                  Permission denied
test_dir/ide10                 Permission denied
test_dir/modCluster.properties Permission denied
test_dir/nb6.5                 Permission denied
test_dir/forms.css             Permission denied
test_dir/platform9             Permission denied
test_dir/websvccommon1        Permission denied

```

4. Para ver un error individual, introduzca el comando `select` y un nombre de error individual. A continuación, introduzca `show`.

Para ver propiedades de error individuales, use el comando `get`.

```

hostname:shares default/file_sys1 shadow errors> select test_dir/nb6.5

hostname:shares default/file_sys1 shadow errors test_dir/nb6.5> show
Properties:
    path = test_dir/nb6.5
    reason = Permission denied

hostname:shares default/file_sys1 shadow errors test_dir/nb6.5> get path
    path = test_dir/nb6.5
hostname:shares default/file_sys1 shadow errors test_dir/nb6.5> get reason
    reason = Permission denied
hostname:shares default/file_sys1 shadow errors test_dir/nb6.5> done
hostname:shares default/file_sys1 shadow errors>

```

Cancelación de migración

La migración se puede cancelar, pero solo se debe hacer en circunstancias extremas cuando el origen ya no está disponible. Una vez que se ha cancelado la migración, no se puede reanudar. La finalidad principal es permitir que se complete la migración cuando existen errores que no se pueden corregir en el origen. Si ha finalizado la migración de todo el sistema de archivos, excepto por algunos archivos y directorios, y no hay manera de corregir estos errores (es decir, el origen está permanentemente dañado), la cancelación de la migración permitirá que el sistema de archivos local vuelva al estado "normal".

Para cancelar la migración en la BUI, haga clic en el ícono de cierre ubicado junto a la barra de progreso en la columna izquierda del recurso compartido en cuestión. En la CLI, migre hacia el nodo `shadow` debajo del sistema de archivos y ejecute el comando `cancel`.

Toma de instantáneas de sistemas de archivos shadow

Se pueden tomar instantáneas de los sistemas de archivos shadow, independientemente de si el estado del contenido de la instantánea es arbitrario. Los archivos que aún no se han migrado no estarán presentes y es posible que los detalles de implementación (como los atributos extendidos de SUNWshadow) estén visibles en la instantánea. Esta instantánea se puede utilizar para restaurar archivos individuales que se han migrado o modificado desde el comienzo de la migración original. Debido a esto, se recomienda mantener todas las instantáneas en el origen hasta finalizar la migración, de manera que se puedan recuperar desde el origen los archivos no migrados, si es necesario. Según la política de retención, podría ser necesario extender la retención en el origen para cumplir con los requisitos de servicio. Si bien se pueden tomar instantáneas, estas no se pueden revertir ni pueden ser el origen de un clon.

Copias de seguridad de sistemas de archivos shadow

Se pueden realizar copias de seguridad de los sistemas de archivos que migran activamente datos shadow mediante NDMP al igual que en cualquier otro sistema de archivos. La configuración de shadow se conserva con el flujo de copias de seguridad, pero solo se restaurará si se lleva a cabo una restauración completa del sistema de archivos y el recurso compartido aún no existe. La restauración de archivos individuales desde dicho flujo de copias de seguridad o la restauración a sistemas de archivos existentes puede generar un estado incoherente o el daño de los datos. Durante la restauración de todo el sistema de archivos, este se encontrará en estado incoherente (más allá de la falta de coherencia habitual de una restauración parcial) y la migración shadow no estará activa. La configuración de shadow solo se podrá restaurar cuando finalice la restauración. Si el origen de shadow ya no está presente o ha cambiado de ubicación, el administrador podrá observar los errores y corregirlos según sea necesario.

Replicación de sistemas de archivos shadow

Los sistemas de archivos que migran activamente datos shadow se pueden replicar mediante el mecanismo normal, pero solo se envían los datos migrados en el flujo de datos. Por lo tanto, el lado remoto contiene solo datos parciales que pueden representar un estado incoherente. La configuración de shadow se envía junto con el flujo de replicación, por eso, cuando se produce un failover en el destino remoto, se mantiene la misma configuración de shadow. De la misma manera que puede suceder con la restauración de un flujo de copias de seguridad de NDMP, esta configuración puede ser incorrecta en el contexto del destino remoto. Después de realizar un failover en el destino, el administrador puede observar los errores y corregir la configuración de shadow según sea necesario para el nuevo entorno.

Migración de sistemas de archivos locales

Además de su finalidad principal de migrar datos desde orígenes remotos, el mismo mecanismo también se puede utilizar para migrar datos de un sistema de archivos local a otro en el dispositivo. Se puede utilizar para cambiar configuraciones que de otro modo no se podrían modificar, como la creación de una versión comprimida de un sistema de archivos o el cambio del tamaño de registro de un sistema de archivos después del hecho. En este modelo, el antiguo recurso compartido (o subdirectorio dentro de un recurso compartido) se hace de solo lectura o se aparta, y se crea un nuevo recurso compartido con la propiedad shadow configurada mediante el protocolo `file`. Los clientes acceden a este nuevo recurso compartido y los datos se escriben con la configuración del nuevo recurso compartido.

Uso de análisis de migración shadow

Además de la supervisión estándar por recurso compartido, también es posible supervisar todo el sistema de migración shadow mediante la herramienta de análisis. El análisis de migración shadow está disponible en la categoría de Movimiento de datos. Existen tres estadísticas básicas disponibles:

- **Solicitudes de migración shadow:** esta estadística rastrea las solicitudes de archivos o directorios no almacenados en la caché y conocidos como locales en el sistema de archivos. Abarca los archivos y directorios migrados y no migrados, y se puede utilizar para rastrear la latencia en la que se incurre como parte de la migración shadow, y para rastrear el progreso de la migración en segundo plano. Puede ser desglosada por archivo, recurso compartido, proyecto o latencia. En la actualidad, comprende la migración síncrona y asíncrona (en segundo plano); por lo tanto, no es posible ver solo la latencia visible para clientes.
- **Bytes de migración shadow:** esta estadística rastrea bytes transferidos como parte de la migración del contenido de archivos o directorios. Esto no se aplica a los metadatos (atributos extendidos, ACL, etc.). Ofrece aproximación de los datos transferidos; sin embargo, los juegos de datos de origen con una gran cantidad de metadatos mostrarán un ancho de banda desproporcionadamente pequeño. El ancho de banda completo se puede observar en los análisis de red. Esta estadística puede ser desglosada por nombre de archivo local, recurso compartido o proyecto.
- **Operaciones de migración shadow:** esta estadística rastrea operaciones que necesitan recurrir al sistema de archivos de origen. Se puede utilizar para rastrear la latencia de las solicitudes desde el origen de la migración shadow. Puede ser desglosada por archivo, recurso compartido, proyecto o latencia.

▼ Prueba de una posible migración shadow con la CLI

Antes de intentar llevar a cabo una migración completa, es importante probar dicha migración para asegurarse de que el dispositivo tenga los permisos adecuados y los atributos de seguridad se hayan traducido correctamente. Una vez que esté seguro de que la configuración básica es funcional, podrá configurar los sistemas de archivos para la migración final.

Nota - Como parte de la planificación de capacidades, recuerde tener en cuenta las cuotas de grupos de usuarios y por defecto porque se pueden superar las cuotas si el origen es mayor que el destino. Además, la migración shadow generará un error si el destino no dispone de suficiente espacio en disco.

1. **Configure el origen de manera que el dispositivo tenga acceso root al recurso compartido. En general, esto comprende la agregación de una excepción basada en el host NFS o la configuración de la asignación de usuario anónimo (esto último tiene consecuencias de seguridad más importantes).**
2. **Cree un recurso compartido en el sistema de archivos local con el atributo shadow establecido en 'nfs://<host>/<snapshotpath>' en la CLI o simplemente '<host>/<snapshotpath>' en la BUI (con el protocolo seleccionado como 'NFS'). La instantánea debe ser una copia de solo lectura del origen. Si no hay instantáneas disponibles, se puede utilizar un origen de lectura y escritura, pero esto puede ocasionar errores no definidos.**
3. **Compruebe que el contenido de los archivos y la asignación de identidad estén conservados correctamente; para ello, recorra la estructura de los archivos.**
4. **Si el origen de datos es de solo lectura (al igual que sucede con una instantánea), permita que finalice la migración y verifique que no se hayan producido errores en la transferencia.**

▼ Migración de datos desde un servidor NFS activo con la CLI

Use el procedimiento siguiente para migrar datos desde un servidor NFS activo mediante la CLI. Tenga en cuenta que la migración shadow genera un fallo si detecta archivos en `procfs` o si existe alguno de los siguientes tipos de archivo especiales: puertas, sockets y puertos de eventos.

1. **Programa tiempo de inactividad durante el cual los clientes se puedan desactivar y volver a configurar para apuntar a un nuevo servidor.**

2. **Configure el origen de manera que el dispositivo tenga acceso root al recurso compartido. En general, esto comprende la agregación de una excepción basada en el host NFS o la configuración de la asignación de usuario anónimo (esto último tiene consecuencias de seguridad más importantes).**
3. **Configure el origen para que sea de solo lectura. Este paso es técnicamente opcional, pero es mucho más sencillo garantizar el cumplimiento si resulta imposible para los clientes con errores de configuración escribir en el origen mientras la migración está en curso.**
4. **Cree un recurso compartido en el sistema de archivos local con el atributo shadow configurado en 'nfs://<host>/<path>' en la CLI o simplemente '<host>/<path>' en la BUI (con el protocolo seleccionado como 'NFS').**
5. **Reconfigure los clientes para que apunten al recurso compartido local en el dispositivo.**

En este punto, la migración shadow se debe ejecutar en segundo plano y las solicitudes de los clientes se deben responder según sea necesario. Podrá observar el progreso según se describe anteriormente. Se pueden crear varios sistemas de archivos durante un único tiempo de inactividad programado mediante la creación de secuencias de comandos de la CLI.

Instantáneas y clones

Nota - La clonación es una característica que se ofrece con licencia para determinados modelos. Para obtener información detallada, consulte "Acuerdo de licencia de software (SLA) de Oracle y derecho de sistemas de hardware con opciones de software integrado" y el Manual de usuario de información sobre licencias para la versión de software.

Las instantáneas y los clones le permiten hacer copias de un momento dado de un recurso compartido o un proyecto. Estas copias pueden ser útiles como copias de seguridad o como distintas versiones de trabajo.

Una instantánea es una copia de solo lectura de un sistema de archivos, un LUN o un proyecto. Tomar una instantánea de un proyecto es equivalente a generar una instantánea de todos los recursos compartidos que se encuentran en él. Una instantánea no consume espacio adicional cuando se la crea, pero, a medida que el recurso compartido activo cambia, la instantánea consume espacio adicional, con un máximo equivalente al tamaño del recurso compartido en el momento de creación de la instantánea.

Un clon es una copia de un sistema de archivos o una instantánea del LUN que permite operaciones de escritura y se puede tratar como si fuera un recurso compartido independiente. No se admiten clones de proyectos. Al igual que una instantánea, un clon no consume espacio adicional cuando se lo crea, pero, a medida que se escriben nuevos datos en él, el espacio requerido para los cambios se asocia con el clon.

Puede generar instantáneas de manera manual o puede definir un programa para generarlas automáticamente cada media hora, una hora, un día, una semana o un mes. Los dispositivos generan automáticamente algunas instantáneas durante las actualizaciones de replicación; estas instantáneas aparecen en la página de instantáneas e incluyen `.ndmp` y `.rr` en sus nombres.

Para obtener información acerca de la gestión del espacio de instantáneas, consulte el siguiente tema:

[“Gestión del espacio de instantáneas” \[591\]](#)

Para generar instantáneas de manera manual o programar instantáneas automáticas de proyectos o recursos compartidos, realice las siguientes tareas:

-
- Toma de una instantánea: [BUI](#), [CLI](#)
 - Programación de instantáneas: [BUI](#), [CLI](#)
 - Configuración de una etiqueta de instantánea programada: [BUI](#), [CLI](#)

Puede crear clones de una instantánea, lo que puede ser útil para crear varias versiones de trabajo de un recurso compartido. Para crear clones, realice las siguientes tareas:

- Clonación de una instantánea: [BUI](#), [CLI](#)
- [Clonación de un clon \[619\]](#)
- Clonación de un paquete de replicación: [BUI](#), [CLI](#)

Para determinar las relaciones entre instantáneas y clones existentes, realice las siguientes tareas:

- Visualización de clones de una instantánea: [BUI](#), [CLI](#)
- Visualización de un origen de clon: [BUI](#), [CLI](#)

Para ver y editar instantáneas, programas de instantáneas y políticas de retención de instantáneas existentes, realice las siguientes tareas:

- Visualización de instantáneas y programas: [BUI](#), [CLI](#)
- Cambio de nombre de una instantánea: [BUI](#), [CLI](#)
- Edición de una política de retención de instantáneas: [BUI](#), [CLI](#)

Puede ver el contenido de las instantáneas de un sistema de archivos mediante el directorio `.zfs/snapshot` del sistema de archivos. No se puede acceder a las instantáneas de LUN directamente, aunque estas se pueden utilizar como destino de reversión o como origen de un clon. Para gestionar el directorio `.zfs/snapshot` y acceder a él, realice las siguientes tareas:

- Visibilidad de un directorio de instantáneas del sistema de archivos: [BUI](#), [CLI](#)
- [Acceso a un directorio oculto de instantáneas del sistema de archivos \(CLI\) \[607\]](#)
- [Acceso a un directorio visible de instantáneas del sistema de archivos \(CLI\) \[608\]](#)

Puede usar una instantánea existente para restaurar un sistema de archivos o un LUN al estado exacto que tenía cuando se generó la instantánea. Para revertir un sistema de archivos, un LUN o un proyecto a una instantánea existente, realice las siguientes tareas:

- Reversión a una instantánea: [BUI](#), [CLI](#)

Para destruir instantáneas, realice las siguientes tareas:

- Destrucción de una instantánea: [BUI](#), [CLI](#)

Gestión del espacio de instantáneas

Las instantáneas presentan un dilema interesante para la gestión del espacio. Representan el juego de bloques físicos a los que hace referencia un recurso compartido en un momento determinado. Inicialmente, esta instantánea no consume espacio adicional. Pero, a medida que se sobrescriban datos nuevos en el nuevo recurso compartido, los bloques del recurso compartido activo solo contendrán los datos nuevos, y los bloques anteriores serán "mantenidos" por las instantáneas más recientes (y posiblemente anteriores). Gradualmente, las instantáneas pueden consumir espacio adicional a medida que el contenido se desvía al recurso compartido activo. Si toma una instantánea de un sistema de archivos de cualquier tamaño y reescribe el 100 % de los datos dentro del sistema de archivos, debe mantener las referencias en el doble de los datos que se encontraban originalmente en el sistema de archivos.

Cada instantánea tiene dos estadísticas de espacio asociadas: espacio único y espacio de referencia. La cantidad de espacio de referencia es el espacio total consumido por el sistema de archivos en el momento en que se tomó la instantánea. Representa el tamaño máximo teórico de la instantánea, si esta permaneciera como única referencia para todos los bloques de datos. El espacio único indica la cantidad de espacio físico al que hace referencia únicamente la instantánea actual. Cuando se destruye una instantánea, el espacio único queda disponible para el resto de la agrupación.

Tenga en cuenta que la cantidad de espacio consumido por todas las instantáneas no equivale a la suma del espacio único de todas las instantáneas. En el caso de un recurso compartido y una única instantánea, una o ambas instantáneas o el recurso compartido deben hacer referencia a todos los bloques. Sin embargo, en el caso de instantáneas múltiples, es posible que un subgrupo de instantáneas, y no una instantánea en particular, haga referencia a un bloque. Por ejemplo, si se crea un archivo, se toman dos instantáneas X e Y, se suprime el archivo y se toma otra instantánea Z, y los bloques dentro del archivo son mantenidos por X e Y, pero no por Z. En este caso, si se destruye Z, no se liberará espacio; esto se logra destruyendo X e Y. Debido a ello, la destrucción de cualquier instantánea puede afectar el espacio único al que hacen referencia las instantáneas cercanas, aunque la cantidad total de espacio consumido por las instantáneas siempre disminuirá.

El tamaño total de un proyecto o recurso compartido siempre tiene en cuenta el espacio consumido por todas las instantáneas, aunque también está disponible el desglose del uso. Las cuotas y reservas se pueden configurar en el nivel de proyecto para aplicar restricciones físicas en este espacio total. Además, se pueden configurar cuotas y reservas en el nivel del sistema de archivos, y estas configuraciones se pueden aplicar solo a datos de referencia o datos totales.

La elección de si las cuotas y las reservas se deben aplicar o no a datos de referencia o datos físicos totales dependerá del entorno administrativo. Si los usuarios no ejercen control de sus instantáneas (es decir, se ha configurado un programa de instantáneas automáticas), las cuotas normalmente no deben incluir las instantáneas en el cálculo. De lo contrario, el usuario se

podría quedar sin espacio y estar confundido al no poder suprimir los archivos. Si no conoce las instantáneas ni los medios para gestionar estas instantáneas, es posible que dicha situación no se pueda recuperar sin la intervención del administrador. En este caso, las instantáneas representan un costo de sobrecarga que se tiene en cuenta para la operación del sistema a fin de proporcionar funciones de copias de seguridad. Por otro lado, existen entornos en los que se factura a los usuarios según sus requisitos de espacio físico y las instantáneas representan una opción para que el usuario proporcione un nivel de copias de seguridad que pueda satisfacer los requisitos según la velocidad de renovación del juego de datos. En estos entornos, resulta más sensato aplicar cuotas según los datos físicos totales, incluidas las instantáneas. Los usuarios conocen el costo de las instantáneas y se les puede proporcionar un medio para gestionarlas de manera activa (como con roles dedicados en el dispositivo).

Temas relacionados

- [“Gestión de espacio de recursos compartidos” \[539\]](#)
- [“Gestión de instantáneas generadas por el usuario” \[677\]](#)

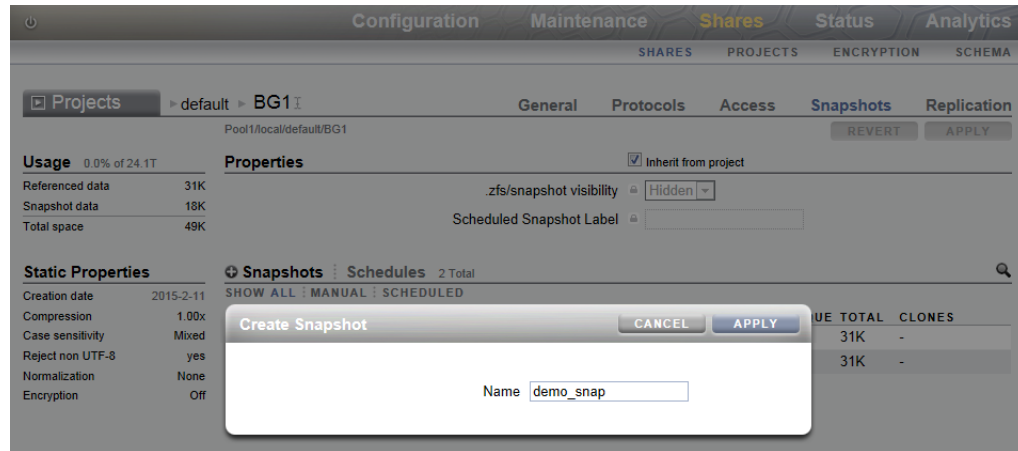
▼ Toma de una instantánea (BUI)

Use el siguiente procedimiento para generar una instantánea manual de un sistema de archivos, un LUN o un proyecto.

Para programar la generación de instantáneas automáticas a intervalos regulares, consulte [Programación de instantáneas \(BUI\) \[594\]](#).

1. **Vaya al recurso compartido o el proyecto para el que desea generar la instantánea.**
 - a. **Para tomar una instantánea de un sistema de archivos, vaya a Recursos compartidos > Recursos compartidos.**
 - b. **Para tomar una instantánea de un LUN, vaya a Recursos compartidos > Recursos compartidos y haga clic en LUN.**
 - c. **Para tomar una instantánea de un proyecto, vaya a Recursos compartidos > Proyectos.**
2. **Mueva el cursor sobre el recurso compartido o el proyecto deseado y haga clic en el ícono de edición .**
3. **Haga clic en la ficha Instantáneas.**

4. Haga clic en el ícono de agregación **+** que se encuentra junto a Instantáneas.
5. Introduzca un nombre para la instantánea.



6. Haga clic en APLICAR.

▼ Toma de una instantánea (CLI)

Use el siguiente procedimiento para generar una instantánea manual de un sistema de archivos, un LUN o un proyecto.

Para programar la generación de instantáneas automáticas a intervalos regulares, consulte [Programación de instantáneas \(CLI\) \[595\]](#).

1. Vaya al recurso compartido o el proyecto para el que desea generar la instantánea.
 - a. Para tomar una instantánea de un proyecto, vaya a **shares** y seleccione el proyecto.

```
hostname:shares> select myproject
hostname:shares myproject>
```

- b. Para tomar una instantánea de un sistema de archivos o un LUN, vaya a **shares**, seleccione el proyecto que contiene el recurso compartido y, a continuación, seleccione el recurso compartido.

```
hostname:shares> select myproject
hostname:shares myproject> select demo_share
```

```
hostname:shares myproject/demo_share>
```

2. Introduzca snapshots.

```
hostname:shares myproject/demo_share> snapshots
```

3. Use el comando snapshot seguido del nombre que desea asignar a la nueva instantánea.

```
hostname:shares myproject/demo_share snapshots> snapshot demo_snap
```

▼ Programación de instantáneas (BUI)

Use el siguiente procedimiento para configurar instantáneas automáticas de un sistema de archivos, un LUN o un proyecto y definir una política de retención para esas instantáneas.

Las instantáneas automáticas se pueden tomar cada media hora, una hora, un día, una semana o un mes y se les asigna un nombre con la estructura `.auto[-<snaplabel>]-<timestamp>`. En la columna Creación de la lista Instantáneas, se muestran las horas correspondientes a la zona horaria local (explorador del cliente). Sin embargo, las horas se almacenan y se ejecutan en formato UTC, sin tener en cuenta convenciones como el horario de verano. Por ejemplo, una instantánea programada para las 10:00 a.m. PST (UTC-8) se almacena y ejecuta a las 18:00 UTC, y esta es la hora que aparece como registro de hora en el nombre de la instantánea.

Las instantáneas automáticas se pueden configurar para un proyecto o un recurso compartido, pero no para ambos. De lo contrario, sería imposible garantizar ambos programas debido a la superposición de las políticas de retención y los programas. La eliminación de un intervalo o el cambio de su política de retención destruirá de inmediato cualquier instantánea automática no cubierta por el nuevo programa. Las instantáneas automáticas con clones se ignoran.

Nota - Versiones anteriores del software permitían instantáneas automáticas con una frecuencia de un minuto. Para ayudar a los usuarios a evitar generar una tensión innecesaria en el sistema, esta característica se eliminó en la versión 2010.Q3. Si se revierte el software, se conservan los minutos existentes. Las instancias previas caducan en función del programa existente, pero no se toman nuevas instantáneas. Se emitirá una alerta, si se encuentra un recurso compartido o proyecto con esta frecuencia.

1. Vaya al proyecto o al recurso compartido.

- a. **Para programar instantáneas de un sistema de archivos, vaya a Recursos compartidos > Recursos compartidos.**
- b. **Para programar instantáneas de un LUN, vaya a Recursos compartidos > Recursos compartidos y haga clic en LUN.**

- c. **Para programar instantáneas de un proyecto, vaya a Recursos compartidos > Proyectos.**
2. **Mueva el cursor sobre el recurso compartido o el proyecto deseado y haga clic en el ícono de edición .**
3. **Haga clic en la ficha Instantáneas.**
4. **Haga clic en Programas.**
5. **Haga clic en el ícono de agregación  que se encuentra junto a Programas.**
6. **Configure cada campo según corresponda.**
 - a. **Configure la frecuencia como media hora, una hora, un día, una semana o un mes para indicar la frecuencia con la que se toma automáticamente la instantánea.**
 - b. **Configure la hora exacta a la que se debe tomar automáticamente la instantánea.**

En el caso de instantáneas que se toman cada media hora o una hora, puede seleccionar cuántos minutos después de la media hora o la hora en punto se toma la instantánea. En el caso de instantáneas diarias, puede seleccionar la hora y minuto de toma de la instantánea, mientras que en el caso de las instantáneas semanales y mensuales, puede especificar el día, la hora y el minuto.
 - c. **Configure la propiedad "Mantener al máximo" para especificar la cantidad de instantáneas que se deben conservar o desmarque la casilla de control para no establecer ninguna política de retención.**

Las instantáneas automáticas se pueden mantener para siempre (excepto las instantáneas tomadas cada media hora y cada hora, cuyo límite es de 48 y 24, respectivamente) o se pueden limitar a un número determinado. Cuando el número de instantáneas excede el número que se especificó aquí, las instantáneas más antiguas se suprimen primero.
7. **Haga clic en Aplicar.**

▼ Programación de instantáneas (CLI)

Use el siguiente procedimiento para configurar instantáneas automáticas de un recurso compartido y definir una política de retención para esas instantáneas.

Las instantáneas automáticas se pueden tomar cada media hora, una hora, un día, una semana o un mes y se les asigna un nombre con la estructura `.auto[-<snaplabel>]-<timestamp>`. Las horas de creación de las instantáneas se almacenan y se ejecutan en formato UTC, sin tener en cuenta convenciones como el horario de verano. Por ejemplo, una instantánea programada para las 10:00 a.m. PST (UTC-8) se almacena y ejecuta a las 18:00 UTC, y esta es la hora que aparece como registro de hora en el nombre de la instantánea.

Las instantáneas automáticas se pueden configurar para un proyecto o un recurso compartido, pero no para ambos. De lo contrario, sería imposible garantizar ambos programas debido a la superposición de las políticas de retención y los programas. La eliminación de un intervalo o el cambio de su política de retención destruirá de inmediato cualquier instantánea automática no cubierta por el nuevo programa. Las instantáneas automáticas con clones se ignoran.

Nota - Versiones anteriores del software permitían instantáneas automáticas con una frecuencia de un minuto. Para ayudar a los usuarios a evitar generar una tensión innecesaria en el sistema, esta característica se eliminó en la versión 2010.Q3. Si se revierte el software, se conservan los minutos existentes. Las instancias previas caducan en función del programa existente, pero no se toman nuevas instantáneas. Se emitirá una alerta, si se encuentra un recurso compartido o proyecto con esta frecuencia.

1. **Vaya a `shares` y seleccione el proyecto o el recurso compartido del que desea generar una instantánea.**

```
hostname:> shares select myproject
hostname:shares myproject> select demo_share
hostname:shares myproject/demo_share>
```

2. **Introduzca `snapshots automatic`.**

```
hostname:shares myproject/demo_share> snapshots automatic
hostname:shares myproject/demo_share snapshots automatic>
```

3. **Use el comando `create` para introducir un contexto de programación sin confirmar.**

```
hostname:shares myproject/demo_share snapshots automatic> create
hostname:shares myproject/demo_share snapshots automatic (uncommitted)>
```

4. **Use el comando `set` para configurar cada campo según corresponda.**

- a. **Configure la frecuencia con el valor `halfhour`, `hour`, `day`, `week` o `month` para indicar con qué frecuencia se debe generar la instantánea de manera automática.**
- b. **Configure el día, la hora y el minuto para especificar el momento exacto en el que se debe tomar la instantánea automática.**

En el caso de instantáneas que se toman cada media hora o una hora, puede seleccionar cuántos minutos después de la media hora o la hora en punto se toma la instantánea. En el caso de instantáneas diarias, puede seleccionar la hora y minuto de toma de la instantánea, mientras que en el caso de las instantáneas semanales y mensuales, puede especificar el día, la hora y el minuto.

c. Configure la propiedad `keep` con el número de instantáneas que desea conservar para este programa.

Las instantáneas automáticas se pueden mantener para siempre (excepto las instantáneas tomadas cada media hora y cada hora, cuyo límite es de 48 y 24, respectivamente) o se pueden limitar a un número determinado. Cuando el número de instantáneas excede el número que se especificó aquí, las instantáneas más antiguas se suprimen primero.

```
hostname:shares myproject/demo_share snapshots automatic (uncommitted)> set frequency=day
frequency = day (uncommitted)
hostname:shares myproject/demo_share snapshots automatic (uncommitted)> set hour=14
hour = 14 (uncommitted)
hostname:shares myproject/demo_share snapshots automatic (uncommitted)> set minute=30
minute = 30 (uncommitted)
hostname:shares myproject/demo_share snapshots automatic (uncommitted)> set keep=7
keep = 7 (uncommitted)
```

Puede usar el comando `get` para ver los valores de configuración actuales que no están confirmados.

```
hostname:shares myproject/demo_share snapshots automatic (uncommitted)> get
frequency = day (uncommitted)
day = (unset)
hour = 14 (uncommitted)
minute = 30 (uncommitted)
keep = 7 (uncommitted)
```

5. Introduzca `commit` para confirmar los cambios y crear el programa de instantáneas automáticas.

```
hostname:shares myproject/demo_share snapshots automatic (uncommitted)> commit
```

Puede utilizar el comando `list` para ver el nuevo programa.

```
hostname:shares myproject/demo_share snapshots automatic> list
NAME          FREQUENCY    DAY          HH:MM KEEP
automatic-000 day          -            14:30    7
```

6. Introduzca `done` para finalizar.

```
hostname:shares myproject/demo_share snapshots automatic> done
hostname:shares myproject/demo_share snapshots>
```

▼ Configuración de una etiqueta de instantáneas programadas (BUI)

Use el siguiente procedimiento para configurar una etiqueta para instantáneas programadas de un sistema de archivos, un LUN o un proyecto.

Esta propiedad opcional agrega una etiqueta definida por el usuario a cada instantánea programada y está en blanco de forma predeterminada. La etiqueta se puede configurar para un recurso compartido individual o para un proyecto y ser heredada por sus recursos compartidos, pero no ambas opciones.

Las etiquetas de las instantáneas ayudan a identificar el proyecto o el recurso compartido para el que se generó la instantánea. Por ejemplo, "project1:share1" puede indicar una instantánea programada tomada en el recurso compartido share1 del proyecto project1. Las etiquetas pueden tener hasta 35 caracteres alfanuméricos e incluir los siguientes caracteres especiales:

_ - . : .

1. **Vaya al recurso compartido o al proyecto para el que desea configurar la etiqueta de instantánea programada.**
 - a. **Para configurar una etiqueta para un sistema de archivos, vaya a Recursos compartidos > Recursos compartidos.**
 - b. **Para configurar una etiqueta para un LUN, vaya a Recursos compartidos > Recursos compartidos y haga clic en LUN.**
 - c. **Para configurar una etiqueta para un proyecto, vaya a Recursos compartidos > Proyectos.**
2. **Mueva el cursor sobre el recurso compartido o el proyecto apropiado y haga clic en el ícono de edición .**
3. **Haga clic en la ficha Instantáneas.**
4. **Debajo de Propiedades, en el campo Etiqueta de instantánea programada, escriba la etiqueta que desea configurar.**
5. **Haga clic en Aplicar para guardar el cambio.**

Esta etiqueta se incluirá en el nombre de cada instantánea programada que se tome a partir de ahora. La etiqueta aparece antes del registro de hora, de modo que el nombre completo de la instantánea será .auto-<snaplabel>-<timestamp>.

▼ Configuración de una etiqueta de instantáneas programadas (CLI)

Use el siguiente procedimiento para configurar una etiqueta para instantáneas programadas de un sistema de archivos, un LUN o un proyecto.

Esta propiedad opcional agrega una etiqueta definida por el usuario a cada instantánea programada y está en blanco de forma predeterminada. La etiqueta se puede configurar para un recurso compartido individual o para un proyecto y ser heredada por sus recursos compartidos, pero no ambas opciones.

Las etiquetas de las instantáneas ayudan a identificar el proyecto o el recurso compartido para el que se generó la instantánea. Por ejemplo, "project1:share1" puede indicar una instantánea programada tomada en el recurso compartido share1 del proyecto project1. Las etiquetas pueden tener hasta 35 caracteres alfanuméricos e incluir los siguientes caracteres especiales:

_ - . : .

1. **Vaya a shares y seleccione el sistema de archivos, el LUN o el proyecto para el que desea configurar la etiqueta.**

```
hostname:shares myproject> select demo_share
hostname:shares myproject/demo_share>
```
2. **Use el comando `set snaplabel` para crear una etiqueta de instantánea programada.**

```
hostname:shares myproject/demo_share> set snaplabel=myproject:demo_share
```

▼ Visualización de instantáneas y programas (BUI)

Use el siguiente procedimiento para visualizar las instantáneas y los programas de instantáneas automáticas correspondientes a un sistema de archivos, un LUN o un proyecto en particular.

1. **Vaya al proyecto o al recurso compartido.**
 - a. **Para ver las instantáneas y los programas de instantáneas de un sistema de archivos, vaya a Recursos compartidos > Recursos compartidos.**
 - b. **Para ver las instantáneas y los programas de instantáneas de un LUN, vaya a Recursos compartidos > Recursos compartidos y haga clic en LUN.**
 - c. **Para ver las instantáneas y los programas de instantáneas de un proyecto, vaya a Recursos compartidos > Proyectos.**

2. **Mueva el cursor sobre el recurso compartido o el proyecto deseado y haga clic en el ícono de edición .**
3. **Haga clic en la ficha Instantáneas.**
4. **Visualice las instantáneas o los programas de instantáneas.**
 - a. **Visualice las instantáneas correspondientes a recursos compartidos debajo de Instantáneas y, de manera opcional, seleccione Manual o Programada para ver solo instantáneas manuales o programadas.**
 Para cada instantánea, puede ver el nombre (NAME), la fecha y la hora de creación (CREATION), la cantidad de espacio único utilizado por la instantánea (UNIQUE), la cantidad total de espacio al que hace referencia la instantánea (TOTAL) y el número de clones de la instantánea (CLONES).
 - b. **Haga clic en Programas para ver los programas de instantáneas automáticas para ese recurso compartido.**
 Para cada programa, puede ver la frecuencia con la que se toma una instantánea, el día y la hora exactos en que se la toma y la cantidad de instantáneas que se conservan.

▼ Visualización de instantáneas y programas (CLI)

Use el siguiente procedimiento para visualizar las instantáneas y los programas de instantáneas automáticas correspondientes a un sistema de archivos, un LUN o un proyecto en particular.

1. **Vaya a shares y seleccione el proyecto o el recurso compartido.**

```
hostname:> shares select myproject
hostname:shares myproject> select demo_share
hostname:shares myproject/demo_share>
```
2. **Introduzca snapshots.**

```
hostname:shares myproject/demo_share> snapshots
hostname:shares myproject/demo_share snapshots>
```
3. **Visualice las instantáneas o los programas de instantáneas mediante los comandos apropiados.**
 - a. **Introduzca list para mostrar una lista de las instantáneas de este recurso compartido o proyecto.**

```
hostname:shares myproject/demo_share snapshots> list
demo_snap1
demo_snap2
hostname:shares myproject/demo_share snapshots>
```

Puede seleccionar una instantánea y usar el comando `list` para ver las siguientes propiedades:

- `creation`: fecha y hora de creación de la instantánea, en formato UTC
- `numclones`: número de clones de la instantánea
- `isauto`: indica si la instantánea se creó de manera manual (`false`) o mediante un programa de instantáneas automáticas (`true`)
- `pool`: agrupación de almacenamiento en la que se encuentra la instantánea
- `canonical_name`: ubicación de la instantánea
- `shadowsnap`: indica si la instantánea se tomó durante una migración shadow (`true`) o no (`false`)
- `space_unique`: cantidad de espacio único que usa la instantánea
- `space_data`: cantidad total de espacio al que hace referencia la instantánea

```
hostname:shares myproject/demo_share snapshots> select demo_snap1
hostname:shares myproject/demo_share snapshots demo_snap1> list
Properties:
    creation = Thu Jan 22 2015 20:19:49 GMT+0000(UTC)
    numclones = 1
    isauto = false
    pool = pool1
    canonical_name = pool1/local/myproject/demo_share@demo_snap1
    shadowsnap = false
    space_unique = 0
    space_data = 31K
```

- b. **Introduzca `automatic` y use el comando `list` para mostrar una lista de los programas de instantáneas automáticas correspondientes a este recurso compartido o proyecto.**

```
hostname:shares myproject/demo_share snapshots> automatic
hostname:shares myproject/demo_share snapshots automatic> list
Properties:
    convert = false

Automatics:
NAME          FREQUENCY  DAY  HH:MM  KEEP
automatic-000 day        -    00:00   4
automatic-001 month      01    00:00  12
```

▼ Edición de una política de retención de instantáneas (BUI)

Use el siguiente procedimiento para editar una política de retención de instantáneas para un sistema de archivos, un LUN o un proyecto. Las políticas de retención de instantáneas se incluyen en los programas de instantáneas automáticas.

1. **Vaya al proyecto o al recurso compartido apropiado.**
 - a. Si la instantánea corresponde a un proyecto, vaya a Recursos compartidos > Proyectos.
 - b. Si la instantánea corresponde a un sistema de archivos, vaya a Recursos compartidos > Recursos compartidos.
 - c. Si la instantánea corresponde a un LUN, vaya a Recursos compartidos > Recursos compartidos y haga clic en LUNs (LUN).
2. **Mueva el cursor sobre el proyecto o el recurso compartido apropiado y haga clic en el ícono de edición .**
3. **Haga clic en la ficha Instantáneas.**
4. **Haga clic en Programas.**
5. **Configure la propiedad "Mantener al máximo" del programa para especificar la cantidad de instantáneas automáticas que se deben conservar o desmarque la casilla de control para no establecer ninguna política de retención.**

Las instantáneas automáticas se pueden mantener para siempre (excepto las instantáneas tomadas cada media hora y cada hora, cuyo límite es de 48 y 24, respectivamente) o se pueden limitar a un número determinado. Cuando el número de instantáneas excede el número que se especificó aquí, las instantáneas más antiguas se suprimen primero.

▼ Edición de una política de retención de instantáneas (CLI)

Use el siguiente procedimiento para editar una política de retención de instantáneas para un sistema de archivos, un LUN o un proyecto. Las políticas de retención de instantáneas se incluyen en los programas de instantáneas automáticas.

1. **Vaya a shares y seleccione el proyecto o el recurso compartido.**

```
hostname:> shares select myproject
hostname:shares myproject> select demo_share
hostname:shares myproject/demo_share>
```

2. **Introduzca `snapshots automatic`.**

Puede usar el comando `list` para mostrar una lista de los programas de instantáneas automáticas correspondientes a este recurso compartido o proyecto.

```

hostname:shares myproject/demo_share> snapshots automatic
hostname:shares myproject/demo_share snapshots automatic> list
Properties:
    convert = false

Automatics:

NAME          FREQUENCY  DAY  HH:MM  KEEP
automatic-000  hour      -    -:02   4

```

3. Seleccione el programa que desea editar.

```
hostname:shares myproject/demo_share snapshots automatic> select automatic-000
```

4. Configure la propiedad `keep` con el número de instantáneas que desea conservar para este programa.

Configure la propiedad `keep` con el número de instantáneas que desea conservar para este programa (en el caso de instantáneas que se toman cada media hora o una hora, la propiedad puede tener un valor máximo de 48 y 24, respectivamente). Cuando el número de instantáneas excede el número que se especificó, las instantáneas más antiguas se suprimen primero.

Puede definir `keep=0` para no aplicar ninguna política de retención. En este caso, las instantáneas automáticas de ese programa se conservan para siempre (excepto en el caso de instantáneas que se toman cada media hora o una hora, a las que se aplica un máximo de 48 y 24, respectivamente).

```
hostname:shares myproject/demo_share snapshots automatic-000> set keep=4
keep=4 (uncommitted)
```

5. Escriba `commit` para guardar el cambio.

```
hostname:shares myproject/demo_share snapshots automatic-000> commit
```

▼ Eliminación de un programa de instantáneas (BUI)

Use el siguiente procedimiento para suprimir un programa de instantáneas automáticas para un sistema de archivos, un LUN o un proyecto.

1. Vaya al proyecto o al recurso compartido apropiado.
 - a. Si la instantánea corresponde a un proyecto, vaya a Recursos compartidos > Proyectos.
 - b. Si la instantánea corresponde a un sistema de archivos, vaya a Recursos compartidos > Recursos compartidos.

- c. Si la instantánea corresponde a un LUN, vaya a Recursos compartidos > Recursos compartidos y haga clic en LUNs (LUN).
 2. Mueva el cursor sobre el proyecto o el recurso compartido apropiado y haga clic en el ícono de edición .
 3. Haga clic en la ficha Instantáneas.
 4. Haga clic en Programas.
 5. Mueva el cursor sobre el programa que desea eliminar y haga clic en el ícono de eliminación .
- Aparece una ventana para advertirle que tal vez se destruyan las instantáneas automáticas existentes.
6. Si desea conservar las instantáneas automáticas existentes, haga clic en Convertir para convertirlas en instantáneas manuales. De lo contrario, haga clic en Desechar para destruirlas.

▼ Eliminación de un programa de instantáneas (CLI)

Use el siguiente procedimiento para suprimir un programa de instantáneas automáticas para un sistema de archivos, un LUN o un proyecto.

1. Vaya al proyecto o al recurso compartido y selecciónelo.

```
hostname:> shares select myproject
hostname:shares myproject> select demo_share
```

2. Introduzca `snapshots automatic`.

```
hostname:shares myproject/demo_share> snapshots automatic
hostname:shares myproject/demo_share snapshots automatic>
```

Puede usar el comando `list` para mostrar una lista de los programas de instantáneas automáticas correspondientes a este recurso compartido o proyecto.

```
hostname:shares myproject/demo_share snapshots automatic> list
Properties:
    convert = false
```

Automatics:

NAME	FREQUENCY	DAY	HH:MM	KEEP
automatic-000	day	-	00:00	4

3. **Si desea conservar las instantáneas automáticas existentes tomadas con este programa, configure la propiedad `convert` con el valor `true`.**

Si conserva el valor `convert = false` para esta propiedad, las instantáneas automáticas tomadas con este programa se desechan cuando se destruye el programa.

```
hostname:shares myproject/demo_share snapshots automatic> set convert=true
convert = true
hostname:shares myproject/demo_share snapshots automatic> commit
```

Puede utilizar el comando `list` para ver el cambio.

```
hostname:shares myproject/demo_share snapshots automatic> list
Properties:
convert = true
```

Automatics:

NAME	FREQUENCY	DAY	HH:MM	KEEP
automatic-000	day	-	00:00	4

4. **Use el comando `destroy` seguido del nombre del programa de instantáneas que desea destruir.**

Se le solicita que confirme.

```
hostname:shares myproject/demo_share snapshots automatic> destroy automatic-000
This will destroy "automatic-000". Are you sure? (Y/N)
```

5. **Escriba `y` para confirmar.**

```
This will destroy "automatic-000". Are you sure? (Y/N) y
```

▼ Visibilidad de un directorio de instantáneas del sistema de archivos (BUI)

Use el siguiente procedimiento para configurar que el directorio `.zfs/snapshot`, que de manera predeterminada está oculto, se mantenga visible como cualquier otro directorio del sistema de archivos.

El directorio `.zfs/snapshot` incluye una lista de todas las instantáneas que se encuentran en el sistema de archivos. El acceso a las instantáneas es igual que el acceso normal a los datos del sistema de archivos, pero las instantáneas son de solo lectura. De manera predeterminada, el directorio `.zfs` no es visible cuando se muestra el contenido de los directorios. Esta configuración evita que el software de copias de seguridad realice involuntariamente copias de seguridad de las instantáneas además de copias de seguridad de los datos nuevos.

Nota - Si se configura el directorio `.zfs/snapshot` con el valor "visible", el software de copia de seguridad puede hacer copias de seguridad de las instantáneas además de copias de seguridad de los datos activos.

1. **Vaya a Recursos compartidos > Recursos compartidos.**
2. **Mueva el cursor sobre el sistema de archivos deseado y haga clic en el ícono de edición .**
3. **Haga clic en la ficha Instantáneas.**
4. **Desmarque el cuadro "Heredar del proyecto" que se encuentra junto a Propiedades o haga clic en el ícono del candado que se encuentra junto a ".zfs/snapshot visibility".**
5. **Seleccione "Visible" en el menú desplegable que se encuentra junto a ".zfs/snapshot visibility".**
6. **Haga clic en Aplicar para guardar los cambios.**

Para que el directorio esté oculto nuevamente, regrese a esta página y seleccione "Oculto" en el menú desplegable y, a continuación, haga clic en Aplicar.

▼ Visibilidad de un directorio de instantáneas del sistema de archivos (CLI)

Use el siguiente procedimiento para configurar que el directorio `.zfs/snapshot`, que de manera predeterminada está oculto, se mantenga visible como cualquier otro directorio del sistema de archivos.

El directorio `.zfs/snapshot` incluye una lista de todas las instantáneas que se encuentran en el sistema de archivos. El acceso a las instantáneas es igual que el acceso normal a los datos del sistema de archivos, pero las instantáneas son de solo lectura. De manera predeterminada, el directorio `.zfs` no es visible cuando se muestra el contenido de los directorios. Esta configuración evita que el software de copias de seguridad realice involuntariamente copias de seguridad de las instantáneas además de copias de seguridad de los datos nuevos.

Nota - Si se configura el directorio `.zfs/snapshot` con el valor "visible", el software de copia de seguridad puede hacer copias de seguridad de las instantáneas además de copias de seguridad de los datos activos.

1. **Vaya al sistema de archivos y selecciónelo.**

```
hostname:> shares select myproject
hostname:shares myproject> select demo_share
hostname:shares myproject/demo_share>
```

2. **Use el comando `set snapdir` para configurar el directorio de instantáneas del sistema de archivos con el valor `visible`.**

```
hostname:shares myproject/demo_share> set snapdir=visible
snapdir=visible(uncommitted)
```

3. **Escriba `commit` para guardar el cambio.**

```
hostname:shares myproject/demo_share> commit
```

4. **Para que el directorio esté oculto nuevamente, regrese a este contexto y use el comando `set snapdir` para configurar el directorio como oculto y, a continuación, escriba `commit` para guardar el cambio.**

```
hostname:shares myproject/demo_share> set snapdir=hidden
snapdir=hidden(uncommitted)
hostname:shares myproject/demo_share> commit
```

Temas relacionados

- [Acceso a un directorio oculto de instantáneas del sistema de archivos \(CLI\) \[607\]](#)
- [Visibilidad de un directorio de instantáneas del sistema de archivos \(BUI\) \[605\]](#)
- [Acceso a un directorio visible de instantáneas del sistema de archivos \(CLI\) \[608\]](#)

▼ Acceso a un directorio oculto de instantáneas del sistema de archivos (CLI)

Use el siguiente procedimiento para acceder a instantáneas del sistema de archivos mediante los protocolos de datos en la instantánea `.zfs/snapshot` ubicada en la raíz del sistema de archivos.

El directorio `.zfs/snapshot` incluye una lista de todas las instantáneas que se encuentran en el sistema de archivos. El acceso a las instantáneas es igual que el acceso normal a los datos del sistema de archivos, pero las instantáneas son de solo lectura. De forma predeterminada, el directorio `.zfs` no está visible en la lista de contenidos del directorio, pero se puede acceder a este mediante una consulta explícita. Esto evita que el software de copias de seguridad realice involuntariamente copias de seguridad de las instantáneas además de los datos nuevos.

1. **En una ventana de terminal, vaya al directorio donde montó el recurso compartido.**
2. **Busque `.zfs/snapshot`.**

Desde allí, puede mostrar una lista de las instantáneas de este sistema de archivos y mirar el contenido de cada instantánea.

ejemplo 6 Acceso a .zfs/snapshot

En este ejemplo, hay dos instantáneas de un sistema de archivos. La primera instantánea tiene tres archivos.

```
$ ls -l /mnt/demo
$ ls -l /mnt/demo/.zfs/snapshot
demo_snap1
demo_snap2
$ ls -l /mnt/demo/.zfs/snapshot/demo_snap1
file1
file2
file3
```

Temas relacionados

- [Visibilidad de un directorio de instantáneas del sistema de archivos \(BUI\) \[605\]](#)
- [Visibilidad de un directorio de instantáneas del sistema de archivos \(CLI\) \[606\]](#)
- [Acceso a un directorio visible de instantáneas del sistema de archivos \(CLI\) \[608\]](#)

▼ Acceso a un directorio visible de instantáneas del sistema de archivos (CLI)

Use el siguiente procedimiento para acceder a las instantáneas del sistema de archivos que se encuentran en el directorio `.zfs/snapshot` después de haberlo configurado como visible.

Antes de empezar Configure el directorio `.zfs/snapshot` con el valor Visible como se describe en [Visibilidad de un directorio de instantáneas del sistema de archivos \(CLI\) \[606\]](#).

1. **Vaya al directorio donde montó el recurso compartido.**
2. **Vaya a `.zfs/snapshot` dentro de ese directorio.**

Desde allí, puede mostrar una lista de las instantáneas de este sistema de archivos y mirar el contenido de cada instantánea.

▼ Cambio de nombre de una instantánea (BUI)

Use el siguiente procedimiento para renombrar una instantánea manual existente. No se puede cambiar el nombre de las instantáneas automáticas, que incluyen `.auto`, `.rr O` `.ndmp` en el nombre.

Si se cambia el nombre a una instantánea de un recurso compartido que forma parte de una instantánea de un proyecto más grande, esta ya no será considerada parte de la misma instantánea, y si se cambia el nombre de alguna instantánea para que tenga el mismo nombre que una de las instantáneas del proyecto principal, esta se considerará parte de la instantánea del proyecto.

Antes de empezar

- Para finalizar este procedimiento, debe tener privilegios de superusuario o una de las siguientes autorizaciones de roles en el ámbito Proyectos y recursos compartidos:
 - `renameSnap`: permite cambiar el nombre de las instantáneas.
 - `rename`: permite cambiar el nombre de los proyectos y los recursos compartidos, incluidos los nombres de las instantáneas.
- Para agregar autorizaciones a un rol, consulte [Edición de autorizaciones de un rol \(BUI\) \[269\]](#).

1. **Vaya al recurso compartido o al proyecto que incluye la instantánea que desea renombrar.**
 - Para renombrar una instantánea de un sistema de archivos, vaya a **Recursos compartidos > Recursos compartidos**.
 - Para renombrar una instantánea de un LUN, vaya a **Recursos compartidos > Recursos compartidos** y haga clic en **LUNs (LUN)**.
 - Para renombrar una instantánea de un proyecto, vaya a **Recursos compartidos > Proyectos**.
2. **Mueva el cursor del mouse sobre el recurso compartido o el proyecto que incluye la instantánea que desea renombrar y haga clic en el ícono de edición .**
3. **Haga clic en la ficha Instantáneas.**
4. **Debajo de Instantáneas, haga clic en la instantánea que desea renombrar.**
El nombre de la instantánea se convierte en un cuadro de entrada de texto.
5. **Escriba el nombre nuevo para la instantánea.**
El nombre debe tener de 1 a 64 caracteres, pero no puede tener espacios ni comenzar con un punto. Los caracteres permitidos son: caracteres alfanuméricos y caracteres especiales (_ - .). :
6. **Pulse Intro para confirmar el cambio.**

Temas relacionados

- [“Descripción de usuarios y roles” \[273\]](#)
- [“Autorizaciones de usuarios” \[274\]](#)

▼ Cambio de nombre de una instantánea (CLI)

Use el siguiente procedimiento para renombrar una instantánea manual existente. No se puede cambiar el nombre de las instantáneas automáticas.

Si se cambia el nombre a una instantánea de un recurso compartido que forma parte de una instantánea de un proyecto más grande, esta ya no será considerada parte de la misma instantánea, y si se cambia el nombre de alguna instantánea para que tenga el mismo nombre que una de las instantáneas del proyecto principal, esta se considerará parte de la instantánea del proyecto.

- Antes de empezar**
- Para finalizar este procedimiento, debe tener privilegios de superusuario o una de las siguientes autorizaciones de roles en el ámbito Proyectos y recursos compartidos:
 - `renameSnap`: permite cambiar el nombre de las instantáneas.
 - `rename`: permite cambiar el nombre de los proyectos y los recursos compartidos, incluidos los nombres de las instantáneas.
 - Para agregar autorizaciones a un rol, consulte [Edición de autorizaciones de un rol \(CLI\) \[270\]](#).

1. Vaya a `shares` y seleccione el proyecto, o seleccione el proyecto y, a continuación, un recurso compartido.

```
hostname:> shares select myproject
hostname:shares myproject> select demo_share
```

2. Introduzca `snapshots`.

```
hostname:shares myproject/demo_share> snapshots
```

3. Introduzca `list` para mostrar una lista de las instantáneas de este proyecto o recurso compartido.

```
hostname:shares myproject/demo_share snapshots> list
demo_snap1
demo_snap2
```

4. Para cambiar el nombre de la instantánea, introduzca `rename` seguido del nombre actual de la instantánea, un espacio y el nombre nuevo para la instantánea.

El nombre debe tener de 1 a 64 caracteres, pero no puede tener espacios ni comenzar con un punto. Los caracteres permitidos son: caracteres alfanuméricos y caracteres especiales (`_` `-` `.`). :

```
hostname:shares myproject/demo_share snapshots> rename demo_snap1 new_name
```

Temas relacionados

- [“Descripción de usuarios y roles” \[273\]](#)
- [“Autorizaciones de usuarios” \[274\]](#)

▼ Reversión de una instantánea (BUI)

Use el siguiente procedimiento para revertir, o restaurar, un sistema de archivos o un LUN a una instantánea existente.

Cuando se produce una reversión, se destruyen las instantáneas más nuevas (y sus clones), y los datos activos vuelven al estado que tenían en el momento en que se tomó la instantánea. Las instantáneas solo incluyen datos, no propiedades, de manera que cualquier configuración de propiedades que se haya cambiado desde la toma de la instantánea se mantendrá. Durante la reversión se pierden los cambios realizados en el acceso al directorio raíz del sistema de archivos.



Atención - Este procedimiento no se puede deshacer.

1. **Vaya al recurso compartido o al proyecto que incluye la instantánea que desea renombrar.**
 - Para restaurar una instantánea de un sistema de archivos, vaya a **Recursos compartidos > Recursos compartidos**.
 - Para restaurar una instantánea de un LUN, vaya a **Recursos compartidos > Recursos compartidos** y haga clic en **LUNs (LUN)**.
2. **Mueva el cursor del mouse sobre el recurso compartido que incluye la instantánea que desea restaurar y haga clic en el ícono de edición .**
3. **Haga clic en la ficha Instantáneas.**
4. **Pase el cursor del mouse sobre la instantánea que desea restaurar, haga clic en el ícono de reversión  y confirme la acción.**

▼ Reversión de una instantánea (CLI)

Use el siguiente procedimiento para revertir, o restaurar, un sistema de archivos o un LUN a una instantánea existente.

Con la restauración de una instantánea se destruyen las instantáneas más recientes y sus clones, y se revierte el contenido de los recursos compartidos al estado en el que se encontraba en el momento en que se tomó la instantánea. La configuración de las propiedades en el recurso compartido no se ven afectadas, pero los cambios en el acceso al directorio raíz del sistema de archivos se pierden durante la reversión.



Atención - Este procedimiento no se puede deshacer.

1. **Vaya al recurso compartido que contiene la instantánea que desea restaurar y selecciónelo.**

```
hostname:> shares select myproject
hostname:shares myproject> select demo_share
```

2. **Introduzca `snapshots`.**

```
hostname:shares myproject/demo_share> snapshots
```

3. **Introduzca `list` para mostrar una lista de las instantáneas de este proyecto o recurso compartido.**

```
hostname:shares myproject/demo_share snapshots> list
demo_snap1
demo_snap2
```

4. **Seleccione la instantánea que desea restaurar y, a continuación, introduzca el comando `rollback`.**

```
hostname:shares myproject/demo_share snapshots> select demo_snap1
hostname:shares myproject/demo_share@demo_snap1> rollback
```

5. **Escriba `y` para confirmar.**

```
hostname:shares myproject/demo_share@demo_snap1> rollback
Rolling back will revert data to snapshot, destroying newer data. Active initiators will be
disconnected.
Continue? (Y/N)
hostname: shares myproject/demo_share@demo_snap1> y
```

▼ Destrucción de una instantánea (BUI)

Utilice el siguiente procedimiento para destruir una instantánea.

- Antes de empezar**
- Para finalizar este procedimiento, debe tener privilegios de superusuario o una de las siguientes autorizaciones de roles en el ámbito Proyectos y recursos compartidos:
 - `destroySnap`: permite destruir instantáneas.
 - `destroy`: permite destruir proyectos y recursos compartidos, incluidas las instantáneas.
 - Para agregar autorizaciones a un rol, consulte [Edición de autorizaciones de un rol \(BUI\) \[269\]](#).

1. Vaya a la instantánea.

- En el caso de una instantánea de un sistema de archivos o un LUN, vaya a **Recursos compartidos > Recursos compartidos** y haga clic en **Sistemas de archivos o LUN**, en función de si la instantánea que desea destruir corresponde a un sistema de archivos o un LUN.
- En el caso de una instantánea de un proyecto, vaya a **Recursos compartidos > Proyectos**.

2. Mueva el cursor sobre el recurso compartido apropiado y haga clic en el ícono de edición .

3. Haga clic en la ficha Instantáneas.

4. Pase el cursor del mouse sobre la instantánea que desea destruir y haga clic en el ícono de destrucción .

Aparece un cuadro de diálogo de confirmación.

Si se hicieron clones de esta instantánea, se le muestra una lista de los clones que se verán afectados. Al destruir una instantánea, también se destruyen los clones de esa instantánea y los descendientes de esos clones.

5. Haga clic en Aceptar para confirmar.

Temas relacionados

- [“Descripción de usuarios y roles” \[273\]](#)
- [“Autorizaciones de usuarios” \[274\]](#)

▼ Destrucción de una instantánea (CLI)

Utilice el siguiente procedimiento para destruir una instantánea.

- Antes de empezar**
- Para finalizar este procedimiento, debe tener privilegios de superusuario o una de las siguientes autorizaciones de roles en el ámbito Proyectos y recursos compartidos:
 - `destroySnap`: permite a los usuarios destruir solo instantáneas.
 - `destroy`: otorga privilegios para eliminar proyectos y recursos compartidos, incluidas las instantáneas.
 - Para agregar autorizaciones a un rol, consulte [Edición de autorizaciones de un rol \(CLI\) \[270\]](#).

1. **Vaya a `shares` y seleccione el proyecto, o seleccione el proyecto y, a continuación, un recurso compartido.**

```
hostname:> shares select myproject
hostname:shares myproject> select demo_share
```

2. **Introduzca `snapshots`.**

```
hostname:shares myproject/demo_share> snapshots
```

3. **Introduzca `list` para mostrar una lista de las instantáneas de este proyecto o recurso compartido.**

```
hostname:shares myproject/demo_share snapshots> list
demo_snap1
demo_snap2
```

4. **Use el comando `destroy` para suprimir una instantánea individual mediante uno de dos métodos:**

- Seleccione la instantánea que desea suprimir y, a continuación, escriba `destroy`.

```
hostname:shares myproject/demo_share snapshots> select demo_snap1
hostname:shares myproject/demo_share@demo_snap1> destroy
```

- Escriba `destroy` seguido del nombre de la instantánea.

```
hostname:shares myproject/demo_share snapshots> destroy demo_snap1
```

5. **Escriba `y` para confirmar la acción.**

```
This will destroy all data in "demo_snap1"! Are you sure? (Y/N) Y
```

Temas relacionados

- [“Descripción de usuarios y roles” \[273\]](#)
- [“Autorizaciones de usuarios” \[274\]](#)

▼ Clonación de una instantánea (BUI)

Nota - La clonación es una característica que se ofrece con licencia para determinados modelos. Para obtener información detallada, consulte "Acuerdo de licencia de software (SLA) de Oracle y derecho de sistemas de hardware con opciones de software integrado" y el Manual de usuario de información sobre licencias para la versión de software.

Use el siguiente procedimiento para hacer un clon de una instantánea existente de un sistema de archivos o un LUN.

Nota - No se admiten clones de proyectos.

1. **Vaya al recurso compartido que desea clonar.**
 - a. **Para clonar un sistema de archivos, vaya a Recursos compartidos > Recursos compartidos.**
 - b. **Para clonar un LUN, vaya a Recursos compartidos > Recursos compartidos y haga clic en LUNs (LUN).**
2. **Mueva el cursor sobre el recurso compartido deseado y haga clic en el ícono de edición .**
3. **Haga clic en la ficha Instantáneas.**
4. **Pase el cursor del mouse sobre la instantánea que desea clonar y haga clic en el ícono de clonación .**
Aparece un cuadro de diálogo con parámetros de configuración y opciones para el nuevo clon.
5. **Configure cada campo según corresponda.**
 - a. **En el menú desplegable Proyecto, seleccione el proyecto de destino.**
Por defecto, el clon se crea dentro del proyecto actual, pero se lo puede crear en otro proyecto.
 - b. **Introduzca un nombre para el clon.**
 - c. **(Opcional) Haga clic en el ícono del candado que se encuentra junto a Punto de montaje y defina un punto de montaje para el clon.**

Si deja este campo bloqueado, el punto de montaje del clon seguirá siendo el valor `/export/<sharename>` por defecto.

d. (Opcional) Haga clic en el ícono del candado que se encuentra junto a Nombre de recurso e introduzca uno de los siguientes valores:

- **off:** SMB está desactivado.
- **on:** SMB está activado, de modo que puede compartir el clon por medio de SMB. El nombre del clon en SMB coincide con el nombre del clon en el dispositivo.
- **<pick_a_name>:** SMB está activado, de modo que puede compartir el clon por medio de SMB. El nombre del clon en SMB es el nombre que especifique aquí en lugar del nombre del clon que se indica en el dispositivo.

Si deja este campo bloqueado, la propiedad Nombre de recurso se hereda de la instantánea que está clonando.

e. (Opcional) Marque la casilla de control Heredar clave o desmarque esa casilla y seleccione en cambio el almacén de claves y el nombre de la clave de cifrado que desea que herede el clon.

Si la casilla está seleccionada, el almacén de claves y el nombre de clave del clon serán los del proyecto de destino.

Si la casilla no está seleccionada, el almacén de claves y el nombre de clave del clon serán los del recurso compartido principal. De manera alternativa, seleccione otro almacén de claves y otro nombre de clave en el menú desplegable.

f. (Opcional) Seleccione la casilla de control Conservar otros valores de configuración local para que las propiedades heredadas se conserven como configuración local en el nuevo clon.

Este campo determina si las propiedades heredadas provienen del juego de datos principal o del proyecto de destino. Por defecto, la casilla no está seleccionada, lo que significa que todas las propiedades heredadas para el nuevo clon provienen del proyecto de destino. Si selecciona la casilla, todas las propiedades actualmente heredadas se conservarán como configuración local en el nuevo clon.

6. Haga clic en Aplicar para confirmar la configuración y crear el clon.

El clon aparece en la lista de recursos compartidos para el proyecto de destino que defina. Puede trabajar con un clon como con cualquier otro recurso compartido.

Temas relacionados

- Para realizar operaciones de recurso compartido en un clon, consulte [Recursos compartidos y proyectos \[483\]](#).

- Para hacer un clon de un clon, consulte [Clonación de un clon \[619\]](#).
- Para ver todos los clones de una instantánea en particular, consulte [Visualización de clones de una instantánea \(BUI\) \[619\]](#).
- Para determinar la instantánea a partir de la que se creó un clon, consulte [Visualización del origen de un clon \(BUI\) \[620\]](#).
- Para hacer un clon de una instantánea en un paquete de replicación, consulte [Clonación de una instantánea en un paquete de replicación \(BUI\) \[687\]](#).

▼ Clonación de una instantánea (CLI)

Nota - La clonación es una característica que se ofrece con licencia para determinados modelos. Para obtener información detallada, consulte "Acuerdo de licencia de software (SLA) de Oracle y derecho de sistemas de hardware con opciones de software integrado" y el Manual de usuario de información sobre licencias para la versión de software.

Use el siguiente procedimiento para hacer un clon de una instantánea existente de un sistema de archivos o un LUN.

Nota - No se admiten clones de proyectos.

1. **Vaya al sistema de archivos, el LUN o el proyecto apropiado y escriba `snapshots`.**

```
hostname:shares myproject/demo_share> snapshots
hostname:shares myproject/demo_share snapshots>
```

2. **Seleccione la instantánea que desea clonar.**

```
hostname:shares myproject/demo_share snapshots> select snap1
```

3. **Use el comando `clone` seguido, de manera opcional, del nombre del proyecto en el que desea crear el clon.**

De manera predeterminada, el clon se crea en el mismo proyecto que la instantánea que se está clonando.

```
hostname:shares myproject/demo_share@snap1> clone project1
```

Pasa a un contexto de recurso compartido sin confirmar. Desde aquí, podrá ajustar las propiedades según sea necesario antes de confirmar los cambios para crear el clon.

4. **Use el comando `get` para ver las propiedades.**

```
hostname:shares myproject/demo_clone (uncommitted clone)> get
aclinherit = restricted (inherited)
```

```
aclmode = discard (inherited)
atime = true (inherited)
checksum = fletcher4 (inherited)
compression = off (inherited)
copies = 1 (inherited)
mountpoint = /export/testbed (inherited)
quota = 0 (default)
readonly = false (inherited)
recordsize = 128K (inherited)
reservation = 0 (default)
secondarycache = all (inherited)
nbmand = false (inherited)
sharesmb = off (inherited)
sharenfs = on (inherited)
snapdir = hidden (inherited)
vscan = false (inherited)
shadedav = off (inherited)
shareftp = off (inherited)
root_group = other (default)
root_permissions = 777 (default)
root_user = nobody (default)
quota_snap = true (default)
reservation_snap = true (default)
```

5. Use el comando `set` para ajustar las propiedades.

```
hostname:shares myproject/demo_clone (uncommitted clone)> set quota=10G
quota = 10G (uncommitted)
```

6. Use el comando `commit` para confirmar los cambios y crear el clon.

```
hostname:shares myproject/demo_clone (uncommitted clone)> commit
hostname:shares myproject/demo_share@demo_clone>
```

Temas relacionados

- Para realizar operaciones de recurso compartido en un clon, consulte [Recursos compartidos y proyectos \[483\]](#).
- Para hacer un clon de un clon, consulte [Clonación de un clon \[619\]](#).
- Para ver todos los clones de una instantánea en particular, consulte [Visualización de clones de una instantánea \(CLI\) \[620\]](#).
- Para determinar la instantánea a partir de la que se creó un clon, consulte [Visualización del origen de un clon \(CLI\) \[621\]](#).
- Para hacer un clon de una instantánea en un paquete de replicación, consulte [Clonación de una instantánea en un paquete de replicación \(CLI\) \[691\]](#).

▼ Clonación de un clon

Nota - La clonación es una característica que se ofrece con licencia para determinados modelos. Para obtener información detallada, consulte "Acuerdo de licencia de software (SLA) de Oracle y derecho de sistemas de hardware con opciones de software integrado" y el Manual de usuario de información sobre licencias para la versión de software.

Use el siguiente procedimiento para hacer un clon de un clon existente.

Después de haber creado un clon de una instantánea de un sistema de archivos o un LUN, puede trabajar con ese clon como con cualquier otro recurso compartido. Puede tomar una instantánea del clon y puede hacer un clon de esa instantánea. Puede continuar este proceso para hacer clones de clones indefinidamente.

1. **Para tomar una instantánea del clon, use uno de estos procedimientos:**
 - [Toma de una instantánea \(BUI\) \[592\]](#)
 - [Toma de una instantánea \(CLI\) \[593\]](#)
2. **Para clonar la instantánea, use uno de estos procedimientos:**
 - [Clonación de una instantánea \(BUI\) \[615\]](#)
 - [Clonación de una instantánea \(CLI\) \[617\]](#)

▼ Visualización de clones de una instantánea (BUI)

Use el siguiente procedimiento para ver una lista de todos los clones creados a partir de una instantánea en particular. Estos clones también se conocen como "clones dependientes" de la instantánea.

1. **Vaya a Recursos compartidos > Recursos compartidos y haga clic en Sistemas de archivos o LUN, según si desea ver los clones de un sistema de archivos o de un LUN.**
2. **Mueva el cursor sobre el recurso compartido apropiado y haga clic en el ícono de edición .**
3. **Haga clic en la ficha Instantáneas.**
4. **Mueva el cursor del mouse sobre la instantánea apropiada y haga clic en "Mostrar...", debajo de Clones.**

Aparece una ventana con una lista de los clones dependientes de la instantánea y los proyectos en los que se encuentran.

Si el enlace "Mostrar..." no aparece, significa que la instantánea no tiene clones.

5. **Haga clic en Aceptar para cerrar la ventana.**

▼ Visualización de clones de una instantánea (CLI)

Use el siguiente procedimiento para ver una lista de todos los clones creados a partir de una instantánea en particular.

1. **Vaya a la instantánea y selecciónela.**

```
hostname:shares myproject/demo_share> snapshots
hostname:shares myproject/demo_share snapshots> select snap1
hostname:shares myproject/demo_share@snap1>
```

2. **Utilice el comando `list clones`.**

```
hostname:shares myproject/demo_share@snap1> list clones
```

Clones: 2 total

PROJECT	SHARE
myproject	demo_clone1
myproject	demo_clone2

```
hostname:shares myproject/demo_share@snap1>
```

El resultado muestra la cantidad de clones que existen, el proyecto en el que reside cada uno y el nombre de cada clon.

▼ Visualización del origen de un clon (BUI)

Use el siguiente procedimiento para determinar la instantánea a partir de la cual se hizo el clon.

1. **Vaya al clon.**
 - a. **Vaya a Recursos compartidos > Recursos compartidos.**
 - b. **Mueva el cursor sobre el clon deseado y haga clic en el ícono de edición .**
2. **Debajo de Propiedades estáticas a la izquierda, haga clic en "Mostrar" junto a "Origen de clon".**

Aparece una ventana que muestra el nombre de la instantánea a partir de la cual se hizo el clon.

▼ Visualización del origen de un clon (CLI)

Use el siguiente procedimiento para determinar la instantánea a partir de la cual se hizo el clon.

1. **Vaya a shares, seleccione el proyecto que contiene el clon y, a continuación, seleccione el clon.**

```
hostname:> shares select myproject
hostname:shares myproject> select demo_clone
hostname:shares myproject/demo_clone>
```

2. **Use el comando `get origin`.**

El comando devuelve la ubicación y el nombre de la instantánea a partir de la cual se hizo el clon.

