Guía de administración de Oracle® ZFS Storage Appliance

Referencia: E54236-02
Junio de 2014

Contenido

Uso de esta documentación

- **Descripción general**: describe cómo administrar Oracle ZFS Storage Appliance.
- **Destinatarios**: técnicos, administradores de sistemas y proveedores de servicios autorizados.
- **Conocimiento necesario**: experiencia práctica con Oracle ZFS Storage Appliance.

Biblioteca de documentación del producto

Visite la biblioteca de documentación del producto http://www.oracle.com/goto/ZFSStorage/docs, para ver la biblioteca de documentación de Oracle ZFS Storage Appliance.

Para consultar documentación relacionada, incluidas las notas del producto, visite http://www.oracle.com/technetwork/server-storage/sun-unified-storage/overview/index.html y haga clic en la ficha de documentación. Si desea obtener información reciente y sobre problemas conocidos de este producto, visite My Oracle Support en http://support.oracle.com.

Acceso a la asistencia técnica de Oracle

Los clientes de Oracle disponen de asistencia a través de Internet en el portal 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 es una persona con discapacidad auditiva.

Comentarios

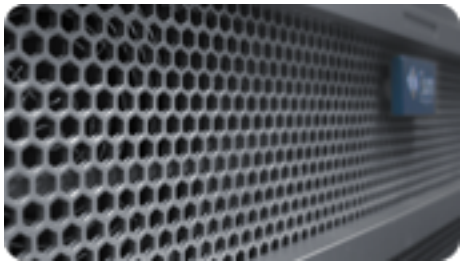
Envíenos comentarios acerca de esta documentación mediante http://www.oracle.com/goto/docfeedback.

♦ ♦ ♦ CAPÍTULO 1

Descripción general de Oracle ZFS Storage Appliance

La familia de productos Oracle ZFS Storage Appliance (ZFSSA) 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.

Funciones clave de ZFSSA



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

- "Análisis" de "Guía de análisis de Oracle ZFS Storage Appliance ", 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 "Vista de hardware" de "Manual de servicio del cliente de Oracle ZFS Storage Appliance ".

- Compatibilidad con una variedad de “Vista de hardware” de “Manual de servicio del cliente de Oracle ZFS Storage Appliance ”.

Protocolos admitidos

Los dispositivos ZFSSA admiten una variedad de protocolos de cliente estándar del sector, entre los que se incluyen los siguientes:

- “SMB” [214]
- “NFS” [208]
- “HTTP and HTTPS” [234]
- “WebDAV” [234]
- “iSCSI” [213]
- “Canal de fibra de SAN” [116]
- “SRP” [134]
- Configuración de destinos iSER [130]
- “FTP” [232]
- “SFTP” [246]

Servicios de datos de dispositivos ZFSSA

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

AVISO DE LICENCIAS: *Las funciones de replicación remota y clonación se pueden evaluar sin cargo, pero para poder usarlas en producción se debe adquirir una licencia independiente por separado. Después del período de evaluación, se debe adquirir la licencia correspondiente para estas funciones o se las debe desactivar. Oracle se reserva el derecho de realizar auditorías en cualquier momento para controlar la existencia de las licencias necesarias. Para obtener información detallada, consulte "Acuerdo de licencia de software (SLA) de Oracle y derecho de sistemas de hardware con opciones de software integrado".*

- Capítulo 5, Configuración del almacenamiento RAID-Z (RAID-5 y RAID-6), reflejada y segmentada
- “Recursos compartidos: instantáneas” [352] ilimitados de solo lectura y de lectura y escritura, con programación de instantáneas
- “Data deduplication” [327]
- Una “data compression” [327] incorporada

- Capítulo 13, Replicación de datos para recuperación ante desastres
- Capítulo 10, Configuración de cluster activa-activa para alta disponibilidad
- Aprovisionamiento fino de unidades “LUN” “iSCSI” [213]
- “Virus scanning and quarantine” [251]
- “NDMP backup and restore” [236]

Disponibilidad de datos

Para maximizar la disponibilidad de los datos en producción, los dispositivos ZFSSA incluyen una arquitectura completa de extremo a extremo para proteger la integridad de los datos, con redundancias en cada nivel de la pila. Las funciones clave incluyen:

- 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
- Capítulo 10, Configuración de cluster activa-activa para alta disponibilidad
- Capítulo 4, Configuración de red para protección contra fallos en la red
- Rutas múltiples de E/S entre el controlador y los estantes de discos
- Reinicio integrado de software en todos los Capítulo 11, Servicios del dispositivo ZFSSA del sistema
- “Phone-Home” [281] de telemetría para todos los problemas de software y hardware
- Gestión fuera de banda de cada sistema para control de encendido remoto y acceso a la consola

Configuración de dispositivos ZFSSA

Para configurar un dispositivo ZFSSA, use las siguientes secciones:

- Capítulo 3, Configuración inicial: configuración inicial
- Capítulo 4, Configuración de red: redes
- Capítulo 11, Servicios del dispositivo ZFSSA: servicios de datos
- Capítulo 6, Configuración de red de área de almacenamiento: configuración de red de área de almacenamiento
- Capítulo 10, Configuración de cluster: agrupación en clusters
- Capítulo 7, Configuración de usuario: cuentas de usuario y control de acceso
- Capítulo 7, Configuración de usuario: preferencias de usuario

- Capítulo 9, Configuración de alertas: alertas personalizadas
- Capítulo 5, Configuración del almacenamiento: reconfiguración de dispositivos de almacenamiento
- Capítulo 12, Recursos compartidos, proyectos y esquemas

Interfaz de usuario basada en explorador (BUI)

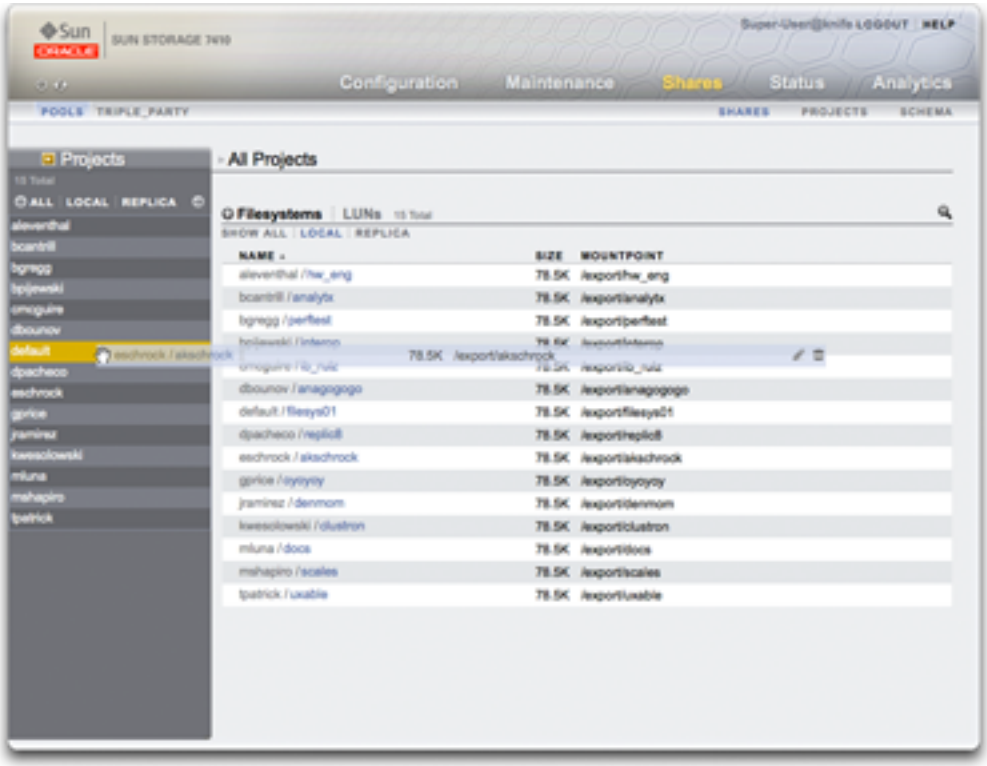
La interfaz de usuario basada en explorador (BUI) del dispositivo ZFSSA es la herramienta gráfica para la administración del dispositivo. La BUI proporciona un entorno intuitivo para las tareas de administración, la visualización de conceptos y el análisis de datos de rendimiento. La BUI proporciona 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).

- “Main Window” [25]: descripción general de los elementos y el diseño de la BUI
- “Uso general” [31]: referencia de íconos
- “Exploradores admitidos” [35]: exploradores admitidos

Ventana principal



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

Cabecera

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.

Alertas

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 “Dashboard” [48] o el log completo disponible en la pantalla “Logs” de “Manual de servicio del cliente de Oracle ZFS Storage Appliance ”.

Navegación

Use los enlaces de navegación principal para alternar entre las áreas de Capítulo 4, Configuración de red, “Mantenimiento” de “Manual de servicio del cliente de Oracle ZFS Storage Appliance ”, Capítulo 12, Recursos compartidos, proyectos y esquemas, Capítulo 2, Estado y “Análisis” de “Guía de análisis de Oracle ZFS Storage Appliance ” de la BUI.

Use los enlaces de navegación secundaria para acceder a las características y funciones de cada área.

Anotación de sesión

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. Consulte Capítulo 7, Configuración de usuario para obtener información detallada acerca de las anotaciones de sesión.

Barra de título

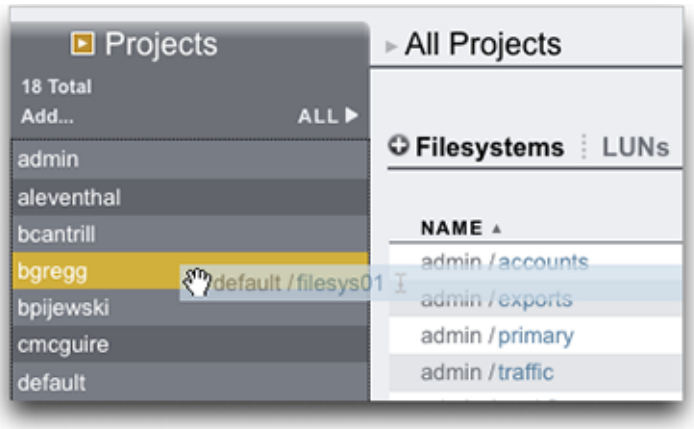
La barra de título aparece debajo de la cabecera y proporciona la función de navegación local y otras funciones que varían según la vista actual.

Por ejemplo, la barra de título del servicio de 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 Propiedades, Reglas y Logs del servicio de asignación de identidad
- Botón para aplicar cambios de configuración hechos en la pantalla actual
- Botón para deshacer los cambios de configuración aplicados en la pantalla actual

Paneles laterales y títulos de menú

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 .



Paneles laterales y títulos de menú de la ventana principal

Agregación de proyectos

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

Movimiento de recursos compartidos

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.

Nombre del objeto

Para cambiar el nombre de un recurso compartido, haga clic en el ícono de cambio de nombre en la fila resaltada de la tabla del recurso compartido.

Control no estándar de la BUI

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

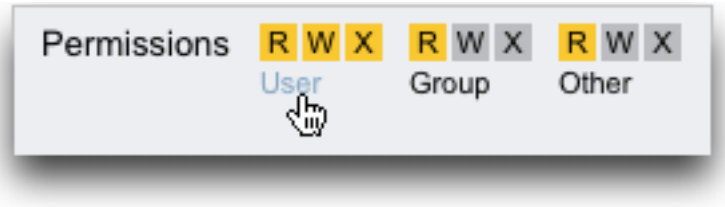
TABLA 1-1 Excepciones de pantalla web clave

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 Apply (Aplicar).
Deshacer cambios guardados	Haga clic en el botón Deshacer.
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).
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.

Resumen de controles de la BUI	
Cambiar el nombre de un elemento	Haga clic en el ícono pata 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.

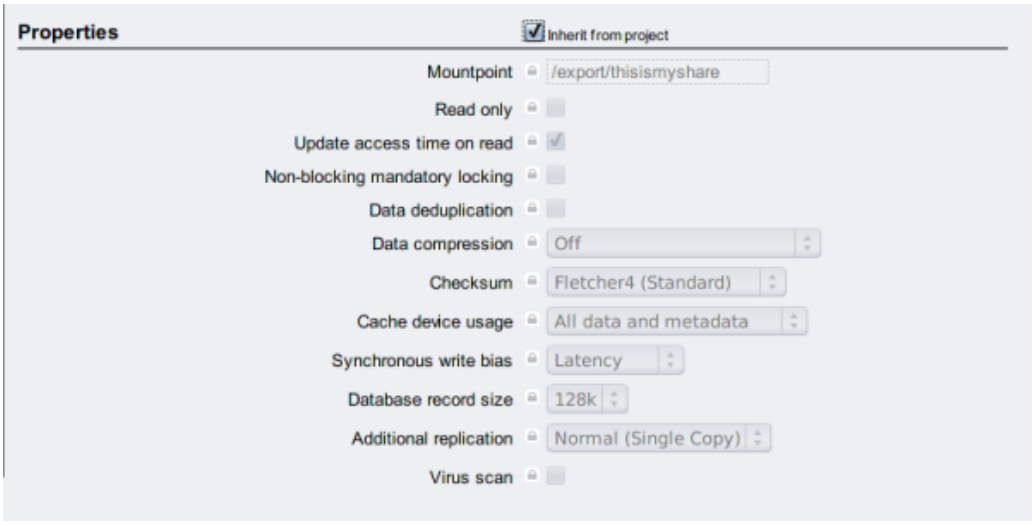
Permisos

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



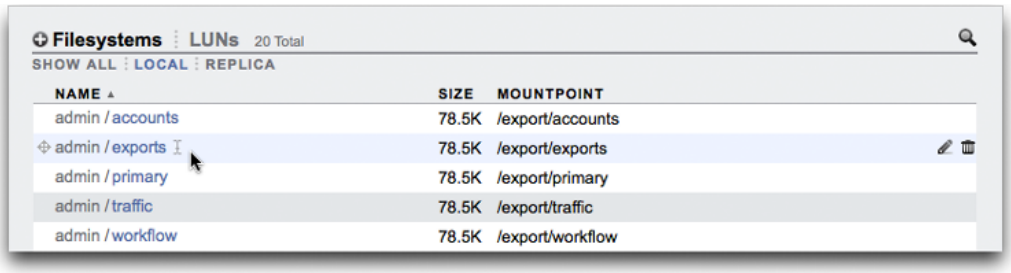
Edición de las propiedades de recursos compartidos

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



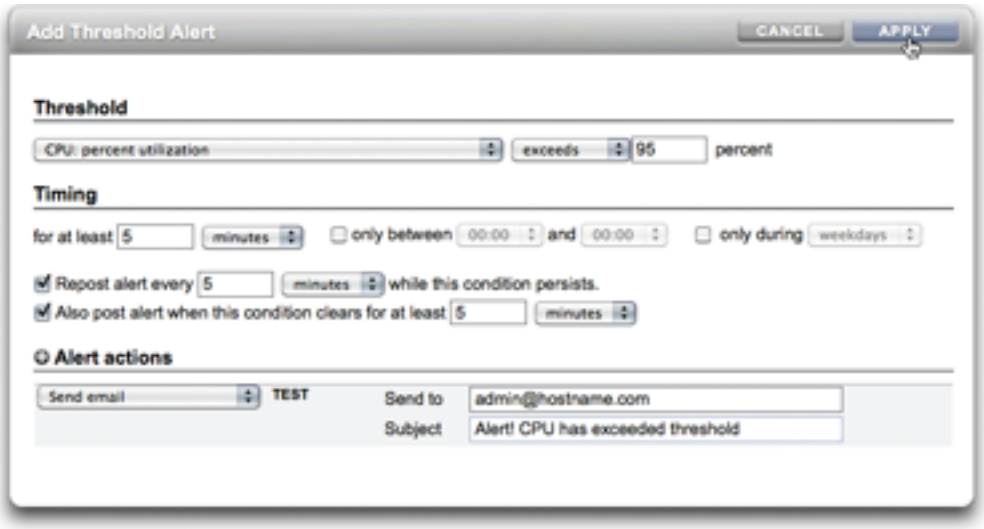
Visualización de controles de elementos de lista

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



Cuadros de diálogo modales

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.



Uso general

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 ayuda relacionada. En las siguientes tablas, se proporciona una clave de las convenciones de la interfaz de usuario.

Estado

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

TABLA 1-2 Indicadores de estado

Ícono	Descripción	Ícono	Descripción
	activado		advertencia
	apagado		desactivado

Uso básico

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

TABLA 1-3 Íconos de la BUI

Ícono*		Descripción	Ícono*		Descripción
--		cambiar nombre (editar texto)	--		cortar
--		mover	--		clonar
		editar	--		revertir
		destruir	--		encender dispositivo
		agregar	--		aplicar
		eliminar	--		revertir
		cancelar/cerrar	--		info
--		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.*

Red

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

TABLA 1-4 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 (partición IB)
	VLAN de enlace de datos de red		
	agregación de enlaces de datos de red		
	VLAN de agregación de enlaces de datos de red		

Umbrales de 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 la “configuración” [57].

TABLA 1-5 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

Analíticas

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 1-6 Íconos de la barra de herramientas de análisis

Ícono	Descripción	Ícono	Descripción
	atrás		mostrar mínimo
	adelantar		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 conjunto de datos
			enviar hoja de trabajo con paquete de asistencia

Asignación de identidad

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

TABLA 1-7 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.*

Íconos varios

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

TABLA 1-8 Íconos varios

Ícono	Descripción	Ícono	Descripción
	permitir		SAS
	denegar		puerto SAS
	agrupación de almacenamiento		

Exploradores admitidos

En esta sección, se define la compatibilidad de los exploradores con la BUI. Para obtener los mejores resultados, use algún explorador de nivel 1.

Nivel 1

El software de la BUI está diseñado para poder utilizarse con todas sus funciones en los siguientes exploradores de nivel 1:

- Firefox 3.x o posterior
- Internet Explorer 7 o posterior
- Safari 3.1 o posterior

- Google Chrome (Stable)
- WebKit 525.13 o posterior

Nivel 2

En los exploradores del nivel 2, los elementos de la BUI pueden aparecer con alguna imperfección visual y algunas de las funcionen 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 de nivel 2:

- Firefox 2.x
- Mozilla 1.7 en Solaris 10
- Opera 9

Exploradores no admitidos

Internet Explorer 6 y las versiones anteriores a ella no son compatibles, porque se sabe que tienen problemas y no permiten completar el inicio de sesión.

Interfaz de línea de comandos (CLI)

La CLI está diseñada para reflejar las capacidades de la BUI y proporcionar a la vez un entorno de secuencias de comandos 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” de “Guía de instalación de Oracle ZFS Storage Appliance ” o “SSH” [297]. Hay varias situaciones en las que es preferible interaccionar 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” de “Guía de instalación de Oracle ZFS Storage Appliance ”, 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.

- 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".
-

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:

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

Inicio de sesión en la CLI

Para iniciar sesión de manera remota mediante la CLI, use un cliente `ssh`. Si no tiene Capítulo 7, Configuración de usuario para administrar el dispositivo, deberá iniciar sesión como usuario `root`. Cuando inicie sesión, la CLI mostrará un indicador, que es el nombre del host seguido por dos puntos y por el signo mayor que:

```
% ssh root@dory
Password:
Last login: Mon Oct 13 15:43:05 2009 from kiowa.sf.fishpo
dory:>
```

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.

Contexto raíz

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 de Capítulo 4, Configuración de red del explorador están disponibles en el contexto `configuration` de la CLI. Para tener acceso, desde el contexto raíz, escriba directamente lo siguiente:

```
dory:> configuration
dory: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.

Contextos secundarios

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

```
dory: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 de Capítulo 6, Configuración de red de área de almacenamiento del explorador, que incluye Capítulo 4, Configuración de red, Capítulo 11, Servicios del dispositivo ZFSSA y Capítulo 7, Configuración de usuario, “Preferences”Capítulo 8, Configuración de preferencias de dispositivos ZFSSA, etc. Para seleccionar uno de estos contextos secundarios, escriba el nombre correspondiente:

```
dory:configuration> preferences
dory: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:

```
dory:> configuration preferences
dory:configuration preferences>
```

Contextos secundarios dinámicos

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. Para navegar a estos contextos, use el comando `select`, seguido del nombre del contexto dinámico. 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.

```
dory:> configuration users
dory: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`:

```
dory:configuration users> select bmc
dory:configuration users bmc>
```

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

```
dory:maintenance logs system> select module=reboot
dory:maintenance logs system entry-034> show
Properties:
  timestamp = 2010-8-14 06:24:41
     module = reboot
   priority = crit
       text = initiated by root on /dev/console syslogd: going down on signal 15
```

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

```
dory:> configuration users select bmc
dory:configuration users bmc>
```

Último contexto

Use el comando `last` para navegar hasta un contexto creado o seleccionado con anterioridad. Este comando actualmente está implementado sólo en el contexto de acciones de replicación.

En el siguiente ejemplo se crea una acción de replicación y, a continuación, se usan los comandos `last` y `get id` para recuperar el identificador de la acción de replicación. Luego se selecciona una acción diferente y se usan los comandos `last` y `get id` para recuperar el identificador de la acción de replicación más recientemente visitada.

```
dory:shares p1/share replication> list
```

```
           TARGET          STATUS     NEXT
action-000  oakmeal         idle       Sync now
action-001  dory            idle       Sync now
dory:shares p1/share replication> create
dory:shares p1/share action (uncommitted)> set target=dory
                       target = dory (uncommitted)
dory:shares p1/share action (uncommitted)> set pool=p0
                          pool = p0 (uncommitted)
dory:shares p1/share action (uncommitted)> commit
dory:shares p1/share replication> last
dory:shares p1/share action-002> get id
                             id = 7034367a-d4d8-e26f-fa93-c3b454e3b595
dory:shares p1/share action-002> done
dory:shares p1/share replication> select action-000
dory:shares p1/share action-000> get id
                             id = 9895d9f4-7b23-ebe1-faf2-d85a581e3dff
dory:shares p1/share action-000> done
dory:shares p1/share replication> last get id
                             id = 9895d9f4-7b23-ebe1-faf2-d85a581e3dff
dory:shares p1/share replication>
```

Regreso a un contexto previo

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

```
dory:configuration> done
dory:>
```

Tenga en cuenta que de esta manera se regresa al contexto previo, que no es necesariamente el contexto principal:

```
dory:> configuration users select bmc
dory:configuration users bmc> done
dory:>
```

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

```
dory:> configuration
dory:configuration> users
dory:configuration users> select bmc
dory:configuration users bmc> done
dory:configuration users> done
dory:configuration> done
dory:>
```

Navegación a un contexto principal

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:

```
dory:> configuration users select bmc
```

```
dory:configuration users bmc> cd ..
dory:configuration users>
```

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

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

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

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

Contextos y uso de la finalización con tabulación

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 sólo quince pulsaciones de teclas, en lugar de las treinta y un veces que se necesitarían si no se usara la finalización con tabulación:

```
dory:> config<tab>
dory:> configuration u<tab>
dory:> configuration users se<tab>
dory:> configuration users select <tab>
bmc   root
dory:> configuration users select b<tab>
dory:> configuration users select bmc<enter>
dory:configuration users bmc>
```

Ejecución de comandos específicos de un contexto

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`:

```
dory: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:

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

Contextos no confirmados

Al crear una nueva entidad en el sistema, el contexto asociado con ella normalmente se crea en un estado *no confirmado*. Por ejemplo, ejecute el comando `create` desde el contexto `configuration alerts threshold` para crear una Capítulo 9, Configuración de alertas:

```
dory:> configuration alerts thresholds create
dory: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:

```
dory: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:

```
dory:configuration alerts threshold (uncommitted)> commit
error: missing value for property "statname"
```

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

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

Propiedades

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:

```
dory: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
```

Obtención de propiedades

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:

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

Obtención del valor de una única propiedad

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

```
dory:configuration preferences> get login_screen
                 login_screen = status/dashboard
```

Finalización con tabulación

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” [213]:

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

Establecimiento de propiedades

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`":

```
dory: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.

Confirmación de un valor definido para una propiedad

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`:

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

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

Configuración de un valor de propiedad con confirmación implícita

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 se regrese el control al contexto de origen. Por ejemplo:

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

Configuración de una propiedad con una lista de valores

Algunas propiedades tienen listas de valores. Para estas propiedades, los elementos de la lista se deben separar con comas. Por ejemplo, la propiedad `servers` de “NTP” [278] se puede configurar con una lista de servidores NTP:

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

Configuración de una propiedad con un valor que contiene caracteres especiales

Si el valor de una propiedad contiene una coma, un signo igual, comillas o un espacio, todo el valor se debe indicar entre comillas. Por ejemplo, para configurar la propiedad `sharenfs` del proyecto predeterminado para que sea de solo lectura pero permita acceso de lectura y escritura al host "kiowa". Para obtener información, consulte el Capítulo 12, Recursos compartidos, proyectos y esquemas.

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

Propiedades invariables

Algunas propiedades son inmutables; es posible obtener sus valores, pero no se los 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 información, consulte el Capítulo 12, Recursos compartidos, proyectos y esquemas.

```
dory:> shares select default
dory:shares default> get space_available
               space_available = 1.15T
dory: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:

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

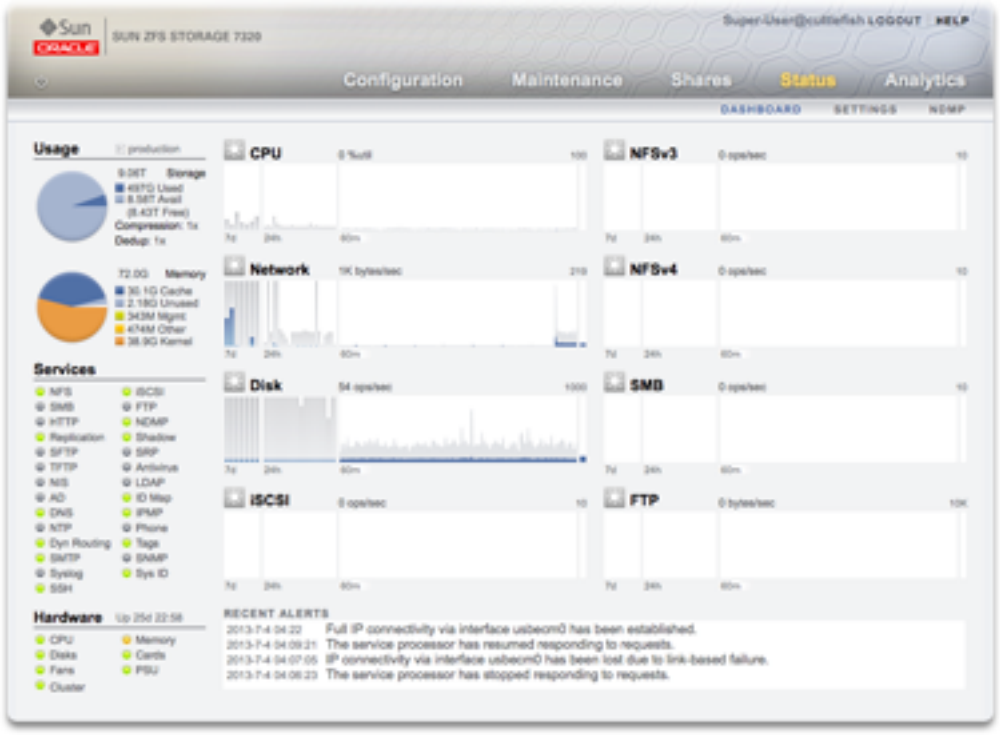
♦ ♦ ♦ CAPÍTULO 2

Estado

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:

- La pantalla “Status (Estado) > Dashboard (Panel de control)” [48] proporciona una vista del almacenamiento, la memoria, los servicios, el hardware, la actividad y las alertas recientes.
- La pantalla “Status (Estado) > Settings (Configuración)” [57] le permite modificar los gráficos que aparecen en el panel de control y personalizar los umbrales asociados con el despliegue de los íconos de clima para cada gráfico del panel de control.
- La pantalla “Status (Estado) > NDMP” [60] proporciona una vista de los dispositivos de NDMP configurados y la actividad reciente de cada sesión de NDMP.

Panel de control



El panel de control resume el estado del dispositivo

Enlaces

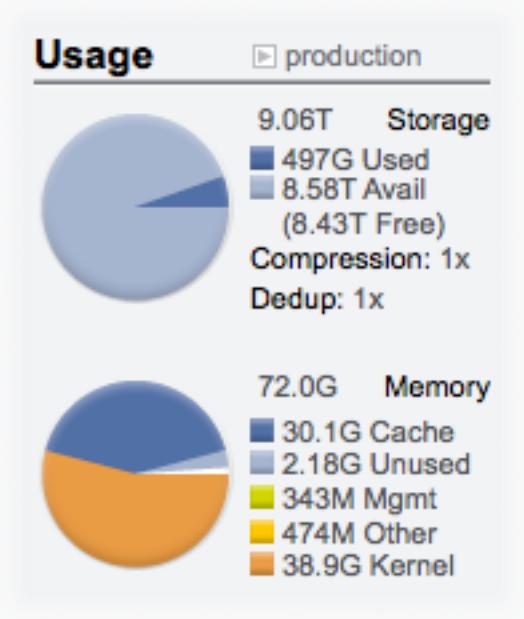
El panel de control de estado proporciona enlaces a todas las pantallas principales de la interfaz de usuario basada en explorador (BUI). En el panel de control, hay más de 100 elementos visibles que enlazan a pantallas asociadas de la BUI; éstos están indicados mediante texto más grueso o resaltado que aparece al pasar el puntero del mouse sobre él. En las siguientes secciones, se describen en detalle las áreas del panel de control.

Uso

El área Usage (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 Usage (uso). Si hay varias agrupaciones configuradas, use la lista desplegable para seleccionar la agrupación que desea visualizar.

FIGURA 2-1 Uso del panel de control de estado



Almacenamiento

La capacidad total de la agrupación se muestra en la parte superior de esta área. En el gráfico circular de almacenamiento, se detalla el espacio utilizado, disponible y libre. Para ir a la pantalla Shares (Recursos compartidos) de la agrupación, haga clic en el gráfico circular Storage (Almacenamiento).

Memoria

La memoria física total del sistema se muestra en la parte superior de esta área. 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 Memory (Memoria).

TABLA 2-1 Resumen de uso de agrupación

Resumen de uso de agrupación	
Usado	Espacio usado por esta agrupación; incluye datos e instantáneas.
Disponible	Cantidad de espacio de disco físico disponible. El espacio disponible para datos de archivos (como se informa en la pantalla Shares [Recursos compartidos]) será menor debido al espacio utilizado por los metadatos del sistema de archivos.
Libre	Cantidad de espacio disponible, dentro de la capacidad LUN, menos el espacio no utilizado reservado para proyectos y recursos compartidos dentro de una agrupación. Proporciona el espacio en disco libre disponible cuando el espacio en disco es asignado por reserva anticipada o cuando se crean LUN.
Compresión	Índice de compresión actual de esta agrupación. Si no está activada la compresión, el índice será 1x.
Anulación de duplicación	Índice de anulación de duplicación de datos actual de esta agrupación. Si no está activada la anulación de duplicación de datos, el índice será 1x.

TABLA 2-2 Resumen de uso de memoria principal

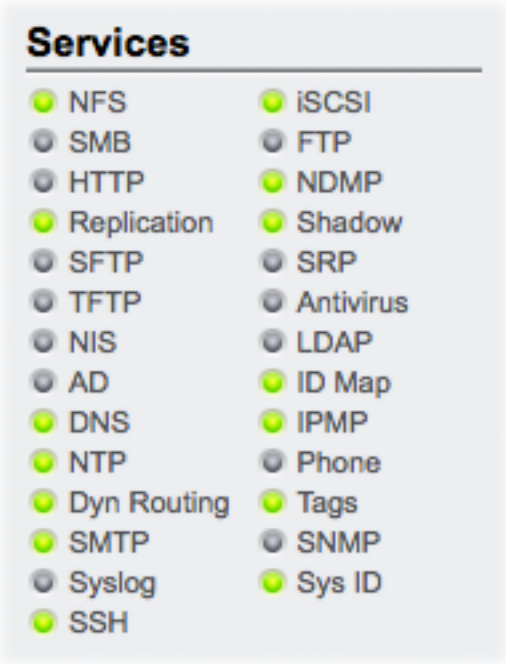
Resumen del uso de la memoria principal (RAM)	
Caché	Bytes en uso por la caché del sistema de archivos para mejorar el rendimiento.
Sin utilizar	Bytes que actualmente no están en uso. Después del inicio, este valor disminuye porque la caché del sistema de archivos utiliza espacio.
Gestión	Bytes en uso 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.

Servicios

Esta área del panel de control muestra el estado de los servicios del dispositivo, con un ícono de una luz para indicar el estado de cada servicio.

FIGURA 2-2 Panel de Control de Servicios



Íconos

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. Consulte la sección de “Uso general” [31] para ver una lista de todos los estados y colores de íconos posibles.

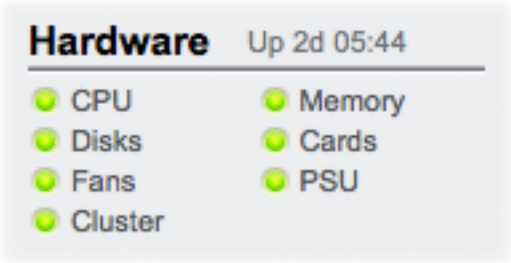
Enlaces

Para ir a la pantalla de configuración asociada, haga clic en el nombre del servicio. La pantalla Properties (Propiedades) aparece con campos que se pueden configurar, íconos de reinicio, activación y desactivación y un enlace a la pantalla Logs asociada del servicio.

Hardware

Esta área del panel de control muestra una descripción general del hardware del dispositivo.

FIGURA 2-3 Panel de control de hardware



Fallos

Si hay un fallo conocido, aparece el ícono de fallo de color ámbar .

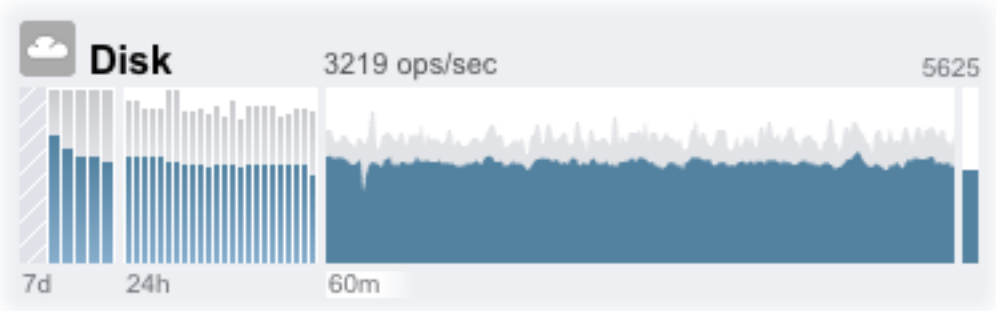
Enlaces

Para ir a la pantalla "Hardware" de "Manual de servicio del cliente de Oracle ZFS Storage Appliance ", en donde se proporciona información detallada del estado del hardware, haga clic en el nombre del componente de hardware.

Actividad

El área de actividad del panel de control muestra de manera predeterminada gráficos de ocho estadísticas de rendimiento. En el ejemplo de esta sección se muestran las operaciones de discos por segundo. El promedio estadístico se representa en azul, mientras que el máximo aparece en gris claro.

FIGURA 2-4 Panel de control de actividad de disco



Para ir a la hoja de trabajo de "Análisis" de "Guía de análisis de Oracle ZFS Storage Appliance " 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 "Status Settings" [57].

Gráficos

TABLA 2-3 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.

Media

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.

Escala vertical

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. De forma predeterminada, 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.

Clima

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” de “Guía de análisis de Oracle ZFS Storage Appliance ” para interpretar correctamente la información sobre el rendimiento del sistema.

Alertas recientes

FIGURA 2-5 Alertas recientes

En esta sección, se muestran las últimas cuatro alertas del dispositivo. Haga clic en el cuadro para ir a la pantalla "Logs" de "Manual de servicio del cliente de Oracle ZFS Storage Appliance " para examinar en detalle todas las alertas recientes.

CLI

Hay una versión de texto de la pantalla Status (Estado) > Dashboard (Panel de control) a la que se puede acceder desde la CLI mediante el comando `status dashboard`:

```
cuttlefish:> status dashboard
Storage:
   pool_0:
      Used     497G bytes
      Avail    8.58T bytes
      Free     8.43T bytes
      State          online
      Compression    1x

Memory:
   Cache        30.1G bytes
   Unused       2.18G bytes
   Mgmt         343M bytes
   Other       474M bytes
   Kernel      38.9G bytes

Services:
   ad                disabled             smb             disabled
   dns               online               ftp              disabled
   http              online               identity         online
   idmap             online               ipmp             online
   iscsi             online               ldap             disabled
   ndmp              online               nfs              online
   nis               online               ntp              online
   routing           online               scrk             maintenance
   snmp              online               ssh              online
   tags              online               vscan            online
```

```
Hardware:
   CPU               online                Cards             online
   Disks             faulted               Fans              online
   Memory            online                PSU               online

Activity:
   CPU             1 %util                 Sunny
   Disk           32 ops/sec               Sunny
   iSCSI           0 ops/sec               Sunny
   NDMP            0 bytes/sec             Sunny
   NFSv3           0 ops/sec               Sunny
   NFSv4           0 ops/sec               Sunny
   Network       13K bytes/sec             Sunny
   SMB             0 ops/sec               Sunny

Recent Alerts:
   2013-6-15 07:46: A cluster interconnect link has been restored.
```

Son válidas las descripciones previas de la sección de la “BUI” [48], con las siguientes diferencias:

- Los gráficos de actividad no se presentan en formato de texto (aunque hemos pensado en utilizar AAlib).
- En la CLI, la sección de uso de almacenamiento mostrará los detalles de todas las agrupaciones disponibles, mientras que en la BUI hay espacio para resumir sólo una.

Hay vistas independientes, por ejemplo `status activity show`:

```
caji:> status activity show
Activity:
   CPU            10 %util                 Sunny
   Disk          478 ops/sec               Partly Cloudy
   iSCSI           0 ops/sec               Sunny
   NDMP            0 bytes/sec             Sunny
   NFSv3         681 ops/sec               Partly Cloudy
   NFSv4           0 ops/sec               Sunny
   Network     22.8M bytes/sec             Partly Cloudy
   SMB             0 ops/sec               Sunny
caji:>
```

▼ Ejecución continua del panel de control

Si deja la pantalla del panel de control abierta en un explorador siempre (las 24 horas, los siete días de la semana), puede sufrir problemas con la memoria de 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 "memory" (Memoria).**
3. **Configure browser.cache.memory.enable = false.**

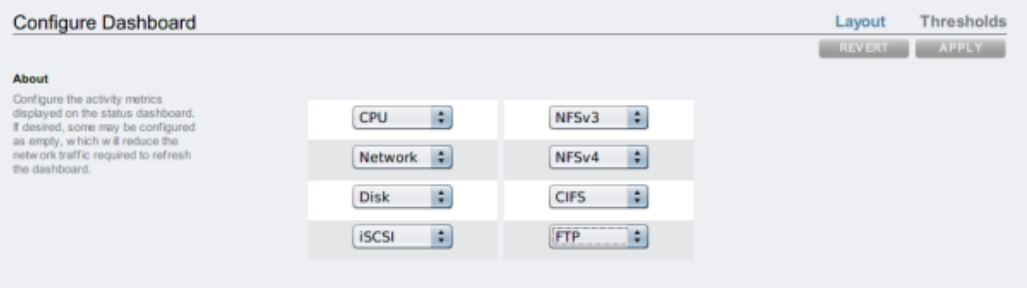
Configuración

Introducción

La pantalla Status (Estado) > Settings (Configuración) le permite personalizar el “panel de control de estado” [48], incluidas las estadísticas que aparecen y los umbrales que indican actividad mediante íconos de clima.

BUI

FIGURA 2-6 Configuración del panel de control



Diseño

Use la ficha Layout (Diseño) para seleccionar los gráficos que aparecen en el área de “actividad del panel de control” [48], como se define en la siguiente tabla.

TABLA 2-4 Configuración de diseño de estado

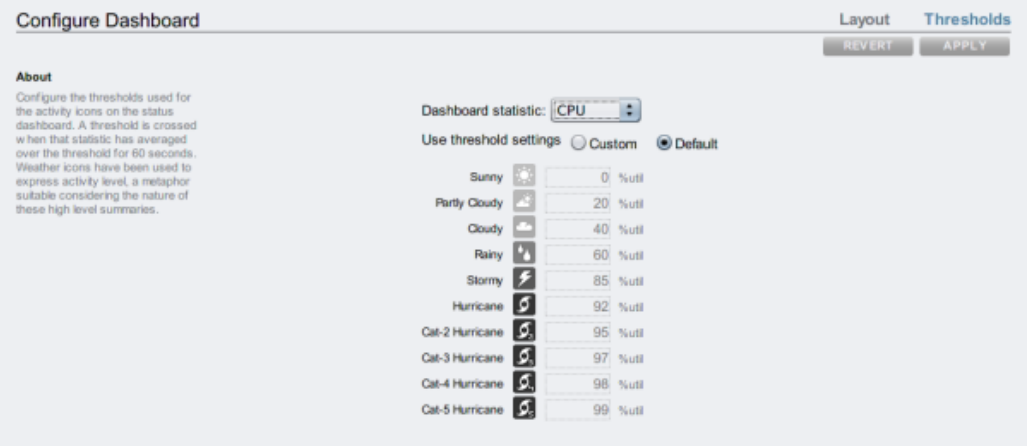
Nombre	Unidades	Descripción
<empty>	-	No se muestra ningún gráfico en esta ubicación.
SMB	operaciones por segundo	Cantidad promedio de operaciones de SMB.
CPU	uso	Cantidad promedio de ciclos que las CPU del dispositivo están activas. Los ciclos de la CPU incluyen los ciclos de espera de la memoria.
Disk	operaciones por segundo	Cantidad promedio de operaciones en los dispositivos de almacenamiento físico.
HTTP	operaciones por segundo	Cantidad promedio de operaciones de HTTP.
iSCSI	operaciones por segundo	Cantidad promedio de operaciones de iSCSI.
FC	operaciones por segundo	Cantidad promedio de operaciones de canal de fibra.
Network	bytes por segundo	Cantidad promedio de bytes por segundo en todas las interfaces de red físicas.
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	operaciones por segundo	Cantidad promedio de operaciones de NFSv4.
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).

Umbrales

Use la pantalla Thresholds (Umbrales) para configurar los íconos de clima de la “actividad del panel de control” [48]. Los valores predeterminados que se proporcionan se basan en cargas de trabajo intensas y tal vez no sean adecuados para su entorno.

FIGURA 2-7 Configuración de actividades del panel de control



El ícono de clima que aparece en el “panel de control” [48] 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%, de forma predeterminada 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.

CLI

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.

Tareas

A continuación se presentan tareas de ejemplo para este tema, con los pasos enumerados.

BUI

▼ Modificación de las estadísticas de las actividades desplegadas

1. **Vaya a la pantalla Status (Estado) > Settings (Configuración) > Layout (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 Apply (Aplicar).**

▼ Modificación de los umbrales de las actividades

1. **Vaya a la pantalla Status (Estado) > Settings (Configuración) > Thresholds (Umbrales).**
2. **Use el menú desplegable para elegir la estadística que desea configurar.**
3. **Haga clic en el botón de radio Custom (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 Apply (Aplicar).**

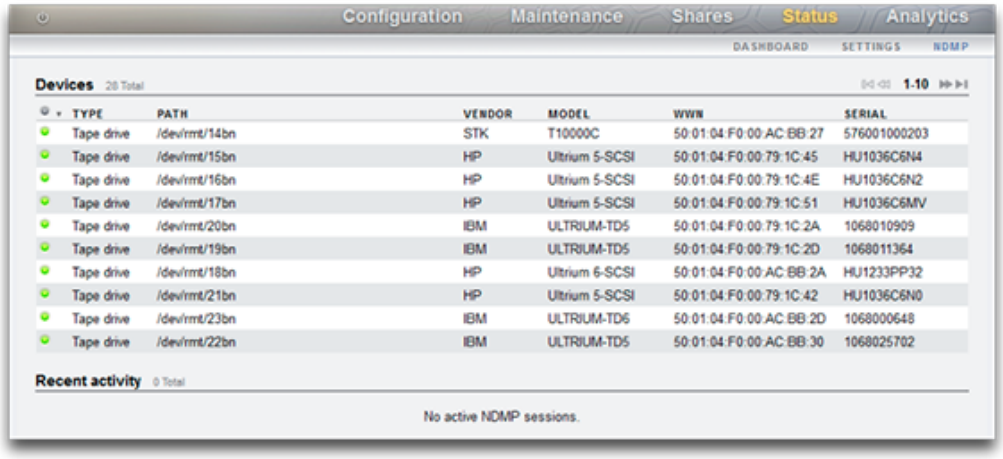
Estado de NDMP

Si el “servicio NDMP” [236] se configuró y está activo, la página Status (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.

Estado de NDMP: BUI

Para cambiar la ordenación de la lista de dispositivos NDMP, haga clic en las cabeceras de la columna Devices (Dispositivos). Para ver los detalles de un dispositivo, haga doble clic en el dispositivo.

FIGURA 2-8 BUI de estado de NDMP



Estado de NDMP: dispositivos

Aquí se muestran los dispositivos de NDMP.

TABLA 2-5 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

Estado de NDMP: actividad reciente

En esta sección, se resume la actividad reciente de NDMP.

TABLA 2-6 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
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	Barra de progreso para esta copia de seguridad.	

Estado de datos de NDMP

El campo 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.
- Connected (Conectado): se estableció la conexión, pero la copia de seguridad o la restauración todavía no comenzó.
- Halted (Detenido): la copia de seguridad o la restauración finalizó correctamente, generó un error o se abortó.
- Listen (Escucha): la operación está esperando a recibir una conexión remota.

Estado de transferencia de NDMP

Este campo muestra el estado del subsistema de dispositivos de NDMP. Ejemplos de dispositivos de cinta:

- Active (Activo): se están leyendo los datos de la cinta o se los está escribiendo en ella.
- Idle (Inactivo): la copia de cinta todavía no comenzó o ya finalizó.
- Paused (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 (Escucha): la operación está esperando a recibir una conexión remota.

Estado de NDMP: CLI

El estado de NDMP no está disponible actualmente desde la CLI.

♦ ♦ ♦ CAPÍTULO 3

Configuración inicial

La configuración inicial incluye las siguientes seis secciones.

- Capítulo 4, Configuración de red
- “DNS” [274]
- “Time” [278]
- Servicios de nombre (“NIS” [254], “LDAP” [256], “Active Directory” [260])
- Capítulo 5, Configuración del almacenamiento
- “Registration & Support” [281]

Requisitos previos

La configuración inicial del sistema se realiza después de encenderlo por primera vez y establecer una conexión, como se documenta en “Installation”.

Nota - Observe que la opción para realizar la configuración inicial de un cluster está disponible solamente en la BUI. Si selecciona esta opción, lea el Capítulo 10, Configuración de cluster antes de comenzar la configuración inicial para obtener información adicional detallada acerca de los pasos requeridos para configurar un cluster correctamente. Preste mucha atención a la sección “Consideraciones de la agrupación en clusters para redes” [176]. De manera alternativa, los dispositivos con capacidad para agruparse en clusters se pueden configurar inicialmente para un funcionamiento independiente mediante el siguiente procedimiento y más adelante se los puede reconfigurar para usarlos como parte de un cluster.

Configuración inicial con la BUI

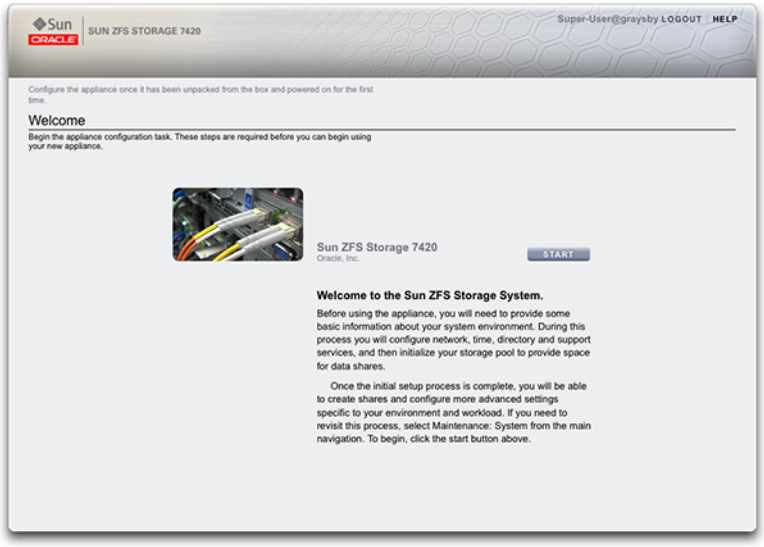
Durante la configuración inicial se configura la conectividad de red, varios servicios de red de clientes y el diseño de las agrupaciones de almacenamiento para el funcionamiento independiente. Cuando se la completa, el dispositivo está listo para el uso pero no tiene ningún

recurso compartido configurado para el acceso de los clientes remotos. Para crear recursos compartidos o repasar la configuración, consulte el Capítulo 12, Recursos compartidos, proyectos y esquemas.

La configuración inicial se puede repetir más adelante; para ello, haga clic en el botón "INITIAL SETUP" (Instalación inicial) de la pantalla “Sistema” de “Manual de servicio del cliente de Oracle ZFS Storage Appliance ” o vaya al contexto `maintenance system setup` en la CLI.

La configuración inicial de la BUI es el método preferido y proporciona una pantalla para cada uno de los pasos de la configuración inicial.

FIGURA 3-1 Página de bienvenida de ZFSSA



▼ Configuración inicial

1. **Para comenzar la configuración inicial, haga clic en Start (Iniciar) en la página Welcome (Bienvenido).**
2. **En cada página, haga clic en Commit (Confirmar) para confirmar los cambios y pasar a la pantalla siguiente.**
3. **Para ir a una pantalla previa, use los botones de las flechas.**

Configuración de puertos de gestión

Todos los controladores independientes deben tener al menos un puerto de la NIC configurado como interfaz de gestión. Seleccione la opción Allow Admin (Permitir administración) en la BUI para activar las conexiones de la BUI en el puerto 215 y las conexiones de la CLI en el puerto 22 de `ssh`.

Todas las instalaciones de cluster deben tener al menos un puerto NIC en cada controlador configurado como interfaz de gestión, como se describió anteriormente. Asimismo, el número de instancia de NIC debe ser único en cada controlador.

Configuración inicial con la CLI

Use la CLI para realizar los pasos de configuración inicial. Cada paso comienza con la impresión de su ayuda, que se puede volver a imprimir mediante el comando `help`. Use el comando `done` para completar cada paso.

Inicie sesión con la contraseña que proporcionó según lo indicado en la sección "Instalación" de "Guía de instalación de Oracle ZFS Storage Appliance ":

```
caji console login: root
Password:
Last login: Sun Oct 19 02:55:31 on console

To setup your system, you will be taken through a series of steps; as the setup
process advances to each step, the help message for that step will be
displayed.

Press any key to begin initial configuration ...
```

En este ejemplo, se comprueba la configuración existente (que se obtuvo del servidor DHCP) y se la acepta mediante el comando `done`. Para personalizar la configuración en este momento, acceda a cada contexto (enlaces de datos, dispositivos e interfaces) y escriba `help` para ver las acciones disponibles para ese contexto. Consulte la sección Capítulo 4, Configuración de red para obtener documentación adicional. Preste mucha atención a la sección "Consideraciones de la agrupación en clusters para redes" [176] si desea configurar una agrupación en clusters.

```
aksh: starting configuration with "net" ...

Configure Networking. Configure the appliance network interfaces. The first
network interface has been configured for you, using the settings you provided
at the serial console.

Subcommands that are valid in this context:

   datalinks            => Manage datalinks
```

```
   devices              => Manage devices

   interfaces           => Manage interfaces

   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 "net"

caji:maintenance system setup net> devices show
Devices:

     DEVICE UP       MAC                     SPEED
       igb0 true     0:14:4f:8d:59:aa        1000 Mbit/s
       igb1 false    0:14:4f:8d:59:ab        0 Mbit/s
       igb2 false    0:14:4f:8d:59:ac        0 Mbit/s
       igb3 false    0:14:4f:8d:59:ad        0 Mbit/s

caji:maintenance system setup net> datalinks show
Datalinks:

   DATALINK CLASS          LINKS       LABEL
       igb0 device         igb0        Untitled Datalink

caji:maintenance system setup net> interfaces show
Interfaces:

  INTERFACE STATE  CLASS LINKS       ADDRS                 LABEL
       igb0 up     ip    igb0        192.168.2.80/22       Untitled Interface

caji:maintenance system setup net> done
```

Consulte la sección “DNS” [274] para obtener documentación adicional sobre DNS.

```
Configure DNS. Configure the Domain Name Service.

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

   abort                => Abort this task (potentially resulting in a
                           misconfigured system)

   done                 => Finish operating on "dns"
```

```
   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.

caji:maintenance system setup dns> show
Properties:
                     <status> = online
                       domain = sun.com
                      servers = 192.168.1.4

caji:maintenance system setup dns> set domain=sf.fishworks.com
                       domain = sf.fishworks.com (uncommitted)
caji:maintenance system setup dns> set servers=192.168.1.5
                      servers = 192.168.1.5 (uncommitted)
caji:maintenance system setup dns> commit
caji:maintenance system setup dns> done
aksh: done with "dns", advancing configuration to "ntp" ...
```

Configure el protocolo de hora de red (NTP) para sincronizar el reloj del dispositivo. Consulte la sección “NTP” [278] para obtener documentación adicional.

```
Configure Time. Configure the Network Time Protocol.

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

   abort                => Abort this task (potentially resulting in a
                           misconfigured system)

   done                 => Finish operating on "ntp"

   enable               => Enable the ntp service

   disable              => Disable the ntp 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.
```

```
caji:maintenance system setup ntp> set servers=0.pool.ntp.org
                      servers = 0.pool.ntp.org (uncommitted)
caji:maintenance system setup ntp> commit
caji:maintenance system setup ntp> done
aksh: done with "ntp", advancing configuration to "directory" ...
```

Consulte las secciones “NIS” [254], “LDAP” [256] y “Active Directory” [260] para obtener documentación adicional.

```
Configure Name Services. Configure directory services for users and groups. You
can configure and enable each directory service independently, and you can
configure more than one directory service.

Subcommands that are valid in this context:

   nis                 => Configure NIS

   ldap                => Configure LDAP

   ad                  => Configure Active Directory

   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 "directory"

caji:maintenance system setup directory> nis
caji:maintenance system setup directory nis> show
Properties:
                     <status> = online
                        domain = sun.com
                     broadcast = true
                     ypservers =

caji:maintenance system setup directory nis> set domain=fishworks
                        domain = fishworks (uncommitted)
caji:maintenance system setup directory nis> commit
caji:maintenance system setup directory nis> done
caji:maintenance system setup directory> done
aksh: done with "directory", advancing configuration to "support" ...
```

Configure las agrupaciones de almacenamiento que se caracterizan por su redundancia de datos subyacente y proporcione espacio compartido entre todos los sistemas de archivos y LUN. Consulte la sección Capítulo 5, Configuración del almacenamiento para obtener documentación adicional.

```
Configure Storage.

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 "storage"

    config <pool>        => Configure the storage pool

    unconfig             => Unconfigure the storage pool

    add                  => Add additional storage to the storage pool

    import               => Search for existing or destroyed pools to import

    scrub <start|stop>   => Start or stop a scrub

    get [prop]           => Get value for property [prop]. ("help properties"
                            for valid properties.) If [prop] is not specified,
                            returns values for all properties.

    set pool=[pool]      => Change current pool

caji:maintenance system setup storage> show
Properties:
                          pool = pool-0
                        status = online
                       profile = mirror
                   log_profile = -
                 cache_profile = -
caji:maintenance system setup storage> done
aksh: done with "storage", advancing configuration to "support" ...
```

Consulte “Phone Home” [281] para obtener documentación adicional sobre la configuración de la asistencia técnica remota.

```
Remote Support. Register your appliance and configure remote monitoring.

Subcommands that are valid in this context:

   tags                 => Configure service tags

   scrk                 => Configure phone home

   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 "support"

caji:maintenance system setup support> done
aksh: initial configuration complete!
```

♦ ♦ ♦ CAPÍTULO 4

Configuración de red

Las funciones de configuración de red permiten crear una variedad de configuraciones de red avanzadas usando los puertos de la red física, 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 estas abstracciones, para usarlas en la conexión con los múltiples servicios de datos en el sistema.

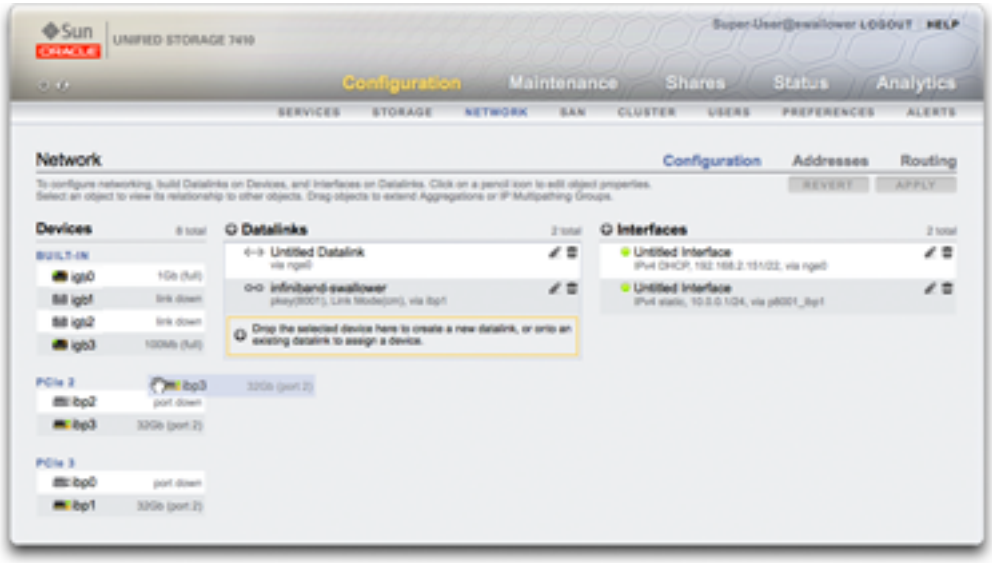
Hay cuatro componentes para la configuración de la red de un sistema:

- Dispositivos: puertos de red física. Corresponden a las conexiones de red física o la IP en las particiones de InfiniBand (IPoIB).
- Enlaces de datos: es el elemento básico para enviar y recibir paquetes. Los enlaces de datos pueden corresponderse 1:1 con un dispositivo (es decir, con un puerto de red física) o una partición de IB, o puede definir enlaces de datos de agregación y de VLAN compuestos por otros dispositivos y enlaces de datos.
- Interfaz: la construcción básica para la configuración y la dirección. Cada interfaz IP se asocia con un único enlace de datos, o se define como grupo de rutas múltiples IP (IPMP) compuesto por otras interfaces.
- Enrutamiento: configuración del enrutamiento IP. Controla la manera en la que el sistema dirige los paquetes IP.

Página de configuración de red

En el modelo ZFSSA, los dispositivos de red representan el hardware disponible: no tienen ajustes configurables. Los enlaces de datos son una entidad capa 2, y deben crearse para aplicar ajustes, como LACP para esos dispositivos de red. Las interfaces son una entidad capa 3 que contiene los ajustes IP, que ponen a disposición mediante un enlace de datos. Este modelo tiene ajustes de interfaz separados en dos partes: enlaces de datos para ajustes de capa 2 e interfaces para ajustes de capa 3.

FIGURA 4-1 Ventana de configuración de red



El siguiente es un ejemplo de una única dirección IP en un único puerto (configuración común):

TABLA 4-1 Ejemplo de dirección IP única en un único puerto

Dispositivos	Enlace de datos	Interfaz
igb0	datalink1	deimos (192.168.2.80/22)

La siguiente configuración es para una agregación de enlaces de 3 niveles:

TABLA 4-2 Ejemplo de configuración para una agregación de enlaces de 3 niveles

Dispositivos	Enlace de datos	Interfaz
igb1, igb2, igb3	aggr1 (agregación de LACP)	phobos (192.168.2.81/22)

La entidad del enlace de datos (llamada "aggr1") agrupa los dispositivos de red de manera que se puedan configurar (política de agregación de LACP). La entidad de interfaz (llamada "phobos") permite configurar la dirección IP, que queda disponible en la red mediante el enlace de datos. Los dispositivos de red (llamados "igb1", "igb2", ..., por el sistema) no tienen

parámetros que se configuren directamente. Se necesitan enlaces de datos para completar la configuración de la red, ya sea que apliquen valores de configuración específicos a los dispositivos de red o no.

Dispositivos

Son creados por el sistema para representar la red disponible o los puertos InfiniBand. No tienen parámetros de configuración propios.

Enlaces de datos

Se encargan de gestionar dispositivos y son utilizados por las interfaces. Admiten el uso de:

- LACP: protocolo de control de agregación de enlaces, que permite agrupar varios dispositivos de red para que actúen como si fuera uno solo. Esto mejora el rendimiento (multiplica el ancho de banda) y la fiabilidad (puede resistir fallos de los puertos de red), pero el dispositivo debe estar conectado a un conmutador que admita LACP y esté activado para esos puertos.
- Particiones IB: pariciones InfiniBand para conectarse a los dominios de tejido IB aislados por lógica.
- VLAN: LAN virtuales para mejorar la seguridad y el aislamiento de la red local. Las VLAN son recomendadas para administrar el dispositivo, de lo contrario, use VNIC.
- VNIC: tarjetas de interfaz de red virtuales, que 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. En la sección “Consideraciones de la agrupación en clusters para redes” [176], a continuación, se proporcionan instrucciones detalladas.

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

El estándar IEEE802.3ad (agregación de enlaces) 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 esta información para reproducirla en una configuración de un solo conmutador.

Se pueden utilizar las siguientes configuraciones de enlaces de datos:

TABLA 4-3 Configuración de enlaces de datos

Propiedad	Descripción
Name	Use el nombre personalizado definido. Por ejemplo: "internal", "external", "adminnet", etc.
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, tal vez sea necesario forzar una velocidad (y dúplex) para garantizar que el enlace de datos funcione según las propiedades de velocidad y dúplex esperadas.
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.
VLAN	Use cabeceras de VLAN.
VLAN ID	Use el identificador de VLAN definido; opcional para VNIC.
VNIC	Use una VNIC.
MTU	Use el tamaño de la unidad de transmisión máxima (MTU) definido. La MTU predeterminada 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 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.
LACP Aggregation	Use la agregación de LACP de varios dispositivos de red.
LACP Policy	Use la política de LACP definida para seleccionar un puerto saliente. L2 aplica el algoritmo hash a la dirección

Propiedad	Descripción
	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.
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, entre ellas Cisco Etherchannel, no utilizan el protocolo de LACP: el modo de LACP se debe configurar con el valor "off" si en la red se usan agregaciones que no sean LACP.
LACP Timer	Use el intervalo definido entre los mensajes de LACP para el modo activo.
IB Partition	Use particiones IB.
Partition Key	Use la partición (dominio de tejido) a la que pertenece el dispositivo del puerto subyacente. La clave de partición (pkey) se encuentra en el gestor de subred, donde se la configura. La clave pkey se puede definir antes de configurar el gestor de subred, pero el enlace de datos permanecerá inactivo hasta que se haya configurado correctamente la partición de la subred con la GUID del puerto como miembro. Es importante que la pertenencia de la partición de los puertos HCA sea congruente con las reglas de “Rutas múltiples de redes IP (IPMP) ” [79] y Capítulo 10, Configuración de cluster del gestor de subred.
IB Link Mode	Use el modo de enlace IB definido. Hay dos modos: Unreliable Datagram (Datagrama no confiable) y Connected (Conectado). Unreliable Datagram (Datagrama no confiable) permite que un par de colas locales se comunique con varios pares de colas en cualquier host y los mensajes se comunican sin reconocerse en la capa IB. El modo Unreliable Datagram (Datagrama no confiable) usa una MTU de 2044. El modo Connected (Conectado) usa pares de colas IB y destina un par de colas locales a la comunicación con un par de colas remotas dedicado. El modo Connected (Conectado) usa una MTU de 65520 y puede ofrecer un mayor rendimiento que el modo Unreliable Datagram (Datagrama no confiable).

Interfaces de red

Las interfaces de red configuran las direcciones IP mediante enlaces de datos. Admiten las siguientes opciones:

- Protocolos IPv4 e IPv6.
- IPMP: rutas múltiples 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.

Se pueden utilizar las siguientes configuraciones de interfaz:

TABLA 4-4 Configuración de la interfaz

Propiedad	Descripción
Name	Nombre personalizado de la interfaz.
Allow Administration	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.
Enable Interface	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.
IPv4 Configure with	Se puede introducir manualmente una lista de direcciones estáticas o se puede seleccionar "DHCP" para solicitudes dinámicas.
IPv4 Address/Mask	Una o varias direcciones IPv4 en notación CIDR (192.168.1.1/24).
IPv6 Configure with	Una lista de direcciones estáticas introducida manualmente o "IPv6 AutoConfiguration" (configuración automática de IPv6) para usar direcciones locales de enlace generadas automáticamente (y locales de sitio si responde un enrutador IPv6).
IPv6 Address/Mask	Una o varias direcciones IPv6 en notación CIDR (1080::8:800:200C:417A/32).
IP MultiPathing Group	Configuración de rutas múltiples IP, que permite el uso de una agrupación de enlaces de datos para redundancia.

Rutas múltiples de redes IP (IPMP)

Los grupos de rutas múltiples IP se utilizan 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 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 sólo 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.

La 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 224.0.01. 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 predeterminada 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” [277]. 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 puede controlar directamente los sistemas de destino seleccionados por el sistema, pero esto se puede 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).

En “Rutas múltiples de redes IP (IPMP) ” [79] se proporcionan instrucciones detalladas para crear grupos IPMP.

Para obtener información acerca de interfaces locales privadas, consulte el Capítulo 10, Configuración de cluster.

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. Así, 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 están vinculadas 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 del enrutamiento de red

El sistema proporciona una única tabla de enrutamiento IP, que está formada por una recopilación de entradas de tabla de enrutamiento. Cuando se necesita enviar un paquete IP a un destino dado, el sistema selecciona la entrada de enrutamiento cuyo destino se asemeje más a la dirección de destino del paquete (sujeto a la política de multiorigen del sistema, como se describe a continuación). A continuación, 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, no se envía el paquete. Si hay varias entradas de enrutamiento que empatan como opción más similar (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.

Entradas de enrutamiento de red

La tabla de enrutamiento está compuesta por entradas de enrutamiento, cada una con los siguientes campos:

TABLA 4-5 Campos de entradas de enrutamiento

Campo	Descripción	Ejemplos
Destination	Rango de direcciones IP de destino (en notación CIDR) que pueden coincidir con la ruta.	192.168.0.0/22
Gateway	Salto siguiente (dirección IP) a donde se enviará el paquete (excepto	192.168.2.80

Campo	Descripción	Ejemplos
	rutas de "sistema", como se describe a continuación).	
Family	Protocolo de Internet.	IPv4, IPv6
Type	Origen de la ruta.	dhcp, estática, sistema
Interface	Interfaz IP sobre la que se enviará el paquete.	igb0

Una entrada de enrutamiento con un campo de "destino" de `0.0.0.0/0` coincide con cualquier paquete (si no hay ninguna otra ruta cuya coincidencia sea mayor), por lo que se la conoce como la ruta "predeterminada". En la BUI, las rutas predeterminadas se distinguen de las no predeterminadas por una propiedad adicional:

TABLA 4-6 Distinción entre rutas predeterminadas y rutas no predeterminadas

Tipo	Tipo de ruta.	Predeterminada, red

Como en el caso anterior, un paquete dado se envía mediante la interfaz IP especificada en el campo "interface" (Interfaz) de la entrada de enrutamiento. 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 se la puede especificar en el campo "interface" (Interfaz) porque no sería una ruta de alta disponibilidad.

Las entradas de enrutamiento provienen de una serie de orígenes diferentes, según se identifica en el campo "type" (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 la puede editar o suprimir, y cómo se lo hace. El sistema admite los siguientes tipos de rutas:

TABLA 4-7 Tipos de ruta admitidos

Tipo	Descripción
Estática	Creada y gestionada por el administrador del dispositivo.
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 "gateway" (Puerta de enlace) identifica la dirección IP del dispositivo en esa subred.
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.

Tipo	Descripción
Dinámica	Creada automáticamente por el dispositivo mediante los protocolos de enrutamiento dinámico RIP y RIPng (si están activados).

Un tipo adicional identifica una ruta estática que actualmente no se puede utilizar:

TABLA 4-8 Tipo de ruta estática no disponible

Inactiva	Ruta estática creada con anterioridad asociada con una interfaz IP que está desactivada o fuera de línea.

Propiedades de enrutamiento de red

TABLA 4-9 Propiedades de enrutamiento

Propiedad	Descripción
Multihoming model	Controla la política del sistema para aceptar y transmitir paquetes IP cuando hay varias interfaces IP activadas simultáneamente. Los valores permitidos son "loose" (Flexible) (predeterminado), "adaptive" (Adaptable) y "strict" (Estricta). A continuación se los describe.

Si un sistema se configura con más de una interfaz IP, puede haber 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. Se admiten tres políticas:

TABLA 4-10 Políticas de multiorigen

Política	Descripción
Flexible	No se aplica ninguna vinculación entre un paquete IP y la interfaz IP usada para enviarlo o recibirlo: 1) El paquete IP se acepta sobre la interfaz IP si la dirección IP de destino se encuentra en el dispositivo. 2) El paquete IP se transmite sobre la interfaz IP vinculada a la ruta que mejor coincida 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 encuentre

Política	Descripción
	en la misma subred que la dirección IP de origen del paquete: 1) El paquete IP se acepta sobre la interfaz IP si la dirección IP de destino se encuentra en el dispositivo. 2) El paquete IP se transmite sobre la interfaz IP vinculada a la ruta que mejor coincida 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: 1) El paquete IP se acepta sobre la interfaz IP si la dirección IP de destino se encuentra en esa interfaz IP. 2) 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. 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 predeterminada para proporcionar acceso remoto a la red de administración y se crea una ruta predeterminada independiente para proporcionar acceso remoto a los protocolos de almacenamiento, entonces la política predeterminada del sistema, la flexible, puede hacer que la ruta administrativa predeterminada se use para tráfico de almacenamiento. Si se cambia a la política adaptable o la 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 política adaptable el sistema usará cualquier ruta disponible, mientras que con la estricta, el sistema descartará el paquete.

Configuración de redes con la BUI

Si se usa la BUI para reconfigurar la red, el sistema hace todo lo posible por mantener la conexión de red actual con el explorador. Sin embargo, algunos cambios de la configuración de la red, por ejemplo, si se suprime la dirección específica con la que se conecta el explorador , inevitablemente harán que el explorador pierda la conexión. Por este motivo, se recomienda asignar una dirección IP y un dispositivo de red específicos para el uso de los administradores y siempre dejar la dirección configurada. También, de ser necesario, puede realizar tareas de reconfiguración de red particularmente complejas desde la CLI mediante la consola serie.

En la sección Configuration (Configuración) >Network (Red) se usan los siguientes íconos:

TABLA 4-11 Íconos de configuración de redes

Ícono	Descripción
	Agregar un nuevo enlace de datos, interfaz o ruta
	Editar la configuración de enlace de datos, interfaz o ruta
	Edición desactivada
	Destruir un enlace de datos, interfaz o ruta
	Destrucción desactivada
	Ícono de arrastrar y soltar
	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 (estados 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)

Ícono	Descripción
	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 reflejada

En la parte superior derecha, se encuentra la navegación local de configuración, direcciones y enrutamiento, que despliegan vistas de configuración alternativas.

Página de configuración de red

La página Configuración es la que se muestra de forma predeterminada; en ella se muestran los dispositivos, los enlaces de datos y las interfaces, junto con botones para la administración. Pase el puntero del mouse sobre las entradas para que aparezca un ícono adicional  y haga clic en las entradas para resaltar los demás componentes asociados con ellas.

La lista Dispositivos muestra los estados de los enlaces a la derecha, con un ícono que refleja el estado del puerto de red. Si los puertos aparecen desconectados, compruebe que estén correctamente conectados a la red.

Para configurar una dirección IP en un dispositivo de red, primero debe crear un enlace de datos y después una interfaz para usar ese enlace de datos. Puede usar el ícono  para realizar ambas acciones; aparecerán cuadros de diálogo para las propiedades del enlace de datos y la interfaz.

Hay más de un método para configurar las interfaces de red. Puede hacer clic en el ícono  de un dispositivo y, a continuación, arrastrarlo a la tabla del enlace de datos. Después, arrastre el enlace de datos a la tabla de interfaces. Hay otros movimientos posibles. Este procedimiento puede resultar útil para configuraciones complejas, ya que se resaltan los movimientos válidos.

Direcciones de red

En esta página, se muestra una tabla de resumen de la configuración de red actual, con los siguientes campos:

TABLA 4-12 Resumen de la configuración actual de la red

Campo	Descripción	Ejemplo
Network Datalink	Nombre del enlace de datos y resumen detallado	datalink1 (mediante igb0)
Network Interface	Nombre de la interfaz y resumen detallado	IPv4 DHCP, mediante datalink1
Network Addresses	Direcciones alojadas por esta interfaz	192.168.2.80/22
Host Names	Nombres de host resueltos para las direcciones de red	caji.sf.example.com

Página de enrutamiento de red

En esta página, se proporciona información de configuración de la tabla de enrutamiento IP y sus propiedades asociadas, como se analizó más arriba. De forma predeterminada, se muestran todas las entradas de la tabla de enrutamiento, pero se puede usar la barra de navegación secundaria para filtrar por tipo.

Para comprobar una ruta específica, use `traceroute` en la CLI.

```
zfssa-source:> traceroute 10.80.198.102
traceroute: Warning: Multiple interfaces found; using 10.80.198.101 @ igb3
traceroute to 10.80.198.102 (10.80.198.102), 30 hops max, 40 byte packets
1 10.80.198.1 (10.80.198.1) 6.490 ms 0.924 ms 0.834 ms
2 10.80.198.102 (10.80.198.102) 0.152 ms 0.118 ms 0.099 ms
zfssa-target:> traceroute 10.80.198.101
traceroute: Warning: Multiple interfaces found; using 10.80.198.102 @ igb3
traceroute to 10.80.198.101 (10.80.198.101), 30 hops max, 40 byte packets
1 10.80.198.1 (10.80.198.1) 1.031 ms 0.905 ms 0.769 ms
2 10.80.198.101 (10.80.198.101) 0.158 ms 0.111 ms 0.109 ms
```

Configuración de redes con la CLI

La configuración de red se encuentra en `configuration net`, que tiene comandos secundarios para `devices`, `datalinks`, `interfaces` y `routing`. Se puede usar el comando `show` con cada uno de ellos para ver la configuración actual:

```
caji:> configuration net
caji:configuration net> devices show
Devices:

DEVICE      UP     SPEED         MAC
igb0        true   1000 Mbit/s   0:14:4f:9a:b9:0
igb1        true   1000 Mbit/s   0:14:4f:9a:b9:1
igb2        true   1000 Mbit/s   0:14:4f:9a:b8:fe
```

```
igb3        true   1000 Mbit/s   0:14:4f:9a:b8:ff

caji:configuration net> datalinks show
Datalinks:

   DATALINK CLASS          LINKS       LABEL
       igb0 device         igb0        datalink1

caji:configuration net> interfaces show
Interfaces:

  INTERFACE STATE  CLASS LINKS       ADDRS                 LABEL
       igb0 up     ip    igb0        192.168.2.80/22       caji

caji:configuration net> routing show
Properties:
                 multihoming = loose

Routes:

ROUTE      DESTINATION                     GATEWAY         INTERFACE TYPE
route-000  0.0.0.0/0                       192.168.1.1     igb0      dhcp
route-001  192.168.0.0/22                  192.168.2.142   igb0      system
```

Escriba `help` en cada sección para ver los comandos relevantes para crear y configurar enlaces de datos, interfaces y rutas. Subcomandos que son válidos en este contexto:

```
  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

  abort                => Abort creation of "vnic"

  done                 => Finish operating on "vnic"

  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.

  available            => Get values that can be assigned to the links
                          parameter when creating a network component.
```

El comando `available` se usa para ver los valores que se pueden asignar al parámetro `links` al crear un componente de red. A continuación se muestra la salida del comando `available` de la CLI:

```
caji:configuration net datalinks> device
caji:configuration net datalinks device (uncommitted)> available
```

```
igb7,igb6

caji:configuration net datalinks> vnic
caji:configuration net datalinks vnic (uncommitted)> available
igb5,igb4,aggr2,aggr1

caji:configuration net datalinks> vlan
caji:configuration net datalinks vlan (uncommitted)> available
igb5,igb4,aggr2,aggr1

caji:configuration net datalinks> aggregation
caji:configuration net datalinks aggregation (uncommitted)> available
igb7,igb6

caji:configuration net interfaces> ip
caji:configuration net interfaces ip (uncommitted)> available
aggr2,aggr1

caji:configuration net interfaces> ipmp
caji:configuration net interfaces ipmp (uncommitted)> available
vnic4,vnic3,igb5,igb4
```

A continuación se muestra cómo crear un enlace de datos con el comando `device` y cómo crear una interfaz con el comando `ip`:

```
caji:configuration net> datalinks
caji:configuration net datalinks> device
caji:configuration net datalinks device (uncommitted)> set links=igb1
                          links = igb1 (uncommitted)
caji:configuration net datalinks device (uncommitted)> set label=datalink2
                          label = datalink2 (uncommitted)
caji:configuration net datalinks device (uncommitted)> set mtu=9000
                          mtu = 9000 (uncommitted)
caji:configuration net datalinks device (uncommitted)> commit
caji:configuration net datalinks> show
Datalinks:

   DATALINK CLASS          LINKS       LABEL
       igb0 device         igb0        datalink1
       igb1 device         igb1        datalink2

caji:configuration net datalinks> cd ..
caji:configuration net> interfaces
caji:configuration net interfaces> ip
caji:configuration net interfaces ip (uncommitted)> set label="caji2"
                         label = caji2 (uncommitted)
caji:configuration net interfaces ip (uncommitted)> set links=igb1
                         links = igb1 (uncommitted)
caji:configuration net interfaces ip (uncommitted)> set v4addrs=10.0.1.1/8
                       v4addrs = 10.0.1.1/8 (uncommitted)
caji:configuration net interfaces ip (uncommitted)> commit
caji:configuration net interfaces> show
Interfaces:

  INTERFACE STATE  CLASS LINKS       ADDRS                LABEL
       igb0 up     ip    igb0        192.168.2.80/22      caji
       igb1 up     ip    igb1        10.0.1.1/8           caji2
```

A continuación se muestra cómo crear una ruta predeterminada mediante `10.0.1.2` mediante la nueva interfaz IP `igb1`:

```
caji:configuration net routing> create
caji:configuration net route (uncommitted)> set family=IPv4
                   family = IPv4 (uncommitted)
caji:configuration net route (uncommitted)> set destination=0.0.0.0
                   destination = 0.0.0.0 (uncommitted)
caji:configuration net route (uncommitted)> set mask=0
                   mask = 0 (uncommitted)
caji:configuration net route (uncommitted)> set interface=igb1
                   interface = igb1 (uncommitted)
caji:configuration net route (uncommitted)> set gateway=10.0.1.2
                   gateway = 10.0.1.2 (uncommitted)
caji:configuration net route (uncommitted)> commit
```

Tareas de configuración de red con la BUI

▼ Creación de una interfaz con un solo puerto

1. **Haga clic en el ícono de enlaces de datos .**
2. **De manera opcional, defina el nombre y seleccione el botón de radio personalizado MTU (escriba 9000 en el cuadro de texto).**
3. **Elija uno de los dispositivos de la lista Dispositivos.**
4. **Haga clic en "APPLY" (Aplicar). El enlace de datos aparece en la lista Datalinks (Enlaces de datos).**
5. **Haga clic en el ícono de interfaz .**
6. **Configure las propiedades deseadas y elija el enlace de datos que creó en el paso anterior.**
7. **Haga clic en "APPLY" (Aplicar). La interfaz aparece en la lista de interfaces.**
8. **La configuración de red del dispositivo en ejecución todavía no ha cambiado. Cuando termine de configurar las interfaces, haga clic en "APPLY" (Aplicar), en la parte superior, para confirmar la configuración.**

Modificación de una interfaz

1. **Haga clic en el ícono de edición del enlace de datos o la interfaz.**
2. **Cambie la configuración con los valores deseados.**
3. **Haga clic en "APPLY" (Aplicar) en el cuadro de diálogo.**
4. **Haga clic en "APPLY" (Aplicar) en la parte superior de la página para confirmar la configuración.**

Creación de una interfaz con un solo puerto (arrastrar y soltar)

1. **Pase el puntero del mouse sobre un dispositivo y haga clic en el ícono para arrastrar y soltar ( ).**
2. **Arrástrelo hasta la lista de enlaces de datos y suéltelo.**
3. **De manera opcional, defina un nombre y una MTU gigante.**
4. **Haga clic en "APPLY" (Aplicar).**
5. **Arrastre el enlace de datos a la lista de interfaces.**
6. **Configure las propiedades deseadas y haga clic en "APPLY" (Aplicar).**
7. **Haga clic en "APPLY" (Aplicar) en la parte superior de la pantalla para confirmar la configuración.**

Creación de una interfaz de enlaces agregados de LACP

1. **Haga clic en el ícono de enlaces de datos .**
2. **De manera opcional, defina el nombre del enlace de datos.**
3. **Seleccione Agregación de LACP.**

4. **Seleccione dos dispositivos o más de la lista de dispositivos y haga clic en "APPLY" (Aplicar).**
5. **Haga clic en el ícono de interfaces .**
6. **Configure las propiedades deseadas, elija el enlace agrupado de la lista de enlaces de datos y haga clic en "APPLY" (Aplicar).**
7. **Haga clic en "APPLY" (Aplicar) en la parte superior para confirmar la configuración.**

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

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. **Cree una o varias interfaces IP "subyacentes" que se utilizarán como componentes del grupo IPMP. Cada interfaz debe tener una dirección IP que se utilice como origen del sondeo (consulte más arriba la tarea independiente de creación de interfaces con un solo puerto).**
2. **Haga clic en el ícono 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 "Active" (Activas) o "Standby" (En espera), según lo desee.**
8. **Haga clic en "APPLY" (Aplicar).**

Creación de un grupo IPMP mediante la detección de fallos por estado del enlace únicamente

1. **Cree una o varias interfaces IP "subyacentes" con la dirección IP 0.0.0.0/8 para utilizarlas como componentes del grupo IPMP (consulte más arriba la tarea independiente de creación de interfaces con un solo puerto).**
2. **Haga clic en el ícono 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 "Active" (Activas) o "Standby" (En espera), según lo desee.**
8. **Haga clic en "APPLY" (Aplicar).**

Ampliación de una agregación de LACP

1. **Pase el puntero del mouse sobre uno de los dispositivos de la lista Dispositivos.**
2. **Haga clic en el ícono  y arrastre el dispositivo hasta un enlace de datos de agregación y suéltelo.**
3. **Haga clic en "APPLY" (Aplicar) en la parte superior de la página para confirmar esta configuración.**

Ampliación de un grupo IPMP

1. **Pase el puntero del mouse sobre una de las interfaces de la lista de interfaces.**

2. **Haga clic en el ícono y arrastre el dispositivo hasta una interfaz IPMP y suéltelo.**
3. **Haga clic en "APPLY" (Aplicar) en la parte superior de la página para confirmar esta configuración.**

Creación de una interfaz y un enlace de datos de partición InfiniBand

1. **Haga clic en el ícono de enlace de datos .**
2. **De manera opcional, defina un nombre.**
3. **Haga clic en la casilla de verificación Partición IB.**
4. **Elija uno de los dispositivos de la lista Dispositivos de partición.**
5. **Haga clic en "APPLY" (Aplicar). El nuevo enlace de datos de la partición aparece en la lista Enlaces de datos.**
6. **Haga clic en el ícono de interfaz .**
7. **Configure las propiedades deseadas y elija el enlace de datos que creó en el paso anterior.**
8. **Haga clic en "APPLY" (Aplicar). La interfaz aparece en la lista de interfaces.**
9. **La configuración de red del dispositivo en ejecución todavía no ha cambiado. Cuando termine de configurar las interfaces, haga clic en "APPLY" (Aplicar), en la parte superior, para confirmar la configuración.**

Creación de una VNIC sin un ID de VLAN para controladores en clusters

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. **Cuando el cluster tiene el estado AKCS_CLUSTERED, haga clic en el ícono Enlaces de datos .**
2. **De manera opcional, defina un nombre y una MTU.**
3. **Elija un dispositivo de la lista Dispositivos y haga clic en "APPLY" (Aplicar). El enlace de datos aparece en la lista Enlaces de datos.**
4. **Haga clic en el ícono de interfaz .**
5. **Configure las propiedades deseadas, elija el enlace de datos antes creado y haga clic en "APPLY" (Aplicar). La interfaz aparece en la lista Interfaces.**
6. **Haga clic en el ícono de enlaces de datos .**
7. **Seleccione la casilla de verificación VNIC, de manera opcional defina un nombre y una MTU (igual o menor que el valor del paso 2) y haga clic en "APPLY" (Aplicar). El nuevo enlace de datos VNIC aparece en la lista Enlaces de datos.**
8. **Haga clic en el ícono de interfaz .**
9. **Configure las propiedades deseadas, elija el enlace de datos VNIC antes creado y haga clic en "APPLY" (Aplicar). La interfaz aparece en la lista Interfaces.**
10. **La configuración de red del dispositivo en ejecución todavía no ha cambiado. Cuando termine de configurar las interfaces, haga clic en "APPLY" (Aplicar), en la parte superior, para confirmar la configuración.**
11. **Haga clic en la ficha Cluster . Las dos interfaces recientemente creadas aparecen en la sección Recurso con los propietarios predeterminados.**
12. **Use la lista desplegable Propietario para asignar una de las dos interfaces al otro nodo principal y haga clic en "APPLY" (Aplicar).**

Creación de VNIC con el mismo ID de VLAN para controladores en clusters

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. **Cuando el cluster tiene el estado AKCS_CLUSTERED, haga clic en el ícono Enlaces de datos .**
2. **Seleccione la casilla de verificación 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 "APPLY" (Aplicar). El nuevo enlace de datos VNIC aparece en la lista Enlaces de datos.**
3. **Haga clic en el ícono de interfaz .**
4. **Configure las propiedades deseadas, elija el enlace de datos VNIC antes creado y haga clic en "APPLY" (Aplicar). La interfaz aparece en la lista Interfaces.**
5. **Cree otra VNIC como se describe en los pasos 1 y 2 con el mismo dispositivo e ID de VLAN, y cree una interfaz para ella como se describe en los pasos 3 y 4.**
6. **La configuración de red del dispositivo en ejecución todavía no ha cambiado. Cuando termine de configurar las interfaces, haga clic en "APPLY" (Aplicar), en la parte superior, para confirmar la configuración.**
7. **Haga clic en la ficha Cluster . Las dos interfaces recientemente creadas aparecen en la sección Recurso con los propietarios predeterminados.**
8. **Use la lista desplegable Propietario para asignar una de las dos interfaces al otro nodo principal y haga clic en "APPLY" (Aplicar).**

Agregación de una ruta estática

1. **Vaya a Configuration (Configuración) > Network (Red) > Routing (Enrutamiento).**
2. **Haga clic en el ícono de agregación.**

3. **Complete las propiedades como se describió anteriormente.**
4. **Haga clic en "ADD" (Agregar). La nueva ruta aparece en la tabla.**

▼ Supresión de una ruta estática

1. **Vaya a Configuration (Configuración) > Network (Red) > Routing (Enrutamiento).**
2. **Pase el puntero del mouse sobre la entrada de la ruta y, a continuación, haga clic en el ícono de la papelera que se encuentra a la derecha.**

Tareas de configuración de red con la CLI

▼ Agregación de una ruta estática

1. **Vaya a `configuration net routing`.**
2. **Escriba `create`.**
3. **Escriba `show` para mostrar las propiedades requeridas y, a continuación, use `set` con cada una.**
4. **Escriba `commit`.**

▼ Supresión de una ruta estática

1. **Vaya a `configuration net routing`.**
2. **Escriba `show` para mostrar las rutas y los nombres de las rutas (por ejemplo, `route-002`).**
3. **Escriba `destroy` *nombre de la ruta*.**

▼ Cambio de la propiedad de multiorigen a estricto

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

♦ ♦ ♦ CAPÍTULO 5

Configuración del almacenamiento

Configure el almacenamiento en agrupaciones que se caracterizan por su redundancia de datos subyacente y proporcione espacio compartido entre todos los sistemas de archivos y LUN. En la sección “Recursos compartidos” [300], 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.

Cada nodo puede tener la cantidad de agrupaciones que se desee, y se puede asignar el propietario de cada agrupación del cluster de manera independiente. 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 y una agrupación RAID-Z. 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.

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 Sun Storage 7000, y es útil en casos de reconfiguración accidental, transferencia de agrupaciones entre nodos principales o en casos de fallos catastróficos de cabezal.

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 normalmente se comienzan a notar cuando la agrupación excede el 80% de la capacidad y pueden ser marcados cuando excede el 90% de la capacidad. Por lo tanto, los mejores resultados se obtienen si se asigna aproximadamente un 20% más del espacio necesario. Se puede usar la “UI de recursos compartidos” [300] para determinar la cantidad de espacio que se está utilizando actualmente.

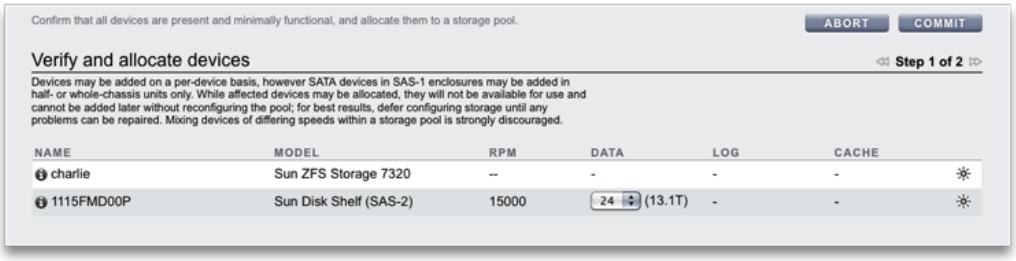
Perfil de configuración de almacenamiento

FIGURA 5-1 Perfil de configuración de almacenamiento

Esta acción configura la agrupación de almacenamiento. En la BUI, haga clic en el botón que se encuentra al lado de la lista de agrupaciones; al hacerlo, se le solicitará el nombre de la agrupación nueva. En la CLI, use el comando `config`, que requiere el nombre de la agrupación como argumento.

Después de iniciar la tarea, la configuración del almacenamiento se clasifica en dos fases diferentes: verificación y configuración.

FIGURA 5-2 Verificación y asignación de dispositivos



Reglas y directrices de configuración de almacenamiento

Para obtener un rendimiento óptimo, tenga presente lo siguiente:

Regla 1: todos los discos de "datos" que se encuentran dentro de un nodo principal o JBOD deben tener la misma velocidad de rotación (velocidad de rotación del soporte). El software del dispositivo ZFSSA detecta configuraciones erróneas y genera un fallo para la condición.

Recomendación 1: debido a problemas de rendimiento impredecibles, evite combinar diferentes velocidades de rotación de disco en una misma agrupación.

Recomendación 2: para obtener un rendimiento óptimo, no combine JBOD 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.

Recomendación 3: cuando configura agrupaciones de almacenamiento que contengan discos de datos de diferentes capacidades, en algunos casos ZFS usa el tamaño del disco de menor capacidad para algunos de los discos de la agrupación de almacenamiento (o todos ellos), lo que reduce la capacidad total esperada. Los tamaños usados dependerán del perfil de almacenamiento, la distribución y la combinación de dispositivos. Evite combinar diferentes capacidades de disco en la misma agrupación.

Verificación de almacenamiento

La verificación garantiza que todo el almacenamiento está conectado y en funcionamiento. Todos los dispositivos de almacenamiento deben estar conectados y en funcionamiento antes de

poder asignarlos. Si asigna una agrupación con dispositivos defectuosos o faltantes, no podrá agregar los dispositivos defectuosos o faltantes más adelante.

En un sistema sin almacenamiento conectado, todas las unidades disponibles se asignan de forma predeterminada. En un sistema ampliable, los estantes de discos se muestran en una lista junto con el nodo principal, y se puede controlar la asignación dentro de cada estante de discos. Este procedimiento será levemente diferente según el modelo del nodo principal o el estante de discos.

Puede seleccionar lo siguiente:

- Tamaño de dispositivo: filtra los dispositivos de datos por tamaño lógico. De forma predeterminada, Cualquiera muestra todos los dispositivos de datos disponibles.
- Dispositivos de datos: muestra todos los dispositivos de datos disponibles o el número disponible según el tamaño del dispositivo seleccionado.

El número de discos asignados de forma predeterminada depende de lo siguiente:

- La cantidad máxima disponible: cuando el almacenamiento conectado contiene únicamente dispositivos que comparten el mismo tamaño y la misma velocidad de rotación, o cuando se selecciona un tamaño entre varios tamaños
- Ninguno: cuando el almacenamiento conectado contiene varias velocidades de rotación.

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.

Asignación de almacenamiento en sistemas SAS-2

Las unidades dentro de todo el chasis se pueden asignar de manera individual, pero se debe tener cuidado al asignar discos de los JBOD 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 JBOD, e idealmente muchos más.

Configuración de perfiles de datos

Una vez que se completa la verificación, el siguiente paso incluye la selección de un perfil de almacenamiento que refleje los objetivos de rendimiento y RAS de la configuración. El conjunto de perfiles posibles presentado depende del almacenamiento disponible. En la siguiente tabla, se muestran todos los perfiles posibles y su descripción.

TABLA 5-1 Configuración de 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.
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

Perfil de datos	Descripción
	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.
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 sobre el rendimiento de lectura. Por lo general, no se recomienda esta configuración.

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 JBOD, no se pierden datos. Tenga en cuenta que los sistemas ya están configurados con redundancia entre casi todos los componentes. Cada JBOD 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 JBOD). Por lo general, la adopción de NSPF reduce la capacidad, ya que tiene requisitos más estrictos con respecto al ancho de los segmentos.

Los dispositivos de log se pueden configurar solamente con perfiles segmentados o reflejados. Como los dispositivos de log se utilizan solamente si se produce un fallo en un nodo, para que se pierdan datos de logs no reflejados es necesario que falle el dispositivo y que el nodo se reinicie inmediatamente después. 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, sólo se pueden crear perfiles de log segmentados.

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.

En un cluster, los dispositivos de caché están disponibles sólo para el nodo para el que se importa la agrupación de almacenamiento. En un cluster, es posible configurar que los dispositivos de caché de ambos nodos 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 un failover, los nuevos dispositivos de caché se pueden utilizar en el nuevo nodo.

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. Los grupos 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.

Importación de grupos de almacenamiento existentes

Permite importar una agrupación de almacenamiento existente, así como agrupaciones de almacenamiento que se hayan desconfigurado desadvertidamente. Se puede usar después de un restablecimiento de fábrica o de 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. Para importar una agrupación en la BUI, haga clic en el botón "IMPORTAR" de la pantalla de configuración de almacenamiento. Para importar una agrupación en la CLI, use el comando "import".

Una vez que se haya completado la fase de detección, aparecerá una lista de las agrupaciones disponibles con algunas características para identificarlos. Si el almacenamiento se destruyó o está incompleto, no se podrá importar la agrupación. A diferencia de la configuración del almacenamiento, el nombre de la agrupación no se especifica al comenzar, sino al seleccionarla. De forma predeterminada, se usa el nombre de la agrupación previa, pero se lo puede cambiar haciendo clic en el nombre, si está en la BUI, o configurando la propiedad "Nombre" si usa la CLI.

Agregación de almacenamiento adicional

Use esta acción para agregar almacenamiento adicional a la agrupación existente. El paso de verificación es idéntico al paso de verificación de la configuración inicial. El almacenamiento se debe agregar usando el mismo perfil que se usó para configurar inicialmente la agrupación.

Si no hay almacenamiento suficiente para configurar el sistema con el perfil actual, se pueden sacrificar algunos atributos. Por ejemplo, si se agrega un único JBOD a una configuración RAID-Z NSPF de paridad doble, es imposible conservar las características NSPF. Sin embargo, igual se puede agregar el JBOD y crear segmentos RAID dentro de él, sacrificando NSPF en el proceso.

Desconfiguración del almacenamiento

Con esta acción se eliminan los sistemas de archivos y los LUN activos y se desconfigura la agrupación de almacenamiento, de manera que queda disponible el almacenamiento sin formato para su configuración futura. Este proceso se puede deshacer importando la agrupación de almacenamiento desconfigurada, siempre y cuando no se haya utilizado el almacenamiento sin formato como parte de una agrupación de almacenamiento activa.

Limpieza de agrupaciones de almacenamiento

Esta acción inicia el proceso de limpieza de la agrupación de almacenamiento mediante la cual se verifica todo el contenido en busca de errores. Si se encuentra algún error irrecuperable, ya sea mediante una operación de limpieza o una operación normal, los archivos afectados se muestran en la BUI. La limpieza también puede detenerse de ser necesario.

Configuración de almacenamiento con la BUI

▼ Configuración de una agrupación de almacenamiento

Se puede llegar a esta tarea de dos maneras: durante la configuración inicial del dispositivo o desde la pantalla Configuration (Configuración) > Storage (Almacenamiento).

1. **Haga clic en el botón  que se encuentra arriba de la lista de agrupaciones de almacenamiento.**
2. **Introduzca un nombre para la agrupación de almacenamiento.**
3. **En la pantalla "Allocate and verify storage" (Asignar y verificar almacenamiento), configure la asignación de JBOD para la agrupación de almacenamiento. La**

asignación de JBOD puede ser ninguna, medio, todo. Si no se detecta ningún JBOD, compruebe el cableado y la alimentación de energía.

4. **Haga clic en "COMMIT" (Confirmar).**
5. **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, para ayudarlo a encontrar la mejor configuración para sus necesidades empresariales.**
6. **Haga clic en "COMMIT" (Confirmar).**

▼ Agregación de dispositivos de caché a una agrupación existente

1. **Instale el nuevo dispositivo Readzilla o Logzilla en la primera ranura disponible. Consulte la ubicación de las ranuras en la sección "Descripción general" de "Guía de instalación de Oracle ZFS Storage Appliance ".**
2. **En la BUI, vaya a Configuration (Configuración) > Storage (Almacenamiento).**
3. **En la lista Available Pools (Agrupaciones disponibles), seleccione la agrupación a la que desea agregar el dispositivo. Asegúrese de que la agrupación esté en línea.**
4. **Haga clic en el botón Add (Agregar) para agregar el dispositivo a la agrupación.**
5. **Seleccione el dispositivo que está agregando a la agrupación y haga clic en Commit (Confirmar).**
6. **Seleccione el perfil de log (si corresponde) y haga clic en Commit (Confirmar).**

Configuración de almacenamiento con la CLI

▼ Agregación de dispositivos de caché a una agrupación existente

1. **Instale el nuevo dispositivo Readzilla o Logzilla en la primera ranura disponible. Consulte la ubicación de las ranuras en la sección “Descripción general” de “Guía de instalación de Oracle ZFS Storage Appliance ”.**
2. **En la línea de comandos, escriba:**
3. `: poc:> configuration storage`
4. **Especifique la agrupación a la que desea agregar el dispositivo:**
5. `: poc:configuration storage (pool_2)> set pool=pool_2`
6. `: pool = pool_2`
7. `: poc:configuration storage (pool_2)> add`
8. **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.**
9. **Muestre la información del dispositivo para la agrupación:**
10. `: poc:configuration storage (pool_2) verify> show`
11. `: ID STATUS ALLOCATION DATA LOG CACHE RPM`
12. `: 0 ok custom 0 0 0/4 1.86T`
13. `: 1 ok custom 0 0/2 34G 0 15000`
14. `: 2 ok custom 0 0/2 34G 0 15000`
15. **Especifique el estante de discos y la cantidad de Logzilla o Readzilla que se debe utilizar. En el siguiente ejemplo, se usa `1-log=1` para asignar un Logzilla del primer estante de discos.**
16. `: poc:configuration storage (pool_2) verify> set 1-log=1`

17. `: 1-log = 1`

18. **Nota: El valor "1-log=2" asignaría dos Logzilla del primer estante de discos.**

19. **En este ejemplo se asigna un Readzilla del primer estante de discos.**

20. `: poc:configuration storage (pool_2) verify> set 1-cache=1`

21. `: 1-cache = 1`

22. **Escriba `done`.**

23. `: poc:configuration storage (pool_2) verify> done`

24. **Nota: Si se agrega una cantidad impar de dispositivos Logzilla a una agrupación, o si la agrupación todavía no tiene un perfil, escriba `set log_profile=log_mirror` para establecer el perfil de log.**

25. **Escriba `show` para visualizar el perfil.**

26. `: poc:configuration storage (pool_2) config> show`

27. `:`

28. `: PROFILE CAPCTY NSPF DESCRIPTION`

29. `:  log_profile = log_stripe 17G no Striped log`

30. **Escriba `done` para completar la tarea:**

31. `: poc:configuration storage (pool_2) config> done`

32. `: poc:configuration storage (pool_2)>`

♦ ♦ ♦ CAPÍTULO 6

Configuración de red de área de almacenamiento

La página SAN configuration (Configuración de SAN) le permite conectar el dispositivo a una red de área de almacenamiento (SAN). Una SAN tiene tres componentes básicos:

- Un cliente, que accede al almacenamiento a través de la red.
- Un dispositivo de almacenamiento, que proporciona el almacenamiento a través de la red.
- Una red para enlazar el cliente con el almacenamiento.

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.

Destinos e iniciadores de SAN

Los destinos y los iniciadores se configuran mediante protocolos. Consulte la documentación del protocolo específico (“Canal de fibra de SAN” [116], “iSCSI” [213] o “SRP” [134]) para obtener información detallada.

Grupos de destinos e iniciadores de SAN

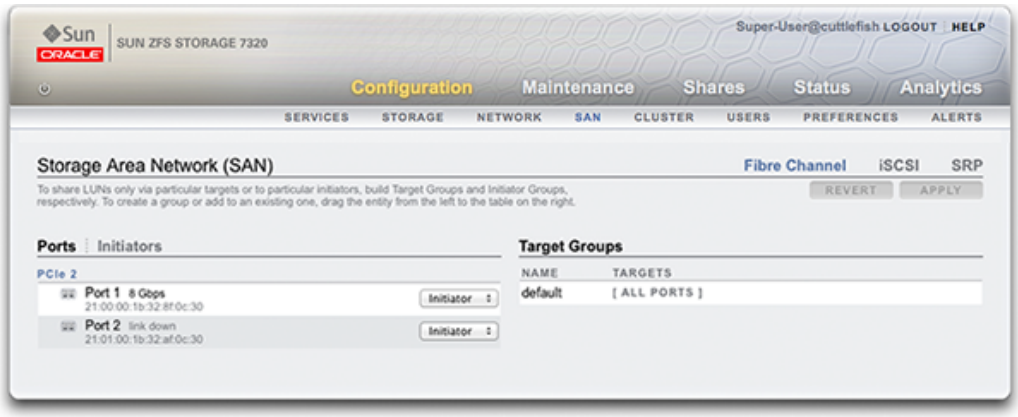
Los grupos de destinos e iniciadores definen conjuntos de destinos e iniciadores que se pueden asociar con LUN. Un LUN asociado con un grupo de destinos se puede ver solamente mediante los destinos del grupo. Si el LUN no está explícitamente asociado con un grupo de destino, se encuentra en el *grupo de destino predeterminado* 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 predeterminado* y se podrá tener acceso a él desde todos los iniciadores. Si bien puede ser útil usar el grupo de iniciadores predeterminado 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.

Configuración de SAN con la BUI

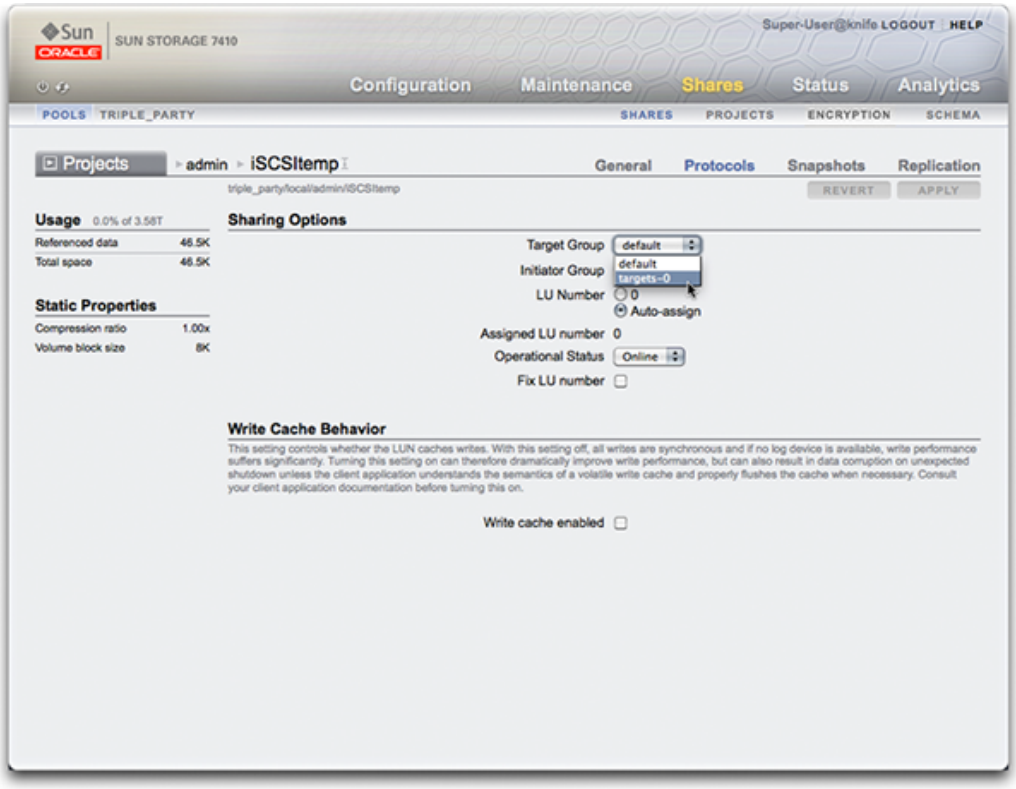
Para configurar destinos, vaya a la página Configuración > SAN de la BUI, utilice Fibre Channel (Canal de fibra), iSCSI y SRP para navegar y, a continuación, configure los controles Ports (Puertos), Initiator (Iniciador) y Target Groups (Grupos de destinos).

FIGURA 6-1 Página SAN de la BUI



Para asociar un LUN, vaya a la página Shares (Recursos compartidos) > Shares (Recursos compartidos) > Protocols (Protocolos) y, a continuación, configure los controles Target Group (Grupo de destinos) e Initiator Group (Grupo de iniciadores).

FIGURA 6-2 Asociación de un LUN



Configuración de SAN con la CLI

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.

Terminología de SAN

Para configurar el dispositivo a fin de utilizarlo con una SAN, debe comprender algunos términos básicos de SAN:

TABLA 6-1 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.
iSCSI	Internet SCSI, un protocolo para compartir almacenamiento SCSI mediante redes IP.
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).
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 iqn.fecha.autoridad:idúnico 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

Término	Descripción
	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.
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, sólo 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 administrador del sistema de almacenamiento crea un destino y es identificado por métodos de direccionamiento exclusivos. Una vez configurado, un destino consiste de 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 la sección “Protocolos” [336] para obtener más información.

Canal de fibra de SAN

El canal de fibra (FC) es una tecnología de redes 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.

Configuración de destino de puertos de FC

De manera predeterminada, todos los puertos FC se configuran en el 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 de FC tiene un nombre World Wide Name (WWN) y, al igual que con otros protocolos de bloque, los destinos de FC se pueden agrupar en “Grupos de destinos e iniciadores de SAN” [111], 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 las notas del producto *Implementación de inicio de SAN de canal de fibra con el dispositivo Sun ZFS Storage de Oracle* en http://www.oracle.com/technetwork/articles/servers-storage-admin/fbsanboot-365291.html (http://www.oracle.com/technetwork/articles/servers-storage-admin/fbsanboot-365291.html) para obtener información detallada acerca de las soluciones de inicio de SAN de FC con el dispositivo Oracle ZFS Storage.

Consideraciones de agrupación en clusters

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 de 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.

Configuración de iniciadores de FC

Los iniciadores se identifican por su nombre WWN y, al igual que con otros protocolos de bloque, se pueden crear alias para ellos. Para ayudar en la creación de alias para los iniciadores de FC, se puede seleccionar un nombre WWN de 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.

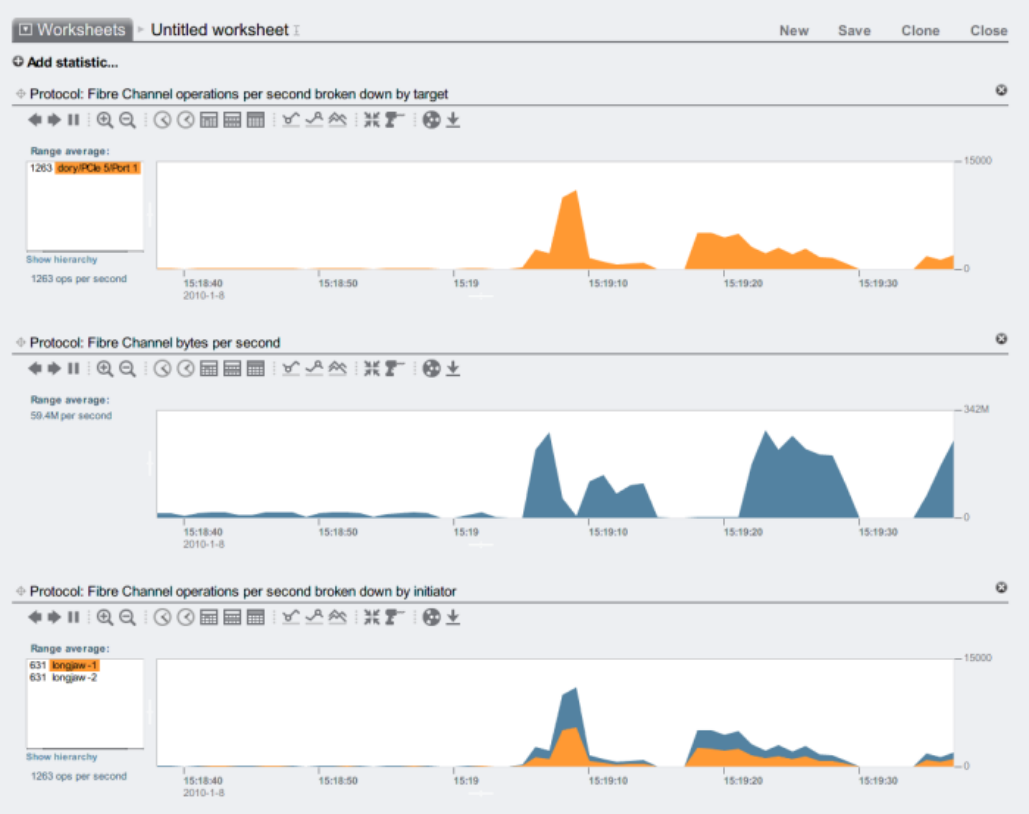
Consideraciones de agrupación en clusters

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.

Consideraciones sobre el rendimiento

El rendimiento de FC se puede observar mediante los “Análisis” de “Guía de análisis de Oracle ZFS Storage Appliance ”, que permiten desglosar las operaciones o el rendimiento por iniciador, destino o LUN:

FIGURA 6-3 Rendimiento de FC



Para las operaciones, también se puede hacer un desglose por compensación, latencia, tamaño y comando SCSI, lo que permite comprender no sólo *qué* es lo que hacen las operaciones de FC, sino también *cómo* lo hacen y *por qué*.

Solución de problemas de FC

Saturación de colas de FC

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, por lo general no es necesario restringir la profundidad de cola en los clientes, ya que los puertos de FC del dispositivo pueden

manejar una gran cantidad de solicitudes concurrentes. 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 aprovisionados. 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 2 puertos de FC y 100 LUN, y el otro tiene 4 puertos de FC y 28 LUN, se debe tomar la menor profundidad de cola máxima como dos puertos por 2048 comandos dividido 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 Solaris se hace ajustando la variable global `ssd_max_throttle`.

Problemas en el nivel del enlace de FC

Para resolver problemas relacionados con los enlaces, por ejemplo una fibra óptica rota o un cable mal conectado, vea las estadísticas de error de cada puerto de 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.

Configuración de FC con la BUI

Cambio de modo de los puertos FC

Para hacer uso de los puertos de FC, desde la pantalla Configuration (Configuración) > SAN de la BUI configúrelos en el modo Target (Destino) mediante el menú desplegable que se muestra en la siguiente captura de pantalla. Debe tener permisos de usuario `root` para realizar esta acción. Tenga en cuenta que en una configuración de cluster, los puertos de cada nodo principal se configuran en el modo Target (Destino) por separado.

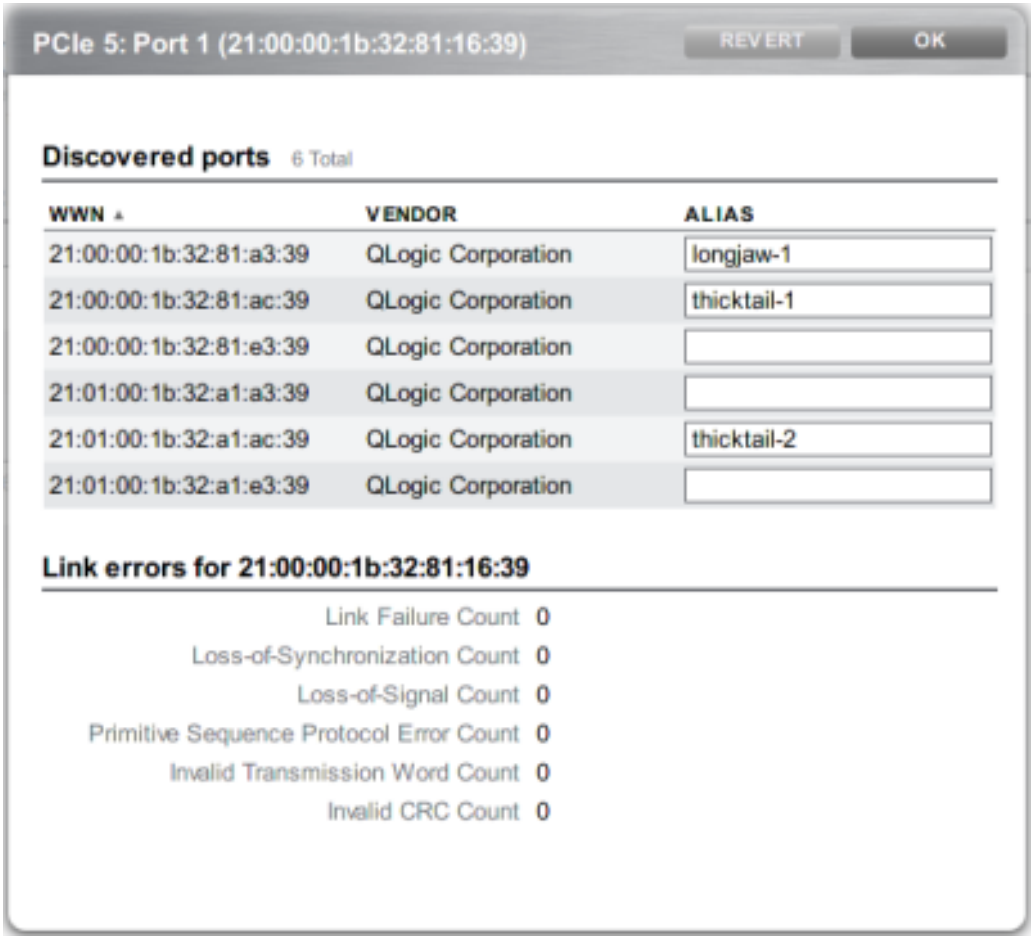
Después de configurar los puertos deseados en el modo Target (Destino), haga clic en el botón Apply (Aplicar). Aparece un mensaje de confirmación que le notifica que el dispositivo se reiniciará de inmediato. Confirme que desea reiniciarlo.

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 .

Visualización de los puertos FC detectados

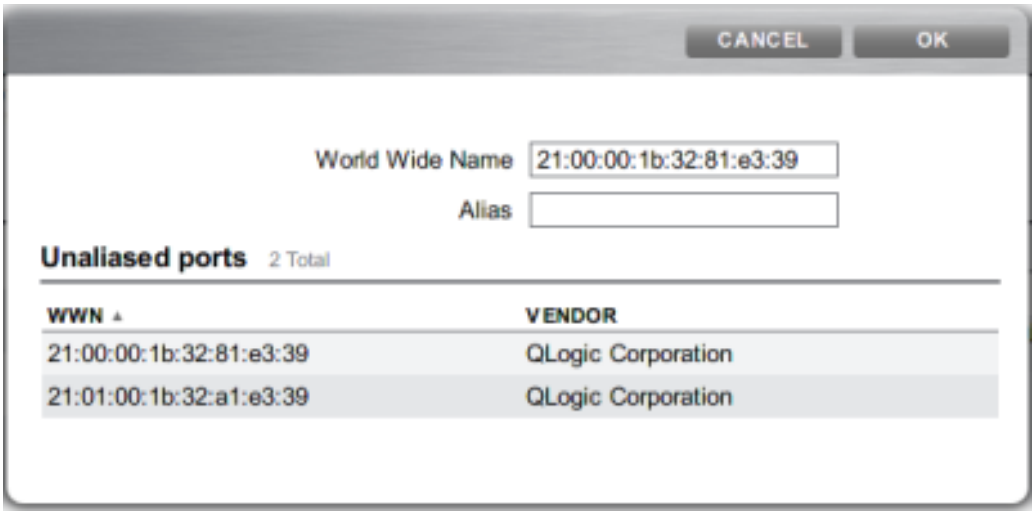
Haga clic en el ícono de información para ver el cuadro de diálogo Discovered Ports (Puertos detectados), desde donde puede resolver errores de enlace. En el cuadro de diálogo Puertos detectados, haga clic en un nombre WWN de la lista para ver los errores de enlace asociados.

FIGURA 6-4 Puertos FC detectados



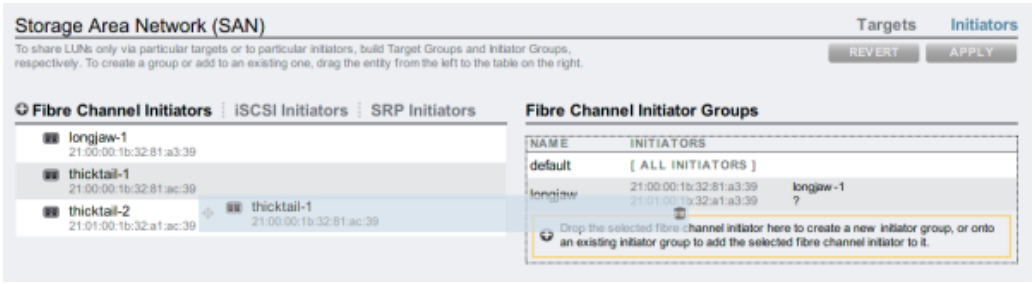
Creación de grupos de iniciadores FC

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.



En la página Initiators (Iniciadores), arrastre los iniciadores a la lista FC Initiator Groups (Grupos de iniciadores de FC) para crear nuevos grupos o agregar iniciadores a grupos existentes.

FIGURA 6-5 Lista de grupos de iniciadores FC

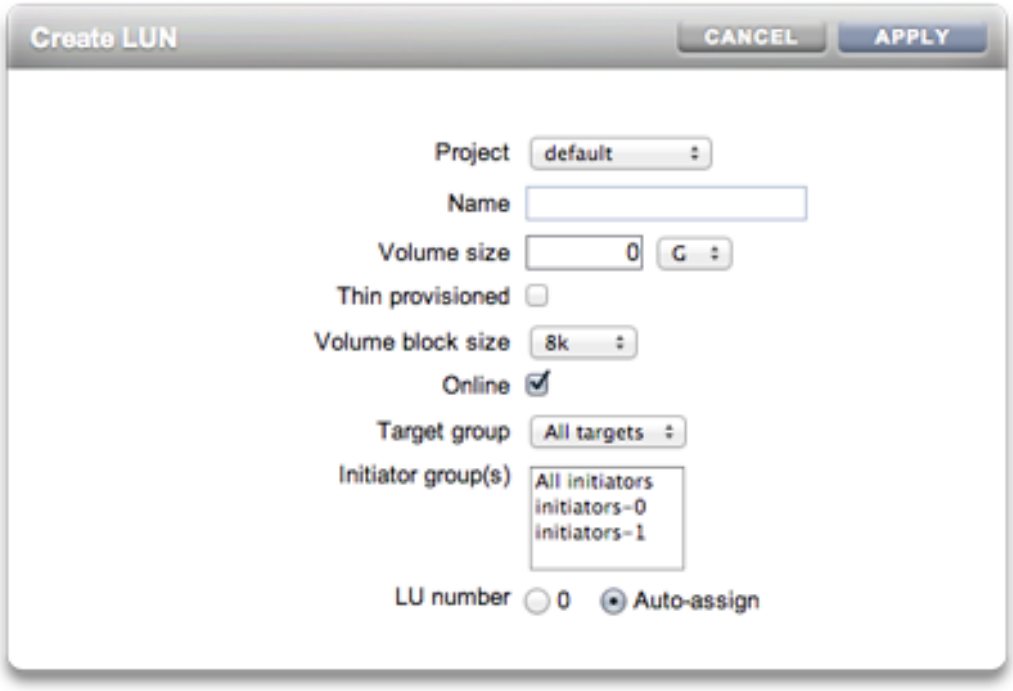


Haga clic en el botón Apply (Aplicar) para confirmar el nuevo grupo de iniciadores. Ahora puede crear un LUN que tenga acceso exclusivo al grupo de iniciadores del cliente.

Asociación de un LUN con un grupo de iniciadores FC

Para crear el LUN, deslice el puntero del mouse sobre el grupo de iniciadores y haga clic en el ícono de agregación de LUN . Aparece el cuadro de diálogo Crear LUN con el grupo de iniciadores asociado seleccionado. Defina el nombre y el tamaño, y haga clic en Aplicar para agregar el LUN a la agrupación de almacenamiento.

FIGURA 6-6 Asociación de un LUN con un grupo de iniciadores FC



Configuración de FC con la CLI

Cambio de modo de los puertos FC