```
hostname:shares myproject/demo_clone> get origin
origin = myproject/demo_share@demo_snapshot
```


Replicación remota

Nota - La replicación y la clonación son características que se ofrecen con licencia para determinados modelos. Para obtener información detallada, consulte "Acuerdo de licencia de software (SLA) de Oracle y derecho de sistemas de hardware con opciones de software integrado" y el Manual de usuario de información sobre licencias para la versión de software.

Oracle ZFS Storage Appliance admite la replicación basada en instantáneas de proyectos y recursos compartidos desde un dispositivo de origen hacia un destino de replicación, una agrupación diferente en el mismo dispositivo o un servidor NFS para replicación fuera de línea. Se puede configurar la replicación para que se ejecute de forma manual, en un programa o de manera continua. Los casos de uso para la replicación remota incluyen recuperación ante desastres, distribución de datos, copia de seguridad disco a disco y migración de datos entre dispositivos cuando se actualiza el hardware o se vuelve a equilibrar el almacenamiento.

Para configurar, supervisar y administrar la replicación remota, use las siguientes tareas:

- [Flujo de trabajo de replicación remota](#) [623]
- [“Configuración de la replicación remota”](#) [624]
- [“Supervisión de la replicación remota”](#) [666]
- [“Gestión de paquetes de replicación”](#) [675]
- [“Recuperación ante desastres con replicación remota”](#) [700]

Para obtener información detallada acerca de la replicación remota, consulte:

- [“Conceptos de replicación remota”](#) [708]

▼ Flujo de trabajo de replicación remota

A continuación, se resumen los pasos básicos para usar la replicación remota. Para obtener información acerca de los conceptos de replicación remota, consulte [“Conceptos de replicación remota”](#) [708].

1. **Compruebe la compatibilidad del software en los dispositivos de origen y destino.**

Para obtener información acerca de la compatibilidad de software, consulte [Comprobación de la compatibilidad de origen y destino \[625\]](#).

2. Configure las interfaces y el enrutamiento de red.

Para obtener información acerca de la configuración del enrutamiento de red, consulte Configuración de interfaces de red y enrutamiento estático: [BUI](#), [CLI](#).

3. Cree un destino de replicación.

Para obtener información acerca de la creación de un destino de replicación, consulte Creación de un destino de replicación: [BUI](#), [CLI](#).

4. Cree una acción de replicación.

Para obtener información acerca de la creación de una acción de replicación, consulte Creación de una acción de replicación: [BUI](#), [CLI](#).

5. Envío de una actualización de replicación según lo especificado en la acción de replicación.

Las actualizaciones de replicación se realizan con la frecuencia especificada, de manera continua o manualmente. Consulte [“Frecuencia de actualización de replicación” \[715\]](#).

6. De manera opcional, configure una replicación fuera de línea.

Para obtener información acerca de la replicación fuera de línea, consulte Configuración de replicación fuera de línea: [BUI](#), [CLI](#).

Configuración de la replicación remota

Use las siguientes tareas para configurar la replicación remota:

- [Comprobación de la compatibilidad de origen y destino \[625\]](#)
- Configuración de interfaces de red y enrutamiento estático: [BUI](#), [CLI](#)
- Creación de un destino de replicación: [BUI](#), [CLI](#)
- Creación de una acción de replicación: [BUI](#), [CLI](#)
- Configuración de gestión de instantáneas automáticas en el destino: [BUI](#), [CLI](#)
- Envío manual de una actualización de replicación: [BUI](#), [CLI](#)
- [Configuración de replicación para una configuración en cluster \[642\]](#)
- Configuración de replicación fuera de línea: [BUI](#), [CLI](#)
- Desactivación de la compresión de replicación: [BUI](#), [CLI](#)

- Prueba de la conexión: [BUI](#), [CLI](#)
- Edición de un destino de replicación: [BUI](#), [CLI](#)
- Edición de una acción de replicación: [BUI](#), [CLI](#)

▼ Comprobación de la compatibilidad de origen y destino

La replicación remota es compatible entre la mayoría de las versiones de software de los dispositivos Oracle ZFS Storage Appliance. Cuando una actualización de replicación utiliza una función que no está admitida en el destino de replicación, se producen errores de compatibilidad. Las funciones se proporcionan mediante actualizaciones de software o como actualizaciones diferidas.

Para obtener información detallada acerca de la compatibilidad y las funciones de las actualizaciones diferidas para cada versión de software, consulte el documento Compatibilidad de la replicación remota en dispositivos Oracle ZFS Storage Appliance (ID de documento 1958039.1) en [My Oracle Support](http://support.oracle.com/) (<http://support.oracle.com/>).

1. Compruebe la versión actual del software en los dispositivos de origen y destino.

Si usa la BUI, vaya a Mantenimiento > Sistema. Si usa la CLI, navegue hasta `maintenance system updates` e introduzca `show`.

2. Asegúrese de que el destino de replicación admita las funciones de las actualizaciones diferidas que se utilizan en el proyecto o el recurso compartido de origen.

Por ejemplo, si el origen usa bloques grandes, asegúrese de que el destino de replicación proporcione compatibilidad para esta función.

3. Actualice el software y aplique las actualizaciones diferidas en el destino de replicación, según sea necesario.

Para obtener más información, consulte [“Deferred Updates” in Oracle ZFS Storage Appliance Customer Service Manual](#).

4. Si el proyecto o el recurso compartido que desea replicar están cifrados, asegúrese de que la clave de cifrado utilizada en el origen también se encuentre disponible en el destino.

Para obtener información sobre la configuración de claves de cifrado, consulte [Cifrado de datos \[795\]](#).

5. **(Opcional) En los dispositivos de origen y de destino, establezca los cifrados y las versiones de SSL/TLS para la replicación, como se describe en “Configuración de cifrados y versiones de SSL/TLS” [318].**

Establezca los valores en función de los requisitos de seguridad del sitio. Las versiones y al menos uno de los cifrados deben ser idénticos en los dispositivos de origen y de destino. Es posible que los sistemas Oracle ZFS Storage Appliance que ejecutan una versión de firmware anterior no admitan los cifrados que se ofrecen en las versiones de TLS más recientes.

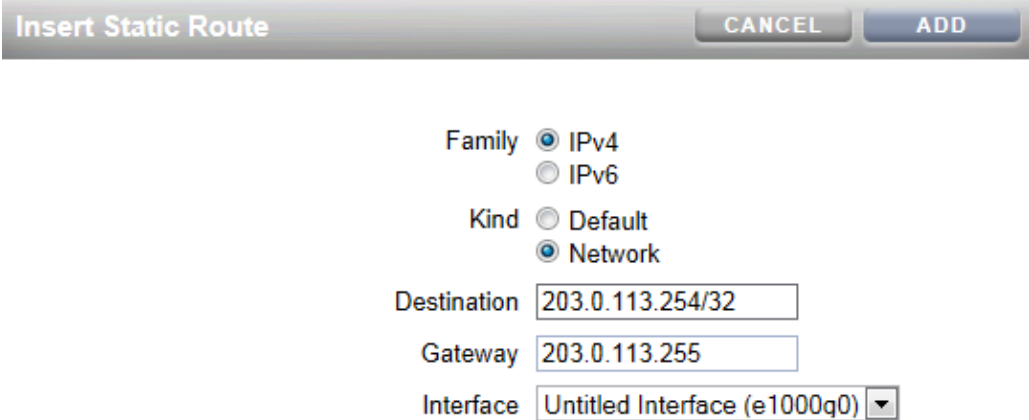
▼ Configuración de interfaces de red y enrutamiento estático (BUI)

Para garantizar que se utilicen las interfaces de red adecuadas para las conexiones de replicación entre los dispositivos de origen y destino, configure rutas estáticas /32 IPv4 (específicas para el host).

Si está configurando la replicación para una configuración de cluster, seleccione una interfaz de red única (desbloqueada) para que, después de una toma de control o un failback en el cluster, la interfaz pase al nodo en el que se está realizando el trabajo de replicación. Los dos nodos del cluster de origen pueden replicarse en el mismo nodo de destino solo si el nodo de destino proporciona dos direcciones IPv4, una para cada nodo del cluster de origen. No se puede replicar a la misma dirección IPv4 de destino desde ambos nodos de un cluster de origen.

1. **Vaya a la página Configuración > Red > Enrutamiento.**

2. Haga clic en el ícono de agregación .



3. En la pantalla Insertar ruta estática, especifique lo siguiente:

- **Familia:** seleccione IPv4.

Nota - La replicación remota no admite IPv6.

- **Tipo:** seleccione Red.
- **Destination** (Destino): introduzca la dirección IPv4 y la máscara de red /32 del dispositivo de destino.
- **Puerta de enlace:** introduzca la dirección de puerta de enlace del dispositivo de destino.
- **Interfaz:** introduzca el nombre de la interfaz.

4. Haga clic en Agregar.
5. Después de definir la ruta estática desde el dispositivo de origen al dispositivo de destino, repita estos pasos en el dispositivo de destino para definir la ruta estática desde el destino al origen.
6. Para verificar que el tráfico se redirija a través de las interfaces de origen y destino correctas, use el comando `tracert`.

Para obtener información acerca del uso de `tracert`, consulte [“Configuración de enrutamiento de red” \[121\]](#).

Nota - Cuando se suprime una interfaz, todas las rutas asociadas con la interfaz también se eliminan.

Temas relacionados

- [“Ejemplo: Configuración de replicación para dispositivos agrupados en clusters” \[730\]](#)
- [Flujo de trabajo de replicación remota \[623\]](#)
- [“Conceptos de replicación remota” \[708\]](#)

▼ Configuración de interfaces de red y enrutamiento estático (CLI)

Para garantizar que se utilicen las interfaces de red adecuadas para las conexiones de replicación entre los dispositivos de origen y destino, configure rutas estáticas /32 IPv4 (específicas para el host).

Si está configurando la replicación para una configuración de cluster, seleccione una interfaz de red única (desbloqueada) para que, después de una toma de control o un failback en el cluster, la interfaz pase al nodo en el que se está realizando el trabajo de replicación. Los dos nodos del cluster de origen pueden replicarse en el mismo nodo de destino solo si el nodo de destino proporciona dos direcciones IPv4, una para cada nodo del cluster de origen. No se puede replicar a la misma dirección IPv4 de destino desde ambos nodos de un cluster de origen.

1. Navegue hasta `configuration services routing` en el dispositivo de origen.

Use una ruta estática /32 (específica para el host) hasta la dirección IPv4 del sistema de destino mediante la interfaz de red dedicada. En el siguiente ejemplo, `mask=32` significa que se trata de una ruta específica para el host.

Nota - La replicación remota no admite IPv6.

```
host_source:configuration services routing> create

host_source:configuration services route (uncommitted)> get
  family = (unset)
  destination = (unset)
  mask = (unset)
  gateway = (unset)
  interface = (unset)
host_source:configuration services route (uncommitted)> set family=IPv4
host_source:configuration services route (uncommitted)> set destination=203.34.56.78
host_source:configuration services route (uncommitted)> set mask=32
host_source:configuration services route (uncommitted)> set gateway=203.34.56.254
```



```

host_source:configuration services route (uncommitted)> set interface=nge3
host_source:configuration services route (uncommitted)> commit
host_source:configuration services routing> show
route-000  0.0.0.0/0                203.24.30.254  nge0      static
route-001  203.24.30.0/32              203.24.30.28   nge0      dynamic
route-002  203.24.150.0/32                203.24.150.10  ibd0      dynamic
route-003  203.24.101.65/32              203.24.30.254  nge1      inactive
route-005  203.34.56.78/32               203.34.56.254  nge3      static

```

- Después de definir la ruta estática desde el dispositivo de origen al dispositivo de destino, repita estos pasos en el dispositivo de destino para definir la ruta estática desde el destino al origen.
- Para asegurarse de que el tráfico se redirija a través de las interfaces de origen y destino correctas, use el comando `traceroute`.

Para obtener información acerca del uso de `traceroute`, consulte [“Configuración de enrutamiento de red” \[121\]](#).

Nota - Cuando se suprime una interfaz, todas las rutas asociadas con la interfaz también se eliminan.

Temas relacionados

- [“Ejemplo: Configuración de replicación para dispositivos agrupados en clusters” \[730\]](#)
- [Flujo de trabajo de replicación remota \[623\]](#)
- [“Conceptos de replicación remota” \[708\]](#)

▼ Creación de un destino de replicación (BUI)

Un destino de replicación establece una conexión de comunicación segura entre los dispositivos de origen y destino.

Antes de empezar Consulte [Comprobación de la compatibilidad de origen y destino \[625\]](#) para comprobar que el destino de replicación sea compatible con el origen.

Si necesita comprobar que el tráfico de replicación se transmite a través de una interfaz de red específica, configure una ruta estática para el destino que especifique esa interfaz como se muestra en [Configuración de interfaces de red y enrutamiento estático \(BUI\) \[626\]](#).

- Desde la BUI del dispositivo de origen, vaya a **Configuración > Servicios > Replicación remota**.
- Haga clic en el ícono de agregación , junto a **Targets (Destinos)**.

Se muestra el cuadro de diálogo Agregar destino de replicación.

3. Introduzca información sobre el destino de replicación.

- **Nombre:** el nombre del destino que se debe mostrar en la BUI y la CLI del dispositivo de origen.
- **Nombre de host:** el nombre de dominio completo o la dirección IPv4 del dispositivo de destino. El valor recomendado para usar es el nombre de dominio completo de destino. Consulte la descripción de la opción Host Match (Coincidencia de host) en el cuadro de diálogo a continuación.
- **Contraseña de usuario root:** la contraseña de usuario root del dispositivo de destino para autorizar la conexión.
- **Host Match** (Coincidencia de host): cuando se activa esta opción, el sistema verifica que el nombre de host especificado en el campo Nombre de host de este cuadro de diálogo coincida con el host especificado en el certificado. Si se especifica una dirección IP o un nombre de dominio no completo para Nombre de host y el certificado solo contiene nombres de dominio completos, se produce un error en la coincidencia de host y no se crea el destino.

Si el destino utiliza un certificado basado en ASN, especifique el nombre de dominio completo del destino en el valor de la propiedad Nombre de host.

Si se desactiva la opción Host Match (Coincidencia de host), no se ejecuta la validación del nombre de host.

Para potenciar la seguridad, establezca el nombre de dominio completo del destino como valor de Nombre de host y asegúrese de que la opción Host Match (Coincidencia de host) esté activada.

4. Haga clic en Agregar.

La comprobación de confianza del certificado se ejecuta para verificar si el certificado es de confianza.

Si el certificado no es de confianza para el origen, se presentará el certificado para que usted lo revise y se le solicitará aceptar o rechazar el certificado como se describe en [Prueba de la conexión \(BUI\) \[660\]](#). Si acepta el certificado, este se agregará a la lista de confianza del origen y se creará el destino. Si rechaza el certificado, este no se agregará a la lista de confianza del origen y no se creará el destino.

Si el certificado ya es de confianza, se creará el destino y no se le solicitará que acepte el certificado.

Temas relacionados

- [Prueba de la conexión \(BUI\) \[660\]](#)
- [Edición de un destino de replicación \(BUI\) \[663\]](#)

- [“Destinos de replicación” \[711\]](#)
- [Flujo de trabajo de replicación remota \[623\]](#)
- [“Conceptos de replicación remota” \[708\]](#)
- [“Copia de seguridad, replicación y restauración de proyectos y recursos compartidos cifrados” \[838\]](#)

▼ Creación de un destino de replicación (CLI)

Un destino de replicación establece una conexión de comunicación segura entre los dispositivos de origen y destino.

Antes de empezar Consulte [Comprobación de la compatibilidad de origen y destino \[625\]](#) para comprobar que el destino de replicación sea compatible con el origen.

Si necesita comprobar que el tráfico de replicación se transmite a través de una interfaz de red específica, configure una ruta estática para el destino que especifique esa interfaz como se muestra en [Configuración de interfaces de red y enrutamiento estático \(CLI\) \[628\]](#).

1. En el dispositivo de origen, vaya a `configuration services replication targets`.

2. Introduzca el comando `target`.

```
host_source:> configuration services replication targets> target
host_source:configuration services replication target (uncommitted)>
```

3. Configure las propiedades de destino.

- `hostname` (Nombre de host): el nombre de dominio completo o la dirección IPv4 del dispositivo de destino. El valor recomendado para usar es el nombre de dominio completo de destino. Consulte la descripción de la propiedad `host_match` a continuación.
- `root_password`: la contraseña de usuario root del dispositivo de destino para autorizar la conexión.
- `label`: el nombre del destino que se debe mostrar en la BUI y la CLI del dispositivo de origen.
- `host_match`: cuando el valor de esta propiedad es `true`, el sistema verifica que el nombre de host de destino especificado en la propiedad `hostname` coincida con el host especificado en el certificado. Por ejemplo, si el nombre común de asunto del certificado solo contiene un nombre de dominio y se especifica una dirección IP para `hostname`, se produce un error en esta comprobación de nombre de host. Si se produce un error en la comprobación de nombre de host, no se ejecuta la comprobación de confianza del certificado descrita en el siguiente paso y no se crea el destino.

Si el destino utiliza un certificado basado en ASN, especifique el nombre de dominio completo del destino para el valor de la propiedad `hostname`.

Si se establece `host_match` en `false`, no se ejecuta la validación de nombre de host.

Para mayor seguridad, establezca el valor de la propiedad `hostname` como el nombre de dominio completo de destino y asegúrese de que la propiedad `host_match` está establecida en `host_match`.

```
hostname:configuration services replication target (uncommitted)> set hostname=hostname
hostname:configuration services replication target (uncommitted)> set root_password=pw
hostname:configuration services replication target (uncommitted)> set label=repl_1
hostname:configuration services replication target (uncommitted)> set host_match=true
```

4. Confirme los cambios.

La comprobación de confianza del certificado se ejecuta para verificar si el certificado es de confianza.

Si el certificado no es de confianza para el origen, se presentará el certificado para que usted lo revise y se le solicitará aceptar o rechazar el certificado como se describe en [Prueba de la conexión \(CLI\) \[661\]](#). Si acepta el certificado, este se agregará a la lista de confianza del origen y se creará el destino. Si rechaza el certificado, este no se agregará a la lista de confianza del origen y no se creará el destino.

Si el certificado ya es de confianza, se creará el destino y no se le solicitará que acepte el certificado.

Temas relacionados

- [Prueba de la conexión \(CLI\) \[661\]](#)
- [Edición de un destino de replicación \(CLI\) \[664\]](#)
- [“Destinos de replicación” \[711\]](#)
- [Flujo de trabajo de replicación remota \[623\]](#)
- [“Conceptos de replicación remota” \[708\]](#)
- [“Copia de seguridad, replicación y restauración de proyectos y recursos compartidos cifrados” \[838\]](#)

▼ Creación de una acción de replicación (BUI)

Una acción de replicación describe el proyecto o el recurso compartido que se replica, la ubicación a la que se debe enviar la replicación, el programa de replicación y las propiedades de la transferencia de datos; por ejemplo, si está activado o desactivado el cifrado del enlace de red.



Atención - No cree más de tres acciones por proyecto. Lo típico es una acción por proyecto.

Si está configurando la replicación remota por primera vez, puede ser útil replicar una cantidad mínima de datos para garantizar que la sincronización se complete correctamente. Puede replicar un proyecto vacío o elegir no replicar las instantáneas que se encuentren en los proyectos o los recursos compartidos.

Si está replicando un juego de datos grande y el ancho de banda es limitado debido a la distancia entre los dispositivos de origen y destino, puede exportar la replicación a medios fuera de línea, como se describe en [“Configuración de replicación fuera de línea \(BUI\)” \[643\]](#).

1. **Desde la BUI del dispositivo de origen, vaya a Recursos compartidos > Proyectos.**
2. **Seleccione el proyecto o el recurso compartido y haga clic en el separador Replicación.**
3. **Haga clic en el ícono de agregación , junto a Acciones.**

4. Seleccione un destino y una agrupación.

Add Replication Action
CANCEL ADD

Properties

Target ar7320-230

Pool Storage_Pool_230

Export data path ☐ nfs://

Limit bandwidth ☐ 0 M/s

Enable SSL-encryption ☒

Disable compression ☐

Enable deduplication ☐

Include snapshots ☒

Retain user snapshots on target ☐

Include clone origin as data ☐

Recovery point objective ☐ hours

Replica lag warning alert ☐ % of Recovery Point Objective

Replica lag error alert ☐ % of Recovery Point Objective

Update frequency ☒ Scheduled ☐ Continuous

⊕ Schedule
⋮ Snapshots

No schedule entries are configured for this action.

5. Seleccione las propiedades para esta acción.

Consulte la descripción de todas las propiedades en [“Propiedades de las acciones de replicación” \[716\]](#).

6. **Seleccione Programada y establezca la frecuencia para la actualización de replicación, o seleccione Continua para enviar actualizaciones de replicación de manera continua.**

Every 5 Minutes
Every 10 Minutes
Every 15 Minutes
Every 20 Minutes
Every Half Hour
Every Hour
Every 2 Hours
Every 4 Hours
Every 8 Hours
Every 12 Hours
Every Day
Every Week
Every Month
Auto-snapshots
Every Half Hour

Include snapshots ☒
Maintain user snapshots on target ☐
Include clone origin as data ☐
Recovery point objective hours
Replica lag warning alert % of Recovery F
Replica lag error alert % of Recovery F
Update frequency ☒ Scheduled ☐ Continu

snapshots

scheduled time: Auto minutes past the hour

7. **Haga clic en Agregar.**

La acción de replicación se agrega a la lista Acciones.

+ Actions		
TARGET ▲	UPDATES	STATUS
sashimi Manual	Never Synced Never Attempted	Sync now
sushi Scheduled	2015-7-1 19:52:03 Synced 2015-7-1 19:52:03 Attempted	2015-7-1 20:05:00 Next

Temas relacionados

- [“Propiedades de las acciones de replicación” \[716\]](#)
- [“Acciones y paquetes de replicación” \[714\]](#)
- [Envío manual de una actualización de replicación \(BUI\) \[641\]](#)

▼ Creación de una acción de replicación (CLI)

Una acción de replicación describe el proyecto o el recurso compartido que se replica, el destino de replicación, el programa de replicación y las propiedades de la transferencia de datos; por ejemplo, si está activado o desactivado el cifrado del enlace de red.



Atención - No cree más de tres acciones por proyecto. Lo típico es una acción por proyecto.

Si está configurando la replicación remota por primera vez, puede ser útil replicar una cantidad mínima de datos para garantizar que la sincronización se complete correctamente. Puede replicar un proyecto vacío o elegir no replicar las instantáneas que se encuentren en los proyectos o los recursos compartidos.

Si está replicando un juego de datos grande y el ancho de banda es limitado debido a la distancia entre los dispositivos de origen y destino, puede exportar la replicación a medios fuera de línea, como se describe en [“Configuración de replicación fuera de línea \(CLI\)” \[648\]](#).

1. Navegue hasta el proyecto o el recurso compartido e introduzca `action`:

```
host_source:shares PROJECT1/SHARE1 replication> action
```

2. Visualice las propiedades.

```
host_source:shares PROJECT1/SHARE1 action (uncommitted)> get
Properties:
    target = (unset)
    pool = (unset)
    enabled = true
    continuous = false
    include_snaps = true
    max_bandwidth = unlimited
    use_ssl = true
```

3. Establezca las propiedades para esta acción.

Consulte la descripción de las propiedades de la CLI en [“Propiedades de las acciones de replicación” \[716\]](#).

```
host_source:shares PROJECT1/SHARE1 action (uncommitted)> set target=repl_sys
    target = repl_sys (uncommitted)
host_source:shares PROJECT1/SHARE1 action (uncommitted)> set pool=pool-0
    pool = pool-0 (uncommitted)
host_source:shares PROJECT1/SHARE1 action (uncommitted)> set include_snaps=false
    include_snaps = false (uncommitted)
host_source:shares PROJECT1/SHARE1 action (uncommitted)> set use_ssl=false
    use_ssl = false (uncommitted)
host_source:shares PROJECT1/SHARE1 action-000> schedule
host_source:shares PROJECT1/SHARE1 action-000 schedule (uncommitted)> set frequency=day
    frequency = day (uncommitted)
host_source:shares PROJECT1/SHARE1 action-000 schedule (uncommitted)> set hour=23
```



```

                                hour = 23 (uncommitted)
host_source:shares PROJECT1/SHARE1 action-000 schedule (uncommitted)> set minute=05
                                minute = 05 (uncommitted)

```

4. Confirme la nueva acción de replicación.

```
host_source:shares PROJECT1/SHARE1 action (uncommitted)> commit
```

5. Para ver las propiedades de la nueva acción, introduzca `ls`:

```

host_source:shares PROJECT1/SHARE1 replication> ls
Properties:
    inherited = false
Actions:
  TARGET      STATUS      NEXT
  action-000  repl_sys    idle       manual

host_source:shares PROJECT1/SHARE1 action-000> ls
Properties:
    id = a751dc0f-abcd-1234-6789-f5e8315eaffa
    target = repl_sys
    enabled = true
    continuous = false
    include_snaps = false
    max_bandwidth = unlimited
    use_ssl = false
    compression = on
    export_path =
    state = idle
    state_description = Idle (no update pending)
    export_pending = false
    offline = false
    next_update = Wed Sep 04 2019 23:05:00 GMT+0000 (UTC)
    last_sync = Wed Sep 04 2019 10:24:05 GMT+0000 (UTC)
    last_try = Wed Sep 04 2019 10:24:05 GMT+0000 (UTC)
    last_result = success

```

6. Para ver el ID de la nueva acción, use el comando `last`, que lo lleva hasta el nodo en donde se encuentra la nueva acción, combinado con `get id`, que recupera el ID de la acción.

El identificador se usa más adelante para seleccionar el nodo de acción de replicación correcto.

```

host_source:shares PROJECT1/SHARE1 replication>last get id
                                id =
                                fb1bb3fd-3361-42e1-e4a1-b06c426172fb

```

Temas relacionados

- [Edición de un destino de replicación \(CLI\) \[664\]](#)
- [“Propiedades de las acciones de replicación” \[716\]](#)
- [“Acciones y paquetes de replicación” \[714\]](#)

▼ Configuración de retención de instantáneas automáticas en un destino (BUI)

Use este procedimiento para establecer un número diferente de instantáneas automáticas retenidas en el destino de replicación que el establecido en el dispositivo de origen. Antes de realizar este procedimiento, debe establecer una acción de replicación en un proyecto o recurso compartido, y programar instantáneas automáticas.

Cuando realice esta tarea, modifique la acción de replicación y el programa de instantáneas desde el proyecto o recurso compartido apropiado. Si la acción de replicación y el programa de instantáneas están configurados en niveles diferentes, edite la acción de replicación en el mismo nivel donde esté configurado el programa, como se muestra en la siguiente tabla:

Acción	Planificación de instantánea	Modificar retención de instantánea automática en:
Nivel de proyecto	Nivel de proyecto	Acción configurada en el nivel de proyecto.
Nivel de recurso compartido	Nivel de recurso compartido	Acción configurada en el nivel de recurso compartido.
Nivel de proyecto	Nivel de recurso compartido	Acción visible en el nivel de recurso compartido. (Acción de nivel de proyecto heredada por recurso compartido).
Nivel de recurso compartido	Nivel de proyecto	Acción configurada en el nivel de recurso compartido.

Consulte [“Gestión de instantáneas automáticas de replicación” \[740\]](#) para obtener más información.

Antes de empezar Antes de configurar la retención de instantáneas automáticas en un destino, debe hacer lo siguiente:

- Crear una acción de replicación en un proyecto o recurso compartido: [Creación de una acción de replicación \(BUI\) \[632\]](#).
- Crear un programa de instantáneas automáticas para el proyecto o recurso compartido: [Programación de instantáneas \(BUI\) \[594\]](#).

1. **En el dispositivo de origen, vaya a Recursos compartidos > Proyectos.**
2. **Seleccione el proyecto o recurso compartido apropiado con la acción de replicación y el programa de instantáneas, y haga clic en el separador Replicación.**
3. **Haga clic en el ícono de editar  de la acción que desea modificar.**

4. **En la parte inferior de la ventana Editar acción de replicación, haga clic en el separador Instantáneas.**

Aparecen los programas de instantáneas automáticas.

5. **En el campo Mantener al máximo, cambie el valor para especificar el número de instantáneas automáticas que se retendrá en el destino.**
6. **Haga clic en la opción para aplicar.**

Nota - La retención de instantáneas automáticas tiene un procesamiento especial durante la replicación inversa. Para obtener más información, consulte [“Gestión de instantáneas de replicación” \[738\]](#).

▼ Configuración de retención de instantáneas automáticas en un destino (CLI)

Use este procedimiento para establecer un número diferente de instantáneas automáticas retenidas en el destino de replicación que el establecido en el dispositivo de origen. Antes de realizar este procedimiento, debe establecer una acción de replicación en un proyecto o recurso compartido, y programar instantáneas automáticas.

Cuando realice esta tarea, modifique la acción de replicación y el programa de instantáneas desde el proyecto o recurso compartido apropiado. Si la acción de replicación y el programa de instantáneas están configurados en niveles diferentes, edite la acción de replicación en el mismo nivel donde esté configurado el programa, como se muestra en la siguiente tabla:

Acción	Planificación de instantánea	Modificar retención de instantánea automática en:
Nivel de proyecto	Nivel de proyecto	Acción configurada en el nivel de proyecto.
Nivel de recurso compartido	Nivel de recurso compartido	Acción configurada en el nivel de recurso compartido.
Nivel de proyecto	Nivel de recurso compartido	Acción visible en el nivel de recurso compartido. (Acción de nivel de proyecto heredada por recurso compartido).
Nivel de recurso compartido	Nivel de proyecto	Acción configurada en el nivel de recurso compartido.

Consulte [“Gestión de instantáneas automáticas de replicación” \[740\]](#) para obtener más información.

Antes de empezar Antes de configurar la retención de instantáneas automáticas en un destino, debe hacer lo siguiente:

- Crear una acción de replicación en un proyecto o recurso compartido: [Creación de una acción de replicación \(BUI\) \[632\]](#).
- Crear un programa de instantáneas automáticas para el proyecto o recurso compartido: [Programación de instantáneas \(BUI\) \[594\]](#).

1. **En el dispositivo de origen, vaya a shares y seleccione el proyecto o recurso compartido apropiado con la acción de replicación y el programa de instantáneas.**

```
hostname:> shares select MyProject
hostname:shares MyProject> select MyShare
hostname:shares MyProject/MyShare>
```

2. **Introduzca replication y, luego, introduzca show para mostrar las acciones existentes.**

```
hostname:shares MyProject/MyShare> replication
hostname:shares MyProject/MyShare replication> show
Properties:
    inherited = false
```

Actions:

	TARGET	STATUS	NEXT
action-000	local	idle	Thu Jan 03 2019 12:04:00 GMT+0000 (UTC)

3. **Seleccione la acción para la cual desee modificar la configuración de retención.**

```
hostname:shares MyProject/MyShare replication> select action-000
hostname:shares MyProject/MyShare action-000>
```

4. **Introduzca autosnaps y, a continuación, show para mostrar los programas de instantánea.**

```
hostname:shares MyProject/MyShare action-000> autosnaps
hostname:shares MyProject/MyShare action-000 autosnaps> show
Properties:
    autosnaps_retention_policies = independent
```

Automatics:

NAME	FREQUENCY	DAY	HH:MM	KEEP
automatic-000	hour	-	-:04	3

5. **Seleccione el programa de instantáneas automatic que desea modificar. A continuación, use set keep= para establecer el número de instantáneas automáticas que se retendrán en el destino.**

```
hostname:shares MyProject/MyShare action-000 autosnaps> select automatic-000
hostname:shares MyProject/MyShare action-000 automatic-000> set keep=10
```

```
keep = 10 (uncommitted)
```

6. **Introduzca `commit` para guardar los cambios y `show` para comprobar que la propiedad `keep` haya cambiado.**

```
hostname:shares MyProject/MyShare action-000 automatic-000> commit
hostname:shares MyProject/MyShare action-000 automatic-000> show
Properties:
    frequency = hour
    day =
    hour =
    minute = 04
    keep = 10
```

Nota - La retención de instantáneas automáticas tiene un procesamiento especial durante la replicación inversa. Para obtener más información, consulte [“Gestión de instantáneas de replicación” \[738\]](#).

▼ Envío manual de una actualización de replicación (BUI)

Si ya se configuró la replicación continua o programada, las actualizaciones de la replicación se realizan de manera automática. También puede realizar una actualización manual mediante la BUI.

1. **Desde el dispositivo de origen, vaya a Recursos compartidos > Proyectos.**
2. **Abra un proyecto y haga clic en el separador Replicación.**
3. **Haga clic en el ícono para sincronizar ahora  ..**

Nota - Esta acción no está disponible (o no funcionará) si se está enviando una actualización de manera activa. Asegúrese de tener espacio en disco suficiente en el destino para replicar todo el proyecto antes de enviar una actualización.

La BUI muestra una barra de progreso e indica cuándo finaliza la actualización.

4. **Si la actualización de la replicación no se realiza correctamente, elimine las acciones o las instantáneas anteriores que haya y vuelva a comenzar.**

Temas relacionados

- [Creación de una acción de replicación \(BUI\) \[632\]](#)

- [Cancelación de una actualización de replicación \(BUI\) \[677\]](#)

▼ Envío manual de una actualización de replicación (CLI)

Si ya se configuró la replicación continua o programada, las actualizaciones de la replicación se realizan de manera automática. También puede realizar una actualización manual mediante la CLI.

1. **Navegue hasta el recurso compartido e introduzca el comando `sendupdate`:**

```
host_source:shares PROJECT1/SHARE1 action-000> sendupdate
```

Cuando la actualización está activa, la CLI muestra el estado `sending`.

2. **Si la replicación no se realiza correctamente, elimine las acciones o las instantáneas anteriores que haya y vuelva a comenzar.**

Temas relacionados

- [Creación de una acción de replicación \(CLI\) \[636\]](#)
- [Cancelación de una actualización de replicación \(CLI\) \[678\]](#)

▼ Configuración de replicación para una configuración en cluster

En esta tarea se describe cómo configurar la replicación en un entorno en cluster. Siga estos pasos para configurar la replicación de manera adecuada para garantizar que los proyectos se sigan replicando después de una toma de control del cluster, un failback en el cluster o después de realizar una replicación inversa en un dispositivo de destino.

Antes de empezar Si es la primera vez que está configurando una replicación para dispositivos en cluster, revise [“Ejemplo: Configuración de replicación para dispositivos agrupados en clusters” \[730\]](#).

1. **En los dispositivos de origen y destino de replicación, seleccione las interfaces de red y direcciones IP que se usarán para el tráfico de replicación utilizando estas directrices:**

- a. **Siempre seleccione una interfaz de red única para garantizar que el nodo par tome el control de esta después de una operación de toma de control o failback del cluster.**
 - b. **En el sistema de origen, asegúrese de que la interfaz de red seleccionada y la agrupación de almacenamiento, desde las cuales se replicarán los datos, estén asignadas al mismo nodo. Esto sucede siempre cuando el cluster de origen se encuentra en estado CLUSTERED (En cluster).**
 - c. **En el sistema de destino, asigne la interfaz de red seleccionada en el dispositivo de destino y la agrupación de almacenamiento, en donde se colocarán los datos replicados, al mismo nodo. Esto mantiene la asociación cuando la configuración de replicación se lleva a cabo mientras el cluster de destino está en el estado CLUSTERED (En cluster).**
 - d. **Asegúrese de que los sistemas de origen y destino se puedan comunicar utilizando las interfaces de red y las direcciones IP seleccionadas.**
2. **En los dispositivos de origen y destino, cree rutas de red (basadas en host) estáticas /32 utilizando las interfaces de red y las direcciones IP seleccionadas.**
 3. **En el dispositivo de origen, configure el objeto de destino de replicación utilizando la dirección IP seleccionada del destino.**

Configuración de replicación fuera de línea (BUI)

Use los siguientes pasos para configurar la replicación fuera de línea:

- [Configuración de un servidor NFS para la replicación fuera de línea \[644\]](#)
- [Configuración de una ruta de exportación para el servidor NFS \(BUI\) \[644\]](#)
- [Exportación de una actualización de replicación \(BUI\) \[645\]](#)
- [Verificación del flujo de replicación en el servidor NFS \[645\]](#)
- [Importación del flujo de replicación desde el servidor NFS \(BUI\) \[646\]](#)
- [Ejecución de una actualización de red manual \(BUI\) \[646\]](#)
- [Reversión de una replicación fuera de línea \(BUI\) \[647\]](#)

▼ Configuración de un servidor NFS para la replicación fuera de línea

Los pasos para configurar un servidor NFS varían en función del tipo de servidor NFS que se use. Consulte la documentación del servidor NFS para obtener instrucciones específicas.

1. **Identifique un servidor que esté listo para conectarse a la red y tenga activados los servicios NFS.**
2. **Como usuario root del servidor NFS, cree un sistema de archivos o un recurso compartido.**
3. **Configure los permisos de archivo para exponer el recurso compartido NFS solo a la dirección IP de los dispositivos de origen y destino.**
4. **Para cifrar el flujo de replicación, active el cifrado en disco para el recurso compartido de NFS en el servidor NFS.**

Nota - Un flujo de replicación exportado nunca es cifrado por el dispositivo.

5. **Exporte el recurso compartido para que el cliente NFS tenga acceso a él.**
6. **Compruebe que el sistema de archivos esté compartido.**

Pasos siguientes

- [Configuración de una ruta de exportación para el servidor NFS \(BUI\) \[644\]](#)

▼ Configuración de una ruta de exportación para el servidor NFS (BUI)

Antes de empezar Identifique o cree un destino. Consulte [Creación de un destino de replicación \(BUI\) \[629\]](#).

1. **Desde la BUI del dispositivo de origen, vaya a Recursos compartidos > Proyectos.**
2. **Abra el proyecto y haga clic en el separador Replicación.**
3. **Haga clic en el ícono de agregación  que se encuentra junto a Acciones.**
4. **En la pantalla Agregar acción de replicación, seleccione una de datos de exportación e introduzca la ruta del recurso compartido NFS con el formato: `nfs://server/path`.**

5. **Seleccione propiedades adicionales para esta acción y, a continuación, haga clic en Agregar.**

Nota - Si configura un programa o selecciona el modo de replicación continua, la actualización se realiza automáticamente después de que hayan finalizado las operaciones de exportación e importación.

Pasos siguientes

- [Exportación de una actualización de replicación \(BUI\) \[645\]](#)

▼ Exportación de una actualización de replicación (BUI)

1. Desde el dispositivo de origen, vaya a **Recursos compartidos > Proyectos**.
2. Abra el proyecto y haga clic en el separador **Replicación**.
3. Haga clic en el ícono de exportación de datos de replicación .
4. Compruebe el estado de la replicación y espere hasta que la replicación finalice.

Pasos siguientes

- [Verificación del flujo de replicación en el servidor NFS \[645\]](#)

▼ Verificación del flujo de replicación en el servidor NFS

1. Navegue hasta el directorio NFS, compruebe el MD5 y vea los metadatos.

```
bigfish25# pwd
/export/init_repl/rr_updates/96366bf2-0b3c-4eec-e85b-e36e1b5bc18c
bigfish25# ls -l
total 67
-rw-r--r--  1 nobody  nobody      633 Nov 17 21:46 metadata.xml
-rw-----  1 nobody  nobody    31016 Nov 17 21:46 stream
-rw-----  1 nobody  nobody      33 Nov 17 21:46 stream.md5
bigfish25# md5sum stream
25b4671c9aaf34455a63e203bcecff49  stream
bigfish25# cat stream.md5
25b4671c9aaf34455a63e203bcecff49
bigfish25# cat metadata.xml
<?xml version="1.0"?>
<!DOCTYPE nvlist SYSTEM "/usr/share/lib/xml/dtd/nvlist.dtd.1">
<nvlist>
  <nvpair name='offline_rr_version'><string value='1.1'/></nvpair>
  <nvpair name='source_asn'><string value='2ea4670f-bc17-cf8f-a420-9211d6edda04'/></
nvpair>
```

```
<nvpair name='project'><string value='default' /></nvpair>
<nvpair name='pkgid'><string value='96366bf2-0b3c-4eec-e85b-e36e1b5bc18c' /></nvpair>
<nvpair name='basesnap'><string value='/'></nvpair>
<nvpair name='newsnap'><string value='.rr-96366bf2-0b3c-4eec-e85b-e36e1b5bc18c-1' /></
nvpair>
<nvpair name='compression'><string value='on' /></nvpair>
</nvlist>
bigfish25#
```

2. **Mueva físicamente el servidor NFS a la ubicación del dispositivo de destino o copie la carpeta `rr_updates` en un medio externo y prepárelo para el envío.**

Pasos siguientes

- [Importación del flujo de replicación desde el servidor NFS \(BUI\) \[646\]](#)

▼ Importación del flujo de replicación desde el servidor NFS (BUI)

1. **Vaya a Recursos compartidos > Proyectos > Replicas Réplicas.**
2. **Seleccione la réplica que indique `awaiting import` (importación está pendiente) para el origen.**
3. **Haga clic en el separador Replicación.**
4. **En el campo Ruta de datos de importación, introduzca la ruta de la réplica.**
- 5.

Haga clic en el ícono de importación de actualización desde medio externo para iniciar la importación. 

Pasos siguientes

Después de haber importado el flujo de replicación en el dispositivo de destino, continúe con una de las siguientes opciones:

- [Ejecución de una actualización de red manual \(BUI\) \[646\]](#)
- [Reversión de una replicación fuera de línea \(BUI\) \[647\]](#)

▼ Ejecución de una actualización de red manual (BUI)

Después de importar el flujo de replicación fuera de línea en el dispositivo de destino, confirme que las actualizaciones de red futuras funcionarán correctamente. Si ya se configuró la

replicación continua o programada, la actualización se realiza de manera automática. De lo contrario, realice una actualización manual.

1. **Vaya al dispositivo de origen.**
2. Consulte [Envío manual de una actualización de replicación \(BUI\) \[641\]](#).

▼ Reversión de una replicación fuera de línea (BUI)

Siga este procedimiento para mover un paquete de replicación fuera de línea a un proyecto local nuevo, configurado para volver a replicarse en un dispositivo de origen.

1. **Importe el paquete de replicación fuera de línea de un servidor NFS a un dispositivo de destino, según se describe en [Importación del flujo de replicación desde el servidor NFS \(BUI\) \[646\]](#).**
2. **En el dispositivo de destino, vaya a Recursos compartidos > Proyectos > Réplica y localice el paquete replicado.**
El proyecto se llama *target_appliance: new_project/share*.
3. **Seleccione el proyecto y haga clic en el ícono de reversión de dirección de replicación correspondiente .**
4. **En la ventana Replicación inversa, introduzca un nombre para el nuevo proyecto local.**
Esta acción permite mover el contenido de este paquete a un proyecto local nuevo configurado para replicarse nuevamente en el origen. Cualquier cambio realizado en los datos o los metadatos del origen a partir de la última actualización correcta se pierde cuando el proyecto nuevo se replica de nuevo en el origen. Si las acciones de replicación en el origen no están desactivadas, se producirán errores en las actualizaciones futuras de este paquete.
5. **Vaya a Recursos compartidos > Proyectos.**
6. **Abra el proyecto y haga clic en el separador Replication (Replicación).**
7. **Haga clic en el ícono de exportación de datos de replicación .**
8. **Compruebe el estado de la replicación y espere hasta que la replicación finalice.**
9. **Cuando la actualización de la replicación haya finalizado, navegue hasta el paquete recién revertido en el nuevo destino.**
La descripción del estado debe ser Idle (awaiting import).

10. Importe la actualización desde el servidor NFS.

Temas relacionados

- [“Configuración de replicación fuera de línea \(BUI\)” \[643\]](#)

Configuración de replicación fuera de línea (CLI)

Use los siguientes pasos para configurar la replicación fuera de línea:

- [Configuración de un servidor NFS para la replicación fuera de línea \[648\]](#)
- [Configuración de una ruta de exportación para el servidor NFS \(CLI\) \[649\]](#)
- [Exportación de una actualización de replicación \(CLI\) \[650\]](#)
- [Verificación de un flujo de replicación en el servidor NFS \[651\]](#)
- [Importación de un flujo de replicación desde el servidor NFS \(CLI\) \[652\]](#)
- [Ejecución de una actualización de red manual \(CLI\) \[653\]](#)
- [Reversión de una replicación fuera de línea \(CLI\) \[654\]](#)

▼ Configuración de un servidor NFS para la replicación fuera de línea

Los pasos para configurar un servidor NFS varían en función del tipo de servidor NFS que se use. Consulte la documentación del servidor NFS para obtener instrucciones específicas.

1. **Identifique un servidor que esté listo para conectarse a la red y tenga activados los servicios NFS.**
2. **Como usuario root del servidor NFS, cree un sistema de archivos o un recurso compartido.**
3. **Configure los permisos de archivo para exponer el recurso compartido NFS solo a la dirección IP de los dispositivos de origen y destino.**
4. **Para cifrar el flujo de replicación, active el cifrado en disco para el recurso compartido de NFS en el servidor NFS.**

Nota - Un flujo de replicación exportado nunca es cifrado por el dispositivo.

5. **Exporte el recurso compartido para que el cliente NFS tenga acceso a él.**

6. Compruebe que el sistema de archivos esté compartido.

Pasos siguientes

- [Configuración de una ruta de exportación para el servidor NFS \(CLI\) \[649\]](#)

▼ Configuración de una ruta de exportación para el servidor NFS (CLI)

1. Identifique o cree un destino de replicación.
2. Cree una acción de replicación, establezca la propiedad `export_path` y ejecute `commit` para la nueva acción.

```
source:shares default replication> action
source:shares default action (uncommitted)> set target=target_a
target = target_a (uncommitted)
source:shares default action (uncommitted)> set pool=pool2
pool = pool2 (uncommitted)
source:shares default action (uncommitted)> set export_path=nfs://nfs_server/export/init_repl
export_path = nfs://nfs_server/export/init_repl (uncommitted)
source:shares default action (uncommitted)>commit
```

Nota - De manera opcional, puede establecer un modo de replicación programada o continua, lo que hará que la actualización se inicie después de que hayan finalizado las operaciones de exportación e importación.

3. Navegue hasta la acción de replicación que acaba de crear y vea el estado actual.

```
source:shares default replication> ls
Actions:
      TARGET      STATUS      NEXT
action-000 target_a      idle      Export replication data

source:shares default replication> last
source:shares default action-000> ls
Properties:
      id = 96366bf2-0b3c-4eec-e85b-e36e1b5bc18c
      target = target_a
      enabled = true
      continuous = false
      include_snaps = true
      max_bandwidth = unlimited
      bytes_sent = 0
      estimated_size = 0
      estimated_time_left = 00:00:00
      average_throughput = 0B/s
      use_ssl = true
      compression = on
```

```
export_path = nfs://nfs_server/export/init_repl
state = idle
state_description = Idle (export pending)
export_pending = true
offline = false
next_update = Export replication data
last_sync = <unknown>
last_try = <unknown>
last_result = <unknown>
```

Pasos siguientes

- [Exportación de una actualización de replicación \(CLI\) \[650\]](#)

▼ Exportación de una actualización de replicación (CLI)

1. **Para exportar la actualización de replicación al servidor NFS, use el comando `sendupdate`.**

```
source:shares default action-000>sendupdate
```

2. **Introduzca `ls` para ver el estado, como se muestra en este ejemplo:**

```
source:shares default action-000> ls
Properties:
    id = 96366bf2-0b3c-4eec-e85b-e36e1b5bc18c
    target = target_a
    enabled = true
    continuous = false
    include_snaps = true
    max_bandwidth = unlimited
    bytes_sent = 0
    estimated_size = 0
    estimated_time_left = 00:00:00
    average_throughput = 0B/s
    use_ssl = true
    compression = on
    export_path = nfs://nfs_server/export/init_repl
    state = sending
    state_description = Exporting update
    export_pending = true
    offline = false
    next_update = Export replication data
    last_sync = <unknown>
    last_try = <unknown>
    last_result = <unknown>
```

3. **Para determinar si la exportación ya finalizó, introduzca `ls` para ver el estado.**

Busque `last_result=success`, como se muestra en este ejemplo:

```
source:shares default action-000> ls
Properties:
    id = 96366bf2-0b3c-4eec-e85b-e36e1b5bc18c
    target = target_a
    enabled = true
```

```

        continuous = false
        include_snaps = true
        max_bandwidth = unlimited
        bytes_sent = 0
        estimated_size = 0
        estimated_time_left = 00:00:00
        average_throughput = 0B/s
        use_ssl = true
        compression = on
        export_path =
        state = idle
        state_description = Idle (no update in progress)
        export_pending = false
        offline = true
        next_update = Sync now
        last_sync = <unknown>
        last_try = Mon Nov 18 2019 04:40:40 GMT+0000 (UTC)
        last_result = success
source:shares default action-000>

```

Pasos siguientes

- [Verificación de un flujo de replicación en el servidor NFS \[651\]](#)

▼ Verificación de un flujo de replicación en el servidor NFS

1. Navegue hasta el directorio NFS, compruebe el MD5 y vea los metadatos.

```

nfs_server# pwd
/export/init_repl/rr_updates/96366bf2-0b3c-4eec-e85b-e36e1b5bc18c
nfs_server# ls -l
total 67
-rw-r--r-- 1 nobody nobody 633 Nov 17 21:46 metadata.xml
-rw----- 1 nobody nobody 31016 Nov 17 21:46 stream
-rw----- 1 nobody nobody 33 Nov 17 21:46 stream.md5
nfs_server# md5sum stream
25b4671c9aaf34455a63e203bcecff49 stream
nfs_server# cat stream.md5
25b4671c9aaf34455a63e203bcecff49
nfs_server# cat metadata.xml
<?xml version="1.0"?>
<!DOCTYPE nvlist SYSTEM "/usr/share/lib/xml/dtd/nvlist.dtd.1">
<nvlist>
  <nvpair name='offline_rr_version'><string value='1.1'></nvpair>
  <nvpair name='source_asn'><string value='2ea4670f-bc17-cf8f-a420-9211d6edda04'></nvpair>
  <nvpair>
    <nvpair name='project'><string value='default'></nvpair>
    <nvpair name='pkgid'><string value='96366bf2-0b3c-4eec-e85b-e36e1b5bc18c'></nvpair>
    <nvpair name='basesnap'><string value='/'></nvpair>
    <nvpair name='newsnap'><string value='.rr-96366bf2-0b3c-4eec-e85b-e36e1b5bc18c-1'></nvpair>
  </nvpair>
  <nvpair name='compression'><string value='on'></nvpair>
</nvlist>
nfs_server#

```

2. Mueva físicamente el servidor NFS a la ubicación del dispositivo de destino o copie la carpeta `rr_updates` en un medio externo y prepárelo para el envío.

Pasos siguientes

- [Importación de un flujo de replicación desde el servidor NFS \(CLI\) \[652\]](#)

▼ Importación de un flujo de replicación desde el servidor NFS (CLI)

1. **Para importar el flujo de replicación desde un servidor NFS, navegue hasta `shares replication packages` en el destino y, luego, introduzca `ls` para mostrar los paquetes.**

```
target_a:> shares replication packages
target_a:shares replication packages> ls
Packages:

ID          STATE DATA_TIMESTAMP      SOURCE      DATASET
package-000 idle   unknown              sourceA     <unknown>
```

2. **Seleccione los paquetes que desea importar.**

Para ver las propiedades, introduzca `ls`.

```
target_a:shares replication packages> select package-000
target_a:shares replication package-000> ls
Properties:

            id = 96366bf2-0b3c-4eec-e85b-e36e1b5bc18c
source_name = sourceA
source_asn  = d1fce51d-b8a9-6cf8-d71e-fcd4fe42cd0e
source_ip   = 10.000.000.000:216
target_pool = poolA
replica_of  = <unknown>
enabled     = true
state       = idle
state_description = Idle (no update in progress)
offline     = false
import_path =
data_timestamp = unknown
last_sync    = unknown
last_try     = unknown
last_result  = unknown
```

3. **Establezca la ruta de importación de los datos replicados y, a continuación, introduzca `commit`.**

```
target_a:shares replication package-000> set import_path=
nfs://nfs_server/export/init_repl
import_path = nfs://nfs_server/export/init_repl (uncommitted)
target_a:shares replication package-000> commit
target_a:shares replication package-000> ls
Properties:

            id = 96366bf2-0b3c-4eec-e85b-e36e1b5bc18c
source_name = sourceA
```



```

source_asn = d1fce51d-b8a9-6cf8-d71e-fcd4fe42cd0e
source_ip = 10.000.000.000:216
target_pool = poolA
replica_of = <unknown>
  enabled = true
  state = receiving
state_description = Importing update
  offline = true
import_path = nfs://nfs_server/export/init_repl
data_timestamp = unknown
  last_sync = unknown
  last_try = unknown
  last_result = unknown

```

Pasos siguientes

Después de haber importado el flujo de replicación en el dispositivo de destino, continúe con una de las siguientes opciones:

- [Ejecución de una actualización de red manual \(CLI\) \[653\]](#)
- [Reversión de una replicación fuera de línea \(CLI\) \[654\]](#)

▼ Ejecución de una actualización de red manual (CLI)

Después de importar el flujo de replicación fuera de línea en el dispositivo de destino, confirme que las actualizaciones de red futuras funcionarán correctamente. Si ya se configuró la replicación continua o programada, la actualización se realiza de manera automática. De lo contrario, realice una actualización manual, como se muestra en el siguiente ejemplo.

1. Vaya al dispositivo de origen y navegue hasta el recurso compartido.

```

source:shares default action-000> ls
Properties:
      id = 96366bf2-0b3c-4eec-e85b-e36e1b5bc18c
      target = target_a
      enabled = true
      continuous = false
      include_snaps = true
      max_bandwidth = unlimited
      bytes_sent = 0
      estimated_size = 0
      estimated_time_left = 00:00:00
      average_throughput = 0B/s
      use_ssl = true
      compression = on
      export_path =
      state = idle
      state_description = Idle (no update in progress)
      export_pending = false
      offline = true
      next_update = Sync now
      last_sync = <unknown>
      last_try = Mon Nov 18 2019 04:40:40 GMT+0000 (UTC)

```

```
last_result = success
```

2. Inicie la actualización con `sendupdate` y, a continuación, consulte el estado con el comando `ls`.

```
source:shares default action-000> sendupdate
source:shares default action-000> ls
Properties:
    id = 96366bf2-0b3c-4eec-e85b-e36e1b5bc18c
    target = target1
    enabled = true
    continuous = false
    include_snaps = true
    max_bandwidth = unlimited
    bytes_sent = 0
    estimated_size = 0
    estimated_time_left = 00:00:00
    average_throughput = 0B/s
    use_ssl = true
    compression = on
    export_path =
    state = sending
    state_description = Ready (awaiting available resources to send update)
    export_pending = false
    offline = true
    next_update = Sync now
    last_sync = <unknown>
    last_try = Mon Nov 18 2019 04:40:40 GMT+0000 (UTC)
    last_result = success

source:shares default action-000> ls
Properties:
    id = 96366bf2-0b3c-4eec-e85b-e36e1b5bc18c
    target = target1
    enabled = true
    continuous = false
    include_snaps = true
    max_bandwidth = unlimited
    bytes_sent = 0
    estimated_size = 0
    estimated_time_left = 00:00:00
    average_throughput = 0B/s
    use_ssl = true
    compression = on
    export_path =
    state = idle
    state_description = Idle (no update in progress)
    export_pending = false
    offline = false
    next_update = Sync now
    last_sync = Mon Nov 18 2019 04:40:40 GMT+0000 (UTC)
    last_try = Mon Nov 18 2019 04:40:40 GMT+0000 (UTC)
    last_result = success
```

▼ Reversión de una replicación fuera de línea (CLI)

Siga este procedimiento para mover un paquete de replicación fuera de línea a un proyecto local nuevo, configurado para volver a replicarse en un dispositivo de origen.

Antes de empezar Importe el flujo de replicación fuera de línea desde un servidor NFS hacia un destino de replicación, como se describe en [Importación de un flujo de replicación desde el servidor NFS \(CLI\)](#) [652].

1. Desde el destino de replicación, navegue al paquete replicado y localice el proyecto:

```
target:> shares replication packages
target: shares replication packages> select package-000
target:shares replication package-000> ls
Properties:

        id = 1c0457eb-45bd-4f91-8e08-bc0dbacd40b7
        source_name = bigfish78
        source_asn = d1fce51d-b8a9-6cf8-d71e-fcd4fe42cd0e
        source_ip = 10.000.000.000:216
        target_pool = poolA
        replica_of = proj1
        enabled = true
        state = idle
        state_description = Idle (no update in progress)
        offline = false
        import_path =
        data_timestamp = Thu Feb 16 2017 19:10:59 GMT+0000 (UTC)
        last_sync = Fri Feb 17 2017 03:10:11 GMT+0000 (UTC)
        last_try = Fri Feb 17 2017 03:10:11 GMT+0000 (UTC)
        last_result = success
```

```
Projects:

        proj1
```

2. Introduzca pkgreverse.

```
target:shares replication package-000> pkgreverse
```

3. (Opcional) Defina un nombre de proyecto nuevo y active la acción con los siguientes comandos:

```
target:shares replication package-000 pkgreverse> set new_project_name=new-kmm3
        new_project_name = new-kmm3
target:shares replication package-000 pkgreverse> set enable_action_upon_reversal=true
        enable_action_upon_reversal = true
```

Nota - El nombre del proyecto debe ser único en el dispositivo en donde se realiza la operación de inversión. Si existe un proyecto con el mismo nombre en el dispositivo en el sitio de producción, la operación de inversión genera un error.

4. Introduzca show para confirmar las propiedades e introduzca commit:

```
target:shares replication package-000 pkgreverse> show
Properties:
        new_project_name = new-kmm3
        enable_action_upon_reversal = true

host-prod:shares replication package-000 pkgreverse> commit
```

This action will move the contents of this package to a new local project configured to replicate back to the source. Any data or metadata changes made on the source since the last successful update will be lost when the new project is replicated back to the source. If replication actions on the source are not disabled, future updates to this package will fail.

5. Navegue hasta shares replication actions.

```
target:shares replication packages> cd /
target:> shares replication actions
```

6. Seleccione la acción creada recientemente usando el ID de paquete de los pasos anteriores.

Use el ID de paquete como origin_pkg_id para seleccionar la acción.

```
target:shares replication actions> select origin_pkg_id=
1c0457eb-45bd-4f91-8e08-bc0dbacd40b7
target:shares replication action-000> ls
Properties:
            id = 6a10ce61-cc87-4850-89dd-8673f7734d03
      origin_pkg_id = 1c0457eb-45bd-4f91-8e08-bc0dbacd40b7
            target = new_target
      target_pool = p
      source_pool = p
    replication_of = dataset1
            enabled = true
      continuous = false
    include_snaps = false
retain_user_snaps_on_target = false
            dedup = false
include_clone_origin_as_data = false
      max_bandwidth = unlimited
            bytes_sent = 0
    estimated_size = 0
estimated_time_left = 00:00:00
    average_throughput = 0B/s
            use_ssl = false
      compression = on
      export_path =
            state = idle
    state_description = Idle (no update in progress)
    export_pending = false
      offline = false
      next_update = Sync now
    replica_data_timestamp = Thu Nov 21 2019 16:17:25 GMT+0000 (UTC)
            last_sync = <unknown>
            last_try = <unknown>
            last_result = <unknown>
      replica_lag = 461:55:40
recovery_point_objective =
    replica_lag_warning_alert =
    replica_lag_error_alert =
    replica_lag_over_warning_limit = false
    replica_lag_over_error_limit = false
```

7. Para exportar la primera actualización de replicación después de la reversión a un servidor NFS, introduzca export_path y la ruta de acceso del servidor NFS. Introduzca commit y, a continuación, introduzca sendupdate:

```

target:shares replication action-000> set export_path=nfs://nfs_server/export/init_repl
      export_path = nfs://nfs_server/export/init_repl (uncommitted)
target:shares replication action-000> commit
target:shares replication action-000> sendupdate
target:shares replication action-000> ls
Properties:
      id = 6a10ce61-cc87-4850-89dd-8673f7734d03
      origin_pkg_id = 1c0457eb-45bd-4f91-8e08-bc0dbacd40b7
      target = new_target
      target_pool = p
      source_pool = p
      replication_of = dataset1
      enabled = true
      continuous = false
      include_snaps = false
      retain_user_snaps_on_target = false
      dedup = false
      include_clone_origin_as_data = false
      max_bandwidth = unlimited
      bytes_sent = 0
      estimated_size = 0
      estimated_time_left = 00:00:00
      average_throughput = 0B/s
      use_ssl = false
      compression = on
      export_path = nfs://nfs_server/export/init_repl
      state = idle
      state_description = Idle (no update in progress)
      export_pending = false
      offline = false
      next_update = Sync now
      replica_data_timestamp = Thu Nov 21 2019 16:17:25 GMT+0000 (UTC)
      last_sync = <unknown>
      last_try = <unknown>
      last_result = <unknown>
      replica_lag = 461:55:40
      recovery_point_objective =
      replica_lag_warning_alert =
      replica_lag_error_alert =
      replica_lag_over_warning_limit = false
      replica_lag_over_error_limit = false

```

- 8. Cuando la actualización de la replicación haya finalizado, navegue hasta el paquete recién revertido en el nuevo destino. La descripción del estado debe indicar Inactivo, como se muestra en el ejemplo:**

```

new_target:shares replication packages> ls
Packages:

ID          STATE DATA_TIMESTAMP    SOURCE    DATASET
package-000 idle   unknown           target    <unknown>

```

- 9. Seleccione el paquete e introduzca `ls` para mostrar las propiedades.**

```

new_target:shares replication packages> select package-000
new_target:shares replication package-000> ls

Properties:
      id = 6a10ce61-cc87-4850-89dd-8673f7734d03

```

```

source_name = target
source_asn = ddbd5d4e-daff-4f52-9417-cd6e893c694a
source_ip = 00.000.00.000:216
source_pool = poolA
target_pool = poolA
replica_of = <unknown>
enabled = true
state = idle
state_description = Idle (no update in progress)
offline = true
import_path =
data_timestamp = unknown
last_sync = unknown
last_try = unknown
last_result = unknown

```

10. Importe la actualización desde el servidor NFS.

```

new_target:shares replication package-000> set import_path=nfs://nfs_server/export/init_repl
import_path = nfs://nfs_server/export/init_repl (uncommitted)

```

11. Introduzca `commit` y, luego, visualice las propiedades del paquete para confirmar que la actualización haya finalizado.

La propiedad `last_result` muestra `success`.

```

new_target:shares replication package-000> commit
new_target:shares replication package-000> ls
Properties:
            id = 6a10ce61-cc87-4850-89dd-8673f7734d03
source_name = target
source_asn = ddbd5d4e-daff-4f52-9417-cd6e893c694a
source_ip = 00.000.00.000:216
source_pool = poolA
target_pool = poolA
replica_of = <unknown>
enabled = true
state = idle
state_description = Idle (no update in progress)
offline = false
import_path =
data_timestamp = unknown
last_sync = Fri Nov 22 2019 22:11:32 GMT+0000 (UTC)
last_try = Fri Nov 22 2019 22:11:32 GMT+0000 (UTC)
last_result = success

```

Temas relacionados

- [Importación de un flujo de replicación desde el servidor NFS \(CLI\) \[652\]](#)
- [“Configuración de replicación fuera de línea \(CLI\)” \[648\]](#)

▼ Desactivación de la compresión de replicación (BUI)

Se puede desactivar la compresión cuando crea o edita una acción de replicación. Por defecto, todos los flujos de replicación se comprimen antes de enviarlos por la red.

1. Desde el dispositivo de origen, vaya a **Recursos compartidos > Proyectos >** y haga doble clic en el proyecto que desea editar.
2. Haga clic en el separador **Replicación**.
3. Haga clic en el ícono de edición .
4. Haga clic en **Desactivar compresión** y, a continuación, haga clic en **Aplicar**.

Temas relacionados

- [“Replicación comprimida” \[746\]](#)
- [Flujo de trabajo de replicación remota \[623\]](#)

▼ Desactivación de la compresión de replicación (CLI)

Se puede desactivar la compresión cuando crea o edita una acción de replicación. Por defecto, todos los flujos de replicación se comprimen antes de enviarlos por la red. Para obtener más información, consulte [“Replicación comprimida” \[746\]](#).

1. Para desactivar la compresión, navegue hasta el proyecto o el recurso compartido y configure la propiedad `compression`, como se muestra en el siguiente ejemplo:

```
eel:shares proj1 action-000> set compression=off
```

2. Introduzca `commit` y, a continuación, `show` para confirmar que la propiedad `compression` esté desactivada.

```
eel:shares proj1 action-000> commit
eel:shares proj1 action-000> show
Properties:
            id = 67f0d3d6-10af-6f30-9d4c-a60d19eb1200
            target = goby-10g
```

```
        enabled = true
        continuous = false
        include_snaps = false
        max_bandwidth = unlimited
        bytes_sent = 0
        estimated_size = 0
estimated_time_left = 00:14:35
        average_throughput = 0B/s
        use_ssl = false
        compression = off
        export_path =
            state = idle
state_description = idle (no update in progress)
        export_pending = false
            offline = false
        next_update = Sync now
            last_sync = <unknown>
            last_try =
last_result =
```

Temas relacionados

- [“Replicación comprimida” \[746\]](#)
- [Flujo de trabajo de replicación remota \[623\]](#)

▼ Prueba de la conexión (BUI)

1. **Vaya a Configuración > Servicios > Replicación remota > Destinos.**
2. **Pase el cursor sobre el nombre del destino con la conexión que desea comprobar y haga clic en el ícono de edición .**
3. **En el cuadro de diálogo Edit Replication Target (Editar destino de replicación), haga clic en el botón Probar conexión.**

Un cuadro de diálogo indicará si el certificado es de confianza.

4. **Verifique el certificado.**

Si el certificado no es de confianza para el origen (por ejemplo, si el origen destruyó el certificado), el cuadro de diálogo presentará el certificado para que usted lo revise y le solicitará aceptar o rechazar el certificado.

Para verificar el certificado, compare la huella del certificado que se muestra con la huella del certificado en el destino.

- a. **En el dispositivo de destino, vaya a Configuración > Valores de configuración > Certificados y haga clic en el separador Sistema.**

- b. Haga clic en el ícono de información  en el certificado predeterminado del sistema.

- Si el certificado predeterminado del sistema se genera automáticamente, haga clic en el ícono de información del certificado basado en el identificador exclusivo universal de ASN.
- Si el sistema utiliza un certificado firmado por una autoridad de certificación, haga clic en el ícono de información de ese certificado.

- c. Compare los certificados.

Compare el certificado que se presenta en el cuadro de diálogo del dispositivo de origen con el certificado que se muestra en el cuadro de diálogo de información del dispositivo de destino.

- **Si las huellas coinciden, acepte el certificado.**
Si las huellas coinciden, el certificado presentado es el certificado del destino y es de confianza. Acepte el certificado. El certificado se agregará a la lista de confianza del origen.
- **Si las huellas no coinciden, rechace el certificado por no ser de confianza.**
El certificado no se agregará a la lista de confianza del origen.

5. Haga clic en el botón Cancelar en el cuadro de diálogo Edit Replication Target (Editar destino de replicación).

Temas relacionados

- [Creación de un destino de replicación \(BUI\) \[629\]](#)
- [Edición de un destino de replicación \(BUI\) \[663\]](#)
- [“Destinos de replicación” \[711\]](#)

▼ Prueba de la conexión (CLI)

1. Vaya a `shares replication targets`.
2. Seleccione el destino cuya conexión desea comprobar.

3. Pruebe la conexión.

Use el comando `test` para probar la conexión. Si el certificado es de confianza para el origen, se presentará el mensaje que se muestra en el siguiente ejemplo.