```
dory:configuration san fc targets> set targets="wwn.2101001B32A11639"
                     targets = wwn.2101001B32A11639 (uncommitted)
dory:configuration san fc targets> commit
```

Visualización de los puertos FC detectados

```
dory: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
dory:configuration san fc targets> select target-000
dory: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
```

Creación de grupos de iniciadores FC

```
dory:configuration san fc initiators> create
dory:configuration san fc initiators (uncommitted)> set name=lefteye
dory:configuration san fc initiators (uncommitted)>
    set initiators=wwn.2101001B32A1AC39,wwn.2100001B3281AC39
dory:configuration san fc initiators (uncommitted)> commit
dory:configuration san fc initiators> list
GROUP     NAME
group-001 lefteye
          |
          +-> INITIATORS
              wwn.2101001B32A1AC39
              wwn.2100001B3281AC39
```

Asociación de un LUN con un grupo de iniciadores FC

En el siguiente ejemplo, se muestra la creación de un LUN llamado `lefty` y su asociación con el grupo de iniciadores `fera`.

```
dory:shares default> lun lefty
dory:shares default/lefty (uncommitted)> set volsize=10
```

```
                    volsize = 10 (uncommitted)
dory:shares default/lefty (uncommitted)> set initiatorgroup=fera
              initiatorgroup = default (uncommitted)
dory:shares default/lefty (uncommitted)> commit
```

Asignación de alias a iniciadores y grupos de iniciadores mediante secuencias de comandos

Consulte las secciones “Uso de la CLI” [36] y “Secuencias de comandos simples de la CLI y comandos por lotes” [36] para obtener información sobre cómo modificar y usar la siguiente secuencia de comandos de ejemplo.

```
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 ..');
}
```

iSCSI

Internet SCSI es uno de los varios protocolos de bloque admitidos por el dispositivo para compartir almacenamiento SCSI.

Configuración de destinos

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:idúnico 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 6-2 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 6-3 Íconos de estado de destino

Ícono	Descripción
	El destino está en línea.
	El destino está sin conexión.

Consideraciones de agrupación en clusters

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.

Configuración de iniciadores

Los iniciadores iSCSI tienen las siguientes propiedades configurables.

TABLA 6-4 Propiedades de iniciadores iSCSI

Propiedad	Descripción
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.

Planificación de la configuración de clientes

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.

Solución de problemas de iSCSI

Para ver consejos para la resolución de errores de configuración comunes en iSCSI, consulte la sección “iSCSI” [213].

Observación del rendimiento de iSCSI

El rendimiento de iSCSI se puede observar mediante los “Análisis” de “Guía de análisis de Oracle ZFS Storage Appliance ”,, que permiten desglosar las operaciones o el rendimiento por iniciador, destino o LUN.

Configuración de iSCSI con la BUI

▼ Creación de una hoja de trabajo de análisis

Para crear una hoja de trabajo de análisis que permita observar las operaciones por iniciador, realice el siguiente procedimiento:

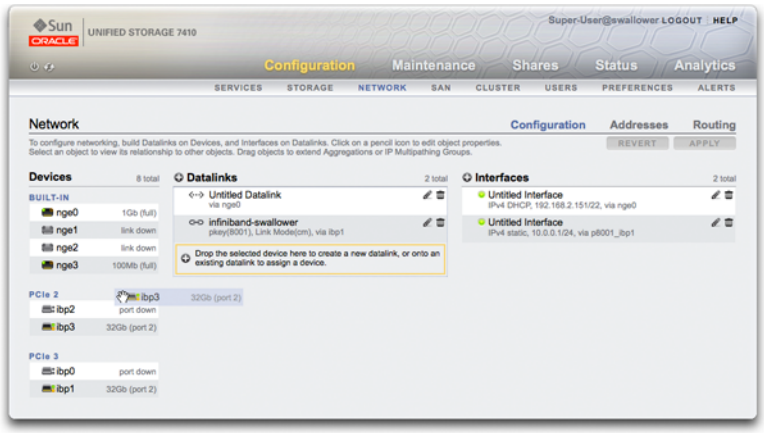
1. **Vaya a la pantalla Análisis.**
2. **Haga clic en el ícono de agregación a fin de agregar estadísticas. Aparece un menú de todas las estadísticas.**
3. **En la sección Protocolos del menú, seleccione Operaciones iSCSI > Desglosado por iniciador. Aparece un gráfico de las operaciones actuales por 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.**

Configuración de destinos iSER

En la BUI, los destinos iSER se gestionan como destinos iSCSI en la pantalla Configuration (Configuración) > SAN.

1. **Para configurar interfaces ibd(x), seleccione la interfaz ibd(x) (o IPMP) deseada y arrástrela hasta la lista Datalinks (Enlaces de datos) para crear el enlace de datos en la pantalla Configuration (Configuración) > Network (Red).**

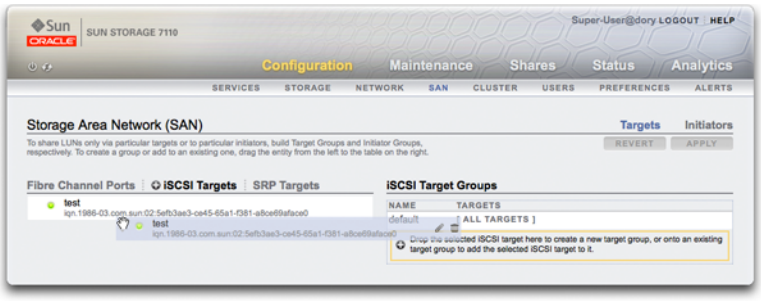
2. **Arrastre el enlace de datos hasta la lista de interfaces para crear una nueva interfaz.**



3. **Para crear un destino iSER, en la página Configuration (Configuración) > SAN, haga clic en el enlace iSCSI Targets (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 iSCSI Target Group (Grupo de destinos iSCSI).**

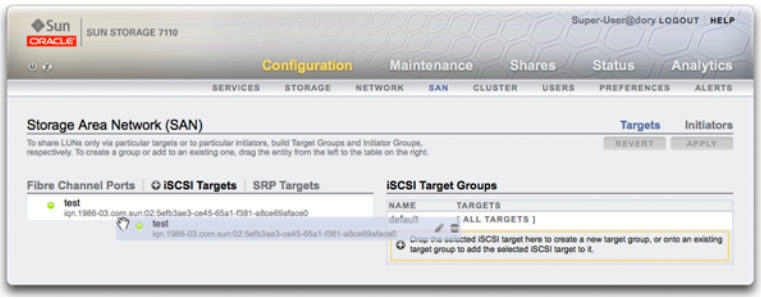


6. **Para crear un iniciador, haga clic en el enlace Iniciador y, a continuación, haga clic en el enlace Iniciadores iSCSI.**

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 OK (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.**

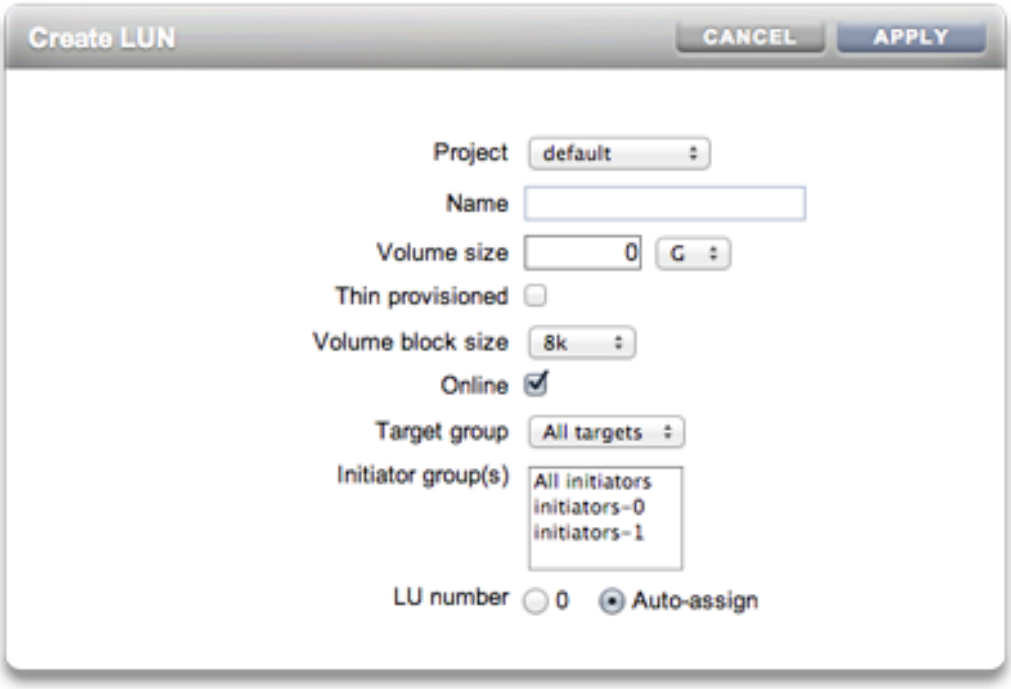
9. **Para crear un grupo, arrastre el iniciador hasta la lista iSCSI Initiator Groups (Grupos de iniciadores iSCSI).**



10. **Para crear un LUN, en la página Shares (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 Target Group (Grupo de destinos) e Initiator Groups (Grupos de iniciadores).**

12. :



Configuración de iSCSI con la CLI

Agregación de un destino iSCSI con un IQN generado automáticamente

```
ahi:configuration san iscsi targets> create
ahi:configuration san iscsi targets target (uncommitted)> set alias="Target 0"
ahi:configuration san iscsi targets target (uncommitted)> set auth=none
ahi:configuration san iscsi targets target (uncommitted)> set interfaces=igb1
ahi:configuration san iscsi targets target (uncommitted)> commit
ahi:configuration san iscsi targets> list
TARGET     ALIAS
target-000 Target 0
           |
           +-> IQN
               iqn.1986-03.com.sun:02:daf0161f-9f5d-e01a-b5c5-e1efa9578416
```

Agregación de un destino iSCSI con un IQN específico y autenticación RADIUS

```
ahi:configuration san iscsi targets> create
ahi:configuration san iscsi targets target (uncommitted)> set alias="Target 1"
ahi:configuration san iscsi targets target (uncommitted)>
     set iqn=iqn.2001-02.com.acme:12345
ahi:configuration san iscsi targets target (uncommitted)> set auth=radius
ahi:configuration san iscsi targets target (uncommitted)> set interfaces=igb1
ahi:configuration san iscsi targets target (uncommitted)> commit
ahi: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
```

Agregación de un iniciador iSCSI que usa autenticación CHAP

```
ahi:configuration san iscsi initiators> create
ahi:configuration san iscsi initiators initiator (uncommitted)>
     set initiator=iqn.2001-02.com.acme:initiator12345
ahi:configuration san iscsi initiators initiator (uncommitted)> set alias="Init 0"
ahi:configuration san iscsi initiators initiator (uncommitted)>
     set chapuser=thisismychapuser
ahi:configuration san iscsi initiators initiator (uncommitted)>
     set chapsecret=123456789012abc
ahi:configuration san iscsi initiators initiator (uncommitted)> commit
ahi:configuration san iscsi initiators> list
NAME          ALIAS
initiator-000 Init 0
              |
              +-> INITIATOR
                  iqn.2001-02.com.acme:initiator12345
```

Agregación de un grupo de destinos iSCSI

```
ahi:configuration san iscsi targets groups> create
ahi:configuration san iscsi targets group (uncommitted)> set name=tg0
ahi: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
ahi:configuration san iscsi targets group (uncommitted)> commit
ahi: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
```

Agregación de un grupo de iniciadores iSCSI

```
ahi:configuration san iscsi initiators groups> create
ahi:configuration san iscsi initiators group (uncommitted)> set name=ig0
ahi:configuration san iscsi initiators group (uncommitted)>
    set initiators=iqn.2001-02.com.acme:initiator12345
ahi:configuration san iscsi initiators group (uncommitted)> commit
ahi:configuration san iscsi initiators groups> list
GROUP     NAME
group-000 ig0
          |
          +-> INITIATORS
             iqn.2001-02.com.acme:initiator12345
```

SRP

Protocolo RDMA SCSI, un protocolo admitido por el dispositivo para compartir almacenamiento SCSI mediante redes que proporcionan servicios RDMA (por ejemplo, InfiniBand).

Configuración de destinos SRP

Los puertos SRP se comparten con otros servicios de puertos IB, por ejemplo, IPoIB y RDMA. El servicio SRP puede funcionar sólo en el modo de destino. Los destinos SRP tienen las siguientes propiedades configurables.

TABLA 6-5 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 6-6 Íconos de estado de destino de SRP

Ícono	Descripción
	El destino está en línea.
	El destino está sin conexión.

Consideraciones de agrupación en clusters

En las plataformas agrupadas en cluster, los destinos de pares de cluster se deben configurar en el mismo grupo de destino 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.

Configuración de iniciadores

Los iniciadores SRP tienen las siguientes propiedades configurables.

TABLA 6-7 Propiedades de iniciadores SRP

Propiedad	Descripción
Initiator EUI	EUI de este iniciador.
Alias	Apodo en lenguaje natural para este iniciador.

Observación del rendimiento de SRP

El rendimiento de SRP se puede observar mediante los “Análisis” de “Guía de análisis de Oracle ZFS Storage Appliance ”, que permiten desglosar las operaciones o el rendimiento por iniciador o destino. {{Server}}/wiki/images/cfg_san_srp.png

Configuración de destinos SRP con la BUI

▼ Configuración de destinos SRP

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 Target Groups (Grupos de destinos).**
7. **Haga clic en la opción para aplicar.**
8. **(Opcional) Para crear un iniciador y un grupo de iniciadores en la pantalla Initiator (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 Target Group (Grupo de destinos) e Initiator Group (Grupo de iniciadores) del cuadro de diálogo Create LUN (Crear LUN) para seleccionar los grupos SRP que desea asociar con el LUN.**

Configuración de destino SRP con la 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:

```
swallower:configuration san targets srp groups> create
swallower:configuration san targets srp group (uncommitted)> set name=targetSRPgroup
                        name = targetSRPgroup (uncommitted)
swallower:configuration san targets srp group (uncommitted)>
set targets=eui.0002C903000489A4
                      targets = eui.0002C903000489A4 (uncommitted)
swallower:configuration san targets srp group (uncommitted)> commit
swallower:configuration san targets srp groups> list
GROUP     NAME
group-000 targetSRPgroup
          |
          +-> TARGETS
```

```
            eui.0002C903000489A4
```

En el siguiente ejemplo, se muestra cómo crear un LUN y asociarlo con el grupo targetSRPgroup con el contexto `shares` de la CLI:

```
swallower:shares default> lun mylun
swallower:shares default/mylun (uncommitted)> set targetgroup=targetSRPgroup
                 targetgroup = targetSRPgroup (uncommitted)
swallower:shares default/mylun (uncommitted)> set volsize=10
                      volsize = 10 (uncommitted)
swallower:shares default/mylun (uncommitted)> commit
swallower:shares default> list
Filesystems:
NAME             SIZE    MOUNTPOINT
test             38K     /export/test
LUNs:
NAME              SIZE    GUID
mylun             10G     600144F0E9D19FFB00004B82DF490001
```

♦ ♦ ♦ CAPÍTULO 7

Configuración de usuario

En esta sección, se describen los *usuarios* que pueden administrar el dispositivo, los *roles* para gestionar las autorizaciones otorgadas a los usuarios y cómo agregarlos al sistema con la BUI o la CLI.

Los usuarios pueden ser:

- Usuarios locales: toda la información de la cuenta se guarda en el dispositivo.
- Usuarios de directorio: utiliza cuentas existentes de “NIS” [254] o “LDAP” [256] y guarda la configuración de autorización complementaria en el dispositivo. Esto permite a los usuarios existentes de NIS o LDAP tener privilegios para iniciar sesión y administrar el dispositivo.

Si bien los usuarios locales pueden utilizar los servicios de datos, hay varias cosas que se deben tener presentes.

- Para los usuarios locales, no se tiene control de los UID. Esto es un problema para NFSv3 con cualquier otra cosa y NFSv4 con AUTH_SYS.
- No se admite el uso de grupos locales.
- La definición de un usuario local con finalidad de datos también permite al usuario local iniciar sesión en la interfaz de administración.

Para otorgar privilegios a los usuarios, se les asignan *roles* personalizados.

Roles de usuario

Un rol es una recopilación de privilegios que se pueden asignar a los usuarios. Puede ser deseable crear los roles de *administrador* y *operador*, con diferentes niveles de autorización. Los integrantes del personal pueden recibir cualquier rol que sea adecuado para sus necesidades, sin asignar privilegios innecesarios.

Se considera que el uso de roles es mucho más seguro que el uso de contraseñas de administrador compartidas, por ejemplo, asignar a todos la contraseña *root*. Los roles restringen a los usuarios a las autorizaciones necesarias solamente y también atribuyen sus acciones al nombre de usuario individual en el log “Logs” de “Manual de servicio del cliente de Oracle ZFS Storage Appliance ”.

De forma predeterminada, existe un rol denominado "Basic administration", que contiene autorizaciones muy básicas.

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 *alcances*, y cada alcance puede tener un conjunto de filtros opcionales para reducir el alcance 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 los ámbitos disponibles:

TABLA 7-1 Ámbitos disponibles para los usuarios

BUI de ámbito	CLI de ámbito	Ejemplo de autorización	Ejemplo de filtro
Active Directory	ad	Unirse a un dominio de Active Directory.	Nombre de dominio
Alertas	alert	Configurar filtros de alerta y umbrales.	.
Análisis	stat	Leer una estadística con este detalle.	Detalles
Agrupación en clusters	cluster	Realizar failback de recursos a un par de cluster.	.
Conjuntos de datos	dataset	Gestionar aspectos de conjuntos de datos de análisis.	Configurar
Hardware	hardware	Discos en línea y sin conexión	
Almacenes de claves	keystore	Configurar almacenes de claves.	.
Red	net	Configurar dispositivos de red, enlaces de datos e interfaces.	.
Proyectos y recursos compartidos	nas	Cambiar propiedades generales de proyectos y recursos compartidos.	Agrupación, proyecto, recurso compartido
Roles	role	Configurar autorizaciones para un rol.	Nombre de rol

BUI de ámbito	CLI de ámbito	Ejemplo de autorización	Ejemplo de filtro
SAN	stmf	Configurar autorizaciones para SAN.	
Servicios	svc	Reiniciar un servicio.	Nombre de servicio
Esquema de propiedades de recursos compartidos	schema	Modificar esquema de propiedades.	.
Sistema	appliance	Reiniciar el dispositivo.	Nombre de dispositivo
Actualizar	update	Actualizar software del sistema.	.
Usuarios	user	Cambiar una contraseña.	Nombre de usuario
Flujo de trabajo	workflow	Modificar flujo de trabajo.	Nombre de flujo de trabajo
Hoja de trabajo	worksheet	Modificar hoja de trabajo.	Nombre de hoja de trabajo

Explore los alcances en la BUI para ver si existen otras autorizaciones. Actualmente hay más de cincuenta autorizaciones diferentes disponibles, y es posible que en actualizaciones futuras del software del dispositivo se agreguen más.

Administración de propiedades de usuario

Cuando se gestionan usuarios y roles, se pueden configurar las siguientes propiedades.

Propiedades de usuario

Todas las siguientes propiedades se pueden configurar cuando se agrega un usuario, y un subconjunto de ellas se pueden configurar cuando se edita un usuario:

TABLA 7-2 Propiedades de usuario

Propiedad	Descripción
Type	Directorio (credenciales de acceso desde NIS o LDAP) o Local (se guarda el usuario en el dispositivo).
Username	Nombre de usuario único para el usuario.
Full Name	Descripción del usuario.
Password/Confirm	Para usuarios locales, escriba la contraseña inicial en los dos campos.

Propiedad	Descripción
Require session annotation	Si esta opción está activada, cuando los usuarios inician sesión en el dispositivo, deben proporcionar una descripción en formato de texto del motivo por el que inician sesión. Esta anotación se puede usar para hacer un seguimiento del trabajo realizado para solicitudes en un sistema de tickets, y el ID del ticket se puede usar como anotación de la sesión. La anotación de la sesión aparece en el log "Logs" de "Manual de servicio del cliente de Oracle ZFS Storage Appliance ".
Kiosk user	Si esta opción está activada, el usuario podrá ver la pantalla solamente en la configuración "Kiosk screen" (Pantalla de quiosco). Se puede usar para restringir a un usuario para que vea sólo el "panel de control" [48], por ejemplo. Los usuarios de quiosco no tienen acceso al dispositivo mediante la CLI.
Kiosk screen	Pantalla a la que está restringido este usuario de quiosco, si se activa la opción "Kiosk user" (Usuario de quiosco).
Roles	Roles que tiene este usuario.
Exceptions	Estas autorizaciones están excluidas de las que normalmente están disponibles debido a los roles seleccionados.

Propiedades de roles

Las siguientes propiedades se pueden configurar cuando se gestionan los roles:

TABLA 7-3 Propiedades de roles

Propiedad	Descripción
Name	Nombre del rol como aparecerá en las listas.
Description	Descripción detallada del rol si se lo desea.
Authorizations	Autorizaciones para este rol.

Página de la BUI de usuarios

En la página Usuarios de la BUI, se muestran los usuarios y los grupos, junto con botones para la administración. Pase el puntero del mouse sobre una entrada para revelar los botones para clonar, editar y destruir. Haga doble clic en una entrada para ver la pantalla de edición correspondiente. Los botones son los siguientes:

TABLA 7-4 Íconos de la página de la BUI de usuarios

Ícono	Descripción
	Permite agregar un nuevo usuario o rol. Aparece un nuevo cuadro de diálogo en el que se pueden proporcionar las propiedades requeridas.
	Muestra un cuadro de búsqueda. Escriba una cadena de búsqueda y pulse Intro para buscar ese texto en las listas de usuarios o roles y desplegar sólo las entradas que coincidan con él. Haga clic en este ícono nuevamente o en "Show All" (Mostrar todo) para regresar a las listas completas.
	Permite clonar un usuario o rol. Agregue un nuevo usuario o rol a partir de los campos basados en los valores de esta entrada.
	Permite editar un usuario o rol.
	Permite eliminar un usuario, rol o autorización.

Configuración de usuarios con la BUI

▼ Agregación de un administrador

1. **Compruebe que aparezca un rol de administrador apropiado en la lista Roles. De no ser así, agregue un rol (consulte la tarea correspondiente).**
2. **Haga clic en el ícono de agregación  que se encuentra junto a Users (Usuarios).**
3. **Configure las propiedades de usuario.**
4. **Haga clic en la casilla de verificación del rol de administrador.**
5. **Haga clic en el botón Add (Agregar) en la parte superior del cuadro de diálogo. El nuevo usuario aparece en la lista Users (Usuarios).**

Agregación de un rol

1. **Haga clic en el ícono de agregación que se encuentra junto a Roles.**
2. **Defina el nombre y la descripción del rol.**
3. **Agregue autorizaciones al rol (consulte la tarea correspondiente).**
4. **Haga clic en el botón Add (Agregar) en la parte superior del cuadro de diálogo. El nuevo rol aparece en la lista Roles.**

Agregación de autorizaciones a un rol

1. **Seleccione "Scope" (Alcance). Si hay filtros disponibles para este alcance, aparecen debajo del selector de alcances.**
2. **Seleccione filtros, si corresponde.**
3. **Haga clic en la casilla de verificación de todas las autorizaciones que desee agregar.**
4. **Haga clic en el botón Add (Agregar) de la sección Authorization (Autorizaciones). Las autorizaciones se agregan al final de la lista del cuadro de diálogo.**

Supresión de autorizaciones de un rol

1. **Pase el puntero del mouse sobre el rol deseado en la lista Roles y haga clic en el ícono de edición .**
2. **Pase el puntero del mouse sobre la autorización deseada al final de la lista y haga clic en el ícono de la papelera que está a la derecha.**
3. **Haga clic en el botón Apply (Aplicar) que se encuentra en la parte superior del cuadro de diálogo.**

▼ Agregación de un usuario que pueda ver sólo el panel de control

1. **Agregue un usuario de directorio o un usuario local (consulte la tarea independiente).**
2. **Configure el modo Kiosk (Quiosco) con el valor true y compruebe que la pantalla Kiosk (Quiosco) esté configurada con el valor "status/dashboard" (Estado/panel de control).**
3. **Ahora el usuario debería poder iniciar sesión pero ver solamente el panel de control.**

Configuración de usuarios con la CLI

Las acciones posibles en la BUI también están disponibles en la CLI. Escriba `help` cuando navega por la administración de usuarios, roles y autorizaciones para que se muestren los comandos disponibles.

Ejemplo de configuración de usuarios con la CLI

Para mostrar la interfaz de usuarios y roles de la CLI, en el siguiente ejemplo se agrega el usuario de NIS "brendan" al sistema y se le otorga autorización para reiniciar el servicio HTTP. Se incluye la creación de un rol para esta autorización.

Comenzaremos con la creación del rol, al que llamaremos "webadmin":

```
caji:> configuration roles
caji:configuration roles> role webadmin
caji:configuration roles webadmin (uncommitted)> set
   description="web server administrator"
                  description = web server administrator (uncommitted)
caji:configuration roles webadmin (uncommitted)> commit
caji:configuration roles> show
Roles:

NAME             DESCRIPTION
basic            Basic administration
webadmin         web server administrator
```

Ahora que hemos creado el rol webadmin, agregaremos la autorización para reiniciar el servicio HTTP. En este ejemplo, también se muestra la salida de la finalización con tabulación, que muestra las entradas válidas y es útil para determinar alcances válidos y opciones de filtro:

```
caji:configuration roles> select webadmin
caji:configuration roles webadmin> authorizations
caji:configuration roles webadmin authorizations> create
caji:configuration roles webadmin auth (uncommitted)> set scope=tab
ad           cluster      net          schema       update
alert        hardware     replication  stat         user
appliance    nas          role         svc          worksheet
caji:configuration roles webadmin auth (uncommitted)> set scope=svc
                        scope = svc
caji:configuration roles webadmin auth (uncommitted)> show
Properties:
                        scope = svc
                      service = *
              allow_administer = false
               allow_configure = false
                 allow_restart = false

caji:configuration roles webadmin auth (uncommitted)> set service=tab
*               ftp             ipmp            nis             ssh
ad              http            iscsi           ntp             tags
smb            identity        ldap            routing         vscan
datalink:igb0   idmap           ndmp            scrk
dns             interface:igb0  nfs             snmp
caji:configuration roles webadmin auth (uncommitted)> set service=http
                      service = http (uncommitted)
caji:configuration roles webadmin auth (uncommitted)> set allow_restart=true
                 allow_restart = true (uncommitted)
caji:configuration roles webadmin auth (uncommitted)> commit
caji:configuration roles webadmin authorizations> list
NAME       OBJECT                              PERMISSIONS
auth-000   svc.http                            restart
```

Ahora que se ha creado el rol, podemos pasar a la sección de usuarios para crear el usuario "brendan" y asignarle el rol "webadmin":

```
caji:configuration roles webadmin authorizations> cd ../../..
caji:configuration> users
caji:configuration users> netuser brendan
caji:configuration users> show
Users:

NAME                    USERNAME                UID        TYPE
Brendan Gregg           brendan                 130948     Dir
Super-User              root                    0          Loc

caji:configuration users> select brendan
caji:configuration users brendan> show
Properties:
                     logname = brendan
                    fullname = Brendan Gregg
             initial_password = **************
           require_annotation = false
                       roles = basic
                  kiosk_mode = false
               kiosk_screen = status/dashboard
```

```
Children:
                      exceptions => Configure this user's exceptions
                     preferences => Configure user preferences
caji:configuration users brendan> set roles=basic,webadmin
                        roles = basic,webadmin (uncommitted)
caji:configuration users brendan> commit
```

El usuario brendan ahora debería poder iniciar sesión con su contraseña de NIS y reiniciar el servicio HTTP en el dispositivo.

▼ Agregación de un administrador

1. **Vaya a `configuration roles`.**
2. **Escriba `show`. Ejecute `select` en cada rol y, a continuación, `authorizations show` para buscar un rol que tenga autorizaciones de administración apropiadas. Si no hay ningún rol apropiado, comience por la creación del rol (consulte la tarea correspondiente).**
3. **Vaya a `configuration users`.**
4. **Para usuarios de directorio (NIS, LDAP), escriba `netuser` seguido por el nombre del usuario existente que desea agregar. Para usuarios locales, escriba `user` seguido por el nombre del usuario que desea agregar; a continuación, escriba `show` para ver las propiedades que se deben configurar. Escriba `set` y, a continuación, escriba `commit`.**
5. **Hasta ahora ha creado un usuario, pero todavía no personalizó todas las propiedades. Escriba `select` seguido por el nombre del usuario.**
6. **Ahora escriba `show` para ver la lista completa de preferencias. Ahora es posible agregar roles y excepciones de autorización, así como realizar lo indicado en el Capítulo 8, Configuración de preferencias de dispositivos ZFSSA.**

▼ Agregación de un rol

1. **Vaya a `configuration roles`.**
2. **Escriba `role` seguido por el nombre del rol que desea crear.**
3. **Defina la descripción y, a continuación, escriba `commit` para confirmar el rol.**

4. **Agregue autorizaciones al rol (consulte la tarea correspondiente).**

▼ Agregación de autorizaciones a un rol

1. **Vaya a `configuration roles`.**
2. **Escriba `select` seguido por el nombre del rol.**
3. **Escriba `authorizations`.**
4. **Escriba `create` para agregar una autorización.**
5. **Escriba `set scope=` seguido por el nombre del alcance. Use la finalización con tabulación para ver la lista.**
6. **Escriba `show` para ver los filtros y las autorizaciones disponibles.**
7. **Escriba `set` para configurar las autorizaciones deseadas en true y configure los filtros (si los hubiera). La finalización con tabulación es útil para ver las configuraciones de filtro válidas.**
8. **Escriba `commit`. Se agregó la autorización.**

▼ Supresión de autorizaciones de un rol

1. **Vaya a `configuration roles`.**
2. **Escriba `select` seguido por el nombre del rol.**
3. **Escriba `authorizations`.**
4. **Escriba `show` para mostrar las autorizaciones.**
5. **Escriba `destroy` seguido por el nombre de la autorización (por ejemplo, "auth-001"). Se destruyó la autorización.**

♦ ♦ ♦ CAPÍTULO 8

Configuración de preferencias de dispositivos ZFSSA

En esta sección, se presentan los valores de configuración de las preferencias de localidad, propiedades de sesión y claves SSH.

Propiedades de preferencias

Si inició sesión en la BUI, puede configurar las siguientes preferencias para su cuenta, pero no puede configurar las preferencias de las cuentas de otros usuarios.

TABLA 8-1 Configuración de preferencias

Propiedad	Descripción
Initial login screen	Primera página que carga la BUI después de iniciar sesión correctamente. De forma predeterminada, es el "panel de control de estado" [48].
Locality	De forma predeterminada, es C. Las ubicaciones C y POSIX admiten sólo 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.
Session timeout	Tiempo desde que el usuario sale de la BUI después del cual el explorador cierra automáticamente la sesión.
Current session annotation	Texto de anotación agregado a los logs de auditoría.
Advanced analytics statistics	Con esta propiedad, aparecen estadísticas adicionales en "Análisis" de "Guía de análisis de Oracle ZFS Storage Appliance ".
SSH Public 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. En la BUI, estas claves se aplican sólo al usuario actual; para agregar claves para otros usuarios, use la CLI.

Configuración de preferencias con la CLI

En la CLI, las preferencias se pueden configurar en `configuration users`. En el siguiente ejemplo, se muestra cómo activar los análisis avanzados para la cuenta del usuario "brendan":

```
caji:> configuration users
caji:configuration users> select brendan
caji:configuration users brendan> preferences
caji:configuration users brendan preferences> show
Properties:
                        locale = C
                   login_screen = status/dashboard
                session_timeout = 15
             advanced_analytics = false

Children:
                              keys => Manage SSH public keys

caji:configuration users brendan preferences> set advanced_analytics=true
             advanced_analytics = true (uncommitted)
caji:configuration users brendan preferences> commit
```

En la CLI, configure las preferencias de su propia cuenta en `configuration preferences`. En el siguiente ejemplo, se muestra cómo configurar una anotación de sesión para su propia cuenta:

```
twofish:> configuration preferences
twofish:configuration preferences> show
Properties:
                        locale = C
                   login_screen = status/dashboard
                session_timeout = 15
             session_annotation =
             advanced_analytics = false

Children:
                              keys => Manage SSH public keys

twofish:configuration preferences> set session_annotation="Editing my user preferences"
             session_annotation = Editing my user preferences (uncommitted)
twofish:configuration preferences> commit
```

Configuración de claves SSH públicas con la CLI

Las claves SSH públicas pueden ser necesarias cuando se automatiza la ejecución de secuencias de comandos de la CLI desde otro host. A continuación se muestra la agregación de una clave SSH desde la CLI:

```
caji:> configuration preferences keys
caji:configuration preferences keys> create
```

```
caji:configuration preferences key (uncommitted)> set type=DSA
caji:configuration preferences key (uncommitted)> set key="...DSA key text..."
                          key = ...DSA key text...== (uncommitted)
caji:configuration preferences key (uncommitted)> set comment="fw-log1"
                       comment = fw-log1 (uncommitted)
caji:configuration preferences key (uncommitted)> commit
caji:configuration preferences keys> show
Keys:

NAME     MODIFIED              TYPE   COMMENT
key-000  10/12/2009 10:54:58   DSA    fw-log1
```

El texto de la clave es simplemente la clave (normalmente cientos de caracteres), sin espacios.

♦ ♦ ♦ CAPÍTULO 9

Configuración de alertas

En esta sección, se describen las alertas del sistema, cómo se las personaliza y la ubicación de los log de alertas. Para supervisar las estadísticas desde “Análisis” de “Guía de análisis de Oracle ZFS Storage Appliance ” cree alertas de umbral personalizadas. Para configurar el sistema para que responda a ciertos tipos de alertas, use las acciones de alertas.

Categorías de alertas

Los eventos importantes del dispositivo, que incluyen fallos de hardware y software, generan alertas. Estas alertas aparecen en “Logs” de “Manual de servicio del cliente de Oracle ZFS Storage Appliance ”, y también se pueden configurar para ejecutar cualquiera de las acciones de alerta.

Las alertas se agrupan en las siguientes categorías:

TABLA 9-1 Categorías de alertas

Categoría	Descripción
Cluster	Eventos de cluster, incluidos fallos de enlace y errores de pares.
Personalizada	Eventos generados a partir de la configuración personalizada de alertas.
Eventos de hardware	Cambios en la configuración del hardware e inicio del dispositivo.
Fallos de hardware	Cualquier fallo de hardware.
Operaciones NDMP	Eventos iniciados y finalizados de copia de seguridad y restauración. Este grupo está disponible como "NDMP: backup only" (Sólo copia de seguridad) y "NDMP: restore only" (Sólo restauración) para eventos de copia de seguridad o restauración solamente.
Red	Eventos y fallos de puertos de red, enlaces de datos e interfaces IP.
Asistencia técnica remota	Eventos de carga de paquetes de asistencia.

Categoría	Descripción
Replicación remota	Eventos y fallos de envío y recepción. Este grupo está disponible como "Remote replication: source only" (Replicación remota: sólo origen) y "Remote replication: target only" (Replicación remota: sólo destino) sólo para eventos de origen o destino.
Fallos de servicios	Eventos de fallo del Capítulo 11, Servicios del dispositivo ZFSSA de software.
Umbrales	Alertas personalizadas basadas en estadísticas de "Análisis" de "Guía de análisis de Oracle ZFS Storage Appliance ".
Agrupación ZFS	Eventos de agrupación de almacenamiento, incluida la limpieza y la activación de discos de reserva.

Acciones de alerta admitidas

Se admiten las siguientes acciones.

Envío de correo electrónico

Se puede enviar un correo electrónico con los detalles de la alerta. La configuración requiere una dirección de correo electrónico y una línea de asunto del mensaje. A continuación se presenta un correo electrónico modelo basado en una alerta de umbral:

```
From aknobody@caji.com Mon Oct 13 15:24:47 2009
Date: Mon, 13 Oct 2009 15:24:21 +0000 (GMT)
From: Appliance on caji <noreply@caji.com>
Subject: High CPU on caji
To: admin@hostname.com

SUNW-MSG-ID: AK-8000-TT, TYPE: Alert, VER: 1, SEVERITY: Minor
EVENT-TIME: Mon Oct 13 15:24:12 2009
PLATFORM: i86pc, CSN: 0809QAU005, HOSTNAME: caji
SOURCE: svc:/appliance/kit/akd:default, REV: 1.0
EVENT-ID: 15a53214-c4e7-eae4-dae6-a652a51ea29b
DESC: cpu.utilization threshold of 90 is violated.
AUTO-RESPONSE: None.
IMPACT: The impact depends on what statistic is being monitored.
REC-ACTION: The suggested action depends on what statistic is being monitored.

SEE: https://192.168.2.80:215/#maintenance/alert=15a53214-c4e7-eae4-dae6-a652a51ea29b
```

Los detalles de la manera en la que el dispositivo envía los mensajes se pueden configurar en la pantalla del servicio "SMTP" [286].

Envío de captura SNMP

Se puede enviar una captura SNMP con los detalles de la alerta, si se configuró un destino de captura SNMP en el servicio “SNMP” [287] y el servicio está en línea. El siguiente ejemplo muestra una captura SNMP como se la ve desde el comando `snmptrapd -P` de la herramienta Net-SNMP:

```
# /usr/sfw/sbin/snmptrapd -P
2009-10-13 15:31:15 NET-SNMP version 5.0.9 Started.
2009-10-13 15:31:34 caji.com [192.168.2.80]:
        iso.3.6.1.2.1.1.3.0 = Timeticks: (2132104431) 246 days, 18:30:44.31
   iso.3.6.1.6.3.1.1.4.1.0 = OID: iso.3.6.1.4.1.42.2.225.1.3.0.1
   iso.3.6.1.4.1.42.2.225.1.2.1.2.36.55.99.102.48.97.99.100.52.45.51.48.
99.49.45.52.99.49.57.45.101.57.99.98.45.97.99.50.55.102.55.49.50.54.
98.55.57 = STRING: "7cf0acd4-30c1-4c19-e9cb-ac27f7126b79"
     iso.3.6.1.4.1.42.2.225.1.2.1.3.36.55.99.102.48.97.99.100.52.45.51.48.
99.49.45.52.99.49.57.45.101.57.99.98.45.97.99.50.55.102.55.49.50.54.
98.55.57 = STRING: "alert.ak.xmlrpc.threshold.violated"
       iso.3.6.1.4.1.42.2.225.1.2.1.4.36.55.99.102.48.97.99.100.52.45.51.
48.99.49.45.52.99.49.57.45.101.57.99.98.45.97.99.50.55.102.55.49.50.
54.98.55.57 = STRING: "cpu.utilization threshold of 90 is violated."
```

Envío de mensaje de Syslog

Se puede enviar un mensaje de Syslog con los detalles de la alerta a uno o varios sistemas remotos, si el servicio Syslog está activado. Consulte la documentación que describe el “Syslog Relay service” [291] para ver ejemplos de cargas útiles de Syslog y una descripción de cómo configurar los receptores de Syslog en otros sistemas operativos.

Reanudación/suspensión de conjunto de datos

Los “Conjuntos de datos” de “Guía de análisis de Oracle ZFS Storage Appliance ” de análisis se pueden reanudar o suspender. Esto resulta particularmente útil cuando se está haciendo un seguimiento de problemas de rendimiento esporádico y no es deseable activar los conjuntos de datos de manera continua.

Por ejemplo: imagine que observó un pico en la actividad de la CPU una o dos veces por semana y otros análisis indicaron una caída asociada en el rendimiento de NFS. Activa algunos conjuntos de datos adicionales, pero no tiene información suficiente para determinar cuál es el problema. Si pudiera activar NFS por nombre de host y los conjuntos de datos por nombre de archivo, comprendería la causa mucho mejor. Sin embargo, estos conjuntos de datos en particular pueden ser pesados, y dejarlos en funcionamiento continuo degradaría el rendimiento para todos. Es en este contexto que las acciones de reanudación y suspensión de conjuntos de datos pueden ser útiles. Se puede configurar una alerta de umbral para *reanudar* los NFS en pausa por nombre de host y juegos de datos por nombre de archivo sólo cuando se detecte algún pico en la actividad de la CPU. Se puede configurar una segunda alerta para *suspender* esos juegos de datos después de un intervalo breve de recolección de datos. El resultado final es que

se obtienen los datos necesarios sólo durante el problema y se minimiza el impacto sobre el rendimiento ocasionado por esta recopilación de datos.

Reanudación/suspensión de hoja de trabajo

Estas acciones se utilizan para reanudar o suspender en su totalidad "Hojas de trabajo abiertas" de "Guía de análisis de Oracle ZFS Storage Appliance " de análisis, que puede incluir muchos conjuntos de datos. Los motivos para hacer esto son similares a los de la reanudación y la suspensión de los conjuntos de datos.

Ejecución de flujo de trabajo

Los flujos de trabajo se pueden ejecutar de manera opcional como acciones de alerta. Para que un flujo de trabajo pueda ser elegible como acción de alerta, la acción `alert` del flujo de trabajo debe estar configurada con el valor `true`. Consulte "Flujos de trabajo como acciones de alerta" [443] para obtener información detallada.

Alertas de umbral

Estas alertas están basadas en las estadísticas de "Análisis" de "Guía de análisis de Oracle ZFS Storage Appliance ". Las siguientes propiedades se configuran durante la creación de las alertas de umbral:

TABLA 9-2 Propiedades de alertas de umbral

Propiedad	Descripción
Threshold	La estadística de umbral se toma de "Análisis" de "Guía de análisis de Oracle ZFS Storage Appliance ", y es autodescriptiva (por ejemplo, "Protocol: NFSv4 operations per second" [Protocolo: operaciones de NFSv4 por segundo]).
exceeds/falls below	Define el valor del umbral en comparación con la estadística actual.
Timing: for at least	Tiempo durante el cual el valor de la estadística actual debe exceder el umbral o estar por debajo de él.
only between/only during	Estas propiedades se pueden configurar para que el umbral se envíe sólo durante ciertas horas del día, por ejemplo, el horario comercial.
Repost alert every ... this condition persists.	Si se activa esta opción, se vuelve a ejecutar la acción de la alerta (por ejemplo, enviar un correo electrónico) cada intervalo definido mientras exista el incumplimiento del umbral.

Propiedad	Descripción
Also post alert when this condition clears for at least ...	Se envía una alerta de seguimiento si el incumplimiento del umbral se soluciona durante al menos el intervalo definido.

El cuadro de diálogo "Add Threshold Alert" (Agregar alerta de umbral) se organizó para que se pueda leer como si fuera un párrafo que describe la alerta. El texto predeterminado dice:

Threshold CPU: percent utilization exceeds 95 percent (CPU de umbral: el porcentaje de uso excede el 95%)

Timing for at least 5 minutes only between 0:00 and 0:00 only during weekdays (Tiempo: durante al menos 5 minutos sólo entre las 0:00 y las 0:00, sólo durante los días de entre semana)

Repost alert every 5 minutes while this condition persists (Volver a publicar alerta cada 5 minutos mientras continúe esa condición)

Also post alert when this condition clears for at least 5 minutes (Publicar alerta también cuando la condición se solucione durante al menos 5 minutos)

Configuración de alertas con la BUI

En la parte superior de la página Configuration (Configuración)->Alerts (Alertas) hay fichas para "Alert Actions" (Acciones de alertas) y "Threshold Alerts" (Alertas de umbral). Consulte Tareas para obtener instrucciones detalladas para configurarlas en la BUI.

▼ Agregación de una alerta de umbral

1. **Haga clic en el ícono para agregar ubicado al lado de "Threshold alerts" (Alertas de umbral).**
2. **Seleccione la estadística que desea supervisar. Puede usar "Estadísticas" de "Guía de análisis de Oracle ZFS Storage Appliance " para ver la estadística y comprobar si corresponde.**
3. **Seleccione excede/está por debajo y el valor deseado.**
4. **Escriba los detalles de tiempo. De forma predeterminada, la alerta se publica sólo si el umbral se ha incumplido durante al menos 5 minutos, se vuelve a publicar cada 5 minutos y se publica después de que el umbral se ha recuperado durante 5 minutos.**

5. **Seleccione la acción de alerta en el menú desplegable y complete los campos requeridos a la derecha.**
6. **Si lo desea, siga agregando acciones de alerta. Para ello, haga clic en el ícono de agregación que está al lado de Alert actions (Acciones de alerta).**
7. **Haga clic en APPLY (Aplicar) en la parte superior del cuadro de diálogo.**

▼ Agregación de una acción de alerta

1. **Haga clic en el ícono para agregar que se encuentra al lado de "Alert actions" (Acciones de alertas).**
2. **Seleccione la categoría o elija All events (Todos los eventos) para incluir todo.**
3. **Elija All Events (Todos los eventos) o Subset of Events (Subconjunto de eventos). Si selecciona la opción del subconjunto, personalice la lista de casillas de verificación para incluir los eventos de alerta deseados.**
4. **Use el menú desplegable de Alert actions (Acciones de alerta) para seleccionar el tipo de alerta.**
5. **Proporcione los detalles de la acción de alerta. Se puede hacer clic en el botón TEST (Probar) para crear una alerta de prueba y ejecutar esta acción de alerta (útil para comprobar si el correo electrónico o SNMP están bien configurados).**
6. **Se puede hacer clic en el ícono de agregación que se encuentra al lado de Alert actions (Acciones de alerta) para agregar varias acciones de alerta.**
7. **Haga clic en ADD (Agregar) en la parte superior derecha.**

Configuración de alertas con la CLI

Las alertas también se pueden configurar desde la CLI con el contexto `configuration alerts`. Consulte Tareas para obtener instrucciones detalladas para configurarlas en la CLI.

▼ Agregación de una alerta de umbral

1. **Introduzca el contexto `configuration alerts thresholds` y escriba el comando `create`.**

2. **Introduzca set statname=, donde [name es la estadística que se desea supervisar. Para determinar el nombre en la CLI, introduzca set statname= y presione la tecla de tabulación. Para obtener información detallada acerca de cada estadística, consulte “Estadísticas” de “Guía de análisis de Oracle ZFS Storage Appliance ” y haga clic en los nombres de las estadísticas.**

3. **Introduzca set limit=, donde `[number` es el umbral deseado.**

4. **Escriba `commit`. Tome nota del identificador "watch", que es el identificador del umbral, si más adelante desea agregar una acción de alerta para esta alerta de umbral.**

5. **Introduzca `list` para determinar el nombre, incluido el número, de la nueva alerta de umbral. Busque un umbral con el mismo límite y nombre de estadística que los que acaba de configurar.**

6. **Introduzca select threshold-, donde `[number` es el mismo número identificado en el paso anterior.**

7. **Introduzca `list`. De ser necesario, corrija ahora los argumentos. De manera predeterminada, los argumentos minimum post (Publicación mínima), frequency (Frecuencia) y minimum cleared (Mínimo sin problemas) se configuran con un valor de 5 minutos. Esto significa que las alertas se publican sólo si el umbral se ha incumplido durante al menos 5 minutos, se vuelve a publicar cada 5 minutos y se publica después de que el umbral se ha recuperado durante 5 minutos.**

8. **Introduzca `done` y, a continuación, introduzca `done` nuevamente.**

▼ Agregación de una acción de alerta

1. **Introduzca el contexto `configuration alerts actions` y escriba el comando `create`.**

2. **Introduzca `get category = (unset)` para ir a la propiedad "category" (Categoría).**

3. **Introduzca `set category=thresholds`.**

4. **Introduzca `set thresholdid=, donde [id es el identificador creado automáticamente para la alerta de umbral.`**

5. **Escriba `commit`.**

6. **Introduzca `list` para determinar el nombre, incluido el número, de la nueva acción de alerta. Búsqueda de umbrales sin acciones ni manejadores asignados.**

7. **Introduzca select actions-, donde `[number` es el mismo número identificado en el paso anterior.**

8. **Introduzca `action` y, a continuación, introduzca `get`.**

9. **De manera predeterminada, el tipo de alerta es email (Correo electrónico). Si es el tipo que desea configurar, siga con el próximo paso. De no ser así, introduzca set handler=, donde [type es `snmptrap`, `syslog`, `resumedataset`, `suspenddataset`, `resumeworksheet`, `suspendworksheet` o `executeworkflow`. A continuación, introduzca `get` para ver los argumentos necesarios. Sólo `snmptrap` y `syslog` no tienen argumentos.**

10. **Configure cada uno de los argumentos necesarios. Por ejemplo, para configurar una línea de asunto para las alertas por correo electrónico, introduzca set subject=, donde `[subject` es la línea de asunto de correo electrónico deseada.**

11. **Use el comando `show` para asegurarse de haber introducido todos los argumentos.**

12. **Introduzca `commit` y, a continuación, introduzca `list`. De ser necesario, corrija ahora los argumentos.**

13. **Introduzca `done` y, a continuación, introduzca `done` nuevamente.**

♦ ♦ ♦ CAPÍTULO 10

Configuración de cluster

El dispositivo Sun ZFS Storage Appliance admite la agrupación en clusters cooperativa de dispositivos. Esta estrategia 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 la redundancia de hardware de un solo dispositivo incorporada en todos los dispositivos Sun ZFS Storage Appliance.

La función de agrupación en clusters utiliza el acceso compartido a los recursos de almacenamiento. Para configurar la agrupación en clusters, ambos nodos principales deben ser del mismo modelo. Tenga en cuenta que el modelo 7420 (con CPU de 2 Ghz o 2,40 GHz) se basa en la misma plataforma y se puede agrupar en clusters con el modelo 7420 existente (con CPU de 1,86 GHz o 2,00 GHz).

Características y ventajas de los clusters

Es importante comprender el alcance de la implementación de agrupaciones en clusters de los dispositivos Sun ZFS Storage Appliance. El término "cluster" se usa en la industria para hacer referencia a numerosas tecnologías diferentes que tienen una variedad de propósitos. Aquí se utiliza para hacer referencia a un metasistema compuesto por dos nodos principales de dispositivos y almacenamiento compartido, que se emplea para proporcionar una mejor disponibilidad en caso de que uno de los nodos presente ciertos fallos de hardware o software. Un cluster contiene exactamente dos controladores de almacenamiento o dispositivos, a los que en este documento se hace referencia como *nodos principales*. Cada nodo principal puede tener asignada una recopilación de recursos de almacenamiento, red y otros recursos del conjunto disponible para el cluster, lo que permite la construcción de una de dos topologías principales. Muchas personas usan el término *activo-activo* para describir un cluster en el que hay dos (o más) agrupaciones de almacenamiento, una asignada a cada nodo principal, junto con recursos de red utilizados por los clientes para alcanzar los datos almacenados en esa agrupación, y el término *activo-pasivo* para hacer referencia a un cluster en el que un único grupo de almacenamiento se asigna al nodo principal designado como *activo* junto con sus interfaces de red asociadas. Ambas topologías son compatibles con Oracle ZFS Storage Appliance. La distinción entre ellas es artificial; no hay ninguna diferencia de software ni hardware entre ellas y se puede alternar libremente entre las dos con la simple agregación o destrucción de una agrupación de almacenamiento. En ambos casos, si uno de los nodos principales falla, el otro (el

par) toma el control de todos los recursos conocidos y proporciona los servicios asociados con esos recursos.

Como alternativa a tener que incurrir en horas o días de tiempo de inactividad mientras se repara el nodo principal, la agrupación en clusters permite al dispositivo que actúa como par proporcionar los servicios mientras se realiza la reparación o el reemplazo. Asimismo, los clusters admiten la actualización gradual del software, lo que puede reducir las interrupciones comerciales asociadas con la migración a software más reciente. Algunas tecnologías de agrupación en clusters tienen ciertas capacidades adicionales más allá de la mejora de la disponibilidad. El subsistema de agrupación en clusters Oracle ZFS Storage Appliance no está diseñado para proporcionarlas. En particular, no proporciona equilibrio de carga entre varios nodos principales, no mejora la disponibilidad en caso de fallo del almacenamiento, no ofrece a los clientes un espacio de nombres de sistema de archivos unificado entre varios dispositivos ni divide la responsabilidad de servicio en un área geográfica amplia con fines de recuperación ante desastres. Estas funciones también están fuera del alcance de este documento. Sin embargo, la familia de productos Oracle ZFS Storage Appliance y los protocolos de datos que ofrece admiten numerosas funciones y estrategias que pueden mejorar la disponibilidad:

- Capítulo 13, Replicación de datos, que se puede utilizar para la recuperación ante desastres en uno o varios sitios geográficamente remotos.
- Reflejo de datos en el cliente, que se puede llevar a cabo con LUN "iSCSI" [213] redundantes proporcionados por varios servidores de almacenamiento desde ubicaciones arbitrarias.
- Equilibrio de carga, que está incorporado en el protocolo "NFS" [208] y se puede proporcionar para otros protocolos mediante hardware o software externos (se aplica a datos de sólo lectura).
- Componentes de hardware redundantes, que incluyen fuentes de alimentación, dispositivos de red y controladores de almacenamiento.
- "Problemas" de "Manual de servicio del cliente de Oracle ZFS Storage Appliance ", software que puede identificar componentes con fallos, retirarlos de servicio y orientar a los técnicos para reparar o reemplazar el hardware correcto.
- Redundancia de tejido de red proporcionada por la funcionalidad LACP y "IPMP" [277].
- Dispositivos de almacenamiento redundante (RAID).

En las secciones correspondientes de este documento, se puede encontrar información adicional acerca de otras funciones de disponibilidad.

Desventajas de los clusters

Al decidir entre una configuración en clusters o independiente para el sistema Oracle ZFS Storage Appliance, es importante considerar los costos y los beneficios de la operación en clusters. En todo el sector informático, es práctica común considerar la agrupación en

clusters como una decisión de arquitectura automática, pero esta concepción refleja una vista idealizada de los riesgos y las recompensas de la agrupación en clusters promulgada por algunos proveedores del sector. Además del evidente mayor costo inicial y continuo de hardware y asistencia técnica asociado con el segundo nodo principal, el uso de la agrupación en clusters también impone riesgos técnicos y operativos adicionales. Algunos de estos riesgos se pueden mitigar asegurándose de que todo el personal esté bien capacitado en operaciones con clusters; otros son intrínsecos del concepto de la operación en clusters. Estos riesgos incluyen:

- El potencial de intolerancia de las aplicaciones con respecto a los comportamientos dependientes del protocolo durante la toma de control.
- La posibilidad de que el software del cluster en sí falle o induzca un fallo en otro subsistema que no habría ocurrido en la operación independiente.
- Aumento de la complejidad de gestión y mayor probabilidad de error de un operador al realizar tareas de gestión.
- La posibilidad de que se produzcan varios fallos o un error de operador grave que generen pérdida o daño de datos que no se habrían producido en una configuración independiente.
- Mayor dificultad para recuperarse de estados de software o hardware no anticipados.

Estos costos y riesgos son fundamentales, se aplican de una u otra forma a todos los productos agrupados en clusters o con capacidad para agruparse en clusters del mercado (incluido Oracle ZFS Storage Appliance) y no se pueden mitigar ni eliminar por completo. Los arquitectos de almacenamiento deben sopesarlos contra la principal ventaja de la agrupación en clusters: la oportunidad de reducir períodos de no disponibilidad de horas o días a minutos o menos en el extraño evento de un fallo catastrófico de hardware o software. El hecho de que el análisis de la relación costo-beneficio favorezca o no el uso de la agrupación en clusters en una implementación del sistema Oracle ZFS Storage Appliance dependerá de factores locales, como condiciones de SLA, personal de asistencia técnica disponible y sus cualificaciones, limitaciones presupuestarias, la probabilidad percibida de diversos fallos posibles y la idoneidad de estrategias alternativas para mejorar la disponibilidad. Estos factores dependen mucho del sitio, la aplicación y la empresa, y se los debe evaluar caso por caso. La comprensión del material detallado en lo que resta de esta sección lo ayudará a hacer las elecciones apropiadas durante el diseño y la implementación de su infraestructura de almacenamiento unificado.

Terminología de clusters

Los términos definidos aquí se utilizan en todo el documento. En la mayoría de los casos, se explican en mayor contexto y detalle junto con los conceptos más amplios que los abarcan. En la siguiente sección, se describen los tipos de recursos y los estados de un cluster. Consulte esta sección cada vez que lo necesite.

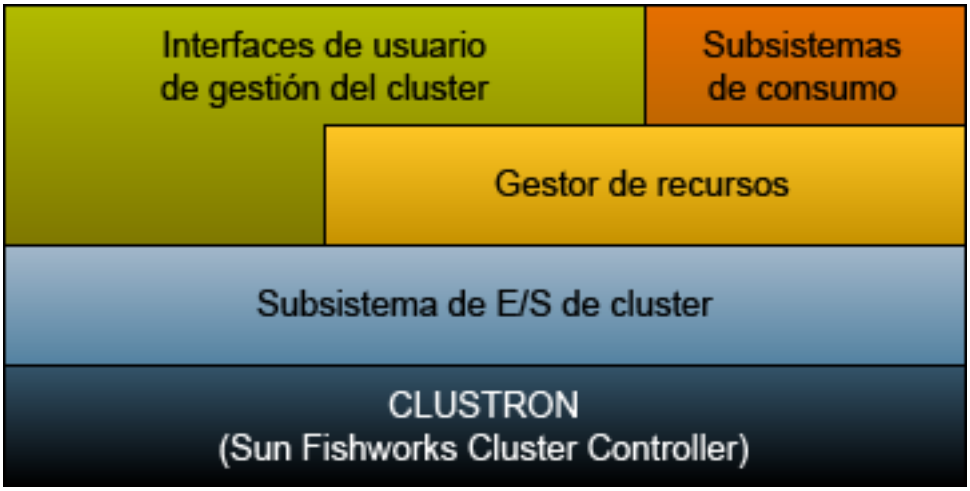
- Exportar: proceso de hacer que un recurso quede inactivo en un nodo principal particular.
- Failback: proceso de pasar del estado AKCS_OWNER al estado AKCS_CLUSTERED, en el que todos los recursos externos (los que se asignaron al par) son exportados y luego importados por el par.

- Importar: proceso de hacer que un recurso esté activo en un nodo principal particular.
- Par: el otro dispositivo de un cluster.
- Volver a unir: recuperar y volver a sincronizar el mapa de recursos del par.
- Recurso: objeto físico o virtual presente, y posiblemente activo, en uno o ambos nodos principales.
- Toma de control: proceso de 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

El subsistema de agrupación en clusters incorporado en la serie está compuesto por tres bloques de creación principales (ilustración 1). El subsistema de E/S del cluster y el dispositivo de hardware proporcionan el transporte para la comunicación entre los nodos principales del cluster y son responsables de la supervisión del estado del par. Este transporte es utilizado por el gestor de recursos, que permite a los proveedores de servicios de datos y otros subsistemas de gestión interaccionar con el sistema de agrupación en clusters. Finalmente, las interfaces de usuario de gestión del cluster proporcionan las operaciones de tareas de configuración, asignación de recursos, supervisión, y failback y toma de control. Cada uno de estos componentes se describe en detalle en las siguientes secciones.

FIGURA 10-1 Subsistema de agrupación en clusters



E/S de interconexión del cluster

Todas las comunicaciones entre los nodos principales constan de uno o varios mensajes transmitidos por uno de los tres enlaces de E/S del cluster proporcionados por el hardware CLUSTRON (como se muestra en la siguiente ilustración). Este dispositivo ofrece dos enlaces serie de baja velocidad y un enlace Ethernet. El uso de los enlaces serie ofrece una mayor fiabilidad, ya que puede suceder que los enlaces Ethernet no reciban servicio con rapidez suficiente cuando el sistema está bajo condiciones de carga extrema. La falsa detección de fallos y la toma de control no deseada son las peores maneras en las que un sistema en cluster puede responder a la carga. Durante la toma de control, no se responderán las solicitudes, sino que quedarán en la cola de los clientes, lo que genera una avalancha de solicitudes demoradas después de la toma de control que se suman a la carga ya intensa. Los enlaces serie utilizados por los dispositivos Oracle ZFS Storage Appliance no son susceptibles a este modo de error. El enlace Ethernet proporciona un transporte de mayor rendimiento para los mensajes sin latido, como la sincronización para volver a unirse, y proporciona un latido de respaldo.

Los tres enlaces se forman con cables EIA/TIA-568B (8 cables, Gigabit Ethernet) rectos comunes. Para poder utilizar cables rectos entre dos controladores idénticos, los cables se deben utilizar para conectar sockets opuestos de los dos conectores, como se muestra a continuación en la sección de cableado.

FIGURA 10-2 Puertos de E/S de cluster de controladores ZS3-2

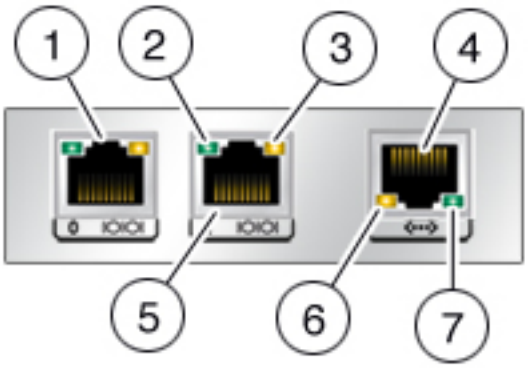


TABLA 10-1 Puertos de E/S de cluster de controladores ZS3-2

Componentes mostrados en la figura			
1 Serie 0	2 LED de actividad serie	3 LED de estado serie	4 Ethernet

Componentes mostrados en la figura			
5 Serie 1	6 LED de estado de Ethernet	7 LED de actividad de Ethernet	

FIGURA 10-3 Puertos de E/S de cluster de controladores ZS3-4 y 7x20

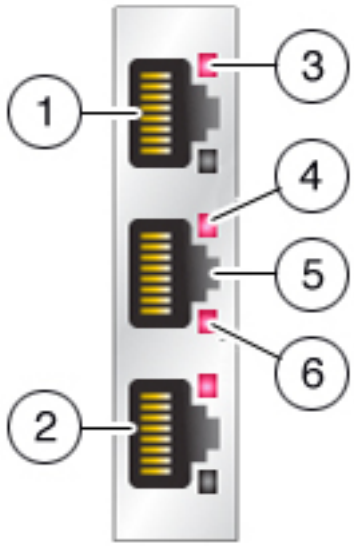


Figure 2. Puertos de E/S de cluster de controladores ZS3-4 y 7x20

TABLA 10-2 Puertos de E/S de cluster de controladores ZS3-4 y 7x20

Componentes mostrados en la figura			
1 Serie 1	2 Serie 0	3 LED de estado serie	4 LED de estado de Ethernet
5 Ethernet	6 LED de actividad de Ethernet		

Los nodos principales en clusters únicamente se comunican entre sí mediante una red privada segura establecida por las interconexiones del cluster y nunca mediante interfaces de red previstas para servicio o administración. El mensaje pertenecerá a una de dos categorías

generales: los latidos regulares utilizados para detectar el fallo de un nodo principal 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 los tres enlaces. Se transmiten de manera continua a intervalos fijos y nunca se confirma su recepción ni se retransmiten, ya que todos los latidos son idénticos y no contienen información exclusiva. Por cualquiera de los enlaces, se puede enviar otro tipo de tráfico; normalmente se utiliza el enlace que esté disponible más rápido en el momento de la transmisión. La recepción de este tráfico se confirma, el tráfico se verifica y se lo retransmite según sea necesario para mantener un transporte confiable para el software de nivel superior.

Independientemente de su tipo u origen, cada mensaje se envía como un único paquete de 128 bytes y contiene una carga útil de datos de 1 a 68 bytes y un número hash de verificación de 20 bytes para asegurar la integridad de los datos. Los enlaces serie funcionan a 115200 bps con 9 bits de datos y un único bit de inicio y fin; el enlace Ethernet funciona a 1 Gbps. Por lo tanto, la latencia de mensaje efectiva en los enlaces serie es de aproximadamente 12,2 ms. La latencia de Ethernet varía mucho. Si bien las latencias típicas son del orden de los microsegundos, las latencias efectivas para el software de gestión del dispositivo pueden ser mucho mayores debido a la carga del sistema.

Normalmente, cada uno de los nodos principales del cluster envía mensajes de latidos por los tres enlaces de E/S a 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 presentó un fallo. Si se produce un fallo en los tres enlaces, se supone que el fallo es del par y se realiza el arbitraje de la toma de control. En el caso de un aviso grave, el nodo principal que falla transmite un único mensaje de notificación por cada uno de los enlaces serie, y el 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 ha fallado 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 descritos en esta sección son fijos; el dispositivo Oracle ZFS Storage Appliance no ofrece la capacidad de ajustar estos parámetros (ni tampoco hay necesidad de hacerlo). Se consideran como detalles de implementación y se los incluye aquí sólo con fines informativos. Se pueden cambiar sin aviso en cualquier momento.

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 condiciones de "separación de redes"” [180].

Descripción de gestión de recursos del cluster

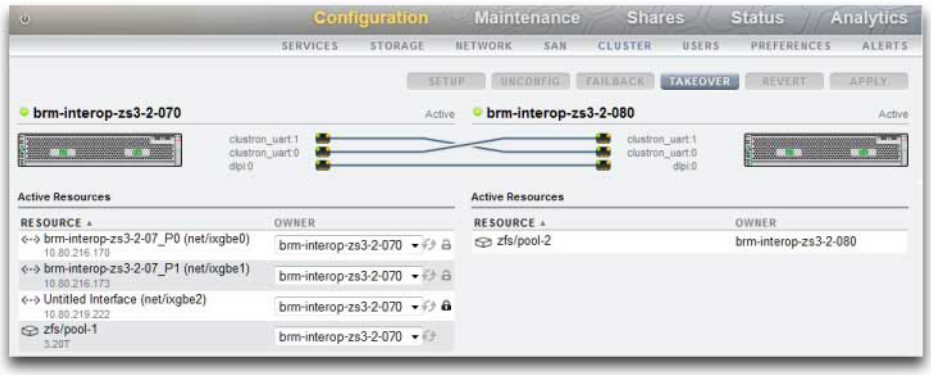
El gestor de recursos es responsable de garantizar que se haya conectado el conjunto correcto de interfaces de red, que estén activas las agrupaciones de almacenamiento correctas y que los numerosos parámetros de configuración permanezcan sincronizados entre dos nodos principales en clusters. La mayoría de las actividades de este subsistema son invisibles para los administradores. Sin embargo, hay un aspecto importante que queda expuesto. 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 por clase de recurso; por ejemplo, una interfaz de red pertenece a la clase neta y está activa cuando se levanta la interfaz. Los tres tipos más importantes de recursos son único, privado y réplica.

Las réplicas son el tipo más simple: no se exponen nunca a los administradores y no aparecen en la pantalla de configuración del cluster (ilustración 4). Las réplicas existen siempre y están siempre activas en ambos nodos principales. Normalmente, estos recursos simplemente actúan como contenedores de propiedades de servicio que se deben sincronizar entre los dos nodos principales.

Al igual que las réplicas, los recursos únicos se utilizan para sincronizar el estado, pero están siempre activos en exactamente uno de los nodos principales. Los administradores pueden elegir el nodo principal en el que cada recurso único normalmente debe estar activo; si ese nodo principal presenta un fallo, el par importa el recurso único. Los recursos únicos son la clave para las características de disponibilidad de la agrupación en clusters: son los recursos que los usuarios se suelen imaginar como que pasan de un nodo principal que falló al par superviviente e 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 conjunto de servicios de almacenamiento, es fundamental que se asigne a cada interfaz el mismo nodo principal que los clientes de la agrupación de almacenamiento esperan ver al acceder a las direcciones de esa interfaz. En la ilustración 4, todas las direcciones asociadas con la interfaz PrimaryA siempre serán provistas por el nodo principal que importó pool-0, mientras que las direcciones asociadas con PrimaryB siempre serán provistas por el mismo nodo principal que pool-1.

Los recursos privados son conocidos sólo por el nodo principal al que se asignan y nunca se toma el control de ellos al producirse un fallo. Esto suele resultar útil sólo para las interfaces de red. Consulte el siguiente análisis de casos de uso específicos.

FIGURA 10-4 Ejemplo de agrupación en clusters ZS3-2



Hay otros tipos de recursos, pero son detalles de implementación que no se muestran a los administradores. Uno de estos tipos es el simbionte, que permite a un recurso seguir a otro cuando se importa y exporta. El uso más importante de este tipo de recursos es para la representación de los discos y los dispositivos flash de la agrupación de almacenamiento. Estos recursos se conocen como conjuntos de discos y se deben importar siempre antes de la agrupación ZFS que contienen. Cada conjunto de discos está formado por la mitad de los discos de un contenedor de almacenamiento externo. Un sistema de almacenamiento en cluster puede tener conectada la cantidad de conjuntos de discos que se desee (según lo que admita el hardware), y cada agrupación ZFS se forma a partir de los dispositivos de almacenamiento de uno o varios conjuntos de discos. Como los conjuntos de discos pueden contener dispositivos ATA, se deben importar y exportar explícitamente para evitar ciertos comportamientos relacionados con la afiliación específicos de los dispositivos ATA que se utilizan en entornos de rutas múltiples. La representación de los discos como recursos proporciona una manera simple de realizar estas actividades en el momento correcto. Cuando un administrador configura o cambia el propietario de una agrupación de almacenamiento, la asignación del propietario de los conjuntos de discos asociados con la agrupación se cambia de manera transparente al mismo tiempo. Como todos los simbiontes, los recursos de los conjuntos de discos no aparecen en la interfaz de usuario de la configuración del cluster.

TABLA 10-3 Gestión de recursos de clusters

Recurso	ícono	Omnipresente	Toma de control cuando hay un fallo
ÚNICO		No	Sí
RÉPLICA	Ninguno	Sí	N/D
PRIVADO		No	No

Recurso	ícono	Omnipresente	Toma de control cuando hay un fallo
SIMBIONTE	Ninguno	Mismo tipo que el principal	Mismo tipo que el principal

Cuando se crea un nuevo recurso, inicialmente se lo asigna al nodo principal en el que se está creando. El propietario no se puede cambiar a menos que el nodo principal se encuentre en el estado AKCS_OWNER. Por lo tanto, es necesario crear recursos en el nodo principal que debería ser su propietario o tomar el control antes de cambiar la propiedad del recurso. Por lo general, es posible destruir los recursos de cualquier nodo principal, pero no se pueden destruir las agrupaciones de almacenamiento que se exportan. Los mejores resultados normalmente se obtienen destruyendo recursos en el nodo principal que los controla en ese momento, sin importar qué nodo principal 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 nodos principales. Por lo tanto, nunca es necesario configurar estos parámetros en ambos nodos principales, independientemente del estado del cluster. Si un dispositivo no está funcionando cuando se hace el cambio de configuración, se replicará en el otro cuando se vuelva a unir al cluster en el siguiente inicio, antes de proporcionar servicios. Existen algunas excepciones:

- Las definiciones y las opciones de recursos compartidos y LUN se pueden configurar sólo en el nodo principal que tiene el control de la agrupación subyacente, sin importar cuál sea el nodo principal al que se suele asignar la agrupación.
- La configuración del servicio "Identity" (Identidad) (es decir, el nombre y la ubicación del dispositivo) no se replica.
- Los nombres proporcionados al chasis son visibles sólo en el nodo principal al que fueron asignados.
- Cada ruta de red está vinculada a una interfaz específica. Si cada nodo principal 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 nodos principales. Consulte la sección sobre consideraciones para redes si desea obtener información más detallada.
- Las claves de host SSH no se replican y nunca se comparten. Por lo tanto, si no se ha configurado ninguna interfaz administrativa privada, se puede esperar que haya discrepancias en las claves al intentar iniciar sesión en la CLI con una dirección asignada a un nodo que ha fallado. Las mismas limitaciones se aplican a los certificados SSL utilizados para acceder a la BUI.

Así, el modelo básico es que la configuración común se replica de manera transparente, y los administradores asignan una recopilación de recursos a cada nodo principal del dispositivo. Esas asignaciones de recursos a su vez forman la vinculación 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.

Toma de control y failback en clusters

Los nodos principales en clusters pueden estar en uno de una pequeña cantidad de estados posibles en cualquier momento dado:

TABLA 10-4 Estados de un cluster

Estado	Ícono	Expresión de la CLI/BUI	Descripción
Sin configurar		La agrupación en clusters no está configurada	Sistema que no está agrupado en clusters en este estado. El sistema se está configurando o la tarea de configuración del cluster nunca se completó.
Propietario		Activo (toma de control completada)	La agrupación en clusters está configurada, y este nodo ha tomado el control de todos los recursos compartidos del cluster. El sistema pasa a este estado inmediatamente después de que se completa la configuración del cluster desde la interfaz del usuario y cuando detecta que el par ha fallado (es decir, después de una toma de control). Permanece en este estado hasta que un administrador ejecuta manualmente una operación de failback.
Segmentado		Listo (esperando failback)	La agrupación en clusters está configurada, y este nodo no controla ninguno de los recursos compartidos. El sistema se segmenta inmediatamente después de que se completa la configuración del cluster desde la interfaz del usuario del otro nodo o después de un reinicio, desconexión de la fuente de alimentación o algún otro fallo. El nodo

Estado	Ícono	Expresión de la CLI/BUI	Descripción
			permanece en este estado hasta que un administrador ejecuta manualmente una operación de failback.
En cluster		Activo	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...	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.
-		Desconocido (desconectado o reiniciando)	El dispositivo par está apagado o se está reiniciando, todos los enlaces de interconexión del cluster están inactivos o todavía no se configuró la agrupación en clusters.

Las transiciones entre estos estados tienen lugar como parte de dos operaciones: toma de control y failback.

La toma de control puede ocurrir en cualquier momento. Como ya se explicó, la toma de control se intenta cuando se detecta un fallo en el par. También se puede iniciar manualmente desde la CLI o la BUI de configuración del cluster. Esto resulta útil para hacer pruebas y realizar actualizaciones de software graduales (actualizaciones en las que se actualiza uno de los nodos principales mientras el otro proporciona los servicios con el software anterior, y a continuación se actualiza el segundo nodo principal una vez que se haya validado el nuevo software). Finalmente, la toma de control se realiza cuando uno de los nodos principales se inicia y detecta que su par está ausente. Esto permite que se reanude el servicio con normalidad cuando uno de los nodos principales falla de manera permanente o cuando ambos nodos principales pierden temporalmente la fuente de alimentación.

El failback nunca se realiza de manera automática. Cuando se repara e inicia un nodo principal que ha fallado, se vuelve a unir al cluster (resincroniza su vista de todos los recursos, sus

propiedades y su propietario) y espera a que un administrador realice la operación de failback. Hasta ese momento, el nodo principal original superviviente continúa proporcionando todos los servicios. Esto permite llevar a cabo una investigación completa del problema que ocasionó la toma de control, validar alguna nueva revisión del software o realizar otras tareas administrativas antes de que el nodo principal regrese al servicio de producción. Como el failback interrumpe la actividad de los clientes, se debe programar en función de las necesidades y los procesos específicos de la empresa. Hay una excepción: Supongamos que el nodo principal A falla y que el nodo principal B toma el control. Cuando el nodo principal A se vuelve a unir al cluster, puede tomar el control si detecta que el nodo principal B está ausente o ha fallado. El principio es que siempre es mejor proporcionar servicio que no hacerlo, aun cuando todavía no se haya podido investigar el problema original. De manera que si nunca se realizará automáticamente un failback a un nodo principal que haya fallado, sí es posible que se realice una toma de control en cualquier momento.

Cuando configura un cluster, el estado inicial tiene el nodo que inició la configuración en el estado Propietario y el otro nodo en el estado Segmentado. Después de realizar una operación inicial de failback para entregar al nodo Segmentado su porción de los recursos compartidos, ambos nodos pasan al estado En cluster. Si se apagan ambos nodos del cluster o se produce un fallo en ellos, cuando vuelvan a iniciar simultáneamente se llevará a cabo un arbitraje y uno de ellos tomará el estado Propietario y el otro el estado Segmentado.

Durante el failback, se exportan todos los recursos externos (los asignados al par) y, a continuación, son importados por el par. Una agrupación no se puede importar porque el estado de fallo haría que el nodo Segmentado se reinicie. Si se intenta realizar failback con una agrupación que tiene un fallo, el nodo Segmentado puede reiniciarse a causa del fallo de importación.

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. Mientras que las propiedades de los recursos compartidos y los LUN se almacenan con los datos de usuario en la agrupación de almacenamiento (de manera que están siempre accesibles para el propietario actual del recurso de almacenamiento), la configuración de los servicios se almacena en cada nodo principal. Para garantizar que ambos nodos principales proporcionen un servicio coherente, es necesario sincronizar todas las propiedades de los servicios cuando se produce algún cambio o cuando uno de los nodos principales 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 nodos principales.

Por lo tanto, no es necesario (y de hecho, es redundante) 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 nodos principales del cluster una vez que se haya completado la configuración inicial. Tenga en cuenta también que el

proceso de la configuración inicial del cluster replica la configuración existente en el par recientemente configurado. Por lo general, hay dos prácticas recomendadas para hacer cambios en la configuración de un cluster:

- Hacer todos los cambios de configuración relacionados con el almacenamiento y la red en el nodo principal que actualmente controla (o que 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 nodos principales, no en los dos. La política del sitio debería especificar cuál de los nodos principales se debe considerar como el *maestro* en este aspecto, y, a su vez, debería depender de cuál de los nodos principales está funcionando y la cantidad de agrupaciones de almacenamiento que se han configurado. Tenga en cuenta que el software del dispositivo no hace esta distinción.

Se exagera mucho acerca de la incidencia del problema de la *amnesia*, que es cuando se hacen cambios de configuración separados en cada nodo y posteriormente se pierden cuando el par no está funcionando. Esto es particularmente así en Oracle ZFS Storage Appliance, que no tiene ningún mecanismo para hacer cambios independientes en la configuración del sistema de cada nodo principal. Esta simplificación alivia bastante la necesidad de tener repositorios de configuración centralizados y favorece un enfoque más simple: se supone que el nodo principal que está en funcionamiento en un momento dado tiene la configuración correcta, de manera que el par se sincroniza con ese nodo principal al iniciarse. Si bien puede haber mejoras futuras del producto que permitan la selección de una política alternativa para resolver divergencias de configuración, este enfoque básico es simple y fácil de comprender: el segundo nodo principal adopta un conjunto de parámetros de configuración que ya están en uso en el sistema de producción existente (y, por lo tanto, es muy probable que sean correctos). Para garantizar que esto sea siempre así, los administradores deben asegurarse de que el nodo principal que falle vuelva a unirse al cluster en cuanto se repare.

Consideraciones de la agrupación en clusters para almacenamiento

Al evaluar un sistema Oracle ZFS Storage Appliance para utilizarlo en un cluster, hay otras dos consideraciones importantes. Tal vez la decisión más importante sea si el propietario de todas las agrupaciones de almacenamiento será el mismo nodo principal o si se dividirá entre los dos. Ambas opciones tienen varias ventajas y desventajas, como se muestra en la siguiente tabla. Por lo general, las agrupaciones se deben configurar en un único nodo principal, excepto cuando se esté optimizando la configuración para el rendimiento durante el funcionamiento nominal o cuando no sea relevante el rendimiento en caso de failover. Los cambios exactos en las características de rendimiento en el estado de failover dependerán en gran medida de la naturaleza y el tamaño de las cargas de trabajo. Por lo general, cuanto más cerca esté un nodo principal 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 nodo. Naturalmente, si hay varias agrupaciones, esta degradación corresponderá a ambas cargas de trabajo.

Tenga en cuenta que en cualquiera de las dos configuraciones, los dispositivos ReadZilla se pueden utilizar solo cuando la agrupación a la que fueron asignados se importa en el nodo principal propietario de esa agrupación. Es decir, cuando se tome el control de una agrupación debido a un fallo en el nodo principal, el almacenamiento en caché de lectura no estará disponible para esa agrupación aunque el nodo que la importó también tenga dispositivos ReadZilla sin utilizar instalados. Por este motivo, los dispositivos ReadZilla que pertenezcan a un cluster activo-pasivo deben configurarse como se describe en la documentación Capítulo 5, Configuración del almacenamiento. Esto no se aplica a los dispositivos LogZilla, que se encuentran en el tejido de almacenamiento y son siempre accesibles para el nodo que haya importado la agrupación.

TABLA 10-5 Consideraciones de la agrupación en clusters para almacenamiento

Variable	Propietario de nodo único	Varias agrupaciones con diferentes nodos 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: sólo un nodo 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 nodo 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 nodo 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 (failover)	ReadZilla no está disponible durante la operación de failover, 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.	ReadZilla no está disponible durante la operación de failover, 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 nodo. Esto se debe a que en el nodo 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 nodo se aproximan a la capacidad máxima del nodo, las latencias en el estado conmutado por error pueden ser extremadamente altas.

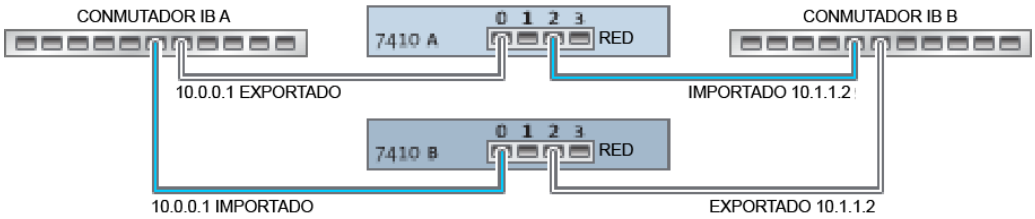
Variable	Propietario de nodo único	Varias agrupaciones con diferentes nodos como propietario
Flexibilidad de almacenamiento	Todo el almacenamiento físico disponible puede ser utilizado por los recursos compartidos y los LUN.	Sólo el almacenamiento asignado a una agrupación en particular puede ser utilizado 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 nodo principal se pueden utilizar mientras ese nodo esté brindando servicio.	Sólo la mitad de los dispositivos de red de cada nodo principal se pueden utilizar mientras ese nodo esté brindando servicio. Por lo tanto, cada agrupación se puede conectar sólo a la mitad de las redes físicamente separadas existentes.

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

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 nodos principales 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.

FIGURA 10-5 Agrupación en clusters para redes



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 nodo a la vez. De manera similar, los dispositivos correspondientes de cada nodo deben estar conectados a las mismas redes para que el servicio se proporcione en un estado conmutado por error. En el diagrama previo se muestra un ejemplo.

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 nodos. Como los identificadores de los dispositivos dependen del tipo de dispositivo y el orden en el que el dispositivo los detectó originalmente, los nodos principales en clusters DEBEN tener instalado hardware idéntico. Cada una de las ranuras de ambos nodos debe completarse con hardware idéntico y se las debe completar en el mismo orden en ambos nodos. 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. En el gestor de recursos las rutas se representan como simbiontes y pueden pasar al modo activo sólo cuando las interfaces a las que están vinculadas están en estado operativo. Por lo tanto, una ruta vinculada a una interfaz que actualmente está en el modo de energía en espera (exportada) no tiene efecto hasta que se active 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 un enrutador que es utilizado por los dispositivos para alcanzar una o varias redes adicionales, se debe configurar una ruta separada (por ejemplo, una segunda ruta predeterminada) y se la 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 sólo para administración a cada nodo principal de los clusters (probablemente sobre una red de gestión dedicada) y designar la interfaz como recurso privado. Esto garantiza que sea posible alcanzar un nodo 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 nodo no esté proporcionando el 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 nodo desde la consola del sistema.

Si no se realiza ninguna de estas acciones, es imposible gestionar o supervisar un nodo recientemente iniciado hasta que se complete el failback. Tal vez sea conveniente supervisar o gestionar el nodo principal que proporciona el servicio para una agrupación de almacenamiento en particular. Es probable que sea útil cuando desee modificar algún aspecto del almacenamiento en sí, por ejemplo, modificar una propiedad de un recurso compartido o 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 nodo que la agrupación que se utiliza para gestionar.

Interfaces IP locales privadas

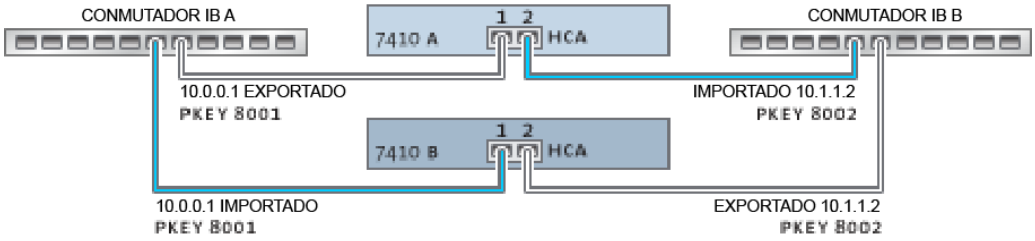
Use las siguientes directrices al crear interfaces IP locales privadas:

- Si se crea una interfaz IP con el mismo nombre que una interfaz IP privada de un par de un cluster, se produce la creación local de una interfaz IP privada.
- Los enlaces de datos que están siendo utilizados por las interfaces privadas del par no se pueden suprimir, de manera que 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 nodo principal. 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 sólo 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 Cluster:Resources (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 Cluster:Resources (Recursos del cluster) porque este tipo o propiedad no se puede modificar.

Consideraciones de la agrupación en clusters para 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.

FIGURA 10-6 Consideraciones de la agrupación en clusters para InfiniBand

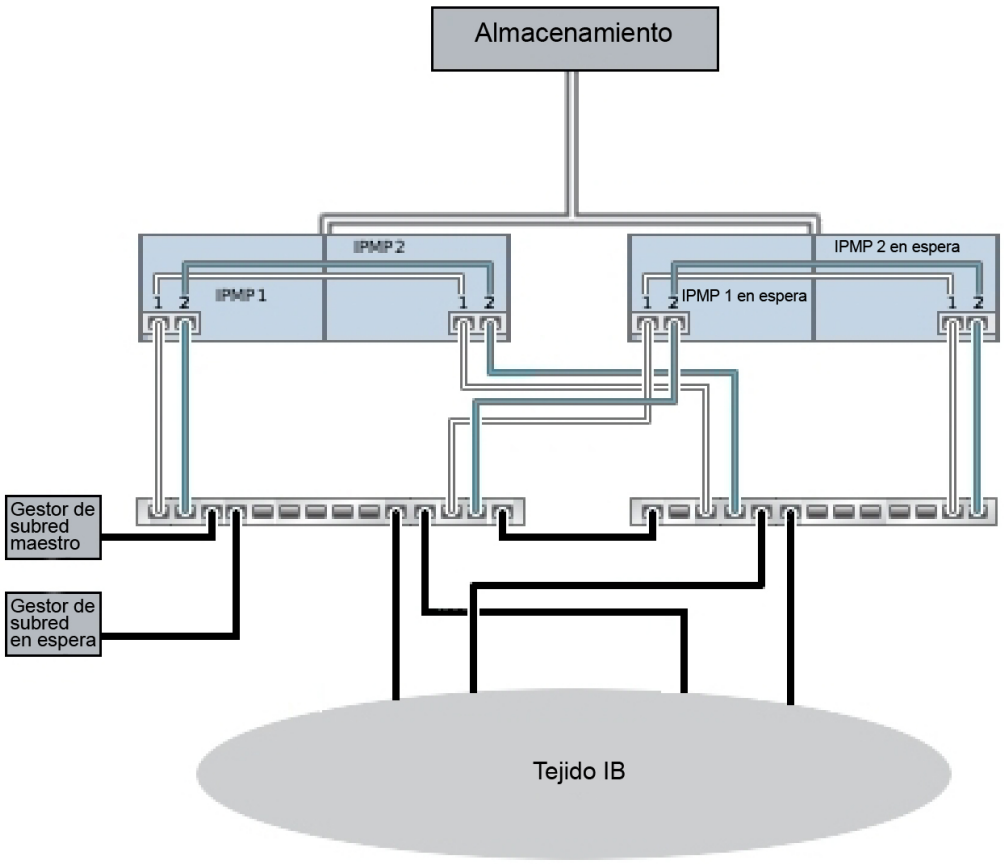


Para garantizar la configuración adecuada del cluster, cada nodo se debe completar con adaptadores de canal de host idénticos en ranuras idénticas. Asimismo, cada puerto de adaptador de canal de host correspondiente debe configurarse en la misma partición (pkey) del gestor de subred con privilegios de pertenencia idénticos y debe conectarse a la misma red. Para reducir la complejidad y garantizar una redundancia correcta, se recomienda que cada puerto pertenezca sólo 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 las configura como recurso único, todos los enlaces de datos y los dispositivos de la partición IB utilizados para construir una interfaz pueden estar activos solamente en un nodo en cualquier momento dado. En la ilustración anterior, se muestra un ejemplo específico. Los cambios de pertenencia a la partición de los puertos correspondientes se deben realizar al mismo tiempo y de una manera que sea coherente con las reglas de agrupación en clusters mencionadas. Su proveedor o representante de servicio autorizado de Oracle lo ayudará a planificar actualizaciones de hardware que cumplan con estos requisitos.

Situaciones de ruta redundante de agrupación en clusters

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

FIGURA 10-7 Configuración de clusters para redundancia de gestor de subred



Prevención de condiciones de "separación de redes"

Un modo de fallo común en los sistemas en clusters es el que se conoce como *separación de redes* (split-brain), donde cada uno de los nodos principales en clusters cree que su par ha fallado e intenta tomar el control. Sin lógica adicional, esta condición puede causar una amplia gama de comportamientos inesperados y destructivos cuyo diagnóstico o corrección pueden ser difíciles. El disparador canónico de esta condición es el fallo del medio de comunicación compartido entre los nodos principales; en el caso de Oracle ZFS Storage Appliance, esto

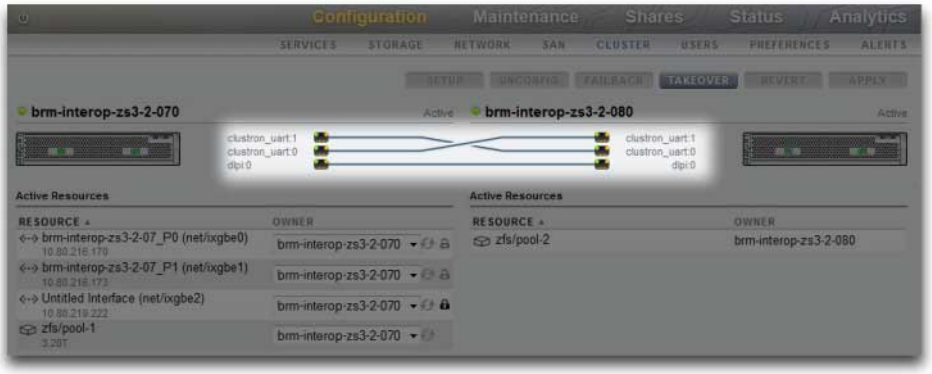
ocurriría si se produjera un fallo en los enlaces de E/S del cluster. Además de la redundancia incorporada de enlace triple (se necesita sólo un enlace para evitar que se active la toma de control), el software del dispositivo también realiza un procedimiento de arbitraje para determinar cuál es el nodo que debe continuar con la toma de control.

Hay una serie de mecanismos de arbitraje que son utilizados por productos similares; normalmente requieren el uso de *discos de quórum* (que usan reservas SCSI) o *servidores de quórum*. Para que sea posible utilizar discos ATA sin necesidad de hardware adicional, Oracle ZFS Storage Appliance utiliza un enfoque diferente que recurre al tejido del almacenamiento en sí para proporcionar la exclusividad mutua requerida. El proceso de arbitraje consiste en intentar ejecutar un comando SAS ZONE LOCK en cada uno de los expansores SAS visibles en el tejido de almacenamiento, en un orden predefinido. El dispositivo que logre obtener correctamente todos los bloqueos tomará el control, mientras que el otro se restablecerá de manera automática. Como un dispositivo en clusters que se inicia y detecta que no se puede comunicar con su par intenta tomar el control y llevar a cabo el mismo proceso de arbitraje, se restablecerá continuamente hasta que se restaure al menos uno de los enlaces de E/S del cluster. Esto garantiza que un fallo subsiguiente del otro nodo no ocasione una interrupción prolongada. Estos bloqueos de la zona SAS se liberan cuando se realiza la operación de failback o aproximadamente 10 segundos desde que el nodo cuyo estado es AKCS_OWNER renueva su propio acceso al tejido de almacenamiento.

Este mecanismo de arbitraje es simple, económico y no requiere hardware adicional, pero requiere que los dos dispositivos en clusters tengan acceso al menos a un expansor SAS común en el tejido de almacenamiento. En condiciones normales, cada dispositivo tiene acceso a todos los expansores, de manera que el arbitraje consistirá en la toma de al menos dos bloqueos de zona SAS. Sin embargo, es posible concebir situaciones de fallos múltiples en las que los dispositivos no tienen acceso a ningún expansor común. Por ejemplo, si se extraen dos de los cables SAS o si se apaga un disco JBOD, cada dispositivo tendrá acceso a subconjuntos separados de expansores. En este caso, cada dispositivo podrá bloquear correctamente todos los expansores a los que tiene acceso, concluirá que el par ha fallado e intentará proceder con la toma de control. Esto puede generar bloqueos irrecuperables debido a conflictos de afiliación de discos y/o daño grave de los datos.

Tenga en cuenta que si bien las consecuencias de esta condición son graves, se puede producir solamente si hay varios fallos (con frecuencia sólo en el caso de 4 fallos o más). La solución de agrupación en clusters incrustada en Oracle ZFS Storage Appliance está diseñada para garantizar que no haya un único punto de fallo y proteger tanto los datos como la disponibilidad contra todo fallo posible sin agregar costos ni complejidad innecesarios en el sistema. Sigue siendo posible que se produzcan varios fallos masivos que ocasionen la pérdida de servicio o datos, de la misma manera en la que ningún diseño RAID puede proteger contra una cantidad ilimitada de fallos de discos.

FIGURA 10-8 Prevención de separación de redes



Afortunadamente, la mayoría de estas situaciones de fallo se producen a causa de errores humanos y son completamente prevenibles con la instalación correcta del hardware y la capacitación del personal en relación con las mejores prácticas para la configuración y la gestión de clusters. Los administradores deben asegurarse siempre que los tres enlaces de E/S del cluster estén conectados y funcionen (como se muestra en la ilustración) y que todos los cables del almacenamiento estén conectados como se muestra en el diagrama de configuración que se incluye con los dispositivos. Es particularmente importante que se detecten dos rutas a cada JBOD (como se muestra en la ilustración) antes de pasar el cluster a producción y que esas rutas estén disponibles en todo momento de allí en más, con la excepción evidente de cambios transitorios de cables para aumentar la capacidad o reemplazar componentes con fallos. Los administradores deben utilizar alertas para supervisar el estado de los enlaces de interconexión del cluster y las rutas JBOD y corregir con rapidez los fallos que puedan producirse. Garantizando la conectividad adecuada, se protege tanto la disponibilidad como la integridad de los datos si falla algún componente de hardware o software.

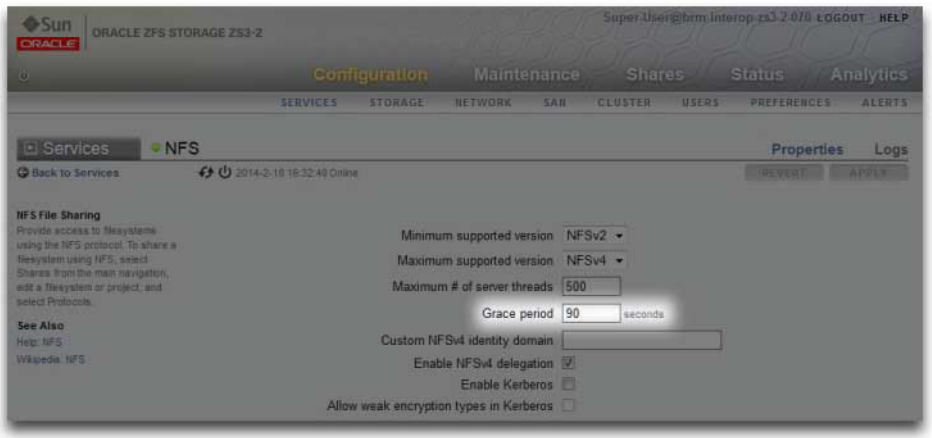
FIGURA 10-9 Dos rutas en un cluster

Estimación y reducción del impacto de la toma de control

Hay un intervalo durante la toma de control y el failback durante 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 incorpora 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 (consulte la ilustración); si se la reduce, se reduce el impacto evidente de la toma de control y el failback. Para interrupciones planificadas, Oracle ZFS Storage Appliance ofrece una recuperación sin período de gracia para clientes de NFSv4, lo cual evita la demora del período de gracia. Para obtener más información acerca de la recuperación sin período de gracia, consulte la propiedad de período de gracia en “Propiedades” [208] de NFS.

FIGURA 10-10 Período de gracia en un cluster



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 hay varios factores que afectan la duración de la toma de control (y su pariente cercano, la duración del failback), en la mayoría de las configuraciones, estos tiempos están dominados por el tiempo requerido para importar los recursos del conjunto 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. Tenga en cuenta que un conjunto de discos está formado por una mitad de un JBOD, siempre que los alojamientos de discos de ese medio JBOD se hayan completado y hayan sido asignadas 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 conjunto de discos no se ve afectado por los parámetros que pueden ser ajustados o alterados por los administradores, de manera que los administradores que están planificando implementaciones en clusters deben:

- limitar el almacenamiento instalado de manera que los clientes puedan tolerar los tiempos de toma de control asociados con ellos o bien;
- ajustar los valores de tiempo de espera 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 registros del log 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 considerablemente la duración del proceso.

La duración del failback suele ser mayor que la de la toma de control para cualquier configuración dada. Esto es así porque 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 nodo A al nodo B para que el nodo A tome el control sobre el nodo 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: Los tiempos estimados indicados en esta sección corresponden a la versión 2009.04.10,1-0 del software/firmware. Otras versiones pueden tener un rendimiento diferente; asimismo, el rendimiento real puede variar. Es importante hacer una prueba del proceso de toma de control para evaluar el impacto exacto que tiene en las aplicaciones de los clientes antes de implementar un dispositivo en clusters en un entorno de producción.

Configuración de clusters con la BUI

Para configurar o desconfigurar un cluster, use los siguientes procedimientos.

La desconfiguración de una agrupación en clusters es una operación destructiva que regresa uno de los controladores de almacenamiento en cluster a la configuración predeterminada de fábrica y reasigna al par superviviente como propietario de todos los recursos. Hay dos motivos para desconfigurar una agrupación en clusters: Ya no desea utilizar una agrupación en clusters y, en su lugar, desea configurar dos dispositivos de almacenamiento independientes.

Está reemplazando un controlador de almacenamiento que falló por nuevo hardware o un controlador de almacenamiento por software de dispositivo recién recibido de la fábrica (este reemplazo normalmente es realizado por el proveedor de servicio).

▼ Configuración de agrupaciones en clusters

1. **Conecte la alimentación y al menos un cable Ethernet a cada dispositivo.**
2. **Conecte los cables de los controladores de interconexión del cluster como se describe a continuación en Cableado de nodos. También puede continuar con la instalación del cluster y agregar estos cables dinámicamente durante el proceso de instalación.**
3. **Conecte los cables de los adaptadores bus de host a los JBOD compartidos, como se muestra en los diagramas de cableado de JBOD del diagrama de configuración incluido con el dispositivo.**
4. **Encienda ambos dispositivos, pero no comience con la configuración. Seleccione sólo uno de los dos dispositivos desde el que realizará la configuración (la selección es arbitraria). Para el proceso de configuración, haremos referencia a este dispositivo como dispositivo primario. Conecte la consola serie a ese dispositivo y acceda a ella. Realice la configuración inicial basada en tty de la misma manera en la que lo haría al configurar un dispositivo independiente. Nota: No realice la configuración inicial basada en tty en el dispositivo secundario; se la configurará automáticamente durante la instalación del cluster.**
5. **En el dispositivo primario, ingrese a la BUI o la CLI para comenzar la instalación del cluster. La instalación del cluster se puede seleccionar como parte de la instalación inicial si ya se instaló el controlador de interconexión del cluster. De manera alternativa, puede realizar una configuración independiente y postergar la instalación del cluster para otro momento. En este caso, puede realizar la tarea de configuración del cluster haciendo clic en el botón Setup (Instalar) en Configuration (Configuración) -> Cluster.**
6. **Como primer paso de la instalación del cluster, aparecerá un diagrama de los enlaces activos del cluster: debería ver en la pantalla tres cables de color azul, uno por cada conexión. Si no es así, agregue ahora los cables que faltan. Cuando vea los tres cables, puede hacer clic en el botón Commit (Confirmar) para continuar.**
7. **Escriba el nombre del dispositivo y la contraseña inicial de usuario root para el segundo dispositivo (es equivalente a realizar la instalación inicial de la consola serie para el nuevo dispositivo). Cuando hace clic en el botón Commit**

(Confirmar), aparecen barras de avance a medida que se configura el segundo dispositivo.

8. **Si está instalando una agrupación en clusters como parte de la instalación inicial del dispositivo primario, se le indicará que realice la configuración inicial de la misma manera en la que lo haría si estuviera configurando un único dispositivo. Todos los cambios de configuración que haga se propagarán automáticamente al otro dispositivo. Continúe con la configuración inicial, teniendo en cuenta las siguientes restricciones y advertencias: No se puede realizar el failover entre los nodos de las interfaces de red configuradas por DHCP, de manera que los clientes no pueden utilizarlas para acceder al almacenamiento. Por lo tanto, asegúrese de asignar direcciones IP estáticas a las interfaces de red que utilizarán los clientes para acceder al almacenamiento. Si durante la configuración inicial basada en tty seleccionó una interfaz de red configurada con DHCP y desea utilizar esa interfaz para el acceso de cliente, deberá cambiar el tipo de dirección a Static (Estática) antes de continuar. Las mejores prácticas incluyen configurar y asignar una interfaz de red privada para la administración de cada nodo, lo que permitirá la administración mediante cualquiera de los dos nodos mediante la red (BUI o CLI) independientemente del estado del cluster. Si se necesitan rutas, asegúrese de crear una ruta sobre una interfaz que se asigne a cada nodo. En la sección anterior, puede consultar un ejemplo específico.**

9. **Continúe con la configuración inicial hasta llegar al paso de la agrupación de almacenamiento. Cuando se produce una toma de control, el par del cluster puede tomar el control de cada grupo de almacenamiento, junto con las interfaces de red que usan los clientes para obtener acceso a esa agrupación de almacenamiento. Si crea dos agrupaciones de almacenamiento, cada nodo normalmente permite a los clientes tener acceso a la agrupación que le fue asignada; si uno de los nodos falla, el otro nodo permitirá el acceso de los clientes a ambas agrupaciones. Si crea una única agrupación de almacenamiento, el nodo al que no se asignó la agrupación proporcionará servicio a los clientes sólo cuando el par haya fallado. Las agrupaciones de almacenamiento se asignan a los nodos cuando se los crea; el cuadro de diálogo de configuración del almacenamiento ofrece la opción de crear una agrupación asignada a cada nodo de manera independiente. La unidad de almacenamiento más pequeña que se puede asignar a una agrupación es un disco. Si crea varias agrupaciones, no es obligatorio que sean todas del mismo tamaño. Tenga en cuenta que 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. Se recomienda que cada agrupación incluya un mínimo de 8 discos, idealmente más, entre todos los JBOD.**

10. **Después de completar la configuración básica, tendrá la oportunidad de asignar recursos a cada nodo. Normalmente, debe asignar sólo las interfaces de red;**

las agrupaciones de almacenamiento se asignaron automáticamente durante el paso de configuración del almacenamiento.

11. **Confirme las asignaciones de recursos y realice el failback inicial desde la interfaz de usuario del cluster, que se describe más adelante. Si todavía está ejecutando la instalación inicial en el dispositivo primario, esta pantalla es la última de la secuencia de instalación. Si está ejecutando la instalación del cluster de manera manual después de haber hecho la instalación inicial, vaya a la pantalla Configuración/Cluster para realizar estas tareas. Consulte la sección Interfaz de usuario del cluster más adelante para obtener información detallada.**

▼ Desconfiguración de una agrupación en clusters

1. **Seleccione el controlador de almacenamiento que se restablecerá con la configuración de fábrica. Tenga en cuenta que si está reemplazando un controlador de almacenamiento que tuvo un fallo, puede pasar directamente al paso 3, siempre que el controlador de almacenamiento que tuvo el fallo no se devuelva para mantenimiento en su sitio.**

2. **Desde la consola del sistema del controlador de almacenamiento que se restablecerá a su configuración de fábrica, realice un restablecimiento de fábrica.**

3. **El controlador de almacenamiento se restablece, y el par comienza el proceso de toma de control normalmente. NOTA: Antes de permitir que el controlador de almacenamiento cuyos valores de fábrica fueron restablecidos comience a iniciarse (es decir, antes de avanzar más allá del menú de inicio), apáguelo y espere a que el par complete la toma de control.**

4. **Desconecte los cables de interconexión del cluster (vea más arriba) y desconecte el controlador de almacenamiento apagado de los contenedores de almacenamiento externos del cluster.**

5. **En el controlador de almacenamiento restante, haga clic en el botón Unconfig (Desconfigurar) en la pantalla Configuration (Configuración) -> Clustering (Agrupación en clusters). Todos los recursos se asignarán a ese controlador de almacenamiento, el cual ya no pertenecerá a ningún cluster.**

6. **El controlador de almacenamiento desconectado, si lo hubiera, ya se puede conectar a su propio almacenamiento, encender y configurar normalmente. Si está reemplazando un controlador de almacenamiento que tuvo un fallo, conecte el reemplazo al controlador de almacenamiento restante y comience la tarea de instalación del cluster que se describió anteriormente.**

Nota - Si el cluster tenía dos agrupaciones o más, después de la desconfiguración el controlador de almacenamiento restante queda configurado como propietario de todas las agrupaciones. En las versiones de software anteriores a 2010.Q1.0.0, esta configuración no estaba admitida; si está ejecutando una versión más antigua del software, debe realizar una de las siguientes acciones: destruir una o ambas agrupaciones, conectar el controlador de almacenamiento de reemplazo, realizar la tarea de instalación del cluster que se describió anteriormente y reasignar al controlador de almacenamiento de reemplazo como propietario de una de las agrupaciones, o bien actualizar su versión del software a 2010.Q1.0.0 o posterior, que admite que un mismo controlador de almacenamiento tenga varias agrupaciones.

Configuración de agrupaciones en clusters con la CLI

▼ Cierre de una configuración en clusters

1. **Verifique el estado de cluster mediante los siguientes comandos de la CLI:**