```
hostname:shares replication target-000> test
Certificate is trusted
```

4. Verifique el certificado.

Si el certificado no es de confianza para el origen (por ejemplo, si el origen destruyó el certificado), se presentará el certificado para que usted lo revise y se le solicitará aceptar o rechazar el certificado.

Para verificar el certificado, compare la huella del certificado que se muestra con la huella del certificado en el destino.

a. **En el dispositivo de destino, vaya a `configuration settings certificates system`.**

b. **Seleccione el certificado predeterminado del sistema.**

- **Si el certificado predeterminado del sistema se genera automáticamente, seleccione el certificado basado en el identificador exclusivo universal de ASN.**
- **Si el sistema utiliza un certificado firmado por una autoridad de certificación, seleccione ese certificado.**

c. **Introduzca el comando `get`.**

d. **Compare los certificados.**

Compare el certificado que se presenta en el dispositivo de origen con el certificado que muestra el comando `get`.

■ **Si las huellas coinciden, acepte el certificado.**

Si las huellas coinciden, el certificado presentado es el certificado del destino y es de confianza. Acepte el certificado. El certificado se agregará a la lista de confianza del origen.

■ **Si las huellas no coinciden, rechace el certificado por no ser de confianza.**

El certificado no se agregará a la lista de confianza del origen.

5. Introduzca el comando `done` y confirme la acción.

Temas relacionados

- [Creación de un destino de replicación \(CLI\) \[631\]](#)
- [Edición de un destino de replicación \(CLI\) \[664\]](#)
- [“Destinos de replicación” \[711\]](#)

▼ Edición de un destino de replicación (BUI)

1. **Vaya a Configuración > Servicios > Replicación remota > Destinos.**
2. **Pase el cursor sobre el nombre del destino que desee editar y haga clic en el ícono de edición .**

3. **Modifique los valores de las propiedades del destino.**

Es posible modificar las propiedades Nombre y Nombre de host, y activar o desactivar la opción Host Match (Coincidencia de host). Para obtener descripciones de estas propiedades, consulte [Creación de un destino de replicación \(BUI\) \[629\]](#).

Se debe resolver una dirección IP o un nombre de host actualizado en el mismo dispositivo. Para indicar un dispositivo diferente al que se configuró anteriormente, cree un nuevo destino para autenticarlo con el nuevo dispositivo.

4. **Haga clic en Aplicar para guardar todos los cambios.**

Se ejecuta la comprobación de confianza del certificado. Una vez creado un destino, su certificado se puede dejar de ser de confianza. Por ejemplo, el administrador de origen podría suprimir el certificado de la lista de certificados de confianza o el administrador de destino podría reemplazar el certificado.

Si el certificado no es de confianza para el origen, se presentará el certificado para que usted lo revise y se le solicitará aceptar o rechazar el certificado como se describe en [Prueba de la conexión \(BUI\) \[660\]](#).

Tareas adicionales

- Vea las acciones configuradas con el destino. Para modificar las propiedades de una acción, consulte [Edición de una acción de replicación \(BUI\) \[665\]](#).
- Destruya el destino, si ninguna acción lo está utilizando.

Nota - No se debe destruir un destino si hay acciones que lo están utilizando. Estas acciones quedarán permanentemente interrumpidas. El sistema hace todo lo posible por aplicar esta mejor práctica, pero no puede garantizar que no existan acciones en las agrupaciones de almacenamiento exportadas que utilicen un destino dado.

Temas relacionados

- [Creación de un destino de replicación \(BUI\) \[629\]](#)
- [Prueba de la conexión \(BUI\) \[660\]](#)
- [“Destinos de replicación” \[711\]](#)
- [Flujo de trabajo de replicación remota \[623\]](#)
- [“Conceptos de replicación remota” \[708\]](#)
- [“Copia de seguridad, replicación y restauración de proyectos y recursos compartidos cifrados” \[838\]](#)

▼ Edición de un destino de replicación (CLI)

1. **Vaya a** `shares replication targets`.

2. **Seleccione el destino que desee editar.**

3. **Modifique los valores de las propiedades del destino.**

Es posible modificar las propiedades `label` y `hostname`, y activar o desactivar el valor de la opción `host_match`. Para obtener descripciones de estas propiedades, consulte [Creación de un destino de replicación \(CLI\) \[631\]](#).

Se debe resolver un valor `hostname` actualizado en el mismo dispositivo. Para indicar un dispositivo diferente al que se configuró anteriormente, cree un nuevo destino para autenticarlo con el nuevo dispositivo.

4. **Confirme todos los cambios.**

Se ejecuta la comprobación de confianza del certificado. Una vez creado un destino, su certificado se puede dejar de ser de confianza. Por ejemplo, el administrador de origen podría suprimir el certificado de la lista de certificados de confianza o el administrador de destino podría reemplazar el certificado.

Si el certificado no es de confianza para el origen, se presentará el certificado para que usted lo revise y se le solicitará aceptar o rechazar el certificado como se describe en [Prueba de la conexión \(CLI\) \[661\]](#).

Tareas adicionales

- Vea las acciones configuradas con el destino. Para modificar las propiedades de una acción, consulte [Edición de una acción de replicación \(CLI\) \[666\]](#).
- Destruya el destino, si ninguna acción lo está utilizando.

Nota - No se debe destruir un destino si hay acciones que lo están utilizando. Estas acciones quedarán permanentemente interrumpidas. El sistema hace todo lo posible por aplicar esta mejor práctica, pero no puede garantizar que no existan acciones en las agrupaciones de almacenamiento exportadas que utilicen un destino dado.

Temas relacionados

- [Creación de un destino de replicación \(CLI\) \[631\]](#)
- [Prueba de la conexión \(CLI\) \[661\]](#)
- [“Destinos de replicación” \[711\]](#)
- [Flujo de trabajo de replicación remota \[623\]](#)
- [“Conceptos de replicación remota” \[708\]](#)
- [“Copia de seguridad, replicación y restauración de proyectos y recursos compartidos cifrados” \[838\]](#)

▼ Edición de una acción de replicación (BUI)

1. Navegue hasta el proyecto o el recurso compartido y haga clic en el separador **Replicación**.
2. Seleccione el proyecto o el recurso compartido que desea editar.
3. Haga clic en el ícono de edición .
4. En la pantalla **Editar acción de replicación**, modifique las propiedades y, a continuación, haga clic en **Aplicar**.

Para leer una descripción de las acciones de replicación, consulte [“Propiedades de las acciones de replicación” \[716\]](#).

Temas relacionados

- [Edición de un destino de replicación \(BUI\) \[663\]](#)

- [“Acciones y paquetes de replicación” \[714\]](#)
- [Flujo de trabajo de replicación remota \[623\]](#)

▼ Edición de una acción de replicación (CLI)

1. **Navegue hasta `shares replication actions` y, luego, introduzca `ls` para mostrar las acciones disponibles.**

```
hostname:> shares replication actions
hostname:shares replication actions> ls
Actions:
```

ID	STATE	REPLICA_DATA_TSTAMP	TARGET	DATASET
action-007	idle	2017-02-17 23:01:19	targetA	berries
action-008	idle	2017-02-17 23:01:40	targetA	cherries
action-003	idle	2017-02-15 23:48:15	targetA	ocean
action-002	disbl	<unknown>	targetA	oceanR
action-004	idle	<unknown>	targetA	berries

2. **Seleccione la acción que desea editar.**

```
hostname:shares replication actions> select action-007
hostname:shares replication action-007>
```

3. **Modifique las propiedades según sea necesario mediante el comando `set`.**

Para consultar la lista de comandos de acciones de replicación para la CLI, consulte [“Propiedades de las acciones de replicación” \[716\]](#).

Temas relacionados

- [Creación de una acción de replicación \(CLI\) \[636\]](#)
- [Flujo de trabajo de replicación remota \[623\]](#)

Supervisión de la replicación remota

Use las siguientes tareas para supervisar el progreso de la replicación, las demoras, los eventos y las alertas. Para investigar el rendimiento de replicación en detalle, use las estadísticas de análisis de replicación.

- Supervisión del avance de la replicación: [BUI](#), [CLI](#)
- Supervisión de demoras de la replicación y RPO: [BUI](#), [CLI](#)
- [“Acciones de auditoría de replicación” \[672\]](#)

- Configuración de alertas de inicio y de finalización de replicación: [BUI](#), [CLI](#)
- “Uso de análisis de replications” [675]

▼ Supervisión del avance de la replicación (BUI)

1. Para supervisar el progreso de una actualización de replicación, vaya a **Recursos compartidos > Proyectos** y seleccione el proyecto replicado; o seleccione un proyecto y, luego, seleccione el recurso compartido replicado.
2. Haga clic en el separador **Replicación**.

Las etapas iniciales de replicación se muestran debajo de la barra de progreso.

TARGET ▲	UPDATES	STATUS
cleo Manual	2016-5-2 10:50:32 Synced 2016-5-2 10:50:32 Attempted	Connecting to replication target

Las diferentes etapas son:

- Conectando a destino de replicación
 - Recibiendo punto de control de destino de replicación
 - Estimando tamaño de actualización
 - Creando tablas de deduplicación
3. Después de que la acción de replicación envíe los datos, puede ver el porcentaje de bytes enviados, el tamaño estimado, el rendimiento promedio y el tiempo restante estimado.

TARGET ▲	UPDATES	STATUS
brmzs3-2-250 Scheduled	2014-12-24 02:49:52 Synced 2014-12-24 02:49:52 Attempted	78% of 2.5T @50MB/s (-03:13:10)

Temas relacionados

- “Acciones de auditoría de replicación” [672]
- “Uso de análisis de replications” [675]
- “Replicación con deduplicación” [727]

▼ Supervisión del avance de la replicación (CLI)

1. **Para supervisar el progreso de la actualización de una replicación, navegue hasta el recurso compartido o el proyecto e introduzca el nodo de replicación.**

```
hostname:shares> select TestProj
hostname:shares TestProj> replication
hostname:shares TestProj replication>
```

2. **Seleccione la acción de replicación y, luego, introduzca get:**

```
hostname:shares TestProj replication> select action-000
hostname:shares TestProj action-000> get
Properties:
    id = aed46331-160b-48ec-8727-dcd563adbd78
    target_id = 4fd3483e-b1f5-4bdc-9be3-b3a4becd0c42
    target = target1
    enabled = true
    continuous = false
    include_snaps = true
    retain_user_snaps_on_target = false
    dedup = true
    include_clone_origin_as_data = false
    max_bandwidth = unlimited
    bytes_sent = 0
    estimated_size = 0
    estimated_time_left = 00:00:00
    average_throughput = 0B/s
    use_ssl = true
    compression = on
    export_path =
    state = sending
    state_description = Connecting to replication target
    export_pending = false
    offline = false
    next_update = Sync now
    replica_data_timestamp = Thu Apr 25 2019 22:18:11 GMT+0000 (UTC)
    last_sync = <unknown>
    last_try = <unknown>
    last_result = <unknown>
    replica_lag = 00:00:09
    recovery_point_objective =
    replica_lag_warning_alert =
    replica_lag_error_alert =
    replica_lag_over_warning_limit = false
    replica_lag_over_error_limit = false
```

3. **Revise la propiedad `state_description` para obtener información sobre el progreso de la replicación.**

Los estados posibles son:

- Conectando a destino de replicación
- Recibiendo punto de control de destino
- Estimando tamaño de actualización
- Building deduplication tables

- Sending update

El estado `Building deduplication tables` se muestra solamente si el proyecto o el recurso compartido tiene activada la deduplicación.

4. Si `state_description` es `Sending update`, revise las siguientes propiedades para determinar el progreso de replicación:

- `bytes_sent`
- `estimated_size`
- `estimated_time_left`
- `average_throughput`

Temas relacionados

- [“Acciones de auditoría de replicación” \[672\]](#)
- [“Uso de análisis de replicaciones” \[675\]](#)
- [“Replicación con deduplicación” \[727\]](#)

▼ Supervisión de demoras de replicación y RPO (BUI)

Con la replicación asíncrona, se produce una demora al escribir datos desde el origen en la réplica en el destino. Se puede configurar una alerta de advertencia y una de error para notificar al administrador cuando la demora de una replicación se está acercando o excede el objetivo de punto de replicación (RPO). Estas alertas solicitan al administrador que compruebe que no haya problemas en la red ni problemas relacionados con las aplicaciones y que use análisis para examinar el estado del dispositivo de almacenamiento.

Las alertas de demora de replicación se pueden configurar al crear o editar una acción de replicación.

Para establecer alertas de demora de replicación:

1. **Vaya a Recursos compartidos > Proyectos.**
2. **Seleccione un proyecto o el recurso compartido y haga clic en el separador Replicación.**
3. **Haga clic en el ícono de agregación , junto a Acciones.**

4. **Seleccione las propiedades para esta acción. Consulte [“Propiedades de las acciones de replicación” \[716\]](#).**
5. **Seleccione "Objetivo de punto de recuperación" e introduzca un valor. A continuación, especifique días, horas, minutos o segundos.**

Recovery point objective ☐ hours

Replica lag warning alert ☐ % of Recovery Point Objective

Replica lag error alert ☐ % of Recovery Point Objective

Update frequency ☒ Scheduled ☐ Continuous

6. **Seleccione "Alerta de advertencia de demora de réplica" y "Alerta de error de demora de réplica" y especifique un porcentaje del RPO para cada propiedad.**
 Al configurar estas propiedades se generan advertencias en distintos momentos. Por ejemplo, introduzca 50 para generar una alerta menor cuando la demora de replicación exceda el 50 % del RPO. Introduzca 180 para generar una alerta mayor cuando la demora de replicación exceda el 180 % del RPO.
 Cuando la demora de réplica cae por debajo de los valores establecidos, una alerta menor informa que la demora de réplica está dentro del límite de advertencia o error.
7. **Establezca una acción de alerta como se describe en [Agregación de una acción de alerta \(BUI\) \[287\]](#).**

Temas relacionados

- [Creación de una acción de replicación \(BUI\) \[632\]](#)
- [“Propiedades de las acciones de replicación” \[716\]](#)

▼ Supervisión de demoras de replicación y RPO (CLI)

Con la replicación asíncrona, se produce una demora al escribir datos desde el origen en la réplica en el destino. Se puede configurar una alerta de advertencia y una de error para notificar al administrador cuando la demora de una replicación se está acercando o excede el objetivo de punto de replicación (RPO). Estas alertas solicitan al administrador que compruebe que no haya problemas en la red ni problemas relacionados con las aplicaciones y que use análisis para examinar el estado del dispositivo de almacenamiento.

Las alertas de demora de replicación se pueden configurar al crear o editar una acción de replicación.

Para establecer alertas de demora de replicación:

1. Navegue hasta el proyecto o el recurso compartido e introduzca `action`:

```
host_source:shares New_Project replication> action
```

2. Introduzca `get` para mostrar las propiedades.

```
host_source:shares New_Project action (uncommitted)> get
origin_pkg_id =
  target = replication-target
  pool = demo_pool
  enabled = true
  continuous = false
  include_snaps = true
  retain_user_snaps_on_target = false
  dedup = false
  include_clone_origin_as_data = false
  max_bandwidth = unlimited
  bytes_sent = 0
  estimated_size = 0
  estimated_time_left = 00:00:00
  average_throughput = 0B/s
  use_ssl = true
  compression = on
  export_path =
  state = idle
  state_description = Idle (no update in progress)
  export_pending = false
  offline = false
  next_update = Sync now
  replica_lag = P1H30M
  replica_data_timestamp = Wed Feb 20 2019 12:12:05 GMT+0000 (UTC)
  last_sync = Wed Feb 20 2019 22:32:59 GMT+0000 (UTC)
  last_try = Wed Feb 20 2019 22:32:59 GMT+0000 (UTC)
  last_result = success
  recovery_point_objective =
  replica_lag_warning_alert =
  replica_lag_error_alert =
```

3. Configure las propiedades de demora de réplica y RPO para esta acción como se muestra en el siguiente ejemplo:

```
host_source:shares New_Project action (uncommitted)> set recovery_point_objective=50min
  recovery_point_objective = 50 minutes (uncommitted)
host_source:shares New_Project action (uncommitted)> set replica_lag_warning_alert=50
  replica_lag_warning = 50% (uncommitted)
host_source:shares New_Project action (uncommitted)> set replica_lag_error_alert=180
  replica_lag_error = 180% (uncommitted)
```

Para leer una descripción de las propiedades, consulte [“Propiedades de las acciones de replicación” \[716\]](#).

4. Confirme los cambios para esta acción.

```
host_source:shares New_Project action (uncommitted)> commit
```

5. Para ver las propiedades actuales de la acción, introduzca `ls`. En el siguiente ejemplo, se muestra la porción de demora de réplica y RPO de la salida:

```
host_source:shares New_Project action (uncommitted)> ls
.
      replica_lag = P1H30M
 replica_data_timestamp = Wed Feb 20 2019 12:12:05 GMT+0000 (UTC)
      last_sync = Wed Feb 20 2019 22:32:59 GMT+0000 (UTC)
      last_try = Wed Feb 20 2019 22:32:59 GMT+0000 (UTC)
      last_result = success
 recovery_point_objective = 50 minutes
 replica_lag_warning_alert = 50%
 replica_lag_error_alert = 180%
```

6. Establezca una acción de alerta como se describe en [Agregación de una acción de alerta \(CLI\) \[289\]](#).

Temas relacionados

- [Creación de una acción de replicación \(CLI\) \[636\]](#)
- [“Propiedades de las acciones de replicación” \[716\]](#)

Acciones de auditoría de replicación

Las siguientes acciones de configuración de replicación se registran y escriben en el log de auditoría. Para ver las entradas del log de auditoría en la BUI, vaya a Mantenimiento > Logs > Auditoría.

- Creación, modificación o destrucción de acciones de replicación
- Agregación o eliminación de recursos compartidos desde un grupo de replicación
- Creación, modificación, clonación, reversión, corte o destrucción de paquetes de replicación en el destino
- Creación, modificación o destrucción de destinos de replicación

▼ Configuración de alertas de inicio y de finalización de replicación (BUI)

El volumen de alertas de inicio y de finalización para las actualizaciones programadas puede opacar otras alertas importantes. Utilice este procedimiento para desactivar o activar las alertas de inicio y de finalización de replicación.

Las alertas de finalización proporcionan estadísticas sobre cada actualización de replicación. En la CLI, el nodo `stats` de una acción de replicación proporciona estadísticas de la actualización más reciente completada o el total acumulado de esta acción de replicación.

1. **Vaya a Configuración > Servicios > Replicación remota > Propiedades.**
2. **Active o desactive la publicación de alertas de inicio/finalización.**
 - **Para desactivar la publicación de alertas de inicio/finalización, desmarque el botón Activar alertas de inicio/finalización.**
Asegúrese de que el botón no muestre una marca de verificación.
 - **Para activar la publicación de alertas de inicio/finalización, marque el botón Activar alertas de inicio/finalización.**
Asegúrese de que el botón muestre una marca de verificación.
Para ver las alertas, vaya a Mantenimiento > Logs > Alertas.
3. **Haga clic en el botón APLICAR de la esquina superior derecha de la página Propiedades.**

Temas relacionados

- [“Alertas de replicación” \[742\]](#)
- [“Alertas de inicio y de finalización” \[743\]](#)
- [Tabla 146, “Propiedades de nodo de estadísticas de acciones de replicación \(CLI, solo lectura\)”](#)

Para especificar una acción de alerta personalizada, consulte [Agregación de una acción de alerta \(BUI\) \[287\]](#) y seleccione una de las siguientes opciones del menú Categoría:

- Replicación remota
- Replicación remota: solo origen
- Replicación remota: solo destino

▼ Configuración de alertas de inicio y de finalización de replicación (CLI)

El volumen de alertas de inicio y de finalización para las actualizaciones programadas puede opacar otras alertas importantes. Utilice este procedimiento para desactivar o activar las alertas de inicio y de finalización de replicación.

Las alertas de finalización proporcionan estadísticas sobre cada actualización de replicación. En la CLI, el nodo `stats` de una acción de replicación proporciona estadísticas de la actualización más reciente completada o el total acumulado de esta acción de replicación.

1. **Vaya a `configuration services replication` e introduzca el comando `get`.**

```
hostname:> configuration services replication
hostname:configuration services replication> get
               <status> = online
enable_start_finish_alerts = true
```

2. **Active o desactive la publicación de alertas de inicio/finalización.**

- **Para desactivar las alertas de inicio/finalización, establezca el valor de la propiedad `enable_start_finish_alerts` en `false`.**

```
hostname:configuration services replication> set enable_start_finish_alerts=false
enable_start_finish_alerts = false (uncommitted)
hostname:configuration services replication> commit
```

- **Para activar las alertas de inicio/finalización, establezca el valor de la propiedad `enable_start_finish_alerts` en `true`.**

Para ver las alertas, introduzca `maintenance logs` y, a continuación, `select alert` y `show`.

3. **Vuelva a introducir `get` para confirmar que el valor sea correcto.**

Temas relacionados

- [“Alertas de replicación” \[742\]](#)
- [“Alertas de inicio y de finalización” \[743\]](#)
- [Tabla 146, “Propiedades de nodo de estadísticas de acciones de replicación \(CLI, solo lectura\)”](#)

Para especificar una acción de alerta personalizada, consulte [Agregación de una acción de alerta \(CLI\) \[289\]](#) y establezca la propiedad `category` en uno de los siguientes valores:

- `replication`
- `replication_source`

- `replication_target`

Uso de análisis de replicaciones

Puede supervisar el progreso de replicación con las siguientes estadísticas de análisis:

- [Data Movement: Replication Bytes \(Data Movement: Bytes de replicación\)](#)
- [Data Movement: Replication Operations \(Movimiento de datos: operaciones de replicación\)](#)
- [Movimiento de datos: latencias de replicación](#) (análisis avanzado)
- [Movimiento de datos: bytes de envío/recepción de replicación](#) (análisis avanzado)

Cada estadística se puede desglosar por dirección, tipo de operación, par, nombre de agrupación, proyecto o juego de datos, o se puede capturar como estadística sin procesar.

En la BUI, vaya a Análisis > Juegos de datos y busque Movimiento de datos: estadísticas de replicación, o vaya a Análisis y agregue Movimiento de datos: estadísticas de replicación a una hoja de trabajo.

En la CLI, vaya a `analytics datasets` o `analytics worksheets` y busque o agregue las estadísticas `repl..`

Para obtener más información sobre los análisis y las estadísticas, consulte [Guía de análisis de Oracle® ZFS Storage Appliance versión OS8.8.x](#).

Gestión de paquetes de replicación

Cuando los proyectos y los recursos compartidos se replican en un destino, los datos se almacenan en un paquete de replicación. Los paquetes de replicación se pueden usar para hacer copias de seguridad de disco a disco, operaciones de failover, realizar pruebas o se los puede montar desde un cliente para acceso de solo lectura.

Use cualquiera de los siguientes métodos para acceder a los datos que están en un paquete de replicación:

- **Exporte un paquete de replicación:** cuando exporta un paquete de replicación seleccionado, los recursos compartidos exportados incluyen los datos de la actualización de replicación finalizada más reciente. Después de exportar los recursos compartidos, puede acceder a datos específicos de la instantánea correspondientes a cualquiera de los recursos compartidos. Para ello, debe navegar hasta el directorio `.zfs/snapshot` dentro del directorio raíz del recurso compartido. Normalmente, el directorio `.zfs` no está visible, pero puede acceder a él especificando explícitamente el nombre del archivo o del subdirectorio, como

se describe en [Acceso a un directorio oculto de instantáneas del sistema de archivos](#). Para obtener información acerca del cambio de la propiedad de visibilidad de una instantánea, consulte la sección Visibilidad de un directorio de instantáneas del sistema de archivos: [BUI](#), [CLI](#).

- **Clone un paquete de replicación:** para la creación de un clon de un paquete de replicación se utilizan los datos recibidos más recientemente del dispositivo de origen. La clonación convierte un paquete de replicación en un proyecto nuevo, lo que otorga acceso de lectura y escritura a todos los datos del proyecto. El proyecto clonado debe tener un nombre, un punto de montaje y un nombre de recurso de SMB únicos que no entren en conflicto con ningún proyecto existente. Para obtener más información, consulte Clonación de un paquete de replicación: [BUI](#), [CLI](#).
- **Clone recursos compartidos de un paquete de replicación:** las instantáneas de recursos compartidos individuales, creadas antes de la replicación más reciente, se pueden clonar desde un paquete de replicación. La clonación de una instantánea individual desde un paquete de replicación proporciona acceso de lectura y escritura a los datos tal como existían en el dispositivo de origen cuando se creó la instantánea. Para obtener más información, consulte la [BUI](#) o la [CLI](#) de clonación de una instantánea.
- **Corte un paquete de replicación:** la operación de corte convierte un paquete de replicación en un proyecto nuevo, lo que permite el acceso de lectura y escritura a los datos del proyecto. La conexión de replicación entre el dispositivo de origen y el dispositivo de destino se corta luego de esta operación. Tenga en cuenta que el nuevo proyecto debe tener un nombre, un punto de montaje y un nombre de recurso de SMB únicos que no generen conflictos con ninguno de los proyectos existentes. Para obtener más información, consulte cómo cortar un paquete de replicación: [BUI](#), [CLI](#).
- **Invierta un paquete de replicación:** la replicación inversa convierte un paquete de replicación en un proyecto nuevo, lo que permite el acceso de lectura y escritura a los datos del proyecto. La conexión de la replicación se conserva y se crea una nueva acción de replicación que permite replicar nuevamente los datos en el dispositivo de origen original. Para obtener más información, consulte [“Reversión de la dirección de replicación” \[790\]](#). La función de reversión de varios destinos envía actualizaciones incrementales desde el origen nuevo hacia todos los destinos configurados originalmente. Para obtener información sobre esta función, incluso sobre la configuración y la resolución de conflictos, consulte [“Reversión a varios destinos” \[750\]](#).

Las tareas adicionales relacionadas con los paquetes de replicación incluyen:

- [Gestión de instantáneas generadas por el usuario](#)
- Cancelación de una actualización de replicación: [BUI](#), [CLI](#)
- Clonación de un paquete de replicación: [BUI](#), [CLI](#)
- Corte de un paquete de replicación: [BUI](#), [CLI](#)
- Edición de un paquete de replicación: [BUI](#), [CLI](#)
- Desactivación de un paquete de replicación: [BUI](#), [CLI](#)

Gestión de instantáneas generadas por el usuario

La copia de seguridad de disco a disco también se puede realizar mediante la configuración de la propiedad "Conservar instantáneas generadas por el usuario en destino". Las instantáneas generadas por el usuario, creadas en un dispositivo de origen, se replican en un destino que sirve como repositorio de copias de seguridad incremental de siempre.

La configuración de esta propiedad permite gestionar las instantáneas generadas por el usuario de manera independiente en un dispositivo de origen y un destino de replicación. Por lo general, cuando se destruyen las instantáneas generadas por el usuario en el dispositivo de origen, las instantáneas se destruyen inmediatamente en el destino de replicación después de una actualización de replicación. Para conservar las instantáneas generadas por el usuario en el destino, configure esta propiedad al crear o editar una acción de replicación.

Cuando las instantáneas generadas por el usuario ya no sean necesarias, destrúyalas manualmente en el destino de replicación. Para destruir instantáneas, consulte [Destrucción de una instantánea: BUI, CLI](#).

Temas relacionados

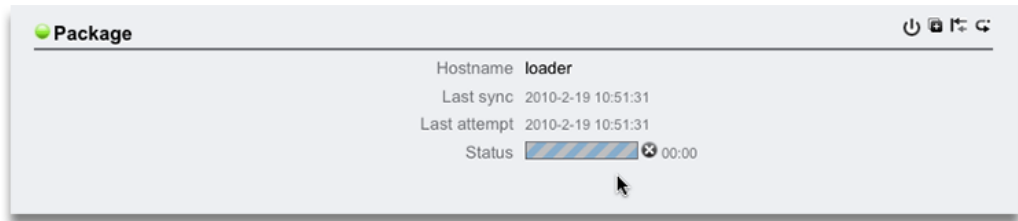
- [“Propiedades de las acciones de replicación” \[716\]](#)
- Creación de una acción de replicación [BUI](#), [CLI](#)
- Edición de una acción de replicación [BUI](#), [CLI](#)
- [“Gestión del espacio de instantáneas” \[591\]](#)

▼ Cancelación de una actualización de replicación (BUI)

Los paquetes de replicación se muestran como proyectos debajo del filtro Réplica.

1. Desde el dispositivo de destino, vaya a **Recursos compartidos > Proyectos** y haga clic en **Réplica**.
2. Haga clic en el separador **Replicación**.

Si hay una actualización en curso, verá una barra de progreso a rayas con un ícono para cancelar  junto a dicha barra:



3. **Haga clic en el ícono de cancelación .**

Pueden pasar varios segundos antes de que finalice la cancelación.

Después de cancelar una actualización, la siguiente actualización programada envía el resto del flujo de datos interrumpido, seguido por una actualización incremental que se basa en el flujo de datos interrumpido.

Nota - No es posible iniciar actualizaciones manuales desde el dispositivo de destino. Debe iniciar sesión en el dispositivo de origen para iniciar una actualización manual.

Temas relacionados

- [“Paquetes de replicación” \[747\]](#)
- [“Replicación reanudable” \[742\]](#)
- [Envío manual de una actualización de replicación \(BUI\) \[641\]](#)

▼ Cancelación de una actualización de replicación (CLI)

Puede cancelar actualizaciones de replicación que estén en curso en el destino de replicación.

1. **Desde el destino de replicación, navegue hasta `shares replication packages` y, luego, introduzca `ls` para mostrar los paquetes.**

```
hostname:> shares replication packages
hostname:shares replication packages> ls
```

ID	STATE	DATA	TIMESTAMP	SOURCE	DATASET
package-002	idle	2019-10-02	19:26:37	hostsource	berries
package-001	idle	2019-10-02	19:26:10	hostsource	berries
package-004	idle	2019-10-02	20:53:51	hostsource	berries/blackberry
package-003	recv	2019-10-02	20:59:52	hostsource	cherries/maraschino

Las entradas se ordenan por source, dataset y data timestamp, respectivamente. La instantánea de réplica más reciente se indica mediante data timestamp.

2. Seleccione un paquete.

```
hostname:shares replication packages> select package-001
```

3. Introduzca cancelupdate.

```
hostname:shares replication package-001> cancelupdate
```

Pueden pasar varios segundos antes de que finalice la cancelación.

Después de cancelar una actualización, la siguiente actualización programada envía el resto del flujo de datos interrumpido, seguido por una actualización incremental que se basa en el flujo de datos interrumpido.

Nota - No es posible iniciar actualizaciones manuales desde el destino de replicación. Debe iniciar sesión en el dispositivo de origen para iniciar una actualización manual.

Temas relacionados

- [“Paquetes de replicación” \[747\]](#)
- [Envío manual de una actualización de replicación \(CLI\) \[642\]](#)

▼ Clonación de un paquete de replicación (BUI)

Los clones de los paquetes de replicación se basan en la instantánea de replicación que se haya recibido más recientemente.

Al crear un proyecto clonado, siga estas directrices para evitar conflictos de nombres:

- El proyecto clonado debe tener un nombre único que no tenga conflictos con ninguno de los proyectos existentes dentro de la misma agrupación.
- El punto de montaje y el nombre de recurso SMB de los recursos compartidos del proyecto clonado no deben tener conflictos con ningún punto de montaje o nombre de recurso SMB existente.

- En el caso de los recursos compartidos que heredan propiedades de un proyecto, resuelva los conflictos mediante la sustitución del punto de montaje o nombre de recurso SMB del nivel del proyecto.
- Para los recursos compartidos que no heredan propiedades del proyecto, defina un sufijo que se agregará al punto de montaje o a los nombres de recurso SMB para resolver conflictos, o sustituya el punto de montaje o el nombre de recurso SMB de manera individual para cada recurso compartido.

Use el procedimiento siguiente para clonar un paquete de replicación.

1. **En el dispositivo de destino, navegue hasta el paquete de replicación que desea clonar.**
2. **Haga clic en el separador Replicación.**
3. **Haga clic en el ícono de clonación .**
4. **En el cuadro de diálogo Clone Replication Project (Proyecto de replicación de clon), complete los siguientes campos:**
 - a. **Proyecto nuevo: introduzca un nombre único para el proyecto nuevo (el clon).**

El nombre debe tener de 1 a 64 caracteres, pero no puede tener espacios ni comenzar con un punto. Los caracteres permitidos son: caracteres alfanuméricos y caracteres especiales (_ - . :).
 - b. **(Opcional) Punto de montaje: introduzca un punto de montaje del nivel del proyecto que sea único para el clon.**

Esta configuración se aplica a los recursos compartidos que hereden el punto de montaje del proyecto. La introducción de un punto de montaje único ayuda a evitar conflictos.
 - c. **(Opcional) Desactivar el uso compartido de SMB: compruebe para desactivar SMB.**

Esta configuración se aplica a los recursos compartidos que hereden el uso compartido de SMB del proyecto. Los recursos compartidos que no hereden el uso compartido de SMB del proyecto no se ven afectados. Desactivar el uso compartido de SMB en el nivel del proyecto no desactivará el uso compartido de SMB para los recursos compartidos que no heredan el uso compartido de SMB del proyecto.
 - d. **(Opcional) Prefijo del nombre de recurso SMB: introduzca un nombre de recurso SMB.**

Esta configuración se aplica a los recursos compartidos que hereden el nombre de recurso SMB del proyecto. La introducción de un nombre de recurso único ayuda a evitar conflictos.

Cuando SMB está activado, puede compartir el clon a través de SMB. El prefijo del nombre de recurso SMB que se usa para compartir los recursos compartidos heredados del proyecto clonado nuevo se construye mediante el prefijo que agrega más el nombre de recurso compartido correspondiente.

5. Haga clic en Aplicar.

Si no hay conflictos de nombres de punto de montaje o recurso, se inicia la operación de clonación.

Si el nombre de proyecto ya está en uso, aparece una alerta y se debe introducir un nuevo nombre de proyecto.

6. (Opcional) Si se detectan conflictos, use los cuadros de diálogo adicionales para resolverlos.

- a. **Resuelva los conflictos que heredan un punto de montaje o nombres de recurso SMB del proyecto.**

Clone Replication Project (Resolve Conflicts) [CANCEL] [APPLY]

New project: clone-project

Conflicts detected for mountpoints and/or SMB resource names that inherit from the project. Use project level setting to resolve the conflicts.

Mountpoint

Disable SMB Sharing ☐

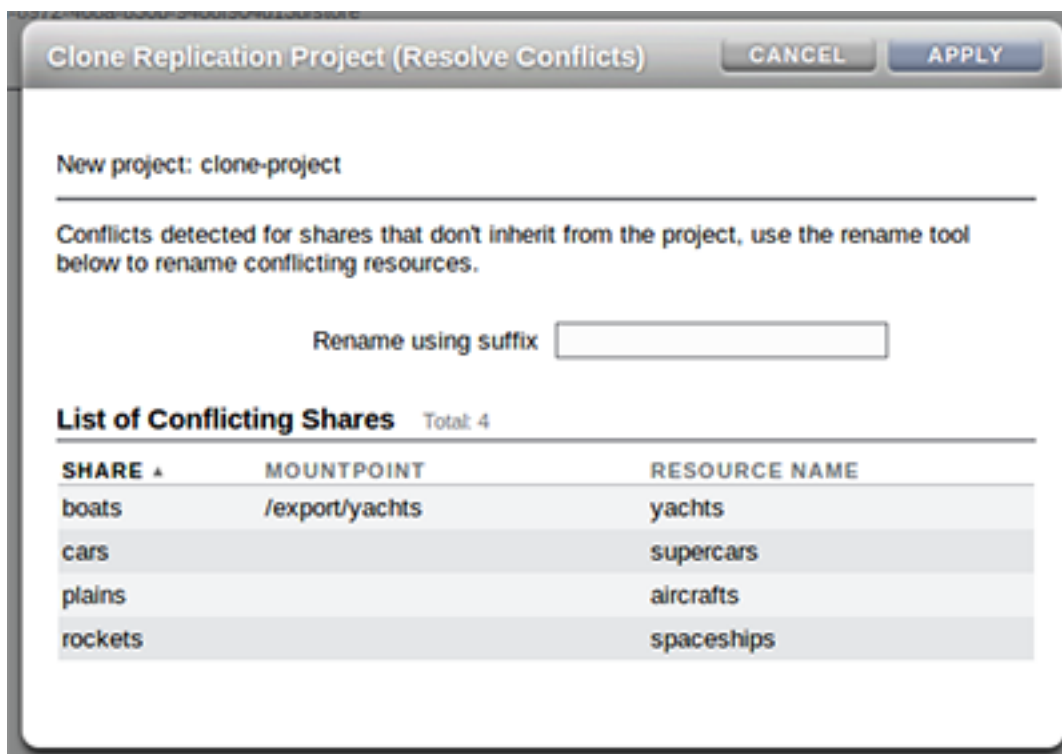
SMB Resource Name Prefix

List of Conflicting Shares Total: 1

-----	-----	-----

- i. Introduzca un punto de montaje que sea único.
 - ii. Desactive el uso compartido de SMB o introduzca un prefijo de nombre de recurso SMB único.
 - iii. Haga clic en Aplicar.
- b. Resuelva los conflictos para los recursos compartidos que no heredan un punto de montaje o nombres de recurso SMB del proyecto.

Este cuadro de diálogo aparece solo después de que haya resuelto todos los conflictos de los recursos compartidos que heredan propiedades del proyecto.



- i. Introduzca un sufijo único para agregarlo a los nombres de punto de montaje o recurso SMB de estos recursos compartidos.
 - ii. Haga clic en Aplicar.
7. Si sigue habiendo conflictos, repita el paso 6 para resolver los conflictos del modo adecuado.

Temas relacionados

- [“Clonación de un recurso compartido o un paquete de replicación” \[748\]](#)
- [“Paquetes de replicación” \[747\]](#)

▼ Clonación de un paquete de replicación (CLI)

Los clones de los paquetes de replicación se basan en la instantánea de replicación que se haya recibido más recientemente.

Al crear un proyecto clonado, siga estas directrices para evitar conflictos de nombres:

- El proyecto clonado debe tener un nombre único que no tenga conflictos con ninguno de los proyectos existentes dentro de la misma agrupación.
- El punto de montaje y el nombre de recurso SMB de los recursos compartidos del proyecto clonado no deben tener conflictos con ningún punto de montaje o nombre de recurso SMB existente.
- En el caso de los recursos compartidos que heredan propiedades de un proyecto, resuelva los conflictos mediante la sustitución del punto de montaje o nombre de recurso SMB del nivel del proyecto.
- Para los recursos compartidos que no heredan propiedades del proyecto, defina un sufijo que se agregará al punto de montaje o a los nombres de recurso SMB para resolver conflictos, o sustituya el punto de montaje o el nombre de recurso SMB de manera individual para cada recurso compartido.

Use el procedimiento siguiente para clonar un paquete de replicación.

1. En el destino de replicación, navegue hasta `shares replication packages` y muestre los paquetes.

```
target:> shares replication packages
target:shares replication packages> list
```

ID	STATE	DATA	TIMESTAMP	SOURCE	DATASET
package-002	idle	2019-10-02	19:26:37	hostsource	berries
package-001	idle	2019-10-02	19:26:10	hostsource	berries
package-004	idle	2019-10-02	20:53:51	hostsource	berries/blackberry
package-003	recv	2019-10-02	20:59:52	hostsource	cherries/maraschino

Las entradas se ordenan por source, dataset y data timestamp, respectivamente. La instantánea de réplica más reciente se indica mediante data timestamp.

2. Seleccione el paquete de replicación que desea clonar.

```
target:shares replication packages> select package-001
```

3. Introduzca `clone` para crear un proyecto de clonación nuevo.

```
target:shares replication package-001> clone
target:shares replication package-001 clone>
```

4. Defina `target_project` con el nombre del proyecto.

El nombre del proyecto debe ser único; de lo contrario, la operación de clonación generará un fallo.

El nombre de un proyecto debe tener de 1 a 64 caracteres, pero no puede tener espacios ni comenzar con un punto. Los caracteres permitidos son: caracteres alfanuméricos y caracteres especiales (`_ - . :`).

```
target:shares replication package-001 clone> set target_project=clone
target_project = clone
```

5. Introduzca `conflicts` para comprobar si hay conflictos.

Si hay algún conflicto, aparece un mensaje similar al siguiente.

```
target:shares replication package-001 clone> conflicts

Cloning cannot proceed because the following shares have mountpoints
or SMB resource names that are invalid or conflict with those of
other shares (either on the system or also being failed over).
Please specify valid mountpoints or SMB resource names for
these shares:
```

SHARE	MOUNTPOINT	SHARESMB
share1	/export/share1	share1
clothes	/export/clothes (inherited)	clothes (inherited)
electronics	/export/electronics	electronics
furniture	/export/furniture (inherited)	furniture (inherited)
groceries	/export/groceries (inherited)	groceries (inherited)
health	/export/health (inherited)	health (inherited)
toys	/export/toys	toys

```
target:shares replication packages package-001 clone>
```

Nota - El comando `conflicts` se puede usar en cualquier momento durante el procedimiento para comprobar la existencia de conflictos de punto de montaje o de asignación de nombres.

6. (Opcional) Configure las propiedades del nivel del proyecto para resolver los conflictos relacionados con los recursos compartidos que heredan propiedades de un proyecto.

Use el comando `get` para ver las propiedades del clon.

```
target:shares replication package-001 clone> get
target_project = clone2
rename_suffix =
original_mountpoint = /export
mountpoint = /export/clone
original_smb_resource_name = off
smb_resource_name = off
```

La propiedad `mountpoint` muestra el punto de montaje actual. La propiedad `smb_resource_name` muestra el nombre de recurso actual.

a. Introduzca un punto de montaje del nivel del proyecto que sea único para el clon.

Esta configuración se aplica a los recursos compartidos que heredan un punto de montaje de un proyecto. Use `set mountpoint` para especificar un punto de montaje único para el clon.

```
target:shares replication package-001 clone> set mountpoint=/export/clone
mountpoint = /export/clone
```

b. Introduzca un nombre de recurso SMB del nivel del proyecto que sea único.

Esta configuración se aplica a los recursos compartidos que heredan el nombre de recurso SMB de un proyecto. Configure `smb_resource_name` en un nombre de recurso SMB único.

```
target:shares replication package-001 clone> set smb_resource_name=clone
smb_resource_name = clone
```

c. Configure `rename_suffix` para resolver los demás conflictos de recursos compartidos.

Esta propiedad crea un sufijo que se agrega a un punto de montaje o a nombres de recurso SMB, si existiera algún conflicto.

```
target:shares replication package-001 clone> set rename_suffix=-clone
rename_suffix = -clone
```

Nota - Esta operación sustituye la herencia. Por ejemplo, si un recurso compartido originalmente hereda su punto de montaje del proyecto pero el nombre del punto de montaje se modifica con un sufijo durante la operación de clonación, el recurso compartido en el proyecto clonado nuevo ya no hereda el punto de montaje, sino que usa el punto de montaje único con el nombre modificado.

7. (Opcional) Para configurar propiedades para un recurso compartido individual:

a. Seleccione un recurso compartido.

```
target:shares replication package-001 clone> select share1
```

b. Sustituya el nombre de punto de montaje o recurso de SMB.

En el siguiente ejemplo, se sustituye el punto de montaje para el recurso compartido.

```
target:shares replication package-001 clone share1> set mountpoint=/export/appliances-clone
target:shares replication package-001 clone share1> set sharesmb=appliances-clone
```

8. Introduzca `confirm commit` para iniciar la operación de clonación.

```
target:shares replication package-001 clone> confirm commit
```

Si se detecta algún conflicto de nombre, aparece un mensaje similar al siguiente:

```
Cloning cannot proceed because the following shares have
mountpoints or SMB resource names that are invalid or conflict
with those of other shares (either on the system or also being
failed over). Please specify valid mountpoints or SMB resource
names for these shares:
```

SHARE	MOUNTPOINT	SHARESMB
share1	/export/share1	share1
clothes	/export/clothes (inherited)	clothes (inherited)
electronics	/export/electronics	electronics
furniture	/export/furniture (inherited)	furniture (inherited)

```
target:shares replication package-001 clone>
```

9. (Opcional) Resuelva los conflictos de nombre restantes y confirme la clonación.

Repita los pasos 6 y 7, según corresponda, hasta que no queden conflictos y, luego, introduzca `commit`.

Temas relacionados

- [“Clonación de un recurso compartido o un paquete de replicación” \[748\]](#)
- [Flujo de trabajo de replicación remota \[623\]](#)

▼ Clonación de una instantánea en un paquete de replicación (BUI)

Nota - La clonación es una característica que se ofrece con licencia. Para obtener información detallada, consulte "Acuerdo de licencia de software (SLA) de Oracle y derecho de sistemas de hardware con opciones de software integrado" y el Manual de usuario de información sobre licencias adecuado para su producto.

Nota - Las instantáneas dentro de un paquete de replicación pueden ser temporales. Es posible que las actualizaciones de replicación destruyan una instantánea de replicación para alojar las instantáneas nuevas del origen. Por lo tanto, en este procedimiento se recomienda desactivar las actualizaciones de replicación para el paquete antes de clonar la instantánea de replicación.

Use el siguiente procedimiento para clonar una instantánea de replicación dentro de un paquete de replicación.

1. Vaya al paquete que contiene el recurso compartido que desea clonar.

a. **Seleccione Recursos compartidos > Proyectos.**

b. **Haga clic en Réplica arriba de la lista de proyectos.**

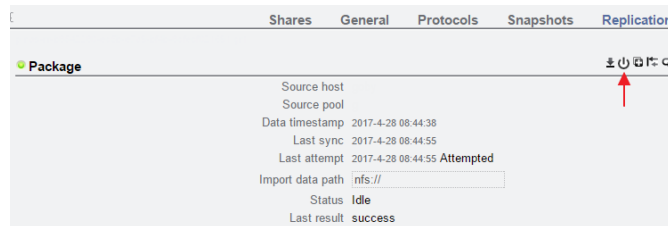
c. **Pase el cursor sobre el paquete deseado y haga clic en el ícono de edición .**

2. Suspenda las actualizaciones de replicación para el paquete de replicación.

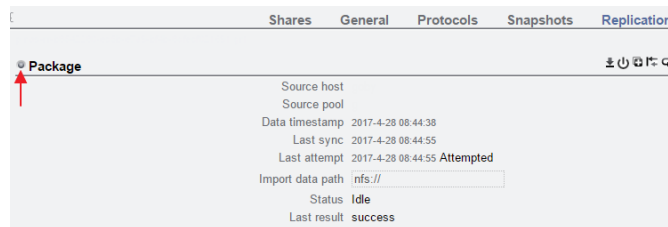
Esto desactivará por completo las actualizaciones de replicación de un paquete, lo que cancelará las actualizaciones en curso y producirá el fallo de las nuevas actualizaciones del dispositivo de origen.

a. **En la página de detalles del paquete de replicación, seleccione Replication (Replicación).**

b. **Haga clic en el ícono de encendido  para desactivar las actualizaciones de replicación.**



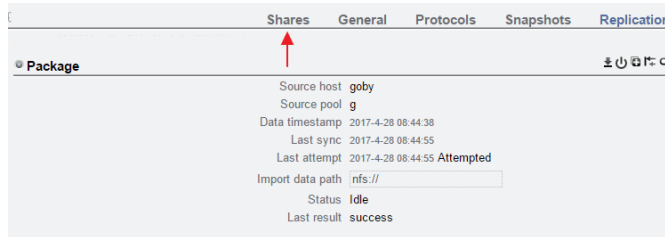
El ícono de estado que se encuentra a la izquierda indica el estado del paquete.



El paquete permanecerá desactivado hasta que lo vuelva a activar con el mismo ícono de encendido .

3. Navegue hasta el recurso compartido que desea clonar.

- a. En la página de detalles del paquete de replicación, seleccione el separador Shares (Recursos compartidos).



- b. Pase el cursor sobre un sistema de archivos o un LUN y haga clic en el ícono de edición .
- c. Haga clic en la ficha Instantáneas.
4. Pase el cursor sobre la instantánea que desea clonar y haga clic en el ícono de clonación .
5. En el cuadro de diálogo Crear clon, configure los siguientes campos.
- En el menú desplegable Proyecto, seleccione el proyecto de destino.**
Por defecto, el clon se crea dentro del proyecto actual, pero puede especificar un proyecto diferente.
 - Introduzca un nombre para el clon.**
 - (Opcional) Haga clic en el ícono de candado  que se encuentra junto a Punto de montaje y defina un punto de montaje para el clon.**
Si deja este campo bloqueado, el punto de montaje del clon seguirá siendo /export/<sharename>.
 - (Opcional) Haga clic en el ícono de candado  que se encuentra junto a Nombre de recurso e introduzca uno de los siguientes valores:**
 - **desactivado:** para desactivar SMB.
 - **on (activado):** para activar SMB, de modo que pueda compartir el clon mediante SMB. El nombre del clon en SMB coincide con el nombre del clon en el dispositivo.

- `<resource_name>`: SMB está activado, de modo que puede compartir el clon mediante SMB. El nombre del clon en SMB es el nombre que especifique aquí en lugar del nombre del clon que se indica en el dispositivo.

Si deja el campo Recurso bloqueado, la propiedad Nombre de recurso se hereda de la instantánea que está clonando.

- e. **(Opcional) Marque la casilla de control Heredar clave o desmarque esa casilla y seleccione en cambio el almacén de claves y el nombre de la clave de cifrado que desea que herede el clon.**

Si la casilla está seleccionada, el almacén de claves y el nombre de clave del clon serán los del proyecto de destino.

Si la casilla no está seleccionada, el almacén de claves y el nombre de clave del clon serán los del recurso compartido principal. De manera alternativa, seleccione otro almacén de claves y otro nombre de clave en el menú desplegable.

- f. **(Opcional) Seleccione la casilla de control Conservar otros valores de configuración local para que las propiedades heredadas se conserven como configuración local en el nuevo clon.**

Este campo determina si las propiedades heredadas provienen del juego de datos principal o del proyecto de destino. Por defecto, la casilla no está seleccionada, lo que significa que todas las propiedades heredadas para el nuevo clon provienen del proyecto de destino. Si selecciona la casilla, todas las propiedades actualmente heredadas se conservarán como configuración local en el nuevo clon.

6. **Haga clic en Aplicar para confirmar la configuración y crear el clon.**

El clon aparece en la lista de recursos compartidos para el proyecto de destino que defina. Puede trabajar con un clon como con cualquier otro recurso compartido.

Nota - Una vez que se clonó la instantánea de un paquete de replicación, ya no podrá ser destruida por las actualizaciones de replicación del origen.

7. **Vuelva a activar las actualizaciones de replicación para el paquete de replicación.**

- a. **Navegue hasta el proyecto principal del recurso compartido que acaba de clonar.**

- b. **Haga clic en el separador Replicación.**

c. **Haga clic en el ícono de energía** .

Asegúrese de que el ícono de estado que se encuentra a la izquierda sea verde, lo que indica que las actualizaciones de replicación están activadas.

Temas relacionados

- [“Clonación de un recurso compartido o un paquete de replicación” \[748\]](#)

▼ Clonación de una instantánea en un paquete de replicación (CLI)

Nota - La clonación es una característica que se ofrece con licencia. Para obtener información detallada, consulte "Acuerdo de licencia de software (SLA) de Oracle y derecho de sistemas de hardware con opciones de software integrado" y el Manual de usuario de información sobre licencias adecuado para su producto.

Nota - Las instantáneas dentro de un paquete de replicación pueden ser temporales. Es posible que las actualizaciones de replicación destruyan una instantánea de replicación para alojar las instantáneas nuevas del origen. Por lo tanto, en este procedimiento se recomienda desactivar las actualizaciones de replicación para el paquete antes de clonar la instantánea de replicación.

Use el siguiente procedimiento para clonar una instantánea de replicación dentro de un paquete de replicación.

1. **Vaya a `shares replication packages` e introduzca `list` para mostrar los paquetes de replicación disponibles.**

```
hostname:> shares replication packages
hostname:shares replication packages> list
Packages:

ID          STATE DATA_TIMESTAMP      SOURCE    DATASET
package-005 idle   2019-04-28 22:28:08 sor1     data1
package-004 idle   2019-04-28 15:44:38 sor1     data1
package-003 disbl  2019-04-27 23:46:20 sor1     data1
package-002 idle   2019-04-27 23:14:10 sor1     data1
package-001 idle   2019-04-17 17:27:05 sor2     data2
```

2. **Seleccione el paquete que contiene el recurso compartido que desea clonar.**

```
hostname:shares replication packages> select package-005
```

3. Suspenda las actualizaciones de replicación para el paquete de replicación.

Esta acción desactiva por completo las actualizaciones de replicación de un paquete, lo que cancela las actualizaciones en curso y produce el fallo de las nuevas actualizaciones del dispositivo de origen.

a. Introduzca `set enabled=false`.

```
hostname:shares replication package-005> set enabled=false
enabled = false (uncommitted)
```

b. Introduzca `commit`.

```
hostname:shares replication package-005> commit
```

4. Seleccione el proyecto que contiene el recurso compartido que desea clonar.**a. Escriba `show` para mostrar el nombre del proyecto.**

```
hostname:shares replication package-005> show
Properties:
    id = 7e184188-2738-432b-f304-123412341234de
    ...
    ...
    ...

Projects:
    proj1
```

b. Seleccione el proyecto.

```
hostname:shares replication package-005> select proj1
```

5. Seleccione el recurso compartido que desea clonar.**a. Introduzca `show` para mostrar los recursos compartidos disponibles.**

```
hostname:shares replication package-005 proj1> show
Properties:
    aclinherit = restricted
    ...
    ...
    ...

Shares:

Filesystems:

NAME      SIZE  ENCRYPTED  MOUNTPOINT
share1    36K   off       /export/share1
share2    36K   off       /export/share2
```

b. Seleccione el recurso compartido.


```
hostname:shares replication package-005 proj1> select share1
```

6. Seleccione la instantánea que desea usar para clonar el recurso compartido.

a. Introduzca `snapshots`.

```
hostname:shares replication package-005 proj1/share1> snapshots
```

b. Introduzca `list` para mostrar las instantáneas disponibles.

```
hostname:shares replication package-005 proj1/share1 snapshots> list
Snapshots:
.rr-e1401958-9f7b-47bf-8245-fa116972d26f-cb
.rr-e1401958-9f7b-47bf-8245-fa116972d26f-ec
.rr-e1401958-9f7b-47bf-8245-fa116972d26f-f2
.rr-e1401958-9f7b-47bf-8245-fa116972d26f-f3
.rr-e1401958-9f7b-47bf-8245-fa116972d26f-f4
.rr-e1401958-9f7b-47bf-8245-fa116972d26f-f5
```

```
Children:
automatic => Configure automatic snapshots
```

c. Seleccione la instantánea que desea clonar.

```
hostname:shares replication package-005 proj1/share1 snapshots> select .rr-e1401958-9f7b-47bf-8245-fa116972d26f-cb
```

7. Clone la instantánea.

a. Use el comando `clone` seguido del nombre del proyecto en el que desea crear el clon y el nombre para el clon.

```
hostname:shares replication package-005 proj1/share1@.rr-e1401958-9f7b-47bf-8245-fa116972d26f-cb> clone proj_name clone1
```

b. Use el comando `get` para ver las propiedades.

```
hostname:shares proj_name/clone1 (uncommitted clone)> get
Properties:
aclinherit = restricted (inherited)
aclmode = discard (inherited)
atime = true (inherited)
checksum = fletcher4 (inherited)
compression = off (inherited)
copies = 1 (inherited)
logbias = latency (inherited)
mountpoint = /export/clone1 (inherited)
quota = 0 (default)
readonly = false (inherited)
...
...
...
```

c. Use el comando `set` para ajustar las propiedades.

```
hostname:shares proj_name/clone1 (uncommitted clone)> set mountpoint=/export/
clone_mountpoint_name
      mountpoint = /export/clone_mountpoint_name (uncommitted)
```

- d. Use el comando `commit` para confirmar los cambios y crear el clon.

```
hostname:shares proj_name/clone1 (uncommitted clone)> commit
hostname:shares replication package-005 proj1/share1@.rr-e1401958-9f7b-47bf-8245-
fa116972d26f-cb>
```

8. Vuelva a activar las actualizaciones de replicación para el paquete de replicación.

- a. Introduzca `cd /` para volver al nivel superior.

```
hostname:shares replication package-005 proj1/share1@.rr-e1401958-9f7b-47bf-8245-
fa116972d26f-cb> cd /
```

- b. Introduzca `shares replication` y use `select` y el nombre del paquete.

```
hostname:> shares replication
hostname:shares replication> select package-005
```

- c. Use `set enabled=true` para volver a activar las actualizaciones de replicación para el paquete. A continuación, introduzca `commit` para guardar los cambios.

```
hostname:shares replication package-005> set enabled=true
      enabled = true (uncommitted)
hostname:shares replication package-005> commit
```

9. Compruebe el destino del proyecto especificado para ver el clon.

- a. Introduzca `cd /` para volver al nivel superior.

```
hostname:shares replication package-005> cd /
```

- b. Use `shares select` con el proyecto que usó para destino del clon.

```
hostname:> shares select proj_name
```

- c. Introduzca `show` para mostrar los recursos compartidos y busque el recurso compartido clonado.

```
hostname:shares proj_name> show
Properties:
      aclinherit = restricted
      aclmode = discard
      ...
      ...
      ...

Shares:
```

Filesystems:

NAME	SIZE	ENCRYPTED	MOUNTPOINT
clone1	1K	off	/export/clone_mountpoint_name

Nota - Una vez que se clonó la instantánea de un paquete de replicación, ya no podrá ser destruida por las actualizaciones de replicación del origen.

Temas relacionados

- [“Clonación de un recurso compartido o un paquete de replicación” \[748\]](#)

▼ Corte de un paquete de replicación (BUI)

Antes de empezar

Compruebe que no haya conflictos de nombres de punto de montaje o recurso compartido de SMB entre los sistemas de archivos replicados y otros sistemas de archivos del sistema. Para resolver conflictos de puntos de montaje (o conflictos de nombres de recurso de SMB), cambie los puntos de montaje del proyecto o los recursos compartidos (o los nombres de recurso de SMB) en el paquete de replicación antes de cortar un paquete de replicación. Para obtener más información, consulte [“Corte de replicación” \[789\]](#).

1. Navegue hasta el paquete de replicación.
2. Haga clic en el separador Replicación.
3. Haga clic en el ícono de corte .
4. Introduzca un nombre para el nuevo proyecto local.

Nota - Si se realiza una actualización de replicación durante una operación del servidor o después de ella, la actualización falla y se muestra la alerta correspondiente. La acción de replicación se desactiva, lo que hace que no haya más actualizaciones desde esta acción para el destino de replicación.

Temas relacionados

- [“Corte de replicación” \[789\]](#)
- [“Conceptos de replicación remota” \[708\]](#)

▼ Corte de un paquete de replicación (CLI)

Antes de empezar Compruebe que no haya conflictos de nombres de punto de montaje o recurso compartido de SMB entre los sistemas de archivos replicados y otros sistemas de archivos del sistema. Para resolver conflictos de puntos de montaje (o conflictos de nombres de recurso de SMB), cambie los puntos de montaje del proyecto o los recursos compartidos (o los nombres de recurso de SMB) en el paquete de replicación antes de cortar un paquete de replicación. Para obtener más información, consulte [“Corte de replicación” \[789\]](#).

1. **En el destino de replicación, navegue hasta el paquete de replicación.**

```
host-target:shares default replication source-001 package-001>
```

2. **Introduzca `sever` y un nombre para el proyecto local nuevo.**

```
host-target:shares default replication source-001 package-001> sever new_project
```

Nota - Si se realiza una actualización de replicación durante una operación del servidor o después de ella, la actualización falla y se muestra la alerta correspondiente. La acción de replicación se desactiva, lo que hace que no haya más actualizaciones desde esta acción para el destino de replicación.

Temas relacionados

- [“Corte de replicación” \[789\]](#)
- [“Conceptos de replicación remota” \[708\]](#)

▼ Edición de un paquete de replicación (BUI)

1. **Desde el dispositivo de destino, vaya a Recursos compartidos > Proyectos y haga clic en Réplica.**

Se muestra el nombre, el tamaño y la fecha de creación de cada paquete de replicación.

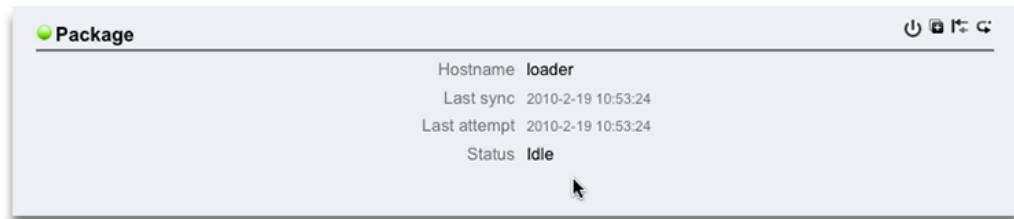


NAME ▲	SIZE	CREATION
loader: default	50.1M	2010-2-18 09:45:49
loader: default	100M	2010-2-18 13:42:25

Nota - Los paquetes se muestran en la BUI solo después del comienzo de la primera actualización de replicación. Es posible que no aparezcan en la lista hasta algún tiempo después de la finalización de la primera actualización.

2. Seleccione un paquete de replicación para editar.

Se muestra la vista Recursos compartidos del proyecto del paquete.



3. Para modificar las propiedades del paquete, haga clic en el separador Replicación.

Consulte una lista de las propiedades que puede modificar en [“Paquetes de replicación” \[747\]](#).

Temas relacionados

- [“Acciones y paquetes de replicación” \[714\]](#)
- [“Conceptos de replicación remota” \[708\]](#)

▼ Edición de un paquete de replicación (CLI)

En la CLI, los paquetes de replicación se organizan en una vista plana en `shares replication packages`, donde se muestran todos los paquetes de replicación del sistema.

1. Desde el destino de replicación, vaya a `shares replication packages` e introduzca `list` para mostrar todos los paquetes de replicación del sistema.

```
hostname:> shares replication packages
hostname:shares replication packages> list
```

ID	STATE	DATA	TIMESTAMP	SOURCE	DATASET

```

package-002 idle 2019-10-04 19:26:37 hostsource berries
package-001 idle 2019-10-04 19:26:10 hostsource berries
package-004 idle 2019-10-04 20:53:51 hostsource berries/blackberry
package-003 recv 2019-10-04 20:59:52 hostsource cherries/maraschino

```

Los paquetes se ordenan por SOURCE, DATASET y DATA_TIMESTAMP (en orden descendente).

2. Seleccione un paquete.

```

hostname:shares replication packages> select package-001
hostname:shares replication packages package-001> show

Properties:
    id = d6137c89-7056-4788-a4d1-b5892fe315e0
    source_name = hostsource
    source_asn = a751dc0f-abcd-1234-6789-f5e8315eaffa
    source_ip = 00.000.00.00:000
    source_pool = poolS
    target_pool = poolT
    replica_of = berries
    enabled = true
    state = idle
state_description = Idle (no update in progress)
    offline = false
    import_path =
data_timestamp = Fri Oct 04 2019 19:26:10 GMT+0000 (UTC)
    last_sync = Fri Oct 04 2019 19:26:10 GMT+0000 (UTC)
    last_try = Fri Oct 04 2019 19:26:10 GMT+0000 (UTC)
    last_result = success

Projects:
    berries

```

Un paquete de replicación se puede seleccionar directamente especificando su ID, como se muestra en el siguiente ejemplo:

```

hostname:shares replication packages> select d6137c89-7056-4788-a4d1-b5892fe315e0
hostname:shares replication packages package-001>

```

3. Para editar las propiedades y los recursos compartidos de los proyectos, seleccione un proyecto.