```
nas-7420-1a:> configuration cluster
nas-7420-1a:configuration cluster> show
```

2. **A continuación se muestra un ejemplo de las propiedades de un cluster: state indica el estado del nodo principal en donde se ejecutó el comando; peer_state indica el estado del otro nodo principal.**

```
state = AKCS_OWNER
description = Active (takeover completed)
peer_asn = 365ed33c-3b9d-c533-9349-8014e9da0408
peer_hostname = nas-7420-1b
peer_state = AKCS_STRIPPED
peer_description = Ready (waiting for failback)
```

3. **Use la siguiente tabla para verificar el estado del nodo.**

Este nodo	Otro nodo	Condición
AKCS_CLUSTERED	AKCS_CLUSTERED	Ambos nodos se ejecutan en condiciones normales.
AKCS_OWNER	AKCS_STRIPPED	Este nodo tiene todos los recursos y es un nodo activo. El otro nodo está en espera y no tiene recursos.

Este nodo	Otro nodo	Condición
AKCS_OWNER	reinicio	Otro nodo se está reiniciando y este nodo tiene todos los recursos.
AKCS_OWNER	unknown	Este nodo no conoce el socio.

Nota - Si el estado de los nodos principales NO concuerda, es posible que haya un problema en el cluster. Comuníquese con la asistencia técnica de Oracle antes de continuar.

Cierre del nodo principal en espera

1. **Cierre el nodo principal en espera; para ello, use la CLI para ejecutar los siguientes comandos:**

```
nas-7420-1b:configuration cluster> cd /
nas-7420-1b:> maintenance system poweroff
This will turn off power to the appliance. Are you sure? (Y/N)
```

2. **Para verificar que desea cerrar el otro nodo principal, escriba Y.**

Nota - Si ambos nodos principales tienen el estado AKCS_CLUSTERED, se inicia automáticamente una toma de control en el nodo principal superviviente.

3. **Confirme que el nodo principal en espera esté apagado y el estado del cluster sea OWNER/unknown.**

4. **Cierre el nodo principal activo; para ello, use la CLI para ejecutar los siguientes comandos:**

```
nas-7420-1a:configuration cluster> cd /
nas-7420-1a:> maintenance system poweroff
This will turn off power to the appliance. Are you sure? (Y/N)
```

5. **Para verificar que desea cerrar el nodo principal activo, escriba Y.**

6. **Confirme que ambos nodos principales están apagados. Desde el indicador de ILOM, ejecute:**

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

7. **Apague los estantes de discos.**

▼ Desconfiguración de una agrupación en clusters

- **La desconfiguración de una agrupación en clusters en la CLI funciona igual que el botón unconfig (Desconfigurar) de la BUI. Si un usuario intenta desconfigurar un cluster que no se encuentra en un estado correcto, aparece un error.**

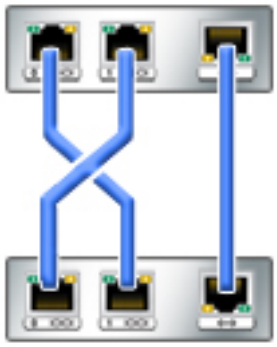
```
configuration cluster> help
Subcommands that are valid in this context:

   resources            => Configure resources

   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

   done                 => Finish operating on "cluster"

   get [prop]           => Get value for property [prop]. ("help properties"
                           for valid properties.) If [prop] is not specified,
                           returns values for all properties.

   setup                => Run through initial cluster setup

   failback             => Fail back all resources assigned to the cluster peer

   takeover             => Take over all resources assigned to the cluster peer

   unconfig             => Unconfigure the cluster

   links                => Report the state of the cluster links
```

Cableado de nodos del cluster

Los nodos principales en clusters se deben conectar mediante los puertos de interconexión del cluster que se encuentran en la parte posterior del controlador.

Cableado de cluster ZS3-2

FIGURA 10-11 Cableado de cluster ZS3-2



El controlador ZS3-2 proporciona tres enlaces redundantes que permiten a los nodos comunicarse: dos enlaces serie (los dos primeros conectores) y un enlace Ethernet (el tercer conector).

Con cables rectos Ethernet Cat 5 o mejores (la configuración del cluster incluye tres cables de 1 m), conecte el nodo principal como se muestra en el diagrama de la izquierda.

El cableado del cluster se puede hacer antes de encender los nodos principales o durante la ejecución de la tarea guiada de instalación del cluster. La interfaz de usuario indica el estado de cada enlace, como se muestra más adelante en esta sección. Para poder continuar con la configuración del cluster, debe haber establecido los tres enlaces.

Cableado de clusters ZS3-4 y 7x20

FIGURA 10-12 Cableado de clusters ZS3-4 y 7x20

Los controladores ZS3-4 y 7x20 proporcionan tres enlaces redundantes que permiten a los nodos comunicarse: dos enlaces serie (los dos conectores externos) y un enlace Ethernet (el conector del medio).

Con cables rectos Ethernet Cat 5 o mejores (la configuración del cluster incluye tres cables de 1 m), conecte el nodo principal como se muestra en el diagrama de la izquierda.

El cableado del cluster se puede hacer antes de encender los nodos principales o durante la ejecución de la tarea guiada de instalación del cluster. La interfaz de usuario indica el estado de cada enlace, como se muestra más adelante en esta sección. Para poder continuar con la configuración del cluster, debe haber establecido los tres enlaces.

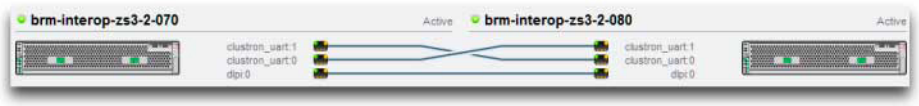
Cableado de estantes de almacenamiento

Debe conectar los estantes de almacenamiento a ambos dispositivos antes de comenzar a configurar el cluster. Consulte “Instalación” de “Guía de instalación de Oracle ZFS Storage Appliance ” o siga las instrucciones del póster de instalación rápida incluido con el sistema.

Página de configuración de clusters de la BUI

La vista Configuration (Configuración) -> Cluster proporciona una vista general gráfica del estado de la tarjeta del cluster, los estados de los nodos principales del cluster y todos los recursos.

FIGURA 10-13 Vista de cluster de configuración



La interfaz contiene los siguientes objetos:

- Una imagen en miniatura de cada sistema; el sistema cuya interfaz administrativa se está accediendo se muestra a la izquierda. Cada imagen en miniatura está etiquetada con el nombre canónico del dispositivo y su estado actual del cluster (el ícono por encima y una etiqueta descriptiva).
- Una imagen en miniatura de cada conexión de tarjeta de cluster que se actualiza dinámicamente con el hardware: el enlace aparece representado con una línea continua si está conectado y activo, y la línea desaparece si esa conexión está rota o cuando el otro sistema se está reiniciando.
- Una lista de los recursos privados y únicos (según se describió en la sección Introducción) actualmente asignados a cada sistema, que se muestran como lista debajo de la imagen en miniatura de cada nodo de cluster, junto con diversos atributos de los recursos.
- Para cada recurso, el dispositivo al que está asignado el recurso, es decir, el dispositivo que proporcionará el recurso cuando ambos se encuentren en el estado En cluster. Cuando el dispositivo actual se encuentra en el estado Propietario, se muestra el campo correspondiente como menú emergente que se puede editar y luego confirmar haciendo clic en Aplicar.
- Para cada recurso, un ícono de un candado que indica si el recurso es privado o no. Cuando el dispositivo actual se encuentra en los estados Propietario o En cluster, es posible hacer clic en el ícono del candado y, a continuación, hacer clic en Aplicar para bloquear los recursos (se vuelven privados) o desbloquearlos (se vuelven únicos). Tenga en cuenta que los recursos privados que pertenecen al par remoto no aparecen en ninguna de las listas de recursos.

La BUI contiene los siguientes botones:

TABLA 10-6 Botones de interfaz de cableado de estantes

Botón	Descripción
Configuración	Si el cluster todavía no está configurado, ejecute la tarea guiada de instalación del cluster y, a continuación, regrese a la pantalla actual. Consulte una descripción detallada de esta tarea en la sección anterior correspondiente.

Botón	Descripción
Desconfiguración	Actualice un nodo para el funcionamiento independiente desconfigurando el cluster. Consulte una descripción detallada de esta tarea en la sección siguiente correspondiente.
Aplicar	Si hay modificaciones de recursos todavía pendientes (filas resaltadas en amarillo), confirma esos cambios en el cluster.
Revertir	Si hay modificaciones de recursos todavía pendientes (filas resaltadas en amarillo), deshace esos cambios y muestra la configuración actual del cluster.
Failback	Si el dispositivo actual (a la izquierda) es el propietario, realiza el failback de los recursos cuyo propietario es el otro dispositivo y ambos nodos quedan en el estado En cluster (activo-activo).
Toma de control	Si el dispositivo actual (a la izquierda) se encuentra en el estado En cluster o Segmentado, hace que el otro dispositivo se reinicie y toma el control de los recursos de ese dispositivo, de manera que el dispositivo actual pasa al estado Propietario.

♦ ♦ ♦ CAPÍTULO 11

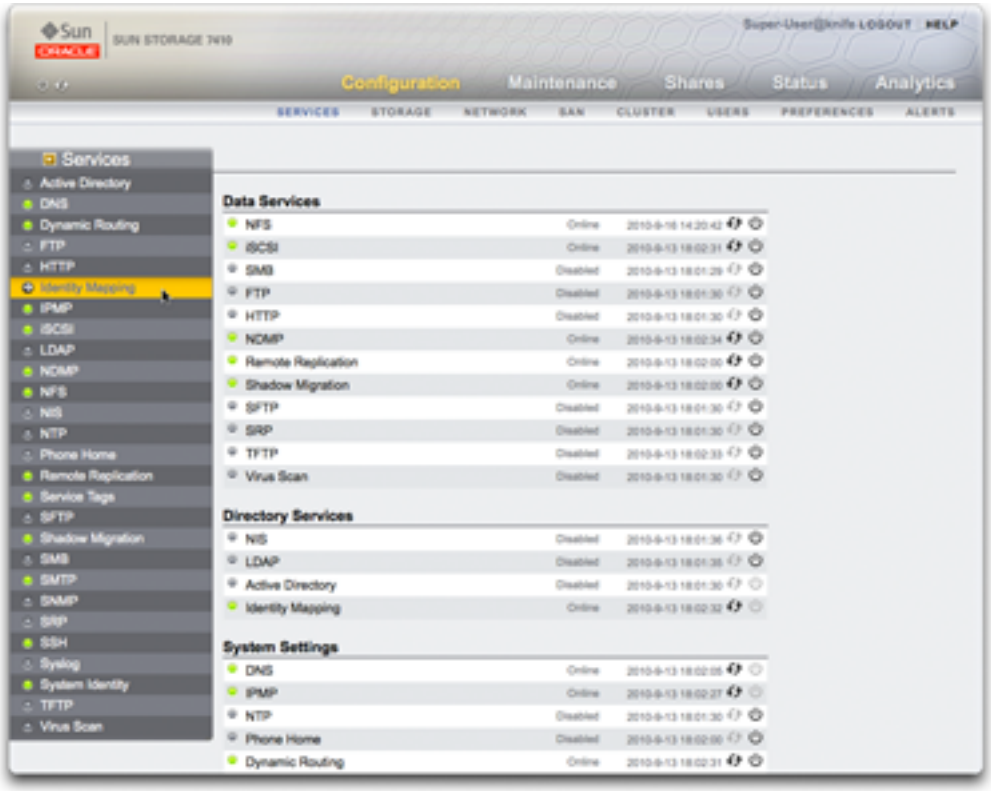
Servicios del dispositivo ZFSSA

La pantalla Services (Servicios) tiene un panel lateral que permite la navegación rápida entre los servicios.

Servicios disponibles

Puede configurar los siguientes servicios del dispositivo ZFSSA:

FIGURA 11-1 Página de configuración de servicios de la BUI



Servicios de datos

TABLA 11-1 Servicios de datos disponibles

Servicio	Descripción	Puertos usados
"NFS" [208]	Acceso al sistema de archivos mediante los protocolos NFSv3 y NFSv4	111 y 2049
"iSCSI" [213]	Acceso al LUN mediante el protocolo iSCSI	3260 y 3205
"SMB" [214]	Acceso al sistema de archivos mediante el protocolo SMB	SMB mediante NetBIOS 139

Servicio	Descripción	Puertos usados
SMB mediante TCP 445		
Datagrama NetBIOS 138		
Servicio de nombres NetBIOS 137		
“FTP” [232]	Acceso al sistema de archivos mediante el protocolo FTP	21
“HTTP” [234]	Acceso al sistema de archivos mediante el protocolo HTTP	80
“NDMP” [236]	Servicio de host NDMP	10000
“Replicación remota” [245]	Replicación remota	216
“Migración shadow” [245]	Migración shadow de datos	
“SFTP” [246]	Acceso al sistema de archivos mediante el protocolo SFTP	218
“SRP” [249]	Acceso de bloque mediante el protocolo SRP	
“TFTP” [250]	Acceso al sistema de archivos mediante el protocolo TFTP	
“Análisis de virus” [251]	Análisis de virus del sistema de archivos	

Servicios de directorio

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 11-2 Servicios de directorio disponibles

Servicio	Descripción	Puertos usados
“NIS” [254]	Autenticación de usuarios y grupos desde un servicio NIS	
“LDAP” [256]	Autenticación de usuarios y grupos desde un directorio LDAP	389
“Active Directory” [260]	Autenticación de usuarios con un servidor Active Directory de Microsoft	

Servicio	Descripción	Puertos usados
“Asignación de identidad” [266]	Asignación entre entidades de Windows e identificadores de Unix	

Valores del servicio

TABLA 11-3 Valores del servicio

Servicio	Descripción	Puertos usados
“DNS” [274]	Cliente de servicio de nombres de dominio	53
“Enrutamiento dinámico” [276]	Protocolos de enrutamiento dinámico RIP y RIPng	
“IPMP” [277]	Rutas múltiples IP para failover por IP	
“NTP” [278]	Cliente de protocolo de tiempo de red	
“Phone Home” [281]	Registro del producto y configuración de asistencia técnica	443
“Etiquetas de servicio” [285]	Asistencia para inventario del producto	443
“SMTP” [286]	Configuración del servidor de correo saliente	
“SNMP” [287]	SNMP para enviar capturas sobre alertas y proporcionar información de estado del dispositivo	
“Syslog” [291]	Relé Syslog para enviar mensajes Syslog sobre alertas y reenviar mensajes Syslog de servicios	
“Identidad del sistema” [296]	Nombre y ubicación del sistema	

Servicios de acceso remoto

TABLA 11-4 Servicios de acceso remoto disponibles

Servicio	Descripción	Puertos usados
“SSH” [297]	SSH para acceso desde la CLI	22
“REST” [285]	API de RESTful	

Servicios de seguridad

TABLA 11-5 Servicios de seguridad disponibles

Servicio	Descripción	Puertos usados
Kerberos	Autenticación de Kerberos V	88
Cambio y restablecimiento de contraseña de Kerberos V (SET_ CHANGE)	464	
Cambio y restablecimiento de contraseña de Kerberos V (RPCSEC_GSS)	749	

Cantidad mínima de puertos 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 cada transacción realizada por la red mediante la especificación del host y el 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 también debe estar abierto.

Configuración de servicios con la BUI

Las pantallas de servicios de la BUI se utilizan para ver y modificar los servicios y los parámetros de configuración descritos en las tablas anteriores. Haga doble clic en una línea de servicio para ver la pantalla de definición de ese servicio. En las siguientes tablas, se describen los íconos y los botones de las pantallas de servicios:

TABLA 11-6 Íconos y botones de la página de servicios de la BUI

Ícono	Descripción
	Vaya a la pantalla de servicios para configurar propiedades y ver logs. Este botón aparece al pasar el puntero del mouse 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.

▼ Visualización de la pantalla de un servicio específico

1. **Para ver o editar las propiedades de un servicio específico, pase el puntero del mouse sobre el ícono de estado del servicio que se encuentra a la izquierda del nombre del servicio.**
2. **El ícono de estado se convierte en un ícono de flecha en el que se puede hacer clic para desplegar la pantalla de propiedades del servicio seleccionado.**

Visualización de la pantalla de un servicio específico

- **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.**

Activación de un servicio

- **Si un servicio no está en línea, haga clic en el ícono de encendido para activar el servicio .**

Desactivación de un servicio

- **Si un servicio está en línea y desea desactivarlo, haga clic en el ícono de encendido para desactivar el servicio .**

Definición de propiedades

1. **Para definir las propiedades de un servicio, haga doble clic en el servicio.**
2. **Cambie las propiedades y, a continuación, haga clic en APPLY (Aplicar).**
3. **Para restablecer las propiedades, haga clic en REVERT (Revertir).**

Visualización de logs de servicio

1. **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 pueden proporcionar la siguiente información:**
   - La hora a la que cambió el estado de un servicio
   - Mensajes de error del servicio

2. **El contenido de los logs es específico para cada servicio individual y está sujeto a cambios con actualizaciones futuras del software del dispositivo. A continuación se muestran mensajes de ejemplo que se utilizan normalmente en esta versión del dispositivo:**

Mensaje de log de ejemplo	Descripción
Executing start method	El servicio se está iniciando.
Method "start" exited with status 0	El servicio informó que el inicio se realizó correctamente (0 == éxito).
Method "refresh" exited with status 0	El servicio actualizó correctamente la configuración en función de los parámetros del servicio.
Executing stop method	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.
Disabled	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.

Configuración de servicios con la CLI

La sección de servicios de la CLI se encuentra en `configuration services` (servicios de configuración). Use el comando `show` para enumerar el estado actual de todos los servicios:

El siguiente ejemplo corresponde al servicio “NTP” [278]:

```
[ Oct 11 21:05:31 Enabled. ]
[ Oct 11 21:07:37 Executing start method (...). ]
[ Oct 11 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.

```
caji:> configuration services
caji:configuration services> show
Services:
                              ad => disabled
                             smb => disabled
                             dns => online
                      dynrouting => online
                             ftp => disabled
```

```
                http => disabled
            identity => online
               idmap => online
                ipmp => online
               iscsi => online
                ldap => disabled
                ndmp => online
                 nfs => online
                 nis => disabled
                 ntp => disabled
         replication => online
                scrk => disabled
                sftp => disabled
              shadow => online
                smtp => online
                snmp => disabled
                 ssh => online
              syslog => disabled
                tags => online
                tftp => disabled
               vscan => disabled


Children:
                  ad => Configure Active Directory
                 smb => Configure SMB
                 dns => Configure DNS
          dynrouting => Configure Dynamic Routing
                 ftp => Configure FTP
                http => Configure HTTP
            identity => Configure System Identity
               idmap => Configure Identity Mapping
                ipmp => Configure IPMP
               iscsi => Configure iSCSI
                ldap => Configure LDAP
                ndmp => Configure NDMP
                 nfs => Configure NFS
                 nis => Configure NIS
                 ntp => Configure NTP
         replication => Configure Remote Replication
                scrk => Configure Phone Home
                sftp => Configure SFTP
              shadow => Configure Shadow Migration
                smtp => Configure SMTP
                snmp => Configure SNMP
                 srp => Configure SRP
                 ssh => Configure SSH
              syslog => Configure Syslog
                tags => Configure Service Tags
                tftp => Configure TFTP
               vscan => Configure Virus Scan
             routing => Configure Routing Table
```

Selección de un servicio

1. **Después de haber seleccionado un servicio, puede ver el estado, activarlo, desactivarlo y configurar las propiedades.**
2. **Para seleccionar un servicio, escriba el nombre del servicio. Por ejemplo, para seleccionar `nis`:**

```
caji:configuration services> nis
caji:configuration services nis>
```

Visualización del estado de un servicio

- **Para ver el estado de un servicio, use el comando `show`:**

```
caji:configuration services nis> show
Properties:
                     <status> = online
                       domain = fishworks
                    broadcast = true
                    ypservers =
```

Activación de un servicio

- **Use el comando `enable` para activar un servicio:**

```
caji:configuration services nis> enable
```

Desactivación de un servicio

- **Use el comando `disable` para desactivar un servicio:**

```
caji:configuration services nis> disable
```

Establecimiento de propiedades

1. **Use el comando `set` para definir las propiedades del servicio seleccionado.**

2. **Después de configurar las propiedades, use el comando `commit` para guardar y activar la nueva configuración:**

```
caji:configuration services nis> set domain="mydomain"
                        domain = mydomain (uncommitted)
caji:configuration services nis> commit
caji:configuration services nis> show
Properties:
                      <status> = online
                        domain = mydomain
                     broadcast = true
                     ypservers =
```

3. **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.**

▼ Visualización de la ayuda de un servicio

- **Escriba `help` para ver todos los comandos disponibles para un servicio:**

```
caji: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.
```

NFS

Sistema de archivos de red (NFS) es un protocolo estándar del sector utilizado para compartir archivos por medio de una red. Sun ZFS Storage Appliance admite las versiones 2, 3 y 4 de NFS. Para obtener más información acerca de cómo se construye el espacio de nombres del sistema de archivos, consulte la sección “filesystem namespace” [312]. Para obtener información acerca de NFS con usuarios locales, consulte el Capítulo 7, Configuración de usuario.

Propiedades

- Minimum supported version (Versión mínima admitida): use esta lista desplegable para controlar las versiones de NFS que admite el dispositivo.
- Maximum supported version (Versión máxima admitida): use esta lista desplegable para controlar las versiones de NFS que admite el dispositivo.
- Maximum # of server threads (Cantidad máxima de subprocesos de servidor): define la cantidad máxima de solicitudes simultáneas de NFS (de 20 a 1000). Debe cubrir al menos la cantidad de clientes NFS simultáneos que anticipa tener.
- Grace period (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 únicamente a los clientes NFS v4 (NFS v3 no tiene estado, por lo tanto, 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 durante interrupciones planificadas. Las interrupciones planificadas se producen durante eventos como las “Actualizaciones” de “Manual de servicio del cliente de Oracle ZFS Storage Appliance ”, y el reinicio del dispositivo con el comando `maintenance system reboot` de la CLI o el reinicio mediante 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.
- Custom NFSv4 identity domain (Dominio de identidades NFSv4 personalizado): use esta propiedad para definir el dominio para asignar identidades de usuarios y grupos de NFSv4. 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.
- Enable NFSv4 delegation (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 sólo 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 afecta solamente a los montajes NFSv4.

- Mount visibility (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 sólo 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).
- Enable Kerberos (Activar Kerberos): activa o desactiva el servicio de Kerberos.
- * Allow weak encryption types in Kerberos (* Permitir tipos de cifrado débil en Kerberos): activa o desactiva la compatibilidad con DES (des-cbc-crc, des-cbc-md5) y Exportable ArcFour con HMAC/md5 (arcfour-hmac-exp). Esta propiedad está desactivada de forma predeterminada.
- * Kerberos realm (* Dominio Kerberos): un dominio es una red lógica, similar a otros dominios, que define un grupo de sistemas que se encuentran bajo el mismo KDC principal. Los nombres de dominios Kerberos pueden ser cualquier cadena ASCII. Normalmente, el nombre del dominio Kerberos es el mismo que el nombre del dominio DNS, excepto que el del dominio Kerberos está en mayúsculas. El uso de esta convención ayuda a diferenciar los problemas del servicio Kerberos de los problemas con el espacio de nombres del DNS, pero sigue usando un nombre conocido.
- * Kerberos master KDC (* KDC maestro de Kerberos): en cada dominio Kerberos, debe incluir un servidor que mantenga la copia maestra de la base de datos del principal. La diferencia más importante entre un KDC maestro y un KDC esclavo es que sólo el maestro atiende las solicitudes de administración de la base de datos. Por ejemplo, para cambiar una contraseña o agregar un nuevo principal, se usa el KDC maestro.
- * Kerberos slave KDC (* KDC esclavo de Kerberos): el KDC esclavo contiene copias duplicadas de la base de datos del principal. Tanto el servidor KDC maestro como el esclavo crean tickets que se usan para establecer autenticación.
- * Kerberos admin principal (* Principal de administración de Kerberos): esta propiedad identifica al administrador. Por convención, el nombre de un principal se divide en tres componentes: el primario, la instancia y el dominio kerberos. Puede especificar un principal como `joe`, `joe/admin` o `joe/admin@ENG.EXAMPLE.COM`. Esta propiedad se usa sólo para configurar los principales del servicio Kerberos del sistema y no se conserva.
- * Kerberos admin password (* Contraseña de administrador de Kerberos): define una contraseña para el administrador. Esta propiedad se usa sólo para configurar los principales del servicio Kerberos del sistema y no se conserva.
- Oracle Intelligent Storage Protocol: el servicio NFSv4 incluye compatibilidad con Oracle Intelligent Storage Protocol, que permite que los clientes NFSv4 de Oracle Database

transmitan información de optimización al servidor NFSv4 de ZFS Storage Appliance. Para obtener más información, consulte “ Oracle Intelligent Storage Protocol ” [497].

Los cambios realizados en las propiedades de los servicios se documentan en las secciones “Configuración de servicios con la BUI” [202] and “Configuración de servicios con la CLI” [204].

La configuración de la versión mínima y la versión máxima de NFS con el mismo valor hace que el dispositivo se comunique 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 sólo la versión que funciona mejor.

Dominios Kerberos

La configuración de un dominio Kerberos crea ciertos principales de servicio y agrega las claves necesarias al keytab local del sistema. Se debe configurar el “servicio NTP” [278] 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. Si el dispositivo está configurado para unirse a un dominio de Active Directory, no se lo puede configurar para que sea parte de un dominio Kerberos.

Para obtener información acerca de la configuración de clientes de KDC y Kerberos, consulte http://docs.oracle.com/cd/E26502_01/html/E29015/index.html. (http://docs.oracle.com/cd/E26502_01/html/E29015/index.html.) Después de configurar las propiedades de NFS para Kerberos, cambie el modo de seguridad en la pantalla Shares (Recursos compartidos) ->; Filesystem (Sistema de archivos) ->; Protocols (Protocolos) a un modo que use Kerberos.

El dispositivo utiliza los siguientes puertos para Kerberos.

- Autenticación de Kerberos V: 88
- Cambio y restablecimiento de contraseña de Kerberos V `SET_CHANGE`: 464

- Cambio y restablecimiento de contraseña de Kerberos V `RPCSEC_GSS`: 749

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 de servicios

Estos logs están disponibles para el servicio NFS:

TABLA 11-7 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 llamada de NFSv4
network-nfs-mapid:default	Log del daemon mapid de NFSv4, que asigna credenciales de usuarios y grupos de NFSv4
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

Análisis de NFS

Puede supervisar la actividad de NFS en la sección “Análisis” de “Guía de análisis de Oracle ZFS Storage Appliance ”. 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

Nota: Cuando el servidor NFS se reinicia o realiza un failover, el nombre de archivo es *desconocido* en el servidor hasta que el cliente lo vuelve a abrir. El archivo aparece como *desconocido* en las hojas de trabajo de los análisis.

Propiedades de NFS en la BUI y la CLI

En la siguiente tabla, se describe la asignación entre las propiedades de la CLI y las descripciones de propiedades de la BUI antes mencionadas.

TABLA 11-8 Propiedades de NFS en la BUI y la CLI

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 NFSv4 personalizado
enable_delegation	Activar delegación NFSv4
mount_visibility	Nivel de restricción de información de recursos compartidos de clientes
krb5_allow_weak_crypto	Uso de tipos de cifrado débil (arcfour-hmac-md5-exp, des-cbc-md5 y des-cbc-crc) en Kerberos
krb5_realm	Dominio Kerberos
krb5_kdc	KDC maestro de Kerberos
krb5_kdc2	KDC esclavo de Kerberos
krb5_admin	Principal de administración de Kerberos

▼ Uso compartido de un sistema de archivos por medio de NFS

1. **Vaya a la pantalla Configuration (Configuración) ->Services (Servicios).**
2. **Compruebe que el servicio NFS esté activado y en línea. De no ser así, actívelo.**
3. **Vaya a la pantalla del Capítulo 12, Recursos compartidos, proyectos y esquemas y edite un recurso compartido existente o cree uno nuevo.**
4. **Haga clic en la ficha Protocols (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).**

Servicio 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 la sección Capítulo 6, Configuración de red de área de almacenamiento.

Propiedades del servicio iSCSI

TABLA 11-9 Propiedades del servicio iSCSI

Propiedad	Descripción
Usar iSNS	Indica si la detección iSNS está activada
Servidor iSNS	Servidor iSNS
Usar RADIUS	Indica si RADIUS está activado
Servidor RADIUS	Servidor RADIUS
Secreto de servidor RADIUS	Secreto del servidor RADIUS

Los cambios realizados en las propiedades de los servicios se documentan en las secciones “Configuración de servicios con la BUI” [202] y “Configuración de servicios con la CLI” [204]. Los nombres de propiedades de CLI son versiones más abreviadas que las mencionadas anteriormente.

Autenticación del servicio iSCSI

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.

Autorización del servicio iSCSI

El servicio iSCSI le permite especificar una lista global de iniciadores que se pueden utilizar en grupos de iniciadores.

Destinos e iniciadores del servicio iSCSI

Para obtener más información acerca de destinos e iniciadores iSCSI, consulte el Capítulo 6, Configuración de red de área de almacenamiento.

Solución de problemas de iSCSI

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 el failover o failback, no sobreviven las E/S de copia reducida de iSER provenientes del cliente Red Hat:

- Modifique el parámetro `node.session.timeo.replacement_timeout` del archivo `/etc/iscsi/iscsid.conf` con el valor 300sec.

Servicio SMB

El servicio SMB proporciona acceso a sistemas de archivos mediante el protocolo SMB. Las versiones admitidas de SMB son: SMB1 y SMB2.0. Para configurar el uso compartido de

recursos por medio de SMB de los sistemas de archivos, use la configuración de Capítulo 12, Recursos compartidos, proyectos y esquemas.

Propiedades del servicio SMB

- LAN Manager compatibility level (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.
- Preferred domain controller (Controlador de dominio preferido): el controlador de dominio preferido para utilizar al unir un dominio de “Active Directory” [260]. 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.
- Active Directory site (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.
- Maximum # of server threads (Cantidad máxima de subprocesos de servidor): cantidad máxima de subprocesos de servidor simultáneos (trabajadores). El valor predeterminado es 1024.
- Enable Dynamic DNS (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 de forma predeterminada.
- Enable Oplocks (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 de forma predeterminada. 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.
- Restrict anonymous access to share list (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.
- System Comment (Comentario de sistema): cadena de texto significativa.
- Idle Session Timeout (Tiempo de espera de sesión inactiva): configuración de tiempo de espera para inactividad de la sesión.
- Primary WINS server (Servidor WINS principal): dirección WINS principal configurada en TCP/IP.
- Secondary WINS server (Servidor WINS secundario): dirección WINS secundaria configurada en TCP/IP.

- Excluded IP addreses from WINS (Direcciones IP excluidas de WINS): direcciones IP excluidas del registro con WINS.
- SMB Signing Enabled (Firma de SMB activada): activa 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).
- SMB Signing Required (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; los clientes que no admitan el uso de firmas no podrán conectarse con el servidor.
- Ignore zero VC (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. De manera predeterminada, 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.

Los cambios realizados en las propiedades del servicio se documentan en las secciones “Configuración de servicios con la BUI” [202] y “Configuración de servicios con la CLI” [204]. Los nombres de propiedades de CLI son versiones más abreviadas que las mencionadas anteriormente.

Propiedades de recursos compartidos de SMB

Hay varias “Propiedades de recursos compartidos” [301] que se deben configurar de cierta manera al exportar un recurso compartido mediante SMB.

TABLA 11-10 Propiedades de recursos compartidos de SMB

Propiedad	Descripción
Capítulo 12, Recursos compartidos, proyectos y esquemas	Los clientes SMB no diferencian mayúsculas de minúsculas, de manera que esta propiedad debe configurarse como "mixed" (combinado) o "insensitive" (indistinto).
Capítulo 12, Recursos compartidos, proyectos y esquemas	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.
Non-Blocking Mandatory Locking (Bloqueo no bloqueante obligatorio)	Esta propiedad se debe activar para permitir que el bloqueo de rango de bytes funcione correctamente.

Propiedad	Descripción
"Protocolos de recursos compartidos" [336]	Nombre que utilizan los clientes para hacer referencia al recurso compartido. Para obtener información acerca de la manera en la que se hereda este nombre de un Capítulo 12, Recursos compartidos, proyectos y esquemas, consulte la documentación de "Protocolos de recursos compartidos" [336].
"Protocolos de recursos compartidos" [336]	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 la documentación de "Protocolos de recursos compartidos" [336].

Las propiedades del Capítulo 12, Recursos compartidos, proyectos y esquemas y Capítulo 12, Recursos compartidos, proyectos y esquemas se pueden configurar solamente al crear un recurso compartido.

Interoperabilidad NFS/SMB

El dispositivo admite el acceso concurrente de clientes "NFS" [208] 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" [260].
- Establezca una estrategia de "Servicio de asignación de identidad" [266] y configure el servicio.
- Configure SMB.
- 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 la documentación de "Shares (Recursos compartidos) > Shares (Recursos compartidos) > Access (Acceso)" [344].

Espacios de nombres de DFS de SMB

El sistema de archivos distribuidos (DFS) 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. Los espacios de nombres de DFS basados en dominios no son admitidos. 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” [260], 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. En el siguiente ejemplo, los pasos permiten al usuario local de SMB `dfsadmin` manipular espacios de nombres de DFS.

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.

Microsoft Windows systems	XP SP3	2003 SP2	2003 R2 SP2	Vista SP2	2008 SP2	2008 R2 SP1	Win7 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 R2	Vista	2008	2008 R2	Win7
	SP3	SP2	SP2	SP2	SP2	SP1	SP1

Notas: s significa que está admitido, n significa que no está admitido y NC significa que no corresponde

- 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.

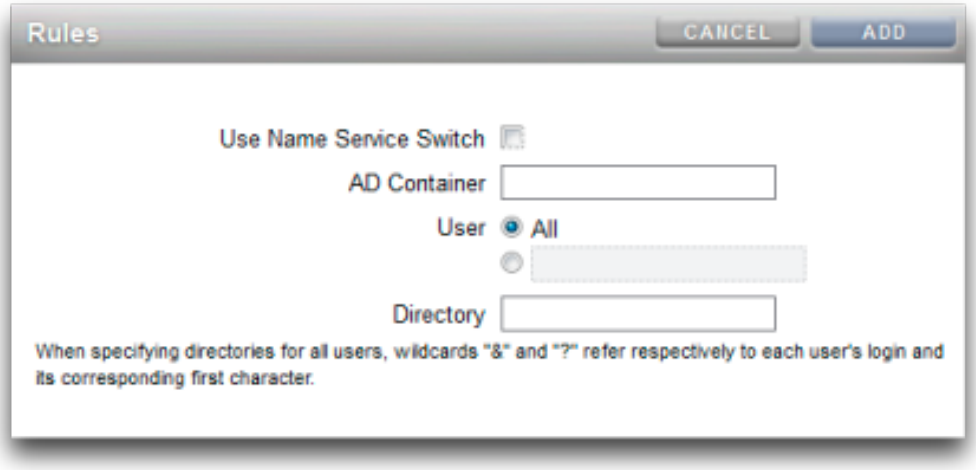
▼ Ejemplo: manipulación de espacios de nombres de DFS

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 que se modificará el espacio de nombres de DFS.**

Servicio de 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 11-2 Configuración de las reglas del directorio raíz automático



- Use Name Service Switch (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.
- User (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.
- Directory (Directorio): define el directorio para la regla, por ejemplo: /export/wdp.

▼ Agregación de reglas de directorio raíz automático de SMB

1. **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:**

```
twofish:> configuration services smb
twofish:configuration services smb> create
twofish:configuration services rule (uncommitted)> set use_nss=false
twofish:configuration services rule (uncommitted)> set user=Bill
twofish:configuration services rule (uncommitted)> set directory=/export/wdp
twofish:configuration services rule (uncommitted)> set container="dc=com,dc=fishworks,
```

```
   ou=Engineering,CN=myhome"
twofish:configuration services rule (uncommitted)> commit
twofish:configuration services smb> list
RULE       NSS      USER         DIRECTORY            CONTAINER
rule-000   false    Bill         /export/wdp          dc=com,dc=fishworks,
   ou=Engineering,CN=myhome
```

2. **Las reglas de directorio raíz automático se pueden crear con caracteres comodín. 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:**

```
twofish:configuration services smb> create
twofish:configuration services rule (uncommitted)> set use_nss=false
twofish:configuration services rule (uncommitted)> set user=*
twofish:configuration services rule (uncommitted)> set directory=/export/?/&
twofish:configuration services rule (uncommitted)> set container="dc=com,dc=fishworks,
   ou=Engineering,CN=myhome"
twofish:configuration services rule (uncommitted)> commit
twofish:configuration services smb> list
RULE       NSS      USER         DIRECTORY            CONTAINER
rule-000   false    Bill         /export/wdp          dc=com,dc=fishworks,
   ou=Engineering,CN=myhome
```

3. **El conmutador de servicios de nombres también se puede usar para crear reglas de directorio raíz automático:**

```
twofish:configuration services smb> create
twofish:configuration services rule (uncommitted)> set use_nss=true
twofish:configuration services rule (uncommitted)> set container="dc=com,dc=fishworks,
   ou=Engineering,CN=myhome"
twofish:configuration services rule (uncommitted)> commit
twofish:configuration services smb> list
RULE       NSS      USER         DIRECTORY            CONTAINER
rule-000   true                                      dc=com,dc=fishworks,
   ou=Engineering,CN=myhome
```

Grupos locales de SMB

Los grupos locales son grupos de usuarios del dominio que confieren privilegios adicionales a esos usuarios.

TABLA 11-11 Grupos locales de SMB

Grupo	Descripción
Administradores	Los administradores pueden pasar por alto permisos de archivos para cambiar la propiedad de los archivos.

Grupo	Descripción
Operadores de copia de seguridad	Los operadores de copia de seguridad pueden pasar por alto los controles de acceso de los archivos para hacer copias de seguridad de los archivos y restaurarlos.

▼ Agregación de usuarios a grupos locales de SMB

- **Para agregar un usuario, haga lo siguiente:**

```
twofish:configuration services smb> groups
twofish:configuration services smb groups> create
twofish:configuration services smb member (uncommitted)> set user=Bill
twofish:configuration services smb member (uncommitted)> set group="Backup Operators"
twofish:configuration services smb member (uncommitted)> commit
twofish:configuration services smb groups> list
MEMBER       USER                        GROUP
member-000   WINDOMAIN\Bill              Backup Operators
```

Cuentas locales de SMB

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 sólo lectura y no se puede configurar para operaciones de lectura/escritura en el dispositivo.

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.

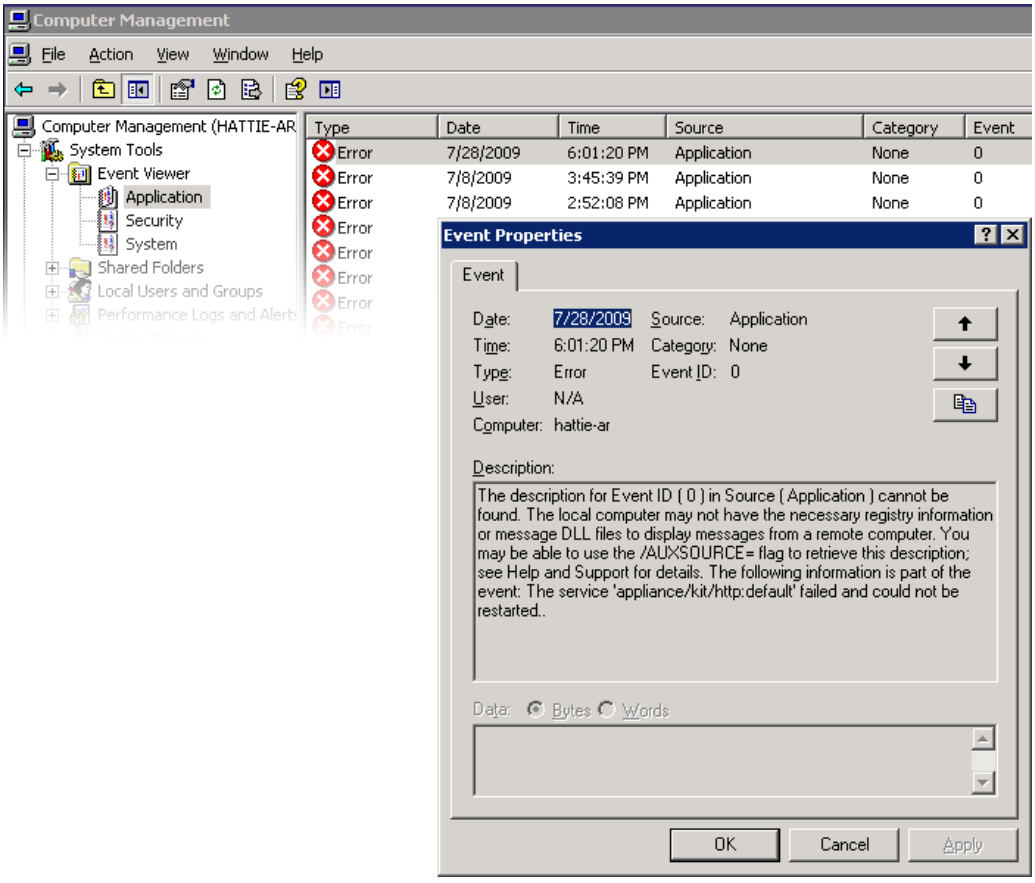
Para usar las funciones de MMC en los dispositivos Sun ZFS Storage 7000 en el modo de grupo de trabajo, asegúrese de agregar el administrador de Windows que utilizará la consola de administración al “grupo local” [214] Administrators (Administradores) del dispositivo. De lo contrario, puede aparecer el error `Access is denied` (Acceso denegado), o uno similar, en el cliente de administración al intentar conectarse con el dispositivo mediante MMC.

Los dispositivos Sun ZFS Storage 7000 admiten las siguientes funciones de Administración de equipos:

Visor de eventos de SMB

Puede usar el complemento Visor de eventos de MMC para desplegar el log de las aplicaciones, el log de seguridad y el log del sistema. Estos logs muestran el contenido de los logs de alertas, auditoría y sistema de Sun ZFS Storage 7000. La siguiente captura de pantalla ilustra el log de aplicaciones y el cuadro de diálogo de propiedades de un evento de error.

FIGURA 11-3 Visor de eventos de SMB



Gestión de recursos compartidos de SMB

La gestión de recursos compartidos permite hacer lo siguiente:

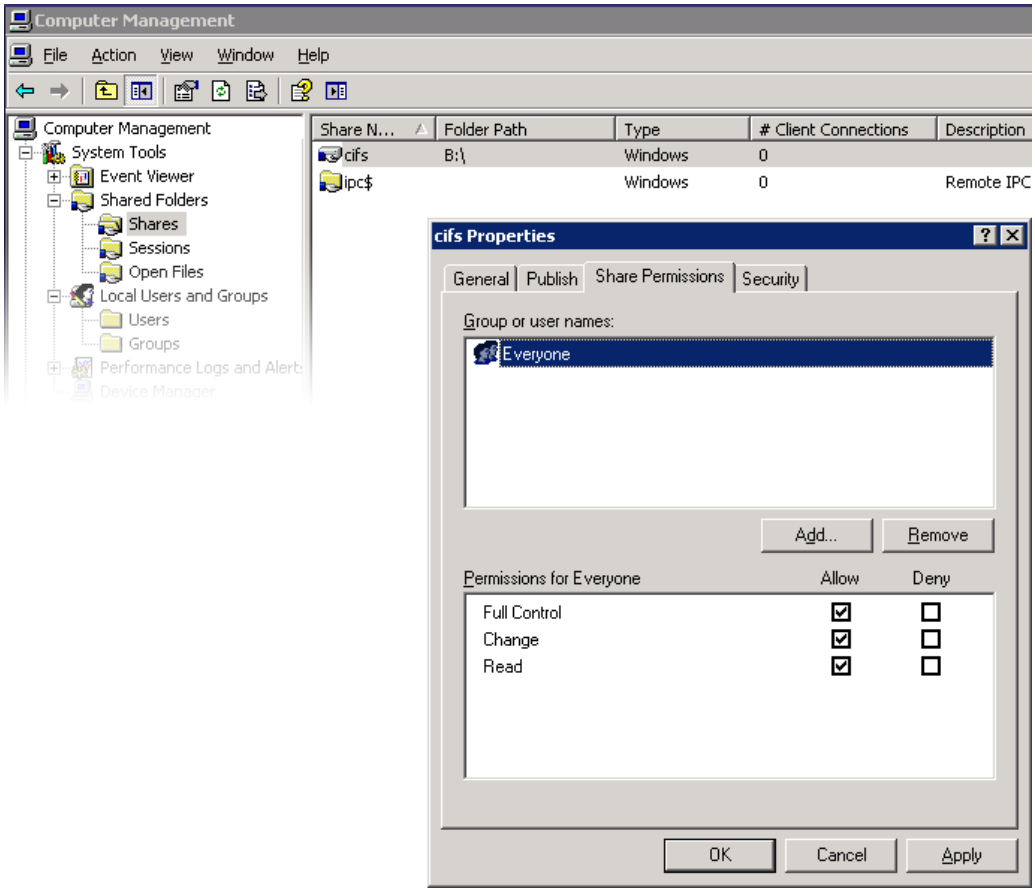
- Enumerar recursos compartidos

- 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

FIGURA 11-4 Propiedades de permisos de recursos compartidos de SMB



Usuarios, grupos y conexiones de SMB

Se admiten las funciones siguientes:

- 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

FIGURA 11-5 Archivos abiertos por conexión

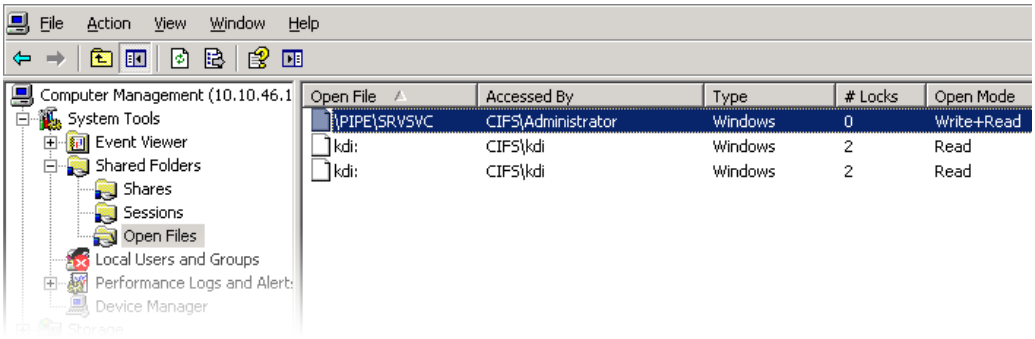
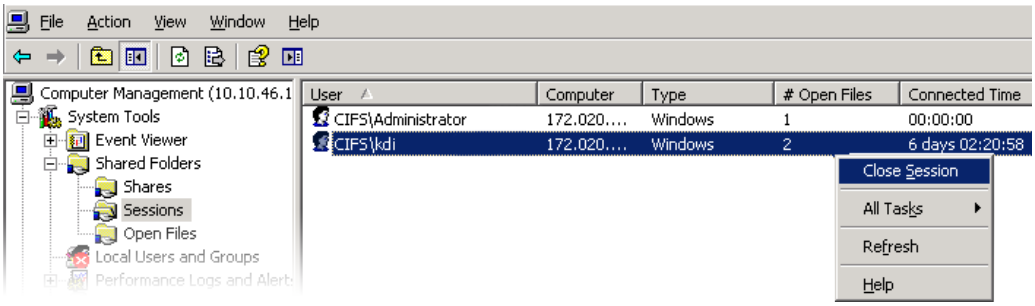


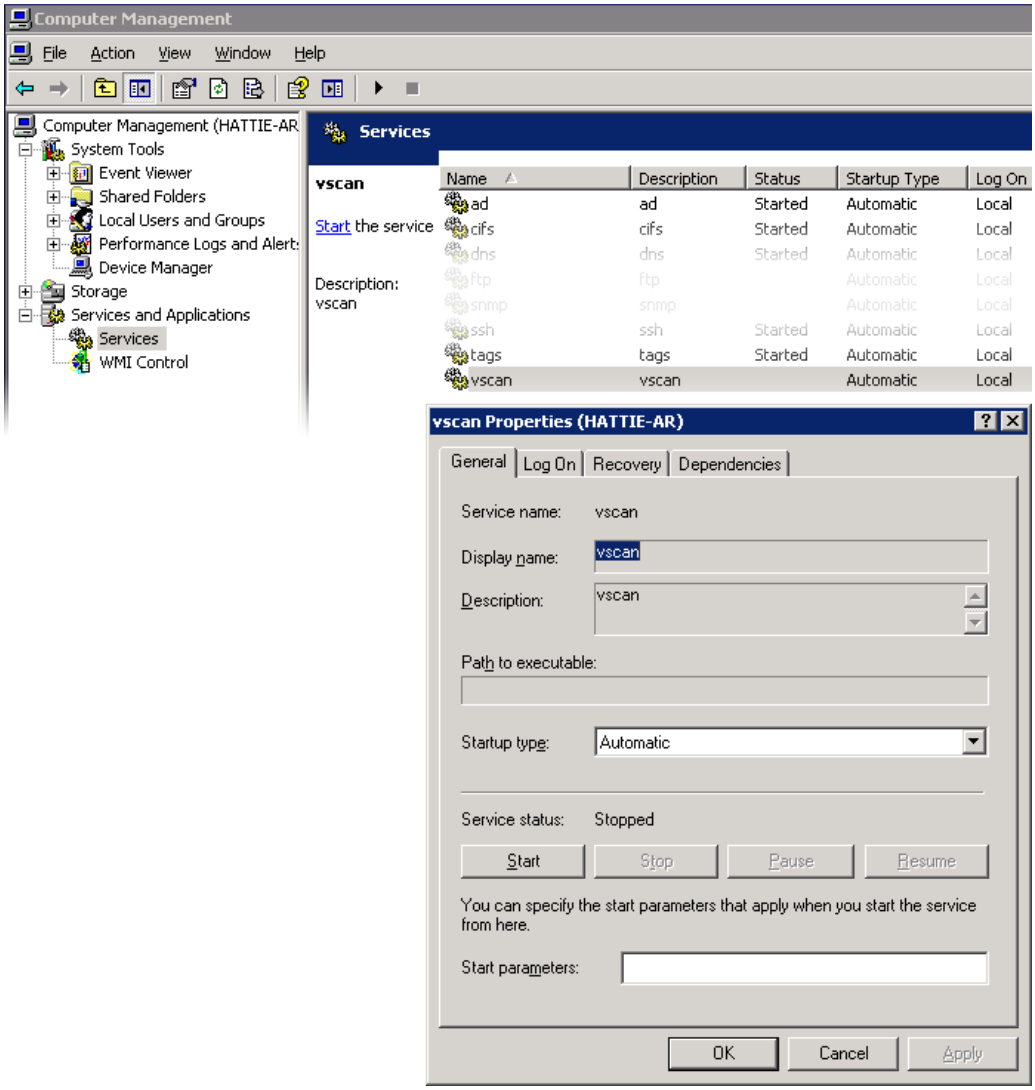
FIGURA 11-6 Sesiones abiertas



Visualización de servicios de SMB

Permite generar listas de servicios del dispositivo ZFSSA. No se pueden activar ni desactivar servicios con la aplicación Administración de equipos de MMC. La siguiente captura de pantalla ilustra las propiedades generales del servicio vscan.

FIGURA 11-7 Propiedades de vscan



Para garantizar que sólo 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 11-12 Usuarios y operaciones permitidas

USUARIOS	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 con la BUI

▼ Configuración inicial

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 Maintenance (Mantenimiento) > System (Sistema) de la BUI o la CLI. En general, en la BUI, se deben seguir los siguientes pasos para realizar la configuración inicial.

1. **Configure dispositivos de red, enlaces de datos e interfaces.**
2. **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.**
3. **Configure las propiedades deseadas y haga clic en el botón Apply (Aplicar) para agregarlas a la lista.**
4. **Configure cada interfaz como activa o en espera, según corresponda.**
5. **Haga clic en el botón Apply (Aplicar) en la parte superior de la página para confirmar los cambios.**
6. **Configure el DNS.**
7. **Proporcione el nombre del dominio base.**

8. **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.**
9. **Configure las claves de autenticación de NTP para garantizar la sincronización del reloj.**
10. **Haga clic en el ícono para agregar una nueva clave.**
11. **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.**
12. **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.**
13. **Especifique Active Directory como servicio de directorio para los usuarios y los grupos.**
14. **Configure el dominio del directorio.**
15. **Haga clic en el botón Apply (Aplicar) para confirmar los cambios.**
16. **Configure una agrupación de almacenamiento.**
17. **Haga clic en el ícono para agregar una nueva agrupación.**
18. **Establezca el nombre de la agrupación.**
19. **En la pantalla "Allocate and verify storage" (Asignar y verificar almacenamiento), configure la asignación de JBOD para la agrupación de almacenamiento. La asignación de JBOD puede ser ninguna, medio, todo. Si no se detecta ningún JBOD, compruebe el cableado y la alimentación de energía.**
20. **Haga clic en el botón Commit (Confirmar) para pasar a la siguiente pantalla.**
21. **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.**
22. **Haga clic en el botón Commit (Confirmar) para activar la configuración.**
23. **Configure la asistencia técnica remota.**

24. **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.**

25. **Escriba el nombre de usuario y la contraseña de la cuenta en línea. Aparece una declaración de privacidad para que lea.**

26. **Elija con cuál de los equipos de inventario desea registrarse. El equipo predeterminado para cada cuenta es igual al nombre de usuario de la cuenta con "$" como prefijo.**

27. **Confirme los cambios de configuración inicial.**

▼ Configuración de Active Directory

1. **Cree una cuenta para el dispositivo en el dominio de Active Directory. Consulte la documentación de Active Directory para obtener instrucciones detalladas.**

2. **En la pantalla Configuration (Configuración) > Services (Servicios) > Active Directory, haga clic en el botón Join Domain (Unirse a dominio).**

3. **Especifique el dominio de Active Directory, el usuario administrativo y la contraseña administrativa, y haga clic en el botón Apply (Aplicar) para confirmar los cambios.**

▼ Configuración de proyectos y recursos compartidos

1. **Cree un proyecto.**

2. **En la pantalla Shares (Recursos compartidos), haga clic en el ícono  para expandir el panel Projects (Proyectos).**

3. **Haga clic en el enlace Add... (Agregar...) para agregar un nuevo proyecto.**

4. **Especifique el nombre del proyecto y aplique el cambio.**

5. **Seleccione un nuevo proyecto del panel Projects (Proyectos).**

6. **Haga clic en el ícono  para agregar un sistema de archivos.**

7. **Haga clic en el ícono del sistema de archivos.**

8. **Haga clic en el enlace General y anule la selección de la casilla de verificación Heredar de proyecto.**

9. **En /export, elija un punto de montaje, aunque el acceso a los recursos compartidos de SMB sea por nombre de recurso.**

10. **En la pantalla Protocols (Protocolos) del proyecto, configure el nombre del recurso con el valor "activado".**

11. **Active sharesmb y la ACL de nivel de recurso compartido para el proyecto.**

12. **Haga clic en el botón Apply (Aplicar) para activar la configuración.**

▼ Configuración de servicios de datos de SMB

1. **En la pantalla Configuration (Configuración) > Services (Servicios) > SMB, haga clic en el ícono para activar el servicio.**

2. **Configure las propiedades de SMB según las recomendaciones de la sección sobre propiedades de esta página y haga clic en el botón Apply (Aplicar) para activar la configuración.**

3. **En la pantalla Configuration (Configuración) > Services (Servicios) > SMB, haga clic en el enlace Autohome (Directorio principal automático) para configurar las reglas de directorio principal automático de manera de asignar los clientes SMB a directorios principales según las descripciones de la sección sobre las reglas de directorio principal automático anterior y haga clic en el botón Apply (Aplicar) para activar la configuración.**

4. **En la pantalla Configuration (Configuración) > Services (Servicios) > SMB, haga clic en el enlace Local Groups (Grupos locales) y use el ícono para agregar usuarios administradores u operadores de copia de seguridad a los grupos locales según las descripciones de la sección sobre grupos locales anterior y haga clic en el botón Apply (Aplicar) para activar la configuración.**

Servicio 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 Services (Servicios).

Propiedades de FTP

Configuración general de FTP

TABLA 11-13 Configuración general de FTP

Propiedad	Descripción
Port (for incoming connections)	Puerto por el que el servicio FTP escucha. El valor predeterminado es 21.
Maximum # of connections ("0" for unlimited)	La cantidad máxima de conexiones FTP simultáneas. Configure este valor de manera de cubrir la cantidad prevista de usuarios simultáneos. El valor predeterminado es 30, porque cada conexión crea un proceso de sistema, y si se permiten demasiadas (miles), se podría producir un ataque de DoS.
Turn on delay engine to prevent timing attacks	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.
Default login root	Ubicación del inicio de sesión de FTP. El valor predeterminado es "/" y corresponde al elemento superior de la jerarquía de recursos compartidos. Todos los usuarios son direccionados a esta ubicación cuando inician sesión después de autenticarse correctamente con el servicio FTP.
Logging level	Nivel de detalle del log proftpd.
Permissions to mask from newly created files and dirs	Permisos de archivo para eliminar al crear archivos. De forma predeterminada, el permiso de escritura de grupos y mundial está enmascarado para evitar que cualquiera pueda escribir en cargas recientes.

Configuración de seguridad de FTP

TABLA 11-14 Configuración de seguridad de FTP

Propiedad	Descripción
Enable SSL/TLS	Permite conexiones FTP cifradas SSL/TLS. Con esta opción, se garantiza que la transacción FTP esté cifrada. De forma predeterminada, está desactivada.
Port for incoming SSL/TLS connections	Puerto por el que el servicio FTP cifrado SSL/TLS escucha. El valor predeterminado es 21.
Permit root login	Permite al usuario root iniciar sesiones FTP. Desactivada de forma predeterminada, porque la autenticación FTP es de texto sin formato, lo que representa un riesgo de seguridad por ataques de examen de red.
Maximum # of allowable login attempts	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 predeterminado es 3.
Permit foreign data connection addresses	Permite que las conexiones FTP externas activen la transferencia directa de archivos entre servidores FTP. Esta propiedad está desactivada de forma predeterminada.

Los cambios realizados en las propiedades de los servicios se documentan en las secciones “Configuración de servicios con la BUI” [202] y “Configuración de servicios con la CLI” [204]. Los nombres de propiedades de CLI son versiones más abreviadas que las mencionadas anteriormente.

Logs de FTP

TABLA 11-15 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.

Configuración de FTP con la BUI

▼ Permiso de acceso FTP a un recurso compartido

1. **Vaya a Configuration (Configuración) ->Services (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 Shares (Recursos compartidos).**
4. **Vaya a la sección Protocols (Protocolos) y compruebe que esté activado el acceso FTP. El modo de acceso (lectura/lectura+escritura) se puede configurar en esta sección también.**

Servicio HTTP

El servicio HTTP proporciona acceso a sistemas de archivos mediante los protocolos HTTP y HTTPS y la extensión WebDAV (sistema distribuido de creación y control de versiones web) de HTTP. Esto 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. Las URL para acceder a estos recursos compartidos de HTTP y HTTPS tienen los siguientes formatos, respectivamente:

http://*hostname*/shares/*mountpoint*/*share_name*

https://*hostname*/shares/*mountpoint*/*share_name*

El servidor HTTPS utiliza un certificado de seguridad autofirmado.

Propiedades de HTTP

TABLA 11-16 Propiedades de HTTP

Propiedad	Descripción
Require client 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, el propietario de los archivos creados será el servicio HTTP, con

Propiedad	Descripción
	usuario "nobody" (nadie). Consulte la sección sobre autenticación a continuación.
Protocols	Seleccione los métodos de acceso que admiten HTTP, HTTPS o ambos.
HTTP Port (for incoming connections)	Puerto HTTP, el valor predeterminado es 80.
HTTPS Port (for incoming secure connections)	Puerto HTTP, el valor predeterminado es 443.

Los cambios realizados en las propiedades de los servicios se documentan en las secciones “Configuración de servicios con la BUI” [202] y “Configuración de servicios con la CLI” [204]. Los nombres de propiedades de CLI son versiones más abreviadas que las mencionadas anteriormente.

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.

Sólo la autenticación HTTP básica está admitida. 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" (nadie) para el control de acceso. El propietario de los archivos creados por los usuarios con privilegios será "nobody" (nadie).

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" (nadie), y todos los usuarios se consideran como "nobody" (nadie) 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).

Logs de HTTP

TABLA 11-17 Logs de HTTP

Log	Descripción
network-http:apache22	Log del servicio HTTP.

Configuración de HTTP

▼ Permiso de acceso HTTP a un recurso compartido

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 Shares (Recursos compartidos).**
4. **Vaya a la sección Protocols (Protocolos) y compruebe que esté activado el acceso HTTP. El modo de acceso (lectura/lectura+escritura) se puede configurar en esta sección también.**

Servicio NDMP

El servicio NDMP (protocolo simple de administración de redes) permite al sistema participar en operaciones de copia de seguridad y restauración basadas en NDMP controladas por un cliente remoto de NDMP denominado DMA (aplicación de gestión de datos). Con NDMP, los datos de usuario del dispositivo (es decir, 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 utilizar para hacer copias de seguridad ni restaurar datos de configuración del sistema. En cambio, use la función de [[Maintenance:System:ConfigurationBackup| Configuration copia de seguridad y restauración de configuración]].

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 visualizar en la pantalla “Estado de NDMP” [60]. 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 sistema 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 11-18 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

Tipo de copia de seguridad	Detalles
	ni recuperación de acceso directo (DAR), pero puede ser más rápido para algunos conjuntos de datos. Sólo 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 dispositivos de la serie 7000 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, y 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.

Copias de seguridad de NDMP con "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, sólo 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 nueva instantánea y hace la copia de seguridad de la ruta dada a partir de la instantánea. Cuando se completa la copia de seguridad, se destruye la instantánea. Si la ruta 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, los tipos "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 en la copia los metadatos del 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 tal 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.

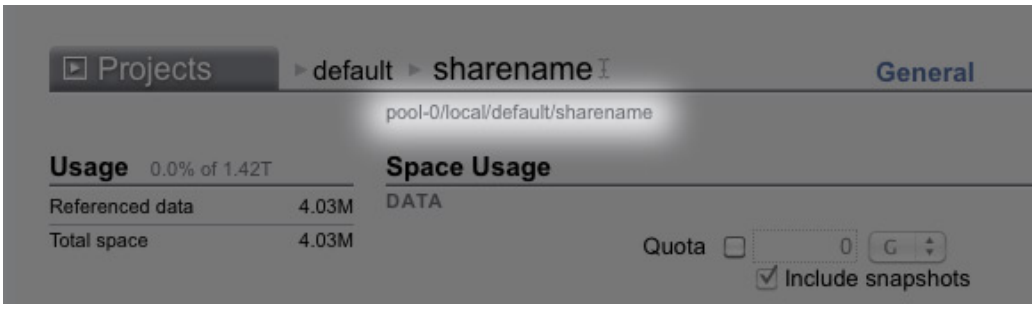
Durante una restauración, si ya existe un proyecto que se hubiese vuelto a crear automáticamente, se usa el proyecto existente en lugar de crearlo automáticamente. Si ya existe un recurso compartido que se hubiese vuelto a crear y si el punto de montaje del recurso coincide con lo que espera el dispositivo 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 nuevo recurso compartido que se cree recibirá un nombre único que comience con "ndmp-" y el punto de montaje correcto.

Se recomienda restaurar un flujo cuyos conjuntos de datos ya no existan en el dispositivo, lo que permitirá al dispositivo volver a crear los conjuntos de datos tal 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.

Copias de seguridad de NDMP con "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, el nombre se encuentra debajo del nombre del recurso compartido:

FIGURA 11-8 Nombre de recursos compartidos de NDMP



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 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 11-19 Copias de seguridad de nombres canónicos y recursos compartidos

Nombre canónico	Recursos compartidos que se incluyen en la copia de seguridad
pool-0/local/default	Nueva instantánea del proyecto local denominado "default" y todos sus recursos compartidos.
pool-0/local/default@yesterday	Instantánea denominada "yesterday" del proyecto local "default" y todos sus recursos compartidos que tienen la instantánea "yesterday".
pool-0/local/default/code	Nueva instantánea del recurso compartido "code" del proyecto local "default". "code" puede ser un sistema de archivos o un volumen.
pool-0/local/default/code@yesterday	Instantánea denominada "yesterday" del recurso compartido "code" del proyecto local "default". "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 predeterminado 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 ACTUALIZACIÓN=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. Consulte "Copias de seguridad incrementales" a continuación para obtener información detallada.

Metadatos de recursos compartidos: En las copias de seguridad "zfs", siempre se incluyen los metadatos de recursos compartidos (es decir, la configuración del recurso compartido). 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. Consulte "Copias de seguridad incrementales" a continuación para obtener información detallada.

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 11-20 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 conjuntos de datos) del servicio NDMP (consulte la sección Propiedades, a continuación).

Propiedades de NDMP

La configuración del servicio NDMP tiene las siguientes propiedades:

TABLA 11-21 Propiedades de NDMP

Propiedad	Descripción
Version	Versión de NDMP admitida por la DMA.
TCP port (v4 only)	El puerto de conexión predeterminado de NDMP es 10000. NDMPv3 usa siempre este puerto. NDMPv4 permite utilizar un puerto diferente de ser necesario.
Default restore pool(s)	Al hacer una restauración completa con los tipos "tar" o "dump", el sistema vuelve a crear los conjuntos de datos si todavía no hay un recurso compartido montado en el destino. Como el protocolo NDMP especifica sólo 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. Sólo 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 predeterminada de manera aleatoria.
Ignore metadata-only changes	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 sólo los metadatos, por ejemplo, permisos o propietarios. Esta opción se aplica solamente a las copias de seguridad "tar" y "dump" incrementales y está desactivada de forma predeterminada.

Propiedad	Descripción
Allow token-based backup	Activa o desactiva el método basado en token para la copia de seguridad ZFS. Esta propiedad está desactivada de forma predeterminada.
ZFS rollback before restore (sólo 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 de esa instantánea. Esta configuración normalmente es controlada por la DMA mediante la variable de entorno "ZFS_FORCE" (consulte "Copias de seguridad incrementales", más arriba), pero esta propiedad se puede usar para anular la configuración de la DMA y revertir siempre estos conjuntos de datos o nunca revertirlos. 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.
Allow direct access recovery	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.
Restore absolute paths (sólo 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 de forma predeterminada.
DMA tape mode (para unidades conectadas localmente)	Especifica si la DMA espera una semántica System V o BSD. La opción predeterminada es System V, que es la recomendada para la mayoría de las DMA. Esta opción se aplica sólo 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, sólo 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.
DMA username and password	Se utiliza para autenticar DMA. El sistema usa MD5 para la autenticación de usuarios.

Los cambios realizados en las propiedades de los servicios se documentan en las secciones “Configuración de servicios con la BUI” [202] y “Configuración de servicios con la

CLI" [204]. Los nombres de propiedades de CLI son versiones más abreviadas que las mencionadas anteriormente.

Logs de NDMP

TABLA 11-22 Logs de NDMP

Log	Descripción
system-ndmpd:default	Log del servicio NDMP.

Replicación remota

El servicio de replicación remota facilita la replicación de proyectos y recursos compartidos entre dispositivos Oracle ZFS Storage Appliance. Esta funcionalidad se describe en detalle en la documentación del Capítulo 13, Replicación.

Cuando se activa este servicio, el dispositivo recibe actualizaciones de replicación de otros dispositivos y envía actualizaciones de replicación para los proyectos y los recursos compartidos locales en función de las acciones que tenga configuradas. Cuando el servicio está desactivado, las actualizaciones de replicación entrantes fallan y no se replica ningún proyecto ni recurso compartido local.

Este servicio no tiene ninguna propiedad, pero permite a los administradores ver los dispositivos que tienen datos replicados en este dispositivo (en Sources [Orígenes]) y configurar los dispositivos en los que se puede replicar este dispositivo (en Targets [Destinos]). En la documentación del Capítulo 13, Replicación, se puede encontrar información detallada acerca de la gestión de la replicación remota.

Migración shadow

El servicio de migración shadow permite la migración automática de datos desde fuentes externas o internas. Esta funcionalidad se describe en mayor detalle en la documentación del Capítulo 14, Migración shadow. 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.

Propiedades de migración shadow

TABLA 11-23 Propiedades de migración shadow

Propiedad	Descripción
Number of Threads	Cantidad de subprocesos 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).

Los cambios realizados en las propiedades de los servicios se documentan en las secciones “Configuración de servicios con la BUI” [202] y “Configuración de servicios con la CLI” [204]. Los nombres de propiedades de CLI son versiones más abreviadas que las mencionadas anteriormente.

Servicio 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.

Propiedades de SFTP

- Port (for incoming connections) (Puerto [para conexiones entrantes]): puerto por el que el servicio SFTP escucha. El valor predeterminado es 218.
- Permit root login (Permitir inicio de sesión root): permite los inicios de sesión de SFTP del usuario root. Está desactivado por defecto.
- Logging level (Nivel de registro): nivel de detalle de los mensajes de log de SFTP.
- SFTP Keys (Claves SFTP): 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, hay que incluir la propiedad "user" (usuario) 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.

Los cambios realizados en las propiedades de los servicios se documentan en las secciones “Configuración de servicios con la BUI” [202] y “Configuración de servicios con la

CLI” [204]. Los nombres de propiedades de CLI son versiones más abreviadas que las mencionadas anteriormente.

Puerto 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. De forma predeterminada, el puerto SFTP es el 218 y se debe especificar en el cliente SFTP antes de establecer la conexión. Por ejemplo, un cliente OpenSolaris que use SFTP se conectaría con el siguiente comando:

```
manta# sftp -o "Port 218" root@guppy
```

Logs de SFTP

TABLA 11-24 Logs de SFTP

Log	Descripción
network-sftp:default	Registra eventos del servicio SFTP.

Configuración de SFTP

▼ Permiso de acceso SFTP a un recurso compartido

1. **Vaya a Configuration (Configuración) ->Services (Servicios).**
2. **Compruebe que el servicio SFTP esté activado y en línea. De no ser así, actívelo.**
3. **Seleccione o agregue un recurso compartido en la pantalla Shares (Recursos compartidos).**
4. **Vaya a la sección Protocols (Protocolos) y compruebe que esté activado el acceso SFTP. El modo de acceso (lectura/lectura+escritura) se puede configurar en esta sección también.**

▼ Configuración de los servicios de SFTP para acceso remoto

1. **Cree un usuario local o un usuario de red (LDAP o NIS) con el rol de administrador apropiado. (Consulte el Capítulo 7, Configuración de usuario).**
2. **Use el comando `ssh-keygen -t dsa` en el host o el cliente de 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 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:**
5. **: ssh-dss AAAAB3NzaC1kc3MAAACBAPMMs5h8UWk1NPf/VJDDEo0OAwT +s6iZxkCmmrgAmLfTX9izWk+**
6. **: bsvNldOlXN/6EgkusLjo/+UaEt5+704vMHClRaq3AlVHLS5tVjeX3iCs +fDo0qwXZg3Brh8QBAaWk3**
7. **:ywr2osuIl1tHh4v/HwEAHZq5mVWXav0pO3bgmxl0/ +VAAAAFQDlJxnm52DfyEdQQMTY+jRVvzGwMQA**
8. **: AAIAhTP6Ey +2gGFiCKkvUofsco4d8pbqH8duE9P6Y88s0+opuj52GkAdRUt2fRrdM9Cf3h4lIOc8Bw9**
9. **: bZIBzrCKBNWBUdZG56tsfLdilW6vS6gxKrmL2v7fSp9WYPsxZGhOLfU29zW4n2WVcVHbGyFEoVe +taq**
10. **: aq+AYJaWoHnjZL1/ LpQAAAIAOLc8+uc3hDOcK3pAkYdg8b2rYIGOAZU4py0rq24DGPeVHd5h5jbe4p**
11. **:WDM70uYqGCOPYiOKeEoMNJpczRX5qjl +BfoUY4sH24WWwsKkT8XX9PUAa0WT+7axEqg2N6YelaTJ95J**
12. **:vMaj6E7HkAIra2Sj2H/LSDktL42UL+j1Wx5A== username sunray**
13. **Vaya a Configuration (Configuración) ->Services (Servicios) > SFTP. En Keys (Claves), haga clic en el signo más (+).**
14. **En la ventana New Key (Nueva clave), seleccione DSA.**

15. **Copie sólo la porción de la clave (en el ejemplo anterior, comienza con AAAA y termina con Wx5A==) y péguela en el campo Key (Clave). Introduzca el nombre de usuario y agregue un comentario como recordatorio.**

16. **: Nota: La clave no debe incluir ningún espacio en blanco.**

17. **Vaya a Shares (Recursos compartidos) > Shares (Recursos compartidos) y haga clic en el signo más (+) para crear un sistema de archivos.**

18. **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).**

19. **Haga clic en el ícono del lápiz para configurar las propiedades del recurso compartido. (Consulte el Capítulo 12, Recursos compartidos, proyectos y esquemas).**

20. **Para acceder al recurso compartido, use el comando `sftp` como se muestra en estos ejemplos:**

21. **: sftp -o "port=218" <username> 10.x.x.151:/export/sftp**

22. **: Conectando con 10.x.xx.151...**

23. **: Cambiando a: /export/sftp**

24. **: sftp>**

25. **: Ejemplo con la opción -v:**

26. **: sftp -v -o "IdentityFile=/home/<username>/.ssh/id_dsa" -o "port=218"**

27. **: root 10.x.xx.151:/export/sftp**

Servicio 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 el Capítulo 6, Configuración de red de área de almacenamiento.

Para consultar ejemplos de administración de destinos SRP, consulte el Capítulo 6, Configuración de red de área de almacenamiento.

Servicio 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 enumerar directorios y, en la actualidad, no ofrece la autenticación de usuarios.

Propiedades de TFTP

TABLA 11-25 Propiedades de TFTP

Propiedad	Descripción
Default Root Directory	Ubicación del inicio de sesión de TFTP. El valor predeterminado es "/export" y corresponde al elemento superior de la jerarquía de recursos compartidos. Todos los usuarios serán direccionados a esta ubicación cuando inicien sesión después de autenticarse correctamente con el servicio TFTP.

Los cambios realizados en las propiedades de los servicios se documentan en las secciones "Configuración de servicios con la BUI" [202] y "Configuración de servicios con la CLI" [204]. Los nombres de propiedades de CLI son versiones más abreviadas que las mencionadas anteriormente.

Configuración de TFTP

▼ Permiso de acceso TFTP a un recurso compartido

1. **Vaya a Configuration (Configuración) ->Services (Servicios).**
2. **Compruebe que el servicio TFTP esté activado y en línea. De no ser así, actívelo.**
3. **Seleccione o agregue un recurso compartido en la pantalla Shares (Recursos compartidos).**

4. **Vaya a la sección Protocols (Protocolos) y compruebe que esté activado el acceso TFTP. El modo de acceso (lectura/lectura+escritura) se puede configurar en esta sección también.**

Servicio 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. 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 ha delegado privilegios de lectura pueden no pasarse de inmediato a cuarentena.

Propiedades de los análisis de virus

TABLA 11-26 Propiedades de los análisis de virus

Propiedad	Descripción
Maximum file size to scan	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 predeterminado es 1 GB.
Allow access to files that exceed maximum file size	Esta opción está activada de forma predeterminada y permite el acceso a los archivos cuyo tamaño es mayor que el 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.

Los cambios realizados en las propiedades de los servicios se documentan en las secciones “Configuración de servicios con la BUI” [202] y “Configuración de servicios con la CLI” [204]. Los nombres de propiedades de CLI son versiones más abreviadas que las mencionadas anteriormente.

Extensiones de archivo de análisis de virus

En esta sección, se describe cómo controlar qué archivos se analizan. Con el valor predeterminado, " * ", 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 11-27 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. En el siguiente ejemplo, no se analizará ningún archivo:

TABLA 11-28 Acciones de análisis de virus

Acción	Patrón
No analizar	*
Explorar	exe
Explorar	com
Explorar	bat
Explorar	doc
Explorar	zip

Acción	Patrón
No analizar	data-archive*.zip

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 11-29 Propiedades de los motores de análisis

Propiedad	Descripción
Enable	Se usa este motor de análisis.
Host	Nombre de host o dirección IP del servidor del motor de análisis.
Maximum Connections	Cantidad máxima de conexiones simultáneas. Algunos motores de análisis funcionan mejor si la cantidad de conexiones se limita a 8.
Port	Puerto para el motor de análisis.

Logs de análisis de virus

TABLA 11-30 Logs de análisis de virus

Log	Descripción
vscan	Log del servicio de análisis de virus.

Configuración de análisis de virus

▼ Configuración de análisis de virus para un recurso compartido

1. **Vaya a Configuration (Configuración) ->Services (Servicios) ->Virus Scan (Análisis de virus).**
2. **Configure las propiedades deseadas.**

3. **Aplique o confirme la configuración.**
4. **Vaya a Shares (Recursos compartidos).**
5. **Edite un sistema de archivos o un proyecto.**
6. **Seleccione la ficha General.**
7. **Active la opción Virus scan (Análisis de virus).**

Servicio NIS

El servicio de información de red (NIS) es un servicio de nombres para la gestión centralizada. El dispositivo puede actuar como cliente NIS para usuarios y grupos, de manera que:

- Los usuarios de NIS puedan iniciar sesión en el "Servicio FTP" [232] y el "Servicio HTTP" [234].
- 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.

Tenga en cuenta que los UID y los GID 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 aplicaciones futuras.

Propiedades de NIS

TABLA 11-31 Propiedades de NIS

Propiedad	Descripción
Domain	Dominio de NIS que se utiliza.
Server(s): Search using broadcast	El dispositivo envía una difusión de NIS para localizar servidores NIS para ese dominio.
Server(s): Use listed servers	Nombres de host o direcciones IP de los servidores NIS.

Los cambios realizados en las propiedades de los servicios se documentan en las secciones "Configuración de servicios con la BUI" [202] y "Configuración de servicios con la CLI" [204]. Los nombres de propiedades de CLI son versiones más abreviadas que las mencionadas anteriormente.

El dispositivo se conecta con el primer servidor NIS de la lista o encontrado mediante difusión, y pasa al siguiente si ese servidor deja de responder.

Logs de NIS

TABLA 11-32 Logs de NIS

Log	Descripción
network-nis-client:default	Log del servicio de clientes NIS.
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.

Configuración de NIS

▼ Agregación de un administrador de dispositivos desde NIS

Si tiene un usuario existente en NIS que desea iniciar sesión con sus credenciales de NIS y administrar el dispositivo:

1. **Vaya a Configuration (Configuración) ->Services (Servicios) -> NIS.**
2. **Configure el dominio y las propiedades de servidor de NIS.**
3. **Aplique o confirme la configuración.**
4. **Vaya a Configuration (Configuración) -> Users (Usuarios).**
5. **Agregue el usuario con tipo "directory" (directorio).**
6. **Configure el nombre de usuario con el nombre de usuario que tiene en NIS.**
7. **Continúe con las instrucciones del Capítulo 7, Configuración de usuario para agregar autorizaciones a este usuario.**

Servicio de LDAP

LDAP (protocolo ligero de acceso a directorios) es un servicio de directorio para centralizar la gestión de usuarios, grupos, nombres de host y otros recursos (denominados objetos). En el dispositivo, este servicio actúa como cliente LDAP de manera que:

- Los usuarios de LDAP puedan iniciar sesión en el “Servicio FTP” [232] y el “Servicio HTTP” [234].
- 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.
- Los usuarios de LDAP puedan recibir privilegios para la administración del dispositivo. El dispositivo complementa la información de LDAP con su propia configuración de privilegios.
- El certificado del servidor LDAP puede ser autofirmado.
- No se puede proporcionar una lista de certificados de CA de confianza; cada certificado debe ser aceptado individualmente por el administrador del dispositivo.
- Cuando caduca un certificado de un servidor LDAP, se debe suprimir el servidor de la lista y volver a agregarlo para aceptar el nuevo certificado.

Tenga en cuenta que 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.

Propiedades de LDAP

Consulte la configuración apropiada para su entorno con el administrador del servidor LDAP.

- Protect LDAP traffic with SSL/TLS (Proteger el tráfico de LDAP con SSL/TLS): Use TLS (seguridad de capa de transporte, descendiente de SSL) para establecer conexiones seguras con el servidor LDAP.
- Base search DN (Nombre distintivo de búsqueda base): Proporciona el nombre distintivo del objeto base, que es el punto inicial para las búsquedas de directorio.
- Search scope (Ámbito de búsqueda): Define los objetos del directorio LDAP que se buscan, en relación con el objeto base. Los resultados de la búsqueda se pueden limitar sólo a objetos que se encuentran directamente debajo del objeto de búsqueda base (un nivel) o pueden incluir cualquier objeto que se encuentra por debajo del objeto de búsqueda base (subárbol). La configuración predeterminada es un nivel.
- Authentication method (Método de autenticación): Método usado para autenticar el dispositivo ante el servidor LDAP. El dispositivo admite autenticación simple (RFC 4513), SASL/DIGEST-MD5 y SASL/GSSAPI. Si se usa el método de autenticación simple, se debe activar SSL/TLS para que el nombre distintivo y la contraseña del usuario no se

envíen como texto sin formato. Al usar el método de autenticación SASL/GSSAPI, sólo el nivel de credencial de autoenlace está disponible.

- Bind credential level (Nivel de credencial de enlace): credenciales usadas para autenticar el dispositivo ante el servidor LDAP.
- * La opción Anonymous (Anónimo) permite al dispositivo acceder sólo a los datos que están disponibles para todos.
- * La opción Proxy hace que el servicio se enlace por medio de una cuenta especificada.
- * Proxy DN (Nombre distintivo de proxy): nombre distintivo de la cuenta usada para la autenticación del proxy.
- * Proxy Password (Contraseña de proxy): contraseña de la cuenta usada para la autenticación del proxy.
- * Self (Automática): se realiza la autenticación automática del dispositivo con la identidad y las credenciales del usuario. La autenticación propia se puede usar solo con el método de autenticación SASL/GSSAPI.
- Schema definition (Definición de esquema): esquema usado por el dispositivo. Esta propiedad permite a los administradores anular el descriptor de búsqueda predeterminado, las asignaciones de atributos y las asignaciones de clases de objetos para usuarios, grupos y grupos de red. Para obtener más información, consulte “Servicio de LDAP” [256].
- Servers (Servidores): lista de servidores LDAP que se utilizan. Si se especifica solo un servidor, el dispositivo usa solo ese servidor y los servicios LDAP no están disponibles si ese servidor falla. Si se especifican varios servidores, los servidores que están en funcionamiento se pueden usar en cualquier momento sin preferencia. 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.

Asignaciones personalizadas de LDAP

Para buscar usuarios y grupos en el directorio de LDAP, el dispositivo usa un descriptor de búsqueda y debe saber cuáles son las clases de objeto que corresponden a los usuarios y los grupos, y cuáles son los atributos que corresponden a las propiedades necesarias. De manera predeterminada, el dispositivo usa las clases de objeto especificadas por RFC 2307 (*posixAccount* y *posixGroup*) y los descriptores de búsqueda predeterminados que se muestran en la lista siguiente, pero se puede personalizar para diferentes entornos. El nombre distintivo de la búsqueda base usado en los siguientes ejemplos es *dc=example,dc=com*:

TABLA 11-33 Asignaciones personalizadas de LDAP

Descriptor de búsqueda	Valor por Defecto	Ejemplo
users	ou=people,*base search DN*	ou=people,dc=example,dc=com
groups	ou=group,*base search DN*	ou=group,dc=example,dc=com
netgroups	ou=netgroup,*base search DN*	ou=netgroup,dc=example,dc=com

El descriptor de búsqueda, las clases de objeto y los atributos usados se pueden personalizar con la propiedad Schema definition (Definición de esquema). Para anular el descriptor de búsqueda predeterminado, escriba el nombre distintivo completo que desea utilizar. El dispositivo usará este valor sin modificar y no tendrá en cuenta los valores de las propiedades Base search DN (Nombre distintivo de búsqueda base) y Search scope (Ámbito de búsqueda). Para anular los objetos y los atributos de usuarios, grupos y grupos de red, elija la ficha apropiada ("Users" [Usuarios], "Groups" [Grupos] o "Netgroups" [Grupos de red]) y especifique asignaciones con la sintaxis *default = new*, donde *default* es el valor predeterminado y *new* es el valor que desea usar. Por ejemplo:

- Para usar *unixaccount* en lugar de *posixAccount* como clase de objeto de usuario, escriba posixAccount = unixaccount en las asignaciones de clases de objetos en la ficha Users (Usuarios).
- Para usar *employeenumber* en lugar de *uid* como atributo para los objetos de usuarios, escriba uid = employeenumber en las asignaciones de atributos en la ficha Users (Usuarios).
- Para usar *unixgroup* en lugar de *posixGroup* como clase de objeto de grupo, escriba posixGroup = unixgroup en las asignaciones de clases de objetos en la ficha Groups (Grupos).
- Para usar *groupaccount* en lugar de *cn* como atributo para los objetos de grupos, escriba cn = groupaccount en las asignaciones de atributos en la ficha Groups (Grupos).