```

hostname:shares replication packages package-001> select berries
hostname:shares replication packages package-001 berries> get mountpoint
    mountpoint = /export
hostname:shares replication packages package-001 berries> get sharenfs
    sharenfs = on

```

Para obtener una lista de las propiedades de paquete que puede modificar, consulte [“Propiedades del paquete de replicación” \[723\]](#).

Temas relacionados

- [“Paquetes de replicación” \[747\]](#)
- [“Conceptos de replicación remota” \[708\]](#)

▼ Desactivación de un paquete de replicación (BUI)

En el caso de las actualizaciones de replicación de un paquete, es posible desactivarlas completamente, lo que cancela las actualizaciones en curso y anula todas las nuevas actualizaciones del dispositivo de origen.

1. **Desde el dispositivo de destino, navegue hasta el paquete.**
2. **Haga clic en el separador Replicación.**
3. **Haga clic en el ícono de energía .**

El ícono de estado de la izquierda indica el estado del paquete (activado, desactivado o con errores). El paquete queda desactivado hasta que se lo vuelva a activar mediante el mismo ícono de energía .

Temas relacionados

- [“Paquetes de replicación” \[747\]](#)
- [Replicación remota \[623\]](#)

▼ Desactivación de un paquete de replicación (CLI)

En el caso de las actualizaciones de replicación de un paquete, es posible desactivarlas completamente, lo que cancela las actualizaciones en curso y anula todas las nuevas actualizaciones del dispositivo de origen.

1. **Desde el dispositivo de destino, navegue hasta el paquete.**
2. **Modifique la propiedad `enabled`.**
3. **Confirme los cambios.**

El paquete queda desactivado hasta que se configure la propiedad `enabled`.

Temas relacionados

- [“Paquetes de replicación” \[747\]](#)
- [“Conceptos de replicación remota” \[708\]](#)

Recuperación ante desastres con replicación remota

Un sitio de recuperación ante desastres de dos sistemas está formado por un dispositivo de origen en un sitio de producción y un destino de replicación que está en un sitio de recuperación en una ubicación geográficamente distinta. En caso de producirse un fallo catastrófico en el sitio de producción, el administrador redirecciona las operaciones de los clientes al sitio de recuperación. Para ello, invierte la replicación en el destino de replicación, de modo de garantizar la continuidad de las operaciones. Cuando el sitio de producción se restaura y funciona normalmente, el administrador lo actualiza mediante la reversión de la replicación en el sitio de recuperación. Para restaurar la relación original entre origen y destino, se vuelve a revertir la replicación.

Para configurar la replicación remota para la recuperación ante desastres, realice estas tareas:

- Configuración de un dispositivo de destino en un sitio de recuperación: [BUI](#), [CLI](#)
- Conmutación de operaciones hacia el sitio de recuperación: [BUI](#), [CLI](#)
- Actualización del sitio de producción: [BUI](#), [CLI](#)
- Reversión de la replicación al sitio de producción: [BUI](#), [CLI](#)

▼ Configuración de un destino de replicación en un sitio de recuperación (BUI)

Para crear un destino de replicación para la recuperación ante desastres:

1. Identifique un destino de replicación en un sitio de recuperación.

El destino de replicación requiere una versión de software que sea compatible con el dispositivo de origen. Para más información, consulte [MOS: ID de documento 1958039.1](https://support.oracle.com/epmos/faces/DocumentDisplay?id=1958039.1) (<https://support.oracle.com/epmos/faces/DocumentDisplay?id=1958039.1>).

2. En el dispositivo de origen, cree un destino como se describe en [Creación de un destino de replicación \(BUI\)](#) [629].

3. Cree una acción de replicación y programe una replicación continua. Consulte [Creación de una acción de replicación \(BUI\)](#) [632].

Nota - La replicación continua minimiza la pérdida de datos en caso de producirse un desastre en el sitio de producción.

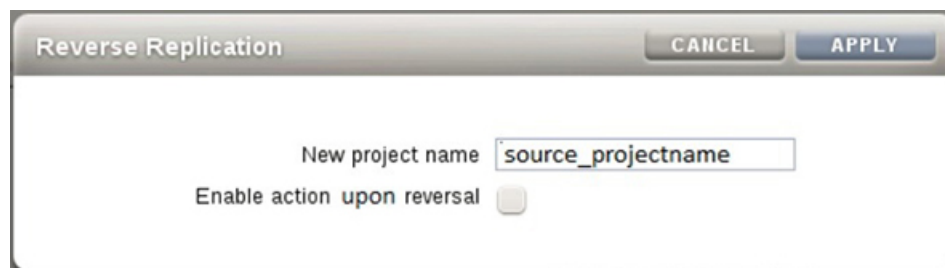
Pasos siguientes

- [Conmutación de operaciones hacia el sitio de recuperación \(BUI\) \[701\]](#)

▼ Conmutación de operaciones hacia el sitio de recuperación (BUI)

Después de producirse un fallo en el sitio de producción, realice una replicación inversa en el sitio de recuperación y, a continuación, redireccione las operaciones de los clientes hacia este sitio.

1. **En el destino de replicación, vaya a Recursos compartidos > Proyectos > Réplica y busque el paquete de replicación proveniente del dispositivo de origen.**
La réplica se llama *source_appliance:project/share*.
2. **Haga doble clic en el paquete de replicación o haga clic en el ícono de edición correspondiente .**
3. **Haga clic en el separador Replicación.**
4. **Haga clic en el ícono de reversión de dirección de replicación .**
5. **Introduzca un nombre para el nuevo proyecto local y active la acción.**
El nombre y la ubicación del proyecto de la acción original se conservan.



Nota - El nombre del proyecto debe ser único en el dispositivo en donde se realiza la operación de inversión. Si existe un proyecto con el mismo nombre en el destino en el sitio de recuperación, la operación de inversión genera un error.

6. Haga clic en Aceptar.

7. Transfiera la actividad de los clientes a la dirección IP del dispositivo que está en el sitio de recuperación.

En función del protocolo utilizado, asigne (clientes SMB) o vuelva a montar (clientes NFS) los recursos compartidos con la dirección IP o el nombre del dispositivo en el sitio de recuperación.

Pasos siguientes

- [Actualización del sitio de producción \(BUI\) \[702\]](#)

▼ Actualización del sitio de producción (BUI)

Después de haber restaurado y vuelto a poner en línea el sitio de producción, replique en el sitio de producción los cambios que se escribieron en el sitio de recuperación durante el tiempo de inactividad.

1. En el dispositivo que está en el sitio de recuperación, vaya a Recursos compartidos > Proyectos > Local y seleccione el nuevo proyecto local.

El proyecto nuevo aparece con el estado *Never synced* (Nunca sincronizado).

2. Haga clic en Sincronizar ahora para iniciar la replicación.

3. Espere hasta que finalice la replicación.

En la parte superior de la ventana, aparece el texto *Finished replicating to the new project on the source appliance* (Finalizó la replicación al nuevo proyecto en el dispositivo de origen).

Pasos siguientes

- [Reversión de la replicación al sitio de producción \(BUI\) \[703\]](#)

▼ Reversión de la replicación al sitio de producción (BUI)

Después de haber replicado todos los cambios del sitio de recuperación en el sitio de producción, vuelva a revertir la replicación para restaurar la relación de replicación original entre el origen y los destinos de replicación. Para enviar actualizaciones incrementales desde el origen nuevo hacia varios destinos configurados originalmente, consulte [“Reversión a varios destinos” \[750\]](#).

1. **En el dispositivo de producción, vaya a Recursos compartidos > Proyectos > Réplica y busque el nombre del proyecto nuevo.**
El proyecto se llama *target_appliance: new_project/share*.
2. **Seleccione el proyecto nuevo y haga clic en el ícono de edición correspondiente .**
3. **Haga clic en el separador Replicación.**
4. **Haga clic en el ícono de reversión de dirección de replicación .**
5. **En la ventana Replicación inversa, introduzca un nombre para el nuevo proyecto local y, a continuación, active la acción.**

Nota - El nombre del proyecto debe ser único en el dispositivo en donde se realiza la operación de inversión. Si existe un proyecto con el mismo nombre en el origen en el sitio de producción, la operación de inversión genera un error.

6. **En función del protocolo que use, reasigne (clientes SMB) o vuelva a montar (clientes NFS) los recursos compartidos en el dispositivo del sitio de recuperación.**
7. **Suprima el proyecto original del dispositivo de origen.**
 - a. **Vaya a Recursos compartidos > Proyectos > Local y busque el proyecto original, que debería estar vacío.**
 - b. **Seleccione el proyecto vacío y haga clic en el ícono de destrucción correspondiente .**
 - c. **Haga clic en Aceptar.**

▼ Configuración de un destino de replicación en un sitio de recuperación (CLI)

Para crear un destino de replicación para la recuperación ante desastres:

1. **Identifique un destino de replicación en el sitio de recuperación.**

El destino de replicación requiere una versión de software que sea compatible con el dispositivo de origen. Para más información, consulte [MOS: ID de documento 1958039.1 \(https://support.oracle.com/epmos/faces/DocumentDisplay?id=1958039.1\)](https://support.oracle.com/epmos/faces/DocumentDisplay?id=1958039.1).

2. **En el dispositivo de origen, cree un destino como se describe en [Creación de un destino de replicación \(CLI\)](#) [631].**

3. **Cree una acción de replicación y programe una replicación continua. Consulte [Creación de una acción de replicación \(CLI\)](#) [636].**

Nota - La replicación continua minimiza la pérdida de datos en caso de producirse un desastre en el sitio de producción.

Pasos siguientes

- [Conmutación de operaciones hacia el sitio de recuperación \(CLI\)](#) [704]

▼ Conmutación de operaciones hacia el sitio de recuperación (CLI)

Después de producirse un fallo en el sitio de producción, realice una replicación inversa en el sitio de recuperación y, a continuación, redireccione las operaciones de los clientes hacia este sitio.

1. **En el destino de replicación, introduzca `shares replication`.**

```
host-offsite:> shares replication
```

2. **Introduzca `sources` para mostrar una lista de los dispositivos de origen que están asociados con este destino.**

```
host-offsite:shares default replication> sources
```

3. **Busque el paquete replicado por el dispositivo de origen.**

En este ejemplo, `source-001` es el número del dispositivo de origen y `host-prod` es el nombre del dispositivo de origen. `kmm2` es el nombre del proyecto local en el número de paquete de replicación `package-001`.

```
source-001 host-prod
PROJECT                STATE                LAST UPDATE
package-000 <unknown>  idle                unknown
package-001 kmm2       idle                Wed May 01 2019 20:06:27 GMT+0000(UTC)
```

4. Introduzca `select` y el número de dispositivo de origen.

```
host-offsite:shares default replication sources> select source-001
```

5. Introduzca `select` y el número de paquete de replicación.

```
host-offsite:shares default replication source-001> select package-001
```

6. Introduzca `pkgreverse`.

```
host-prod:shares replication source-005 package-000> pkgreverse
```

El comando `pkgreverse` conserva las propiedades de la acción de replicación original, incluidos los programas.

7. (Opcional) Defina un nombre de proyecto nuevo y active la acción con los siguientes comandos:

```
host-prod:shares replication source-000 package-000 pkgreverse> set new_project_name=new-kmm2
new_project_name = new-kmm2
host-prod:shares replication source-000 package-000 pkgreverse> set
enable_action_upon_reversal=true
enable_action_upon_reversal = true
```

Nota - El nombre del proyecto debe ser único en el dispositivo en donde se realiza la operación de inversión. Si existe un proyecto con el mismo nombre en el destino en el sitio de recuperación, la operación de inversión genera un error.

8. Introduzca `show` para confirmar las propiedades e introduzca `commit`:

```
host-prod:shares replication source-000 package-000 pkgreverse> show
Properties:
    new_project_name = new-kmm2
    enable_action_upon_reversal = true

host-prod:shares replication source-000 package-000 pkgreverse> commit
This action will move the contents of this package to a new local project
configured to replicate back to the source. Any data or metadata changes made
on the source since the last successful update will be lost when the new
project is replicated back to the source. If replication actions on the source
are not disabled, future updates to this package will fail.
```

9. Transfiera la actividad de los clientes a la dirección IP del dispositivo que está en el sitio de recuperación.

En función del protocolo utilizado, asigne (clientes SMB) o vuelva a montar (clientes NFS) los recursos compartidos con la dirección IP o el nombre del dispositivo en el sitio de recuperación.

Pasos siguientes

- [Actualización del sitio de producción \(CLI\) \[706\]](#)

▼ Actualización del sitio de producción (CLI)

Después de restaurar y volver a poner en línea el sitio de producción, replique en el sitio de producción los cambios que se escribieron en el sitio de recuperación durante el período de interrupción.

1. **En el dispositivo que está en el sitio de recuperación, vaya a `shares` y seleccione el proyecto nuevo.**

```
host-offsite:> shares
host-offsite:shares pool> select new-kmm2
```

2. **Introduzca `list` para buscar el nombre del recurso compartido.**

```
host-offsite:shares pool new-kmm2> list
Filesystems:
NAME          SIZE  ENCRYPTED  MOUNTPOINT
karen2        31K   off       /export/karen2
host:shares pool new-kmm2> replication
host:shares pool new-kmm2 replication> show
Actions:
TARGET        STATUS      NEXT
action-000    idle       Sync now
host2
```

3. **Seleccione el número de acción y, a continuación, introduzca `sendupdate` para iniciar la replicación en el dispositivo de producción.**

```
host-offsite:shares pool new-kmm2 replication> select action-000
host-offsite:shares pool new-kmm2 action-000> sendupdate
```

4. **Espere hasta que finalice la replicación.**

Cuando la replicación finaliza, el estado cambia a `idle`.

Pasos siguientes

- [Reversión de la replicación al sitio de producción \(CLI\) \[707\]](#)

▼ Reversión de la replicación al sitio de producción (CLI)

Después de haber replicado todos los cambios del sitio de recuperación en el sitio de producción, vuelva a revertir la replicación para restaurar la relación de replicación original entre el origen y los destinos de replicación. Para enviar actualizaciones incrementales desde el origen nuevo hacia varios destinos configurados originalmente, consulte [“Reversión a varios destinos” \[750\]](#).

1. **En el destino de replicación, navegue hasta `shares replication packages` y muestre los paquetes.**

```
loader:> shares replication packages
loader:shares replication packages> list
```

ID	STATE	DATA	TIMESTAMP	SOURCE	DATASET
package-002	idle	2019-10-02	19:26:37	hostsource	berries
package-001	idle	2019-10-02	19:26:10	hostsource	berries
package-004	idle	2019-10-02	20:53:51	hostsource	berries/blackberry
package-003	recv	2019-10-02	20:59:52	hostsource	cherries/maraschino

El paquete con el `data timestamp` más reciente para este juego de datos es el que tiene los datos más actualizados para el juego de datos de origen correspondiente.

2. **Seleccione el paquete de replicación que desea revertir.**

```
loader:shares replication packages> select package-002
```

3. **Introduzca `pkgreverse`.**

```
host-prod:shares replication package-002> pkgreverse
```

4. **(Opcional) Defina un nombre de proyecto nuevo y active la acción con los siguientes comandos:**

```
host-prod:shares replication package-002 pkgreverse> set new_project_name=new-kmm3
new_project_name = new-kmm3
host-prod:shares replication package-002 pkgreverse> set enable_action_upon_reversal=true
enable_action_upon_reversal = true
```

Nota - El nombre del proyecto debe ser único en el dispositivo en donde se realiza la operación de inversión. Si existe un proyecto con el mismo nombre en el dispositivo en el sitio de producción, la operación de inversión genera un error.

5. **Introduzca `show` para confirmar las propiedades e introduzca `commit`:**

```
host-prod:shares replication package-002 pkgreverse> show
Properties:
    new_project_name = new-kmm3
    enable_action_upon_reversal = true
```

```
host-prod:shares replication package-002 pkgreverse> commit
This action will move the contents of this package to a new local project
configured to replicate back to the source. Any data or metadata changes made
on the source since the last successful update will be lost when the new
project is replicated back to the source. If replication actions on the source
are not disabled, future updates to this package will fail.
```

6. **En función del protocolo que use, reasigne (clientes SMB) o vuelva a montar (clientes NFS) los recursos compartidos en el dispositivo del sitio de producción.**

Temas relacionados

- [“Reversión de la dirección de replicación” \[790\]](#)
- [“Conceptos de replicación remota” \[708\]](#)

Conceptos de replicación remota

La replicación de Oracle ZFS Storage Appliance es una característica que se ofrece con licencia para determinados modelos y ofrece una replicación basada en instantáneas de proyectos y recursos compartidos desde un dispositivo de origen hasta uno o varios destinos de replicación. La replicación realiza una actualización completa de todo el contenido de un proyecto o un recurso compartido, seguida por actualizaciones incrementales que contienen solo los cambios que se produjeron desde la última actualización.

Para obtener información detallada sobre las licencias, consulte "Acuerdo de licencia de software (SLA) de Oracle y derecho de sistemas de hardware con opciones de software integrado" y el Manual de usuario de información sobre licencias para la versión de software.

En este tema, se describen los conceptos clave de la replicación remota (o simplemente "replicación") y la terminología relacionada con la replicación.

La replicación remota tiene las siguientes características importantes:

- **Replicación asíncrona basada en instantáneas:** el subsistema de replicación toma una instantánea como parte de cada operación de actualización. En el caso de una actualización inicial, se envía todo el contenido del proyecto o el recurso compartido. En el caso de una actualización incremental, sólo se envían los cambios desde la última instantánea de replicación para la misma acción. Dado que la replicación toma instantáneas y luego las envía, los datos ya están confirmados en el almacenamiento estable antes de que la replicación comience a enviarlos. La replicación continua envía de manera eficaz flujos continuos de cambios del sistema de archivos, pero aún es asíncrona respecto de los clientes NAS y SAN.
- **Nivel de bloque:** cada operación de actualización recorre el sistema de archivos en el nivel de bloque y envía los metadatos y datos del sistema de archivos adecuados hacia el destino.

- **Incluye todos los metadatos:** el flujo de replicación subyacente serializa los datos de usuario y los metadatos, incluida la mayoría de las propiedades configuradas en la pantalla Recursos compartidos. Estas propiedades se pueden modificar en el destino después de finalizar la primera actualización de replicación, aunque no surtirá efecto por completo hasta cortar la conexión de replicación. Por ejemplo, esto permite el uso compartido mediante NFS hacia un conjunto de hosts diferentes al origen. Para obtener más información, consulte [“Paquetes de replicación” \[747\]](#).
- **Seguridad:** la capa de conexión segura (SSL) se usa siempre para garantizar el uso del protocolo de control de replicación con los productos Oracle ZFS Storage Appliance y, opcionalmente, con las transferencias de datos de replicación. El dispositivo puede realizar operaciones de replicación con otro dispositivo de origen o destino únicamente después de un proceso de autenticación manual. Para obtener más información, consulte [“Destinos de replicación” \[711\]](#).
- **Recursos compartidos y proyectos cifrados:** cuando esta opción está activada, se usa cifrado transparente de los datos para proteger los recursos compartidos individuales (sistemas de archivos y LUN) y los proyectos. Para obtener más información, consulte [Cifrado de datos \[795\]](#).
- **Independiente del protocolo:** el dispositivo admite volúmenes de almacenamiento de archivos y basados en bloques. El mecanismo de replicación es independiente del protocolo.
- **Replicación comprimida:** la compatibilidad con flujos de replicación comprimidos aumenta el rendimiento de la replicación y mejora el aprovechamiento del rendimiento entre varias ubicaciones que tengan conexiones de ancho de banda limitadas. Para obtener más información, consulte [“Replicación comprimida” \[746\]](#).

La replicación tiene las siguientes limitaciones conocidas:

- No es posible mover acciones entre agrupaciones
- El rendimiento de red se limita a un máximo de 200 MB/s por replicación de nivel de proyecto. Con la replicación comprimida, la velocidad de transmisión de datos efectiva puede superar la velocidad de transmisión de datos real de la red física.

Para obtener información acerca de los conceptos de replicación remota, consulte:

- [“Terminología de replicación” \[710\]](#)
- [“Destinos de replicación” \[711\]](#)
- [“Acciones y paquetes de replicación” \[714\]](#)
- [“Propiedades de las acciones de replicación” \[716\]](#)
- [“Agrupaciones de almacenamiento de replicación” \[724\]](#)
- [“Replicación de proyectos frente a replicación de recursos compartidos” \[725\]](#)
- [“Autorizaciones de replicación” \[726\]](#)
- [“Replicación con deduplicación” \[727\]](#)
- [“Configuración de replicación para dispositivos agrupados en clusters” \[729\]](#)

- [“Ejemplo: Configuración de replicación para dispositivos agrupados en clusters” \[730\]](#)
- [“Instantáneas de replicación y coherencia de datos” \[737\]](#)
- [“Gestión de instantáneas de replicación” \[738\]](#)
- [“Configuraciones de iSCSI y replicación” \[741\]](#)
- [“Replicación reanudable” \[742\]](#)
- [“Alertas de replicación” \[742\]](#)
- [“Fallos de replicación” \[744\]](#)
- [“Replicación comprimida” \[746\]](#)
- [“Paquetes de replicación” \[747\]](#)
- [“Clonación de un recurso compartido o un paquete de replicación” \[748\]](#)
- [“Reversión a varios destinos” \[750\]](#)
- [“Replicación en cascada” \[768\]](#)
- [“Exportación de sistemas de archivos replicados” \[788\]](#)
- [“Corte de replicación” \[789\]](#)
- [“Reversión de la dirección de replicación” \[790\]](#)
- [“Destrucción de un paquete de replicación” \[793\]](#)
- [“Copias de seguridad de réplicas de destino” \[793\]](#)

Terminología de replicación

En la siguiente lista, se detallan términos comunes de replicación.

- **Clon:** paquete replicado que se puede clonar y convertir en un proyecto mutable. Un clon se puede gestionar como cualquier otro proyecto del sistema.
- **Sincronización completa o actualización completa:** operación de replicación que envía todo el contenido de un proyecto y algunos de sus recursos compartidos. La sincronización inicial de un proyecto o un recurso compartido siempre es una sincronización completa.
- **Actualización incremental:** operación de replicación que envía solo las diferencias de un proyecto y sus recursos compartidos desde la actualización anterior (independientemente de si dicha actualización era completa o incremental).
- **Objetivo de punto de recuperación (RPO):** cantidad máxima tolerable de pérdida de datos, expresada en unidad de tiempo, en caso de desastre o una interrupción de servicio importante. El RPO se define como parte de un plan de recuperación ante desastres y representa el último juego de datos coherente disponible para recuperación. Cuanto menor sea el valor del RPO, menor será la pérdida de datos.
- **Réplica:** datos replicados incluidos en el paquete de replicación en el destino de replicación.
- **Acción de replicación:** describe los datos que se replican, el programa de replicación y las propiedades de la transferencia de datos, por ejemplo, si está activado o desactivado el cifrado del enlace de red. Consulte [“Propiedades de las acciones de replicación” \[716\]](#).

- **Grupo de replicación:** conjunto de juegos de datos (exactamente un proyecto y algunos recursos compartidos) replicados como unidad. Consulte [“Replicación de proyectos frente a replicación de recursos compartidos”](#) [725].
- **Paquete de replicación:** existe en el destino de replicación y está asociado con una acción de replicación. Es un objeto especial que contiene la réplica. Un paquete de replicación se puede exportar, clonar, cortar o revertir, lo que permite acceso de escritura a los datos dentro del proyecto.
- **Origen de replicación:** dispositivo que envía actualizaciones de replicación a uno o varios dispositivos de destino de manera periódica, continua o a petición. Los dispositivos individuales pueden actuar como origen y *destino*, pero actuarán solo como uno de ellos en el contexto de una *acción* de replicación en particular.
- **Destino de replicación:** dispositivo que recibe y almacena los datos replicados provenientes de uno o varios dispositivos de *origen*. Además, este término hace referencia a un objeto de configuración del dispositivo que permite replicar hacia otro dispositivo.
- **Replicación inversa:** relación de replicación que intercambia los roles de origen y destino. Después de una recuperación ante desastres, los roles se pueden volver a invertir.

Destinos de replicación

Un destino de replicación puede ser lo siguiente:

- Una agrupación diferente en el dispositivo de origen.
- Un servidor NFS aparte para la replicación fuera de línea.

Al crear un destino de replicación, primero introduzca un nombre para el destino. Este nombre se utiliza para identificar el destino en la BUI y la CLI del dispositivo de origen.

Establecimiento de una conexión segura

El destino de replicación y el dispositivo de origen establecen una conexión que permite la comunicación segura entre un origen y un destino. Para establecer la conexión, proporcione la siguiente información:

- Nombre de dominio completo o dirección IPv4 del dispositivo de destino: el valor que se recomienda utilizar es el nombre de dominio del destino.
- Contraseña root del destino de replicación: esto autoriza al administrador a configurar la conexión en el destino de replicación.

El origen y el destino intercambian claves que utilizan para identificarse entre sí de manera segura en las comunicaciones posteriores. Estas claves se almacenan como parte de la

configuración del dispositivo, y se conservan en reinicios y actualizaciones. Estas claves se pierden cuando se realiza una reinstalación o un restablecimiento de fábrica del dispositivo.

La contraseña root nunca se almacena permanentemente. Un cambio en la contraseña root del destino o del origen no requiere cambios en la configuración de replicación. Nunca se transmite la contraseña sin cifrar. El intercambio de identidad inicial y todas las otras operaciones de replicación se protegen con SSL.

Si necesita comprobar que el tráfico de replicación se transmite a través de una interfaz de red específica, configure una ruta estática para el destino que especifique esa interfaz como se muestra en Configuración de interfaces de red y enrutamiento estático [BUI](#), [CLI](#).

Verificación del certificado de destino

Cuando crea un destino de replicación, se realiza la verificación del certificado. La verificación del certificado consta de los siguientes pasos:

1. Comprobación de nombre de host del certificado
2. Comprobación de confianza del certificado

Si se produce un error en la comprobación de nombre de host o la comprobación de confianza, no se crea el destino.

Comprobación de nombre de host

El valor de la propiedad `hostname` puede ser un nombre de dominio completo o una dirección IPv4. El valor recomendado para usar es el nombre de dominio completo de destino.

La comprobación de nombre de host verifica que el nombre de host especificado para el destino coincida con el host especificado en el certificado. Si se especifica una dirección IP o un nombre de dominio no completo para el nombre de host, y el certificado solo contiene nombres de dominio completos, se produce un error en la comprobación de nombre de host y no se crea el destino.

Si el destino utiliza un certificado basado en ASN, especifique el nombre de dominio completo del destino para el valor de la propiedad `hostname`.

La comprobación del nombre de host se realiza por defecto. Es posible desactivar la opción `Host Match` (Coincidencia de host) para omitir la comprobación de nombre de host.

Para potenciar la seguridad, establezca el nombre de dominio completo del destino como valor de la propiedad `nombre de host` y asegúrese de que la opción `Host Match` (Coincidencia de host) esté activada.

Comprobación de confianza del certificado

La verificación de confianza del certificado verifica que uno de los siguientes certificados se haya agregado a la lista de certificados de confianza de origen y esté habilitado para uso entre pares:

- El certificado del dispositivo de destino.
- El certificado de la autoridad de certificación que emitió el certificado del dispositivo de destino.

El certificado se verifica cuando se crea o se edita un destino, y cada vez que el origen y el destino intentan conectarse. El usuario también puede comprobar la conexión en cualquier momento.

- Creación de un destino. Cuando agregue un destino, si el certificado no es de confianza para el origen, se presentará el certificado para que usted lo revise y se le solicitará aceptar o rechazar el certificado. Si acepta el certificado, este se agregará a la lista de confianza del origen y se creará el destino. Si rechaza el certificado, este no se agregará a la lista de confianza del origen y no se creará el destino. Si el certificado ya es de confianza, se creará el destino y no se le solicitará que acepte el certificado.

Una vez creado el destino, su certificado puede dejar de ser de confianza. Por ejemplo, el administrador de origen podría suprimir el certificado de la lista de certificados de confianza o el administrador de destino podría reemplazar el certificado.

- Edición de un destino. Cuando aplique cambios, si el certificado no es de confianza para el origen, se presentará el certificado para que usted lo revise y se le solicitará aceptar o rechazar el certificado. Si acepta el certificado, este se agregará a la lista de confianza del origen. Si rechaza el certificado, este no se agregará a la lista de confianza del origen.
- Prueba de conexión. Puede comprobar si el certificado es de confianza en cualquier momento. Si el certificado no es de confianza para el origen, se presentará el certificado para que usted lo revise y se le solicitará aceptar o rechazar el certificado. Consulte Prueba de la conexión [BUI](#), [CLI](#).
- Conexión de replicación y de pares. La verificación de confianza del certificado se realiza para cada par y conexión de replicación. Si el certificado no es de confianza, el origen rechaza la conexión.

Temas relacionados

- Creación de un destino de replicación: [BUI](#), [CLI](#)
- Prueba de la conexión: [BUI](#), [CLI](#)
- Edición de un destino de replicación: [BUI](#), [CLI](#)

Otras consideraciones sobre el destino de replicación

Si el origen de replicación usa NIS o LDAP y asigna directamente los usuarios o los grupos de este servicio en la configuración del recurso compartido, la configuración equivalente debe

estar presente en el destino de replicación. De lo contrario, las operaciones de reversión y corte de replicación pueden presentar fallos.

De forma predeterminada, la conexión del destino de replicación no es bidireccional. Por ejemplo, si un administrador configura la replicación del origen *S* al destino *T*, el destino *T* no puede usar automáticamente *S* como destino. Sin embargo, se admite la reversión de la dirección de la replicación. Esta crea automáticamente un destino para *S* en *T* (si todavía no existe) de manera que se pueda volver a replicar *T* en *S*. Para obtener más información, consulte [“Reversión de la dirección de replicación” \[790\]](#).

Temas relacionados

- Creación de un destino de replicación: [BUI](#), [CLI](#).
- [Flujo de trabajo de replicación remota \[623\]](#)
- [“Conceptos de replicación remota” \[708\]](#)

Acciones y paquetes de replicación

Una acción de replicación especifica dónde y cómo replicar un proyecto o recurso compartido. Las acciones de replicación se crean en el dispositivo de origen con la siguiente información:

- Un grupo de replicación que incluye un proyecto o recursos compartidos individuales
- Nombre del destino de replicación
- El nombre de una agrupación de almacenamiento en el destino de replicación (usada únicamente durante la instalación inicial)
- La frecuencia (programada o continua) de la actualización
- Número de instantáneas automáticas (Instantáneas planificadas) retenidas en el destino
- Opciones adicionales, por ejemplo, el cifrado del flujo de datos o la desactivación de la compresión

Un grupo de replicación se especifica de manera implícita en el proyecto o el recurso compartido en donde se configura la acción (consulte [“Agrupaciones de almacenamiento de replicación” \[724\]](#)). La agrupación de almacenamiento y el destino de replicación no se pueden cambiar después de crear la acción; sin embargo, las otras acciones se pueden modificar en cualquier momento. Si hay una actualización de replicación en curso cuando se modifica una opción, el valor nuevo se aplica cuando comienza la siguiente actualización (a excepción del parámetro `max bandwidth`, que se aplica inmediatamente después de la modificación).

Cuando se crea una acción de replicación en el dispositivo de origen, se crea un paquete en el destino en la agrupación de almacenamiento especificada. El paquete que está en el destino de replicación contiene una copia exacta del proyecto de origen y los recursos compartidos donde se configura la acción a partir de la fecha de inicio de la última actualización de replicación. Las acciones son la unidad principal de la configuración de replicación del dispositivo.

Frecuencia de actualización de replicación

Las replicaciones se pueden ejecutar manualmente o se las puede configurar en la acción de replicación para enviarlas de manera continua o a horas programadas. Los tres modos de replicación son:

- **Manual:** el administrador inicia la replicación manualmente en cualquier momento. Una actualización de replicación manual puede ser útil para realizar pruebas y para aplicaciones que requieren que los datos estén en un estado específico para que se pueda realizar la replicación. Consulte Envío manual de una actualización de replicación [BUI](#), [CLI](#).
- **Programada:** la replicación se ejecuta automáticamente en función de un programa seleccionado. La frecuencia programada se puede configurar para replicar en el destino cada 5, 10, 15, 20 o 30 minutos; cada 1, 2, 4, 8 o 12 horas; cada día, cada semana o cada mes. Se pueden configurar frecuencias de actualización más granulares mediante la definición de varios programas para una misma acción de replicación.

La selección **Auto**, que está disponible al crear el primer programa para una acción de replicación, es una hora de inicio generada por el dispositivo. Cuando se configuran varias acciones de replicación en el dispositivo, la hora de inicio generada automáticamente puede minimizar la superposición de actualizaciones de replicación y mejorar el equilibrio de carga.

Update frequency ☒ Scheduled ☐ Continuous

+ Schedule **⋮ Snapshots**

FREQUENCY

every half hour scheduled time: Auto minutes past the hour

La frecuencia programada también se puede configurar para que replique en el destino según los programas de instantáneas automáticas configurados en el proyecto o recurso compartido. Cuando se selecciona esta opción, las actualizaciones de replicación se realizan cuando se crean las instantáneas automáticas programadas.

Update frequency ☒ Scheduled ☐ Continuous

+ Schedule **⋮ Snapshots**

FREQUENCY

auto-snapshots

- **Continua:** la replicación se ejecuta de manera continua. Tan pronto como se finaliza una actualización de replicación, se inicia la actualización subsiguiente. Los cambios se transmiten con la mayor frecuencia posible, lo que genera el envío de un flujo constante

de todos los cambios del sistema de archivos al sistema de destino. En el caso de los sistemas de archivos con mucha renovación (se crean y se destruyen muchos archivos en intervalos breves), puede ocasionar una réplica de muchos más datos que lo que es realmente necesario. Sin embargo, en tanto y en cuanto la replicación pueda mantenerse a la par de los cambios de datos, se perderá una cantidad mínima de datos en caso de desastre ante pérdida de datos en el sistema de origen.

Relación de paquetes y acciones de replicación

La acción de replicación y el paquete están vinculados entre sí. Si el paquete se daña o se destruye de alguna manera, la acción no puede enviar actualizaciones de replicación, incluso si el destino aún tiene los datos y las instantáneas asociadas con la acción. Del mismo modo, si se destruye la acción, el paquete no podrá recibir nuevas actualizaciones de replicación (incluso si el origen aún tiene los mismos datos y las mismas instantáneas). Si se intenta realizar una operación que destruiría la conexión entre la acción y el paquete, se genera una advertencia tanto en la BUI como en la CLI. Si un error o una operación administrativa explícita interrumpen la conexión entre la acción y el paquete de tal manera que ya no fuera posible realizar una actualización incremental, debe cortar o destruir el paquete y la acción, y después generar una nueva acción en el origen.

Nota - El dispositivo evita la destrucción de datos en el destino, a menos que lo solicite explícitamente el administrador. Como resultado, si se produce un fallo en la actualización de replicación inicial de una acción después de replicar algunos datos y se dejan datos incompletos dentro del paquete, se producirán fallos en las actualizaciones de replicación posteriores con la misma acción porque el dispositivo no podrá sobrescribir los datos antes recibidos. Para resolver esta situación, los administradores deben destruir el paquete y la acción existentes, crear una nueva acción y reiniciar la replicación.

Temas relacionados

- [“Propiedades de las acciones de replicación” \[716\]](#)
- [“Paquetes de replicación” \[747\]](#)

Propiedades de las acciones de replicación

Las propiedades de las acciones de replicación que se ven en la BUI y la CLI son diferentes, como se describe en las siguientes tablas.

- [Tabla 143, “Propiedades de las acciones de replicación \(BUI y CLI\)”](#)
- [Tabla 144, “Propiedades de acciones de replicación \(CLI, solo lectura\)”](#)
- [Tabla 145, “Nodos secundarios de las acciones de replicación \(solo CLI\)”](#)

- [Tabla 146, “Propiedades de nodo de estadísticas de acciones de replicación \(CLI, solo lectura\)”](#)

Nota - Cuando cambia una propiedad de acción de replicación, la configuración nueva entra en efecto con la siguiente actualización de replicación, a menos que se especifique lo contrario.

En la siguiente tabla, se describen las propiedades de las acciones de replicación que se encuentran disponibles en la BUI y la CLI.

TABLA 143 Propiedades de las acciones de replicación (BUI y CLI)

Propiedad de la BUI	Propiedad de la CLI	Descripción
Desactivar compresión	compression	Por defecto, el flujo de replicación se comprime. Si la compresión se proporciona por otro medio, por ejemplo, un acelerador de WAN, desactive la compresión. Para obtener más información, consulte “Replicación comprimida” [746] .
Destino distante	distant_target	En una configuración de replicación en cascada y reversión de varios destinos, esta opción define la transformación de la topología durante la reversión en el origen potencial. Se puede establecer solamente en el nivel de proyecto para acciones que no sean en cascada cuando <code>potential_target</code> se define en <code>TRUE</code> . Para obtener más información, consulte “Replicación en cascada” [768] .
Frecuencia de actualización	continuous	En la BUI, seleccione la frecuencia de actualización Programada o Continua. En la CLI, establezca la propiedad <code>continuous</code> en <code>true</code> o <code>false</code> . Para obtener más información, consulte Frecuencia de actualización de replicación .
Activar deduplicación	dedup	Cuando está configurada, activa la deduplicación en los flujos de replicación. Para obtener más información, consulte “Replicación con deduplicación” [727] .
Ícono de encendido 	enabled	Cuando está activada (<code>true</code> en la CLI), se pueden enviar actualizaciones de replicación. Cuando está desactivada (<code>false</code> en la CLI), el ícono de encendido  no aparece resaltado y no se pueden enviar actualizaciones de replicación.
Ruta de exportación de datos	export_path	Especifica la ruta de un recurso compartido de NFS para esta acción, con el formato: <code>nfs://server/path</code> . Esta propiedad exporta el flujo de replicación a un archivo que está en un servidor NFS, el cual se puede transportar físicamente a la ubicación de destino remota y, a continuación, importarlo a un destino de replicación. Para conocer los procedimientos, consulte Creación de una replicación fuera de línea BUI, CLI .

Propiedad de la BUI	Propiedad de la CLI	Descripción
Incluir origen de clon como datos	<code>include_clone_origin_as_data</code>	Permite controlar la replicación de cada recurso compartido que se clonó a partir de un recurso compartido que es externo al paquete de replicación en el destino. Seleccione esta opción para insertar una copia completa de los datos de la instantánea de origen del clon en la réplica del clon. Si anula la selección de esta opción, un clon creado a partir de una instantánea de origen externa compartirá almacenamiento con la réplica de la instantánea de origen del clon que reside en la agrupación del destino de la replicación. El uso compartido del almacenamiento permite ahorrar espacio, pero si el destino de replicación no contiene la instantánea de origen del clon externo, la replicación del clon generará un error. Para obtener información detallada, consulte “Clonación de un recurso compartido o un paquete de replicación” [748] .
Incluir instantáneas	<code>include_snaps</code>	Determina si las actualizaciones de replicación incluyen instantáneas de no replicación. Para obtener información detallada, consulte “Gestión de instantáneas de replicación” [738] .
Límite de ancho de banda	<code>max_bandwidth</code>	Especifica una velocidad máxima para esta actualización de replicación (en términos de cantidad de datos transferidos por la red por segundo). Use esta propiedad para limitar el ancho de banda, especialmente durante una actualización de replicación inicial. Si cambia esta propiedad durante una actualización de replicación, la configuración nueva entra en efecto de inmediato.
Agrupación	<code>pool</code>	Agrupación de almacenamiento en el destino donde se replicará este proyecto. Esta propiedad se especifica cuando se configura inicialmente una acción y no se muestra en lo sucesivo.
Origen potencial	<code>potential_source</code>	Cuando se configura la reversión de varios destinos, el destino correspondiente puede realizar una reversión del paquete. Se puede establecer solamente en el nivel de proyecto para acciones que no sean en cascada. Para obtener más información, consulte “Reversión a varios destinos” [750] .
Objetivo de punto de recuperación [☐] <i>unit of time</i>	<code>recovery_point_objective</code>	Especifica la cantidad máxima tolerable de pérdida de datos en caso de desastre o una interrupción de servicio importante. El objetivo de punto de recuperación (RPO) se puede especificar en días, horas, minutos o segundos. Configure esta propiedad al crear o editar una acción de replicación. Esta propiedad solo se usa en conjunto con las alertas de error y de advertencia de demora de réplica.

Propiedad de la BUI	Propiedad de la CLI	Descripción
Alerta de error de demora de réplica [] Porcentaje de objetivo de punto de recuperación	replica_lag_error_alert	Especifica un límite representado como porcentaje del RPO. El dispositivo de origen genera una alerta mayor cuando la demora de réplica excede el límite especificado. Cuando la demora de réplica cae por debajo de este valor, una alerta menor indica que la demora de réplica está dentro del límite de error.
Alerta de advertencia de demora de réplica [] Porcentaje de objetivo de punto de recuperación	replica_lag_warning_alert	Especifica un límite representado como porcentaje del RPO. El dispositivo de origen genera una alerta menor cuando la demora de réplica excede el límite especificado. Cuando la demora de réplica cae por debajo de este valor, una alerta menor indica que la demora de réplica está dentro del límite de advertencia.
Retener instantáneas de usuario en destino	retain_user_snaps_on_target	Conserva las instantáneas generadas por el usuario en el destino de la replicación para la acción asociada, incluso después de que las instantáneas se destruyen en el dispositivo de origen. Las instantáneas conservadas en el destino se pueden utilizar como parte de una solución de copia de seguridad de datos o de disco a disco. Para obtener detalles, consulte “Gestión de instantáneas generadas por el usuario” [677] .
Destino	target	Identificador único del sistema de destino de replicación. Esta propiedad se especifica cuando se configura inicialmente una acción y no se puede editar.
ID de paquete de destino	target_pkgid	Solo lectura. ID del paquete de replicación en el dispositivo de destino. A partir de OS8.8.0, es posible que <code>package id</code> y <code>action id</code> no coincidan en algunos casos.
Agrupación de destino	target_pool	Agrupación de almacenamiento en el destino donde se replicará este proyecto. Esta propiedad se muestra al editar una acción de replicación existente.
Activar cifrado SSL	use_ssl	Cuando se configura, cifra datos en el cable mediante SSL. El uso de esta función puede afectar el rendimiento de la replicación por acción.
Demora de actualización de cascada	update_cascade_delay	La demora de actualización cuando se utiliza con la opción de programación de replicación en cascada <code>after_update</code> . En la BUI, en Programación en cascada cuando se selecciona Después de la actualización. Para obtener más información, consulte “Replicación en cascada” [768] .

En la siguiente tabla, se describen las propiedades de las acciones de replicación que se encuentran disponibles solamente en la CLI. Todas estas propiedades son de solo lectura.

TABLA 144 Propiedades de acciones de replicación (CLI, solo lectura)

Propiedad de la CLI	Descripción
average_throughput	Describe el rendimiento de replicación promedio.
bypassed_id	ID de la acción de replicación en cascada que se omitió. Se activa la localización de una acción omitida. Disponible solamente después de ejecutar el procedimiento de redireccionamiento/omisión que se describe en “Replicación en cascada” [768] .
bytes_sent	Número de bytes enviados al destino de replicación.
estimated_size	Tamaño estimado de los datos para replicar.
estimated_time_left	Tiempo estimado restante hasta la finalización de la actualización de replicación.
export_pending	Indica si hay una exportación pendiente. El valor es <code>true</code> o <code>false</code> .
id	Identificador único de la acción de replicación. El identificador se puede usar para seleccionar una acción o el paquete de replicación asociado mediante la siguiente sintaxis: <code>select id=<uniqueid></code> .
next_update	Fecha y hora del próximo intento. Este valor podría ser una fecha (para una actualización programada), <code>sync now</code> o <code>continuous</code> .
offline	Indica si la actualización de replicación está fuera de línea. El valor es <code>true</code> o <code>false</code> .
origin_pkg_id	Identificador único del paquete de replicación del cual se creó esta acción cuando se revirtió el paquete. El identificador del paquete de origen se muestra después de que finaliza la primera actualización de replicación correcta.
replica_lag	Demora de réplica actual con el formato <code>hh:mm:ss</code> .
replica_lag_over_error_limit	El valor es <code>true</code> si la demora de réplica superó el límite de error especificado mediante la combinación de <code>recovery_point_objective</code> y el umbral <code>replica_lag_error_alert</code> .
replica_lag_over_warning_limit	El valor es <code>true</code> si la demora de réplica superó el límite de advertencia especificado mediante la combinación de <code>recovery_point_objective</code> y el umbral <code>replica_lag_warning_alert</code> .
replication_of	Nombre del proyecto o el recurso compartido (dentro del proyecto) donde está configurada la acción.
source_pool	Nombre de la agrupación del proyecto/recurso compartido de origen.
state	Describe si la replicación está en curso o no. Los valores son <code>sending</code> o <code>idle</code> .
state_description	Especifica detalles sobre el progreso de replicación. Los estados posibles son: ■ Conectando a destino de replicación ■ Recibiendo punto de control de destino ■ Estimando tamaño de actualización ■ Building deduplication tables ■ Sending update

Propiedad de la CLI	Descripción
	El estado <code>Building deduplication tables</code> se muestra solamente si el proyecto o el recurso compartido tiene activada la deduplicación.
<code>target_id</code>	Identificador único del objeto de destino de la replicación que describe el destino de esta acción de replicación.

En la siguiente tabla, se describen los nodos de una acción de replicación. Estos nodos solamente se pueden ver en la CLI. Las propiedades de estos nodos son de solo lectura.

TABLA 145 Nodos secundarios de las acciones de replicación (solo CLI)

Nodo secundario de acción de replicación	Descripción
<code>autosnaps</code>	Instantáneas programadas de manera automática, con el subnodo <code>automatic</code> . Para cambiar el número de instantáneas retenidas para un paquete de replicación, seleccione un nodo <code>automatic</code> individual y modifique la propiedad <code>keep</code> . Para obtener información sobre la gestión de instantáneas automáticas, consulte “Gestión de instantáneas automáticas de replicación” [740] . Para obtener más información acerca de la configuración de instantáneas automáticas, consulte Configuración de retención de instantáneas automáticas en un destino (CLI) [639] .
<code>schedules</code>	La configuración de programación. Es posible configurar los programas de replicación en cascada y de origen. Para obtener más información, consulte “Replicación en cascada” [768] .
<code>stats</code>	Estadísticas de la actualización de replicación más reciente y estadísticas acumuladas durante la duración de esta acción de replicación. Las estadísticas se actualizan después de que finaliza la actualización de replicación.

En la siguiente tabla, se describen las propiedades de nodo `stats`. Las propiedades de nodo `stats` brindan informes de estadísticas de la actualización de replicación más reciente (`last`) y estadísticas acumuladas durante la vida útil de esta acción de replicación (`total`). Para ver las estadísticas de una actualización de replicación anterior a la actualización más reciente, consulte la alerta de finalización asociada como se describe en [“Alertas de inicio y de finalización” \[743\]](#). Para obtener más información sobre las propiedades con `dedup` y `dd_` en sus nombres, consulte [“Replicación con deduplicación” \[727\]](#).

TABLA 146 Propiedades de nodo de estadísticas de acciones de replicación (CLI, solo lectura)

Propiedad de la CLI	Descripción
<code>replica_data_timestamp</code>	La hora de creación de la instantánea utilizada en la actualización de replicación más reciente completada (<code>last_sync</code>).
<code>last_result</code>	El resultado de la actualización <code>last_sync</code> . El valor de <code>last_result</code> es <code>success</code> o <code>failed</code> .

Propiedad de la CLI	Descripción
<code>last_sync</code>	La última vez que se envió correctamente una actualización de replicación. Este valor puede ser desconocido si el sistema no envió una actualización correcta desde el inicio.
<code>last_try</code>	La última vez que se intentó una actualización de replicación. Este valor puede ser desconocido si el sistema no intentó enviar una actualización desde el inicio. Si el valor de <code>last_result</code> es <code>success</code> , <code>last_sync</code> y <code>last_try</code> tienen el mismo valor de hora.
<code>last_logical_bytes</code>	El número de bytes que el flujo de datos de actualización <code>last_sync</code> tendría si no se hubieran comprimido los datos en el disco y si no se hubiera realizado ninguna otra compresión o deduplicación.
<code>last_phys_bytes</code>	El número de bytes en el flujo de datos de actualización de replicación interno <code>last_sync</code> antes de la deduplicación de replicación o la compresión del flujo de datos de replicación.
<code>last_after_dedup</code>	El número de bytes en el flujo de datos de actualización de replicación interno <code>last_sync</code> después de cualquier deduplicación del flujo de datos de replicación.
<code>last_to_network</code>	El número de bytes que el pipeline de compresión del flujo de datos de actualización <code>last_sync</code> proporciona a la red. Este valor muestra la consecuencia de la compresión del flujo de datos de replicación en el caso de que esté activada.
<code>last_duration</code>	El tiempo transcurrido para ejecutar la actualización <code>last_sync</code> .
<code>last_dd_table_build</code>	El tiempo para crear las tablas de deduplicación de actualización <code>last_sync</code> antes de que se transmita la actualización de replicación.
<code>last_dd_table_mem</code>	La cantidad máxima de memoria que consumieron las tablas de deduplicación de actualización <code>last_sync</code> .
<code>total_updates</code>	El número de actualizaciones de replicación correctas para esta acción.
<code>total_logical_bytes</code>	El número de bytes que los flujos de datos de actualización de todas las actualizaciones de esta acción tendrían si no se hubieran comprimido los datos en el disco y si no se hubiera realizado ninguna otra compresión o deduplicación.
<code>total_phys_bytes</code>	El número de bytes en los flujos de datos de actualización de replicación internos de todas las actualizaciones de esta acción antes de la deduplicación de replicación o la compresión del flujo de datos de replicación.
<code>total_after_dedup</code>	El número de bytes en los flujos de datos de actualización de replicación internos de todas las actualizaciones de esta acción después de cualquier deduplicación del flujo de datos de replicación.
<code>total_to_network</code>	El número de bytes que los pipelines de compresión del flujo de datos de replicación proporcionaron a la red para todas las actualizaciones de esta acción. Este valor muestra la consecuencia de la compresión del flujo de datos de replicación en el caso de que esté activada.
<code>total_duration</code>	El tiempo transcurrido para ejecutar todas las actualizaciones de esta acción.
<code>dd_total_updates</code>	El número de actualizaciones de replicación con deduplicación correctas para esta acción.
<code>dd_total_logical_bytes</code>	El número de bytes que los flujos de datos de actualización de todas las actualizaciones con deduplicación de esta acción tendrían si no se hubieran comprimido los datos en el disco y si no se hubiera realizado ninguna otra compresión o deduplicación.

Propiedad de la CLI	Descripción
dd_total_phys_bytes	El número de bytes en los flujos de datos de actualización de replicación internos de todas las actualizaciones con deduplicación de esta acción antes de la deduplicación de replicación o la compresión del flujo de datos de replicación.
dd_total_after_dedup	El número de bytes en los flujos de datos de actualización de replicación internos de todas las actualizaciones con deduplicación de esta acción después de la deduplicación del flujo de datos de replicación.
dd_total_to_network	El número de bytes que los pipelines de compresión del flujo de datos de replicación proporcionaron a la red para todas las actualizaciones con deduplicación de esta acción. Si se activó la compresión del flujo de datos de replicación, dd_total_to_network muestra el grado de eficiencia de la compresión.
dd_total_duration	El tiempo transcurrido para ejecutar todas las actualizaciones con deduplicación de esta acción.
dd_total_table_build	El tiempo para crear las tablas de deduplicación antes de que se transmita la actualización de replicación para todas las actualizaciones con deduplicación de esta acción.
dd_total_table_mem	La cantidad máxima de memoria que consumieron las tablas de deduplicación para todas las actualizaciones con deduplicación de esta acción.

Temas relacionados

- [Creación de una acción de replicación \(BUI\) \[632\]](#)
- [Creación de una acción de replicación \(CLI\) \[636\]](#)

Propiedades del paquete de replicación

Las propiedades del paquete de replicación que se ven en la BUI y la CLI difieren levemente, como se describe en la siguiente tabla.

TABLA 147 Propiedades del paquete de replicación (BUI y CLI)

Propiedad de la BUI	Propiedad de la CLI	Descripción
Host de origen	source_name	Nombre del origen de este paquete.
Agrupación de origen	source_pool	Agrupación de almacenamiento del origen desde donde se replica este proyecto. Esta propiedad se especifica cuando se configura inicialmente una acción.
	enabled	Cuando está activada (<code>true</code> en la CLI), se pueden recibir actualizaciones de replicación. Cuando está desactivada, (<code>false</code> en la CLI), el ícono  no aparece resaltado y no se pueden recibir actualizaciones de replicación.
Registro de hora de datos	data_timestamp	Hora de creación de la instantánea usada en la última actualización correcta.

Propiedad de la BUI	Propiedad de la CLI	Descripción
Última sincronización	last_sync	Tiempo de finalización de última actualización correcta.
Último intento	last_try	Tiempo de finalización de último intento de actualización.
Ruta de importación de datos	import_path	URI de medios externos para importación pendiente.
Estado	state	Estado actual de actualizaciones de replicación.
Último resultado	last_result	Resultado de último intento de actualización. El valor es <code>success</code> o <code>failed</code> .

En la siguiente tabla, se describen las propiedades del paquete de replicación de solo lectura de la CLI.

TABLA 148 Propiedades del paquete de replicación (CLI, solo lectura)

Propiedad de la CLI	Descripción
id	Identificador único del paquete de replicación. El identificador se puede usar para seleccionar un paquete introduciendo <code>select id= unique-id</code> .
source_asn	ID de la acción de replicación asociada con este paquete.
source_ip	Dirección IP del origen de este paquete.
target_pool	Agrupación de destino de este paquete.
replica_of	Juego de datos replicado en este paquete.
state_description	Estado actual de actualizaciones de replicación.
fuera de línea	Permite indicar que el paquete está esperando una actualización fuera de línea.

Agrupaciones de almacenamiento de replicación

Cuando una acción de replicación se configura inicialmente, el administrador tiene la opción de elegir la agrupación de almacenamiento en el destino que debe contener los datos replicados. Una vez que se haya creado la acción, la agrupación de almacenamiento que contenga la acción no se podrá cambiar. La generación de la acción crea el paquete vacío en la agrupación de almacenamiento especificada en el destino. Después de esta operación, el origen no tiene conocimiento de la configuración de almacenamiento en el destino. No realiza un seguimiento de la agrupación hacia la cual se realiza la replicación, ni se actualiza con los cambios de configuración de almacenamiento en el destino.

Cuando el destino es un sistema agrupado en cluster, la agrupación de almacenamiento elegida debe ser propiedad del mismo controlador propietario de la dirección IP utilizada por el origen de la replicación porque solo esas agrupaciones tienen siempre garantía de accesibilidad cuando

el origen se pone en contacto con el destino mediante esa dirección IP. Es exactamente análogo a la configuración de clientes NAS, por ejemplo, NFS o SMB, donde la dirección IP y la ruta solicitada en una operación de montaje deben cumplir con la misma limitación. Cuando se llevan a cabo operaciones que cambian la titularidad de las agrupaciones de almacenamiento y direcciones IP en un cluster, los administradores deben tener en cuenta el impacto sobre los orígenes que replican hacia el cluster. En la actualidad, no hay manera de mover los paquetes de una agrupación de almacenamiento a otra.

Temas relacionados

- [Flujo de trabajo de replicación remota \[623\]](#)
- [Replicación remota \[623\]](#)

Replicación de proyectos frente a replicación de recursos compartidos

Si bien es posible configurar la replicación remota en el nivel de proyecto y en el nivel de recurso compartido, se recomienda la replicación en el nivel de proyecto por los siguientes motivos:

- Las instantáneas de replicación siempre se generan en el nivel de proyecto. Si se hacen varias replicaciones en el nivel de los recursos compartidos de un mismo proyecto, se puede generar una cantidad de sobrecarga sustancial y consumir espacio en la agrupación.
- Al revertir replicaciones realizadas en el nivel de los recursos compartidos, el recurso compartido se coloca en su propio proyecto. Esto significa que las reversiones de las replicaciones a la larga separan el recurso compartido de los demás recursos compartidos del proyecto, a menos que se los replique a todos juntos.

Al igual que otras propiedades configurables en la pantalla Recursos compartidos, cada recurso compartido puede heredar o sustituir la configuración de su proyecto principal. Heredar la configuración no solo significa que el recurso compartido se replica en el mismo programa hacia el mismo destino con las mismas opciones que su proyecto principal, sino que, además, el recurso compartido se replicará en el mismo flujo con las mismas instantáneas de nivel de proyecto que los demás recursos compartidos que heredan la configuración del proyecto. Esto puede ser importante para aplicaciones que requieren coherencia entre los datos almacenados en varios recursos compartidos. La sustitución de la configuración significa que el recurso compartido no se replicará con acciones de nivel de proyecto, aunque se podría replicar con sus propias acciones de nivel de recurso compartido que incluirán el proyecto. No es posible sustituir una parte de la configuración de replicación del proyecto y heredar el resto.

Más precisamente, la configuración de replicación de un proyecto y sus recursos compartidos definen una cantidad de *grupos* de replicación, donde cada uno se replicará con un único flujo con instantáneas tomadas simultáneamente. Todos los grupos contienen el proyecto en sí mismo

(que esencialmente incluye solo sus propiedades). Un grupo de nivel de proyecto incluye todos los recursos compartidos que heredan la configuración de replicación del proyecto principal. Los recursos compartidos que sobrescriben la configuración del proyecto forman un nuevo grupo compuesto únicamente por el proyecto y el recurso compartido.

Por ejemplo, supongamos lo siguiente:

- Tiene un proyecto `home` y recursos compartidos `bill`, `cindi` y `dave`.
- `home` tiene una replicación configurada con un determinado número de acciones.
- `home/bill` y `home/cindi` heredan la configuración de replicación del proyecto.
- `home/dave` sustituye la configuración de replicación del proyecto, utilizando su propia configuración con un determinado número de acciones.

Esta configuración define los siguientes grupos de replicación, donde cada uno se replica como un único flujo por acción con instantáneas tomadas simultáneamente en el proyecto y los recursos compartidos:

- Un grupo en el nivel del proyecto, que incluye `home`, `home/bill` y `home/cindi`.
- Un grupo en el nivel del recurso compartido, que incluye `home` y `home/dave`.

Nota - Debido a limitaciones actuales, no combine replicaciones de nivel de proyecto con replicaciones de nivel de recursos compartidos en el mismo proyecto. Esto evita resultados impredecibles al revertir la dirección de replicación o al replicar clones. Para obtener información detallada, consulte [“Paquetes de replicación” \[747\]](#) y [“Clonación de un recurso compartido o un paquete de replicación” \[748\]](#).

Temas relacionados

- [Flujo de trabajo de replicación remota \[623\]](#)
- [Replicación remota \[623\]](#)

Autorizaciones de replicación

El subsistema de replicación proporciona dos autorizaciones de usuario en el ámbito "Projects and Shares" (Proyectos y recursos compartidos):

Autorización	Detalles
<code>rrsource</code>	Permite a los administradores crear, editar y destruir destinos y acciones de replicación. Asimismo, permite a los administradores enviar y cancelar actualizaciones para acciones de replicación.
<code>rrtarget</code>	Permite a los administradores gestionar paquetes replicados, incluidos la desactivación de la replicación

Autorización	Detalles
	en el nivel del paquete, la clonación de un paquete o de sus miembros, la modificación de propiedades de juegos de datos recibidos y el corte o la reversión de la replicación. Es posible que sea necesario obtener otras autorizaciones para algunas de estas operaciones (como definir propiedades o clonar recursos compartidos individuales). Para obtener más información, consulte las autorizaciones disponibles en el ámbito de proyectos y recursos compartidos.

Se requiere autorización `rrsource` para configurar destinos de replicación en un dispositivo, incluso cuando se configura en la pantalla de servicio Replicación remota. Para obtener ayuda con las autorizaciones, consulte [“Configuración de usuarios” \[257\]](#).

Temas relacionados

- [Flujo de trabajo de replicación remota \[623\]](#)
- [Replicación remota \[623\]](#)

Replicación con deduplicación

La replicación con deduplicación proporciona la capacidad de reducir la cantidad de datos que los trabajos de replicación envían mediante la red. Esta función es útil para reducir los requisitos de ancho de banda de datos en el cable de la replicación, especialmente cuando se usa una red de alto costo, ancho de banda bajo y latencia alta.

Nota - Esta función impone un costo en forma de preprocesamiento y mayor sobrecarga de memoria. La eficacia de la deduplicación depende, en gran medida, de los datos. Por lo tanto, se recomienda verificar los ahorros de la deduplicación con juegos de datos representativos antes de usar esta función en un entorno de producción. La replicación con deduplicación es más eficaz cuando existen más datos duplicados.

La replicación con deduplicación está desactivada por defecto. Para activar la replicación con deduplicación en acciones de replicación individuales, haga clic en Activar deduplicación en el cuadro de diálogo Agregar acción de replicación de la BUI o establezca la propiedad `dedup` en `true` en la CLI.

Estadísticas de replicación con deduplicación

En la CLI, cada acción de actualización de replicación tiene un nodo `stats`. El nodo `stats` registra información sobre la actualización de replicación más reciente, además de

las estadísticas acumuladas durante la vida útil de la acción de replicación. Para ver las estadísticas de una actualización específica que no es la actualización más reciente, consulte la alerta de finalización para la actualización como se describe en [“Alertas de inicio y de finalización” \[743\]](#).

Estas propiedades del nodo `stats` de la acción de replicación cuantifican:

- Los beneficios de la compresión en el disco
- Los beneficios de la deduplicación
- Los beneficios de la compresión de flujo de datos de replicación
- La duración de la actualización de replicación
- El tiempo de construcción de las tablas de deduplicación (antes del envío de datos)
- El consumo de memoria máximo de las tablas de deduplicación

En [Tabla 146, “Propiedades de nodo de estadísticas de acciones de replicación \(CLI, solo lectura\)”](#), se describen las propiedades del nodo `stats` de la acción para un flujo de replicación con deduplicación. Consulte especialmente las propiedades con `dedup` y `dd_` en sus nombres.

Medición de estadísticas de replicación con deduplicación

Cuando se activa la deduplicación para un flujo de replicación, los datos se transforman por medio de varias capas de deduplicación y de compresión. Las velocidades de datos se miden y se registran a medida que se transforman los datos.

Para determinar si la deduplicación surtió efecto en la acción de replicación, examine las estadísticas de replicación en el nodo `stats` de una acción de replicación en la CLI o en las alertas de finalización de la BUI o la CLI.

Comparación de beneficios de una única actualización de replicación con deduplicación

- En la BUI, use las alertas de finalización de replicación para comparar las estadísticas de `phys_bytes` y `after_dedup`, y evaluar el beneficio de la replicación con deduplicación. Para obtener información sobre las alertas de finalización de replicación, consulte [“Alertas de inicio y de finalización” \[743\]](#).
- En la CLI, utilice las alertas de finalización de replicación para comparar las estadísticas de `phys_bytes` y `after_dedup`, o utilice el nodo `stats` de la acción de replicación para comparar las estadísticas de `last_phys_bytes` y `last_after_dedup`, y evaluar el beneficio de la replicación con deduplicación. Para obtener información sobre las estadísticas en el nodo `stats`, consulte [Tabla 146, “Propiedades de nodo de estadísticas de acciones de replicación \(CLI, solo lectura\)”](#).

Comparación de beneficios promedio de actualizaciones de replications con deduplicación

Para determinar el beneficio promedio de todas las actualizaciones de replicación con deduplicación llevadas a cabo mediante la acción de replicación, use el nodo `stats` de la acción de replicación para comparar las estadísticas de `dd_total_phys_bytes` y `dd_total_after_dedup`. Para obtener información sobre las estadísticas en el nodo `stats`, consulte [Tabla 146](#), “Propiedades de nodo de estadísticas de acciones de replicación (CLI, solo lectura)”.

Configuración de replicación para dispositivos agrupados en clusters

La replicación se puede configurar desde cualquier dispositivo de origen a cualquier destino de replicación, independientemente de si cada uno forma parte de un cluster y de si el par del cluster del dispositivo tiene una replicación configurada en cualquier dirección.

Las siguientes reglas rigen el comportamiento de las actualizaciones de replicación para los dispositivos agrupados en clusters:

- Las actualizaciones de replicación para proyectos y recursos compartidos se envían desde cualquier par de cluster que haya importado la agrupación de almacenamiento contenedora.
- Las agrupaciones de almacenamiento de las que cada controlador es propietario se pueden replicar en el mismo destino de replicación solo si se instaló OS8.6.0 (o posterior) en ambos controladores.
- Las actualizaciones de replications son recibidas por cualquier par que haya importado la dirección IP configurada en la acción de replicación en el origen. Los administradores deben garantizar que el controlador con esta dirección IP siempre tenga la agrupación de almacenamiento que contiene la réplica importada. Para garantizarlo, se asignan los recursos de agrupación y dirección IP al mismo controlador durante la configuración del cluster.
- Se producirá un error en las actualizaciones de replicación (desde y hacia el dispositivo) que estén en curso cuando un dispositivo exporta la dirección IP o la agrupación de almacenamiento correspondiente (como parte de una toma de control o un failback). Las actualizaciones de replicación que utilizan agrupaciones de almacenamiento y direcciones IP que no se ven afectadas por una operación de toma de control o de failback no se verán afectadas por la operación.

Temas relacionados

- [“Ejemplo: Configuración de replicación para dispositivos agrupados en clusters” \[730\]](#)

Ejemplo: Configuración de replicación para dispositivos agrupados en clusters

El objetivo de este ejemplo es configurar la replicación de manera adecuada para garantizar que los proyectos se sigan replicando después de la toma de control del cluster, un failback en el cluster o después de realizar una replicación inversa en un dispositivo de destino.

- [Configuration Guidelines](#)
- [Example: Configuring Replication for Clustered Appliances](#)
- [Replication Data Path Illustrated Examples](#)

Directrices de configuración

Al configurar la replicación para dispositivos en cluster, siga estas directrices:

- Asegúrese de que tanto los dispositivos de destino y de origen de la replicación estén en estado CLUSTERED (En cluster). Para obtener detalles, consulte [Tabla 12, “Estados de clusters”](#).
- Seleccione las interfaces de red y las direcciones IP que se usarán para el tráfico de replicación en los dispositivos de origen y destino de replicación.
 - Seleccione una interfaz de red única. A diferencia de una interfaz de red privada, una interfaz de red única se transfiere al controlador superviviente después de la pérdida de uno de los controladores del cluster. El uso de una interfaz única garantiza que la replicación se realice correctamente después de la toma de control del cluster o la transición de failback. Para obtener más información acerca de las interfaces únicas, consulte [Tabla 13, “Tipos de recursos de cluster”](#).
 - Asegúrese de que la interfaz de red seleccionada en el dispositivo de origen y la agrupación desde la cual se replicarán los datos estén asignadas al mismo controlador. Esto sucede siempre cuando el cluster de origen se encuentra en estado CLUSTERED (En cluster).
 - De manera similar para el cluster de destino, la interfaz de red seleccionada en el dispositivo de destino y la agrupación en la cual se replicarán los datos deben estar asignadas al mismo controlador. Esta asociación está garantizada cuando la configuración de replicación se lleva a cabo mientras el cluster de destino está en estado CLUSTERED (En cluster).
 - Los dispositivos de origen y de destino deben poder comunicarse correctamente mediante las interfaces de red y las direcciones IP seleccionadas.
- Cree un enrutamiento estático basado en host /32 entre los dispositivos de destino y de origen para garantizar que en la siguiente reversión de replicación, la interfaz seleccionada

se use para el tráfico de replicación de salida cuando la reversión haya transformado el destino actual en un origen de replicación.

- Una vez que se haya creado la ruta estática, configure el objeto de destino de la replicación en un dispositivo de origen mediante la dirección IP seleccionada del destino.
- Cuando el dispositivo de destino se encuentra en el estado OWNER (Propietario), se toma el control de todos los recursos compartidos, incluidas las interfaces de red y las agrupaciones de almacenamiento, y pasan a ser propiedad del controlador superviviente que, ahora, se encuentra en el estado OWNER (Propietario). En el controlador que está en el estado OWNER (Propietario), se puede seleccionar una interfaz de red que esté asignada a un controlador y usarla para transmitir el tráfico de replicación a una agrupación que esté asignada a un controlador diferente. Cuando se regresen los controladores al estado CLUSTERED (En cluster), se regresan las interfaces de red y las agrupaciones de almacenamiento a los controladores asignados. Por lo tanto, no se podrán llevar a cabo actualizaciones de replicación debido a que el dispositivo de origen usará la interfaz de red en el controlador de destino que ya no es propietario de la agrupación. Este error de configuración no se originará cuando la configuración de replicación se realice mientras el dispositivo de destino se encuentra en el estado CLUSTERED (En cluster).

Ejemplo: Configuración de replicación para dispositivos agrupados en clusters

El procedimiento de ejemplo usa las siguientes interfaces de red y direcciones IP de origen y destino:

El cluster del dispositivo de origen está compuesto por los controladores de origen s1 y s2. La agrupación de almacenamiento sp1 se asigna a s1 y la agrupación sp2 se asigna a s2. Las interfaces de red del cluster están compuestas por:

- La interfaz privada ixgbe0 en s1 con la dirección IP 198.51.100.81/24.
- La interfaz privada ixgbe0 en s2 con la dirección IP 198.51.100.82/24.
- La interfaz única ixgbe1 con la dirección IP 192.0.2.101/25 asignada a s1.
- La interfaz única ixgbe2 con la dirección IP 192.0.2.102/25 asignada a s2.
- La interfaz única ixgbe3 con la dirección IP 192.0.2.201/25 asignada a s1.
- La interfaz única ixgbe4 con la dirección IP 192.0.2.202/25 asignada a s2.

Inicialmente, el dispositivo se encuentra en el estado CLUSTERED (En cluster) en donde:

- s1 es propietario de sp1, ixgbe1 e ixgbe3.
- s2 es propietario de sp2, ixgbe2 e ixgbe4.

El cluster del dispositivo de destino está compuesto por los controladores t1 y t2. La agrupación de almacenamiento tp1 se asigna a t1 y la agrupación tp2 se asigna a t2. Las interfaces de red del cluster están compuestas por:

- La interfaz privada `ixgbe0` en τ_1 con la dirección IP 198.51.100.83/24.
- La interfaz privada `ixgbe0` en τ_2 con la dirección IP 198.51.100.84/24.
- La interfaz única `ixgbe1` con la dirección IP 192.0.2.103/25 asignada a τ_1 .
- La interfaz única `ixgbe2` con la dirección IP 192.0.2.104/25 asignada a τ_2 .
- La interfaz única `ixgbe3` con la dirección IP 192.0.2.203/25 asignada a τ_1 .
- La interfaz única `ixgbe4` con la dirección IP 192.0.2.204/25 asignada a τ_2 .

Inicialmente, el dispositivo se encuentra en el estado CLUSTERED (En cluster) en donde:

- τ_1 es propietario de `tp1`, `ixgbe1` e `ixgbe3`.
- τ_2 es propietario de `tp2`, `ixgbe2` e `ixgbe4`.

En los siguientes pasos, se describe cómo configurar la replicación mediante la CLI para proyectos Red (Rojo), Blue (Azul) y Green (Verde).

1. Seleccione las interfaces de red y las direcciones IP.

- Comience por seleccionar las interfaces de red y las direcciones IP para la replicación del proyecto Red (Rojo).

El hecho de que el origen s se encuentre en el estado CLUSTERED (En cluster), es motivo suficiente para garantizar que las interfaces de red y las direcciones IP seleccionadas no son privadas. Por lo tanto, en s_1 use ya sea `ixgbe1` o `ixgbe3`.

- Lo mismo se aplica al destino τ , por lo tanto, use ya sea `ixgbe1` o `ixgbe3` en el dispositivo τ_1 . Ya que `ixgbe1` y `ixgbe3` en s_1 y τ_1 pertenecen a la misma subred, seleccione cualquiera para llevar a cabo la replicación del proyecto Red (Rojo). Para este ejemplo, seleccione la interfaz `ixgbe1` en s_1 y en τ_1 .

2. Configure una ruta estática en s_1 .

En el siguiente ejemplo, se configura la ruta estática para la replicación del proyecto Red (Rojo) en el controlador de origen s_1 :