La siguiente es una lista de las clases y los atributos de objetos que puede ser necesario asignar:

- Clases:
- * posixAccount
- * posixGroup
- * shadowAccount
- Atributos de usuarios:
- * uid
- * uidNumber
- * gidNumber
- * gecos
- * homeDirectory
- * loginShell
- * userPassword
- Atributos de grupos:
- * uid
- * memberUid
- * cn
- * userPassword
- * gidNumber

- * member
- * uniqueMember
- * memberOf
- * isMemberOf

Logs de LDAP

A continuación, se muestra un ejemplo de log.

TABLA 11-34 Logs de LDAP

Log	Descripción
appliance-kit-nsswitch:default	Log del servicio de nombres del dispositivo, por medio del cual se hacen las consultas de LDAP.

Configuración de LDAP

▼ Agregación de un administrador de dispositivos

Para permitir que un usuario de LDAP existente inicie sesión con las credenciales de LDAP y administre el dispositivo, use el siguiente procedimiento:

1. **En la página Configuration (Configuración) => Services (Servicios) => LDAP, introduzca las propiedades que desee utilizar. Para obtener información acerca de las propiedades disponibles, consulte “Propiedades de LDAP” [256].**
2. **Para aplicar las propiedades seleccionadas, haga clic en Apply (Aplicar) o haga clic en Revert (Revertir) para volver a empezar.**
3. **Para agregar servidores LDAP, en la sección Servers (Servidores) haga clic en el ícono para agregar . Para obtener información acerca de los servidores, consulte la sección sobre servidores en “Propiedades de LDAP” [256].**
4. **Para configurar el servidor LDAP, en el cuadro New LDAP Server (Nuevo servidor LDAP) introduzca la dirección del servidor LDAP y seleccione el origen del certificado de LDAP que desee usar. Para el origen del certificado, si selecciona la opción Server (Servidor), se inicia una búsqueda en el servidor actual y se recupera el certificado (de manera no segura) y se lo usa en futuro para validar el certificado presentado posteriormente.**

5. **En la página Configuration (Configuración) => Users (Usuarios), use los nombres de usuario de LDAP para agregar usuarios según sea necesario. Para obtener información acerca del procedimiento para agregar usuarios, consulte el Capítulo 7, Configuración de usuario.**

Active Directory

El servicio Active Directory 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 tiene dos modos: modo de dominio y modo de grupo de trabajo, que dictan la manera en la que se autentican los usuarios de "SMB" [214]. Al operar en modo de dominio, los clientes "SMB" [214] se autentican por medio del controlador de dominios de AD. En el modo de grupo de trabajo, los clientes "SMB" [214] se autentican localmente como usuarios locales. Consulte "Users" para obtener más información acerca de usuarios locales.

Propiedades de Active Directory

Unión a un dominio de Active Directory

Si la cuenta todavía no existe en Active Directory de manera predeterminada, se crea automáticamente una cuenta de confianza del equipo para el sistema en el contenedor predeterminado para las cuentas de equipos (cn = equipos) 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:

- Active Directory Domain (Dominio de Active Directory): nombre completo o nombre de NetBIOS de un dominio de Active Directory
- User (Usuario): usuario de AD que tiene credenciales para crear una cuenta en Active Directory.

- Password (Contraseña): contraseña del usuario administrativo.
- Additional DNS Search Path (Ruta de búsqueda de DNS adicional): cuando se especifica esta propiedad opcional, las consultas de DNS se resuelven según este dominio, además del dominio de DNS primario y el dominio de Active Directory
- Organizational Unit (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.
- Use Pre-created Account (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.

Unión a un grupo de trabajo de Active Directory

En la siguiente lista, se describen las propiedades configurables para unirse a grupos de trabajo.

- Windows Workgroup (Grupo de trabajo de Windows): un grupo de trabajo

Los cambios realizados en las propiedades de los servicios se documentan en las secciones “Configuración de servicios con la BUI” [202] y “Configuración de servicios con la CLI” [204]. Los nombres de propiedades de CLI son versiones más abreviadas que las mencionadas anteriormente.

Dominios y grupos de trabajo de Active Directory

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 dado. 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.

Uniéndose a un grupo de trabajo se abandona de manera implícita un dominio de Active Directory, y los clientes “SMB” [214] que se almacenan en la base de datos de Active Directory no pueden conectarse a los recursos compartidos.

Si se configuró un dominio kerberos para poder utilizar NFS con Kerberos, el sistema no se puede configurar para unirse a un dominio de Active Directory.

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 dominio, mientras que las firmas de SMB se aplican a las comunicaciones entre los clientes SMB y el dispositivo de almacenamiento.

Compatibilidad de Active Directory con Windows Server 2012

Windows Server 2012 se admite completamente en la versión de software 2011.1.5 y posterior.

Compatibilidad de Active Directory con Windows Server 2008

TABLA 11-35 Compatibilidad de Active Directory con Windows Server 2008

Versión de Windows	Versiones de software admitidas	Soluciones alternativas
Windows Server 2003	Todas	Ninguna.
Windows Server 2008 SP1	2009.Q2 3.1 y anteriores	Aplique la revisión para KB957441, según sea necesario (consulte la sección B).
	2009.Q2 4.0 - 2011.1.1	Debe aplicar las revisiones para KB951191 y KB957441, según sea necesario (consulte las secciones A y B).
	2011.1.2 y posteriores	Debe aplicar la revisión para KB951191 (consulte la sección A).
Windows Server 2008 SP2	2009.Q2 4.0 - 2011.1.1	Consulte la sección C.
	2011.1.2 y posteriores	Ninguna.
Windows Server 2008 R2	2009.Q2 4.0 - 2011.1.1	Consulte la sección C.
	2011.1.2 y posteriores	Ninguna.

Compatibilidad de Active Directory con Windows Server 2008, sección A: Problema de Kerberos (KB951191)

- Si realiza una actualización a la versión 2009.Q2.4.0 o posteriores y el controlador de dominio de Windows 2008 ejecuta Windows Server 2008 SP2 o R2, no es necesario realizar ninguna acción.
- Si realiza una actualización a la versión 2009.Q2.4.0 o posteriores y el controlador de dominio de Windows 2008 ejecuta Windows Server 2008 SP1, debe aplicar la revisión que se describe en KB951191 o instalar Windows 2008 SP2.

Compatibilidad de Active Directory con Windows Server 2008, sección B: Problema de NTLMv2 (KB957441)

- Lo siguiente se aplica únicamente si el dispositivo ejecuta una versión de software anterior a 2011.1.2:
- Si el controlador de dominio ejecuta Windows Server 2008 SP1, también debe aplicar la revisión para http://support.microsoft.com/kb/957441/ (http://support.microsoft.com/kb/957441/) que resuelve un problema de NTLMv2 que no deja que el dispositivo se una al dominio con la configuración predeterminada de LMCompatibilityLevel.
- Si LMCompatibilityLevel en el controlador de dominio de Windows 2008 SP1 está configurada con el valor 5, se debe instalar esta revisión. Después de aplicar la revisión, debe crear y configurar una nueva clave de registro, como se describe en KB957441.
- Si realiza una actualización a la versión 2011.1.2 o posteriores, no necesita la revisión antes mencionada.

Compatibilidad de Active Directory con Windows Server 2008, sección C: Nota sobre NTLMv2

- Lo siguiente se aplica únicamente si el dispositivo ejecuta una versión de software anterior a 2011.1.2: Si el controlador de dominio ejecuta Windows Server 2008 SP2 o R2, no es necesario aplicar la revisión, pero se debe aplicar la configuración de registro que se describe en KB957441.
- Si realiza una actualización a la versión 2011.1.2 o posteriores, no se necesita ninguna acción.

Configuración de Active Directory con la BUI

▼ Unión a un dominio

1. **Configure un sitio de Active Directory en el contexto de "SMB" [214] (opcional).**
2. **Configure un controlador de dominio preferido en el contexto de "SMB" [214] (opcional).**
3. **Active "NTP" [278] 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" [274] se delegue correctamente al dominio de Active Directory o agregue la dirección IP del controlador de dominio como servidor de nombres adicional en el contexto de "DNS" [274].**
5. **Configure el dominio, el usuario administrativo y la contraseña administrativa de Active Directory.**
6. **Aplique o confirme la configuración.**

▼ Unión a un grupo de trabajo

1. **Configure el nombre del grupo de trabajo.**
2. **Aplique o confirme la configuración.**

Configuración de Active Directory con la CLI

Para demostrar la interfaz de la CLI, en el siguiente ejemplo, se muestra la configuración existente, se une a un grupo de trabajo y, finalmente, se une a un dominio.

▼ Ejemplo de configuración de Active Directory con la CLI

1. **Visualice una configuración existente.**

```
twofish:> configuration services ad
twofish:configuration services ad> show
Properties:
                    <status> = online
                        mode = domain
                      domain = eng.fishworks.com

Children:
                          domain => Join an Active Directory domain
                       workgroup => Join a Windows workgroup
```

2. **Observe que el dispositivo actualmente se encuentra operando en el dominio "eng.fishworks.com". En el siguiente ejemplo, se abandona ese dominio y se une a un grupo de trabajo.**

```
twofish:configuration services ad> workgroup
twofish:configuration services ad workgroup> set workgroup=WORKGROUP
twofish:configuration services ad workgroup> commit
twofish:configuration services ad workgroup> done
twofish:configuration services ad> show
Properties:
                    <status> = disabled
                        mode = workgroup
                   workgroup = WORKGROUP
```

3. **En el siguiente ejemplo, se muestra la configuración del sitio y el controlador de dominio preferido como preparación para unirse a otro dominio.**

```
twofish:configuration services ad> done
twofish:> configuration services smb
twofish:configuration services smb> set ads_site=sf
twofish:configuration services smb> set pdc=192.168.3.21
twofish:configuration services smb> commit
twofish:configuration services smb> show
Properties:
                    <status> = online
                lmauth_level = 4
                         pdc = 192.168.3.21
                    ads_site = sf
twofish:configuration services smb> done
```

4. **En el siguiente ejemplo, se muestra cómo unirse al nuevo dominio tras configurar las propiedades. Al unirse a un dominio de AD, debe establecer el usuario y la contraseña cada vez que confirme el nodo.**

```
twofish:> configuration services ad
twofish:configuration services ad> domain
twofish:configuration services ad domain> set domain=fishworks.com
twofish:configuration services ad domain> set user=Administrator
twofish:configuration services ad domain> set password=*******
```

```
twofish:configuration services ad domain> set searchdomain=it.fishworks.com
twofish:configuration services ad domain> commit
twofish:configuration services ad domain> done
twofish:configuration services ad> show
Properties:
                    <status> = online
                        mode = domain
                      domain = fishworks.com
```

Servicio de asignación de identidad

El servicio de asignación de identidad gestiona las identidades de usuarios de Windows y Unix simultáneamente mediante UID (y GID) de Unix y SID de Windows tradicionales. Para obtener información acerca del uso de la BUI y la CLI para la asignación de identidades, consulte “Configuración de servicios con la BUI” [202] y “Configuración de servicios con la CLI” [204].

Propiedades de la asignación de identidades

El servicio de asignación de identidad crea y mantiene una base de datos de asignaciones entre identificadores SID, UID y GID. Es posible utilizar tres enfoques de asignación diferentes; si ya hay asignaciones para una identidad dada, el servicio crea una asignación efímera. Se pueden utilizar los siguientes modos de asignación:

Asignación basada en reglas de asignación de identidad

El enfoque de la asignación basada en reglas requiere la creación de diversas reglas que asignan identidades por nombre. Estas reglas establecen equivalencias entre identidades de Windows e identidades de Unix.

Asignación basada en directorios de asignación de identidad

La asignación basada en directorios implica la anotación de un objeto de “LDAP” [256] o “Active Directory” [260] con información acerca de la manera en la que la identidad del objeto se asigna a una identidad equivalente en la plataforma opuesta. Si se usa la asignación basada en directorios, se deben asignar los siguientes atributos:

- AD Attribute - Unix User Name (Atributo de AD - Nombre de usuario de Unix): nombre incluido en la base de datos de AD para el nombre de usuario de Unix equivalente
- AD Attribute - Unix Group Name (Atributo de AD - Nombre de grupo de Unix): nombre incluido en la base de datos de AD para el nombre de grupo de Unix equivalente

- Native LDAP Attribute - Windows User Name (Atributo nativo de LDAP - Nombre de usuario de Windows): nombre incluido en la base de datos de LDAP para la identidad de Windows equivalente

Los nombres de propiedades de CLI son versiones más abreviadas que las mencionadas anteriormente.

Para obtener información acerca de la ampliación de los esquemas de “Active Directory” [260] o “LDAP” [256], consulte la sección Gestión de asignación de identidad basada en directorios para usuarios y grupos (mapa de tareas) de la Guía de administración de Solaris CIFS.

Asignación de identidad IDMU

Microsoft ofrece una función denominada "Gestión de identidades para Unix" o IDMU. Este software está disponible para Windows Server 2003 y viene incluido con Windows Server 2003 R2 y versiones posteriores. Esta función es parte de lo que se denomina "Servicios para Unix" en su forma independiente.

El uso principal de IDMU es permitir el uso de Windows como servidor NIS/NFS. IDMU agrega el panel "UNIX Attributes" (Atributos de UNIX) a la interfaz de usuario Users and Computers (Usuarios y equipos) de Active Directory, que permite al administrador especificar una serie de parámetros relacionados con UNIX: UID, GID, shell de inicio de sesión, directorio principal y similares para grupos. Estos parámetros están disponibles por medio de AD mediante un esquema similar (pero no igual) al de RFC2307 y por medio del 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 usa enfoque, no se puede utilizar ningún otro método de asignación basada en directorios.

Reglas de asignación de identidad

Esta página permite crear asignaciones mediante las siguientes propiedades:

- Mapping type (Tipo de asignación): autoriza o deniega credenciales. Para obtener más información, consulte “Asignaciones de denegación” [266].
- Mapping direction (Dirección de asignación): dirección de la asignación. Una asignación puede asignar credenciales en ambas direcciones, sólo de Windows a Unix o sólo de Unix a Windows. Para obtener más información, consulte “Símbolos de dirección de reglas de asignación” [266].

- Windows Domain (Dominio de Windows): dominio de Active Directory de la identidad de Windows.
- Windows Identity (Identidad de Windows): nombre de la identidad de Windows.
- Unix Identity (Identidad de Unix): nombre de la identidad de Unix.
- Unix Identity Type (Tipo de identidad de Unix): tipo de la identidad de Unix, que puede ser usuario o grupo.

Asignaciones de denegación

Las reglas de asignación de denegación evitan que los usuarios obtengan asignaciones, incluidos los identificadores efímeros, del servicio de asignación de identidad. Puede crear asignaciones de denegación para todo el dominio o específicas para un usuario tanto para usuarios de Windows como de Unix. Por ejemplo, puede crear una asignación para denegar el acceso a recursos compartidos de “SMB” [214] para todos los usuarios de Unix del grupo "guest". No puede crear asignaciones de denegación que están en conflicto con otras asignaciones.

Símbolos de dirección de reglas de asignación

Después de crear una asignación basada en nombres, los siguientes símbolos indican la semántica de cada regla.

- align="center"| - Asigna identidades de Windows a identidades de Unix, e identidades de Unix a identidades de Windows.
- align="center"| - Asigna identidades de Windows a identidades de Unix.
- align="center"| - Asigna identidades de Unix a identidades de Windows.
- align="center"| - Impide que las identidades de Windows obtengan credenciales.
- align="center"| - Impide que las identidades de Unix obtengan credenciales.

Si un ícono aparece de color gris en lugar de color negro (, , , ,), esa regla coincide con una identidad de Unix que no se puede resolver.

Asignaciones de asignación de identidad

La página Mappings (Asignaciones) muestra la manera en la que diversas identidades se asignan en función del conjunto de reglas actual. Al especificar una entidad de Windows o una entidad de Unix, la entidad se asigna a su identidad correspondiente en la plataforma opuesta. La información resultante que aparece en las secciones Propiedades de usuario y Propiedades de grupo indica la identidad de la asignación, incluido el origen de la asignación. Los botones

Show (Mostrar) y Flush (Vaciar) de esta página permiten visualizar y suprimir asignaciones existentes.

Logs de asignación de identidad

En esta página, se muestra un log de la actividad reciente.

Prácticas recomendadas de asignación de identidad

- La configuración de reglas de asignación de identidad específicas se utiliza solamente cuando se desea que el mismo usuario tenga acceso a un conjunto de archivos comunes como cliente "NFS" [208] y cliente "SMB" [214]. Si los clientes "NFS" [208] y "SMB" [214] 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" [214]. 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, debe configurar 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 sólo 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 *sólo* 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" [214] usa el servicio de asignación de identidad para asociar identidades de Windows y Unix. Cuando el servicio "SMB" [214] 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” [214] y “NFS” [208]. Mediante la asociación de las identidades de Windows y Unix, los clientes “NFS” [208] y “SMB” [214] pueden compartir la misma identidad y así tener acceso al mismo conjunto 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” [260]. Cada usuario y cada grupo tienen un SID. El SID identifica de manera exclusiva el usuario o el grupo 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” [254] y “LDAP” [256]. Cada usuario y cada grupo de Unix tienen 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.

Distinción entre mayúsculas y minúsculas en la asignación de identidades

Los nombres de Windows no distinguen entre mayúsculas y minúsculas, y 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, sólo 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, después de pasar el nombre de usuario de Windows a minúsculas, el servicio sigue sin encontrar ninguna coincidencia, no se obtiene una asignación para el usuario. Puede crear una regla para establecer coincidencias entre cadenas que difieren sólo en el uso de mayúsculas y minúsculas. Por ejemplo, puede crear una asignación específica

de usuario que asigne el usuario "JSmith@sun.com" 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.

Persistencia de la asignación

Cuando el servicio de asignación de identidad proporciona una asignación de nombre, la almacena 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. Si el servidor “SMB” [214] solicita una asignación para el usuario una vez que la primera asignación caduca, el servicio vuelve a evaluar las asignaciones.

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.

Reglas de asignación de identidad para todo el dominio

Una regla de asignación para todo el dominio establece coincidencias entre algunos de los nombres de un dominio de Windows, o todos ellos, con nombres de Unix. Los nombres de usuario de ambos lados deben coincidir exactamente (excepto por conflictos con la distinción entre mayúsculas y minúsculas, que están sujetos a las reglas ya descritas). Por ejemplo, puede crear una regla bidireccional para asociar todos los usuarios de Windows de "myDomain.com" con los usuarios de Unix que tengan el mismo nombre, y viceversa. O bien, puede crear una regla que asigne todos los usuarios de Windows en "myDomain.com" del grupo "Engineering" a los usuarios de Unix que tengan el mismo nombre. No puede crear asignaciones para todo el dominio que están en conflicto con otras asignaciones.

Asignación efímera

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 una asignación de denegación. 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” [214] ven que el propietario de ese archivo es la identidad de Windows. Sin embargo, los clientes “NFS” [208] ven que el propietario del archivo es "nobody" (nadie).

Ejemplos de asignación de identidad

En el siguiente ejemplo, se muestra cómo agregar dos reglas basadas en nombres desde la CLI. En el primer ejemplo, se crea una asignación bidireccional basada en nombres entre un usuario de Windows y un usuario de Unix.

```
twofish:> configuration services idmap
twofish:configuration services idmap> create
twofish:configuration services idmap (uncommitted)> set
   windomain=eng.fishworks.com
twofish:configuration services idmap (uncommitted)> set winname=Bill
twofish:configuration services idmap (uncommitted)> set direction=bi
twofish:configuration services idmap (uncommitted)> set unixname=wdp
twofish:configuration services idmap (uncommitted)> set unixtype=user
twofish:configuration services idmap (uncommitted)> commit
twofish:configuration services idmap> list
MAPPING      WINDOWS ENTITY                    DIRECTION    UNIX ENTITY
idmap-000    Bill@eng.fishworks.com        (U) ==           wdp (U)
```

En el siguiente ejemplo, se crea una asignación de denegación para impedir que todos los usuarios de Windows de un dominio obtengan credenciales.

```
twofish:configuration services idmap> create
twofish:configuration services idmap (uncommitted)> list
Properties:
                    windomain = (unset)
                      winname = (unset)
                    direction = (unset)
                     unixname = (unset)
                     unixtype = (unset)

twofish:configuration services idmap (uncommitted)> set
   windomain=guest.fishworks.com
twofish:configuration services idmap (uncommitted)> set winname=*
twofish:configuration services idmap (uncommitted)> set direction=win2unix
twofish:configuration services idmap (uncommitted)> set unixname=
twofish:configuration services idmap (uncommitted)> set unixtype=user
twofish:configuration services idmap (uncommitted)> commit
twofish: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)
```

Configuración de asignaciones de identidad

▼ Configuración de asignaciones de identidad

1. **Asegúrese de estar unido al menos a un dominio de Active Directory. Para obtener información acerca de Active Directory, consulte la sección “Active Directory” [260].**
2. **En la página Configuration (Configuración) => Services (Servicios) => Identity Mapping (Asignación de identidad) => Properties (Propiedades), seleccione el modo de asignación que desee utilizar. Para obtener información acerca de los modos de asignación, consulte “Propiedades” [266].**
3. **Si selecciona la asignación basada en directorios, debe configurar propiedades adicionales. Para obtener más información acerca de estas propiedades, consulte “Asignación basada en directorios” [266].**
4. **Para guardar la configuración, haga clic en Apply (Aplicar), o haga clic en Revert (Revertir) para volver a empezar.**
5. **Para crear asignaciones, haga clic en Rules (Reglas).**
6. **En la página Rules (Reglas), haga clic en el ícono para agregar  .**
7. **En el cuadro Add Mapping Rule (Agregar regla de asignación), introduzca la información requerida. Para obtener más información, consulte “Reglas” [266].**
8. **Para guardar la configuración, haga clic en Add (Agregar), o haga clic en Cancel (Cancelar). Cuando se crea una asignación, la asignación aparece en la lista Rules (Reglas).**

▼ Visualización o vaciado de asignaciones

1. **Para ver asignaciones existentes, en la página Configuration (Configuración) => Services (Servicios) => Identity Mapping (Asignación de identidad) => Mappings (Asignaciones), introduzca la información requerida. Para obtener información acerca de asignaciones, consulte “Asignaciones” [266].**
2. **Haga clic en Show (Mostrar). Aparece la asignación designada.**

3. **Para suprimir la asignación, haga clic en Flush (Vaciar). La asignación se elimina.**

Servicio DNS

El cliente DNS (servicio de nombres de dominio) proporciona la capacidad de resolver direcciones IP como nombres de host, y viceversa, y está siempre activado en el dispositivo. 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, incluidos los logs de "Logs" de "Manual de servicio del cliente de Oracle ZFS Storage Appliance " para indicar la ubicación desde la cual un usuario realizó una acción auditable y los "Análisis" de "Guía de análisis de Oracle ZFS Storage Appliance " para proporcionar estadísticas por cliente.

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.

Propiedades de DNS

TABLA 11-36 Propiedades de DNS

Propiedad	Descripción
DNS Domain	Nombre de dominio en el que se busca primero al realizar búsquedas de nombres de host parciales.
DNS Server(s)	Uno o varios servidores DNS. Se deben usar direcciones IP.
Allow IPv4 non-DNS resolution	Las direcciones IPv4 se pueden resolver como nombres de host, y viceversa, mediante NIS y/o LDAP si se configuran y activan.
Allow IPv6 non-DNS resolution	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 servicios con la BUI" [202] y "Configuración de servicios con la CLI" [204]. Los nombres de propiedades de CLI son versiones más abreviadas que las mencionadas anteriormente.

Configuración de DNS

La CLI incluye comandos incorporados para `nslookup` y `getent hosts`, que se pueden usar para probar si la resolución de nombres de host está funcionando:

```
caji:> nslookup deimos
192.168.1.109   deimos.sf.fishworks.com
caji:> getent hosts deimos
192.168.1.109   deimos.sf.fishworks.com
```

Logs de DNS

TABLA 11-37 Logs de DNS

Log	Descripción
network-dns-client:default	Registra los eventos del servicio DNS

Active Directory y DNS

Si tiene pensado utilizar “Active Directory” [260], los servidores debe poder resolver registros de servidores y nombres de host en la porción 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.

Resolución no DNS

DNS es un mecanismo estándar, de nivel empresarial, altamente escalable y confiable para generar 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 sólo 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 sólo 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

El dispositivo no admite operaciones sin DNS y, si se realizara alguna, podrían obtenerse resultados no deseables. Hay varias características que no funcionan correctamente sin DNS, entre las que se incluyen:

- Los "Análisis" de "Guía de análisis de Oracle ZFS Storage Appliance " no podrán resolver direcciones de cliente como nombres de host.
- La función de "Active Directory" [260] no funcionará (no podrá unirse a dominios).
- El uso de "LDAP" [256] 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.

Servicio de direccionamiento dinámico

Protocolos de enrutamiento dinámico RIP y RIPng

RIP (protocolo de información de enrutamiento) 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 "dynamic" (dinámico) en la tabla de enrutamiento. RIP y RIPng escuchan en los puertos UDP 520 y 521, respectivamente.

Logs de enrutamiento dinámico

TABLA 11-38 Enrutamiento dinámico

Log	Descripción
network-routing-route:default	Registra eventos del servicio RIP.
network-routing-ripng:quagga	Registra eventos del servicio RIPng.

Servicio 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 el Capítulo 4, Configuración de red.

Propiedades de IPMP

TABLA 11-39 Propiedades de IPMP

Propiedad	Descripción
Failure detection latency	Tiempo que necesita IPMP para declarar que una interfaz de red ha fallado y conmutar por error sus direcciones IP.
Enable fail-back	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 servicios con la BUI” [202] y “Configuración de servicios con la CLI” [204]. Los nombres de propiedades de CLI son versiones más abreviadas que las mencionadas anteriormente.

Logs de IPMP

TABLA 11-40 Logs de IPMP

Log	Descripción
network-initial:default	Registra el proceso de configuración de red.

Servicio 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.

Propiedades de NTP

TABLA 11-41 Propiedades de NTP

Propiedad	Descripción	Ejemplos
multicast address	Escriba una dirección de multidifusión para localizar automáticamente un servidor NTP.	224.0.1.1
NTP server(s)	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
NTP Authentication Keys	Escriba una o varias claves de autenticación de NTP para que use el dispositivo al autenticar la validez de los servidores NTP. Consulte la sección Autenticación, a continuación.	Clave de autenticación: 10, tipo: ASCII, clave privada: SUN7000

Los cambios realizados en las propiedades de los servicios se documentan en las secciones “Configuración de servicios con la BUI” [202] y “Configuración de servicios con la CLI” [204]. Los nombres de propiedades de CLI son versiones más abreviadas que las mencionadas anteriormente.

Validación de NTP

Si se proporciona una configuración no válida, aparece un mensaje de 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 de NTP

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, sino que son utilizadas solamente por 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 11-42 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.

Reloj de NTP de la BUI

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.

Consejos para NTP

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 11-43 Sincronización del reloj de NTP

Log	Descripción
network-ntp:default	Log del servicio NTP.

Configuración de NTP con la BUI

Para agregar claves de autenticación de NTP en la BUI, haga clic en el ícono del signo más y especifique el número de clave, el tipo de clave y el valor privado de la nueva clave. Después de haber agregado la clave, aparecerá como opción al lado de cada servidor NTP especificado.

▼ Sincronización del reloj de la BUI

Esta tarea permite configurar la hora del dispositivo para que coincida con la hora del explorador.

1. **Desactive el servicio NTP.**
2. **Haga clic en el botón SYNC (Sincronizar).**

Configuración de NTP con la CLI

En `configuration services ntp`, edite las autorizaciones con el comando `authkey`:

```
clownfish:configuration services ntp> authkey
clownfish:configuration services ntp authkey>
```

Desde este contexto, se pueden agregar nuevas claves con el comando `create`:

```
clownfish:configuration services ntp authkey> create
clownfish:configuration services ntp authkey-000 (uncommitted)> get
                        keyno = (unset)
                         type = (unset)
                          key = (unset)
clownfish:configuration services ntp authkey-000 (uncommitted)> set keyno=1
                        keyno = 1 (uncommitted)
clownfish:configuration services ntp authkey-000 (uncommitted)> set type=A
                         type = A (uncommitted)
clownfish:configuration services ntp authkey-000 (uncommitted)> set key=coconuts
                          key = ******** (uncommitted)
clownfish:configuration services ntp authkey-000 (uncommitted)> commit
clownfish:configuration services ntp authkey>
```

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, para usar la clave creada más arriba para autenticar los servidores "gefilte" y "carp":

```
clownfish:configuration services ntp> set servers=gefilte,carp
                      servers = gefilte,carp (uncommitted)
clownfish:configuration services ntp> set serverkeys=1,1
                   serverkeys = 1,1 (uncommitted)
clownfish:configuration services ntp> commit
clownfish:configuration services ntp>
```

Para autenticar el servidor "gefilte" con la clave 1, "carp" con la clave 2 y "dory" con la clave 3:

```
clownfish:configuration services ntp> set servers=gefilte,carp,dory
                      servers = gefilte,carp,dory (uncommitted)
clownfish:configuration services ntp> set serverkeys=1,2,3
                   serverkeys = 1,2,3 (uncommitted)
clownfish:configuration services ntp> commit
clownfish:configuration services ntp>
```

Para autenticar los servidores "gefilte" y "carp" con la clave 1, y tener, además, un servidor NTP no autenticado "dory":

```
clownfish:configuration services ntp> set servers=gefilte,carp,dory
                      servers = gefilte,carp,dory (uncommitted)
clownfish:configuration services ntp> set serverkeys=1,1,0
                   serverkeys = 1,1,0 (uncommitted)
clownfish:configuration services ntp> commit
clownfish:configuration services ntp>
```

Servicio de 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 la función Oracle Auto Service Request (ASR) (http://oracle.com/asr). La función ASR de Oracle abre automáticamente las solicitudes de servicio (SR) de problemas específicos informados por el dispositivo. La operación de registro conecta el dispositivo con My Oracle Support (MOS) 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 "Problemas" de "Manual de servicio del cliente de Oracle ZFS Storage Appliance ".

- Latidos: se envían mensajes diarios de latidos a Oracle para indicar que el sistema está encendido y 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 las versiones actuales de software y hardware, la configuración del dispositivo 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 "Sistema" de "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 "Notificación de actualizaciones de software" de "Manual de servicio del cliente de Oracle ZFS Storage Appliance ".

Debe registrarse para usar el servicio de asistencia técnica remota.

Cuenta de inicio de sesión único de Oracle

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 http://support.oracle.com (http://support.oracle.com) y haga clic en Register (Registrarse) para crear su cuenta.

Propiedades de la asistencia técnica remota

Los cambios realizados en las propiedades de los servicios se documentan en las secciones "Configuración de servicios con la BUI" [202] y "Configuración de servicios con la CLI" [204]. El servicio de asistencia técnica remota se conoce como `scrk` en la CLI.

Proxy web del servicio de 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 información detallada acerca de los paquetes de asistencia, consulte "Sistema" de "Manual de servicio del cliente de Oracle ZFS Storage Appliance ".

TABLA 11-44 Configuración del proxy web del servicio de asistencia técnica remota

Propiedad	Descripción
Use proxy	Conexión mediante un proxy web.
Host/port	Nombre de host o dirección IP del proxy web, y puerto.
Username	Nombre de usuario del proxy web.
Password	Contraseña del proxy web.

Registro del dispositivo

Para registrar el dispositivo por primera vez, debe proporcionar una cuenta de inicio de sesión único de Oracle. Vaya a My Oracle Support (http://support.oracle.com) y haga clic en Register (Registrarse) para crear su cuenta.

▼ Registro del dispositivo con la BUI

1. **Escriba el nombre de usuario y la contraseña de la cuenta de inicio de sesión único de Oracle. Aparece una declaración de confidencialidad. Se puede visualizar en cualquier momento tanto en la BUI como en la CLI.**
2. **Confirme los cambios.**
3. **Use My Oracle Support (http://support.oracle.com/) para completar la activación de Auto Service Request (ASR) (http://oracle.com/asr). Consulte "Cómo gestionar y aprobar activos pendientes de ASR en My Oracle Support" (ID de documento 1329200.1).**

▼ Registro del dispositivo con la CLI

1. **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.**
2. **Confirme los cambios.**
3. **Use My Oracle Support (http://support.oracle.com/) para completar la activación de Auto Service Request (ASR) (http://oracle.com/asr). Consulte "Cómo gestionar y aprobar activos pendientes de ASR en My Oracle Support" (ID de documento 1329200.1).**

ejemplo 11-1 Registro mediante CLI

```
dory:> configuration services scrk
dory:configuration services scrk>set soa_id=myuser
                           soa_id = myuser(uncommitted)
dory:configuration services scrk> set soa_password=mypass
                  soa_password = ****** (uncommitted)
dory:configuration services scrk> commit
```

▼ Cambio de la información de la cuenta

1. **Haga clic en Change account... (Cambiar cuenta...) para cambiar la cuenta de inicio de sesión único de Oracle que utiliza el dispositivo.**
2. **Confirme los cambios.**
3. **Use My Oracle Support para completar la activación de Auto Service Request (ASR). Consulte "Cómo gestionar y aprobar activos pendientes de ASR en My Oracle Support" (ID de documento 1329200.1).**

Estado del servicio de asistencia técnica remota

TABLA 11-45 Estado del servicio de asistencia técnica remota

Propiedad	Descripción
Last heartbeat sent at	Hora a la que se envió el último latido al servicio de asistencia técnica de Oracle.

Estado del servicio de asistencia técnica remota

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.

Logs del servicio de asistencia técnica remota

Hay un log de eventos del servicio de asistencia técnica remota en “Logs” de “Manual de servicio del cliente de Oracle ZFS Storage Appliance ”.

REST

API de RESTful

La API de RESTful del dispositivo ZFSSA 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 ZFSSA 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.

Si desea leer documentación completa sobre la API de RESTful de ZFSSA, consulte la documentación del dispositivo Oracle ZFS Storage Appliance.

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.

Propiedades de etiquetas de servicio

TABLA 11-46 Propiedades de puertos UDP/TCP

Propiedad	Descripción
Discovery Port	Puerto UDP usado para la detección de etiquetas de servicio. El valor predeterminado es 6481.
Listener Port	Puerto TCP usado para hacer consultas de datos de etiquetas de servicio. El valor predeterminado es 6481.

Los cambios realizados en las propiedades de los servicios se documentan en las secciones “Configuración de servicios con la BUI” [202] y “Configuración de servicios con la CLI” [204]. Los nombres de propiedades de CLI son versiones más abreviadas que las mencionadas anteriormente.

Servicio 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, sólo envía correo generado automáticamente por el dispositivo.

De forma predeterminada, 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.

Propiedades SMTP

TABLA 11-47 Propiedades SMTP

Propiedad	Descripción
Send mail through smarthost	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 servidor de correo saliente.
Allow customized from address	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 que se debe usar para los mensajes de correo electrónico salientes.

Los cambios realizados en las propiedades de los servicios se documentan en las secciones “Configuración de servicios con la BUI” [202] y “Configuración de servicios con la CLI” [204]. Los nombres de propiedades de CLI son versiones más abreviadas que las mencionadas anteriormente.

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.

Logs de SMTP

TABLA 11-48 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).

Servicio SNMP

El servicio SNMP (protocolo simple de administración de redes) proporciona dos funciones diferentes en el dispositivo:

- La información de estado del dispositivo puede ser proporcionada mediante SNMP.
- Es posible configurar Capítulo 9, Configuración de alertas para enviar capturas SNMP.

Cuando este servicio está activado, las versiones v1, v2c y v3 de SNMP están disponibles. El dispositivo admite un máximo de 50 interfaces de red físicas y lógicas. La presencia de más de 50 interfaces de red podría provocar retrasos en la conexión en el caso de comandos como snmpwalk y snmpget. Si necesita más de 50 interfaces de red, póngase en contacto con la asistencia técnica de Oracle.

Propiedades de SNMP

- Version (Versión): Alterna entre v1/2c y v3.
- Community name (Nombre de la comunidad): alterna entre público e introducido por el usuario. Si selecciona user-input (Introducido por el usuario), también debe introducir un nombre de comunidad. Si selecciona v3, esta propiedad no está disponible.
- Authorized network/subnet (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.
- Appliance contact (Contacto de dispositivo): introduzca un contacto apropiado para el dispositivo.

- Username/password (Nombre de usuario y 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.
- Authentication (Autenticación): alterna entre los algoritmos de autenticación MD5 y SHA. Si selecciona v1/2c, esta propiedad no está disponible.
- Privacy (Privacidad): alterna entre None (Ninguna) y el algoritmo de cifrado DES. Si selecciona v1/2c, esta propiedad no está disponible.
- Engine ID (Identificador del motor): valor de identificador del motor procesado con un algoritmo hash por snmpd. Si no se activó SNMP, la etiqueta indica “0x000”.
- Trap destinations (Destinos de capturas): permite agregar direcciones IPv4. Use los botones “+” y “-” para agregar o quitar direcciones.

Los cambios realizados en las propiedades de los servicios se documentan en las secciones “Configuración de servicios con la BUI” [202] y “Configuración de servicios con la CLI” [204]. Los nombres de propiedades de CLI son versiones más abreviadas que las mencionadas anteriormente.

El servicio SNMP también proporciona la cadena de ubicación MIB-II. Esta propiedad se obtiene de la configuración de “System Identity” [296].

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 11-49 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.
.1.3.6.1.4.1.42	MIB de Sun Enterprise (SUN-MIB.mib.txt).
.1.3.6.1.4.1.42.2.195	Sun FM: estadísticas de la gestión de fallos (abajo se incluye un enlace al archivo de la MIB).
.1.3.6.1.4.1.42.2.225	Sun AK: estadísticas e información del dispositivo (abajo se incluye un enlace al archivo de la MIB).

Nota: Los archivos MIB de Sun están disponibles en https://*your IP address or host name*:215/docs/snmp/

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 11-50 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
.1.3.6.1.4.1.42.2.195.1.5	Recursos defectuosos de la gestión de fallos

Consulte las descripciones completas en el archivo de la MIB cuyo enlace se proporcionó más arriba.

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
- Estado de los recursos compartidos: nombre, tamaño, bytes usados y bytes disponibles

Hay tres tablas principales para leer:

TABLA 11-51 MIB de Sun AK

OID	Tabla de contenidos
.1.3.6.1.4.1.42.2.225.1.4	Información general del dispositivo

OID	Tabla de contenidos
.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

Consulte las descripciones completas en el archivo de la MIB cuyo enlace se proporcionó más arriba.

Configuración de SNMP

▼ Configuración de SNMP para proporcionar información de estado del dispositivo

1. **Configure el nombre de comunidad, la red autorizada y la cadena de contacto.**
2. **Si lo desea, configure el destino de captura con un host SNMP remoto o establezca el valor 127.0.0.1.**
3. **Aplique o confirme la configuración.**
4. **Reinicie el servicio.**

▼ Configuración de SNMP para enviar capturas

1. **Configure el nombre de comunidad, la cadena de contacto y los destinos de las capturas.**
2. **Si lo desea, configure la red autorizada para permitir el acceso de clientes SNMP o establezca el valor 127.0.0.1/8.**
3. **Aplique o confirme la configuración.**
4. **Reinicie el servicio.**
5. **Debe configurar alertas para enviar las capturas que desea recibir. Para obtener más información acerca de las alertas, consulte Capítulo 9, Configuración de alertas.**

Servicio Syslog

El servicio Relé Syslog ofrece dos funciones diferentes en el dispositivo:

- Capítulo 9, Configuración de alertas se puede utilizar para enviar mensajes Syslog a uno o varios sistemas remotos.
- 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 a continuación los detalles del formato del mensaje.
- Un mensaje que describe el evento en sí mismo. Consulte a continuación los detalles del formato del mensaje.

Los receptores Syslog se proporcionan con la mayoría de los sistemas operativos, incluidos 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" descripto por RFC 3164, o el formato de salida nuevo, con versión, descripto 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 fallas complejas en la red, es posible que se pierdan o se rechacen algunos mensajes.

Propiedades de Syslog

TABLA 11-52 Propiedades de Syslog

Propiedad	Descripción
Protocol Version	Versión del protocolo Syslog que se utilizará, ya sea Classis (Clásico) o Modern (Moderno).

Propiedad	Descripción
Destinations	Lista de direcciones IPv4 e IPv6 de destino hacia donde se transmiten los mensajes.

Los cambios realizados en las propiedades de los servicios se documentan en las secciones “Configuración de servicios con la BUI” [202] y “Configuración de servicios con la CLI” [204]. Los nombres de propiedades de CLI son versiones más abreviadas que las mencionadas anteriormente.

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 corresponderá a una de las etiquetas descriptas a continuación.

El nombre de host será el nombre canónico del dispositivo según se define en la configuración de “System Identity” [296].

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 Syslog transmitidos por los sistemas Sun Storage establecerán los campos procid, msgid y structured-data de RFC 5424 en un valor nulo (-) para indicar que estos campos no contienen datos.

El nombre de la aplicación corresponderá a una de las etiquetas descriptas a continuación.

El nombre de host será el nombre canónico del dispositivo según se define en la configuración de “System Identity” [296].

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 dispositivos Sun Storage utilizan la etiqueta del subsistema 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 Sun Storage.

TABLA 11-53 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	El servicio "Asignación de identidad" [266] para conversión de identidad de POSIX y Windows.
daemon	smbd	"Protocolo de datos SMB" [214] para acceder a recursos compartidos.

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 del campo en letras MAYÚSCULAS seguido de dos puntos y un carácter de espacio.

TABLA 11-54 Formatos de los mensajes de alerta de Syslog

Nombre del 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 informativo correspondiente que se encuentra en sun.com/msg/.
TYPE	Tipo de condición. Esta será una de las etiquetas: Fault (Fallo), que indica un error en el conector o componente de hardware, Defect (Defecto), que indica un problema de configuración o defecto de software, Alert (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

Nombre del campo	Descripción
	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.
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: Fri Aug 14 21:34:22 2009 (Vie Ago 14 21:34:22 2009).
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” [296].
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 mórtem 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 11-55 Campos de gravedad de Syslog

Gravedad	Nivel de Syslog	Descripción
Menor	LOG_WARNING	Se produjo un inconveniente que en la actualidad no afecta el servicio, pero el problema se debe corregir antes de que se torne más grave.
Mayor	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.

Ejemplos de configuración del receptor

La mayoría de los sistemas operativos incluyen un receptor Syslog, pero es posible que se requieran algunos pasos de configuración para activarlo. A continuación, se muestran algunos ejemplos de sistemas operativos comunes. Para obtener información específica sobre la configuración del receptor Syslog, consulte la documentación del sistema operativo o del software de gestión.

Configuración de un receptor Solaris

Solaris incluye un syslogd(1M) que puede actuar como receptor Syslog, pero la capacidad de recepción remota está desactivada de forma predeterminada. Para activar 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 refresh system/system-log
```

Solaris syslogd sólo comprende el protocolo Syslog clásico. Consulte la página del comando man syslog.conf(4) de Solaris para obtener información sobre cómo configurar el filtrado y el registro de los mensajes recibidos.

De forma predeterminada, 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.sf.fishpong.com poptart ak: SUNW-MSG-ID: AK-8000-LM, \
TYPE: alert, VER: 1, SEVERITY: Minor\nEVENT-TIME: Fri Aug 14 21:34:22 2009\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.
```

Configuración de un receptor Linux

La mayoría de las distribuciones de Linux incluyen un daemon sysklogd(8) que puede actuar como receptor Syslog, pero la capacidad de recepción remota está desactivada de forma predeterminada. 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 de forma predeterminada 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
```

De forma predeterminada, 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: Wed Aug 12 22:03:14 2009 \
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.
```

Identidad del sistema

Este servicio permite configurar el nombre y la ubicación del sistema. Posiblemente deba cambiar estos valores si el dispositivo se traslada a otra ubicación de la red o se utiliza con un propósito diferente.

Propiedades de identidad del sistema

TABLA 11-56 Propiedades de identidad del sistema

Propiedad	Descripción
System Name	Nombre canónico único que identifica el dispositivo y aparece en la interfaz de usuario. Este nombre es independiente de los nombres DNS que se usan para conectarse al sistema (que se configurarían en los servidores DNS remotos). Este nombre se puede cambiar en cualquier momento.
System Location	Cadena de texto que describe la ubicación física del dispositivo. Si “SNMP” [287] está activado, se exporta como la cadena *syslocation* en MIB-II.

Los cambios realizados en las propiedades de los servicios se documentan en las secciones “Configuración de servicios con la BUI” [202] y “Configuración de servicios con la CLI” [204]. Los nombres de propiedades de CLI son versiones más abreviadas que las mencionadas anteriormente.

Logs de identidad del sistema

TABLA 11-57 Logs de identidad del sistema

Log	Descripción
system-identity:node	Registra los eventos y los errores del servicio de identidad del sistema.

Servicio 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 “Análisis” de “Guía de análisis de Oracle ZFS Storage Appliance ”.

Propiedades de SSH

TABLA 11-58 Propiedades de SSH

Propiedad	Descripción	Ejemplos
Server key length	Cantidad de bits de la clave efímera.	768
Key regeneration interval	Intervalo de regeneración de claves efímeras, en segundos.	3600
Login grace period	La conexión SSH se desconecta después de esta cantidad de segundos si el cliente no logró autenticarse.	120
Permit root login	Permite al usuario root iniciar sesión con SSH.	sí

Los cambios realizados en las propiedades de los servicios se documentan en las secciones "Configuración de servicios con la BUI" [202] y "Configuración de servicios con la CLI" [204]. Los nombres de propiedades de CLI son versiones más abreviadas que las mencionadas anteriormente.

Logs de SSH

TABLA 11-59 Logs de SSH

Log	Descripción
network-ssh:default	Log de eventos y errores del servicio SSH.

Configuración de SSH

▼ Desactivación de acceso SSH para root

1. **Establezca el permiso de inicio de sesión root en false.**
2. **Aplique o confirme la configuración.**

♦ ♦ ♦ CAPÍTULO 12

Recursos compartidos, proyectos y esquemas

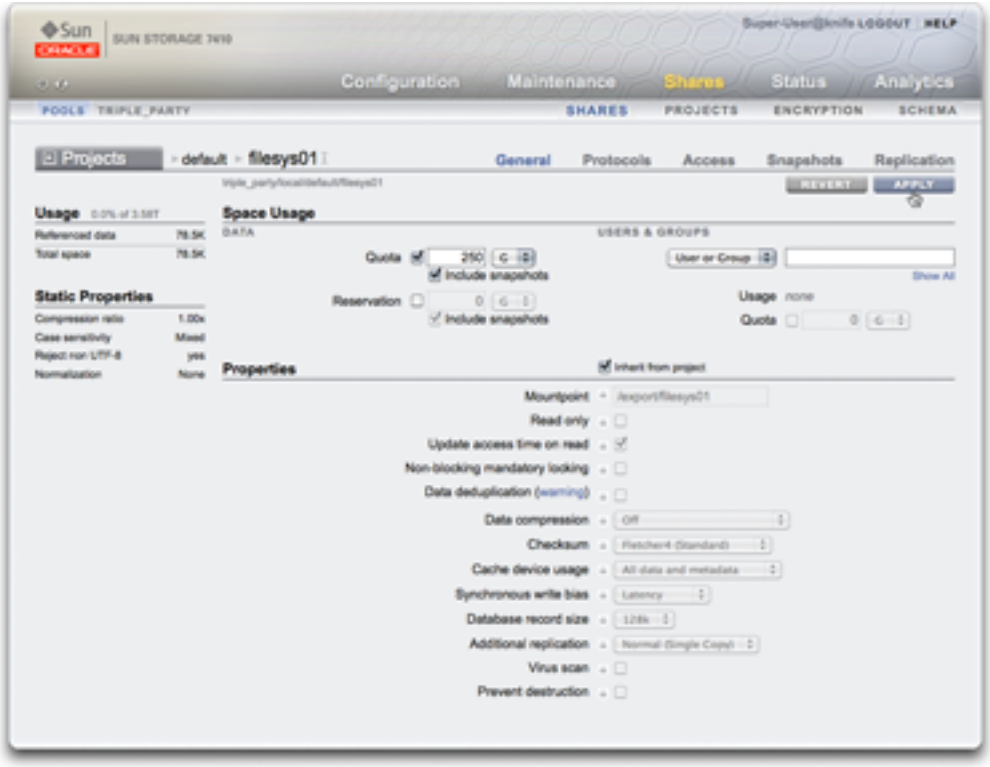
En esta sección se describen los recursos compartidos, los proyectos y los esquemas del dispositivo ZFSSA.

Para tareas administrativas comunes, incluidas la gestión del espacio y la configuración general, los recursos compartidos se pueden agrupar en proyectos del dispositivo ZFSSA. 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.

Comprensión de recursos compartidos

Agrupaciones de almacenamiento

FIGURA 12-1 Los recursos compartidos similares se pueden agrupar en un proyecto.



El dispositivo ZFSSA está basado en el sistema de archivos ZFS. ZFS agrupa los dispositivos de almacenamiento subyacentes en agrupaciones y sistemas de archivos, y los LUN se asignan desde este almacenamiento, según sea necesario. Antes de crear sistemas de archivos o LUN, debe realizar la Capítulo 5, Configuración del almacenamiento en el dispositivo ZFSSA. 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 “Gestión de espacio de recursos compartidos” [304].

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 Capítulo 5, Configuración del almacenamiento. 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' (agrupación). Si hay solo una agrupación configurada, se ocultarán esos controles. Cuando se seleccionan varias agrupaciones, la agrupación predeterminada 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.

Uso de recursos compartidos

Los recursos compartidos son los sistemas de archivos y LUN exportados mediante protocolos de datos admitidos a los clientes del dispositivo ZFSSA. Los sistemas de archivos exportan una jerarquía basada en archivos y se puede acceder a ellos mediante “SMB” [214], “NFS” [208], “HTTP/WebDav” [234] y “FTP” [232]. Los LUN exportan volúmenes basados en bloques y se puede acceder a ellos mediante “iSCSI” [213] o canal de fibra. La tupla de *proyecto/recurso compartido* es un identificador único de un recurso compartido dentro de una agrupación. Diversos proyectos pueden contener recursos compartidos con el mismo nombre; sin embargo, un único proyecto no puede contener recursos compartidos con el mismo nombre. Un único proyecto puede contener sistemas de archivos y LUN, y ellos comparten el mismo espacio de nombres.

Propiedades de recursos compartidos

Todos los proyectos y recursos compartidos tienen diversas propiedades asociadas. Estas propiedades se incluyen en los siguientes grupos:

TABLA 12-1 Propiedades de proyectos y recursos compartidos

Tipo de propiedad	Descripción
Inherited	Es el tipo más común de propiedad y 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

Tipo de propiedad	Descripción
	para reflejar el nuevo valor. Cuando se heredan, todas las propiedades tienen el mismo valor que el objeto 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.
Read-only	Estas propiedades 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.
Space Management	Estas propiedades (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.
Create time	Estas propiedades se pueden especificar en la creación del LUN o del sistema de archivos, 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.
Project default	Estas propiedades se configuran en un proyecto, pero no afectan al proyecto en sí mismo. 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 conjunto 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.
Filesystem local	Estas propiedades sólo 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.
LUN local	Estas propiedades sólo se aplican a los LUN y no se heredan. No se pueden configurar en los proyectos.
Custom	Son propiedades definidas por el usuario. Para obtener más información, consulte “Esquemas” [374].

Instantáneas de recursos compartidos

Una instantánea es una copia de un momento dado del sistema de archivos o LUN. Las instantáneas se pueden crear manualmente o mediante la configuración de un programa automático. Inicialmente, las instantáneas no consumen espacio adicional, pero a medida que cambia el recurso compartido activo, los bloques anteriores sin referencia se mantienen como parte de la última instantánea. Con el transcurso del tiempo, la última instantánea ocupará espacio adicional, con un máximo equivalente al tamaño del sistema de archivos en el momento en que se tomó la instantánea.