```
S1:configuration net routing> create
S1:configuration net route (uncommitted)> set family=IPv4
                                     family = IPv4 (uncommitted)
S1:configuration net route (uncommitted)> set destination=192.0.2.103
                                     destination = 192.0.2.103 (uncommitted)
S1:configuration net route (uncommitted)> set mask=32
                                     mask = 32 (uncommitted)
S1:configuration net route (uncommitted)> set interface=ixgbe1
                                     interface = ixgbe1 (uncommitted)
S1:configuration net route (uncommitted)> set gateway=192.0.2.1
                                     gateway = 192.0.2.1 (uncommitted)
S1:configuration net route (uncommitted)> commit
S1:configuration net routing> list
```



```

ROUTE      DESTINATION      GATEWAY      INTERFACE      TYPE      STATUS
...
route-003  192.0.2.103/32  192.0.2.1  ixgbe1        static  active

```

3. Configure una ruta estática en τ_1 .

En el siguiente ejemplo, se configura la ruta estática para la replicación del proyecto Red (Rojo) en el controlador de destino τ_1 :

```

T1:configuration net routing> create
T1:configuration net route (uncommitted)> set family=IPv4
                                         family = IPv4 (uncommitted)
T1:configuration net route (uncommitted)> set destination=192.0.2.101
                                         destination = 192.0.2.101 (uncommitted)
T1:configuration net route (uncommitted)> set mask=32
                                         mask = 32 (uncommitted)
T1:configuration net route (uncommitted)> set interface=ixgbe1
                                         interface = ixgbe1 (uncommitted)
T1:configuration net route (uncommitted)> set gateway=192.0.2.1
                                         gateway = 192.0.2.1 (uncommitted)
T1:configuration net route (uncommitted)> commit
T1:configuration net routing> list
ROUTE      DESTINATION      GATEWAY      INTERFACE      TYPE      STATUS
...
route-003  192.0.2.101/32  192.0.2.1  ixgbe1        static  active

```

4. Cree un destino de replicación en s_1 .

En el siguiente ejemplo, se crea el objeto de destino de replicación en s_1 que se usará para replicar el proyecto Red (Rojo) de sp_1 a tp_1 :

```

S1:shares replication targets>target
S1:shares replication target (uncommitted)> set hostname=192.0.2.103
                                         hostname = 192.0.2.103 (uncommitted)
S1:shares replication target (uncommitted)> set label=t1-1
                                         label = t1-1 (uncommitted)
S1:shares replication target (uncommitted)> set root_password=(set)
                                         root_password = (set) (uncommitted)
S1:shares replication target (uncommitted)> commit

```

5. Cree una acción de replicación para cada proyecto.

- Replique el proyecto Red (Rojo) de la agrupación sp_1 a tp_1 .
- Replique el proyecto Blue (Azul) de la agrupación sp_1 a la agrupación tp_2 .
- Replique el proyecto Green de la agrupación sp_2 a tp_2 .

En el siguiente ejemplo, se crea la acción de replicación para el proyecto Red (Rojo):

```

S1:> shares select Red replication action

```

```
S1:shares Red action (uncommitted)> set target=t1-1
                                target=t1-1 (uncommitted)
S1:shares Red action (uncommitted)> set pool=tp1
                                pool=tp1 (uncommitted)
S1:shares Red action (uncommitted)> commit
```

6. Realice la configuración para replicar el proyecto Blue (Azul) de la agrupación sp1 a tp2.

Comience con la selección de interfaz y dirección, y seleccione las interfaces s1/ixgbe3 y t2/ixgbe4; tenga en cuenta que tanto s como t se encuentran en el estado CLUSTERED (En cluster) y que las direcciones de la interfaz se encuentran en la misma subred, 192.0.2.128/25. Luego, defina las rutas estáticas en ambos dispositivos de manera similar a los ejemplos mencionados anteriormente. A continuación, cree un objeto de destino de replicación t2-2 en s1 y cree la acción de replicación en s1 para el proyecto Blue (Azul) mediante el objeto de destino t2-2.

7. Realice la configuración para replicar el proyecto Green (Verde) de la agrupación sp2 a tp2.

Comience con la selección de la interfaz y seleccione las interfaces s2/ixgbe2 y t2/ixgbe2. Cree rutas estáticas en s2 y t2 mediante las interfaces seleccionadas y sus direcciones, defina el objeto de destino de replicación t2-1 mediante la dirección de t2/ixgbe2 y, finalmente, cree la replicación para el proyecto Green (Verde) mediante el objeto de destino t2-1.

8. Inicie la replicación para las tres acciones.

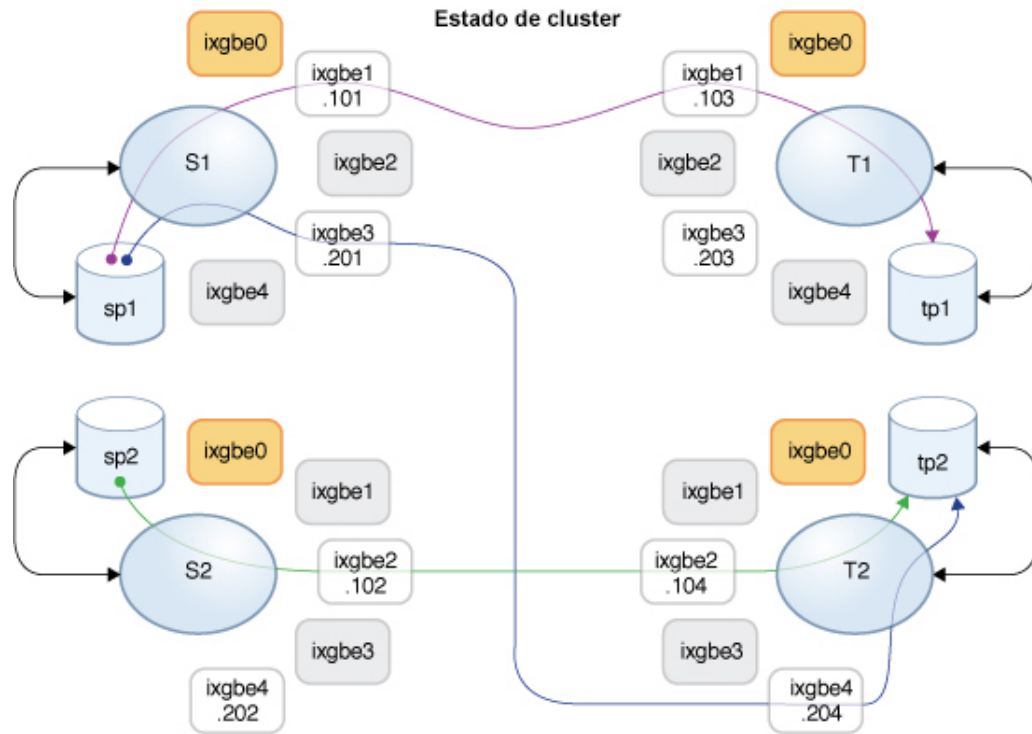
- a. Comience con el proyecto Red (Rojo):

```
S1:> shares select Red replication select action-000
S1:shares Red action-000> sendupdate
```

- b. Inicie la replicación para las acciones de los proyectos Blue (Azul) y Green (Verde) siguiendo el ejemplo anterior.

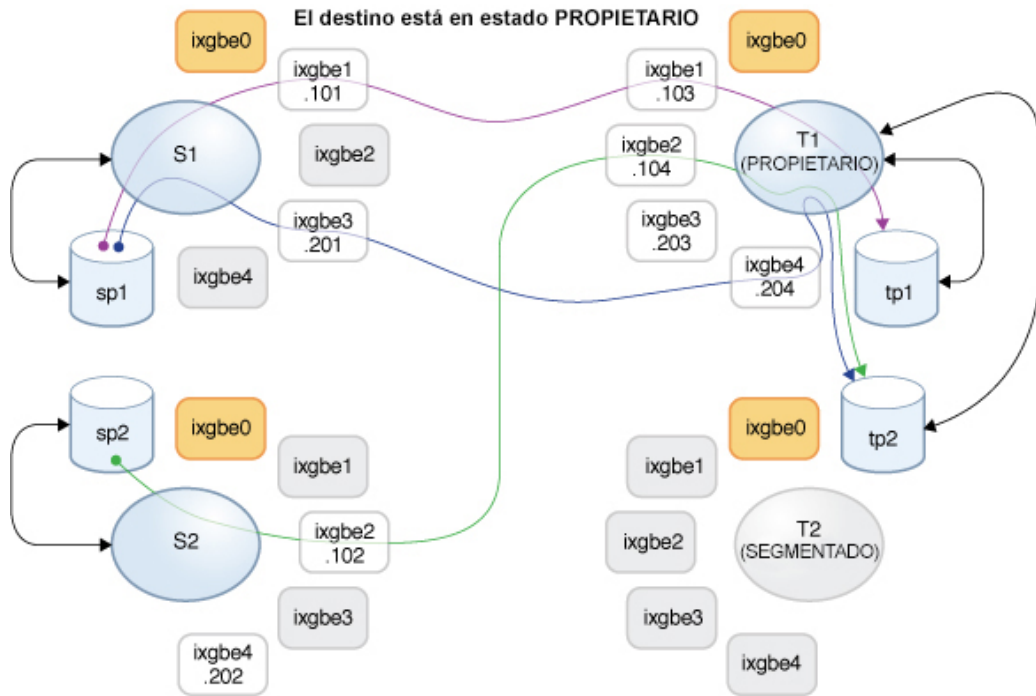
Ejemplos ilustrados de la ruta de datos de replicación

En las siguientes figuras, se ilustran las rutas de datos de replicación durante actualizaciones de replicación para las acciones de replicación de los proyectos Red (Rojo), Blue (Azul) y Green (Verde):

FIGURA 26 Ruta de datos de replicación normal

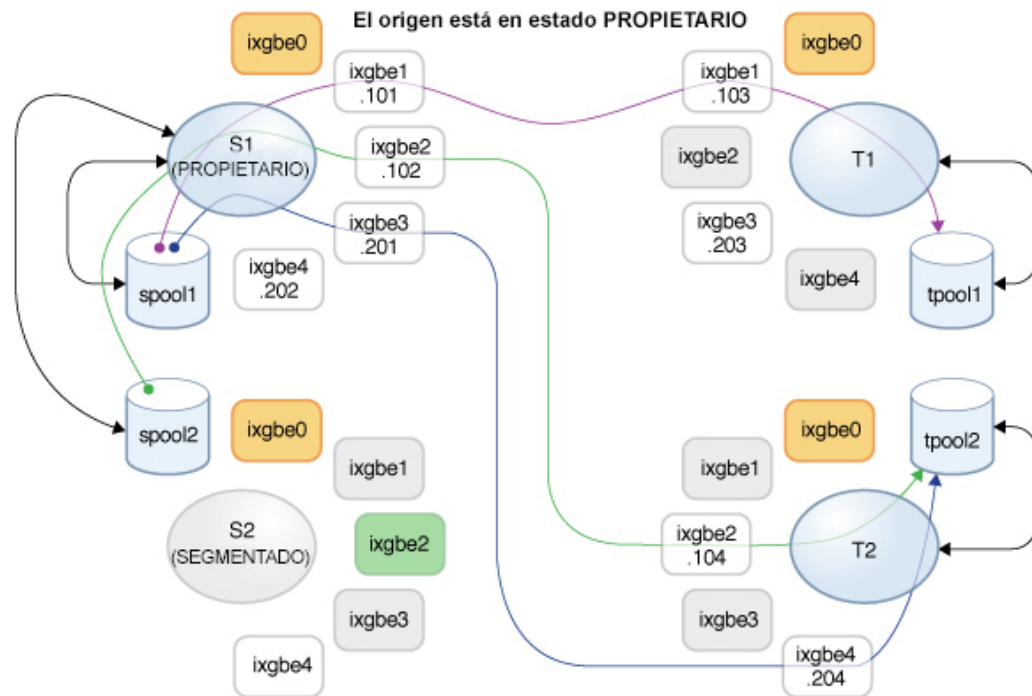
Suponga que el controlador τ_2 ha sido retirado para mantenimiento. τ_1 realizó una toma de control y ahora es propietario de todos los recursos. Las actualizaciones de replicación para los proyectos Blue (Azul) y Green (Verde) se cancelarán en caso de que se encuentren en curso durante la toma de control. Luego de que τ_1 realiza la toma de control, estas actualizaciones de replicación se pueden reanudar de manera manual, o se reanudarán automáticamente si se configuran planificaciones para las acciones de replicación correspondientes.

Una vez que el controlador τ_1 haya completado la toma de control, se convierte en el propietario de las interfaces $ixgbe2$ y $ixgbe4$ que son necesarias para continuar las actualizaciones de replicación para los proyectos Blue (Azul) y Green (Verde). En la siguiente figura, se muestra la ruta de datos de replicación después de que τ_1 haya completado la toma de control.

FIGURA 27 Ruta de datos de replicación después de la toma de control de T1

Después de que r_2 se encuentra nuevamente en línea, se lleva a cabo un failback en el controlador r_1 y toma control de sus recursos. Las actualizaciones de replicación de los proyectos Blue (Azul) y Green (Verde) que estén en curso se cancelarán y se podrán reanudar después de que se complete el failback.

El controlador s_2 se retira para mantenimiento y la toma de control que se realiza en el controlador s_1 provoca que este se adueñe de todos los recursos, incluida la interfaz necesaria para continuar con la replicación del proyecto Green (Verde). Si una actualización de replicación del proyecto Green (Verde) está en progreso, se cancelará y se podrá reanudar una vez que finalice la toma de control.

FIGURA 28 Ruta de datos después del failback en T1 y la toma de control en S1**Temas relacionados**

- [Configuración de replicación para una configuración en cluster \[642\]](#)
- [Flujo de trabajo de replicación remota \[623\]](#)
- [Replicación remota \[623\]](#)

Instantáneas de replicación y coherencia de datos

El dispositivo de origen replica las instantáneas de manera automática en el destino, lo que significa que el contenido de la réplica siempre coincide exactamente con el del recurso compartido del origen en el momento en el que se realizó la instantánea. Dado que las instantáneas de todos los recursos compartidos enviadas en un grupo en particular se obtienen en el mismo momento, después de finalizar correctamente una actualización de replicación, el

contenido de todo el paquete coincide exactamente con el contenido del grupo en el momento de la creación de la instantánea en el origen.

Sin embargo, las instantáneas de cada recurso compartido se replican por separado; por lo tanto, es posible que algunos recursos compartidos de un paquete se hayan actualizado con una instantánea más reciente que la de otros recursos compartidos del mismo paquete. Esto es así durante la actualización de replicación y después de una actualización de replicación que generó fallos.

En resumen:

- Cada recurso compartido siempre es coherente con el momento del destino.
- Cuando no hay una actualización de replicación en curso y se ha realizado correctamente la actualización de replicación anterior, los recursos compartidos de cada paquete también son coherentes con el momento entre sí.
- Cuando hay una actualización de replicación en curso o se ha producido un error en la actualización anterior, es posible que los recursos compartidos de los paquetes no sean coherentes entre sí, pero cada uno aún será coherente en sí mismo. Si la coherencia del paquete es importante para una aplicación, se debe clonar el paquete de replicación, que siempre clona la instantánea recibida con mayor éxito de cada recurso compartido.

Temas relacionados

- [“Gestión de instantáneas de replicación” \[738\]](#)

Gestión de instantáneas de replicación

Las instantáneas son la base de la replicación. El origen y el destino siempre deben compartir una instantánea en común para continuar con la replicación de manera incremental, y el origen debe conocer la instantánea más reciente que tiene el destino. Para facilitar esto, el subsistema de replicación crea y gestiona sus propias instantáneas. En general, los administradores no necesitan preocuparse por ello, pero aquí se describen los detalles, ya que las instantáneas pueden tener efectos significativos en la utilización del almacenamiento.

Cada actualización de replicación para una acción en particular está compuesta por los siguientes pasos:

- Determine si esto es una actualización incremental o completa basado en si:
 - Se realizó un intento de replicar esta acción antes.
 - El destino ya cuenta con la instantánea necesaria para una actualización incremental.
- Tome una nueva instantánea de nivel de proyecto.

- Envíe la actualización. Para obtener una actualización completa, envíe el contenido de todo el grupo a la nueva instantánea. Para obtener una actualización incremental, envíe la diferencia existente entre la instantánea anterior (base) y la nueva instantánea.
- Registre la nueva instantánea como instantánea base para la siguiente actualización y destruya la instantánea base anterior (para actualizaciones incrementales). La instantánea base permanece en el destino hasta que se reciba la siguiente actualización, en cuyo momento es lo primero que se destruye.

Esto tiene diversas consecuencias para la gestión de instantáneas:

- Durante la primera actualización de replicación y después de la actualización inicial, cuando la replicación no está activa, hay exactamente una instantánea de nivel de proyecto para cada acción configurada en el proyecto o cualquier recurso compartido del grupo. Es posible que una acción de replicación cree instantáneas en recursos compartidos que están en el mismo proyecto que los recursos compartidos del grupo replicado por la acción, pero que no se envían como parte de la actualización para el grupo.
- Durante las posteriores actualizaciones de replicación de una acción en particular, podría haber dos instantáneas de nivel de proyecto asociadas con la acción. Ambas instantáneas pueden permanecer una vez finalizada la actualización, si se produce un error en el que el origen no pudo determinar si el destino recibió con éxito la nueva instantánea (como en el caso de una interrupción del servicio de red durante la actualización, que genera un error).
- Ninguna de las instantáneas asociadas a una acción de replicación puede ser destruida por el administrador sin interrumpir la replicación incremental. El sistema no permitirá a los administradores destruir instantáneas en el origen o el destino que sean necesarias para la replicación incremental. Para destruir dichas instantáneas en el origen, se debe destruir la acción (lo cual destruye las instantáneas asociadas a la acción). Para destruir dichas instantáneas en el destino, primero, se debe cortar el paquete (lo cual destruye la capacidad del paquete de recibir actualizaciones incrementales).
- Los administradores no deben revertir a las instantáneas creadas antes de las instantáneas de replicación. Esto destruirá las instantáneas de replicación posteriores e interrumpirá la replicación incremental de las acciones que utilizan esas instantáneas.
- El uso de instantáneas para la replicación requiere que los administradores que utilizan la replicación comprendan la space management en el dispositivo, en particular su aplicación a las instantáneas.

Instantáneas de replicación intermedias

Una acción de replicación se puede configurar para incluir instantáneas de no replicación. Cuando la propiedad "Incluir instantáneas" está configurada, las actualizaciones de replicación incluyen instantáneas de no replicación creadas después de la actualización de replicación anterior (o desde la creación del recurso compartido, en el caso de la primera actualización

completa). Esto incluye instantáneas automáticas e instantáneas creadas por el administrador. Esta propiedad se puede desactivar para omitir estas instantáneas y enviar solo los cambios ocurridos entre las instantáneas de replicación con cada actualización.

La propiedad de acción `include_snaps` debe estar activada para replicar cualquier instantánea, incluidas las instantáneas automáticas.

Temas relacionados

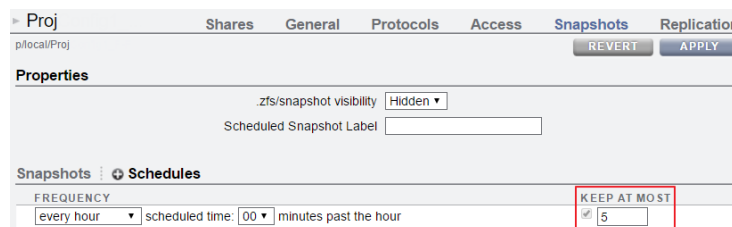
- [“Gestión de espacio de recursos compartidos” \[539\]](#)
- [“Gestión de instantáneas generadas por el usuario” \[677\]](#)

Gestión de instantáneas automáticas de replicación

La función de instantáneas programadas automáticamente permite crear y destruir automáticamente instantáneas de proyectos o recursos compartidos según programas proporcionados por el administrador. El programa especifica cuándo crear una instantánea automática y cuántas instantáneas debe retener. Se pueden crear varios programas para un proyecto o recurso compartido.

Con Replicación remota, las instantáneas, incluidas las instantáneas automáticas, pueden incluirse en actualizaciones de replicación y estarán disponibles en el destino de replicación como parte del paquete de replicación correspondiente.

Por defecto, el número de instantáneas automáticas retenidas en el destino corresponde a la configuración de retención (Mantener al máximo) en el programa de instantáneas del proyecto o recurso compartido.



Las acciones de replicación se pueden configurar para retener un número específico por separado de instantáneas automáticas en el destino mediante actualizaciones de replicación.

Schedule : **Snapshots**

Auto snapshot retention policies ☐ synchronized ☒ independent

Configure auto snapshot retention on the target

FREQUENCY KEEP AT MOST 10

every hour scheduled time: 00 minutes past the hour

Gestión de replicación inversa e instantáneas automáticas

Al realizar la replicación inversa, se mantiene la configuración de retención de instantáneas automáticas: El origen y el destino seguirán manteniendo su configuración de retención.

Ejemplo:

- El Origen A tiene instantáneas automáticas configuradas y retiene **5** instantáneas en el Origen A.
- Mediante una acción de replicación en el Origen A, el Destino B se configuró para retener **10** instantáneas automáticas.

Después de la replicación inversa, el origen y el destino cambiaron a **Origen B** y **Destino A**.

- Ahora el Origen B tiene el programa de instantáneas automáticas y aún retiene **10** instantáneas.
- El Destino A sigue configurado para retener **5** instantáneas. Ahora se puede definir la configuración de retención mediante la acción de replicación en el Origen B.

Al realizar otra replicación inversa, se revertirá el origen y el destino a su configuración original.

Para obtener más información sobre la configuración de retención de instantáneas automáticas en un destino, consulte:

- [Configuración de retención de instantáneas automáticas en un destino \(BUI\) \[638\]](#)
- [Configuración de retención de instantáneas automáticas en un destino \(CLI\) \[639\]](#)

Configuraciones de iSCSI y replicación

Las actualizaciones de replicación comprenden la mayor parte de la configuración especificada en la pantalla Recursos compartidos de un proyecto y sus recursos compartidos. Esto incluye grupos de destino y de inicio asociados a LUN replicados.

Quando se utilizan grupos de inicio y de destino no predeterminados, los administradores deben asegurarse de que los grupos de inicio y de destino utilizados por los LUN dentro del proyecto también existan en el destino de replicación. Si el grupo de destino o el grupo de iniciadores no existe en el sistema de destino, se producirá un error en la clonación, el corte o la replicación

inversa. Aparece un mensaje de error que indica que el nombre del grupo de destino o el grupo de iniciadores que se encuentra en el sistema de destino cambió o se lo suprimió.

El GUID SCSI asociado a un LUN se replica con el LUN. Como resultado, el LUN del dispositivo de destino tendrá el mismo GUID SCSI que el LUN del dispositivo de origen. Sin embargo, los clones de LUN replicados tendrán GUID diferentes (de la misma manera que los clones de LUN locales tienen GUID distintos de sus orígenes).

Temas relacionados

- [Flujo de trabajo de replicación remota \[623\]](#)
- [Replicación remota \[623\]](#)

Replicación reanudable

Cuando una actualización de replicación programada o continua se interrumpe debido a un fallo de red, una interrupción del sistema o la acción de un operador, la transferencia de datos se reanuda *automáticamente* desde el punto de interrupción. Esta característica está disponible en versiones OS8.7.0 o posteriores y debe estar instalada en el origen y el destino de replicación. Por ejemplo, si una replicación programada transfiere 100 bytes de datos antes de que se produzca el fallo, la siguiente actualización de replicación reanuda la transferencia de datos en el byte 101. El tamaño de datos estimado, que se muestra en el monitor de progreso de la replicación, incluye los datos que se deben enviar como parte de ambas acciones.

Si se produce un fallo durante una actualización de replicación manual, la actualización no se vuelve a intentar automáticamente. Sin embargo, la transferencia de datos se reanudará desde el punto de interrupción en la siguiente actualización de replicación.

Alertas de replicación

El dispositivo publica alertas cuando se produce alguno de los siguientes eventos de replicación:

- Una actualización de replicación manual o programada comienza o finaliza correctamente (en el origen y en el destino). Consulte [“Alertas de inicio y de finalización” \[743\]](#).
- Un administrador cancela de manera explícita una actualización (en el origen y en el destino).
- Se produce un fallo en una actualización (en el origen y en el destino).
- Se omite una actualización programada debido a que ya existe otra actualización en curso para la misma acción.
- Una replicación continua se inicia por primera vez, falla o se reanuda después de un fallo.

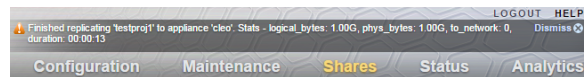
- Una demora del tiempo de réplica excede el umbral especificado.

Alertas de inicio y de finalización

Según la cantidad de proyectos que se replican y la frecuencia del programa de replicación, la cantidad de alertas de inicio y de finalización para las actualizaciones programadas puede opacar otras alertas importantes. Para desactivar las alertas de inicio y de finalización de las actualizaciones programadas, consulte Configuración de alertas de inicio y de finalización de replicación: [BUI](#), [CLI](#).

Si se activan las alertas de inicio y de finalización de replicación, cuando se completa correctamente la replicación en un destino, el sistema muestra la alerta de finalización en la parte superior de la ventana de la BUI, junto con el registro de la alerta en el log de alertas.

En la siguiente figura, se muestra una alerta de finalización de una actualización de replicación en la parte superior de la ventana de la BUI.



A continuación, se muestra una alerta de finalización de actualización de replicación de muestra en Mantenimiento > Logs > Alertas o en `maintenance logs > select alert > show`.

```
entry-71160 2020-11-18 00:03:23 019a9e92-6b12-400b-aea7-b900a58d30a6, Finished
replicating 'proj-9' to appliance 'zfs-storage'. Action -
4b9b1450-4300-4892-b89d-e170832ef531.. Stats - logical_bytes: 225K, phys_bytes:
67.4K, to_network: 33.4K, duration: 00:00:57, Minor Alert
```

En la siguiente tabla, se describen las propiedades de las alertas de finalización para cada actualización de replicación. Para ver las estadísticas de la actualización más reciente completada o el total acumulado durante la vida útil de esta acción de replicación, consulte [Tabla 146, “Propiedades de nodo de estadísticas de acciones de replicación \(CLI, solo lectura\)”](#). Si se desactivan las alertas de inicio y de finalización, no se pueden ver las estadísticas de actualizaciones anteriores específicas, pero sí las estadísticas de la actualización más reciente completada. Para obtener más información sobre las propiedades con `dedup` y `dd_` en sus nombres, consulte [“Replicación con deduplicación” \[727\]](#).

TABLA 149 Propiedades de las alertas de finalización de actualización de replicación

Propiedad de la CLI	Descripción
<code>logical_bytes</code>	Número de bytes que tendría el flujo de datos de actualización de replicación si no se hubieran comprimido los datos en el disco y si no se hubiera realizado ninguna otra compresión o deduplicación.

Propiedad de la CLI	Descripción
phys_bytes	Número de bytes en el flujo de datos de replicación interno antes de la deduplicación de replicación o la compresión del flujo de datos de replicación.
to_network	Número de bytes que el pipeline de compresión del flujo de datos de replicación proporciona a la red. Esto muestra la consecuencia de la compresión del flujo de datos de replicación, si está activada.
after_dedup	Número de bytes en el flujo de datos de replicación interno después de una deduplicación del flujo de datos de replicación.
duration	Tiempo transcurrido para llevar a cabo la actualización de replicación.
dd_table_build	Tiempo para crear las tablas de deduplicación antes de la transmisión de la actualización de replicación.
dd_table_mem	Cantidad máxima de memoria que consumieron las tablas de deduplicación.

Fallos de replicación

Se pueden producir fallos en las actualizaciones de replications individuales por diversos motivos. El dispositivo informa el motivo del fallo mediante alertas publicadas en el dispositivo de origen o el destino de replicación, o en la pantalla Replication (Replicación) de la acción que produjo el fallo. Para obtener información detallada sobre el fallo, debe hacer clic en el ícono de alerta naranja que representa el estado de la acción.

Los siguientes son algunos fallos de replicación comunes:

Error	Detalles
Cancelada	La actualización de replicación fue cancelada por el administrador. La replicación se puede cancelar en el origen o el destino.
Error de conectividad de red	El dispositivo no pudo establecer conexión con el destino de replicación debido a un problema de la red. Compruebe si hay alguna configuración errónea en el origen, el destino o la red.
Error de verificación de par	El dispositivo no pudo verificar la identidad del destino. Esto ocurre con más frecuencia cuando el destino se ha vuelto a instalar o ha sufrido un restablecimiento de fábrica. Se debe configurar un nuevo destino de replicación en el dispositivo de origen para un destino que se ha reinstalado o restablecido a los valores de fábrica para generar un nuevo conjunto de claves de autenticación. Consulte “Destinos de replicación” [711].
Error de RPC de par	Se produjo un error en una llamada a procedimiento remoto en el sistema de destino. Esto ocurre con más frecuencia cuando el destino de replicación ejecuta un software incompatible. Consulte Oracle ZFS Storage Appliance: Compatibilidad de la replicación remota [ID de documento 1958039.1] https://support.oracle.com/epmos/faces/DocumentDisplay?id=1958039.1 .
Colisión de nombres	Se produjo un error en la replicación de <project/share> desde <source> debido a una colisión de nombres con @<snapname> que NDMP retuvo en el destino. Para recuperar, cambie el nombre de la instantánea que se encuentra en el origen de la replicación y que tiene el mismo nombre que la

Error	Detalles
	instantánea retenida por NDMP en el destino (la que se indica en la alerta), o elimine dicha instantánea, a menos que comience con .rr. A continuación, realice una sincronización manual o permita que el origen de la replicación vuelva a intentar la actualización de la replicación de manera automática.
Sin paquetes	Se produjo un error en la replicación porque no existe un paquete en el destino que contenga los datos replicados. Dado que el paquete se crea al configurar la acción, este error generalmente se produce después de que el administrador ha destruido el paquete en el destino. Este error también puede ocurrir si la agrupación de almacenamiento que contiene el paquete no se importa en el sistema de destino, lo cual puede ocurrir si hay errores en la agrupación o si se ha vuelto a configurar el almacenamiento o la conectividad de red en el destino de replicación.
Desactivada	Se produjo un error en la replicación porque está desactivada en el destino. El servicio de replicación está desactivado en el destino o se ha desactivado la replicación para el paquete específico que se está replicando.
Destino ocupado	Se produjo un error en la replicación porque el sistema de destino ha alcanzado el número máximo de actualizaciones de replications simultáneas. El sistema limita la cantidad máxima de operaciones de replicación en curso para evitar el agotamiento de recursos. Cuando se alcanza este límite, si posteriormente se intentan recibir actualizaciones, se producirá este error, mientras que si posteriormente se intentan enviar actualizaciones, estas se acumularán hasta que los recursos estén disponibles.
Falta el destino	La actualización de replicación más reciente falló porque falta el destino. Si el destino ya no está configurado en el origen, la acción quedará desactivada de manera permanente. Si se produce este error, destruya la acción de replicación, y vuelva a configurar el destino de replicación y la acción.
Sin espacio	Se produjo un error en la replicación porque el sistema de origen no tenía suficiente espacio para crear una nueva instantánea. Esto se puede deber a la falta de espacio físico disponible en la agrupación de almacenamiento, o a que el proyecto o uno de sus recursos compartidos excede la cuota debido a reservaciones que no incluyen instantáneas.
Clave no disponible	Se produjo un error en la replicación porque la clave de cifrado utilizada por el recurso compartido no está disponible en el sistema de origen o en el de destino. Revise las alertas del sistema de origen y el destino de replicación para asegurarse de que la clave esté disponible en ambos sistemas. Consulte “Copia de seguridad, replicación y restauración de proyectos y recursos compartidos cifrados” [838] para obtener información acerca de la replicación de recursos compartidos y proyectos cifrados.
Destino incompatible	Se produjo un error en la replicación porque el sistema de destino no puede recibir el formato del flujo de datos del sistema de origen. Esto puede ocurrir debido a la actualización de un sistema de origen y a la aplicación de actualizaciones diferidas sin haber actualizado ni aplicado las mismas actualizaciones en el destino. Para obtener información acerca de actualizaciones diferidas que afectan la replicación remota, consulte Oracle ZFS Storage Appliance: Compatibilidad de la replicación remota [ID de documento 1958039.1] https://support.oracle.com/epmos/faces/DocumentDisplay?id=1958039.1 .
Falta el destino/iniciador iSCSI	Se produjo un error en la operación de reversión, corte o clon de replicación porque no existen los LUN del grupo de destino o el grupo de iniciadores

Error	Detalles
	para los LUN incluidos en el paquete de replicación. El nombre del grupo de destino o el grupo de iniciadores que está en el destino de replicación cambió o se lo suprimió.
Varios	Se produjo un error en la replicación, pero no hay información adicional disponible en el origen. Verifique el log de alertas en el sistema de destino y, si es necesario, comuníquese con el servicio de asistencia para obtener ayuda. Algunos de los modos de error que en la actualidad están comprendidos en esta categoría incluyen espacio en disco insuficiente en el destino para recibir la actualización e intentar replicar un clon cuya instantánea de origen no existe en el sistema de destino.

Se producirá un error en la actualización de replicación si se produce un error en cualquier parte de la actualización. Los recursos compartidos dentro de un proyecto se replican en serie y los cambios no se revierten si se produce un fallo en la actualización. Como resultado, cuando falla una actualización, es posible que algunos recursos compartidos del destino estén actualizados y otros no. Para obtener más información, consulte [“Instantáneas de replicación y coherencia de datos” \[737\]](#).

Cuando se producen fallos en una replicación continua o programada, el sistema aguarda algunos minutos y vuelve a intentarlo. El sistema continuará intentando las replicaciones continuas o programadas con errores de manera indefinida. En cualquier momento del procedimiento de reintento, el inicio de una actualización manual inmediatamente comenzará un reintento, lo cual eludirá la demora normal entre reintentos sucesivos. Si la actualización manual se completa correctamente, finaliza la secuencia de reintento y la acción de replicación se restablece a su funcionamiento normal de actualizaciones continuas o programadas.

Para obtener más información acerca de fallos o interrupciones en actualizaciones de replicación, consulte [“Replicación reanudable” \[742\]](#).

Cuando hay una actualización de replicación en curso y hay otra actualización programada, se retrasa la replicación programada hasta que se completa la actualización anterior y se emite una alerta.

Temas relacionados

- *Cómo resolver problemas con la replicación* (ID de documento 1397959.1) en [My Oracle Support](#) (<http://support.oracle.com/>)

Replicación comprimida

La función de replicación comprimida mejora el rendimiento cuando se replican datos que se pueden comprimir entre ubicaciones de origen y destino que tienen un ancho de banda limitado. Antes de que el flujo de replicación se envíe al destino, se lo comprime automáticamente a un

índice de compresión que depende de la utilización actual de la CPU y el rendimiento de E/S de la red. El flujo de replicación a continuación se descomprime cuando lo recibe el destino de replicación. Si alguna parte de los datos no se puede comprimir, esa porción se envía como si la compresión estuviera desactivada.

Todos los flujos de replicación se comprimen a menos que se desactive explícitamente la compresión. Si el equipo de la WAN proporciona compresión, por ejemplo, mediante un acelerador de WAN, desactive la función de compresión como se describe en el procedimiento [Desactivación de la compresión de replicación BUI](#), [CLI](#).

El dispositivo de origen y el destino de replicación requieren la versión 2013.1.4.0 (o posterior) del software para que sea posible la compresión de la replicación. Si el destino tiene una versión anterior, aparece un ícono de advertencia  junto al nombre del destino. Deberá actualizar el destino de replicación con la versión mínima.

Puede ver las estadísticas del rendimiento de la replicación en el dispositivo de origen, debajo de la barra de avance de la replicación.

Actions		
TARGET ▲	UPDATES	STATUS
 hog-10g Manual	Never Synced Never Attempted	 43% of 10.0G @548MB/s (-00:00:11)

Paquetes de replicación

Los paquetes son contenedores de los recursos compartidos y los proyectos replicados. Cada acción de replicación en un dispositivo de origen se corresponde a un paquete en un destino de replicación.

Puede usar la BUI o la CLI para explorar proyectos replicados, recursos compartidos, instantáneas y propiedades, de manera similar a como lo hace con los proyectos locales y los recursos compartidos. Sin embargo, como los recursos compartidos replicados deben coincidir exactamente con sus contrapartes en el dispositivo de origen, hay muchas operaciones de administración que no están permitidas dentro de los paquetes de replicación.

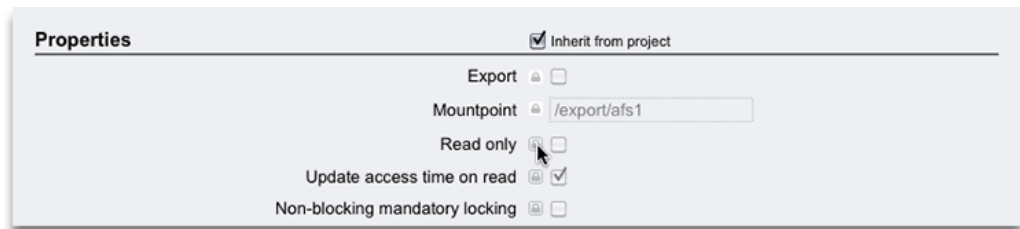
Puede modificar las siguientes propiedades de los proyectos y los recursos compartidos replicados:

- **Reserva, compresión, copias, deduplicación de datos y caché:** estas propiedades se pueden cambiar en el destino de replicación para afectar diferentes políticas de fiabilidad, rendimiento, flexibilidad y costos en el destino de replicación desde el origen.

- **Propiedades de punto de montaje y uso compartido** (por ejemplo, sharenfs, nombre de recurso SMB): estas propiedades controlan la manera en que se exportan los recursos compartidos a los clientes NAS y la forma en que se pueden cambiar para afectar diferentes políticas de protección o seguridad en el destino de replicación desde el origen.

Estas modificaciones de propiedades persisten en las actualizaciones de replicaciones.

FIGURA 29 Gestión de propiedades de paquetes de replicación



Temas relacionados

- [“Propiedades de proyectos y recursos compartidos” \[502\]](#)
- [“Corte de replicación” \[789\]](#)

Clonación de un recurso compartido o un paquete de replicación

Un *clon* de un paquete replicado es un proyecto local y mutable que puede ser gestionado como cualquier otro proyecto en el sistema. Cuando se crea el proyecto de clonación, se usa la instantánea más reciente de los recursos compartidos replicados para crear los recursos compartidos en el proyecto de clonación. Estos clones comparten el almacenamiento con las instantáneas de origen de la misma manera en la que lo hacen los clones de las instantáneas de los recursos compartidos (consulte Clonación de instantáneas [BUI](#), [CLI](#)). Este mecanismo se puede utilizar para el failover en caso de un problema catastrófico en el origen de la replicación o simplemente para proporcionar una versión local de los datos que se pueden modificar.

Mientras exista un clon, no se podrá destruir la instantánea de origen. Cuando se destruye una instantánea (posiblemente como resultado de la destrucción de un recurso compartido, proyecto o paquete de replicación del cual es miembro la instantánea), el sistema advierte a los administradores sobre clones dependientes que serán destruidos mediante la operación. Recuerde que las instantáneas también pueden ser destruidas en el origen en cualquier momento.

y dichas instantáneas se destruyen en el destino como parte de la actualización de replicación posterior. Si la instantánea en cuestión tiene clones, no se la podrá destruir hasta que se haya destruido el último clon.

Replicación de clones

Al replicar clones, es importante comprender la relación entre una réplica de un clon y su instantánea de origen. Por defecto, la réplica de un clon mantiene su relación con la instantánea de origen, lo que hace que también exista una réplica de la instantánea de origen en el destino. La réplica de una instantánea de origen del clon debe residir en la misma agrupación que el clon, pero no es necesario que esté en el mismo proyecto.

Para mantener la relación entre un clon replicado y su instantánea de origen, la instantánea de origen debe:

- haberse replicado en el destino antes de la replicación inicial del clon, o
- haberse replicado como parte de la misma actualización.

El software del dispositivo no controla que se cumpla esta restricción, pero se la debe respetar para garantizar que la actualización de la replicación se realice correctamente.

Hay varias maneras de garantizar la replicación correcta de un clon y mantener su relación con la instantánea de origen:

- Si la instantánea de origen de un clon está en el mismo proyecto, utilice la replicación de nivel de proyecto.
- Si el recurso compartido que incluye la instantánea de origen del clon no se encuentra en el mismo proyecto, o si el clon o el recurso compartido de origen se omitieron de la replicación en el nivel del proyecto, replique primero el recurso compartido de origen y, a continuación, replique el clon mediante replicación en el nivel del proyecto o el nivel del recurso compartido.
- En el sistema de destino, no destruya el origen del clon a menos que también desee destruir el clon en sí.

Para garantizar que la instantánea de origen se envíe al destino, siempre configure la propiedad Incluir instantáneas para la acción de replicación del origen.

De la misma manera en la que un clon y su instantánea de origen conservan espacio en el dispositivo de origen, un clon replicado y su instantánea de origen replicada conservan espacio en el destino de replicación. Si la conservación de espacio en el destino de replicación es menos importante, el administrador puede configurar la propiedad `Include clone origin as data`. Cuando se configura la propiedad, y la instantánea de origen del clon *no* se replica en la misma actualización que el clon, el dispositivo de origen inserta una copia del contenido de los datos de origen del clon en el clon de réplica. Así, no hay necesidad de replicar primero el recurso compartido de origen del clon, pero la copia de los datos de origen del clon consume espacio de almacenamiento adicional en el destino.

Cuando se configuran `Include snapshots` e `Include clone origin as data`, el clon de réplica incluye solo las instantáneas que están presentes en el clon en el origen. El dispositivo de origen inserta el contenido de los datos de origen del clon, no las instantáneas de origen del clon, en el clon de réplica. Esto garantiza que las instantáneas presentes en el clon de réplica coincidan con las instantáneas presentes en el clon que se encuentra en el origen.

La propiedad `Include clone origin as data` no afecta la replicación de un clon ni su instantánea de origen cuando se los replica en la misma actualización. Cuando se los replica juntos en la misma acción de replicación, la relación entre el clon y su instantánea de origen se conserva, y se mantiene la ventaja de uso compartido de espacio en el destino.

Temas relacionados

- [“Replicación de proyectos frente a replicación de recursos compartidos” \[725\]](#)
- Clonación de un paquete de replicación: [BUI](#), [CLI](#)
- [“Propiedades de proyectos y recursos compartidos” \[502\]](#)

Reversión a varios destinos

En una configuración de recuperación ante desastres que consiste en la replicación de un proyecto de un origen a varios destinos, cuando se realiza una replicación a uno de los destinos, la función de reversión a varios destinos permite seguir enviando actualizaciones incrementales desde el origen nuevo a todos los demás destinos configurados originalmente.

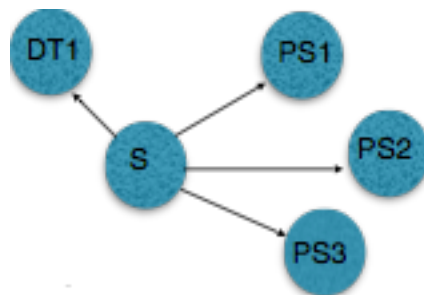
Configuración básica

Una configuración típica de reversión a varios destinos consta de las siguientes entidades:

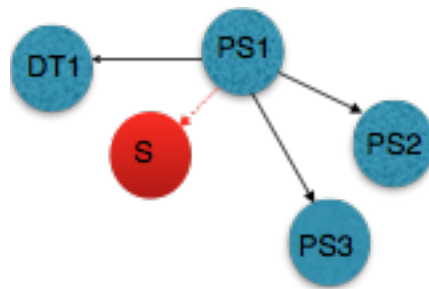
- **Origen:** un origen de replicación responsable de enviar actualizaciones de replicación y realizar la gestión de instantáneas. Debe haber exactamente un origen.
- **Origen potencial:** un origen potencial es un destino de replicación en la configuración de reversión a varios destinos que necesita hacerse cargo de enviar actualizaciones de replicación incrementales (además de otras tareas, como la gestión de instantáneas, etc.) a todos los destinos. Debe haber por lo menos un origen potencial.
- **Destino dedicado:** un destino dedicado es un destino de replicación en la configuración de reversión a varios destinos que no puede realizar una operación de reversión. El destino dedicado necesita menos instantáneas que un origen potencial. Los dispositivos que ejecutan una versión de software más antigua se pueden configurar como destino dedicado en una configuración de reversión a varios destinos. Los destinos dedicados pueden estar presentes o no en una configuración de reversión a varios destinos.
- **Grupo de reversión a varios destinos:** un grupo de acciones de replicación para el mismo juego de datos que permite realizar una reversión en uno de los destinos

potenciales. Después de la reversión, el origen nuevo puede seguir enviando actualizaciones incrementales a todos los destinos configurados originalmente.

En la siguiente figura, este ejemplo de configuración de reversión a varios destinos consta de un origen (S), tres orígenes potenciales (PS1, PS2 y PS3) y un destino dedicado (DT1). El origen es responsable de enviar actualizaciones a los destinos. Cuando el origen se apaga, se elige uno de los orígenes potenciales (en este caso, PS1) para que sea el origen nuevo.



Cuando se realiza una reversión en este origen nuevo, este sigue enviando actualizaciones incrementales a los demás destinos, como se muestra en la siguiente figura.



Gestión de grupo de reversión a varios destinos

Los grupos de reversión a varios destinos se crean mediante la configuración de por lo menos una acción de nivel de proyecto como origen potencial. En ausencia de un origen potencial, no se crea el grupo de reversión a varios destinos, y se permite la reversión en cualquier destino, pero esta solo creará una acción de replicación para replicar de nuevo al origen original.

Nota - Mientras se esté usando la reversión a varios destinos, se podrán conservar varias instantáneas de replicación para cada acción en el grupo de reversión a varios destinos.

Creación de un grupo de reversión a varios destinos

1. Configure un origen potencial.

El origen potencial se puede configurar en una acción de replicación de nivel de proyecto, como se muestra en la siguiente figura de la BUI.

Los cambios de configuración de una acción de replicación se propagan como parte de una actualización de replicación. No existen garantías de que dichos cambios de configuración se vayan a entregar a todos los miembros del grupo de varios destinos al mismo tiempo.

Add Replication Action [CANCEL] [ADD]

Properties

Target: spadefish

Pool: p

Export data path: ☐ nfs://

Limit bandwidth: ☐ 0 M/s

Enable SSL-encryption: ☒

Disable compression: ☐

Enable deduplication: ☐

Include snapshots: ☒

Retain user snapshots on target: ☐

Include clone origin as data: ☐

Disaster Recovery

Recovery point objective: ☐ hours

Replica lag warning alert: ☐ % of Recovery Point Objective

Replica lag error alert: ☐ % of Recovery Point Objective

Potential Source ☒

Distant Target: ☐

Schedule ... Cascading Schedule ... Snapshots

2. Cree destinos de replicación en los orígenes potenciales como se describe en [Creación de un destino de replicación \(BUI\) \[629\]](#) o [Creación de un destino de replicación \(CLI\) \[631\]](#).

Cuando se realice una reversión en un origen potencial, se crearán acciones en todos los destinos originales. Si no hay destinos de replicación configurados en el origen potencial, las acciones recién creadas no tendrán destinos de replicación. Por lo tanto, estas acciones nuevas estarán desenlazadas. Cuando se creen los destinos de replicación correspondientes más adelante, las acciones desenlazadas se enlazarán automáticamente a los destinos correctos.

Nota - Dado que el proceso de enlace automático utiliza la dirección IP del destino, es necesario crear destinos para los mismos dispositivos y las mismas direcciones IP que se utilizaron en el origen original.

Visualización de acciones desenlazadas en el origen mediante el uso de la CLI

- a. Seleccione el proyecto adecuado.
- b. Vaya al subnodo `replication` de ese proyecto.
- c. Utilice el comando `show` para visualizar las acciones como se muestra en la siguiente figura. El destino de las acciones desenlazadas es `<undefined>`.

```
eel:> shares select PRJ1
eel:shares PRJ1> replication
eel:shares PRJ1 replication> show
Properties:
    conflct_detected = false

Actions:

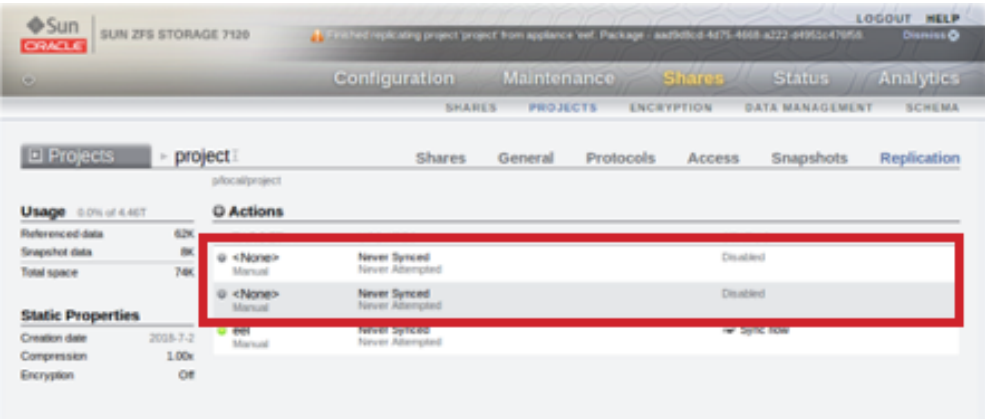

|            | TARGET      | STATUS | NEXT     |
|------------|-------------|--------|----------|
| action-000 | <undefined> | idle   | Disabled |
| action-001 | badenov     | idle   | Sync now |
| action-002 | <undefined> | idle   | Disabled |


Children:
    conflict => Conflict

eel:shares PRJ1 replication> █
```

Visualización de acciones desenlazadas en el origen mediante el uso de la BUI

- a. Seleccione el proyecto adecuado.
- b. Haga clic en Replicación.
- c. El destino de las acciones desenlazadas es indefinido (<None>).



Supervisión de destinos potenciales

Los paquetes de replicación de orígenes potenciales muestran una lista de destinos potenciales. Durante la reversión, se crearán acciones para los destinos potenciales además de la acción para replicar de nuevo al origen original. La lista incluye el nombre del destino o su dirección IP y el ID de paquete del destino correspondiente.

Los destinos potenciales se pueden supervisar como se muestra en la siguiente figura de CLI.

```

badenov:shares replication package-005> show
Properties:
    id = 5882bf43-34c9-4de3-a72a-ba6088fd40f0
    source_name = eel
    source_asn = 55e0948f-6659-4ec1-d6c6-b3acad5126eb
    source_ip = 10.133.64.218:216
    source_pool = e
    target_pool = ba
    replica_of = etl
    enabled = true
    conflict_detected = false
    state = idle
    state_description = Idle (no update in progress)
    offline = false
    import_path =
    data_timestamp = Mon Aug 06 2018 14:57:14 GMT+0000 (UTC)
    last_sync = Mon Aug 06 2018 14:57:32 GMT+0000 (UTC)
    last_try = Mon Aug 06 2018 14:57:32 GMT+0000 (UTC)
    last_result = success

Projects:
    etl

Children:
    potential_targets => Show Potential Targets to be created after Reverse

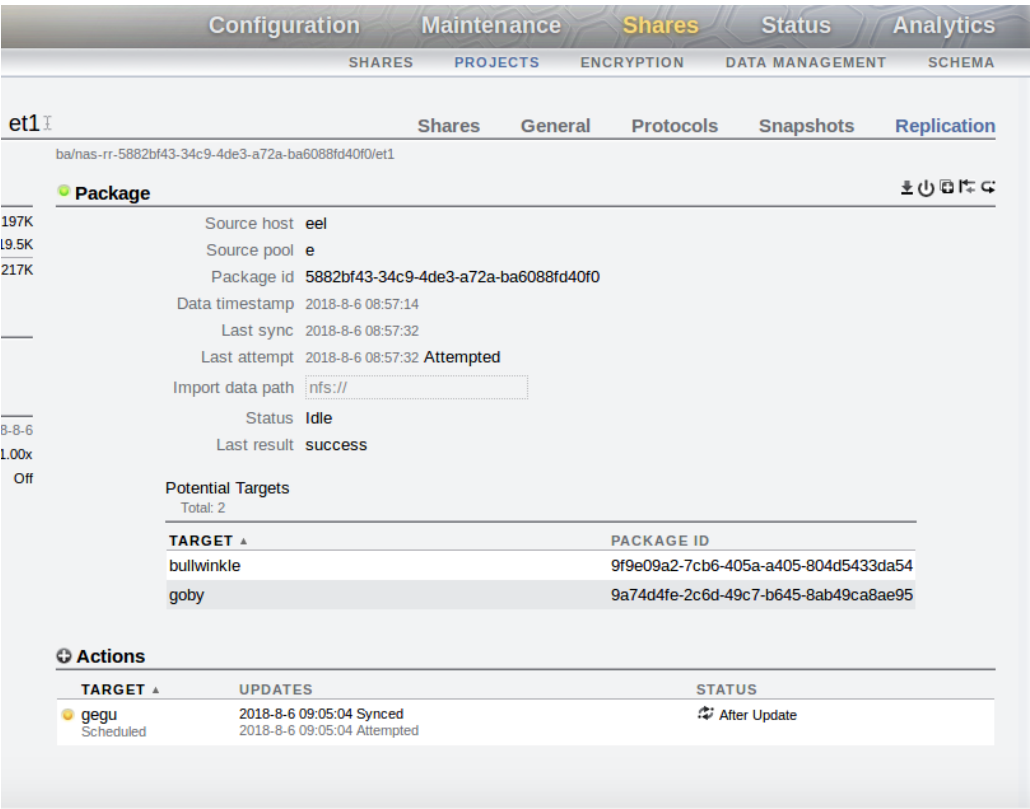
badenov:shares replication package-005> potential_targets
badenov:shares replication package-005 potential_targets> show
Targets:

NODE      TARGET      PACKAGE ID
target-000 goby        9a74d4fe-2c6d-49c7-b645-8ab49ca8ae95
target-001 bullwinkle 9f9e09a2-7cb6-405a-a405-804d5433da54

badenov:shares replication package-005 potential_targets> 

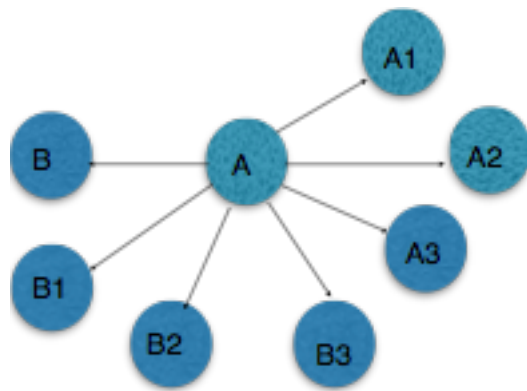
```

Los destinos potenciales se pueden supervisar como se muestra en la siguiente figura de BUI.



Detección y resolución de conflictos

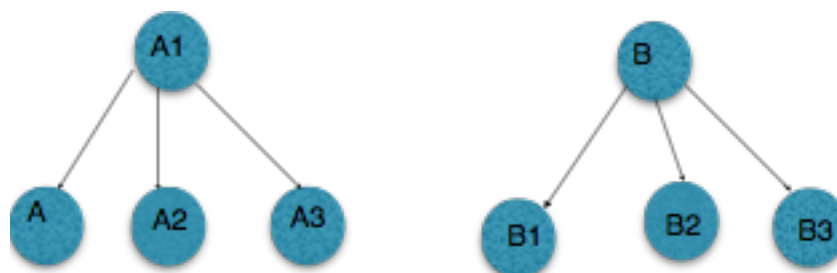
En la siguiente figura de un grupo de reversión a varios destinos, A es el origen del grupo.



En cualquier momento, debería existir solo un origen en un grupo de reversión a varios destinos. Puede surgir un conflicto cuando exista más de un origen, como en los siguientes escenarios.

- A causa de un error de administración cuando se realiza una reversión en dos o más orígenes potenciales que reciben actualizaciones del mismo origen de replicación.
- En caso de que ocurra una segmentación de la red, el administrador puede optar por crear varios segmentos de reversión a varios destinos, cada uno con su propio origen. Después de recuperarse de la segmentación de la red, los orígenes de cada uno de los segmentos de reversión a varios destinos intentan enviarse actualizaciones entre sí y esto origina un conflicto.

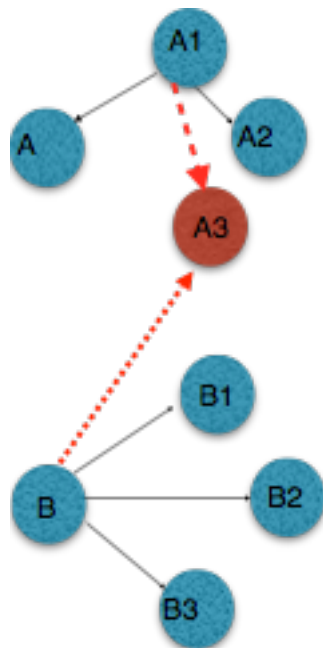
Como se muestra en la siguiente figura, ahora hay dos orígenes: A1 y B.



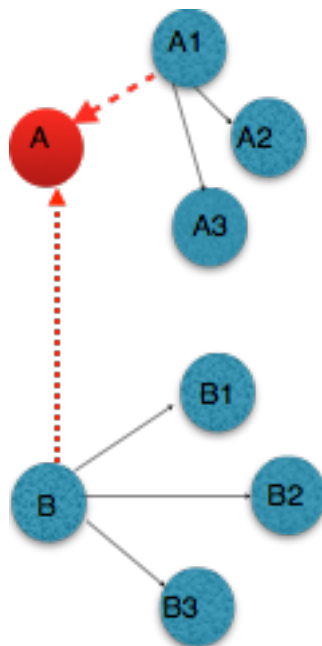
Detección de conflictos en el origen y el destino

1. Como se muestra en la siguiente figura, se detecta un conflicto en los destinos cuando dos o más orígenes intentan enviar actualizaciones al mismo destino. En este escenario, las

actualizaciones de un origen se llevarán a cabo sin problemas y ese origen podrá seguir enviando actualizaciones correctas al destino. Las actualizaciones de otros orígenes fallarán con una alerta específica, y el destino mostrará una notificación de conflicto que le pedirá al administrador que seleccione el origen correcto para resolver el conflicto. Una vez que el conflicto se haya resuelto, el destino recibirá la actualización del origen definido por el administrador. Sin embargo, si el origen incorrecto sigue enviando una actualización, se emitirá una alerta nueva en el origen incorrecto, y se emitirá nuevamente una notificación de resolución de conflicto en el destino.



2. Se detecta un conflicto cuando el origen (nodo B) de un grupo envía una actualización a un origen de otro grupo (nodo A1), como se muestra en la siguiente figura. La actualización del nodo que envía la actualización (nodo B) fallará con una alerta, y el origen que recibe la actualización (nodo A1) mostrará una notificación de conflicto que le pedirá al administrador que seleccione el origen correcto para resolver el conflicto. Una vez que se haya resuelto el conflicto, el origen incorrecto convertirá su proyecto a un paquete en la siguiente actualización y, por lo tanto, se convertirá en destino.



Nota - Cuando el destino recibe actualizaciones de orígenes incorrectos, la reversión de datos se puede realizar durante la primera actualización del origen correcto.

Ejemplo de una alerta de CLI emitida en el origen que ocasionó el conflicto:

```
entry-44068 2018-7-6 20:22:24 18b967b0-ebef-4adf-b360-e7d8afd83ca3,
Replication of 'PRJ1' to 'eel' failed because
the target's reversal history is out-of-sync
with this appliance. Action -
dd0bcea7-d8d6-41ca-9d2e-bce7d89e37de., Minor
Alert
goby:maintenance logs alert> select entry-44068
goby:maintenance logs alert entry-44068> show
Properties:
        timestamp = 2018-7-6 20:22:24
        uuid = 18b967b0-ebef-4adf-b360-e7d8afd83ca3
        description = Replication of 'PRJ1' to 'eel' failed because th
e target's reversal history is out-of-sync with this appliance. Action - dd0bcea7
-d8d6-41ca-9d2e-bce7d89e37de.
        type = Minor Alert
goby:maintenance logs alert entry-44068> █
```

Ejemplo de una alerta de BUI emitida en el origen que ocasionó el conflicto:

The screenshot shows the Oracle ZFS Storage Appliance web interface. At the top, there is a navigation bar with tabs for Configuration, Maintenance (highlighted), Shares, Status, and Analytics. Below this is a sub-navigation bar with links for Hardware, System, Problems, Logs, and Workflows. The main content area displays an 'Alert Details' for entry-44068. The alert description states: 'Replication of 'PRJ1' to 'eel' failed because the target's reversal history is out-of-sync with this appliance. Action - dd0bcea7-d8d6-41ca-9d2e-bce7d89e37de.' The alert type is 'Minor Alert' and the impact is 'The replication update failed.' The recommended action is to override the replication source on the target system. The event time is 2018-7-6 14:22:24 and the unique identifier is 18b967b0-ebef-4adf-b360-e7d8afd83ca3. The status is 'The problem associated with this alert has been repaired.'

Pasos generales para resolver un conflicto

1. Desactive las actualizaciones de todos los orígenes.

2. Seleccione el origen correcto.
3. En el destino, defina el origen correcto para resolver el conflicto. Para ello, siga el siguiente procedimiento de Destino en la CLI o la BUI.
4. En el origen incorrecto, defina el origen correcto para resolver el conflicto. Para ello, siga el siguiente procedimiento de Origen en la CLI o la BUI.
5. Active las actualizaciones del origen correcto.

Nota - 1) Las actualizaciones de otros orígenes harán que se muestren las notificaciones de conflicto correspondientes.

2) La herramienta de resolución de conflictos no almacena información de forma persistente. Si el nodo se reinicia por cualquier motivo, las selecciones de conflicto y resolución serán descartadas, y las actualizaciones de los orígenes que habían ocasionado el conflicto antes del reinicio mostrarán la notificación de conflicto nuevamente.

Destino: uso de la CLI para resolver conflictos

1. Seleccione el paquete de replicación adecuado, vaya al proyecto y luego seleccione replication.
2. Compruebe el valor de la propiedad `conflict_detected`. Cuando es `true`, indica que se ha detectado un conflicto.
3. Vaya al subnodo `conflict` y, para resolver el conflicto, configure el valor de la propiedad `source` en el origen correcto, como se muestra en la siguiente figura.

```

bullwinkle:> shares replication packages
bullwinkle:shares replication packages> list
ID          STATE DATA_TIMESTAMP SOURCE DATASET
package-002 idle unknown alestes all
package-001 idle 2018-07-03 23:26:31 alestes al2
package-004 idle 2018-06-29 23:48:41 badenov sa
package-005 idle 2018-07-06 20:21:08 eel PRJ1
package-003 idle 2018-07-02 01:56:36 spadefish sl
bullwinkle:shares replication packages> select package-005
bullwinkle:shares replication package-005> select PRJ1 replication
bullwinkle:shares replication package-005 PRJ1 replication> show
Properties:
    conflict_detected = true

Children:
    conflict => Conflict

bullwinkle:shares replication package-005 PRJ1 replication> conflict
bullwinkle:shares replication package-005 PRJ1 replication conflict> show
Properties:
    source = (unset)

Sources:
SOURCE      HOSTNAME ACTION_ID PROJECT
current     eel      ccc77f57-450e-42a1-99fe-b3f319003954 PRJ1
source-0    goby     78915d04-44e4-420e-b48a-8eac3f027f71 PRJ1

bullwinkle:shares replication package-005 PRJ1 replication conflict> set source=current
    source = current (uncommitted)
bullwinkle:shares replication package-005 PRJ1 replication conflict> commit
bullwinkle:shares replication package-005 PRJ1 replication conflict> show
Properties:
    source = (unset)

bullwinkle:shares replication package-005 PRJ1 replication conflict> █

```

Destino: uso de la BUI para resolver conflictos

1. Seleccione el paquete de replicación.
 2. Haga clic en Replicación.
- Debería aparecer una notificación de conflicto, como se muestra en la siguiente figura.

The screenshot shows the SpadeFish web interface. At the top, there's a navigation bar with 'Configuration', 'Maintenance', 'Shares' (highlighted), 'Status', and 'Analytics'. Below this is a sub-navigation bar with 'SHARES', 'PROJECTS', 'ENCRYPTION', 'DATA MANAGEMENT', and 'SCHEMA'. The main content area is titled 'project' and has tabs for 'Shares', 'General', 'Protocols', 'Snapshots', and 'Replication' (selected). The 'Replication' tab shows a list of packages. One package is highlighted with a red box, indicating a conflict. The package details are as follows:

Package
Source host: eel
Source pool: g
Package id: ae40a38f-d5d6-43de-b10e-8d32555ae920
Data timestamp: 2018-7-2 14:25:53
Last sync: 2018-7-2 14:26:11
Last attempt: 2018-7-2 14:26:11 Attempted
Import data path: nfs://
Status: Idle
Last result: success

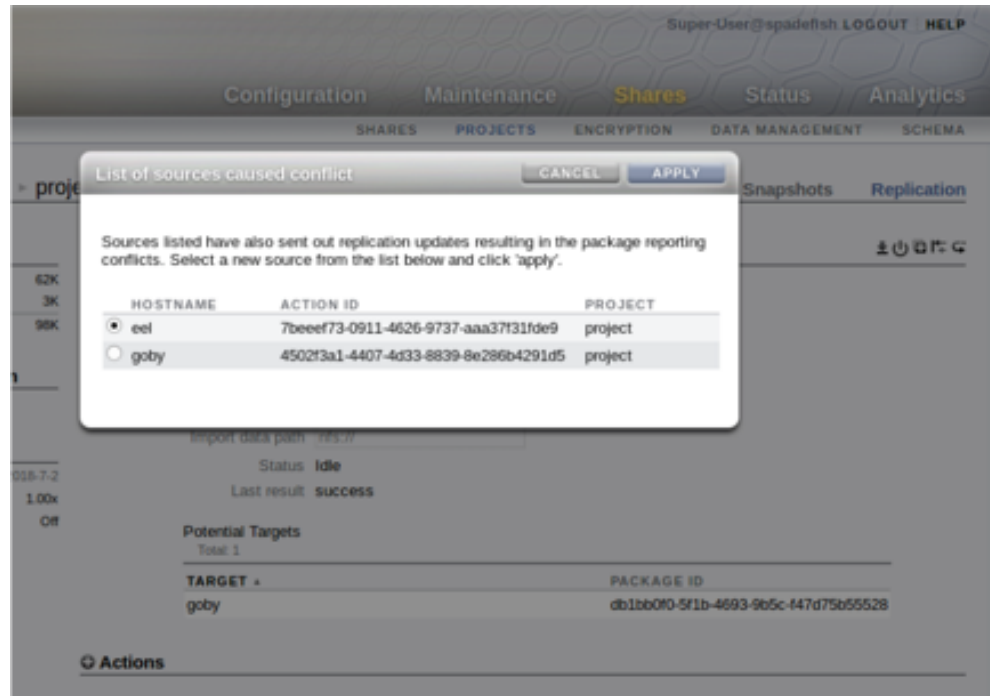
Potential Targets

TARGET	PACKAGE ID
goby	db1bb0f0-5f1b-4693-9b5c-f47d75b55528

Actions

No replication actions are in effect.
Click to define a new replication action.

3. Haga clic en la notificación de conflicto para abrir el cuadro de diálogo de resolución de conflicto de replicación, como se muestra en la siguiente figura.



4. Seleccione el origen correcto y haga clic en APLICAR.
Ahora no se producirán errores al ejecutar las actualizaciones de ese origen.

Origen: uso de la CLI para resolver conflictos

1. Seleccione el proyecto revertido de manera incorrecta.
2. Vaya al subnodo `replication` de ese proyecto.
3. Compruebe el valor de la propiedad `conflict_detected`. Cuando es `true`, indica que se ha detectado un conflicto.
4. Vaya al subnodo `conflict` y, para resolver el conflicto, configure el valor de la propiedad `source` en el origen correcto, como se muestra en la siguiente figura.

A partir de este punto, la actualización del origen seleccionado hará que el proyecto se convierta en un paquete de replicación.


```

goby:> shares select PRJ1 replication
goby:shares PRJ1 replication> show
Properties:
    conflict_detected = true

Actions:

    TARGET      STATUS      NEXT
action-000     badenov     idle       Sync now
action-001     eel         idle       Sync now
action-002     bullwinkle  idle       Sync now

Children:
    conflict => Conflict

goby:shares PRJ1 replication> conflict
goby:shares PRJ1 replication conflict> show
Properties:
    source = (unset)

Sources:

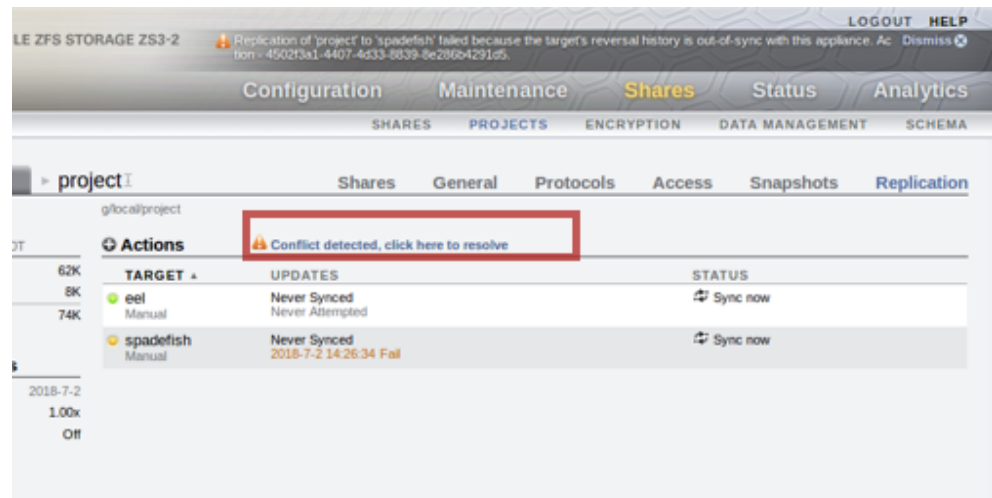
SOURCE      HOSTNAME      ACTION_ID      PROJECT
current     <current>
source-0    10.133.65.110  e99f0ea4-7328-488e-925e-8dccb3084b3d  PRJ1

goby:shares PRJ1 replication conflict> set source=source-0
    source = source-0 (uncommitted)
goby:shares PRJ1 replication conflict> commit
goby:shares PJ1 replication conflict> 

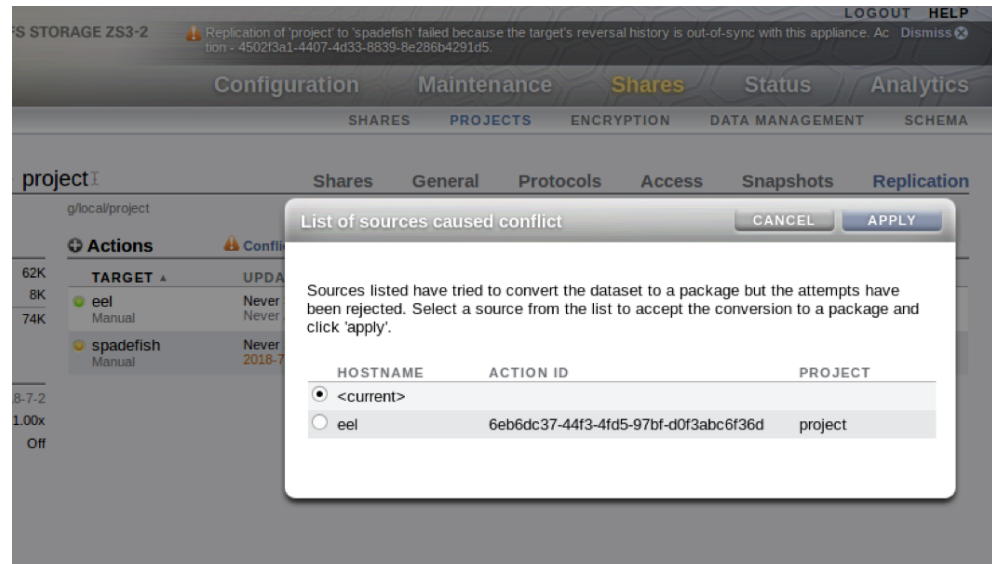
```

Origen: uso de la BUI para resolver conflictos

1. En el origen incorrecto, seleccione el proyecto creado por la reversión no deseada.
2. Haga clic en Replicación.
Debería aparecer la notificación de conflicto, como se muestra en la siguiente figura.



3. Haga clic en la notificación de conflicto para abrir el cuadro de diálogo de resolución de conflicto de replicación, como se muestra en la siguiente figura.



4. Seleccione el origen correcto y haga clic en APLICAR.

La primera actualización de ese origen convertirá el proyecto en un paquete de replicación y la actualización de ese origen debería completarse correctamente.

Consideraciones de compatibilidad

Cuando configure la reversión a varios destinos, siga estas reglas de compatibilidad:

- Solo los destinos que son compatibles con la reversión a varios destinos o que ejecutan una versión de firmware OS8.7.0 y posterior pueden ser miembros de un grupo de reversión a varios destinos.
- Solo los destinos que son compatibles con la reversión a varios destinos se pueden configurar como orígenes potenciales.
- Solo los destinos que ejecutan una versión de firmware OS8.7.0 y posterior se pueden configurar como destinos dedicados en un grupo de reversión a varios destinos.

Los siguientes fallos se producen debido a la incompatibilidad. Esta lista no es exhaustiva.

- Se produce un error durante la configuración de un origen potencial en una acción de replicación a un destino que no es compatible con la reversión a varios destinos.
- Se produce un error durante la configuración de un origen potencial en un juego de datos con acciones de replicación existentes a destinos que ejecutan una versión de firmware anterior a OS8.7.0.
- Se produce un error durante la configuración de una acción de replicación a un destino que ejecuta una versión de firmware anterior a OS8.7.0 en un grupo de reversión a varios destinos existente.
- Los destinos que forman parte de un grupo de reversión a varios destinos y que están configurados como destinos dedicados, pero ejecutan una versión de firmware anterior a OS8.8.6, pueden realizar una reversión de replicación. No obstante, estos no podrán ejecutar una actualización de replicación en su origen. No se pueden recuperar relaciones de replicación en ese escenario.

Implicaciones de retención de instantánea automática

Cuando se utiliza la retención de instantáneas automática para algunos destinos, pero no para otros, en la configuración de una reversión a varios destinos, después de la reversión, los destinos que no especificaron un valor de retención de instantáneas automática conservan la misma cantidad de instantáneas que el origen nuevo, que puede ser distinta a la de los destinos anteriores. Para evitar esta situación, configure la política de retención para cada destino de un grupo de varios destinos como "independiente". Para obtener más información,

consulte [Configuración de retención de instantáneas automáticas en un destino \(BUI\) \[638\]](#) o [Configuración de retención de instantáneas automáticas en un destino \(CLI\) \[639\]](#).

Temas relacionados

- [Recuperación ante desastres con replicación remota](#)
- [Managing Replication Packages](#)
- [“Reversión de la dirección de replicación” \[790\]](#)

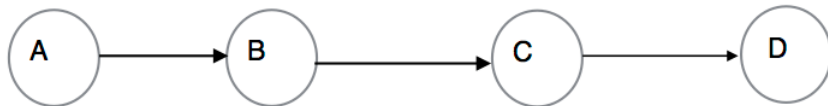
Replicación en cascada

La replicación en cascada permite configurar acciones de replicación en paquetes de replicación para replicar datos. Es posible crear varias acciones de replicación en el mismo paquete para replicarlo en varios dispositivos de destino.

Configuración básica

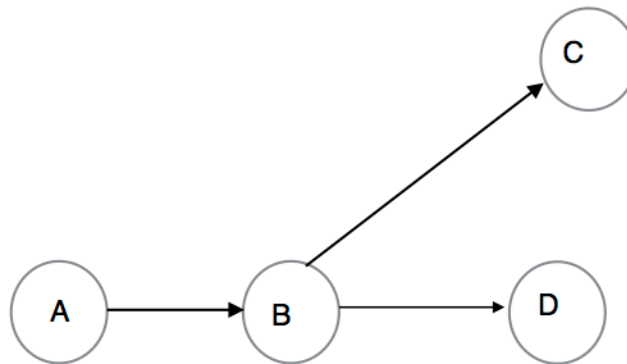
Una configuración básica de replicación en cascada se compone de un origen, uno o varios destinos intermedios y un destino final.

En el siguiente ejemplo, la replicación en cascada se compone de un nodo de origen A que contiene una acción configurada en uno de sus proyectos para replicarlo en un paquete del nodo B. A su vez, el nodo B contiene una acción creada para replicar este paquete en otro paquete del nodo C, y el nodo C contiene una acción configurada en este paquete para replicarlo en un paquete del nodo D. Por tanto, el nodo B y el nodo C colocan en cascada una réplica del nodo A en el nodo D, como se muestra en la siguiente figura.



Como se muestra en la siguiente figura, el nodo de origen A contiene una acción configurada en uno de sus proyectos para replicarlo en un paquete del nodo B. A su vez, el nodo B contiene

acciones creadas para replicar este paquete en el nodo c y el nodo d. Por tanto, el nodo b coloca en cascada una réplica del nodo a en los nodos c y d.



La replicación inversa de una configuración en cascada solo se admite en los nodos que reciben actualizaciones de replicación directamente del origen (el nodo b en el ejemplo anterior), y la reversión se encuentra desactivada en los otros nodos (los nodos c y d). Se recomienda considerar la reversión de varios destinos cuando se planea ejecutar la recuperación ante desastres en una configuración de replicación en cascada. Consulte [“Reversión a varios destinos” \[750\]](#) y "Uso de la propiedad `distant_target` para gestionar reversiones" en las siguientes secciones.

Gestión de replicaciones en cascada

La gestión de una replicación en cascada abarca dos tareas:

- Crear una acción en el paquete de replicación
- Configurar programas de replicación en cascada

Crear una acción en el paquete de replicación

De forma similar a la creación de una acción de replicación en un proyecto, es posible crear una acción de replicación en un paquete de replicación. En la siguiente figura, se muestra la forma de crear una acción en un paquete de replicación mediante la BUI.

Tenga en cuenta que la replicación en el nivel de recurso compartido no admite la replicación en cascada. No se pueden configurar acciones en recursos compartidos de paquetes de replicación

ni acciones en paquetes creados como resultado de una replicación en el nivel de recurso compartido.

Add Replication Action [CANCEL] [ADD]

Properties

Target: system-A
 Pool: ba
 Export data path: ☐ nfs://
 Limit bandwidth: ☐ 0 M/s
 Enable SSL-encryption: ☒
 Disable compression: ☐
 Enable deduplication: ☐
 Include snapshots: ☒
 Retain user snapshots on target: ☐
 Include clone origin as data: ☐

Disaster Recovery

Recovery point objective: ☒ 30 hours
 Replica lag warning alert: ☒ 80 % of Recovery Point Objective
 Replica lag error alert: ☒ 95 % of Recovery Point Objective

Cascading Schedule : Schedule : Snapshots

Replication Schedules

FREQUENCY
 After Update delay: ☐ minutes

En la siguiente figura, se muestra la forma de crear una acción en un paquete de replicación mediante la CLI.

```

bullwinkle:> shares replication packages select id=17dc3fdf-0a69-411d-84eb-b6ae3f0baca0
bullwinkle:shares replication package-006> select fyl8 replication
bullwinkle:shares replication package-006 fyl8 replication> action
bullwinkle:shares replication package-006 fyl8 action (uncommitted)> set target=syste
system-A system-C
bullwinkle:shares replication package-006 fyl8 action (uncommitted)> set target=system-C
target = system-C (uncommitted)
bullwinkle:shares replication package-006 fyl8 action (uncommitted)> set pool=p
pool = p (uncommitted)
bullwinkle:shares replication package-006 fyl8 action (uncommitted)> commit
bullwinkle:shares replication package-006 fyl8 replication> 

```

Configurar programas de replicación en cascada

Cada acción tiene dos programas:

- Un programa en una acción configurada como parte de un proyecto se denomina programa de origen.
- Un programa en una acción configurada como parte de un paquete se denomina programa en cascada.

En la siguiente figura, se muestra la forma de configurar un programa en cascada nuevo en una acción de replicación mediante la CLI.

```

bullwinkle:> shares replication packages select id=f8e61e67-3d6c-434f-85e7-d9d2e08fe60d
bullwinkle:shares replication package-006> select fy18 replication
bullwinkle:shares replication package-006 fy18 replication> list
      TARGET      STATUS      NEXT
action-000 system-C      idle      Sync now
bullwinkle:shares replication package-006 fy18 replication> select action-000
bullwinkle:shares replication package-006 fy18 action-000> list
bullwinkle:shares replication package-006 fy18 action-000> schedule
bullwinkle:shares replication package-006 fy18 action-000 schedule (uncommitted)> set frequency=halfhour
      frequency = halfhour (uncommitted)
bullwinkle:shares replication package-006 fy18 action-000 schedule (uncommitted)> set minute=25
      minute = 25 (uncommitted)
bullwinkle:shares replication package-006 fy18 action-000 schedule (uncommitted)> commit
bullwinkle:shares replication package-006 fy18 action-000> list

NAME                FREQUENCY      DAY      HH:MM
schedule-000        halfhour      -      -:25
bullwinkle:shares replication package-006 fy18 action-000> schedules
bullwinkle:shares replication package-006 fy18 action-000 schedules> list
Properties:
      active_schedule = cascading

Children:
      cascading => Configure cascading replication update schedules
      source => Configure source replication update schedules

bullwinkle:shares replication package-006 fy18 action-000 schedules> cascading
bullwinkle:shares replication package-006 fy18 action-000 schedules cascading> list

NAME                FREQUENCY      DAY      HH:MM
schedule-000        halfhour      -      -:25
bullwinkle:shares replication package-006 fy18 action-000 schedules cascading> cd ..
bullwinkle:shares replication package-006 fy18 action-000 schedules> cd ..
bullwinkle:shares replication package-006 fy18 action-000>

```

En la siguiente figura, se muestra la forma de configurar un programa en cascada nuevo en una acción de replicación mediante la BUI.

Cascading Schedule :: **Schedule** :: **Snapshots**

Replication Schedules

FREQUENCY

After Update delay: ☒ 1 minutes

Es posible configurar ambos programas en cualquier momento, pero solamente un programa entra en vigor, según la ubicación donde se configure la acción. Si se produce un cambio en la topología de replicación como resultado de una conversión o reversión de replicación, el

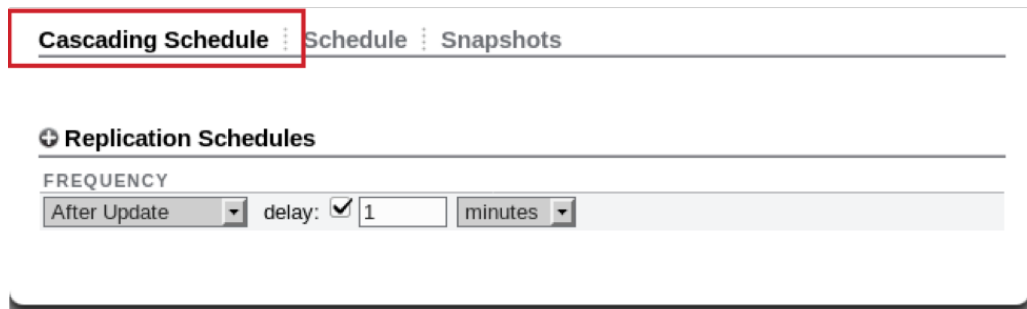
programa vigente puede cambiar. Por ejemplo, cuando se ejecuta una reversión en un paquete de replicación, las acciones configuradas en el paquete revertido pasan a configurarse en el proyecto y sus programas de origen se activan. De forma similar, cuando se ejecuta una conversión de replicación en un proyecto, las acciones anteriormente configuradas en el proyecto pasan a configurarse en el paquete y sus programas en cascada se activan.

En la siguiente figura, se muestra la forma de ver el programa vigente mediante la CLI.

```
bullwinkle:> shares replication packages select id=17dc3fdf-0a69-411d-84eb-b6ae3f0baca0
bullwinkle:shares replication package-006> select fy18 replication
bullwinkle:shares replication package-006 fy18 replication> list
      TARGET      STATUS      NEXT
action-000 system-C      idle      Fri Jul 20 2018 17:55:00 GMT+0000 (UTC)
bullwinkle:shares replication package-006 fy18 replication> select action-000
bullwinkle:shares replication package-006 fy18 action-000> list

NAME          FREQUENCY      DAY      HH:MM
schedule-000  halfhour      -        -:25
schedule-001  after_update  -        -: -
bullwinkle:shares replication package-006 fy18 action-000> schedules
bullwinkle:shares replication package-006 fy18 action-000 schedules> show
Properties:
    active_schedule = cascading
Children:
    cascading => Configure cascading replication update schedules
    source => Configure source replication update schedules
bullwinkle:shares replication package-006 fy18 action-000 schedules> █
```

En la siguiente figura, se muestra la forma de ver el programa vigente mediante la BUI. El separador de programa en el extremo izquierdo de una acción es el programa vigente.



Cuando se crean acciones nuevas durante la reversión de una replicación, se conservan los programas de origen y en cascada. Consulte [“Reversión de la dirección de replicación” \[790\]](#) y [“Reversión a varios destinos” \[750\]](#).

La opción `after_update` se encuentra disponible para los programas en cascada. Cuando se establece, esta opción inicia la actualización únicamente después de que se completa una actualización entrante.

Es posible utilizar la propiedad `update_cascade_delay` para especificar la demora entre la finalización de una actualización de replicación entrante y el inicio de la actualización en cascada saliente. Esta propiedad entra en vigor solamente cuando se selecciona la opción `after_update`.

La opción `after_update` y la propiedad `update_cascade_delay` se pueden configurar como se muestra en la siguiente figura.

```

bullwinkle:> shares replication packages select id=17dc3fdf-0a69-411d-84eb-b6ae3f0baca0
bullwinkle:shares replication package-006> select fy18 replication
bullwinkle:shares replication package-006 fy18 replication> select id=c6cc1699-12f9-476b-8e75-a15a29de98bd
bullwinkle:shares replication package-006 fy18 action-000> list
NAME                FREQUENCY          DAY                HH:MM
schedule-000        halfhour            -                  -:25
schedule-001        after update        -                  -: -
bullwinkle:shares replication package-006 fy18 action-000> schedules
bullwinkle:shares replication package-006 fy18 action-000 schedules> list
Properties:
    active_schedule = cascading

Children:
    cascading => Configure cascading replication update schedules
    source => Configure source replication update schedules

bullwinkle:shares replication package-006 fy18 action-000 schedules> cascading
bullwinkle:shares replication package-006 fy18 action-000 schedules cascading> show
Properties:
    update_cascade_delay = 2 minutes

Schedules:
NAME                FREQUENCY          DAY                HH:MM
schedule-000        halfhour            -                  -:25
schedule-001        after update        -                  -: -

bullwinkle:shares replication package-006 fy18 action-000 schedules cascading> set update_cascade_delay=90sec
error: invalid property value "90sec": Must be a valid time unit. Valid units: seconds,minutes,hours,days,weeks,month
and their singular form
bullwinkle:shares replication package-006 fy18 action-000 schedules cascading> set update_cascade_delay=90seconds
update_cascade_delay = 90 seconds (uncommitted)
bullwinkle:shares replication package-006 fy18 action-000 schedules cascading> commit
bullwinkle:shares replication package-006 fy18 action-000 schedules cascading>

```

Tenga en cuenta que la opción de programa continuo no se encuentra disponible para las acciones en paquetes y que las acciones de replicación en cascada no crean instantáneas de replicación nuevas. Cuando el origen emite una actualización nueva, las acciones en cascada utilizan la última instantánea de paquete para ejecutar las actualizaciones de replicación en sus

destinos. Por lo tanto, si se ejecuta una actualización en una acción en cascada sin antes recibir una actualización del origen, esta no surtirá efecto; se establecerá el estado de actualización correcta y se actualizará la propiedad `last_try`.

Uso de la propiedad `distant_target` para gestionar reversiones

En una replicación en cascada, una relación de destino distante entre los dos nodos diferencia los destinos locales y distantes. La propiedad `distant_target` conserva esta relación tras las transformaciones de la topología que se producen cuando se ejecuta una conversión o reversión de replicación.

En los siguientes escenarios de configuración, se ilustra la propiedad `distant_target`:

1. Cuando no se establece la propiedad `distant_target` y no se configura ninguna reversión de varios destinos. En este caso, cuando se ejecuta una reversión en un destino, no se conservan todas las acciones. Para obtener más información, consulte [“Reversión a varios destinos” \[750\]](#). Como se muestra en la siguiente figura, ni el nodo A ni el B tienen una relación de destino distante, y el nodo B no se configuró como origen potencial (acción AB: `potential_source=false`, `distant_target=false`).



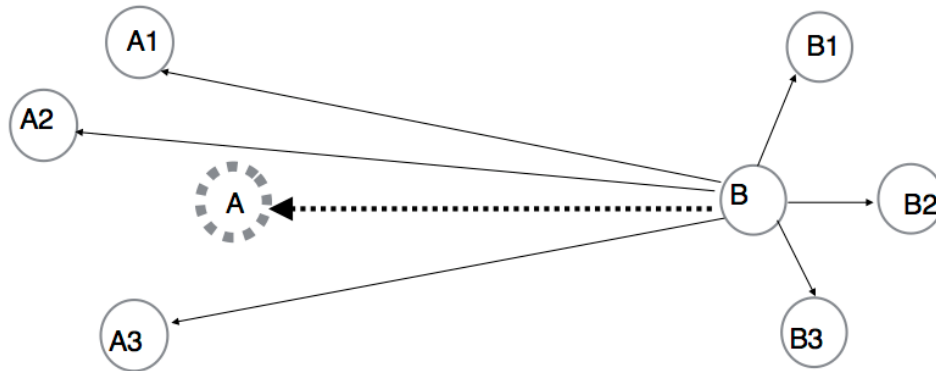
Cuando se produce un fallo en A y se ejecuta una reversión en B, no se crea ninguna acción en A{1..3}, como se muestra en la siguiente figura.



2. Cuando no se establece la propiedad `distant_target` y se configura una reversión de varios destinos. En este caso, cuando se ejecuta una reversión en un origen potencial, se crean acciones en todos los destinos del grupo de reversiones de varios destinos. No existe una relación de destino distante; por lo tanto, no se diferencian los destinos locales de los distantes. El nodo `A` es el origen y el nodo `B` es el origen potencial, como se muestra en la siguiente figura. Los nodos `A` y `B` no tienen una relación de destino distante (acción `AB`: `potential_source=true`, `distant_target=false`).



No obstante, cuando se produce un fallo en el nodo A y el nodo B es el nuevo origen después de que se ejecuta una reversión, se crean acciones en A{1..3}, como se muestra en la siguiente figura.



3. Cuando se establece la propiedad `distant_target` y se configura una reversión de varios destinos. En este caso, cuando se ejecuta una reversión en un origen potencial, no se crean acciones en los destinos que son locales para el origen distante. El nodo A es el origen y el nodo B es el origen potencial, como se muestra en la siguiente figura. Los nodos A y B tienen una relación de destino distante (acción AB: `potential_source=true`, `distant_target=true`).



Cuando se produce un fallo en el nodo A, después de una reversión en el nodo B, el nodo B se convierte en el nuevo origen. No obstante, debido a la relación de destino distante entre A y B, no se crean acciones en A{1..3}. Una vez que A se recupera, coloca en cascada su paquete en A{1..3}.



En la siguiente figura, se muestra la forma de configurar un destino distante mediante la CLI.

```
badenov:> shares
badenov:shares> replication
badenov:shares replication> actions
badenov:shares replication actions> select action-005
badenov:shares replication action-005> get distant_target
    distant_target = false
badenov:shares replication action-005> set distant_target=true
    distant_target = true (uncommitted)
badenov:shares replication action-005> commit
badenov:shares replication action-005> □
```

En la siguiente figura, se muestra la forma de configurar un destino distante mediante la BUI.

Edit Replication Action
CANCEL
APPLY

Properties

Target system-B [Retarget](#)
Target pool bu
Target package id 17dc3fdf-0a69-411d-84eb-b6ae3f0baca0
Export data path ☐ nfs://
Limit bandwidth ☐ 0 M/s
Enable SSL-encryption ☐
Disable compression ☐
Enable deduplication ☐
Include snapshots ☒
Retain user snapshots on target ☐
Include clone origin as data ☐

Disaster Recovery

Recovery point objective ☐ hours
Replica lag warning alert ☐ % of Recovery Point Objective
Replica lag error alert ☐ % of Recovery Point Objective
Potential Source ☒
Distant Target ☒

Schedule :: Cascading Schedule :: Snapshots

Update frequency ☒ Scheduled ☐ Continuous

Replication Schedules

FREQUENCY
Every 10 Minutes scheduled time: 00, 10, 20, ..., 50 minutes past the hour

Para configurar una reversión de varios destinos, si se utiliza la replicación en cascada, se recomienda establecer un origen potencial; de lo contrario, es posible que no se pueda regresar a la configuración en cascada original después de varias versiones de replicación. Además,

solamente se puede establecer un destino distante si existe un origen potencial configurado. Para obtener más información, consulte [“Reversión a varios destinos” \[750\]](#).

Escenarios de fallo

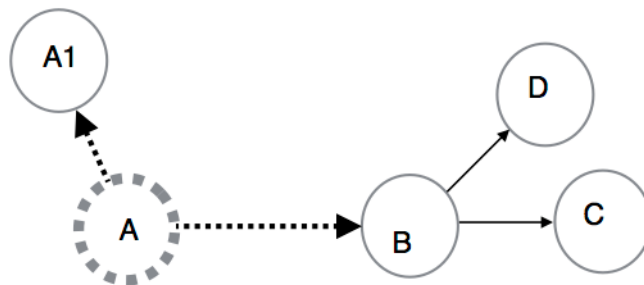
El fallo de un solo nodo en una replicación en cascada puede afectar a varios dispositivos o varios centros de datos conectados entre sí por relaciones de replicación. Si bien la topología de replicación en cascada no presenta limitaciones, los siguientes escenarios de fallo son típicos:

- Fallo en el origen original
- Fallo en el destino intermedio
- Fallo en el sitio de origen

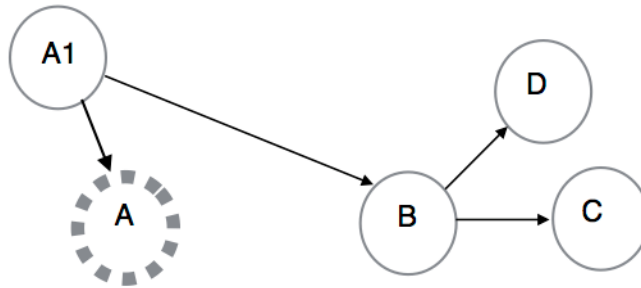
Fallo en el origen original

En este escenario, se produce un fallo en el origen de la cadena en cascada. La recuperación de este fallo requiere una configuración inicial de reversión de varios destinos en el origen. El proceso se inicia en un destino con la ejecución de una reversión de replicación. El destino revertido se convierte en el origen y continúa enviando las actualizaciones incrementales a los demás destinos originales y al origen original. Para obtener más detalles, consulte [“Reversión a varios destinos” \[750\]](#).

Como se muestra en la siguiente figura, A es el origen y A1 es el origen potencial. A se replica en A1 y B. A su vez, B se replica en C y D, y el origen A falla.

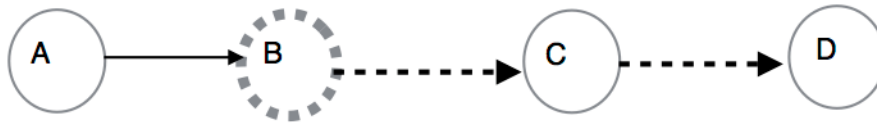


Como se muestra en la siguiente figura, después de que se ejecuta una reversión en A1, este se replica en A (cuando A se recupera) y en B, el cual, a su vez, continúa enviando las actualizaciones a C y D.

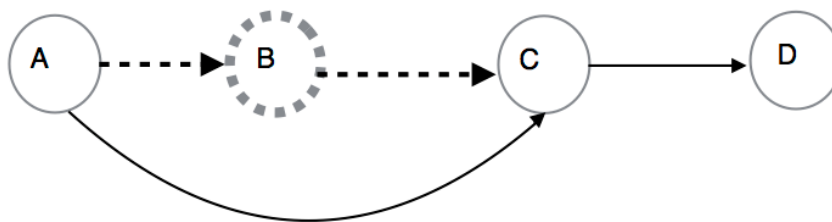


Fallo en el destino intermedio

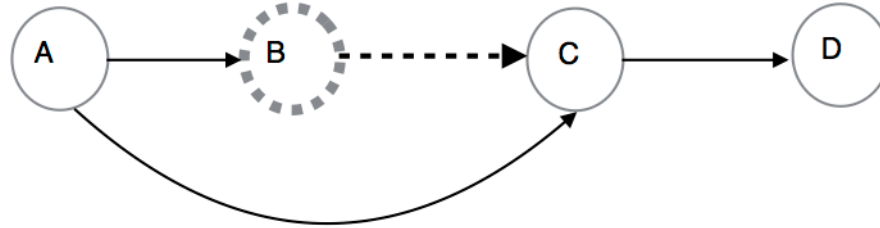
Este escenario de fallo corresponde al fallo de un nodo intermedio en una cadena en cascada. Para lograr la recuperación de este escenario, se puede seguir el procedimiento de redireccionamiento. Como se muestra en la siguiente figura, se produce un fallo en el nodo intermedio B de la cadena en cascada.



Como se muestra en la siguiente figura, después de que se aplica el procedimiento de redireccionamiento/omisión, el origen A omite el nodo con el fallo B y continúa enviando las actualizaciones al nodo C, el cual, a su vez, envía una actualización al nodo D.



Como se muestra en la siguiente figura, cuando B se recupera, se restaura la acción entre A y B mientras la acción entre B y C permanece omitida.



Omisión de un nodo con fallos mediante la CLI:

1. Seleccione la acción para el nodo con fallos en el origen.
2. Introduzca `retarget`.
3. Defina la propiedad `retarget_mode` en `bypass`.
4. Defina que el destino sea el destino de omisión, como se muestra en la siguiente figura.

```

badenov:> shares replication actions
badenov:shares replication actions> select action-005
badenov:shares replication action-005> retarget
badenov:shares replication action-005 retarget> show
Properties:
    retarget_mode =
    target =
    bypass_targets = 0

badenov:shares replication action-005 retarget> set retarget_mode=bypass
    retarget_mode = bypass (uncommitted)
badenov:shares replication action-005 retarget> set target=system
system-B system-C system-D
badenov:shares replication action-005 retarget> set target=system-C
    target = system-C (uncommitted)
badenov:shares replication action-005 retarget> commit
badenov:shares replication action-005> show
Properties:
    id = 17dc3fdf-0a69-411d-84eb-b6ae3f0baca0
    target_pkgid = 17dc3fdf-0a69-411d-84eb-b6ae3f0baca0
  
```

5. La propiedad `bypassed_id` que se muestra en la acción de omisión se puede utilizar para seleccionar la acción original destinada a ejecutar una restauración de redireccionamiento luego de la recuperación del nodo con fallos. Es posible ver el valor de `bypassed_id` generado, como se muestra en la siguiente figura.

```

badenov:shares replication actions> select action-006
badenov:shares replication action-006> list
NAME                FREQUENCY          DAY                HH:MM
schedule-000        10min              -                  -:00
badenov:shares replication action-006> show
Properties:
      id = 478f7f11-8e6b-4b4b-9372-ad7949e11fc4
    target_pkgid = c6cc1699-12f9-476b-8e75-a15a29de98bd
      target_id = 6f73a106-cb58-471e-bb0c-fbbdbf42ee7c
        target = system-C
      target_pool = p
      source_pool = ba
    replication_of = fy18
      bypassed_id = 17dc3fdf-0a69-411d-84eb-b6ae3f0baca0

```

6. En una etapa posterior, cuando B se haya recuperado, utilice el procedimiento de redireccionamiento/restauración para regresar a la topología en cascada original, como se muestra en la siguiente figura.

```

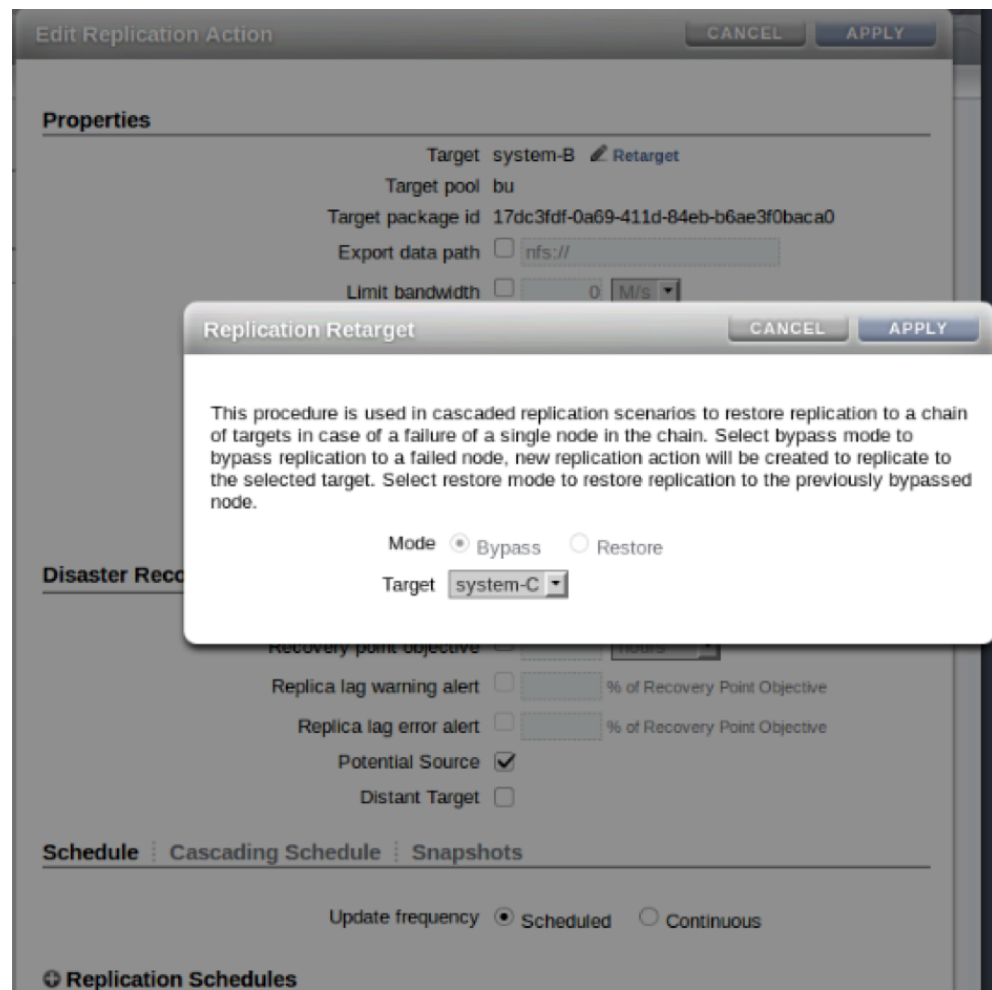
badenov:shares replication action-005> retarget
badenov:shares replication action-005 retarget> show
Properties:
      retarget_mode =
        target =
      bypass_targets = 1

badenov:shares replication action-005 retarget> set retarget_mode=restore
      retarget_mode = restore (uncommitted)
badenov:shares replication action-005 retarget> set target=system-C
        target = system-C (uncommitted)
badenov:shares replication action-005 retarget> commit
badenov:shares replication action-005> 

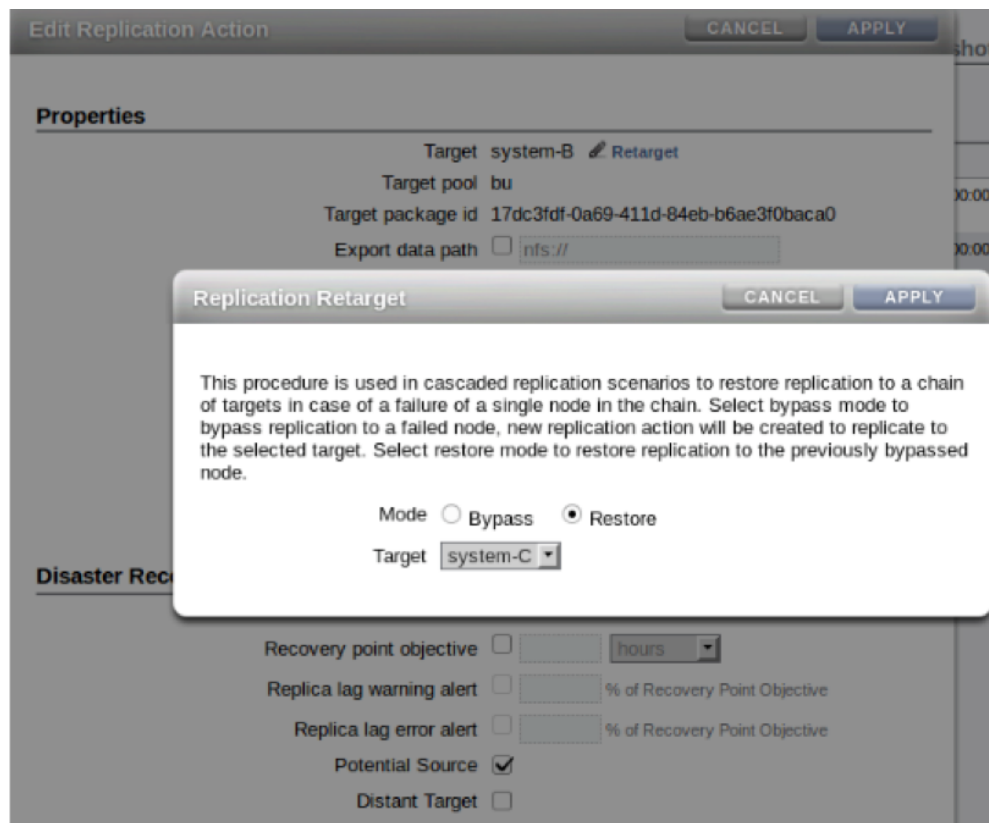
```

Omisión de un nodo con fallos mediante la BUI:

1. En el nodo de origen, seleccione la acción para el nodo con fallos.
2. En el cuadro de diálogo Editar acción de replicación, haga clic en Redireccionar.
3. En el cuadro de diálogo Redireccionamiento de replicación, establezca el modo en Omitir.
4. En la lista desplegable, seleccione el destino que debe ser el destino de omisión, como se muestra en la siguiente figura.



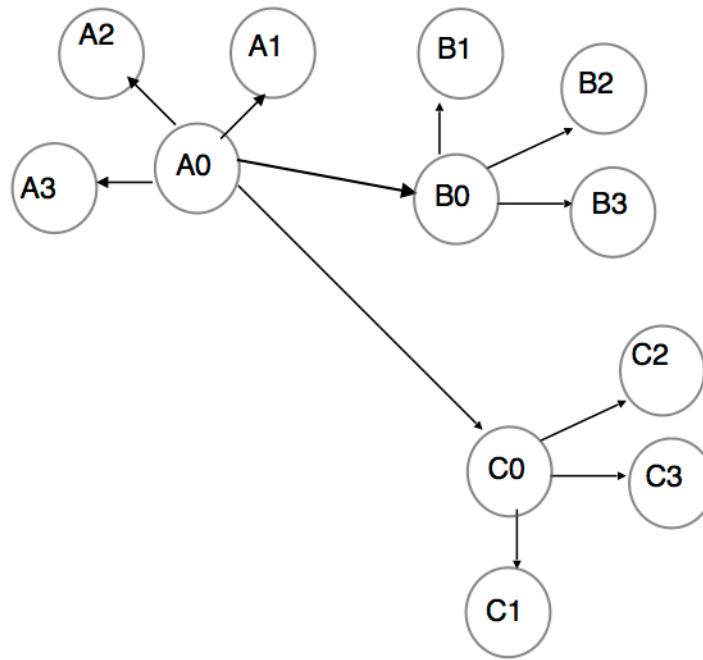
5. Haga clic en APLICAR.
6. En una etapa posterior, cuando se haya recuperado, utilice el procedimiento de restauración para regresar a la topología en cascada original, como se muestra en la siguiente figura.



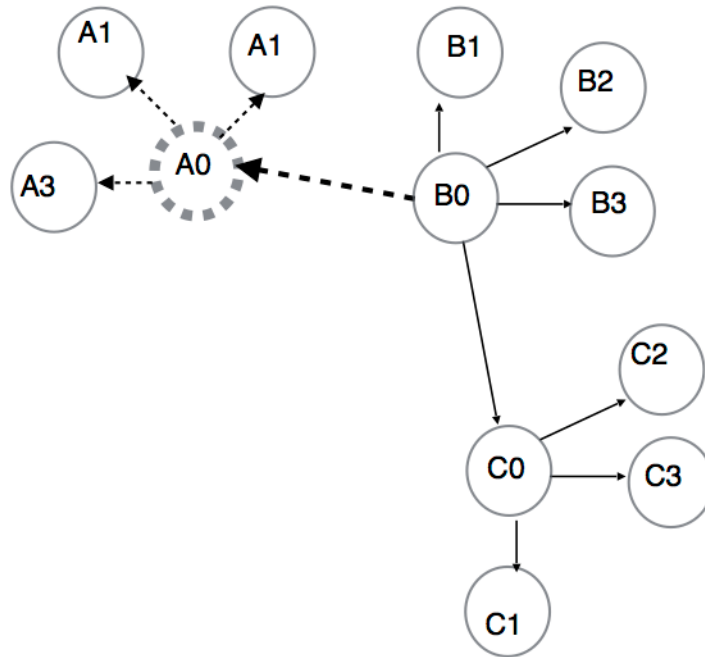
Fallo en el sitio de origen

En este escenario, el origen y todos sus destinos locales directos no se encuentran disponibles y se reemplazan por un nuevo origen en uno de los destinos distantes. La recuperación de este escenario requiere una configuración de reversión de varios destinos en el origen. Para obtener más detalles, consulte [“Reversión a varios destinos” \[750\]](#). También requiere que se configuren algunos destinos como destinos distantes. Para obtener detalles, consulte "Uso de la propiedad distant_target para gestionar reversiones".

Como se muestra en la siguiente imagen, A_0 , B_0 y C_0 forman un grupo de reversiones de varios destinos, donde B_0 y C_0 son orígenes potenciales y destinos distantes. A_0 , B_0 y A_0 , C_0 forman una relación de destino distante (A_0B_0 y A_0C_0 deben configurarse como origen potencial y destino distante), mientras que A_1 , A_2 , A_3 forman una relación local con A_0 , y B_1 , B_2 , B_3 forman una relación local con B_0 .



Cuando se ejecuta una reversión en B0, como se muestra en la siguiente figura, A1, A2, A3 son tratados como destinos locales de A0; por lo tanto, no se vuelven a crear acciones en A1, A2, A3. Debido a las propiedades de la reversión de varios destinos, B0 envía las actualizaciones a C0.



Consideraciones de compatibilidad

Al configurar una replicación en cascada, siga estas reglas de compatibilidad:

- Los nodos con un firmware anterior a OS8.7.0 no se pueden configurar como parte de una replicación en cascada.
- Los nodos con un firmware posterior a OS8.7.0 pueden configurarse como nodos finales.
- Los nodos finales con un firmware que no admite la replicación en cascada pueden llevar a cabo una reversión de replicación. No obstante, estos no podrán ejecutar una actualización de replicación en su origen. No se pueden recuperar relaciones de replicación en ese escenario.
- No se puede ejecutar un redireccionamiento en los nodos finales con un firmware que no admite la replicación en cascada.
- Las reglas de compatibilidad de replicación de los destinos con un firmware diferente en cadenas en cascada son iguales para todos los orígenes y destinos. Por ejemplo, cuando un destino no admite una función que utiliza el origen, se puede producir un fallo en la actualización de replicación desde el origen correspondiente.

- El rollback del sistema a una versión de firmware que no admite la replicación en cascada producirá la destrucción de todas las acciones de replicación en cascada.

Temas relacionados

- [“Propiedades de las acciones de replicación” \[716\]](#)
- [“Reversión a varios destinos” \[750\]](#)

Exportación de sistemas de archivos replicados

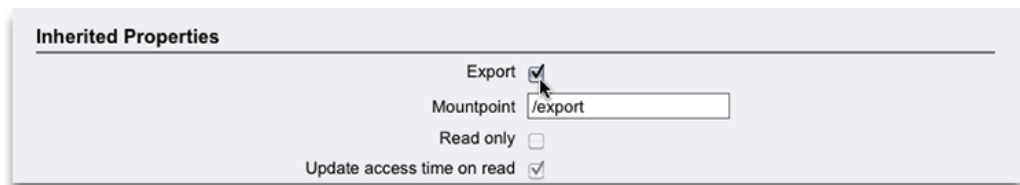
Los sistemas de archivos replicados se pueden exportar en formato de solo lectura a los clientes NAS. Se puede utilizar para verificar los datos replicados o para llevar a cabo copias de seguridad u otras operaciones intensivas sobre los datos replicados (mediante la descarga de dicho trabajo del dispositivo de origen).

El contenido del sistema de archivos siempre coincide con la instantánea de replicación recibida más recientemente para ese sistema de archivos. Es posible que sea más nueva que la instantánea recibida más recientemente para todo el paquete, y que no coincida con la instantánea más reciente para otros recursos compartidos del mismo paquete. Para obtener información detallada, consulte [“Instantáneas de replicación y coherencia de datos” \[737\]](#).

Las actualizaciones de replicación se aplican automáticamente en el nivel del sistema de archivos. Los clientes que miren los archivos replicados verán las actualizaciones de replicación como un cambio instantáneo en el sistema de archivos subyacente. Los clientes que trabajen con los archivos suprimidos en la actualización más reciente verán errores. Los clientes que trabajen con archivos cambiados en la actualización más reciente verán de inmediato el contenido actualizado.

Los sistemas de archivos replicados no se exportan de forma predeterminada. Para exportarlos, se debe modificar la propiedad "exportado" del proyecto o recurso compartido mediante la BUI o la CLI:

FIGURA 30 Propiedades heredadas



Esta propiedad es heredada como otras propiedades de recursos compartidos. Esta propiedad no se muestra para recursos compartidos y proyectos locales porque estos siempre se exportan. Además, el corte de la replicación (que convierte el paquete en un proyecto local) genera la exportación de los recursos compartidos del paquete.

En la actualidad, los LUN replicados no se pueden exportar. Primero, se deben clonar o el paquete de replicación se debe cortar para exportar el contenido.

Temas relacionados

- [Flujo de trabajo de replicación remota \[623\]](#)
- [“Propiedades heredadas” \[503\]](#)

Corte de replicación

Un paquete de replicación se puede convertir en un proyecto modificable local, que se comporta como otros proyectos locales (es decir, sin restricciones de gestión aplicadas a los paquetes de replicación) mediante el corte de la conexión de la replicación. El corte de un paquete de replicación se puede usar para migrar datos entre dispositivos o en otras situaciones que no incluyen la replicación de los datos recibidos nuevamente en el dispositivo de origen.

Si se realiza una actualización de replicación durante una operación del servidor o después de ella, la actualización fallará y mostrará la alerta correspondiente. La acción de replicación se desactiva, lo que hace que no haya más actualizaciones desde esta acción para el destino de replicación.

Se requiere una nueva acción de replicación y una actualización completa del mismo proyecto para enviar actualizaciones de replicación a un nuevo paquete de replicación.

Para evitar conflictos de punto de montaje o nombre de SMB, resuelva los conflictos antes de cortar el paquete de replicación mediante la reconfiguración del proyecto, los puntos de montaje de los recursos compartidos o los nombres de los recursos de SMB. Como siempre se exportan todos los recursos compartidos locales, y tal vez se los esté compartiendo por medio de SMB, la operación de corte genera un error si hay algún conflicto de nombres de recursos de SMB o puntos de montaje entre los sistemas de archivos replicados y otros sistemas de archivos del sistema.

Temas relacionados

- Corte de paquetes de replicación: [BUI](#), [CLI](#)
- [Recuperación ante desastres con replicación remota](#)
- [Gestión de instantáneas generadas por el usuario](#)

Reversión de la dirección de replicación

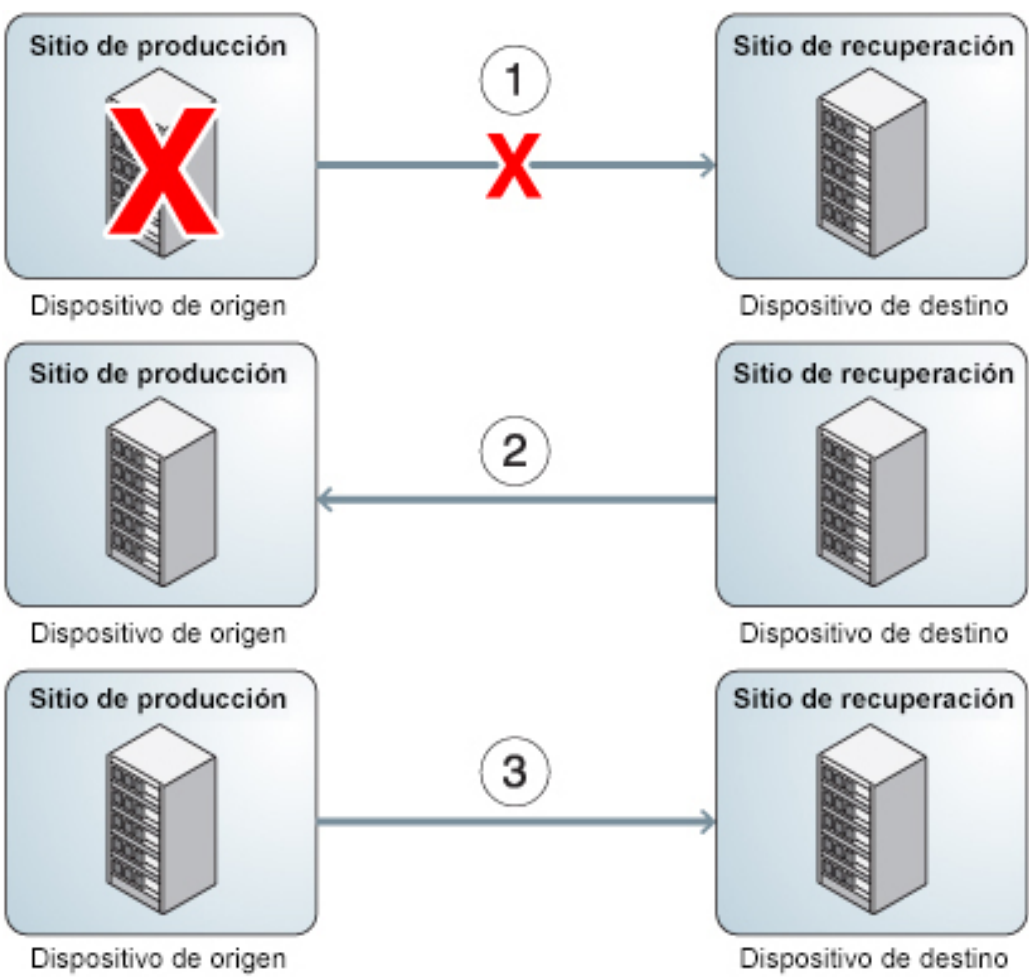
Se puede revertir la dirección de la replicación para admitir planes de recuperación ante desastres de dos sistemas y copias de seguridad de disco a disco.

Reversión de la replicación para la recuperación ante desastres

La operación de replicación inversa convierte el paquete de replicación en un proyecto local. Esta operación también configura una acción de replicación en el proyecto local nuevo mediante la cual se realizará una replicación incremental en el dispositivo de origen. El primer intento de actualización convierte el proyecto original del sistema de origen en un paquete de replicación y revierte los cambios realizados desde la última actualización de replicación finalizada correctamente desde ese sistema.

En la figura siguiente, se describe la secuencia de eventos típica de una replicación inversa.

FIGURA 31 Uso de la replicación remota para la recuperación ante desastres



Leyenda	Descripción
1	El sistema de producción es el dispositivo de origen que proporciona al cliente la carga de trabajo y se replica en el destino de replicación que está en un sitio de recuperación. En el sitio de producción se genera un fallo total del dispositivo de origen.

Leyenda	Descripción
	En el sitio de recuperación, el administrador invierte la dirección de replicación. Esta operación convierte el paquete de replicación en un proyecto local en el que se puede escribir. El administrador redirecciona las cargas de trabajo del cliente y ejecuta una operación de failover de las direcciones IP hacia el sitio de recuperación.
2	Cuando el sitio de producción se restaura y vuelve a funcionar normalmente, el administrador inicia una actualización de replicación desde el sitio de recuperación hacia el sitio de producción. Esta operación convierte la copia de producción en un paquete de replicación y deshace los cambios escritos en el sitio de recuperación mientras el sitio de producción estaba inactivo.
3	Después de actualizar el sitio de producción, el administrador invierte nuevamente la dirección de replicación, lo que hace que se pueda escribir en la copia del sitio de producción. El administrador, luego, redirecciona las cargas de trabajo del cliente y ejecuta una operación de failover de las direcciones IP hacia el sitio de producción. Se restaura la relación original entre el dispositivo de origen del sitio de producción y el destino de replicación del sitio de recuperación.

Reversión en el nivel del recurso compartido y el nivel del proyecto

Cuando el proyecto de origen original se convierte en un paquete de replicación en el dispositivo de origen original (que ahora funciona como destino), los recursos compartidos que se replicaron como parte de la acción o el paquete que actualmente se está invirtiendo se trasladan a un nuevo paquete de replicación y no se exportan. El proyecto original permanece en la recopilación local, pero podría terminar vacío si la acción o el paquete incluyeran todos los recursos compartidos. Cuando se revierte la replicación de nivel de recurso compartido, todos los demás recursos compartidos del proyecto original no se modifican.

Antes de revertir la dirección de replicación de un paquete, detenga las actualizaciones de replicación de ese proyecto desde el dispositivo de origen. Si hay una actualización de replicación en curso cuando el administrador revierte la dirección de la replicación de un proyecto, los administradores no podrán saber qué instantánea de replicación coherente se utilizó para crear el proyecto resultante en el destino de replicación anterior (que ahora es el dispositivo de origen).

Si se realiza una actualización de replicación durante una operación de reversión o después de ella, la actualización falla y se muestra la alerta correspondiente. La acción de replicación se desactiva, lo que hace que no haya más actualizaciones desde esta acción para el destino de replicación. Se requiere una acción de replicación nueva y una actualización completa para enviar actualizaciones desde el proyecto original a un paquete de replicación nuevo.

Dado que se exportan todos los recursos compartidos locales, todos los recursos compartidos del paquete se exportan cuando se invierte el paquete, independientemente de que se hayan exportado previamente. Si existen conflictos de punto de montaje entre los sistemas de archivos replicados y otros sistemas de archivos del sistema, se producirá un error en la operación de reversión. Estos conflictos se deben resolver antes de realizar el corte mediante la reconfiguración de los puntos de montaje de los recursos compartidos correspondientes. Dado que esta operación, generalmente, forma parte de la ruta crítica de restauración del servicio de producción, se recomienda resolver estos conflictos de punto de montaje cuando los sistemas se configuran por primera vez, en lugar de hacerlo en el momento en que se produce el failover de la recuperación ante desastres.

Temas relacionados

- [Recuperación ante desastres con replicación remota](#)
- [Managing Replication Packages](#)
- [“Reversión a varios destinos” \[750\]](#)

Destrucción de un paquete de replicación

El proyecto y los recursos compartidos incluidos en un paquete no se pueden destruir sin destruir el paquete completo. Este paquete completo se puede destruir desde la BUI, mediante la destrucción del proyecto correspondiente. El paquete se puede destruir desde la CLI usando el comando `destroy` en el nodo `shares replication packages`.

Cuando se destruye un paquete, se producirán errores en las actualizaciones de replicación posteriores de la acción correspondiente. Para reanudar la replicación, será necesario recrear la acción en el origen para crear un nuevo paquete en el destino, en el cual se recibirá una nueva copia de los datos.

Copias de seguridad de réplicas de destino

Puede usar el tipo de copia de seguridad NDMP zfs para hacer copias de seguridad de los juegos de datos de réplica de destino (proyectos o recursos compartidos). Para activar la copia de seguridad de las réplicas en el dispositivo, se debe aplicar la actualización diferida de compatibilidad para la copia de seguridad NDMP-zfs de réplicas. La función de copia de seguridad de réplicas elige la instantánea más reciente generada por el sistema para hacer la copia de seguridad, a menos que se especifique una instantánea generada por el usuario (o sea, cuya la extensión no sea `.rr`). Para obtener más información, consulte [“Copias de seguridad de réplicas” \[419\]](#).

Algunas instantáneas de replicación más antiguas, las que originalmente se conservaron para futuras copias de seguridad incrementales, pueden no ser necesarias y se las puede suprimir. Si

NDMP retiene la instantánea, aparece una advertencia de confirmación del efecto potencial para las copias de seguridad en curso y futuras de NDMP.

La siguiente secuencia de eventos ocasiona un error en la replicación y genera una alerta. Para obtener información sobre cómo recuperarse de este error, consulte, "Colisión de nombres" en ["Fallos de replicación" \[744\]](#).

1. NDMP retiene una instantánea de réplica en el destino de replicación (para una copia de seguridad en curso o una copia de seguridad incremental futura).
2. La instantánea correspondiente en el dispositivo de origen se suprime o se le cambia el nombre.
3. Se crea una nueva instantánea en el dispositivo de origen con el mismo nombre que la instantánea de réplica que se mantuvo en el destino de replicación.
4. Se intenta realizar una actualización de la replicación.

Cifrado de datos

Nota - El cifrado es una característica que se ofrece con licencia para ciertos modelos. Para obtener información detallada, consulte "Acuerdo de licencia de software (SLA) de Oracle y derecho de sistemas de hardware con opciones de software integrado" y el Manual de usuario de información sobre licencias para la versión de software.

Oracle ZFS Storage Appliance ofrece cifrado transparente de los datos para agrupaciones y recursos compartidos individuales (sistemas de archivos y LUN) y recursos compartidos creados dentro de proyectos.

Para configurar y gestionar el cifrado, realice las siguientes tareas:

- [Flujo de trabajo de cifrado de datos \[796\]](#)
- Configuración de cifrado de almacén de claves LOCAL: [BUI](#), [CLI](#)
- Configuración de cifrado de almacén de claves de OKM: [BUI](#), [CLI](#)
- Configuración de cifrado de almacén de claves de KMIP: [BUI](#), [CLI](#)
- Creación de una agrupación cifrada: [BUI](#), [CLI](#)
- Cambio de una clave de cifrado de agrupación: [BUI](#), [CLI](#)
- Creación de un proyecto cifrado: [BUI](#), [CLI](#)
- Cambio de una clave de cifrado de proyecto: [BUI](#), [CLI](#)
- Creación de sistemas de archivos o LUN cifrados: [BUI](#), [CLI](#)
- Cambio de clave de cifrado de recurso compartido: [BUI](#), [CLI](#)
- Copia de seguridad de una clave LOCAL: [BUI](#), [CLI](#)
- Supresión de una clave de cifrado: [BUI](#), [CLI](#)
- Restauración de una clave LOCAL: [BUI](#), [CLI](#)
- Clonación de una instantánea: [BUI](#), [CLI](#)

Para comprender el cifrado de datos, consulte los siguientes temas:

- [“Propiedades de cifrado” \[832\]](#)
- [“Gestión de claves de cifrado” \[833\]](#)
- [“Impacto del cifrado en el rendimiento” \[837\]](#)

- [“Ciclo de vida de clave de cifrado” \[838\]](#)
- [“Copia de seguridad, replicación y restauración de proyectos y recursos compartidos cifrados” \[838\]](#)

▼ Flujo de trabajo de cifrado de datos

En los siguientes pasos, se muestra el procedimiento general para configurar y usar el cifrado de datos. Para obtener información acerca de las propiedades de cifrado, consulte [“Propiedades de cifrado” \[832\]](#).

1. **Configure el cifrado del almacén de claves LOCAL, almacén de claves de Oracle Key Manager (OKM) o almacén de claves del protocolo de interoperabilidad de gestión de claves (KMIP).**

- Configuración de cifrado de almacén de claves LOCAL: [BUI](#), [CLI](#)
- Configuración de cifrado de almacén de claves de OKM: [BUI](#), [CLI](#)
- Configuración de cifrado de almacén de claves de KMIP: [BUI](#), [CLI](#)

2. **Cree claves de cifrado y certificados.**

Siga los mismos procedimientos del paso anterior.

3. **(Opcional) Cree una agrupación utilizando una clave de cifrado.**

Para obtener información, consulte Creación de una agrupación cifrada: [BUI](#), [CLI](#).

4. **(Opcional) Cree un proyecto utilizando una clave de cifrado.**

Para obtener información, consulte Creación de un proyecto cifrado: [BUI](#), [CLI](#).

5. **Cree un recurso compartido en un proyecto que utilice una clave de cifrado o cree un recurso compartido utilizando una clave de cifrado.**

Para obtener información acerca de la creación de un recurso compartido, consulte [Recursos compartidos y proyectos \[483\]](#) o Creating an Encrypted Project - [BUI](#), [CLI](#).

Temas relacionados

- [“Gestión de claves de cifrado” \[833\]](#)
- [“Impacto del cifrado en el rendimiento” \[837\]](#)
- [“Ciclo de vida de clave de cifrado” \[838\]](#)
- [“Copia de seguridad, replicación y restauración de proyectos y recursos compartidos cifrados” \[838\]](#)

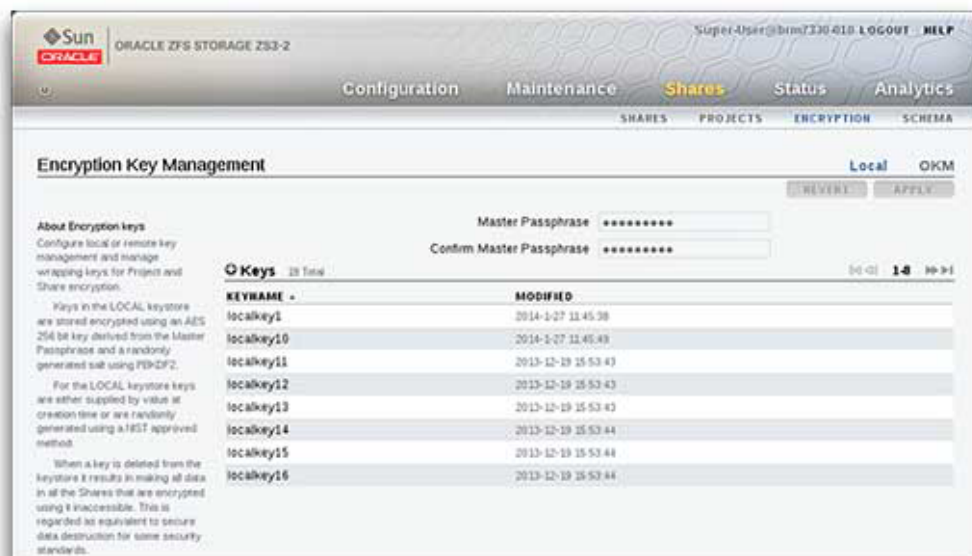
▼ Configuración de cifrado de almacén de claves LOCAL (BUI)

Para configurar el cifrado utilizando el almacén de claves LOCAL, primero defina la frase de contraseña maestra y luego cree las claves. Para obtener información acerca de las propiedades de cifrado, consulte [“Propiedades de cifrado” \[832\]](#).

1. **Vaya a Recursos compartidos > Cifrado.**

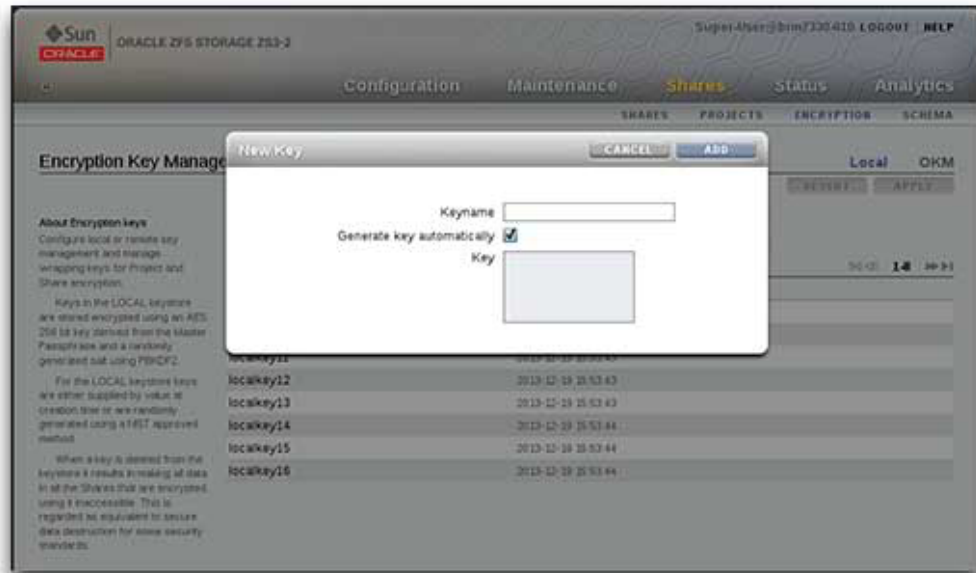
2. **Haga clic en Local.**

Se muestra la información del almacén de claves de LOCAL.



3. **Para configurar la frase de contraseña maestra, escriba la frase de contraseña proporcionada por su administrador y vuelva a escribirla en la siguiente casilla.**
4. **Para guardar la frase de contraseña maestra, haga clic en Aplicar.**
5. **Para crear una clave, haga clic en ícono de agregar .**

Se muestra el cuadro de diálogo Nueva clave.



6. Introduzca el nombre de la clave.

7. (Opcional) Introduzca una clave.

Si deja la casilla de verificación "Generar clave automáticamente" activada, se genera una clave de forma automática.

Para proporcionar su propia clave, haga lo siguiente:

- a. Desactive la casilla de verificación "Generar clave automáticamente".
- b. Introduzca la clave raw de 256 bits hexadecimal en la casilla de verificación Clave.

8. Para guardar la clave, haga clic en AGREGAR.

Cuando hace clic en AGREGAR, la nueva clave aparece en la lista de claves con la fecha de creación.

Temas relacionados

- [Configuración de cifrado de almacén de claves de OKM \(BUI\) \[800\]](#)
- [Configuración de cifrado de almacén de claves de KMIP \(BUI\) \[803\]](#)
- [Configuración de cifrado de almacén de claves LOCAL \(CLI\) \[799\]](#)
- [Creación de una agrupación cifrada \(BUI\) \[810\]](#)
- [Creación de un proyecto cifrado \(BUI\) \[816\]](#)

▼ Configuración de cifrado de almacén de claves LOCAL (CLI)

Para configurar el cifrado utilizando el almacén de claves LOCAL, primero defina la frase de contraseña maestra y luego cree las claves. Para obtener información acerca de las propiedades de cifrado, consulte [“Propiedades de cifrado” \[832\]](#).

1. Configure el cifrado del almacén de claves LOCAL.

Para configurar el cifrado del almacén de claves LOCAL, defina la frase de contraseña maestra.

```
hostname:> shares encryption
hostname:shares encryption> show
Children:
    local => Manage LOCAL keystore
    okm => Register keys with Oracle Key Manager

hostname:shares encryption> local
hostname:shares encryption local> show
Properties:
    master_passphrase =

Children:
    keys => Manage this Keystore's Keys

hostname:shares encryption local> set master_passphrase
Enter new master_passphrase:
Re-enter new master_passphrase:
    master_passphrase = (set) (uncommitted)
b7420-16m:shares encryption local> commit
b7420-16m:shares encryption local> show
Properties:
    master_passphrase = (set)

Children:
    keys => Manage this Keystore's Keys
```

2. Cree una clave LOCAL.

Para crear una clave, introduzca un nombre de clave. El valor de la propiedad `keyname` es el nombre que se utiliza en la CLI y la BUI cuando se asigna una clave a una agrupación, un proyecto o un recurso compartido.

Puede dejar la propiedad `key` en blanco para que el sistema genere un valor de clave aleatorio o puede proporcionar un valor de clave raw de 256 bits hexadecimal. En el siguiente ejemplo, el sistema genera el valor `key`.

La clave se almacena de forma cifrada utilizando la frase de contraseña maestra del paso 1.

```
hostname:shares encryption local> keys
hostname:shares encryption local keys> show
Keys:

NAME      CREATED          CIPHER KEYNAME
Properties:
          cipher = AES
          key =
          keyname = (unset)
hostname:shares encryption local> create
hostname:shares encryption local key-000 (uncommitted)> set keyname=Key-0
          keyname = Key-0 (uncommitted)
hostname:shares encryption local key-000 (uncommitted)> commit
hostname:shares encryption local keys> show
Keys:

NAME      CREATED          CIPHER KEYNAME
key-000   2019-7-1 18:43:33  AES    Key-0
hostname:shares encryption local keys> select key-000
hostname:shares encryption local key-000> show
Properties:
          cipher = AES
          key =
          ce968122d0bba26c3d66b6985ee358d18a786607f80eb4ebd834e4404fe8aa84
          keyname = Key-0
```

Temas relacionados

- [Configuración de cifrado de almacén de claves de OKM \(CLI\) \[802\]](#)
- [Configuración de cifrado de almacén de claves de KMIP \(CLI\) \[806\]](#)
- [Configuración de cifrado de almacén de claves LOCAL \(BUI\) \[797\]](#)
- [Creación de una agrupación cifrada \(CLI\) \[812\]](#)
- [Creación de un proyecto cifrado \(CLI\) \[817\]](#)

▼ Configuración de cifrado de almacén de claves de OKM (BUI)

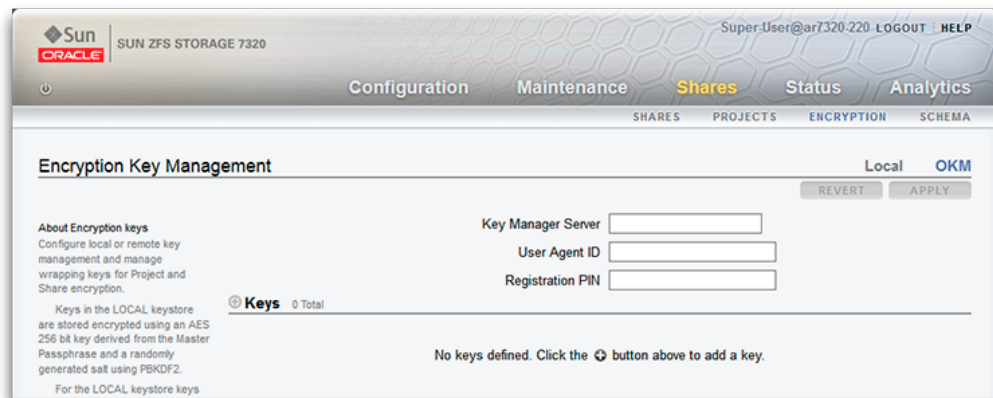
Para configurar el cifrado utilizando OKM, primero defina la información del Servidor de gestión de claves y luego cree las claves. Para obtener información acerca de las propiedades de cifrado, consulte [“Propiedades de cifrado” \[832\]](#).

Nota - Si el dispositivo está en un cluster, no debe usar la configuración "frase de contraseña de un solo uso" para la creación del agente de servidor de OKM. Si en esta situación utiliza la configuración "frase de contraseña de un solo uso", el registro en el otro nodo de cluster fallará, y las claves no estarán disponibles en el failover.

1. **Vaya a Recursos compartidos > Cifrado.**

2. **Haga clic en OKM.**

Se muestra la información del almacén de claves de OKM.



3. **Para configurar la información del servidor, introduzca la siguiente información:**

- Servidor de gestión de claves
- ID de agente de usuario
- PIN de registro

4. **Para guardar la información del servidor, haga clic en Aplicar.**

5. **Para crear una clave, haga clic en ícono de agregar +.**

Se muestra el cuadro de diálogo Nueva clave.

6. **Introduzca un nombre para la clave.**

7. **Para guardar la clave, haga clic en AGREGAR.**

Cuando hace clic en AGREGAR, la nueva clave aparece en la lista de claves con la fecha de creación.

Temas relacionados

- [“Almacén de claves de Oracle Key Manager \(OKM\)” \[834\]](#)
- [Configuración de cifrado de almacén de claves LOCAL \(BUI\) \[797\]](#)
- [Configuración de cifrado de almacén de claves de KMIP \(BUI\) \[803\]](#)
- [Configuración de cifrado de almacén de claves de OKM \(CLI\) \[802\]](#)
- [Creación de una agrupación cifrada \(BUI\) \[810\]](#)
- [Creación de un proyecto cifrado \(BUI\) \[816\]](#)

▼ Configuración de cifrado de almacén de claves de OKM (CLI)

Para configurar el cifrado utilizando OKM, primero defina la información del Servidor de gestión de claves y luego cree las claves. Para obtener información acerca de las propiedades de cifrado, consulte [“Propiedades de cifrado” \[832\]](#).

Nota - Si el dispositivo está en un cluster, no debe usar la configuración "frase de contraseña de un solo uso" para la creación del agente de servidor de OKM. Si en esta situación utiliza la configuración "frase de contraseña de un solo uso", el registro en el otro nodo de cluster fallará, y las claves no estarán disponibles en el failover.

1. Configure el cifrado del almacén de claves de OKM.

Para configurar el cifrado del almacén de claves de OKM, defina el ID de agente, el PIN de registro (proporcionado por su responsable de seguridad de OKM) y la dirección IP del servidor.

```
hostname:> shares encryption
hostname:shares encryption> show
Children:
    local => Manage LOCAL keystore
    okm => Register keys with Oracle Key Manager

hostname:shares encryption> okm
hostname:shares encryption okm> show
Properties:
    agent_id = ExternalClient041
    registration_pin = (set)
    server_addr = 10.80.180.109

Children:
    keys => Manage this Keystore's Keys
```

2. Crear una clave de OKM.

Para crear una clave, introduzca un nombre de clave.

```
hostname:shares encryption okm keys> create
hostname:shares encryption okm key-372 (uncommitted)> ls
Properties:
    cipher = AES
    keyname = (unset)
hostname:shares encryption okm key-372 (uncommitted)> set keyname=anykey
    keyname = anykey (uncommitted)
hostname:shares encryption okm key-372 (uncommitted)> commit
```

Temas relacionados

- [“Almacén de claves de Oracle Key Manager \(OKM\)” \[834\]](#)
- [Configuración de cifrado de almacén de claves LOCAL \(CLI\) \[799\]](#)
- [Configuración de cifrado de almacén de claves de KMIP \(CLI\) \[806\]](#)
- [Configuración de cifrado de almacén de claves de OKM \(BUI\) \[800\]](#)
- [Creación de una agrupación cifrada \(CLI\) \[812\]](#)
- [Creación de un proyecto cifrado \(CLI\) \[817\]](#)

▼ Configuración de cifrado de almacén de claves de KMIP (BUI)

Para configurar el cifrado mediante KMIP, cargue la clave y los certificados, y especifique el servidor de KMIP.

Antes de empezar Antes de configurar el almacén de claves de KMIP en controladores agrupados, realice los siguientes procedimientos:

- Para cada nodo de cluster, configure un recurso de red privada que pueda llegar hasta los servidores de KMIP. Esta interfaz de red privada garantiza que cada nodo de cluster se pueda comunicar con el servidor de KMIP en caso de se produzca un failover de las interfaces de red de servicio de datos. Para obtener más información sobre recursos privados, consulte [“Gestión de recursos de clusters” \[78\]](#).
- Configure, de manera adecuada, una ruta para cada servidor de KMIP para el enlace de red privada. Para obtener información sobre la configuración de rutas, consulte [“Configuración de enrutamiento de red” \[121\]](#).



Atención - En caso de que estos requisitos previos no se cumplan, se producirá una interrupción del servicio durante las operaciones de toma de control y failback.

1. Vaya a Configuración > Valores de configuración > Certificados.

2. Cargue la clave privada.

- a. **Haga clic en icono de carga**  **ubicado a la izquierda de Sistema.**
- b. **Haga clic en Browse (Examinar).**

Navegue hasta la ubicación en la que están almacenados sus certificados y su clave.

Para Oracle Key Vault, la clave y los certificados están en un archivo jar que debe haber recibido del administrador de Oracle Key Vault.
- c. **Seleccione el archivo de formato PEM que contiene la clave privada.**

Para Oracle Key Vault, el archivo es `key.pem`.
- d. **Haga clic en el botón CARGAR.**

En la tabla Sistema aparecerá una nueva fila con el valor de Tipo `key`.

3. Cargue el certificado del sistema.

Seleccione el archivo de formato PEM que contiene el certificado de cliente para este sistema. Para Oracle Key Vault, el archivo es `cert.pem`.

Siga los mismos pasos que usó para cargar la clave privada.

La fila que tenía un valor de Tipo `key` cambia de modo que ahora tiene un valor de Tipo `cert`. Se confronta el certificado con la clave existente y se lo combina en un solo objeto en el dispositivo. Se completan los campos Asunto, Emitido por (CN) y Caduca. Haga clic en el ícono de información  en la fila para ver los valores completos de estos campos y obtener más información.

4. Cargue el certificado de anclaje de confianza.

- La autoridad de certificación es el emisor del certificado de cliente.
- Seleccione el archivo de formato PEM que contiene el certificado de la autoridad de certificación que emitió el certificado de cliente. Para Oracle Key Vault, el archivo es `ca.pem`.
- a. **Haga clic en el separador De confianza.**
 - b. **Haga clic en el icono de carga**  **ubicado a la izquierda de De confianza.**
 - c. **Haga clic en Browse (Examinar).**

- d. **Seleccione el archivo `CA.pem`.**
- e. **Haga clic en el botón CARGAR.**
En la tabla De confianza aparece una nueva fila.
- f. **Haga clic en el ícono de edición  en la fila nueva.**
- g. **En la parte inferior del cuadro de diálogo Detalles de certificado, verifique el cuadro `kmip` y haga clic en Aceptar.**
En la fila de la tabla, ahora, aparece `kmip` en la columna Servicio.
5. **Vaya a Recursos compartidos > Cifrado> KMIP.**
6. **En el menú desplegable Certificado, seleccione el certificado que acaba de cargar.**
7. **Introduzca el nombre de host o la dirección IP del servidor de KMIP.**
El valor recomendado que se debe usar es el nombre de host del servidor de KMIP. Consulte la discusión sobre la validación de nombre de host en [“Almacén de claves del protocolo de interoperabilidad de gestión de claves \(KMIP\)” \[835\]](#).
Si especifica una dirección IP, consulte con su administrador del servidor de KMIP acerca de si debe incluir el número de puerto.
8. **Verifique las opciones de confrontación de nombre de host y eliminación de una clave.**
Por defecto, estas opciones están activadas (marcadas). Consulte [“Almacén de claves del protocolo de interoperabilidad de gestión de claves \(KMIP\)” \[835\]](#) para obtener información sobre lo que hacen estas opciones.
9. **Haga clic en Aplicar.**
Si recibe una advertencia que indica que el servidor no pudo validar en el certificado, haga clic en Cancelar en el cuadro de diálogo de la advertencia y verifique si especificó el nombre de host de servidor correcto en el campo KMIP Server (Servidor de KMIP). Si especifica una dirección IP para el servidor de KMIP y el nombre común de asunto del certificado firmado por la autoridad de certificación solo tiene un nombre de dominio, se produce un error en la validación de host del certificado.
Si anula la selección de la opción de confrontación de nombre de host, no se realizará la validación de host y la seguridad se debilitará.
10. **Asigne un nombre a la clave.**

- a. Haga clic en el ícono de adición  ubicado a la izquierda de Claves.
 - b. Introduzca un nombre de clave y haga clic en AGREGAR.
11. **(Opcional) Identifique las agrupaciones, los proyectos y los recursos compartidos que están cifrados con esta clave.**

Para identificar qué agrupaciones, proyectos y recursos compartidos están cifrados con esta clave, inicie el proceso de supresión de la clave, pero cancele la operación de supresión de clave después de ver la lista de datos que se verán afectados. Al iniciar el proceso de supresión de clave, aparece una advertencia que indica que no se podrá acceder a ninguno de los datos cifrados con esta clave. En la advertencia se muestra una lista de agrupaciones, proyectos y recursos compartidos cifrados con esta clave. Para cancelar la supresión de la clave, haga clic en el botón Cancelar, no en el botón Aceptar. Para obtener más detalles, consulte [Supresión de una clave de cifrado \(BUI\) \[827\]](#).

Temas relacionados

- [“Almacén de claves del protocolo de interoperabilidad de gestión de claves \(KMIP\)” \[835\]](#)
- [Configuración de cifrado de almacén de claves LOCAL \(BUI\) \[797\]](#)
- [Configuración de cifrado de almacén de claves de OKM \(BUI\) \[800\]](#)
- [Configuración de cifrado de almacén de claves de KMIP \(CLI\) \[806\]](#)
- [Creación de una agrupación cifrada \(BUI\) \[810\]](#)
- [Creación de un proyecto cifrado \(BUI\) \[816\]](#)

▼ Configuración de cifrado de almacén de claves de KMIP (CLI)

Para configurar el cifrado mediante KMIP, cargue la clave y los certificados, y especifique el servidor de KMIP.

Antes de empezar Antes de configurar el almacén de claves de KMIP en controladores agrupados, realice los siguientes procedimientos:

- Para cada nodo de cluster, configure un recurso de red privada que pueda llegar hasta los servidores de KMIP. Esta interfaz de red privada garantiza que cada nodo de cluster se pueda comunicar con el servidor de KMIP en caso de se produzca un failover de las interfaces de red de servicio de datos. Para obtener más información sobre recursos privados, consulte [“Gestión de recursos de clusters” \[78\]](#).

- Configure, de manera adecuada, una ruta para cada servidor de KMIP para el enlace de red privada. Para obtener información sobre la configuración de rutas, consulte [“Configuración de enrutamiento de red” \[121\]](#).



Atención - En caso de que estos requisitos previos no se cumplan, se producirá una interrupción del servicio durante las operaciones de toma de control y failback.

1. Vaya a configuration settings certificates system.

2. Cargue la clave privada.

a. Copie el contenido del archivo de formato PEM que contiene la clave privada.

Para Oracle Key Vault, la clave y los certificados están en un archivo jar que debe haber recibido del administrador de Oracle Key Vault. El archivo de la clave privada es el archivo `key.pem`.

b. Introduzca el comando `import`. Pegue la clave cuando se le solicite.

```
hostname:configuration settings certificates system> import
("." to end)> -----BEGIN RSA PRIVATE KEY-----
...
("." to end)> -----END RSA PRIVATE KEY-----
("." to end)> .
```

c. Introduzca el comando `list`.

La tabla de certificados del sistema tiene una nueva fila con un valor de Tipo `key`.

```
hostname:configuration settings certificates system> list
CERT      TYPE SUBJECT COMMON NAME      ISSUER COMMON NAME      NOT AFTER
cert-001 key  RSA-2048
```

3. Cargue el certificado del sistema.

El certificado del sistema es el archivo en formato PEM que contiene el certificado del cliente para este sistema. Para Oracle Key Vault, el archivo es `cert.pem`.

Copie el contenido del archivo del certificado, introduzca el comando `import` y pegue el certificado.

```
hostname:configuration settings certificates system> import
("." to end)> -----BEGIN CERTIFICATE-----
...
("." to end)> -----END CERTIFICATE-----
("." to end)> .
```

4. Cargue el certificado de anclaje de confianza.

La autoridad de certificación es el emisor del certificado de cliente. Para Oracle Key Vault, el archivo es `CA.pem`.

a. **Introduzca el comando `up trusted`.**

b. **Copie el contenido del archivo de la autoridad de certificación, introduzca el comando `import` y pegue el certificado de la autoridad de certificación.**

La tabla de certificados de confianza tiene una fila nueva.

```
hostname:configuration settings certificates trusted> list
CERT      TYPE SUBJECT COMMON NAME      ISSUER COMMON NAME      NOT AFTER
cert-001 cert CA                      CA                      2022-8-11
```

c. **Defina la propiedad `services` del certificado en `kmip`.**

```
hostname:configuration settings certificates trusted> select cert-001
hostname:configuration settings certificates cert-001> get services
services =
hostname:configuration settings certificates cert-001> set services=kmip
services = kmip (uncommitted)
hostname:configuration settings certificates cert-001> commit
hostname:configuration settings certificates cert-001> done
```

5. **Vaya a `shares encryption kmip`.**

```
hostname:shares encryption kmip> get
server_list =
client_cert =
host_match = true
destroy_key_on_remove = true
```

6. **Defina `client_cert` en el certificado que acaba de cargar.**

Por defecto, el comando `list` muestra los servidores de KMIP. Use el comando `list certs` para obtener una lista de certificados disponibles.

```
hostname:shares encryption kmip> list certs
CERT      TYPE SUBJECT COMMON NAME      ISSUER COMMON NAME      NOT AFTER
cert-001 cert iogo7PmhIY          CA                      2023-1-25
```

Defina el valor de `client_cert` mediante el comando `set` o el comando `client_cert`.

```
hostname:shares encryption kmip> set client_cert=cert-001
hostname:shares encryption kmip> client_cert cert-001
```

Para la secuencia de comandos, necesita un identificador persistente para el certificado. Use el comando `client_cert` con finalización con tabulación para mostrar las propiedades de los certificados.

```
hostname:shares encryption kmip> client_cert tab
cert-001      notafter
cert-002      notbefore
comment      sha1fingerprint
dns          sha256fingerprint
```

ip	subject_commonname
issuer_commonname	subject_countryname
issuer_countryname	subject_localityname
issuer_localityname	subject_organizationalunitname
issuer_organizationalunitname	subject_organizationname
issuer_organizationname	subject_stateorprovincename
issuer_stateorprovincename	type
key_bits	uri
key_type	uuid

Cada certificado tiene un `subject_commonname` único, de modo que puede usar el valor de esa propiedad para definir la propiedad `client_cert`.

```
hostname:shares encryption kmip> client_cert subject_commonname=tab
ip-addr iogo7PmhIY
hostname:shares encryption kmip> client_cert subject_commonname=iogo7PmhIY
hostname:shares encryption kmip> get client_cert
client_cert = cert-001 (uncommitted)
```

7. Defina `server_list` en el nombre de host o la dirección IP del servidor de KMIP.

El valor recomendado para esta propiedad es el nombre de host del servidor de KMIP. Consulte la discusión sobre la validación de nombre de host en [“Almacén de claves del protocolo de interoperabilidad de gestión de claves \(KMIP\)” \[835\]](#).

Si especifica una dirección IP, consulte con su administrador del servidor de KMIP acerca de si debe incluir el número de puerto.

```
hostname:shares encryption kmip> set server_list=knip-server-hostname-or-IP-address
server_list = knip-server-hostname-or-IP-address (uncommitted)
hostname:shares encryption kmip> commit
```

Si recibe una advertencia que indica que el servidor no pudo validar el certificado, verifique si especificó el nombre de host de servidor correcto en `server_list`. Si especifica una dirección IP para `server_list` y el nombre común de asunto del certificado firmado por la autoridad de certificación solo tiene un nombre de dominio, se produce un error en la validación de host del certificado.

Si define el valor de `host_match` en `false`, no se realizará la validación de host y la seguridad se debilitará.

8. Verifique las opciones `host_match` y `destroy_key_on_remove`.

Por defecto, ambas opciones están definidas en `true`. Consulte [“Almacén de claves del protocolo de interoperabilidad de gestión de claves \(KMIP\)” \[835\]](#) para obtener información sobre lo que hacen estas opciones.

9. Asigne un nombre a la clave.

Cree una clave y defina la propiedad `keyname`.

```
hostname:shares encryption kmip> keys
hostname:shares encryption keys> list
NAME      CREATED      CIPHER KEYNAME
hostname:shares encryption keys> create
```

```
hostname:shares encryption kmip key-000 (uncommitted)> set keyname=atz-1-27-2021
keyname = atz-1-27-2021 (uncommitted)
hostname:shares encryption kmip key-000 (uncommitted)> commit
hostname:shares encryption keys> list
NAME      CREATED      CIPHER KEYNAME
key-000   2021-1-27 07:14:31  AES     atz-1-27-2021
```

10. (Opcional) Identifique las agrupaciones, los proyectos y los recursos compartidos que están cifrados con esta clave.

Para identificar qué agrupaciones, proyectos y recursos compartidos están cifrados con esta clave, inicie el proceso de supresión de la clave, pero cancele la operación de supresión de clave después de ver la lista de datos que se verán afectados. Al iniciar el proceso de supresión de clave, aparece una advertencia que indica que no se podrá acceder a ninguno de los datos cifrados con esta clave. En la advertencia se muestra una lista de agrupaciones, proyectos y recursos compartidos cifrados con esta clave. Introduzca `n` para cancelar la supresión de la clave.

```
hostname:shares encryption keys> destroy key-000
This key has the following dependents:
  pool-0/local/default/fs-enc
Destroying this key will render the data inaccessible. Are you sure? (Y/N) n
```

Temas relacionados

- [“Almacén de claves del protocolo de interoperabilidad de gestión de claves \(KMIP\)” \[835\]](#)
- [Configuración de cifrado de almacén de claves LOCAL \(CLI\) \[799\]](#)
- [Configuración de cifrado de almacén de claves de OKM \(CLI\) \[802\]](#)
- [Configuración de cifrado de almacén de claves de KMIP \(BUI\) \[803\]](#)
- [Creación de una agrupación cifrada \(CLI\) \[812\]](#)
- [Creación de un proyecto cifrado \(CLI\) \[817\]](#)

▼ Creación de una agrupación cifrada (BUI)

Para obtener información más detallada sobre cómo crear una agrupación, consulte [Creación de una agrupación de almacenamiento \(BUI\)](#).

Los valores del almacén de claves y el nombre de la clave de la agrupación se pueden modificar en cualquier momento una vez que se ha creado la agrupación. Sin embargo, no puede agregar información de cifrado a una agrupación que ya se creó sin cifrar.

Los juegos de datos que se creen en una agrupación cifrada también estarán cifrados. No puede crear proyectos ni recursos compartidos sin cifrar en una agrupación cifrada.

Antes de empezar Para crear una agrupación de almacenamiento cifrada, actualice el software a la versión OS8. 8.0 o posterior, y acepte todas las actualizaciones diferidas, incluida la Activación de cifrado de agrupación. Consulte [“Activación de actualización diferida de cifrado de agrupación” en el Manual de servicio del cliente de Oracle ZFS Storage Appliance](#).

Para poder crear una agrupación de clave de cifrado, debe crear una clave de cifrado. Consulte [Cifrado de datos \[795\]](#).

- Dado que el almacén de claves se debe configurar antes de crear la agrupación, no puede crear una agrupación cifrada durante la configuración inicial del sistema ni después del restablecimiento de fábrica.
- Antes de configurar la replicación para un proyecto o recurso compartido en una agrupación cifrada, asegúrese de que la clave de cifrado utilizada en el origen también se encuentre disponible en el destino.

1. **Vaya a Configuración > Almacenamiento.**
2. **Haga clic en el ícono de agregación , junto a Agrupaciones disponibles.**
3. **Escriba un nombre para la agrupación de almacenamiento y haga clic en Aplicar.**
4. **Seleccione el número de unidades de datos para la agrupación de almacenamiento para cada estante de discos deseado. También puede seleccionar dispositivos de caché, log y metadispositivos disponibles.**
Para obtener más información sobre cómo seleccionar unidades de datos y metadispositivos, consulte [Creación de una agrupación de almacenamiento \(BUI\)](#).
5. **Haga clic en Confirmar.**
Las unidades se asignan a la agrupación de almacenamiento y se las verifica para determinar que estén presentes y ofrezcan un mínimo de funcionalidad. Si la verificación falla, haga clic en Abortar, corrija el problema y vuelva a iniciar este procedimiento. Si asigna una agrupación con dispositivos defectuosos o faltantes, no podrá agregar los dispositivos defectuosos o faltantes más adelante.
6. **En la pantalla Seleccionar perfil de almacenamiento, seleccione el perfil de datos que cumpla con los objetivos de confiabilidad, disponibilidad, facilidad de mantenimiento y rendimiento.**
Para obtener una descripción de cada perfil, haga clic en el nombre del perfil de datos o consulte [“Perfiles de datos para agrupaciones de almacenamiento” \[167\]](#).
7. **Si asignó dispositivos de log, caché o metadispositivos, seleccione los perfiles apropiados.**
Para obtener más información, consulte [Creación de una agrupación de almacenamiento \(BUI\)](#).

8. Configure el tipo de cifrado, el almacén de claves y el nombre de la clave.

Utilice los campos Cifrado y Clave de la sección Configuración opcional que se encuentra en la parte inferior de la pantalla Seleccionar perfil de almacenamiento.

El campo Cifrado se encuentra desactivado si no se configura ningún almacén de claves: para poder crear la agrupación, debe crear una clave de cifrado. Consulte [Cifrado de datos \[795\]](#).

Por defecto, los valores Cifrado y Clave están desactivados. Cuando selecciona un tipo en el campo Cifrado (consulte [“Descripción de los valores de claves de cifrado” \[836\]](#)), debe seleccionar un almacén de claves y un nombre de clave en el campo Clave.

9. Haga clic en Confirmar.

Una vez que lo selecciona, el valor Cifrado es inmutable. Sin embargo, los valores de Clave se pueden modificar en cualquier momento. Consulte [Cambio de clave de cifrado de agrupación \(BUI\) \[814\]](#).

Todos los proyectos creados en esta agrupación se cifran automáticamente con estos valores de cifrado, aunque los valores de Clave se pueden modificar. Consulte [Creación de un proyecto cifrado \(BUI\) \[816\]](#).

Temas relacionados

- [“Propiedades de cifrado” \[832\]](#)
- [“Gestión de claves de cifrado” \[833\]](#)

▼ Creación de una agrupación cifrada (CLI)

Para obtener información más detallada sobre cómo crear una agrupación, consulte [Creación de una agrupación de almacenamiento \(CLI\)](#).

Los valores del almacén de claves y el nombre de la clave de la agrupación se pueden modificar en cualquier momento una vez que se ha creado la agrupación. Sin embargo, no puede agregar información de cifrado a una agrupación que ya se creó sin cifrar.

Los juegos de datos que se creen en una agrupación cifrada también estarán cifrados. No puede crear proyectos ni recursos compartidos sin cifrar en una agrupación cifrada.

Antes de empezar

Para crear una agrupación de almacenamiento cifrada, actualice el software a la versión OS8.8.0 o posterior, y acepte todas las actualizaciones diferidas, incluida la Activación de cifrado de agrupación. Consulte [“Activación de actualización diferida de cifrado de agrupación” en el Manual de servicio del cliente de Oracle ZFS Storage Appliance](#).

Para poder crear una agrupación de clave de cifrado, debe crear una clave de cifrado. Consulte [Cifrado de datos \[795\]](#).

- Dado que el almacén de claves se debe configurar antes de crear la agrupación, no puede crear una agrupación cifrada durante la configuración inicial del sistema ni después del restablecimiento de fábrica.
- Antes de configurar la replicación para un proyecto o recurso compartido en una agrupación cifrada, asegúrese de que la clave de cifrado utilizada en el origen también se encuentre disponible en el destino.

1. **Vaya a configuration storage.**
2. **Introduzca `config` y un nombre para la agrupación de almacenamiento nueva.**
3. **Introduzca `show` para ver la información de dispositivo de la agrupación.**
4. **Introduzca `set` y el ID de controlador o de estante de discos, además del número de unidades de datos que desea usar. También puede seleccionar dispositivos de caché, log y metadispositivos disponibles.**
Para obtener más información sobre cómo seleccionar unidades de datos y metadispositivos, consulte [Creación de una agrupación de almacenamiento \(CLI\)](#).
5. **Escriba `done`.**
6. **Escriba `show` para visualizar el perfil.**
7. **Si asignó dispositivos de log a la agrupación, introduzca `set log_profile=` y configure el perfil de log como `log_mirror` o `log_stripe`. Use `log_mirror` si la agrupación incluye un número par de dispositivos de log.**
8. **Si asignó metadispositivos a la agrupación, introduzca `set meta_profile=` y configure el metaperfil como `meta_mirror` o `meta_stripe`.**
9. **Configure el tipo de cifrado, el almacén de claves y el nombre de la clave.**

Utilice las propiedades `encryption`, `keystore` y `keyname`.

Las propiedades `encryption`, `keystore` y `keyname` están ocultas y son inmutables si no se configura ningún almacén de claves. Para poder crear la agrupación, debe crear una clave de cifrado.

Consulte [Cifrado de datos \[795\]](#).

Por defecto, la propiedad `encryption` debe estar establecida en `off`.

```
hostname:configuration storage (pool1) config> ls
      PROFILE      CAPCTY NSPF DESCRIPTION
profile = mirror    4.92G  no   Mirrored
mirror3             4.92G  no   Triple mirrored
stripe              14.8G  no   Striped

encryption = off
```

```
keyname =  
keystore =
```

Configure un tipo de cifrado (consulte [“Descripción de los valores de claves de cifrado” \[836\]](#)), un almacén de claves y un nombre de clave. Si el valor de la propiedad encryption no es off, se deben configurar las propiedades keystore y keyname.

```
hostname:configuration storage (pool1) config> set encryption=aes-128-ccm  
encryption = aes-128-ccm  
hostname:configuration storage (pool1) config> set keystore=LOCAL  
keystore = LOCAL  
hostname:configuration storage (pool1) config> set keyname=MyKey  
keyname = MyKey
```

10. Escriba `done` para completar la tarea.

```
hostname:configuration storage config (pool1)> done
```

Verifique los valores.

```
hostname:configuration storage (pool1)> get encryption keystore keyname keystorestatus  
encryption = aes-128-ccm  
keystore = LOCAL  
keyname = MyKey  
keystorestatus = available
```

Una vez que lo selecciona, el valor encryption es inmutable. Sin embargo, los valores keystore y keyname se pueden modificar en cualquier momento. Consulte [Cambio de clave de cifrado de agrupación \(CLI\) \[815\]](#).

Todos los proyectos creados con esta agrupación se cifran automáticamente con estos valores de cifrado, aunque los valores keystore y keyname se pueden modificar. Consulte [Creación de un proyecto cifrado \(CLI\) \[817\]](#).

Temas relacionados

- [“Propiedades de cifrado” \[832\]](#)
- [“Gestión de claves de cifrado” \[833\]](#)

▼ Cambio de clave de cifrado de agrupación (BUI)

Puede cambiar la clave de cifrado para una agrupación en cualquier momento, incluso cuando la están usando sistemas cliente.

Cuando se modifica una clave de cifrado de una agrupación, cambia la clave de los proyectos y los recursos compartidos que heredan la clave de la agrupación.

- 1. Vaya a Configuración > Almacenamiento.**
- 2. Seleccione la agrupación para la que desea cambiar la clave de cifrado.**

3. Cambie la clave de cifrado de la agrupación.

Haga clic en el nombre o en el ícono de edición  que se encuentra a la derecha del campo Clave para mostrar el cuadro de diálogo y editar el almacén de claves y el nombre de la clave utilizados para cifrar la agrupación seleccionada.

4. Haga clic en Aplicar.

Todos los proyectos que ya estén heredando la configuración de cifrado de esta agrupación también heredarán la nueva configuración de cifrado. Consulte [Creación de un proyecto cifrado \(BUI\) \[816\]](#).

Temas relacionados

- [Supresión de una clave de cifrado \(BUI\) \[827\]](#)
- [“Propiedades de cifrado” \[832\]](#)

▼ Cambio de clave de cifrado de agrupación (CLI)

Puede cambiar la clave de cifrado para una agrupación en cualquier momento, incluso cuando la están usando sistemas cliente.

Cuando se modifica una clave de cifrado de una agrupación, cambia la clave de los proyectos y los recursos compartidos que heredan la clave de la agrupación.

1. Vaya a `configuration storage`.**2. Seleccione la agrupación para la que desea cambiar la clave de cifrado.**

Si la agrupación que está seleccionada no es la que desea, use el comando `set pool` para seleccionar otra agrupación.

3. Cambie la clave de cifrado de la agrupación.

Configure los valores de las propiedades `keystore` y `keyname`.

4. Introduzca el comando `commit`.

Todos los proyectos que ya estén heredando la configuración de cifrado de esta agrupación también heredarán la nueva configuración de cifrado. Consulte [Creación de un proyecto cifrado \(CLI\) \[817\]](#).

Temas relacionados

- [Supresión de una clave de cifrado \(BUI\) \[827\]](#)

- [“Propiedades de cifrado” \[832\]](#)

▼ Creación de un proyecto cifrado (BUI)

Los proyectos heredan las propiedades de la agrupación principal. Los proyectos heredan las propiedades del proyecto principal. Para ver una lista de las propiedades que se pueden heredar, consulte [“Propiedades heredadas” \[503\]](#).

Los proyectos que se crean en una agrupación cifrada se cifran automáticamente y heredan la configuración de cifrado de la agrupación. Puede modificar la configuración de la clave de cifrado, pero no puede descifrar el proyecto ni crear un proyecto descifrado en una agrupación cifrada.

Este procedimiento describe cómo crear un proyecto cifrado en una agrupación cifrada o descifrada.

Antes de empezar Para usar el cifrado, primero debe configurarlo. Consulte [Cifrado de datos \[795\]](#).

1. **Vaya a Recursos compartidos > Proyectos.**
2. **Haga clic en el ícono de agregación  que se encuentra junto a Proyectos o en el panel Proyectos expandido. Para expandir el panel Proyectos, haga clic en el ícono de la flecha.**
3. **En el cuadro de diálogo Crear proyecto, introduzca un nombre para el proyecto nuevo.**

El nombre debe tener entre 1 y 64 caracteres de longitud. El nombre no puede comenzar con un punto (.) ni puede incluir espacios. Los caracteres permitidos son los alfanuméricos y los siguientes caracteres especiales:

_ - . :
4. **Si la agrupación principal de este proyecto no está cifrada, configure un tipo de cifrado.**

Si la agrupación principal de este proyecto no está cifrada, el valor por defecto del campo Cifrado será Desactivado. Para crear un proyecto cifrado, configure un valor nuevo en el campo Cifrado. Consulte [“Descripción de los valores de claves de cifrado” \[836\]](#) para ver descripciones de los valores del campo Cifrado.

Si la agrupación principal de este proyecto está cifrada, el valor de Cifrado se hereda y no se puede modificar.
5. **Seleccione un almacén de claves y un nombre de clave.**

Si la agrupación principal del proyecto no está cifrada, seleccione un almacén de claves y un nombre de clave.

Si la agrupación principal del proyecto está cifrada, decida si desea que herede la configuración de cifrado de la agrupación. Los proyectos o juegos de datos que se crean en una agrupación cifrada, incluido el proyecto por defecto, se pueden configurar de manera tal que hereden el almacén de claves y el nombre de clave de la agrupación, o que especifiquen su propio almacén de claves y nombre de clave. En ese caso, no se usarán los valores de clave heredados.

- **Para heredar el almacén de claves y el nombre de clave de la agrupación, en el cuadro de diálogo, marque la casilla de control Heredar clave.**

Si un proyecto hereda la configuración cifrada de la agrupación, todos sus juegos de datos heredan la configuración cifrada de la agrupación.

Cuando marca la casilla de control Heredar clave, las dos selecciones de Clave (almacén de claves y nombre de clave) aparecen atenuadas y no se pueden seleccionar. La clave solo se puede modificar desde la agrupación principal.

- **Para configurar un almacén de claves y un nombre de clave distintos, desmarque la casilla de control Heredar clave.**

Seleccione un almacén de claves y un nombre de clave.

6. Configure las demás propiedades de este proyecto según corresponda.

Las propiedades de los proyectos se describen en [“Propiedades de proyecto” \[517\]](#).

7. Haga clic en Aplicar.

El proyecto nuevo se agrega a la lista Proyectos.

Todos los recursos compartidos creados en este proyecto se cifran automáticamente con estos valores de cifrado, aunque los valores de Clave se pueden modificar. Consulte [Creación de sistemas de archivos o LUN cifrados \(BUI\) \[821\]](#).

Temas relacionados

- [“Propiedades de cifrado” \[832\]](#)
- [“Gestión de claves de cifrado” \[833\]](#)
- [Cambio de clave de cifrado de un proyecto \(BUI\) \[819\]](#)

▼ Creación de un proyecto cifrado (CLI)

Para obtener información más detallada sobre cómo crear un proyecto, consulte [Creación de un proyecto \(CLI\)](#).

Los proyectos heredan las propiedades de la agrupación principal. Los proyectos heredan las propiedades del proyecto principal. Para ver una lista de las propiedades que se pueden heredar, consulte [“Propiedades heredadas” \[503\]](#).

Los proyectos que se crean en una agrupación cifrada se cifran automáticamente y heredan la configuración de cifrado de la agrupación. Puede modificar la configuración de la clave de cifrado, pero no puede descifrar el proyecto ni crear un proyecto descifrado en una agrupación cifrada.

Este procedimiento describe cómo crear un proyecto cifrado en una agrupación cifrada o descifrada.

Antes de empezar Para usar el cifrado, primero debe configurarlo. Consulte [Cifrado de datos \[795\]](#).

1. **Vaya a `shares`.**
2. **Introduzca el comando `project` y un nombre para el proyecto.**
3. **Si la agrupación principal de este proyecto no está cifrada, configure un tipo de cifrado.**

Si la agrupación principal de este proyecto no está cifrada, el valor por defecto de la propiedad `encryption` es `off`. Para crear un proyecto cifrado, configure un valor nuevo en la propiedad `encryption`. Consulte [“Descripción de los valores de claves de cifrado” \[836\]](#) para ver descripciones de los valores de la propiedad `encryption`.

Si la agrupación principal de este proyecto está cifrada, el valor de la propiedad `encryption` se hereda y no se puede modificar.

4. **Configure un almacén de claves y un nombre de clave.**

Si la agrupación principal de este proyecto no está cifrada, configure las propiedades `keystore` y `keyname`.

Si la agrupación principal de este proyecto está cifrada, los valores de las propiedades `keystore` y `keyname` se heredan de la agrupación por defecto. Puede usar los valores heredados o modificarlos.

```
hostname:shares myproject (uncommitted)> get encryption keyname keystore
encryption = aes-128-ccm
keystore = LOCAL
keyname = MyKey
```

Use el comando `set` a fin de configurar valores nuevos para `keystore` y `keyname` como se muestra en el siguiente ejemplo:

```
hostname:shares myproject (uncommitted)> set keyname=NewKey
keyname = NewKey (uncommitted)
```

5. **Use los comandos `get` y `set` para configurar las demás propiedades de este proyecto según corresponda.**

Las propiedades de los proyectos se describen en [“Propiedades de proyecto” \[517\]](#).

6. **Introduzca el comando `commit`.**

Todos los recursos compartidos creados en este proyecto se cifran automáticamente con estos valores de cifrado, aunque los valores `keystore` y `keyname` se pueden modificar. Consulte [Creación de sistemas de archivos o LUN cifrados \(CLI\) \[823\]](#).

Temas relacionados

- [“Propiedades de cifrado” \[832\]](#)
- [“Gestión de claves de cifrado” \[833\]](#)
- [Cambio de clave de cifrado de proyecto \(CLI\) \[820\]](#)

▼ Cambio de clave de cifrado de un proyecto (BUI)

Puede cambiar la clave de cifrado para un proyecto en cualquier momento, incluso cuando la están usando sistemas cliente.

Cambiar una clave de cifrado de un proyecto, cambia la clave de los recursos compartidos que heredan la clave del proyecto.

Si la agrupación principal del proyecto está cifrada, el proyecto hereda las claves de cifrado de la agrupación principal por defecto. Puede modificar la clave de un proyecto sin cambiar la clave de la agrupación principal.

1. **Vaya a Recursos compartidos > Proyectos.**
2. **Para encontrar el proyecto que desea modificar, haga clic en Mostrar todo, Local o Réplica.**
3. **Mueva el cursor sobre el proyecto que desea modificar y haga clic en el ícono de edición .**
4. **Haga clic en General.**
Se muestran los parámetros del proyecto.
5. **Si es necesario, desmarque Heredar de la agrupación.**
Si la opción Heredar de la agrupación está marcada, la clave solo se puede modificar desde la agrupación principal.

6. **Para cambiar la clave de cifrado del proyecto, seleccione el almacén de claves y el nombre de la clave que desee usar.**

7. **Haga clic en Aplicar.**

Cuando hace clic en Aplicar, se graban los cambios y aparece la nueva clave en el área de clave de cifrado. Todos los recursos compartidos de este proyecto heredan la nueva configuración de cifrado.

Todos los recursos compartidos que ya estén heredando la configuración de cifrado de este proyecto también heredarán la nueva configuración de cifrado. Consulte [Creación de sistemas de archivos o LUN cifrados \(BUI\) \[821\]](#).

Temas relacionados

- [Cambio de clave de cifrado de proyecto \(CLI\) \[820\]](#)
- [Supresión de una clave de cifrado \(BUI\) \[827\]](#)
- [“Propiedades de cifrado” \[832\]](#)

▼ Cambio de clave de cifrado de proyecto (CLI)

Puede cambiar la clave de cifrado para un proyecto en cualquier momento, incluso cuando la están usando sistemas cliente.

Cambiar una clave de cifrado de un proyecto, cambia la clave de los recursos compartidos que heredan la clave del proyecto.

Si la agrupación principal del proyecto está cifrada, el proyecto hereda las claves de cifrado de la agrupación principal por defecto. Puede modificar la clave de un proyecto sin cambiar la clave de la agrupación principal.

1. **Vaya a `shares`.**
2. **Seleccione el proyecto para el que desea cambiar la clave de cifrado.**
Si el proyecto que está seleccionado no es el que desea, use el comando `select project-name` para seleccionar uno distinto.
3. **Cambie la clave de cifrado del proyecto.**
Configure los valores de las propiedades `keystore` y `keyname`.
4. **Introduzca el comando `commit`.**

Todos los recursos compartidos que ya estén heredando la configuración de cifrado de este proyecto también heredarán la nueva configuración de cifrado. Consulte [Creación de sistemas de archivos o LUN cifrados \(CLI\)](#) [823].

Temas relacionados

- [Cambio de clave de cifrado de un proyecto \(BUI\)](#) [819]
- [Cambio de clave de cifrado de recurso compartido \(CLI\)](#) [825]
- [Supresión de una clave de cifrado \(CLI\)](#) [828]
- [“Propiedades de cifrado”](#) [832]

▼ Creación de sistemas de archivos o LUN cifrados (BUI)

Los sistemas de archivos y los LUN que se crean dentro de un proyecto heredan las propiedades del proyecto principal. Para ver una lista de las propiedades que se pueden heredar, consulte [“Propiedades heredadas”](#) [503].

Los sistemas de archivos y los LUN que se crean en un proyecto cifrado se cifran automáticamente y heredan la configuración de cifrado del proyecto. Puede cambiar la configuración de la clave de cifrado sin importar si el recurso compartido se crea en un proyecto cifrado o descifrado.

Una manera sencilla de crear un conjunto de recursos compartidos cifrado es crearlos en un proyecto cifrado.

Antes de empezar Para usar el cifrado, primero debe configurar un almacén de claves y las claves. Consulte [Cifrado de datos](#) [795].

1. **Vaya a Recursos compartidos > Recursos compartidos.**
2. **Seleccione Sistemas de archivos o LUN.**
3. **Haga clic en el ícono de agregación .**
4. **Complete los campos del cuadro de diálogo Crear sistema de archivos o Crear LUN.**
 - En el caso de los sistemas de archivos, seleccione un proyecto e introduzca un nombre.
 - En el caso de los LUN, seleccione un proyecto, introduzca un nombre y especifique el tamaño del volumen.

El nombre debe tener entre 1 y 64 caracteres de longitud. El nombre no puede comenzar con un punto (.) ni puede incluir espacios. Los caracteres permitidos son los alfanuméricos y los siguientes caracteres especiales:

_ - . :

5. Si el proyecto principal de este sistema de archivos o LUN no está cifrado, configure un tipo de cifrado.

Si el proyecto principal de este recurso compartido no está cifrado, el valor por defecto del campo Cifrado será Desactivado. Para crear un recurso compartido cifrado, configure un valor nuevo en el campo Cifrado. Consulte [“Descripción de los valores de claves de cifrado” \[836\]](#) para ver descripciones de los valores del campo Cifrado.

Si el proyecto principal de este recurso compartido está cifrado, el valor de Cifrado se hereda y no se puede modificar.

6. Seleccione un almacén de claves y un nombre de clave.

Si el proyecto principal del recurso compartido no está cifrado, seleccione un almacén de claves y un nombre de clave.

Si el proyecto principal del recurso compartido está cifrado, decida si desea que herede la configuración de cifrado del proyecto. Los recursos compartidos que se crean en un proyecto cifrado se pueden configurar de manera tal que hereden el almacén de claves y el nombre de clave del proyecto, o que especifiquen su propio almacén de claves y nombre de clave. En ese caso, no se usarán los valores de clave heredados.

■ **Para heredar el almacén de claves y el nombre de clave del proyecto, en el cuadro de diálogo, marque la casilla de control Heredar clave.**

Las dos selecciones de Clave (almacén de claves y nombre de clave) aparecen atenuadas y no se pueden seleccionar. La clave solo se puede modificar desde el proyecto principal.

■ **Para configurar un almacén de claves y un nombre de clave distintos, desmarque la casilla de control Heredar clave.**

Seleccione un almacén de claves y un nombre de clave.

7. Haga clic en Aplicar.

Temas relacionados

- [“Propiedades de cifrado” \[832\]](#)
- [“Gestión de claves de cifrado” \[833\]](#)
- [Cambio de clave de cifrado de recurso compartido \(BUI\) \[824\]](#)

▼ Creación de sistemas de archivos o LUN cifrados (CLI)

Los sistemas de archivos y los LUN que se crean dentro de un proyecto heredan las propiedades del proyecto principal. Para ver una lista de las propiedades que se pueden heredar, consulte [“Propiedades heredadas” \[503\]](#).

Los sistemas de archivos y los LUN que se crean en un proyecto cifrado se cifran automáticamente y heredan la configuración de cifrado del proyecto. Puede cambiar la configuración de la clave de cifrado sin importar si el recurso compartido se crea en un proyecto cifrado o descifrado.

Una manera sencilla de crear un conjunto de recursos compartidos cifrado es crearlos en un proyecto cifrado.

Antes de empezar Para usar el cifrado, primero debe configurarlo. Consulte [Cifrado de datos \[795\]](#).

1. Vaya a shares.

2. Seleccione el proyecto.

Si el proyecto que está seleccionado no es el que desea, use el comando `select project-name` para seleccionar uno distinto.

3. Cree el sistema de archivos o LUN.

Introduzca `filesystem filesystem-name` o `lun lun-name`.

El nombre debe tener entre 1 y 64 caracteres de longitud. El nombre no puede comenzar con un punto (.) ni puede incluir espacios. Los caracteres permitidos son los alfanuméricos y los siguientes caracteres especiales:

`_ - . :`

En el ejemplo siguiente, se crea un sistema de archivos llamado `fs-1` en el proyecto `default`.

```
hostname:shares default> filesystem fs-1
hostname:shares default/fs-1 (uncommitted)>
```

4. Si está creando un LUN, introduzca `set volsize=` y el tamaño del volumen.

```
hostname:shares default/lun1 (uncommitted)> set volsize=2G
volsize = 2G (uncommitted)
```

5. Si el proyecto principal de este sistema de archivos o LUN no está cifrado, configure un tipo de cifrado.

Si el proyecto principal de este recurso compartido no está cifrado, el valor por defecto de la propiedad `encryption` es `off`. Para crear un recurso compartido cifrado, configure un valor nuevo en la propiedad `encryption`. Consulte [“Descripción de los valores de claves de cifrado” \[836\]](#) para ver descripciones de los valores de la propiedad `encryption`.

Si el proyecto principal de este recurso compartido está cifrado, el valor `encryption` se hereda y no se puede modificar.

6. Configure un almacén de claves y un nombre de clave.

Si el proyecto principal de este recurso compartido no está cifrado, configure las propiedades `keystore` y `keyname`.

Si el proyecto principal de este recurso compartido está cifrado, los valores de las propiedades `keystore` y `keyname` se heredan del proyecto por defecto. Puede usar los valores heredados o puede modificarlos como se muestra en el siguiente ejemplo:

```
hostname:shares default/fs-1 (uncommitted)> set keyname=MyKey
keyname = MyKey (uncommitted)
```

7. Use los comandos `get` y `set` para configurar las demás propiedades de este sistema de archivos o LUN según corresponda.

Las propiedades del recurso compartido se describen en [“Propiedades de sistema de archivos” \[525\]](#) y [“Propiedades de LUN” \[534\]](#).

8. Introduzca el comando `commit`.

```
hostname:shares default/fs-1 (uncommitted)> commit
```

Temas relacionados

- [“Propiedades de cifrado” \[832\]](#)
- [“Gestión de claves de cifrado” \[833\]](#)
- [Cambio de clave de cifrado de recurso compartido \(CLI\) \[825\]](#)

▼ Cambio de clave de cifrado de recurso compartido (BUI)

Puede cambiar la clave de cifrado para un recurso compartido en cualquier momento, incluso cuando la están usando sistemas cliente.

Por defecto, los recursos compartidos heredan las claves de cifrado del proyecto principal. Puede modificar la clave de un recurso compartido sin cambiar la clave del proyecto principal.

- 1. Vaya a Recursos compartidos > Recursos compartidos.**
- 2. Seleccione Sistemas de archivos o LUN.**
- 3. Para encontrar el recurso compartido que desea modificar, haga clic en Mostrar todos, Local o Réplica.**

4. **Mueva el cursor sobre el recurso compartido que desea modificar y haga clic en el ícono de edición .**

Se muestran las propiedades de recursos compartidos.

5. **Si es necesario, desmarque Heredar del proyecto.**

Si la opción Heredar del proyecto está marcada, la clave solo se puede modificar desde el proyecto principal.

6. **Para modificar la clave de cifrado, seleccione el almacén de claves y la clave que desea usar.**

7. **Haga clic en Aplicar.**

Cuando hace clic en Aplicar, se graban los cambios y aparece la nueva clave en el área de clave de cifrado.

Temas relacionados

- [Cambio de clave de cifrado de un proyecto \(BUI\) \[819\]](#)
- [Supresión de una clave de cifrado \(BUI\) \[827\]](#)
- [“Propiedades de cifrado” \[832\]](#)

▼ Cambio de clave de cifrado de recurso compartido (CLI)

Puede cambiar la clave de cifrado para un recurso compartido en cualquier momento, incluso cuando la están usando sistemas cliente.

Por defecto, los recursos compartidos heredan las claves de cifrado del proyecto principal. Puede modificar la clave de un recurso compartido sin cambiar la clave del proyecto principal.

1. **Seleccione el sistema de archivos o LUN para el que desea cambiar la clave de cifrado.**
 - a. **Vaya a shares.**
 - b. **Seleccione el proyecto.**

Si el proyecto que está seleccionado no es el que desea, use el comando `select project-name` para seleccionar uno distinto.
 - c. **Seleccione el sistema de archivos o LUN.**

Introduzca `select filesystem-name` o `select lun-name`.

2. **Cambie la clave de cifrado del proyecto.**
Configure los valores de las propiedades `keystore` y `keyname`.
3. **Introduzca el comando `commit`.**

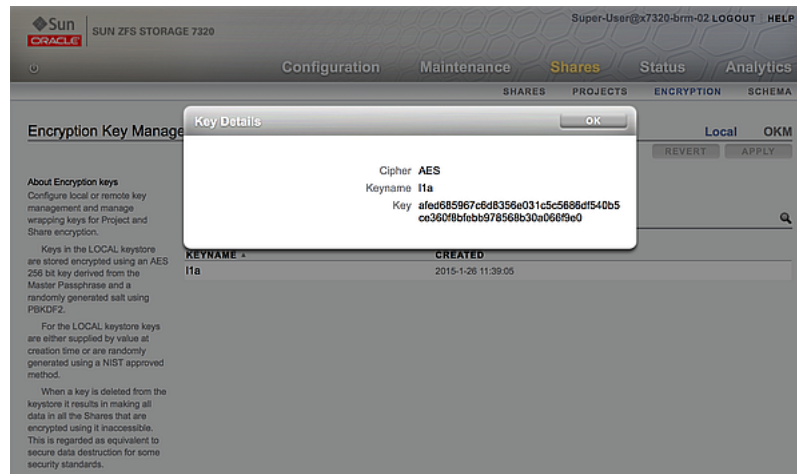
Temas relacionados

- [Cambio de clave de cifrado de proyecto \(CLI\) \[820\]](#)
- [Supresión de una clave de cifrado \(CLI\) \[828\]](#)
- [“Propiedades de cifrado” \[832\]](#)

▼ Copia de seguridad de una clave LOCAL (BUI)

Use el siguiente procedimiento para recuperar la información para una clave LOCAL única y hacer una copia de seguridad de la clave.

1. **Vaya a Recursos compartidos > Cifrado > Local.**
2. **Haga clic en la clave de la que desea hacer una copia de seguridad.**
Aparece un cuadro de diálogo con el nombre y el valor de la clave.



3. **Con el método de su preferencia, registre esta información en una ubicación de copia de seguridad también de su preferencia y, a continuación, haga clic en Aceptar.**

▼ Copia de seguridad de una clave LOCAL (CLI)

Use el siguiente procedimiento para recuperar la información para una clave LOCAL única y hacer una copia de seguridad de la clave.

1. **Seleccione la clave:**

```
hostname:shares encryption local keys> select keyname=Mykey
```

2. **Obtenga el valor de la clave:**

```
hostname:shares encryption local key-005> get key
key = d6a5b801fffb93fcb19ef70a11d662d8092f243c5d4ccd0cd34264b15dd0b7739
```

3. **Con el método de su preferencia, registre esta información en una ubicación de copia de seguridad también de su preferencia.**

▼ Supresión de una clave de cifrado (BUI)

Suprimir una clave de cifrado es una forma fácil y efectiva de convertir grandes cantidades de datos en inaccesibles. Las claves se pueden suprimir aun si están en uso. Si la clave está en uso, aparece una advertencia y se pide una confirmación. Todos los recursos compartidos, proyectos o agrupaciones que usan esa clave quedan sin compartir, y los clientes ya no pueden acceder a ellos.

Si hay probabilidades de que vuelva a usar una clave LOCAL para acceder a los recursos compartidos asociados a ella, haga una copia de seguridad del nombre y el valor de la clave antes de suprimirla según se describe en [Copia de seguridad de una clave LOCAL \(BUI\) \[826\]](#). Así, cuando lo necesite, puede llevar a cabo un procedimiento de restauración como se describe en [Restauración de una clave LOCAL \(BUI\) \[830\]](#).

Cuando se suprime una clave de cifrado que está siendo usada por una agrupación, un proyecto o un recurso compartido, todas las agrupaciones, proyectos y recursos compartidos se muestran como dependientes de la clave en el cuadro de diálogo de claves para destruir. Cuando se suprime la clave, el valor de Estado de clave cambia a "no disponible" y se muestra un indicador de aviso  a la derecha del ícono de bloqueo  para la agrupación o el recurso compartido afectados.

Realice el siguiente procedimiento para suprimir una clave de cifrado.

1. **Vaya a Recursos compartidos > Cifrado.**
2. **Seleccione el separador de almacén de claves correspondiente.**

3. **Mueva el cursor sobre la clave que desea suprimir y haga clic en el ícono de supresión .**

Se muestra una alerta que le avisa que todos los recursos compartidos que estén utilizando esta clave dejarán de estar montados y compartidos. Si suprime esta clave, todos los datos de los recursos compartidos que estén cifrados con esta clave se volverán inaccesibles de forma permanente e irre recuperable. Luego, la alerta muestra las agrupaciones y los recursos compartidos que dependen de esta clave.

4. **Para suprimir la clave, haga clic en Aceptar. Para conservar la clave, haga clic en CANCELAR.**

Cuando se suprime una clave, todos los datos de todas las agrupaciones y todos los recursos compartidos que utilizan la clave se vuelven inaccesibles. Esto equivale a asegurar la destrucción de los datos y es una acción permanente e irrevocable a menos que esté preparado para restablecer la clave por medio de una copia de seguridad de la clave. Para obtener más información acerca de la copia de seguridad y la restauración de claves, consulte [Copia de seguridad de una clave LOCAL \(BUI\) \[826\]](#) y [Restauración de una clave LOCAL \(BUI\) \[830\]](#).

Temas relacionados

- [Cambio de clave de cifrado de recurso compartido \(BUI\) \[824\]](#)
- [Supresión de una clave de cifrado \(CLI\) \[828\]](#)
- [“Gestión de claves de cifrado” \[833\]](#)
- [“Ciclo de vida de clave de cifrado” \[838\]](#)

▼ Supresión de una clave de cifrado (CLI)

Suprimir una clave de cifrado es una forma fácil y efectiva de convertir grandes cantidades de datos en inaccesibles. Las claves se pueden suprimir aun si están en uso. Si la clave está en uso, aparece una advertencia y se pide una confirmación. Todos los recursos compartidos, proyectos o agrupaciones que usan esa clave quedan sin compartir, y los clientes ya no pueden acceder a ellos.

Si hay probabilidades de que vuelva a usar una clave LOCAL para acceder a los recursos compartidos asociados a ella, haga una copia de seguridad del nombre y el valor de la clave antes de suprimirla. Así, cuando lo necesite, puede llevar a cabo un procedimiento de restauración como se describe en [Restauración de una clave LOCAL \(CLI\) \[831\]](#).

Cuando se suprime una clave de cifrado que está siendo usada por una agrupación, un proyecto o un recurso compartido, todas las agrupaciones, proyectos y recursos compartidos se muestran

como dependientes de la clave. Cuando se suprime la clave, el valor de la propiedad `keystatus` cambia a `unavailable`.

Realice el siguiente procedimiento para suprimir una clave de cifrado.

1. **Vaya a `shares encryption`.**
2. **Vaya a la configuración del almacén de claves correspondiente.**
3. **Suprima la clave.**

Utilice el comando `destroy keyname` para suprimir la clave.

```
hostname:shares encryption local local_keys> destroy keyname=MyKey
```

This key has the following dependent shares:

```
pool-1
pool-1/local/default
pool-1/local/default/fs-1
```

Destroying this key will render the data inaccessible. Are you sure? (Y/N)

Lea la advertencia y confirme que desea suprimir la clave.

Cuando se suprime una clave, todos los datos de todas las agrupaciones y todos los recursos compartidos que utilizan la clave se vuelven inaccesibles. Esto equivale a asegurar la destrucción de los datos y es una acción permanente e irrevocable a menos que esté preparado para restablecer la clave por medio de una copia de seguridad de la clave. Para obtener más información acerca de la copia de seguridad y la restauración de claves, consulte [Copia de seguridad de una clave LOCAL \(CLI\) \[827\]](#) y [Restauración de una clave LOCAL \(CLI\) \[831\]](#).

4. **Verifique que ya no sea posible acceder al recurso compartido usando esa clave.**

- El valor de la propiedad `keystatus` cambia a `unavailable`.
- La propiedad `keystatus` se marca como crítica.
- La clave faltante se considera un error.

```
hostname:> shares select default select fs-1
hostname:shares default/fs-1> get encryption keystore keyname keystatus
```

```
encryption = aes-128-ccm (inherited)
keystore = LOCAL (inherited)
keyname = MyKey (inherited)
keystatus = unavailable
```

Errors:

```
key_unavailable
```

5. **Para mostrar los dependientes, use los siguientes comandos de la CLI:**

```
hostname:shares (pool-1) encryption local keys> select keyname=1 hostname:shares
(pool-010) encryption local key-002> list

Properties:
            cipher = AES
            keyname = 1

hostname:shares (pool-010) encryption local key-002> list dependents DEPENDENTS
pool-010/local/default/a hostname:shares (pool-010) encryption local key-002>
```

Temas relacionados

- [Cambio de clave de cifrado de recurso compartido \(CLI\) \[825\]](#)
- [Copia de seguridad de una clave LOCAL \(CLI\) \[827\]](#)
- [Restauración de una clave LOCAL \(CLI\) \[831\]](#)

▼ Restauración de una clave LOCAL (BUI)

Para restaurar una clave LOCAL que se suprimió, cree una nueva clave LOCAL que tenga el mismo nombre y valor de clave que la clave suprimida. Para ello, primero debe haber registrado esta información, o haberla incluido en una copia de seguridad, antes de suprimir la clave original. El procedimiento de copia de seguridad se describe en [Copia de seguridad de una clave LOCAL \(BUI\) \[826\]](#). Si bien al suprimir una clave LOCAL, los recursos compartidos se vuelven inaccesibles, es posible volver a tener acceso a dichos recursos si se vuelve a crear la clave LOCAL.

Para obtener información sobre cómo restaurar las claves en el almacén de claves de OKM, consulte la [documentación de Oracle Key Manager](#) en el [Centro de Ayuda de Oracle](#).

Use el siguiente procedimiento para restaurar una clave LOCAL de una copia de seguridad.

Nota - Si el nombre de clave está en uso con un valor de clave diferente para recursos compartidos existentes, cambie la clave utilizada para esos recursos compartidos antes de restaurar la clave LOCAL original. Para obtener más información, consulte [Cambio de clave de cifrado de recurso compartido \(BUI\) \[824\]](#).

1. **Recupere el nombre y el valor de la clave para la clave LOCAL desde la ubicación de la copia de seguridad.**
2. **Vaya a Recursos compartidos > Cifrado > Local y haga clic en el ícono de agregación .**
3. **Introduzca el mismo nombre de clave que el de la copia de seguridad.**

4. **Desactive la opción "Generar clave automáticamente" y establezca el valor de la clave con el mismo que el de la copia de seguridad.**
5. **Haga clic en Agregar para guardar la clave restaurada.**
Si el nombre de clave se está usando con recursos compartidos existentes, aparece un cuadro de diálogo. Para sobrescribir el valor de la clave en los recursos compartidos existentes, haga clic en Aceptar. Haga clic en CANCELAR para no agregar la nueva clave. Después puede cambiar la clave usada para esos recursos compartidos antes de repetir este procedimiento y restaurar la clave original. Para obtener más información, consulte [Cambio de clave de cifrado de recurso compartido \(BUI\) \[824\]](#).

Temas relacionados

- [Cambio de clave de cifrado de recurso compartido \(BUI\) \[824\]](#)
- [Copia de seguridad de una clave LOCAL \(BUI\) \[826\]](#)
- [Supresión de una clave de cifrado \(BUI\) \[827\]](#)

▼ Restauración de una clave LOCAL (CLI)

Para restaurar una clave LOCAL que se suprimió, cree una nueva clave LOCAL que tenga el mismo nombre y valor de clave que la clave suprimida. Para ello, primero debe haber registrado esta información, o haberla incluido en una copia de seguridad, antes de suprimir la clave original. El procedimiento de copia de seguridad se describe en [Copia de seguridad de una clave LOCAL \(CLI\) \[827\]](#). Si bien al suprimir una clave LOCAL, los recursos compartidos se vuelven inaccesibles, es posible volver a tener acceso a dichos recursos si se vuelve a crear la clave LOCAL.

Para obtener información sobre cómo restaurar las claves en el almacén de claves de OKM, consulte la [documentación de Oracle Key Manager](#) en el [Centro de Ayuda de Oracle](#).

Use el siguiente procedimiento para restaurar una clave LOCAL de una copia de seguridad.

Nota - Si el nombre de clave está en uso con un valor de clave diferente para recursos compartidos existentes, cambie la clave utilizada para esos recursos compartidos antes de restaurar la clave LOCAL original. Para obtener más información, consulte [Cambio de clave de cifrado de recurso compartido \(CLI\) \[825\]](#).

1. **Recupere el nombre y el valor de la clave para la clave LOCAL desde la ubicación de la copia de seguridad.**
2. **Cree una clave en el almacén de claves LOCAL:**

```
hostname:shares encryption local keys> create
```

3. Coloque un nombre a la clave en función de la copia de seguridad:

```
hostname:shares encryption local key-005 (uncommitted)> set keyname=Mykey  
keyname = Mykey (uncommitted)
```

4. Defina el valor de clave en función de la copia de seguridad:

```
hostname:shares encryption local key-005 (uncommitted)> set key=key-value  
key = key-value (uncommitted)
```

5. Guarde la clave:

```
hostname:shares encryption local key-005 (uncommitted)> commit
```

Si el nombre de clave se está usando con recursos compartidos existentes, aparece una alerta:

```
Existing shares reference the key Mykey from the LOCAL keystore. Are you sure? (Y/N)
```

Para sobrescribir el valor de la clave en los recursos compartidos existentes, escriba Y (Sí). Escriba N (No) para no agregar la nueva clave. Después puede cambiar la clave usada para esos recursos compartidos antes de repetir este procedimiento y restaurar la clave original. Para obtener más información, consulte [Cambio de clave de cifrado de recurso compartido \(CLI\) \[825\]](#).

Temas relacionados

- [Cambio de clave de cifrado de recurso compartido \(CLI\) \[825\]](#)
- [Copia de seguridad de una clave LOCAL \(CLI\) \[827\]](#)
- [Supresión de una clave de cifrado \(CLI\) \[828\]](#)

Propiedades de cifrado

En la siguiente lista, se muestran las propiedades de cifrado disponibles para crear y gestionar claves, y para crear agrupaciones, proyectos y recursos compartidos cifrados.

- **Propiedades de gestión de claves LOCAL**
 - **Master Passphrase (Frase de contraseña maestra):** la frase de contraseña maestra se usa para generar una clave AES para cifrar las claves almacenadas en el almacén de claves LOCAL. Se usa el algoritmo PKCS#5 PBKDF para generar la clave, que es generada y gestionada aleatoriamente por el sistema.
- **Propiedades de creación de claves LOCALES**
 - **Nombre de clave:** nombre para identificar la clave.
 - **Clave:** clave raw de 256 bits hexadecimal, que se almacena cifrada.
- **Propiedades de gestión de claves de OKM** (proporcionadas por el administrador de OKM)
 - **Servidor de gestión de claves:** dirección IP del servidor de OKM.

- **ID de agente de usuario:** ID de agente.
- **PIN de registro:** PIN de registro.
- **Propiedades de creación de claves de OKM**
 - **Nombre de clave:** nombre para identificar la clave.
- **Propiedades de gestión de claves de KMIP**
 - **Servidor de KMIP :** nombre de host o dirección IP de un servidor de KMIP. Esta propiedad puede tener varios valores.
 - **Certificado:** certificado que cargó en el dispositivo a partir de archivos proporcionados por el administrador de su servidor de KMIP.
- **Propiedades de creación de claves de KMIP**
 - **Nombre de clave:** nombre para identificar la clave.
- **Opciones de KMIP**

Consulte [“Almacén de claves del protocolo de interoperabilidad de gestión de claves \(KMIP\)” \[835\]](#) para obtener más información.

 - Valide el nombre de host del servidor con la identidad del servidor en el certificado del servidor.
 - Destruya o preserve una clave en el servidor de KMIP cuando esa clave es una clave suprimida en el dispositivo.
- **Propiedades de cifrado de agrupación, proyecto y recursos compartidos**
 - **Encryption (Cifrado):** tipo de cifrado AES y longitud de clave. Para obtener más información, consulte [“Descripción de los valores de claves de cifrado” \[836\]](#).
 - **Almacén de claves:** LOCAL, OKM o KMIP.
 - **Clave:** el nombre de una clave LOCAL, OKM o KMIP específica.
 - **Último cambio de clave:** fecha en que se modificó la clave por última vez.
 - **Estado de clave:** si el valor de esta propiedad es “no disponible”, la clave se suprimió.

Temas relacionados

- [Flujo de trabajo de cifrado de datos \[796\]](#)
- [“Gestión de claves de cifrado” \[833\]](#)
- [“Impacto del cifrado en el rendimiento” \[837\]](#)
- [“Ciclo de vida de clave de cifrado” \[838\]](#)

Gestión de claves de cifrado

El dispositivo incluye un almacén de claves LOCAL incorporado y la capacidad de conectarse con los almacenes de claves OKM y KMIP. Cada agrupación, proyecto o recurso compartido

cifrado requiere una clave de encapsulado de un almacén de claves. Las claves de cifrado de datos se gestionan mediante el dispositivo de almacenamiento y se almacenan cifradas de forma persistente mediante la clave de encapsulado desde el almacén de claves.

Almacén de claves de Oracle Key Manager (OKM)

OKM es un sistema de gestión de claves (KMS) integral que aborda la necesidad creciente de cifrado de datos basado en almacenamiento que tienen las empresas. Desarrollada para cumplir con los estándares abiertos, esta función proporciona la capacidad, escalabilidad e interoperabilidad para gestionar centralmente las claves de cifrado en infraestructuras de almacenamiento ampliamente distribuidas y heterogéneas.

OKM aborda los desafíos únicos de la gestión de claves de almacenamiento, entre los que se incluyen los siguientes:

- **Retención de claves a largo plazo:** OKM garantiza que los datos archivados estén siempre disponibles y retiene de manera segura las claves de cifrado durante todo el ciclo de vida de los datos.
- **Interoperabilidad:** OKM proporciona la interoperabilidad necesaria para admitir una amplia variedad de dispositivos de almacenamiento conectados a plataformas de sistemas abiertos o mainframe en un único servicio de gestión de claves de almacenamiento.
- **Alta disponibilidad:** con agrupación en clusters de N nodos activa, el equilibrio de carga dinámico y el failover automatizado, OKM proporciona alta disponibilidad, sin importar si los dispositivos están juntos o distribuidos por todo el mundo.
- **Alta capacidad:** OKM gestiona una gran cantidad de dispositivos de almacenamiento y una cantidad aún mayor de claves de almacenamiento. Un único dispositivo en cluster puede proporcionar servicios de gestión de claves para miles de dispositivos de almacenamiento y millones de claves de almacenamiento.
- **Configuración de clave flexible:** por cluster de OKM, las claves se pueden generar de forma automática o individualmente para un almacén de claves LOCAL o de OKM. Los administradores de seguridad son responsables de proporcionar los nombres de clave que, al combinarse con el almacén de claves, asocian una clave de encapsulado con una agrupación, un proyecto o un recurso compartido.

Nota - Si el dispositivo está en un cluster, no debe usar la configuración "frase de contraseña de un solo uso" para la creación del agente de servidor de OKM. De lo contrario, el registro en el otro nodo de cluster fallará y las claves no estarán disponibles en el failover.

Almacén de claves del protocolo de interoperabilidad de gestión de claves (KMIP)

El almacén de claves de KMIP se usa junto con los servidores compatibles con KMIP, incluido Oracle Key Vault. Oracle Key Vault es un dispositivo de software que se instala en un servidor dedicado y es compatible con el estándar OASIS KMIP.

Si se muestran varios servidores de KMIP, el dispositivo hará un failover para alternar entre servidores si el servidor actual no responde. Cada servidor de KMIP configurado debe presentar el mismo juego de claves al dispositivo y debe aceptar el mismo certificado presentado por el dispositivo para la autenticación de cliente.

El juego de servidores de KMIP y el certificado del cliente se pueden cambiar sin eliminar las claves del almacén de claves.

Confrontación de nombre de host

Cuando esta opción está activada, el sistema intenta verificar si el servidor de KMIP especificado coincide con el host especificado en el certificado de servidor par.

KMIP le permite usar el nombre de host o la dirección IP para especificar un servidor de KMIP. Si especifica una dirección IP para el servidor de KMIP y el nombre común de asunto del certificado firmado por la autoridad de certificación solo tiene un nombre de dominio, se produce un error en la validación de host del certificado. Si la opción de BUI Match Hostname (Confrontar nombre de host) está desactivada o la propiedad de CLI `host_match` se define en `false`, la validación de host no se realizará.

Para obtener mayor seguridad, realice la validación de host. Use el nombre de host para especificar el servidor de KMIP y active la opción de validación de host.

Destrucción o preservación de una clave en el servidor

KMIP tiene la opción de destruir o preservar una clave en el servidor de KMIP cuando esta clave se suprime en el dispositivo. Cuando la opción está activada, si una clave se suprime de la lista de claves conocidas por el dispositivo, también se destruye en el servidor de claves. Cuando la opción está desactivada, las claves permanecen en el servidor de claves después de que se suprimen de la lista de claves del dispositivo.

Un ejemplo de cuando desea mantener claves en el servidor de claves después de que se suprimen del dispositivo es cuando se configuran varios dispositivos distintos en Oracle Key Vault para ver el mismo juego de claves. Si suprime una clave en un dispositivo y la clave se suprime del servidor de claves, la clave permanecerá en la lista de los demás dispositivos y usted no podrá suprimirla porque no se encontrará y parecerá estar suprimida.

Otro ejemplo de cuando desea mantener claves en el servidor de claves después de que se suprimen del dispositivo es cuando se usa la replicación para reasignar el dispositivo. Mueve (replica) todos los orígenes fuera del dispositivo y desea cifrar ese origen movido con las mismas claves. Cuando el proceso de replicación limpia el dispositivo de origen original y suprime la clave, los recursos compartidos en la réplica no se podrán cifrar con esa clave si esta se suprime del servidor de claves.

Mantenimiento de claves

Se puede seguir accediendo a los recursos compartidos, los proyectos y las agrupaciones que usan claves de OKM o KMIP que están desactivadas. Para evitar que una clave de OKM o KMIP se use, debe suprimir explícitamente esa clave.

Para garantizar que pueda accederse a las agrupaciones, los recursos compartidos y los proyectos cifrados, realice una copia de seguridad de las configuraciones y de los valores de claves del almacén de claves LOCAL del dispositivo. Si una clave se vuelve inaccesible, los recursos compartidos, los proyectos o las agrupaciones que usan esa clave se vuelven inaccesibles.

- Si la clave de la agrupación no está disponible, no se pueden crear nuevos proyectos en esa agrupación.
- Si la clave del proyecto no está disponible, no se pueden crear nuevos recursos compartidos en el proyecto.

Las claves se pueden volver no disponibles de las siguientes maneras:

- Se suprimen las claves.
- Se revierte la versión a una que no admite cifrado.
- Se revierte la versión a una que no tiene configuradas las claves.
- Restablecimiento de configuración predeterminada
- El servidor de OKM o KMIP no está disponible.

Descripción de los valores de claves de cifrado

En la siguiente tabla, se muestran los valores de claves de cifrado de la CLI y la BUI con sus respectivas descripciones. Además, se indica si el tipo de cifrado funciona con la anulación de duplicación.

TABLA 150 Valores de claves de cifrado

Valor de la BUI	Valor de la CLI	Descripción
Desactivada	desactivado	Recurso compartido/proyecto/agrupación sin cifrar

Valor de la BUI	Valor de la CLI	Descripción
AES-128-CCM	aes-128-ccm	Cifrado de menor impacto en la CPU. Se puede anular la duplicación.
AES-192-CCM	aes-192-ccm	Se puede anular la duplicación.
AES-256-CCM	aes-256-ccm	Se puede anular la duplicación.
AES-128-GCM	aes-128-gcm	Conforme a recomendación de NIST SP800-38D. No se puede anular la duplicación.
AES-192-GCM	aes-192-gcm	Conforme a recomendación de NIST SP800-38D. No se puede anular la duplicación.
AES-256-GCM	aes-256-gcm	Cifrado que mayor impacto tiene en la CPU. Conforme a recomendación de NIST SP800-38D. No se puede anular la duplicación.

Impacto del cifrado en el rendimiento

El uso del cifrado con recursos compartidos puede afectar el rendimiento de la CPU, como se describe a continuación:

- El modo AES-128-CCM tiene el menor impacto en el rendimiento de la CPU y se recomienda para todas las cargas de trabajo que no impliquen requisitos LOCAL de seguridad.
- Cuando se leen los datos cifrados, estos se almacenan sin cifrar y se descomprimen en DRAM. Para cargas de trabajo con predominio de lectura que se pueden procesar como cargas con predominio de lectura desde la caché DRAM, la acción de descifrar los datos tiene un impacto mínimo.
- Cuando se usan dispositivos de caché SSD, los bloques de datos rechazados en la DRAM que quedan en la caché se comprimen y se cifran, por lo que deben ser descifrados y descomprimidos cuando regresan a la DRAM.
- Para las cargas de trabajo con predominio de escritura que usan bloques de gran tamaño (en especial de 128 KB y 1 MB), es posible que haya un impacto significativo en la CPU y disminuya el rendimiento. Es muy probable que se produzca esta situación si el tamaño de registro del sistema de archivos o el tamaño del bloque de volumen de LUN supera el tamaño del bloque de la aplicación.

Temas relacionados

- [Flujo de trabajo de cifrado de datos \[796\]](#)
- [“Propiedades de cifrado” \[832\]](#)
- [“Gestión de claves de cifrado” \[833\]](#)
- [“Ciclo de vida de clave de cifrado” \[838\]](#)

Ciclo de vida de clave de cifrado

El ciclo de vida de la clave de cifrado es flexible porque puede cambiar las claves en cualquier momento sin poner fuera de línea los servicios de datos.

Cuando se suprime una clave del almacén de claves, todos los recursos compartidos que la usan se desmontan y sus datos se vuelven inaccesibles.

- Las copias de seguridad de claves en el almacén de claves LOCAL se incluyen como parte de la copia de seguridad de la configuración del sistema. Para el almacén de claves es LOCAL, también se puede proporcionar la clave por valor en el momento de la creación para permitir que sea custodiada en un sistema externo, lo cual proporciona una alternativa de copia de seguridad/restauración.
- Las copias de seguridad de claves en el almacén de claves de OKM se deben realizar utilizando los servicios de copia de seguridad de OKM.
- El servicio correspondiente debe realizar una copia de seguridad de las claves del almacén de claves de KMIP en el servidor de KMIP.

Temas relacionados

- [Flujo de trabajo de cifrado de datos \[796\]](#)
- [“Propiedades de cifrado” \[832\]](#)
- [“Gestión de claves de cifrado” \[833\]](#)
- [“Impacto del cifrado en el rendimiento” \[837\]](#)

Copia de seguridad, replicación y restauración de proyectos y recursos compartidos cifrados

Utilice uno de los siguientes métodos para realizar copias de seguridad y restaurar proyectos y recursos compartidos cifrados:

- NDMP. Consulte [“Configuración de NDMP” \[411\]](#).
- Replicación remota. Consulte [Replicación remota \[623\]](#).

En el caso de la replicación remota de proyectos o recursos compartidos cifrados, tanto el origen como el destino deben ser compatibles con el cifrado y cumplir los siguientes requisitos:

- Versión de software 2013.1.3.0, o posterior
- Las claves de encapsulado de cifrado que el proyecto o el recurso compartido usan deben estar disponibles.

- El nombre de clave de OKM o KMIP debe ser idéntico en el almacén de claves, tanto en el origen de replicación como en el destino de replicación.
- El ID de agente de OKM o el nombre de host de KMIP deben ser únicos en los dispositivos de origen de replicación y destino de replicación. Los dispositivos de par de replicación no pueden usar el mismo agente o host.
- Los agentes de OKM o los servidores de KMIP para los pares de replicación se deben configurar en el servidor de OKM o KMIP a fin de que vean los mismos grupos de claves.

Si se intenta replicar un proyecto o recurso compartido cifrado, y el destino no admite el cifrado, se producirá un fallo en la replicación. Si la clave de ajuste no está disponible en el sistema de origen o el de destino, o si la versión del software del destino es anterior a 2013.1.3.0, se emite una alerta. Revise las alertas, tanto en el sistema de origen como en el de destino, para determinar el motivo por el que se produjo el error en la replicación.

Temas relacionados

- [Flujo de trabajo de cifrado de datos \[796\]](#)
- [“Gestión de claves de cifrado” \[833\]](#)
- [“Ciclo de vida de clave de cifrado” \[838\]](#)
- Oracle ZFS Storage Appliance: Compatibilidad de la replicación remota (ID de documento 1958039.1) en <https://support.oracle.com/>

Configuración de la propiedad heredada después de la restauración de la copia de seguridad

En esta descripción, "original" es el proyecto o el recurso compartido del que se realiza la copia de seguridad, antes de la restauración.

Si el proyecto o el recurso compartido original hereda las propiedades de su agrupación o proyecto principal, el proyecto o recurso compartido restaurado hereda las propiedades de su destino principal. Si la configuración de la propiedad del principal original es distinta de la del destino principal, la configuración de la propiedad heredada del proyecto o recurso compartido cambia cuando se restaura el proyecto o recurso compartido.

Si desea que el proyecto o recurso compartido restaurado tenga la misma configuración de la propiedad que el proyecto o recurso compartido original, configure esos valores de manera explícita en el proyecto o recurso compartido original en lugar de que estos hereden la configuración.

Por ejemplo, si un recurso compartido cifrado hereda la configuración de la propiedad cifrada de su proyecto principal, especifique la configuración de la propiedad cifrada de manera

explícita en el recurso compartido antes de realizar la copia de seguridad y restaurar el recurso compartido a un proyecto distinto con otra configuración de cifrado.

Flujos de trabajo de mantenimiento

Un flujo de trabajo es una secuencia de comandos de la CLI cargada y gestionada por el propio dispositivo. Los flujos de trabajo se pueden configurar con parámetros y se pueden ejecutar con facilidad desde la interfaz del explorador o la interfaz de línea de comandos. Los flujos de trabajo también se pueden ejecutar opcionalmente como alerta o a una hora designada. Así, los flujos de trabajo permiten que el dispositivo se *extienda* para capturar políticas y procedimientos específicos y se pueden usar (por ejemplo) para codificar formalmente las mejores prácticas para una organización o aplicación en particular.

Para trabajar con flujos de trabajo, use las siguientes secciones:

- [Descripción de flujos de trabajo](#)
- [Descripción de los parámetros de flujos de trabajo](#)
- [Parámetros restringidos de flujos de trabajo](#)
- [Optional Workflow Parameters](#)
- [Workflow Error Handling](#)
- [Workflow Input Validation](#)
- [Auditoría y generación de informes de ejecución de flujos de trabajo](#)
- [Descripción de control de versiones de flujos de trabajo](#)
- [Uso de los flujos de trabajo para acciones de alerta](#)
- [“Creación y publicación de alertas personalizadas dentro de un flujo de trabajo” \[853\]](#)
- [Uso de flujos de trabajo programados](#)
- [Uso de flujo de trabajo programado](#)
- [Codificación de programas de flujo de trabajo](#)
- [Creación de una hoja de trabajo basada en un tipo de unidad especificado](#)
- [Carga y ejecución de flujos de trabajo con la BUI](#)
- [Descarga de flujos de trabajo mediante el uso de la CLI](#)
- [Mostrar flujos de trabajo mediante el uso de la CLI](#)
- [Ejecución de flujos de trabajo con la CLI](#)
- [Auditoría de flujos de trabajo mediante el uso de la CLI \[867\]](#)

Descripción de flujos de trabajo

Los flujos de trabajo se incluyen en un archivo ECMAScript válido que contiene una única variable global: `workflow`. El objeto `workflow` debe contener por lo menos tres miembros:

TABLA 151 Miembros objeto `workflow` requeridos

Miembro requerido	Tipo	Descripción
<code>name</code>	Cadena	Nombre del flujo de trabajo.
<code>description</code>	Cadena	Descripción del flujo de trabajo
<code>execute</code>	Función	Función que ejecuta el flujo de trabajo.

EJEMPLO 7 Flujo de trabajo Hello World

En este ejemplo, se muestra un flujo de trabajo simple.

```
var workflow = {
  name: 'Hello world',
  description: 'Bids a greeting to the world',
  execute: function () { return ('hello world!') }
};
```

Al cargar este flujo de trabajo, se genera un nuevo flujo de trabajo llamado "Hello world". Al ejecutar este flujo de trabajo, se genera la salida "hello world!"

EJEMPLO 8 Uso del flujo de trabajo de la función Ejecutar para devolver el uso de CPU

Los flujos de trabajo se ejecutan de manera asíncrona en el shell del dispositivo y utilizan (por defecto) el usuario que ejecuta el flujo de trabajo. Así, los flujos de trabajo tienen a su disposición la utilidad de secuencias de comandos del dispositivo (consulte [“Trabajo con secuencias de comandos de la CLI” \[45\]](#)) y pueden interactuar con el dispositivo de la misma manera que otra instancia del shell del dispositivo. Por ejemplo, los flujos de trabajo pueden ejecutar comandos, analizar salidas y modificar estados. Este ejemplo más complejo usa la función `run` para devolver el uso actual de la CPU.

```
var workflow = {
  name: 'CPU utilization',
  description: 'Displays the current CPU utilization',
  execute: function () {
    run('analytics datasets select name=cpu.utilization');
    cpu = run('csv 1').split('\n')[1].split(',');
    return ('At ' + cpu[0] + ', utilization is ' + cpu[1] + '%');
  }
};
```

Descripción de los parámetros de flujos de trabajo

Los flujos de trabajo que no funcionan con entrada de datos tienen un alcance limitado, ya que muchos flujos de trabajo necesitan parámetros ajustables para ser de utilidad. Para ello, se agrega un miembro `parameters` al objeto global `workflow`. El miembro `parameters` es a su vez un objeto que se espera que tenga un miembro para cada parámetro. Cada miembro `parameters` debe tener los siguientes miembros:

TABLA 152 Miembros de parámetros de flujo de trabajo requeridos

Miembro obligatorio	Tipo	Descripción
<code>label</code>	Cadena	Etiqueta para adornar la entrada del parámetro del flujo de trabajo.
<code>type</code>	Cadena	Tipo de parámetro de flujo de trabajo.

El miembro `type` debe ser de uno de estos tipos:

TABLA 153 Nombres de tipos de miembros de flujo de trabajo

Nombre del tipo	Descripción
<code>Boolean</code>	Valor booleano
<code>ChooseOne</code>	Un valor de una serie de valores especificados
<code>EmailAddress</code>	Dirección de correo electrónico
<code>File</code>	Archivo que se transfiere al dispositivo
<code>Host</code>	Host válido, como nombre o decimal con punto
<code>HostName</code>	Nombre de host válido
<code>HostPort</code>	Puerto válido disponible
<code>Integer</code>	Número entero
<code>NetAddress</code>	Dirección de red
<code>NodeName</code>	Nombre de nodo de red
<code>NonNegativeInteger</code>	Número entero mayor o igual que cero
<code>Number</code>	Cualquier número, incluido el punto flotante
<code>Password</code>	Contraseña
<code>Permissions</code>	Permisos de POSIX
<code>Port</code>	Número de puerto
<code>Size</code>	Tamaño
<code>String</code>	Cadena
<code>StringList</code>	Lista de cadenas

EJEMPLO 9 Flujo de trabajo con dos parámetros

En función de los tipos especificados, se genera una entrada apropiada al ejecutarse el flujo de trabajo. Por ejemplo, el siguiente flujo de trabajo tiene dos parámetros, el nombre de una unidad de negocio (que se usa como proyecto) y el nombre de un recurso compartido (que se usa como nombre del recurso compartido):

```
var workflow = {
  name: 'New share',
  description: 'Creates a new share in a business unit',
  parameters: {
    name: {
      label: 'Name of new share',
      type: 'String'
    },
    unit: {
      label: 'Business unit',
      type: 'String'
    }
  },
  execute: function (params) {
    run('shares select ' + params.unit);
    run('filesystem ' + params.name);
    run('commit');
    return ('Created new share "' + params.name + '"');
  }
};
```

Si se carga y ejecuta este flujo de trabajo, aparecerá un cuadro de diálogo para que complete el nombre del recurso compartido y la unidad de negocio. Cuando se haya creado el recurso compartido, se genera un mensaje para indicar que se lo creó.

Parámetros restringidos de flujos de trabajo

Para algunos parámetros, no se desea permitir una cadena arbitraria, sino más bien limitar la entrada a una de una cantidad pequeña de alternativas. Estos parámetros se deben definir con el tipo `chooseOne`, y el objeto que contiene el parámetro debe tener dos miembros adicionales:

TABLA 154 Miembros requeridos de parámetros restringidos

Miembro obligatorio	Tipo	Descripción
<code>options</code>	Matriz	Matriz de cadenas que especifica las opciones válidas.
<code>optionlabels</code>	Matriz	Matriz de cadenas que especifica las etiquetas asociadas con las opciones especificadas en <code>options</code> .

EJEMPLO 10 Uso de parámetro ChooseOne de flujo de trabajo

Con el tipo de parámetro `chooseOne`, se puede mejorar el ejemplo previo para limitar que la unidad de negocio sea una de una cantidad pequeña de valores predefinidos:

```
var workflow = {
  name: 'Create share',
  description: 'Creates a new share in a business unit',
  parameters: {
    name: {
      label: 'Name of new share',
      type: 'String'
    },
    unit: {
      label: 'Business unit',
      type: 'ChooseOne',
      options: [ 'development', 'finance', 'qa', 'sales' ],
      optionlabels: [ 'Development', 'Finance',
        'Quality Assurance', 'Sales/Administrative' ],
    }
  },
  execute: function (params) {
    run('shares select ' + params.unit);
    run('filesystem ' + params.name);
    run('commit');
    return ('Created new share "' + params.name + '"');
  }
};
```

Cuando se ejecuta este flujo de trabajo, el parámetro `unit` no se introduce manualmente, sino que se lo selecciona de la lista especificada de opciones posibles.

Parámetros de flujo de trabajo opcionales

Algunos parámetros se pueden considerar *opcionales* porque la UI no necesita que se les asigne ningún valor para poder ejecutar el flujo de trabajo. Para denotar este tipo de parámetros se usa el campo `optional` del miembro `parameters`:

TABLA 155 Miembros requeridos para parámetros opcionales

Miembro opcional	Tipo	Descripción
<code>optional</code>	Booleano	Si se configura con el valor <code>true</code> , significa que no es necesario configurar el parámetro, es decir, la UI puede permitir la ejecución del flujo de trabajo sin que se especifique un valor para el parámetro.

Si el parámetro es opcional y no está configurado, el miembro correspondiente del objeto de parámetros que se pasa a la función `execute` se configura con el valor `undefined`.

Manejo de errores de flujo de trabajo

Si durante la ejecución de un flujo de trabajo se produce un error, el sistema arroja una excepción. Si el flujo de trabajo no captura la excepción (o si el flujo de trabajo arroja una excepción que no se captura por otro medio), se produce un error en la ejecución del flujo de trabajo y se presenta al usuario la información relacionada con la excepción. Para manipular errores correctamente, se deben capturar y procesar las excepciones. Por ejemplo, en el ejemplo anterior, al intentar crear un recurso compartido en un proyecto inexistente, se produce una excepción no capturada.

EJEMPLO 11 Manejo de errores de flujo de trabajo

Este ejemplo se puede modificar para capturar el error y crear el proyecto en el caso de que no exista:

```
var workflow = {
  name: 'Create share',
  description: 'Creates a new share in a business unit',
  parameters: {
    name: {
      label: 'Name of new share',
      type: 'String'
    },
    unit: {
      label: 'Business unit',
      type: 'ChooseOne',
      options: [ 'development', 'finance', 'qa', 'sales' ],
      optionlabels: [ 'Development', 'Finance',
        'Quality Assurance', 'Sales/Administrative' ],
    }
  },
  execute: function (params) {
    try {
      run('shares select ' + params.unit);
    } catch (err) {
      if (err.code != EAKSH_ENTITY_BADSELECT)
        throw (err);

      /*
       * We haven't yet created a project that corresponds to
       * this business unit; create it now.
       */
      run('shares project ' + params.unit);
      run('commit');
      run('shares select ' + params.unit);
    }

    run('filesystem ' + params.name);
    run('commit');
```

```

    return ('Created new share "' + params.name + '"');
  }
};

```

Validación de entradas de flujo de trabajo

Los flujos de trabajo pueden, de manera opcional, validar la entrada que reciben; para ello, agregan un miembro `validate` que toma como parámetro un objeto que contiene los parámetros del flujo de trabajo como miembros. La función `validate` debe devolver un objeto en el que cada miembro tenga el nombre del parámetro que falló la validación y el valor de cada miembro sea el mensaje de fallo de validación que se debe mostrar al usuario.

EJEMPLO 12 Validación de entradas de flujo de trabajo

Para ampliar nuestro ejemplo a fin de generar un error claro si el usuario intenta crear un recurso compartido existente:

```

var workflow = {
  name: 'Create share',
  description: 'Creates a new share in a business unit',
  parameters: {
    name: {
      label: 'Name of new share',
      type: 'String'
    },
  },
  unit: {
    label: 'Business unit',
    type: 'ChooseOne',
    options: [ 'development', 'finance', 'qa', 'sales' ],
    optionlabels: [ 'Development', 'Finance',
      'Quality Assurance', 'Sales/Administrative' ],
  },
},
validate: function (params) {
  try {
    run('shares select ' + params.unit);
    run('select ' + params.name);
  } catch (err) {
    if (err.code == EAKSH_ENTITY_BADSELECT)
      return;
  }

  return ({ name: 'share already exists' });
},
execute: function (params) {
  try {
    run('shares select ' + params.unit);
  } catch (err) {
    if (err.code != EAKSH_ENTITY_BADSELECT)
      throw (err);
  }

  /*
   * We haven't yet created a project that corresponds to
   * this business unit; create it now.

```

```
    */
    run('shares project ' + params.unit);
    set('mountpoint', '/export/' + params.unit);
    run('commit');
    run('shares select ' + params.unit);
  }

  run('filesystem ' + params.name);
  run('commit');
  return ('Created new share "' + params.name + '"');
};
```

Auditoría y generación de informes de ejecución de flujos de trabajo

Los flujos de trabajo pueden emitir registros de auditoría si llaman a la función `audit()`. El único argumento de la función `audit` es una cadena que se colocará en el log de auditoría.

La función `audit()` muestra el usuario real que ejecutó el flujo de trabajo solo si `setid` está configurado en `false`. Sin embargo, si el propietario de un flujo de trabajo es el usuario `root` y `setid` está configurado en `true`, los logs de auditoría mostrarán `root` como el usuario de ejecución, aun si el flujo de trabajo fue ejecutado por otro usuario.

Para determinar qué usuario está ejecutando el flujo de trabajo independientemente de la configuración de `setid`, use la función `whoami()`.

EJEMPLO 13 Función `whoami` de prueba de flujo de trabajo

```
var workflow = {
  name: "Test whoami",
  description: "Print current username",
  execute: function () {
    return ("Hello " + whoami());
  }
};
```

Para los flujos de trabajo complicados cuya ejecución requiere bastante tiempo, puede ser útil proporcionar información clara acerca del progreso para el usuario que ejecuta el flujo de trabajo. Para permitir que se genere un informe sobre la ejecución de un flujo de trabajo de esta manera, el miembro `execute` debe devolver una matriz de *pasos*. Cada elemento de la matriz debe contener los siguientes miembros:

TABLA 156 Miembros requeridos para la generación de informes de ejecución

Miembro obligatorio	Tipo	Descripción
<code>step</code>	Cadena	Cadena que denota el nombre del paso de ejecución.

Miembro obligatorio	Tipo	Descripción
execute	Función	Función que ejecuta el paso del flujo de trabajo.

Al igual que con la función `execute` para el flujo de trabajo como un todo, el miembro `execute` de cada paso toma como argumento un objeto que contiene los parámetros del flujo de trabajo.

EJEMPLO 14 Generación de informes de ejecución de flujos de trabajo

Como ejemplo, en el siguiente flujo de trabajo, se crea un nuevo proyecto, recurso compartido y registro de auditoría en tres pasos:

```
var steps = [ {
  step: 'Checking for associated project',
  execute: function (params) {
    try {
      run('shares select ' + params.unit);
    } catch (err) {
      if (err.code != EAKSH_ENTITY_BADSELECT)
        throw (err);
    }

    /*
     * We haven't yet created a project that corresponds to
     * this business unit; create it now.
     */
    run('shares project ' + params.unit);
    set('mountpoint', '/export/' + params.unit);
    run('commit');
    run('shares select ' + params.unit);
  }
}, {
  step: 'Creating share',
  execute: function (params) {
    run('filesystem ' + params.name);
    run('commit');
  }
}, {
  step: 'Creating audit record',
  execute: function (params) {
    audit('created "' + params.name + '" in "' + params.unit);
  }
}
];

var workflow = {
  name: 'Create share',
  description: 'Creates a new share in a business unit',
  parameters: {
    name: {
      label: 'Name of new share',
      type: 'String'
    },
    unit: {
      label: 'Business unit',
      type: 'ChooseOne',
      options: [ 'development', 'finance', 'qa', 'sales' ],

```

```

        optionlabels: [ 'Development', 'Finance',
            'Quality Assurance', 'Sales/Administrative' ],
    },
    validate: function (params) {
        try {
            run('shares select ' + params.unit);
            run('select ' + params.name);
        } catch (err) {
            if (err.code == EAKSH_ENTITY_BADSELECT)
                return;
        }

        return ({ name: 'share already exists' });
    },
    execute: function (params) { return (steps); }
};

```

Mediante el uso de la función de correo, los flujos de trabajo pueden enviar ciertas salidas del flujo de trabajo por correo electrónico. La función de correo debe contener los siguientes argumentos: un objeto con `to` y `subject`, y una cadena `messageBody`.

EJEMPLO 15 Ejecución del flujo de trabajo con una aplicación de correo

```

var workflow = {
    name: 'email controller state',
    description: 'email controller state',
    execute: function () {

        // verify state of the controller
        var faulted = run('maintenance hardware "chassis-000" get faulted');

        var messageBody = faulted;

        emailAddress = 'first.last@xyz.com';
        subjectLine = 'Controller State';
        mail({To: emailAddress, Subject: subjectLine}, messageBody);

    }
};

```

Descripción de control de versiones de flujos de trabajo

El control de versiones tiene dos aspectos relevantes para los flujos de trabajo: el primero es la expresión de la versión del software de dispositivo de la que depende el flujo de trabajo, y el segundo es la expresión de la versión del flujo de trabajo en sí. El control de versiones se expresa mediante dos miembros opcionales en el flujo de trabajo:

TABLA 157 Miembros opcionales para el control de versiones

Miembro opcional	Tipo	Descripción
<code>required</code>	Cadena	Versión mínima requerida del software de dispositivo para poder ejecutar el flujo de trabajo, incluidos el año, mes, día, compilación y rama.
<code>version</code>	Cadena	Versión de este flujo de trabajo, en formato decimal con puntos (principal.secundaria.micro).

Control de versiones de dispositivo - Para expresar una versión de software de dispositivo mínima requerida, agregue el campo opcional `required` al flujo de trabajo. Las versiones de los dispositivos corresponden al año, el mes y el día de desarrollo del software, seguido por un número de compilación y un número de rama, expresado como `"year.month.day.build-branch"`. Por ejemplo `"2018.04.10,12-0"` sería la compilación doce del software originalmente desarrollado el 10 de abril de 2018. Para obtener la versión de software actual del kit de dispositivos, ejecute el comando `configuration version get version` de la CLI o consulte el campo Versión de la pantalla Sistema en la BUI. A continuación se presenta un ejemplo del uso del campo `required`:

EJEMPLO 16 Uso del campo Requerido del flujo de trabajo

A continuación se presenta un ejemplo del uso del campo `required`:

```
var workflow = {
  name: 'Configure FC',
  description: 'Configures fibre channel target groups',
  required: '2018.12.25,1-0',
  ...
}
```

Si un flujo de trabajo requiere una versión de software que es más reciente que la versión cargada en el dispositivo, se producirá un error al intentar cargar el flujo de trabajo y aparecerá un mensaje que explicará la discrepancia.

Control de versiones de flujos de trabajo - Además de especificar la versión requerida para el software del dispositivo, también se puede usar el campo `version` para generar versiones de los flujos de trabajo. Esta cadena denota el número principal, secundario y micro de la versión del flujo de trabajo, y permite la existencia de varias versiones del mismo flujo de trabajo en el equipo. Al cargar un flujo de trabajo, se suprimen todas las versiones *anteriores* y *compatibles* del mismo flujo de trabajo. Se considera que un flujo de trabajo es *compatible* si tiene el mismo número principal, y se considera que un flujo de trabajo es *anterior* si tiene un número de versión menor. Por lo tanto, si se carga la versión `"2.1"` de un flujo de trabajo, se eliminará la versión `"2.0"` (o la versión `"2.0.1"`) de ese mismo flujo de trabajo, pero no las versiones `"1.2"` ni `"0.1"`.

Uso de los flujos de trabajo para acciones de alerta

Un flujo de trabajo puede ejecutarse como acción de alerta. Un flujo de trabajo que se ejecuta como acción de alerta es el flujo de trabajo seleccionado para la acción de alerta (BUI) Ejecutar flujo de trabajo o es el valor de la propiedad `workflow` del gestor `execute_workflow` (CLI), como se describe en [“Agregación de acciones de alerta” \[287\]](#).

Para permitir que un flujo de trabajo se ejecute como acción de alerta, la variable global `workflow` debe especificar un miembro `alert: true`.

Por defecto, los flujos de trabajo se ejecutan bajo el usuario que los está ejecutando. Sin embargo, un flujo de trabajo que se ejecuta como acción de alerta se ejecuta por defecto bajo el usuario que creó el flujo de trabajo. Para poder ejecutarse como acción de alerta, la variable global `workflow` del flujo de trabajo debe especificar un miembro `setid: true`.

Las acciones de alerta tienen un parámetro de objeto único que tiene los siguientes miembros.

TABLA 158 Miembros requeridos para el contexto de ejecución de las alertas

Miembro obligatorio	Tipo	Descripción
<code>class</code>	Cadena	Clase de alerta.
<code>code</code>	Cadena	Código de alerta.
<code>items</code>	Objeto	Objeto que describe la alerta.
<code>timestamp</code>	Fecha	Fecha/hora de la alerta.

El miembro `items` del objeto de parámetros tiene los siguientes miembros:

TABLA 159 Miembros requeridos para el miembro de elementos

Miembro obligatorio	Tipo	Descripción
<code>url</code>	Cadena	Dirección URL de la página web en donde se describe la alerta.
<code>action</code>	Cadena	Acción que debe realizar el usuario en respuesta a la alerta.
<code>impact</code>	Cadena	Impacto del evento que generó la alerta.
<code>description</code>	Cadena	Cadena en lenguaje natural en donde se describe la alerta.
<code>severity</code>	Cadena	Gravedad del evento que generó la alerta.

EJEMPLO 17 Flujo de trabajo auditoría de errores al reiniciar

Los flujos de trabajo que se ejecutan como acciones de alerta pueden utilizar la función `audit` para generar entradas de log de auditoría. Por ejemplo, la información de depuración debe escribirse en el log de auditoría.

Consulte los distintos usos de la función `audit` en el siguiente ejemplo. Este flujo de trabajo:

- Se ejecuta en respuesta a que la alerta `params.uuid` especifica la ejecución de este flujo de trabajo.
- Reinicia el sistema solamente si los dos sistemas están en estado en cluster.
- Audita todos los fallos que puedan producirse al reiniciar.

```
var workflow = {
  name: 'Failover',
  description: 'Fail the node over to its clustered peer',
  alert: true,
  setid: true,
  execute: function (params) {
    var uuid = params.uuid;
    var clustered = 'AKCS_CLUSTERED';

    audit('attempting failover in response to alert ' + uuid);

    try {
      run('configuration cluster');
    } catch (err) {
      audit('could not get clustered state; aborting');
      return;
    }

    if ((state = get('state')) != clustered) {
      audit('state is ' + state + '; aborting');
      return;
    }

    if ((state = get('peer_state')) != clustered) {
      audit('peer state is ' + state + '; aborting');
      return;
    }

    run('cd /');
    run('confirm maintenance system reboot');
  }
};
```

Creación y publicación de alertas personalizadas dentro de un flujo de trabajo

Puede publicarse una alerta dentro de un flujo de trabajo en respuesta a un evento definido en el flujo de trabajo. La acción de alerta puede crearse en el flujo de trabajo o a través de la BUI o la CLI. La alerta debe publicarse dentro del flujo de trabajo.

Pueden utilizarse alertas personalizadas para ayudar a garantizar la conformidad o las políticas administrativas. Las alertas personalizadas también pueden ayudar a diagnosticar problemas en un flujo de trabajo.

La siguiente tabla describe las autorizaciones que debe tener un usuario para crear acciones de alerta personalizadas y publicar alertas personalizadas.

TABLA 160 Autorizaciones requeridas para utilizar alertas personalizadas

Tarea	Autorización de BUI	Autorización de CLI	Descripción
Crear una acción de alerta personalizada	Ámbito: alertas Autorización: configurar	Ámbito: alert Autorización: allow_configure	Necesario para crear una acción de alerta personalizada utilizando la BUI, la CLI o la función <code>createalert</code> en un flujo de trabajo.
Publicar una alerta personalizada	Ámbito: alertas Autorización: publicación	Ámbito: alert Autorización: allow_post	Necesario para usar la función <code>postalert</code> en un flujo de trabajo.
Ejecutar un flujo de trabajo	Ámbito: flujo de trabajo Autorización: lectura	Ámbito: workflow Autorización: allow_read	Necesario para ejecutar un flujo de trabajo.

Para acceder a instrucciones sobre cómo otorgar autorizaciones a usuarios, consulte [“Configuración de usuarios” \[257\]](#).

Creación de una alerta personalizada

Utilice uno de los siguientes métodos para crear una alerta personalizada:

- Especifique la categoría de evento Personalizada o `custom` al crear una acción de alerta, como se describe en la siguiente documentación:
 - Agregación de una acción de alerta para un evento definido en un flujo de trabajo: [BUI](#), [CLI](#)
 - [“Personalizar alertas” de Guía de la API de RESTful de Oracle® ZFS Storage Appliance \(versión OS8.8.x\)](#)
- Utilice la función `createalert` en una secuencia de comandos o un flujo de trabajo. Para usar `createalert` en una secuencia de comandos, consulte [Uso de las funciones de alertas personalizadas \[51\]](#). El resto de esta sección describe cómo utilizar `createalert` en un flujo de trabajo.

Nota - Cada vez que se invoca `createalert`, se crea una nueva alerta con un UUID diferente. En lugar de crear más copias de la misma acción de alerta cada vez que se ejecuta un flujo de trabajo que utiliza `createalert`, quizás le convenga utilizar la BUI o la CLI para crear una acción de alerta y luego pasar el UUID de esa acción de alerta a la función `postalert`, como se muestra en [Ejemplo 20, “Publicación de una alerta personalizada con un UUID de acción de alerta existente”](#).

La función `createalert` toma los siguientes parámetros y devuelve el UUID de la acción de alerta personalizada que se ha creado.

TABLA 161 Parámetros de la función `createalert`

Parámetro	Tipo	Descripción
<code>actions</code>	Objeto	Necesario. Una lista de controladores (acciones de alerta) junto con los argumentos correspondientes. Consulte la columna "Tipo de acción de la CLI" en Tabla 49, “Tipos de acciones de alerta” . Nota - Si se especifica <code>execute_workflow</code> como acción (handler), el flujo de trabajo ejecutado no podrá publicar una alerta.
<code>severity</code>	Cadena	Opcional. Gravedad del evento que generó la alerta. Los valores válidos son: crítico, menor o grave.
<code>description</code>	Cadena	Necesario. Una descripción del evento que generó la alerta.
<code>response</code>	Cadena	Opcional. Una descripción de las acciones que realizará el sistema para mitigar los efectos de este evento.
<code>impact</code>	Cadena	Opcional. Una descripción del efecto que este evento tiene sobre el dispositivo.
<code>recommended_action</code>	Cadena	Opcional. Una descripción de las acciones que debe realizar el administrador para mitigar los efectos de este evento.

EJEMPLO 18 Creación de una alerta personalizada dentro de un flujo de trabajo

Este ejemplo muestra un flujo de trabajo que crea una alerta personalizada con el UUID `custom_alert_uuid`.

```
var workflow = {
  name: 'createalert',
  description: 'Create a Custom Alert',
  version: '1.0',
  origin: 'Oracle',
  alert: false,
  setid: true,
  execute: function () {
    var actions = [{
      handler: 'email',
      args: {
        address: 'admin@example.com',
        subject: 'Custom Alert Response'
      }
    }];
    var createparams = {
```

```
        description: 'createalert from within a workflow'
    };
    var custom_alert_uuid = createalert(actions, createparams);
}
};
```

Al crear una alerta personalizada con un flujo de trabajo, la alerta aparece en la lista de acciones de alerta en la BUI y la CLI.

Al crear una alerta personalizada con un flujo de trabajo, se crea una entrada del log de auditoría con el siguiente resumen:

```
Workflow name_of_workflow: created custom alert value_of_custom_alert_uuid
```

Al crear una alerta personalizada con la BUI o la CLI, o a través de la ejecución de una secuencia de comandos (con el comando `script`), se crea una entrada del log de auditoría con el siguiente resumen:

```
Created custom alert value_of_custom_alert_uuid
```

Publicación de una alerta personalizada

Utilice la función `postalert` para publicar una alerta personalizada dentro de un flujo de trabajo en respuesta a un evento que se produce en ese flujo de trabajo.

La función `createalert` puede invocarse dentro de una secuencia de comandos a través del comando `script`, mientras que la función `postalert` solo puede invocarse dentro de una definición de flujo de trabajo.

La función `postalert` toma los mismos parámetros que la función `createalert`, salvo el primer parámetro: `createalert` toma una lista de controladores o acciones de alerta, y `postalert` toma el UUID de la alerta que se publicará. Para conocer las descripciones del resto de los parámetros, consulte [Tabla 161, “Parámetros de la función `createalert`”](#).

Los valores de los parámetros que son opciones para `createalert` (`severity`, `response`, `impact` y `action`) no son opcionales para `postalert`. Para la llamada `postalert`, estos valores se determinan en función de las siguientes reglas:

- Si se proporcionan valores de parámetros opcionales para `createalert`, pero no para la llamada `postalert` de ese UUID, la llamada `postalert` hereda esos valores de parámetros de la llamada `createalert` correspondiente.
- Si no se proporcionan valores de parámetros opcionales para `createalert`, pero sí para la llamada `postalert` de ese UUID, la llamada `postalert` utiliza los valores especificados en la llamada `postalert`.
- Si se proporcionan valores de parámetros opcionales tanto para `createalert` como para la llamada `postalert` correspondiente, cada llamada utiliza los valores de parámetros especificados en esa llamada.

- Si no se proporcionan valores de parámetros opcionales para la llamada `createalert` ni para la llamada `postalert` correspondiente, un mensaje de error le indica al usuario que proporcione valores para la llamada `postalert`.

La función `postalert` devuelve el UUID de la alerta personalizada que se ha publicado.

EJEMPLO 19 Creación y publicación de una alerta personalizada dentro de un flujo de trabajo

Este ejemplo publica la alerta que se creó en [Ejemplo 18](#), “[Creación de una alerta personalizada dentro de un flujo de trabajo](#)”. La llamada `postalert` se realiza en respuesta a un evento que se produjo en el flujo de trabajo. En este ejemplo, se omite el código que define el evento que ocurre antes de la llamada `postalert`.

```
var workflow = {
  name: 'createalert and postalert',
  description: 'Create and Post a Custom Alert',
  version: '1.0',
  origin: 'Oracle',
  alert: false,
  setid: true,
  execute: function () {
    var actions = [{
      'handler': 'resume_dataset',
      'args': {
        'dataset': 'dataset_to_resume'
      }
    }];
    var createparams = {
      description: 'createalert and postalert from within a workflow'
    };
    var postparams = {
      severity: 'Minor',
      description: 'postalert from within a workflow',
      response: 'The alert action resumes dataset dataset_to_resume',
      impact: 'What happened to the appliance',
      recommended_action: 'What the administrator should do'
    };
    var custom_alert_uuid = createalert(actions, createparams);
    var posted_alert_uuid = postalert(custom_alert_uuid, postparams);
  }
};
```

Al ejecutar un flujo de trabajo que invoca la función `postalert`, se crea una entrada de log de alerta con el siguiente resumen:

Custom: *name_of_workflow*

EJEMPLO 20 Publicación de una alerta personalizada con un UUID de acción de alerta existente

En lugar de propagar copias de la misma acción de alerta, quizás le convenga utilizar el UUID de una alerta personalizada existente como primer argumento de la función `postalert`.

1. Utilice la BUI, la CLI, una secuencia de comandos, un flujo de trabajo o la API de RESTful para crear una acción de alerta personalizada.
2. Utilice la BUI, la CLI o el log de auditoría para recuperar el UUID de la acción de alerta personalizada.
3. Utilice el UUID recuperado como primer argumento de la función `postalert`.

```
var workflow = {
  name: 'postalert',
  description: 'Post a Custom Alert using existing uuid',
  version: '1.0',
  origin: 'Oracle',
  alert: false,
  setid: true,
  execute: function () {
    var postparams = {
      severity: 'Minor',
      description: 'postalert from within a workflow',
      response: 'What the system will do',
      impact: 'What happened to the appliance',
      recommended_action: 'What the administrator should do'
    };
    var posted_alert_uuid = postalert('uuid_of_existing_custom_alert', postparams);
  }
};
```

Uso de flujos de trabajo programados

Es posible iniciar un flujo de trabajo mediante un evento de temporizador. Para ello, se debe definir un programa para el flujo de trabajo. Para crear y mantener programas para un flujo de trabajo, es necesario agregar la propiedad `scheduled` al flujo de trabajo Objeto y establecerla en `true`. Consulte la propiedad `scheduled` en [Ejemplo 22, “Uso de las propiedades de flujo de trabajo”](#) en [Codificación de programas de flujo de trabajo](#).

Los programas se pueden crear de una de las siguientes maneras:

- Mediante la interfaz CLI, como se describe en [“Uso de flujo de trabajo programado”](#) [859]
- Mediante una propiedad de tipo de matriz con el nombre `schedules` en el flujo de trabajo Objeto, como se describe en [“Codificación de programas de flujo de trabajo”](#) [860]

Un administrador con las autorizaciones apropiadas para el flujo de trabajo puede cambiar los programas a través de la interfaz CLI.

Uso de flujo de trabajo programado

Una vez que el flujo de trabajo que contiene la propiedad `scheduled: true` se carga en un dispositivo, se puede definir o modificar el programa mediante la interfaz de la CLI. Consulte la propiedad `scheduled` en [Ejemplo 22, “Uso de las propiedades de flujo de trabajo”](#) en [Codificación de programas de flujo de trabajo](#).

Cada entrada del programa tiene las siguientes propiedades:

TABLA 162 Propiedades de programas de flujo de trabajo

Propiedad	Tipo	Descripción
NAME	Cadena	Nombre del programa. Este valor es generado por el sistema.
frequency	Cadena	Los valores pueden ser minuto, media hora, hora, día, semana, mes
day	Cadena	Los valores pueden ser lunes, martes, miércoles, jueves, viernes, sábado o domingo. Este valor se puede definir solamente cuando <code>frequency</code> es <code>week</code> o <code>month</code> .
hour	Cadena	Los valores pueden ser 00, 01..., 23. Este valor se puede definir solamente cuando <code>frequency</code> es <code>day</code> , <code>week</code> o <code>month</code> .
minute	Cadena	00, 01..., 59. Este valor se puede configurar solamente cuando se define <code>hour</code> .

EJEMPLO 21 Flujo de trabajo programado en la CLI

Este ejemplo muestra cómo agregar dos horarios de ejecución a un flujo de trabajo llamado "My Scheduled Workflow". El primer horario de ejecución es todos los días a las 10:05 a. m. El segundo horario de ejecución programado para este flujo de trabajo es los lunes a la 1:15 p. m.

```
hostname:> maintenance workflows
hostname:maintenance workflows> select name="My Scheduled Workflow"
hostname:maintenance workflow-002> schedules
hostname:maintenance workflow-002 schedules> create
hostname:maintenance workflow-002 schedule (uncommitted)> set frequency=day
frequency = day (uncommitted)
hostname:maintenance workflow-002 schedule (uncommitted)> set hour=10
hour = 10 (uncommitted)
hostname:maintenance workflow-002 schedule (uncommitted)> set minute=05
minute = 05 (uncommitted)
hostname:maintenance workflow-002 schedule (uncommitted)> commit
hostname:maintenance workflow-002 schedules> list
NAME          FREQUENCY    DAY          HH:MM
schedule-001  day          -            10:05
hostname:maintenance workflow-002 schedules> create
hostname:maintenance workflow-002 schedule (uncommitted)> set frequency=week
frequency = week (uncommitted)
hostname:maintenance workflow-002 schedule (uncommitted)> set day=Monday
day = Monday (uncommitted)
hostname:maintenance workflow-002 schedule (uncommitted)> set hour=13
```

```

                                hour = 13 (uncommitted)
hostname:maintenance workflow-002 schedule (uncommitted)> set minute=15
                                minute = 15 (uncommitted)
hostname:maintenance workflow-002 schedule (uncommitted)> commit
hostname:maintenance workflow-002 schedules> list
NAME          FREQUENCY    DAY          HH:MM
schedule-001  day          -            10:05
schedule-002  week         Monday       13:15
hostname:maintenance workflow-002 schedules>

```

Codificación de programas de flujo de trabajo

Como alternativa a la definición de programas mediante la interfaz CLI como se describe en [Uso de flujo de trabajo programado](#), es posible definir programas en el código del flujo de trabajo como una propiedad en el flujo de trabajo Objeto. Las propiedades que se utilizan en los flujos de trabajo Objeto son diferentes a las que se utilizan en la creación de un programa en la CLI.

En los flujos de trabajo Objeto, se utilizan las siguientes propiedades:

TABLA 163 Propiedades de programas de flujo de trabajo

Propiedad	Tipo	Descripción
offset	Número	Determina el punto inicial del período definido.
period	Número	Define la frecuencia del programa.
unit	Cadena	Especifica si se utilizan segundos o meses como unidad en la definición del período y el desplazamiento.

Un administrador con las autorizaciones apropiadas para el flujo de trabajo puede cambiar los programas codificados en el flujo de trabajo como se muestra en [Uso de flujo de trabajo programado](#).

EJEMPLO 22 Uso de las propiedades de flujo de trabajo

El siguiente código ejemplifica el uso de las propiedades. Tenga en cuenta que la aritmética en línea facilita la legibilidad de las definiciones del período y el desplazamiento.

```

// Example of using Schedule definitions within a workflow
var MyTextObject = {
  MyVersion: '1.0',
  MyName: 'Example 9',
  MyDescription: 'Example of use of Timer',
  Origin: 'Oracle'
};

```



```

var MySchedules = [
  // half hr interval
  { offset: 0, period: 1800, units: "seconds" },
  // offset 2 days, 4hr, 30min , week interval
  {offset: 2*24*60*60+4*60*60+30*60, period: 604800,units: "seconds" }
];

var workflow = {
  name:      MyTextObject.MyName,
  description: MyTextObject.MyDescription,
  version:   MyTextObject.MyVersion,
  alert:     false,
  setid:     true,
  schedules: MySchedules,
  scheduled: true,
  origin:    MyTextObject.Origin,
  execute:   function () {
    audit('workflow started for timer');
  }
}

```

Las unidades de las propiedades en el objeto MySchedules especifican el tipo de unidades que se utilizan para las propiedades `offset` y `period`. Se pueden establecer en `seconds` o `month`. La propiedad `period` especifica la frecuencia del evento y `offset` especifica las unidades dentro del período. En el ejemplo anterior, el período del segundo programa se definió en una semana, a partir del segundo día, a las 4:30 a. m. Es posible definir varios programas en la propiedad `Schedules`.

El objeto MySchedules del ejemplo usa las siguientes tres propiedades:

- `offset` es el desplazamiento inicial desde el 1 de enero de 1970 para el programa. El desplazamiento se expresa en las unidades definidas por la propiedad `units`.
- `period` es el período entre repeticiones del programa, que también se expresa en las unidades definidas por la propiedad `units`.
- `units` se puede definir en `seconds` o `months`.

El punto inicial para los programas semanales es el jueves. Esto se debe a que el inicio del período es el 1 de enero de 1970, que fue jueves.

EJEMPLO 23 Programa de flujo de trabajo que se muestra en la CLI

En el ejemplo anterior, en el período del segundo programa se usa un desplazamiento inicial de 2 días + 4 horas + 30 minutos. Como resultado, la fecha inicial es el 3 de enero de 1970 a las 4:30 a. m. El programa se repite indefinidamente el sábado de cada semana a las 4:30 a. m. A continuación, se puede ver el programa como se muestra en la CLI.

```

hostname:> maintenance workflows
hostname:maintenance workflows> list
WORKFLOW  NAME                                OWNER SETID ORIGIN      VERSION
workflow-018 Check metaslab_unload_delay root false Oracle ZFSSA  1.0
workflow-019 Check metaslab_unload_timeout root false Oracle ZFSSA  1.0
workflow-020 Example 9                root true  <local>         1.0
workflow-021 Set DNLC size and ncsiz root false Data and App 2.0

```

```
workflow-022 Stop Existing SSH Sessions      root  false <local>      0.2
hostname: maintenance workflows> select name="Example 9"
hostname: maintenance workflow-020> schedules
hostname: maintenance workflow-020 schedules> ls
Schedules:
NAME          FREQUENCY      DAY          HH:MM
schedule-000  halfhour       -            --:00
schedule-001  week          Saturday     04:30
```

Crear una hoja de trabajo basada en un tipo de unidad especificado

El siguiente ejemplo es un flujo de trabajo que crea una hoja de trabajo basada en un tipo de unidad especificada:

EJEMPLO 24 Selección de tipo de dispositivo de flujo de trabajo

```
var steps = [ {
  step: 'Checking for existing worksheet',
  execute: function (params) {
    /*
     * In this step, we're going to see if the worksheet that
     * we're going to create already exists. If the worksheet
     * already exists, we blow it away if the user has indicated
     * that they desire this behavior. Note that we store our
     * derived worksheet name with the parameters, even though
     * it is not a parameter per se; this is explicitly allowed,
     * and it allows us to build state in one step that is
     * processed in another without requiring additional global
     * variables.
     */
    params.worksheet = 'Drilling down on ' + params.type + ' disks';

    try {
      run('analytics worksheets select name="' +
        params.worksheet + '"');

      if (params.overwrite) {
        run('confirm destroy');
        return;
      }

      throw ('Worksheet called "' + params.worksheet +
        '" already exists!');
    } catch (err) {
      if (err.code != EAKSH_ENTITY_BADSELECT)
        throw (err);
    }
  }, {
    step: 'Finding disks of specified type',
    execute: function (params) {
      /*
       * In this step, we will iterate over all chassis, and for
```

```

    * each chassis iterates over all disks in the chassis,
    * looking for disks that match the specified type.
    */
    var chassis, name, disks;
    var i, j;

    run('cd /');
    run('maintenance hardware');

    chassis = list();
    params.disks = [];

    for (i = 0; i < chassis.length; i++) {
        run('select ' + chassis[i]);

        name = get('name');
        run('select disk');
        disks = list();

        for (j = 0; j < disks.length; j++) {
            run('select ' + disks[j]);

            if (get('use') == params.type) {
                params.disks.push(name + '/' +
                    get('label'));
            }

            run('cd ..');
        }

        run('cd ../../');
    }

    if (params.disks.length === 0)
        throw ('No ' + params.type + ' disks found');
    run('cd /');
}
}, {
step: 'Creating worksheet',
execute: function (params) {
    /*
    * In this step, we're ready to actually create the worksheet
    * itself: we have the disks of the specified type and
    * we know that we can create the worksheet. Note that we
    * create several datasets: first, I/O bytes broken down
    * by disk, with each disk of the specified type highlighted
    * as a drilldown. Then, we create a separate dataset for
    * each disk of the specified type. Finally, note that we
    * aren't saving the datasets -- we'll let the user do that
    * from the created worksheet if they so desire. (It would
    * be straightforward to add a boolean parameter to this
    * workflow that allows that last behavior to be optionally
    * changed.)
    */
    var disks = [], i;

    run('analytics worksheets');
    run('create "' + params.worksheet + '"');
    run('select name="' + params.worksheet + '"');
    run('dataset');
    run('set name=io.bytes[disk]');

```

```
for (i = 0; i < params.disks.length; i++)
  disks.push('"' + params.disks[i] + '"');

run('set drilldowns=' + disks.join(', '));
run('commit');

for (i = 0; i < params.disks.length; i++) {
  run('dataset');
  run('set name="io.bytes[disk=' +
    params.disks[i] + ']"');
  run('commit');
}
}
} ];

var workflow = {
  name: 'Disk drilldown',
  description: 'Creates a worksheet that drills down on system, ' +
    'cache, or log devices',
  parameters: {
    type: {
      label: 'Create a new worksheet drilling down on',
      type: 'ChooseOne',
      options: [ 'cache', 'log', 'system' ],
      optionlabels: [ 'Cache', 'Log', 'System' ]
    },
    overwrite: {
      label: 'Overwrite the worksheet if it exists',
      type: 'Boolean'
    }
  },
  execute: function (params) { return (steps); }
};
```

Carga y ejecución de flujos de trabajo con la BUI

Puede cargar un flujo de trabajo en el dispositivo haciendo clic en el ícono de signo más . Puede ejecutar un flujo de trabajo haciendo clic en la fila que especifica el flujo de trabajo, o pasando el cursor sobre la fila de flujo de trabajo y haciendo clic en el ícono de ejecución . También puede editar o suprimir un flujo de trabajo pasando el cursor sobre la fila de flujo de trabajo y haciendo clic en el ícono adecuado.

FIGURA 32 Flujos de trabajo que se ven en la BUI

Workflows Total: 5		
NAME ▲	DESCRIPTION	VERSION
Clear locks	Clear locks held on behalf of an NFS client	1.0.0
Configure for Oracle Enterprise Manager Monitoring	Sets up environment to be monitored by Oracle Enterprise Manager	1.1
Configure for Oracle Solaris Cluster NFS	Sets up environment for Oracle Solaris Cluster NFS	1.0.0  
Unconfigure Oracle Enterprise Manager Monitoring	Removes the artifacts from the appliance used by Oracle Enterprise Manager	1.0
Unconfigure Oracle Solaris Cluster NFS	Removes the artifacts from the appliance used by Oracle Solaris Cluster NFS	1.0.0

Para ver la lista de flujos de trabajo ampliada, mantenga presionada la tecla Mayús y haga clic en el ícono del signo más . Para ocultar la lista ampliada, mantenga presionada la tecla Shift y haga clic en el ícono del signo más  nuevamente.

▼ Descarga de flujos de trabajo mediante el uso de la CLI

1. Los flujos de trabajo se descargan al dispositivo mediante el comando `download`; el mecanismo es similar al utilizado para las actualizaciones de software:

```
hostname:maintenance workflows> download
hostname:maintenance workflows download (uncommitted)> get
      url = (unset)
      user = (unset)
      password = (unset)
```

2. Debe configurar la propiedad "url" con una dirección URL válida para el flujo de trabajo. Puede ser una dirección local de la red o una dirección de Internet. La URL puede ser HTTP (que comienza con "http://") o FTP (que comienza con "ftp://"). Si se necesita autenticación del usuario, puede ser parte de la dirección URL (por ejemplo, "ftp://myusername:mypasswd@myserver/export/foo") o se puede excluir el nombre de usuario y la contraseña de la dirección URL, y configurar las propiedades de usuario y contraseña.

```
hostname:maintenance workflows download (uncommitted)> set url=ftp://foo/example1.akwf
      url = ftp://foo/example1.akwf
hostname:maintenance workflows download (uncommitted)> set user=bmc
      user = bmc
hostname:maintenance workflows download (uncommitted)> set password
Enter password:
      password = (set)
```

```
hostname:maintenance workflows download (uncommitted)> commit
Transferred 138 of 138 (100%) ... done
```

▼ Mostrar flujos de trabajo mediante el uso de la CLI

1. Para ver una lista de los flujos de trabajo, use el comando `list` desde el contexto `maintenance workflows`:

```
hostname:maintenance workflows> list
WORKFLOW  NAME                               OWNER SETID ORIGIN      VERSION
workflow-018 Check metaslab_unload_delay    root  false Oracle ZFSSA  1.0
workflow-019 Check metaslab_unload_timeout  root  false Oracle ZFSSA  1.0
workflow-020 Example 9                      root  true  <local>      1.0
workflow-021 Set DNLC size and ncsiz        root  false Data and App  2.0
workflow-022 Stop Existing SSH Sessions     root  false <local>      0.2
```

2. Para seleccionar un flujo de trabajo, use el comando `select`:

```
hostname:maintenance workflows> select workflow-018
hostname:maintenance workflow-018>
```

3. Para obtener las propiedades de un flujo de trabajo, use el comando `get` desde el contexto del flujo de trabajo seleccionado:

```
hostname:maintenance workflow-018> get
name = Check metaslab_unload_delay
description = Check the value of the metaslab_unload_delay property
uuid = uuid
checksum = checksum
installdate = 2019-5-8 20:54:33
owner = root
origin = Oracle ZFSSA
setid = false
alert = false
version = 1.0
scheduled = true
```

▼ Ejecución de flujos de trabajo con la CLI

1. Para ejecutar un flujo de trabajo, use el comando `run` desde el contexto del flujo de trabajo seleccionado.

```
hostname:maintenance workflow-000> run
```

2. El contexto se convertirá en un contexto cautivo en el que se deben especificar parámetros para un flujo de trabajo que tiene parámetros:

```
hostname:maintenance workflow-000> run
hostname:maintenance workflow-000 run(uncommitted)> get
type = (unset)
overwrite = (unset)
```

Para un flujo de trabajo que no tiene parámetros, puede confirmar directamente después de introducir el contexto cautivo:

```
hostname:maintenance workflow-000> run
hostname:maintenance workflow-000 run(uncommitted)> commit
hello world!
```

3. **Todo intento de confirmar la ejecución del flujo de trabajo sin antes haber definido los parámetros requeridos generará un fallo explícito:**

```
hostname:maintenance workflow-000 run(uncommitted)> commit
error: cannot execute workflow without setting property "type"
```

4. **Para ejecutar el flujo de trabajo, defina los parámetros especificados y, a continuación, use el comando `commit`:**

```
hostname:maintenance workflow-000 run (uncommitted)> set type=system
type = system
hostname:maintenance workflow-000 run (uncommitted)> set overwrite=true
overwrite = true
hostname:maintenance workflow-000 run (uncommitted)> commit
```

5. **Si el flujo de trabajo tiene pasos especificados, estos se mostrarán mediante la CLI, por ejemplo:**

```
hostname:maintenance workflow-000 run (uncommitted)> commit
Checking for existing worksheet ... done
Finding disks of specified type ... done
Creating worksheet ... done
```

▼ Auditoría de flujos de trabajo mediante el uso de la CLI

Todos los flujos de trabajo tienen una propiedad de total de control calculada por el sistema. Este total de control es el resumen de SHA-256 del contenido del flujo de trabajo. Para determinar si un flujo de trabajo ha cambiado, compare el total de control del flujo de trabajo actual con el previo.

- **Para obtener la propiedad de total de control de un flujo de trabajo, use el comando `get checksum` desde el contexto `maintenance workflows`:**

```
hostname:maintenance workflows> select workflow-001
hostname:maintenance workflow-001> get checksum
checksum = 15f4188643d7add37b5ad8bda6d9b4e7210f1cd890a73df176382e800aec
```


Integración

Oracle ZFS Storage Appliance está diseñado para integrarse sin problemas con otros productos de Oracle y, también, con entornos de terceros y virtualizados. El dispositivo ofrece un conjunto completo de protocolos de datos para comunicarse con una amplia variedad de hosts de aplicaciones. Si desea mejorar el rendimiento de la aplicación, proporcionar compatibilidad con copia de seguridad efectiva o integrarse mejor con el entorno de su aplicación, y gestionar y supervisar dispositivos de almacenamiento, consulte estos recursos para obtener una lista de plugins descargables, resúmenes técnicos y documentación en la que se detallan las mejores prácticas y recomendaciones de configuración y despliegue para maximizar el rendimiento:

- [Descargas de Oracle ZFS Storage Appliance Plug-in](#)
- [Documentación de almacenamiento NAS](#)

Configuración de Oracle ZFS Storage Appliance para clientes de Oracle Database

El dispositivo ofrece diversas funciones exclusivas diseñadas para su integración con clientes de Oracle Database, que incluyen compresión de columnas híbridas (HCC) y Oracle Intelligent Storage Protocol (OISP).

Para activar estas funciones, el servicio SNMP de Oracle ZFS Storage Appliance debe estar configurado para permitir consultas SNMP mediante clientes de bases de datos. El cliente usa este mecanismo para identificar un dispositivo de almacenamiento como un dispositivo Oracle ZFS Storage Appliance. Para especificar el nombre de host o la dirección IP del cliente de base de datos como el destino de captura, consulte [Configuración de SNMP para proporcionar información de estado del dispositivo \(BUI\) \[465\]](#).

Para comprobar que el servicio SNMP del dispositivo esté configurado correctamente, ejecute el comando `snmpget(1)` del sistema cliente y reemplace `<host>` con el nombre o la dirección IP del dispositivo.

```
-bash-4.1$ snmpget -v1 -c public <host> .1.3.6.1.4.1.42.2.225.1.4.2.0
SNMPv2-SMI::enterprises.42.2.225.1.4.2.0 = STRING: "Oracle ZFS Storage Appliance"
```

Protocolo de almacenamiento inteligente de Oracle

Oracle Intelligent Storage Protocol (OISP) permite al cliente de NFS directo (dNFS) de Oracle codificar y transferir atributos asociados con solicitudes de E/S al dispositivo. Estos atributos contienen, por ejemplo, información acerca del tipo de archivo de base de datos al que está dirigida la solicitud de E/S, el tamaño de registro del archivo, si los datos de E/S se deben almacenar en caché y la identidad de la base de datos que emite la solicitud de E/S.

El dispositivo decodifica los atributos y los utiliza para simplificar la configuración de la base de datos, mejorar el rendimiento de la base de datos y permitir observar el origen de las cargas de trabajo de E/S generadas por clientes de base de datos.

Tamaño de registro de base de datos

El cliente dNFS de Oracle puede transferir el tamaño de registro óptimo en función del tipo de archivo para cada solicitud de E/S. Si se transfiere un tamaño de registro, se sustituye el valor de la propiedad de tamaño de registro de la base de datos en el recurso compartido o el proyecto. El tamaño de registro solamente se puede definir para los archivos recién creados. Si ya existe un archivo, el tamaño de registro no se modifica.

Indicación de desviación de escritura síncrona

El cliente dNFS de Oracle puede transferir una "indicación" de desviación de escritura asociada con las solicitudes de E/S de escritura para indicar al dispositivo que trate las solicitudes de E/S como sensibles a la latencia u orientadas al rendimiento. Si se transfiere la indicación, se sustituye el valor de la propiedad de desviación de escritura síncrona en el recurso compartido o el proyecto.

Desglose de análisis por nombre de base de datos

El cliente dNFS 12c o posterior de Oracle Database puede transferir la identificación de la base de datos (SID) o la base de datos de contenedor y la base de datos conectable (SID:SID) responsable de la emisión de las solicitudes de E/S. Los análisis del dispositivo Oracle ZFS Storage Appliance pueden mostrar las estadísticas de E/S desglosadas por nombre de SID de la base de datos; para ello, se debe seleccionar la opción para desglosar o aumentar el nivel de detalle por ID de aplicación.

Si Oracle ZFS Storage Appliance tiene el firmware OS8.7 y posterior, se puede mostrar un análisis adicional de bases de datos de OISP. Las operaciones de OISP por cliente, nombre de archivo, nombre de base de datos, tipo de archivo de base de datos, función de base de datos, recurso compartido, proyecto, tamaño de archivo, desplazamiento y latencia están disponibles.

Almacenamiento de indicaciones en caché

El cliente dNFS Oracle Database 12.2 o posterior incluye el almacenamiento en caché de indicaciones en solicitudes de E/S. El almacenamiento negativo en caché de indicaciones se incluye en las solicitudes de E/S que no esperan volver a hacer referencia pronto a los datos leídos o escritos, como la lectura de bloques de archivos de datos y porciones de copia de seguridad escritas como parte de una copia de seguridad de Oracle Recovery Manager (Oracle RMAN). Esto ayuda al dispositivo a hacer el mejor uso posible de la memoria disponible al almacenar en caché datos del sistema de archivos. Las principales operaciones con almacenamiento negativo en caché son: operaciones de lectura y escritura de Oracle RMAN, creación de archivos redo log y archivos de datos de bases de datos de Oracle, y operaciones de lectura y escritura de Oracle Database Archiver.

Protocolos y clientes compatibles con OISP

- Protocolos: NFSv4.0 y NFSv4.1
- Clientes: Cliente de NFS directo (dNFS) de Oracle Database