Se puede acceder a las instantáneas del sistema de archivos mediante los protocolos estándar en la instantánea `.zfs/snapshot` ubicada en la raíz del sistema de archivos. Este directorio está oculto de manera predeterminada, y sólo se puede acceder a él pasando explícitamente al directorio `.zfs`. Este comportamiento se puede cambiar en la vista “Instantánea” [352], pero podría hacer que el software de copias de seguridad realice copias de seguridad de las instantáneas además de los datos activos. No se puede acceder a las instantáneas de LUN directamente, aunque éstas se pueden utilizar como destino de reversión o como origen de un clon. Las instantáneas del proyecto equivalen a la toma de instantáneas de todos los recursos compartidos del proyecto, y las instantáneas se identifican por nombre. Si se cambia el nombre a una instantánea de un recurso compartido que forma parte de una instantánea de un proyecto más grande, ésta 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, ésta se considerará parte de la instantánea del proyecto.

Los recursos compartidos admiten la capacidad de reversión a instantáneas anteriores. 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 sólo incluyen datos, no propiedades, de manera que cualquier configuración de propiedades que se haya cambiado desde la toma de la instantánea se mantendrá.

Clones de recursos compartidos

AVISO DE LICENCIAS: *Las funciones de replicación remota y clonación se pueden evaluar sin cargo, pero para poder usarlas en producción se debe adquirir una licencia independiente por separado. Después del período de evaluación, se debe adquirir la licencia correspondiente para estas funciones o se las debe desactivar. Oracle se reserva el derecho de realizar auditorías en cualquier momento para controlar la existencia de las licencias necesarias. Para obtener información detallada, consulte "Acuerdo de licencia de software (SLA) de Oracle y derecho de sistemas de hardware con opciones de software integrado".*

Un clon es una copia modificable de la instantánea del recurso compartido, que se trata como un recurso compartido independiente con fines administrativos. Al igual que las instantáneas, inicialmente, un clon no ocupará espacio adicional, pero a medida que se escriban datos en el clon, el espacio necesario para los nuevos cambios estará asociado con el clon. No se admiten clones de proyectos. Dado que el espacio se comparte entre instantáneas y clones, y la

instantánea puede tener varios clones, no se puede destruir una instantánea sin destruir también todos los clones activos.

Gestión de espacio de recursos compartidos

El comportamiento de los sistemas de archivos y los LUN respecto de la gestión del almacenamiento físico es diferente en la serie 7000 en comparación con otros sistemas. Según se describe en la página “Concepts” [300], el dispositivo ZFSSA aprovecha un modelo de almacenamiento con agrupaciones donde todos los sistemas de archivos y los LUN comparten un espacio en común. Los sistemas de archivos nunca tienen un tamaño específico asignado a ellos y sólo ocupan la cantidad de espacio que necesitan. Los LUN reservan suficiente espacio físico para escribir todo el contenido del dispositivo, a menos que cuenten con poco aprovisionamiento, en cuyo caso se comportan como sistemas de archivos y utilizan sólo 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 los datos por parte del usuario, requiere una gestión más cuidadosa. En esta sección, se describen algunas de las herramientas disponibles para el administrador para controlar y gestionar el uso del espacio.

Terminología de espacio 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 ZFSSA.

- 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 ZFSSA con un algoritmo de compresión diferente no consumirá más que esta cantidad. Esta estadística no se exporta explícitamente y, por lo general, sólo 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.

Descripción de instantáneas

Las instantáneas presentan un dilema interesante para la gestión del espacio. Representan el conjunto 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 sólo 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.

Otros sistemas intentarán ocultar el costo de las instantáneas simulando que son gratuitas o "reservando" espacio dedicado a mantener datos de instantáneas. Dichos sistemas tratan de disimular el hecho básico intrínseco de las instantáneas. Si toma una instantánea de un sistema de archivos de cualquier tamaño, y reescribe el 100% de los datos dentro del sistema de archivos, por definición debe mantener las referencias en el doble de los datos que se encontraban originalmente en el sistema de archivos. Las instantáneas no son gratuitas y la única manera en que los demás sistemas pueden presentar esta abstracción es destruyendo silenciosamente las instantáneas cuando se ocupa todo el espacio. En general, esto es lo peor que se puede hacer, ya que un proceso que reescribe datos sin control puede destruir todas las instantáneas anteriores, lo cual impediría cualquier tipo de restauración del proceso.

En Sun Storage 7000, el costo de las instantáneas está siempre explícito, y se proporcionan herramientas para gestionar este espacio de una manera que coincida con el modelo administrativo de un entorno determinado. 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 ésta 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 subconjunto 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 toma 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 sólo 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 conjunto 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 ZFSSA).

Configuración del sistema de archivos y los 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 la “sección de instantáneas” [304], 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 está configurada la propiedad 'Incluir instantáneas', la cuota sólo 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 está configurada la propiedad 'Incluir instantáneas', la reserva sólo se aplica a los datos inmediatos del sistema de archivos. Como se describe en la “sección de instantáneas” [304], es posible que el comportamiento durante la toma de instantáneas no siempre sea 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 dinámico). 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 usuarios y grupos

Visualización del uso actual

Independientemente de si las cuotas de usuario y de grupo están en uso, se puede consultar el uso actual por usuario o por grupo para sistemas de archivos y proyectos. Es posible que las agrupaciones de almacenamiento creadas en versiones anteriores de software necesiten aplicar "Actualizaciones" de "Manual de servicio del cliente de Oracle ZFS Storage Appliance " antes de utilizar esta función. Después de aplicar la actualización diferida, puede tomar algún tiempo actualizar los sistemas de archivos a una versión compatible con las cuotas y el uso por usuario y por grupo.

▼ Visualización del uso actual en la BUI

1. **Para visualizar el uso actual en la BUI, vaya a Shares (Recursos compartidos) > Shares (Recursos compartidos) > General.**
2. **En la sección Space Usage - Users and Groups (Uso de espacio: usuarios y grupos), haga clic en la lista desplegable User or Group (Usuario o grupo) para seleccionar un usuario o un grupo y consultar el uso actual correspondiente a ese usuario o ese grupo en un recurso compartido o para todo el proyecto.**

3. **Escriba el nombre del usuario o el grupo sobre el que desea consultar. La consulta se va realizando a medida que escribe.**

   Cuando finaliza la consulta, se muestra el uso actual. Además, el enlace "Show All" (Mostrar todo) abre un cuadro de diálogo con una lista del uso actual de todos los usuarios o grupos. Este cuadro de diálogo sólo puede realizar consultas para un tipo en particular (usuarios o grupos) y no admite la consulta de ambos al mismo tiempo. La lista muestra el nombre canónico de UNIX y Windows (si las asignaciones están activadas), además del uso y la cuota (de los sistemas de archivos).

▼ Visualización del uso actual en la CLI

1. **En la CLI, use los comandos `users` y `groups` en el contexto de un recurso compartido o un proyecto en particular.**

2. **Use el comando `show` para mostrar el uso actual en formato tabular.**

3. **Para recuperar el uso correspondiente a un usuario o un grupo en particular, seleccione el usuario o el grupo deseado y use el comando `get`.**

```
clownfish:> shares select default
clownfish:shares default> users
clownfish:shares default users> list
USER       NAME                            USAGE
user-000   root                             325K
user-001   ahl                             9.94K
user-002   eschrock                        20.0G
clownfish:shares default users> select name=eschrock
clownfish:shares default user-002> get
                         name = eschrock
                     unixname = eschrock
                       unixid = 132651
                      winname = (unset)
                        winid = (unset)
                        usage = 20.0G
```

Configuración de cuotas de usuarios o grupos

Se pueden configurar cuotas en un usuario o grupo en el nivel del sistema de archivos. 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 sólo se pueden aplicar a los sistemas de archivos.
- 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.

▼ Configuración de cuotas de usuarios o grupos con la BUI

1. **En la BUI, vaya a Shares (Recursos compartidos) > Shares (Recursos compartidos) > General.**

2. **En la sección Space Usage - Users and Groups (Uso de espacio: usuarios y grupos), haga clic en la lista desplegable User or Group (Usuario o grupo) para seleccionar un usuario o un grupo y consultar el uso actual correspondiente a ese usuario o ese grupo en un recurso compartido o para todo el proyecto.**

3. **En el explorador, las cuotas de usuario se gestionan desde la ficha "general" [327] en Space Usage (Uso de espacio) -> Users & Groups (Usuarios y grupos). De la misma manera que la visualización del uso, el uso actual se muestra a medida que se escribe un usuario o grupo. Cuando haya finalizado de introducir el nombre del usuario o grupo y se muestre su uso actual, podrá configurar la cuota marcando la casilla ubicada junto a "cuota" e introduciendo el valor en el campo de tamaño. Para desactivar una cuota, desactive el cuadro. Cuando se hayan aplicado los cambios, haga clic en el botón 'Aplicar' para realizar los cambios.**

4. **Si bien todas las propiedades de una página se confirman juntas, las cuotas de usuario y grupo se validan aparte de las demás propiedades. Si se introduce un usuario y grupo no válido y otra propiedad no válida, sólo se mostrará uno de los errores de validación. Una vez corregido el error, al intentar aplicar los cambios nuevamente se mostrará el otro error.**

▼ Configuración de cuotas de usuarios o grupos con la CLI

- **En la CLI, las cuotas de usuario se gestionan mediante el comando 'users' o 'groups' del contexto de recursos compartidos. Las cuotas se pueden configurar mediante la selección de un usuario o grupo en particular y mediante el uso del comando 'set quota'. Cualquier usuario que no consuma espacio en el sistema de archivos y no tenga cuotas configuradas no aparecerá en la lista de usuarios activos. Para definir una cuota para dicho usuario o grupo, utilice el comando 'quota', después del cual se podrán configurar el nombre y la cuota. Para borrar una cuota, configúrela con valor '0'.**

```
clownfish:> shares select default select eschrock
clownfish:shares default/eschrock> users
clownfish:shares default/eschrock users> list
USER       NAME                            USAGE  QUOTA
user-000   root                             321K      -
user-001   ahl                             9.94K      -
user-002   eschrock                        20.0G      -
clownfish:shares default/eschrock users> select name=eschrock
clownfish:shares default/eschrock user-002> get
                         name = eschrock
                     unixname = eschrock
                       unixid = 132651
                      winname = (unset)
                        winid = (unset)
                        usage = 20.0G
                        quota = (unset)
clownfish:shares default/eschrock user-002> set quota=100G
                        quota = 100G (uncommitted)
clownfish:shares default/eschrock user-002> commit
clownfish:shares default/eschrock user-002> done
clownfish:shares default/eschrock users> quota
clownfish:shares default/eschrock users quota (uncomitted)> set name=bmc
                         name = bmc (uncommitted)
clownfish:shares default/eschrock users quota (uncomitted)> set quota=200G
                        quota = 200G (uncommitted)
clownfish:shares default/eschrock users quota (uncomitted)> commit
clownfish:shares default/eschrock users> list
USER       NAME                            USAGE  QUOTA
user-000   root                             321K      -
user-001   ahl                             9.94K      -
user-002   eschrock                        20.0G   100G
user-003   bmc                                 -   200G
```

Gestión de Identidad

Las cuotas de usuario y grupo aprovechan el servicio de “asignación de identidad” [266] en el dispositivo ZFSSA. 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.

Espacio de nombres del sistema de archivos

A cada sistema de archivos del dispositivo ZFSSA, 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 éstos sólo 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 sólo 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.

Acceso del protocolo de espacio de nombres a los puntos de montaje

Independientemente de la configuración del protocolo, cada sistema de archivos debe tener un punto de montaje. Sin embargo, la manera de usar estos puntos de montaje depende del protocolo.

Espacio de nombres en NFSv2 y NFSv3

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.

Espacio de nombres en NFSv4

NFSv4 tiene diversas 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 (incluido Linux) admiten montajes automáticos del lado del cliente, en ocasiones denominados "montajes reflejados". 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.

Shares (Recursos compartidos) > Shares (Recursos compartidos)

Working with Shares (Trabajo con recursos compartidos) > Shares (Recursos compartidos) en la BUI

Para acceder a la interfaz de usuario de recursos compartidos , se utiliza Shares (Recursos compartidos) > Shares (Recursos compartidos). La vista predeterminada muestra recursos compartidos en todos los proyectos del sistema.

Lista de recursos compartidos

La vista predeterminada es una lista de todos los recursos compartidos del sistema. Esta lista permite cambiar el nombre de los recursos compartidos, moverlos entre proyectos y editar recursos compartidos individuales. Los recursos compartidos se dividen en dos listas "Filesystems" (Sistemas de archivos) y "LUNs" (LUN) que se pueden seleccionar cambiando de ficha en esta vista. Se muestran los siguientes campos para cada recurso compartido:

TABLA 12-2 Lista de recursos compartidos de la BUI

Campo	Descripción
Name	Nombre del recurso compartido. Al observar todos los proyectos, se incluirá también el nombre del proyecto. El nombre del recurso compartido es un campo de texto editable. Al hacer clic en el nombre, podrá introducir un nombre nuevo. Para confirmar el cambio, debe presionar la tecla de retorno o alejar el enfoque del nombre. Se le solicitará que confirme la acción, ya que para cambiar el nombre de los recursos compartidos, se deben desconectar los clientes activos.
Size	En el caso de los sistemas de archivos, se trata del tamaño total del sistema de archivos. En el caso de los LUN, se trata del tamaño del volumen, que puede contar con poco aprovisionamiento, o no. Consulte “Estadísticas de uso” [316] para obtener más información.
Mountpoint	Punto de montaje del sistema de archivos. Se trata de la ruta disponible mediante NFS y la ruta relativa para FTP y HTTP. Los sistemas de archivos exportados mediante SMB solo utilizan el nombre del recurso, aunque cada uno aún necesitará un punto de montaje único en algún lugar del sistema.
GUID	SCSI GUID del LUN. Para obtener más información, consulte la página de la BUI “Página Shares (Recursos compartidos) > Shares (Recursos compartidos) > Protocols (Protocolos) de la BUI” [336].

Las siguientes herramientas están disponibles para cada recurso compartido:

TABLA 12-3 Íconos de Shares (Recursos compartidos) > Shares (Recursos compartidos) de la BUI

Ícono	Descripción
	Permite mover un recurso compartido a un proyecto diferente. Si el panel del proyecto no está expandido, esta opción expandirá automáticamente el panel hasta que se coloque el recurso compartido en un proyecto.
	Permite editar un recurso compartido individual (al que se puede acceder haciendo doble clic sobre la fila).

Ícono	Descripción
	Permite destruir el recurso compartido. Se le solicitará que confirme la acción, ya que destruirá todos los datos del recurso compartido y esta acción no se puede deshacer.

Edición de un recurso compartido

Para editar un recurso compartido, haga clic en el ícono de lápiz o haga doble clic en la fila de la lista de recursos compartidos. De esta manera, seleccionará el recurso compartido y tendrá diferentes fichas entre las que podrá elegir para editar las propiedades del recurso compartido. Podrá encontrar el conjunto completo de funcionalidades en la sección correspondiente a cada ficha:

- “General” [327]
- “Protocols” [336]
- “Access” [344]
- “Snapshots” [352]
- Capítulo 13, Replicación

El nombre del recurso compartido se presenta en la esquina superior izquierda, a la derecha del panel del proyecto. El primer componente del nombre es el proyecto contenedor, y al hacer clic en el nombre del proyecto, navegará hasta [[Shares:Projects|project details]]. Para cambiar el nombre del recurso compartido, también puede hacer clic en el nombre y escribir el nuevo texto. Se le solicitará que confirme la acción, ya que será necesario desconectar los clientes activos del recurso compartido.

Estadísticas de uso

A la izquierda de la vista (debajo del panel del proyecto expandido), 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. Se muestran las siguientes estadísticas de uso:

- Available space (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.
- Referenced Data (Datos de referencia): cantidad de datos a los 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.

- Snapshot Data (Datos de instantánea): 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.
- Unused Reservation (Reserva sin uso): si un sistema de archivos tiene un conjunto 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 ZFSSA 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 sobre reservas, consulte la sección “propiedades generales” [327].
- Total Space (Espacio total): suma de los datos de referencia, los datos de instantáneas y la reserva sin uso.

Propiedades estáticas

El lado izquierdo de la vista de recursos compartidos también muestra las propiedades estáticas (hora de creación) al editar un recurso compartido en particular. Estas propiedades se configuran en el momento de la creación y, una vez configuradas, no se pueden modificar. Se muestran las siguientes propiedades estáticas:

- Compression Ratio (Ratio de compresión): si la compresión está activada, muestra la relación de compresión obtenida en la actualidad 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 sobre la compresión y los algoritmos disponibles, consulte la sección “propiedades generales” [327].
- Case Sensitivity (Distinción entre mayúsculas y minúsculas): controla si en las consultas del directorio se distingue entre mayúsculas y minúsculas. Admite las siguientes opciones:

Valor de la BUI	Valor de la CLI	Descripción
Mixed	mixed	La distinción entre mayúsculas y minúsculas depende del protocolo que se utiliza. 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. Éste es

Valor de la BUI	Valor de la CLI	Descripción
		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.
Insensitive	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 sólo 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.
Sensitive	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.

- Reject non UTF-8 (Rechazar codificación que no sea UTF-8): esta configuración 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 sólo afecta a NFSv3, donde la codificación no está definida por el estándar. NFSv4 utiliza siempre UTF-8, y SMB negocia la codificación adecuada. Generalmente, esta configuración debe tener el valor "on" (Activado), de lo contrario, SMB (que debe conocer la codificación para realizar comparaciones para distinguir entre mayúsculas

y minúsculas, entre otras cosas) no podrá decodificar los nombres de archivos creados con una codificación UTF-8 no válida. Esta configuración sólo debe tener el valor "off" (Desactivado) en las implementaciones NFSv3 preexistentes, donde los clientes se han configurado para utilizar codificaciones diferentes. La activación de SMB o NFSv4 cuando esta propiedad se establece en "off" (Desactivado) puede generar resultados indefinidos, si un cliente NFSv3 crea un archivo o directorio que no tiene una codificación de UTF-8 válida. Esta propiedad se debe configurar con el valor "on" (activado), si la propiedad de normalización está configurada con un valor distinto de "none" (ninguno).

- Normalization (Normalización): esta configuración controla la normalización de unicode que se lleva a cabo (si existe alguna) 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 esta propiedad se configura con un valor distinto de "none" (ninguno), que es el valor predeterminado, la propiedad "Reject non UTF-8" (Rechazar codificación que no sea UTF-8) también se debe configurar con el valor "on" (activado). Para obtener más información sobre cómo funciona la normalización y los diferentes formularios, consulte la entrada de Wikipedia sobre normalización unicode.

Valor de la BUI	Valor de la CLI	Descripción
None	none	No se lleva a cabo ninguna normalización.
Form C	formC	*Composición canónica del formulario de normalización (NFC, Normalization Form Canonical Composition)*: los caracteres se descomponen y, luego, se recomponen mediante equivalencia canónica.
Form D	formD	*Descomposición canónica del formulario de normalización (NFC, Normalization Form Canonical Decomposition)*: los caracteres se descomponen mediante equivalencia canónica.
Form KC	formKC	*Composición de compatibilidad del formulario de normalización (NFKC, Normalization Form Compatibility Composition)*: los caracteres se descomponen por equivalencia de compatibilidad y, luego, se recomponen mediante equivalencia canónica.
Form KD	formKD	*Descomposición de compatibilidad del formulario de normalización*

Valor de la BUI	Valor de la CLI	Descripción
		(NFKC, Normalization Form Compatibility Decomposition): los caracteres se descomponen mediante equivalencia de compatibilidad.

- Volume Block Size (Tamaño del bloque de volumen): tamaño del bloque nativo para LUN. Puede tener cualquier potencia de 2 desde 512 bytes hasta 1M; el valor predeterminado es 8K.
- Origin (Origen): si se trata de un clon, se refiere al nombre de la instantánea desde la cual se clonó.
- Data Migration Source (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 la sección sobre Capítulo 14, Migración shadow.

Panel de proyecto de recursos compartidos

En la BUI, el conjunto de proyectos disponibles siempre está disponible en el panel del proyecto, ubicado en el lado izquierdo de la vista. Para expandir o reducir el panel del proyecto, haga clic en el triángulo ubicado junto a la barra de título "Projects" (Proyectos).

TABLA 12-4 Íconos del panel del proyecto

Ícono	Descripción
	Permite expandir el panel del proyecto.
	Permite reducir el panel del proyecto.

Al seleccionar un proyecto desde el panel, se podrá navegar hasta la vista de “Proyectos” [362] del proyecto seleccionado. Este panel del proyecto también se expandirá automáticamente al hacer clic en la herramienta de movimiento sobre una fila de la lista de recursos compartidos. Luego puede arrastrar y soltar el recurso compartido para moverlo de un proyecto a otro. El panel del proyecto también proporciona un acceso directo para crear nuevos proyectos y volver a la lista de recursos compartidos de todos los proyectos. Hacer clic en el texto "All" (Todos) equivale a seleccionar el artículo "Shares" (Recursos compartidos) en la barra de navegación.

El panel del proyecto resulta cómodo para los sistemas con un número de proyectos relativamente bajo. No fue diseñado para actuar como interfaz principal para gestionar una gran cantidad de proyectos. Para esta tarea, consulte la vista de “Proyectos” [362].

▼ Creación de un recurso compartido

1. **Para ver los recursos compartidos de un proyecto o para todos los proyectos, vaya a Shares (Recursos compartidos) > Shares (Recursos compartidos).**

2. **Seleccione Filesystems (Sistemas de archivos) o LUNs (LUN).**

3. **Haga clic en el ícono más junto a Filesystems (Sistemas de archivos) o LUNs (LUN).**

   Aparece el cuadro de diálogo Create Filesystem (Crear sistema de archivos) o Create LUN (Crear LUN).

4. **En el cuadro de diálogo Create Filesystem (Crear sistema de archivos) o Create LUN (Crear LUN), seleccione o escriba las propiedades que desea usar.**

   Las propiedades correspondientes a cada tipo de recurso compartido se definen en las siguientes ubicaciones:

   Para los sistemas de archivos:

   - "User" [344]
   - "Group" [344]
   - "Permissions" [344]
   - "Mountpoint" [327]
   - Capítulo 12, Recursos compartidos, proyectos y esquemas (solo hora de creación)
   - Capítulo 12, Recursos compartidos, proyectos y esquemas (solo hora de creación)
   - Capítulo 12, Recursos compartidos, proyectos y esquemas (solo hora de creación)

   Para los LUN:

   - "Volume size" [327]
   - "Thin provisioned" [327]
   - Capítulo 12, Recursos compartidos, proyectos y esquemas (solo hora de creación)

Working with Shares (Trabajo con recursos compartidos) > Shares (Recursos compartidos) en la CLI

La CLI de recursos compartidos se encuentra en `shares`.

Navegación

Antes de seleccionar un recurso compartido, debe seleccionar un proyecto (incluido el proyecto predeterminado):

```
clownfish:> shares
clownfish:shares> select default
clownfish:shares default> select foo
clownfish:shares default/foo> get
Properties:
                    aclinherit = restricted (inherited)
                       aclmode = discard (inherited)
                         atime = true (inherited)
               casesensitivity = mixed
                      checksum = fletcher4 (inherited)
                   compression = off (inherited)
                  compressratio = 100
                         copies = 1 (inherited)
                       creation = Mon Oct 13 2009 05:21:33 GMT+0000 (UTC)
                     mountpoint = /export/foo (inherited)
                  normalization = none
                          quota = 0
                      quota_snap = true
                        readonly = false (inherited)
                      recordsize = 128K (inherited)
                     reservation = 0
                reservation_snap = true
                  secondarycache = all (inherited)
                          nbmand = false (inherited)
                        sharesmb = off (inherited)
                        sharenfs = on (inherited)
                         snapdir = hidden (inherited)
                       snaplabel = project1:share1
                        utf8only = true
                           vscan = false (inherited)
                        sharedav = off (inherited)
                        shareftp = off (inherited)
                     space_data = 43.9K
               space_unused_res = 0
                space_snapshots = 0
                space_available = 12.0T
                    space_total = 43.9K
                     root_group = other
               root_permissions = 700
                      root_user = nobody
```

Operaciones de recursos compartidos

Para crear un recurso compartido, debe seleccionar el proyecto y ejecutar el comando `filesystem` o `lun`. Las propiedades se pueden modificar según sea necesario antes de confirmar los cambios:

```
clownfish:shares default> filesystem foo
clownfish:shares default/foo (uncommitted)> get
                    aclinherit = restricted (inherited)
                       aclmode = discard (inherited)
                         atime = true (inherited)
                      checksum = fletcher4 (inherited)
                   compression = off (inherited)
                        copies = 1 (inherited)
                    mountpoint = /export/foo (inherited)
                         quota = 0 (inherited)
                      readonly = false (inherited)
                    recordsize = 128K (inherited)
                   reservation = 0 (inherited)
                secondarycache = all (inherited)
                          nbmand = false (inherited)
                       sharesmb = off (inherited)
                       sharenfs = on (inherited)
                        snapdir = hidden (inherited)
                     snaplabel = project1:share1
                          vscan = false (inherited)
                       sharedav = off (inherited)
                       shareftp = off (inherited)
                    root_group = other (default)
              root_permissions = 700 (default)
                     root_user = nobody (default)
               casesensitivity = (default)
                 normalization = (default)
                       utf8only = (default)
                    quota_snap = (default)
              reservation_snap = (default)
                    custom:int = (default)
                 custom:string = (default)
                  custom:email = (default)
clownfish:shares default/foo (uncommitted)> set sharenfs=off
                       sharenfs = off (uncommitted)
clownfish:shares default/foo (uncommitted)> commit
clownfish:shares default>
```

Se puede destruir un recurso compartido mediante el comando `destroy` desde el contexto de recursos compartidos:

```
clownfish:shares default/foo> destroy
This will destroy all data in "foo"! Are you sure? (Y/N)
clownfish:shares default>
```

Se puede cambiar el nombre de un recurso compartido desde el contexto del proyecto mediante el comando `rename`:

```
clownfish:shares default> rename foo bar
clownfish:shares default>
```

Se puede mover un recurso compartido entre proyectos desde el contexto del proyecto mediante el comando `move`:

```
clownfish:shares default> move foo home
clownfish:shares default>
```

Las cuotas y el uso de usuario y de grupo se pueden gestionar mediante los comandos `users` o `groups` después de seleccionar el recurso compartido o proyecto en particular. Para obtener más información sobre cómo gestionar cuotas de usuarios y grupos, consulte la sección "Gestión de espacio" [304].

Propiedades de la CLI para Shares (Recursos compartidos) > Shares (Recursos compartidos)

Las siguientes propiedades están disponibles en la CLI, con su equivalente en la BUI. Las propiedades se pueden configurar mediante los comandos CLI estándar `get` y `set`. Además, las propiedades se pueden heredar del proyecto principal mediante el comando `unset`.

TABLA 12-5 Propiedades de la CLI para Shares (Recursos compartidos) > Shares (Recursos compartidos)

Nombre de la CLI	"Tipo" [300]	Nombre de la BUI	Ubicación de la BUI
aclinherit	inherited	"ACL inheritance behavior" [344]	Acceso
aclmode	inherited	"ACL behavior on mode change" [344]	Acceso
atime	inherited	"Update access time on read" [327]	General
casesensitivity	create time	Capítulo 12, Recursos compartidos, proyectos y esquemas	Estática
checksum	inherited	Capítulo 12, Recursos compartidos, proyectos y esquemas	General
compression	inherited	"Data compression" [327]	General
compresratio	read-only	Capítulo 12, Recursos compartidos, proyectos y esquemas	Estática
copies	inherited	"Additional replication" [327]	General
creation	read-only	-	-
dedup	inherited	"Data deduplication" [327]	General

Nombre de la CLI	"Tipo" [300]	Nombre de la BUI	Ubicación de la BUI
exported	inherited, solo paquetes de replicación	Capítulo 13, Replicación	General
fixednumber	LUN local	"Initiator group" [336]	Protocolos
initiatorgroup	LUN local	"Initiator group" [336]	Protocolos
logbias	inherited	"Synchronous write bias" [327]	General
lunumber	LUN local	"LU number" [336]	Protocolos
lunguid	read-only, LUN local	"GUID" [336]	Protocolos
mountpoint	inherited	"Mountpoint" [327]	General
nbmand	inherited	"Non-blocking mandatory locking" [327]	General
nodestroy	inherited	"Prevent destruction" [327]	General
normalization	create time	Capítulo 12, Recursos compartidos, proyectos y esquemas	Estática
origin	read-only	Capítulo 12, Recursos compartidos, proyectos y esquemas	Estática
quota	space management	"Quota" [304]	General
quota_snap	space management	"Quota / Include snapshots" [304]	General
readonly	inherited	"Read-only" [327]	General
recordsize	inherited	"Database record size" [327]	General
reservation	space management	"Reservation" [304]	General
reservation_snap	space management	"Reservation / Include snapshots" [304]	General
root_group	filesystem local	"Group" [344]	Acceso
root_permissions	filesystem local	"Permissions" [344]	Acceso
root_user	filesystem local	"User" [344]	Acceso
rstchown	inherited	"Restrict ownership change" [327]	General
secondary cache	inherited	"Cache device usage" [327]	General

Nombre de la CLI	"Tipo" [300]	Nombre de la BUI	Ubicación de la BUI
shadow	create time	Capítulo 14, Migración shadow	Estática
sharedav	inherited	"Protocols / HTTP / Share mdoe" [336]	Protocolos
shareftp	inherited	"Protocols / FTP / Share mode" [336]	Protocolos
sharenfs	inherited	"Protocols / NFS / Share mode" [336]	Protocolos
sharesmb	inherited	"Protocols / SMB / Resource name" [336]	Protocolos
snapdir	inherited	".zfs/snapshot visibility" [352]	Instantáneas
snaplabel	inherited	"Scheduled snapshot label" [352]	Instantáneas
space_available	read-only	Capítulo 12, Recursos compartidos, proyectos y esquemas	Uso
space_data	read-only	Capítulo 12, Recursos compartidos, proyectos y esquemas	Uso
space_snapshots	read-only	Capítulo 12, Recursos compartidos, proyectos y esquemas	Uso
space_total	read-only	Capítulo 12, Recursos compartidos, proyectos y esquemas	Uso
space_unused_res	read-only	Capítulo 12, Recursos compartidos, proyectos y esquemas	Uso
sparse	LUN local	"Thin provisioned" [327]	General
targetgroup	LUN local	"Target group" [336]	Protocolos
utf8only	create time	"Reject non UTF-8"	Estática
volblocksize	create time	Capítulo 12, Recursos compartidos, proyectos y esquemas	Estática
vscan	inherited	"Virus scan" [327]	General

Página Shares (Recursos compartidos) > Shares (Recursos compartidos) > General de la BUI

Esta sección de la BUI controla los valores de configuración generales del recurso compartido que son independientes de cualquier protocolo particular y no se relacionan con las instantáneas ni el control de acceso. Si bien la CLI agrupa todas las propiedades en una única lista, en esta sección, se describe el comportamiento de las propiedades en ambos contextos.

Son propiedades estándar que se pueden heredar del proyecto o se pueden configurar de manera explícita en el recurso compartido. La BUI solo permite heredar todas las propiedades a la vez, mientras que la CLI permite heredar propiedades individuales.

Para obtener más información sobre cómo se asignan estas propiedades a la CLI, consulte la sección “Working with Shares (Trabajo con recursos compartidos) > Shares (Recursos compartidos) en la CLI” [321].

Uso del espacio

El espacio dentro de la agrupación de almacenamiento se comparte entre todos los recursos compartidos. Los sistemas de archivos pueden crecer o reducirse dinámicamente según sea necesario, aunque también es posible aplicar restricciones de espacio a cada recurso compartido. Las cuotas y las reservas se pueden aplicar para cada sistema de archivos. Las cuotas también se pueden aplicar por usuario y por grupo. Para obtener más información sobre la manera de gestionar el uso del espacio para sistemas de archivos, incluidas las cuotas y reservas, consulte la sección “Space Management” [304].

Tamaño del volumen

Tamaño lógico del LUN exportado mediante iSCSI. Esta propiedad sólo es válida para los LUN. Esta propiedad controla el tamaño del LUN. De forma predeterminada, los LUN reservan suficiente espacio para llenar el volumen por completo. Para obtener más información, consulte la propiedad “Thin provisioned” [327]. 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

Controla si el espacio está reservado para el volumen. Esta propiedad sólo es válida para los LUN. 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 sólo 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 “Reserva de proyectos” [369].

Punto de montaje

Ubicación donde está montado el sistema de archivos. Esta propiedad sólo 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 conjunto de datos actual se anexa a la configuración de punto de montaje del proyecto, y se une mediante una barra diagonal ('/'). Por ejemplo, si el proyecto de "home" (inicio) tiene 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 sólo de SMB deben tener un único punto de montaje válido en el dispositivo ZFSSA.

Los puntos de montaje se pueden anidar debajo de otros recursos compartidos, aunque con algunas limitaciones. Para obtener más información, consulte la sección sobre “espacio de nombres del sistema de archivos” [312].

Sólo lectura

Controla si el contenido del sistema de archivos es de sólo lectura. Esta propiedad sólo es válida para los sistemas de archivos. Independientemente de la configuración de protocolo, el

contenido de un sistema de archivos de sólo 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 sólo lectura, las propiedades de "Control de acceso" [344] 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

Controla si la hora de acceso a los archivos está actualizada en el momento de la lectura. Esta propiedad sólo 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 éste fue leído. Para ello, se deben enviar datos escritos al sistema de archivos subyacente, incluso para una carga de trabajo que mayormente es de sólo lectura. En el caso de los conjuntos 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

Controla si la semántica de bloqueo de SMB tiene prioridad sobre la semántica de POSIX. Esta propiedad sólo 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.

Anulación de duplicación de datos

Controla si se eliminan las copias de datos duplicadas. La anulación de duplicación es un proceso síncrono, de toda la agrupación, basado en bloques y que se puede activar por proyecto o por recurso compartido. Para activar este proceso, seleccione la casilla de verificación Anulación de duplicación de datos en la pantalla de propiedades generales para proyectos o recursos compartidos. La relación de anulación de duplicación aparecerá en el área de uso del panel de control de estado.

Los datos escritos con la anulación de duplicación activada se introducen en la tabla de anulación de duplicación indexada por el total de control de datos. La anulación de duplicación

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 anulación de duplicación solo se produce entre bloques del mismo tamaño y con datos escritos con el mismo tamaño de registro. Como siempre, 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.

Si los datos no contienen duplicados, al activar la opción Anulación de duplicación de datos se agregará más sobrecarga (un total de control más intenso en la CPU y entradas de tabla de anulación de duplicación en el disco) sin proporcionar beneficios. Si los datos contienen duplicados, la activación de la opción Anulación de duplicación de datos ahorrará espacio ya que almacenará solo una copia de un bloque determinado independientemente de la cantidad de veces que ocurra. La anulación de duplicación necesariamente afectará el rendimiento ya que el total de control es más costoso para computar y se debe acceder a los metadatos de la tabla de anulación de duplicación y mantenerlos.

Recuerde que la anulación de duplicación no afecta el tamaño calculado de un recurso compartido, pero sí afecta la cantidad de espacio utilizado para la agrupación. Por ejemplo, si dos recursos compartidos contienen el mismo archivo de 1 GB, cada uno parecerá tener 1 GB de tamaño, pero el total de la agrupación será de solo 1 GB y la relación de anulación de duplicación se informará como el doble.

Advertencia de rendimiento: por naturaleza, para realizar una anulación de duplicación, es necesario modificar la tabla de anulación de duplicación cuando se escribe o se libera un bloque. Si la tabla de anulación de duplicación no encaja en la DRAM, los datos escritos y las liberaciones podrían generar una considerable actividad de lectura aleatoria donde anteriormente no existía ninguna. Como resultado, el impacto en el rendimiento al activar la anulación de duplicación puede ser alto. Además, en algunos casos (en particular, cuando se suprimen instantáneas o recursos compartidos) la degradación del rendimiento derivada de la activación de la anulación de duplicación se puede sentir en toda la agrupación. En general, no se recomienda activar la anulación de duplicación, a menos que se sepa que un recurso compartido tiene una tasa muy elevada de datos duplicados, y que dichos datos duplicados y la tabla a la que se hace referencia pueden residir cómodamente en la DRAM. Para determinar si el rendimiento se ha visto afectado de manera negativa por la anulación de duplicación, active Capítulo 8, Configuración de preferencias de dispositivos ZFSSA y, luego, utilice “Análisis” de “Guía de análisis de Oracle ZFS Storage Appliance ” para medir las operaciones de DMU de ZFS desglosadas por tipo de objeto de DMU y verificar si existe una tasa más elevada de operaciones de DDT continuas (operaciones de la tabla de duplicación de datos) en comparación con las operaciones de ZFS. Si ocurre esto, significa que hay más E/S para abastecer la tabla de anulación de duplicación que la E/S de archivos.

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 manera 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
Off	off	No se realiza ninguna compresión.
LZJB (Fastest)	lzjb	Codificación simple a lo largo de la ejecución que sólo funciona con entradas lo suficientemente simples, pero no consume mucha CPU.
GZIP-2 (Fast)	gzip-2	Versión liviana del algoritmo de compresión gzip.
GZIP (Default)	gzip	Algoritmo de compresión gzip estándar.
GZIP-9 (Best Compression)	gzip-9	La mayor compresión posible mediante gzip. Consume una cantidad significativa de la CPU y, a menudo, puede proporcionar sólo utilidad marginal.

Total de control

Controla el total de control utilizado para los bloques de datos. En el dispositivo ZFSSA, 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 predeterminado (fletcher4) es suficiente para el funcionamiento normal, pero los usuarios paranoicos 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 sólo 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.

Uso del dispositivo de caché

Controla si los dispositivos de caché se utilizan para el recurso compartido. De manera predeterminada, todos los conjuntos de datos utilizan dispositivos de la caché en el sistema. Los dispositivos de la caché están configurados como parte de la agrupación de almacenamiento y proporcionan una capa adicional de almacenamiento en caché para obtener acceso organizado en niveles más veloz. Para obtener más información sobre dispositivos de la caché, consulte la sección Capítulo 5, Configuración del almacenamiento. 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" (todos) aunque no haya dispositivos de la 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.
Sólo metadatos	metadata	Sólo 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 caché	none	Ningún dato de este recurso compartido está almacenado en caché en el dispositivo de caché. Los datos sólo se almacenan en la caché principal o se almacenan en dispositivos de datos.

Desviación de escritura síncrona

Esta configuración 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 'rendimiento' en la base de datos principal mientras se deja el sistema de archivos de log en 'latencia'. Esta configuración cambiará el comportamiento aun cuando no haya dispositivos de log presentes, aunque los efectos pueden ser menos dramáticos.

Oracle Intelligent Storage Protocol puede omitir la configuración 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 de Oracle Database. El valor de la desviación de escritura enviado por el cliente NFSv4 de Oracle Database se utiliza únicamente para esa solicitud de cliente. Para obtener más información, consulte “ Oracle Intelligent Storage Protocol ” [497].

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 global	throughput	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.

Tamaño de registro de la base de datos

Especifica un tamaño de bloque sugerido para los archivos del sistema de archivos. Esta propiedad es válida sólo 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 predeterminado 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 sólo los archivos que se creen después del cambio; los archivos existentes y los datos recibidos no sufren cambios.

NOTA: Si se usan tamaños de bloques mayores que 128K 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.

Oracle Intelligent Storage Protocol puede omitir la configuración 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 de Oracle Database. El tamaño del bloque proporcionado por el cliente NFSv4 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 “ Oracle Intelligent Storage Protocol ” [497].

Replicación adicional

Controla la cantidad 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 paranoicos.

Valor de la BUI	Valor de la CLI	Descripción
Normal (una copia)	1	Comportamiento predeterminado. Almacena una única copia de bloques de datos.
Dos copias	2	Almacena dos copias de cada bloque de datos.
Tres copias	3	Almacena tres copias de cada bloque de datos.

Análisis de virus

Controla si se analiza la presencia de virus en este sistema de archivos. Esta propiedad sólo 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 la sección “Análisis de virus” [251].

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 ZFSSA 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.

Restricción de 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, la propiedad del archivo puede ser cambiada por el propietario del archivo o directorio, 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 personalizadas

Se pueden agregar propiedades personalizadas según sea necesario para anexar etiquetas definidas por el usuario a proyectos y recursos compartidos. Para obtener más información, consulte “Esquemas” [374].

Página Shares (Recursos compartidos) > Shares (Recursos compartidos) > Protocols (Protocolos) de la BUI

Protocolos de recursos compartidos

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. Las propiedades “NFS” [208], “SMB” [214], “HTTP” [234] y “FTP” [232] sólo se aplican a los sistemas de archivos, mientras que las propiedades “iSCSI” [213] se aplican sólo a los LUN.

En la BUI, cada protocolo muestra la ruta mediante la cual los clientes que usan ese protocolo harán referencia al recurso compartido. Por ejemplo, el sistema de archivos "fs0" en el servidor "twofish" estaría disponible en las siguientes ubicaciones:

TABLA 12-6 Protocolos de recursos compartidos

Protocolo	Ubicación
NFS	twofish:/export/fs0
SMB	\\twofish\fs0
HTTP	//twofish/shares/export/fs0/
FTP	ftp://twofish/export/fs0/
SFTP	/export/fs0/

En el caso de iSCSI, los iniciadores pueden detectar el destino mediante uno de los mecanismos descritos en Capítulo 6, Configuración de red de área de almacenamiento.

Protocolos de recursos compartidos: NFS

TABLA 12-7 Protocolos de recursos compartidos: propiedades de NFS

Propiedad de la BUI	Propiedad de la CLI	Descripción
Modo de recurso compartido	off/ro/rw	Determina si el recurso compartido está disponible sólo para lectura, para lectura y escritura, o para ninguna de estas opciones. En la CLI, "on" es un alias para "rw".
Desactivar creación del archivo setuid/setgid	nosuid	Si esta opción está seleccionada, los clientes no podrán crear archivos

Propiedad de la BUI	Propiedad de la CLI	Descripción
		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	Si esta opción está seleccionada, los clientes no podrán montar subdirectorios directamente. Se les obligará a montar la raíz del recurso compartido. Nota: Esto sólo se aplica a los protocolos NFSv2 y NFSv3, no a NFSv4.
Asignación de usuarios anónimos	anon	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 del archivo se evaluarán normalmente.
Codificación de caracteres	Consulte la información que se muestra abajo	Configura el juego de caracteres predeterminado para todos los clientes. Para obtener más información, consulte la sección sobre codificaciones de juegos de caracteres.
Modo de seguridad	Consulte la información que se muestra abajo	Configura el modo de seguridad de todos los clientes.

Es posible definir excepciones para los modos de uso compartido general para los clientes o las recopilaciones de clientes. Cuando un cliente intenta obtener acceso, éste se otorga según la primera excepción de la lista que coincida con el cliente, pero si no existe dicha excepción, se otorgará según los modos de recursos compartidos globales que se hayan definido más arriba. Estas recopilaciones de clientes se pueden definir mediante uno de estos tres tipos:

TABLA 12-8 Tipos de recopilación de clientes

Tipo	Prefijo de la CLI	Descripción	Ejemplo
Host(FQDN) o grupo de red	ninguno	Un único cliente cuya dirección IP se convierte en el nombre completo especificado o un grupo de red que contiene los nombres completos en los cuales se convierte la dirección IP del cliente.	caji.sf.example.com

Tipo	Prefijo de la CLI	Descripción	Ejemplo
Dominio DNS	.	Todos los clientes con direcciones IP que se convierten en un nombre completo que termina con este sufijo.	sf.example.com
Red	@	Todos los clientes con direcciones IP que se encuentran dentro de la subred IP especificada, expresada en la notación CIDR.	192.168.20.0/22

Para cada cliente o recopilación de clientes que se especifique, deberá expresar dos parámetros: si se le permitirá al cliente tener acceso de sólo lectura o de lectura y escritura al recurso compartido, y si el usuario root del lado del cliente será tratado como usuario root (si se selecciona) o como usuario desconocido.

Si se utilizan grupos de red, éstos se convertirán a partir de “NIS” [254] (si está activado) y, luego, a partir de “LDAP” [256] (si está activado). Si se utiliza LDAP, los grupos de red se deben encontrar en la ubicación predeterminada, ou=Netgroup, (Base DN), y se debe utilizar un esquema estándar. El componente de nombre de usuario de una entrada de grupo de red generalmente no afecta el NFS; sólo el nombre de 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 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” [274]. La gestión de grupos de red puede ser compleja; considere utilizar las reglas de subred de IP o las reglas de dominio DNS en su lugar cuando sea posible.

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.

Protocolos de recursos compartidos: CLI

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 con coma de las tablas anteriores. Debe comenzar con "ro", "rw", u "off", como análogo a los modos de recursos compartidos globales descriptos para la BUI. Por ejemplo:

```
set sharenfs=ro
```

configura el modo de recurso compartido para todos los clientes en sólo lectura. Los usuarios root de todos los clientes tendrán acceso a los archivos del recurso compartido como si fueran el usuario genérico "nobody" (nadie).

También se podrá incluir cualquiera de las opciones "nosuid" y "anon", o ambas. Recuerde que en la CLI, los valores de las propiedades que contengan el carácter "=" deben estar entre comillas. Por lo tanto, para definir la asignación de todos los usuarios desconocidos con el número de identificación de usuario (UID) 153762, debería especificar:

```
set sharenfs="ro,anon=153762"
```

Se pueden especificar excepciones adicionales agregando el texto de formato "option=collection", donde "option" equivale a "ro", "rw" y "root", que 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 anterior 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"
```

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" (ingeniería) de la siguiente manera:

```
set sharenfs="ro,rw=engineering"
```

Para especificar los modos de seguridad, se agrega texto en el formato "option=mode", donde la opción es "sec" y el modo es una de las siguientes opciones: "sys", "krb5", "krb5:krb5i" o "krb5:krb5i:krb5p".

```
set sharenfs="sec=krb5"
```

Modos de seguridad

Los modos de seguridad se configuran por archivo y pueden afectar el rendimiento. En la siguiente tabla, se describe la configuración de seguridad de Kerberos.

TABLA 12-9 Configuración de seguridad de Kerberos

Configuración	Descripción
krb5	Autenticación de usuario final mediante Kerberos V5.
krb5i	krb5 más protección de integridad (los paquetes de datos están protegidos contra alteraciones).

Configuración	Descripción
krb5p	krb5i más protección de privacidad (los paquetes de datos están protegidos contra alteraciones y cifrados).

Al definir modos de seguridad, se pueden especificar combinaciones de varias configuraciones de Kerberos. La combinación de modos de seguridad permite que los clientes realicen el montaje con cualquiera de las configuraciones de Kerberos enumeradas.

TABLA 12-10 Configuración de modo de seguridad

Configuración	Menú
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 deben realizar el montaje con esta configuración.

Para obtener más información sobre NFS y Kerberos, consulte:

- http://www.ietf.org/rfc/rfc2623.txt (http://www.ietf.org/rfc/rfc2623.txt) (seguridad de NFSv2 y NFSv3)
- http://www.ietf.org/rfc/rfc3530.txt (http://www.ietf.org/rfc/rfc3530.txt) (protocolo de NFSv4)

Codificaciones de juegos de caracteres

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 debería usar UTF-8, pero no todos los clientes lo hacen y el servidor no aplica esta restricción. Si la opción de sólo 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 sólo 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-cn
- euc-jp
- euc-jpms
- euc-kr
- euc-tw
- iso8859-1
- iso8859-2
- iso8859-5
- iso8859-6
- iso8859-7
- iso8859-8
- iso8859-9
- iso8859-13
- iso8859-15
- koi8-r
- shift_jis

El comportamiento predeterminado 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:

```
set sharenfs="rw,euc-kr=*"
```

Compartirá el sistema de archivos con 'euc-kr' como la codificación predeterminada. Lo siguiente:

```
set sharenfs="rw,euc-kr=host1.domain.com,euc-jp=host2.domain.com"
```

Utilizará la codificación predeterminada para todos los clientes, excepto para 'host1' y 'host2', que 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.

Recursos compartidos: SMB

- Resource name (Nombre de recurso): nombre mediante el cual los clientes "SMB" [214] hacen referencia a este recurso compartido. El nombre del recurso "off" indica que ningún cliente "SMB" [214] puede acceder al recurso compartido, y el nombre del recurso "on" indica que el recurso compartido se exportará con el nombre del sistema de archivos.
- Enable Access-based Enumeration (Activar enumeración basada en el acceso): opción mediante la cual se realiza una enumeración basada en el acceso, cuando está activada. La enumeración basada en el acceso filtra las entradas de directorio según las credenciales del cliente. Cuando el cliente no tiene acceso a un archivo o directorio, ese archivo no se incluye en la lista de entradas devueltas al cliente. Esta opción no está activada de forma predeterminada.
- Is a DFS Namespace (Es un espacio de nombres de DFS): propiedad que indica si este recurso compartido está aprovisionado como un "espacio de nombres de DFS" [214] independiente.
- Share-level ACL (ACL de nivel de recurso compartido): una ACL combinada con la ACL de un archivo o directorio en el recurso compartido para determinar los permisos vigentes para ese archivo. De forma predeterminada, 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 sólo 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.

No puede haber dos recursos compartidos "SMB" [214] en el mismo sistema que compartan el mismo nombre de recurso. Los nombres de recursos heredados de proyectos tienen un comportamiento especial; para obtener más información, consulte la sección sobre "Proyectos" [362]. 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 sólo 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 sólo lectura, se producirá un error en esa solicitud abierta, pero el archivo aún será incluido en la lista de entradas.

Recursos compartidos: iSCSI

- Target group (Grupo de destinos): destinos a los cuales se exporta este LUN.
- Initiator group(s) (Grupo de iniciadores): iniciadores que pueden acceder a este LUN. A partir de la versión de software 2013.1.0, se pueden asignar varios grupos de iniciadores

a un LUN. Al editar grupos de iniciadores, si se selecciona la casilla de verificación PERSIST (opción predeterminada), se conserva el número LUN del grupo de iniciadores correspondiente. Si no se la selecciona, el dispositivo ZFSSA puede reasignar los LUN después de un cambio de configuración de la SAN o un reinicio.

- LU (logical unit) number (Número de LU [unidad lógica]): a medida que los LUN se asocian a grupos de iniciadores y destinos, se les asigna un número de unidad lógica único por grupo de destino y par de iniciador. No puede haber dos LUN a los que tiene acceso un iniciador a través de un grupo de destinos que tengan el mismo número de unidad lógica. Esta propiedad controla si una unidad lógica debe tener el número cero o un número asignado automáticamente.
- Operational status (Estado operativo): estado operativo del LUN. Los iniciadores no pueden acceder a un LUN fuera de línea, independientemente de la configuración del iniciador o del destino.
- Write cache behavior (Comportamiento de la caché de escritura): esta configuración controla la escritura de la caché del LUN. Cuando esta configuración está desactivada, todas las escrituras serán síncronas y, si no hay un dispositivo de log disponible, el rendimiento de la escritura se verá afectado considerablemente. Por consiguiente, cuando se activa esta configuración, mejora radicalmente el rendimiento de la escritura, pero también se podrán producir daños en los datos en caso de un cierre inesperado o un failover, excepto que la aplicación del cliente comprenda la semántica de una caché de escritura volátil y alinee la caché correctamente cuando sea necesario. Antes de activar esta opción, consulte la documentación de la aplicación del cliente.
- GUID: el GUID del LUN es un identificador de sólo lectura único global que identifica el dispositivo SCSI. Este GUID permanece constante dentro de diferentes nodos principales y entornos replicados.

Recursos compartidos: HTTP

TABLA 12-11 Propiedades HTTP de recursos compartidos

Propiedad	Descripción
Share mode	Modo de recurso compartido de HTTP para este sistema de archivos: ninguno, sólo lectura o lectura/escritura.

Recursos compartidos: FTP

TABLA 12-12 Propiedades FTP de recursos compartidos

Propiedad	Descripción
Share mode	Modo de recurso compartido de FTP para este sistema de archivos: ninguno, sólo lectura o lectura/escritura.

Recursos compartidos: SFTP

TABLA 12-13 Propiedades SFTP de recursos compartidos

Propiedad	Descripción
Share mode	Modo de recurso compartido de SFTP para este sistema de archivos: ninguno, sólo lectura o lectura/escritura.

Shares (Recursos compartidos) > Shares (Recursos compartidos) > Access (Acceso)

Control de acceso

Esta vista le permite configurar opciones para controlar el comportamiento de la ACL, además de controlar el acceso al directorio raíz del sistema de archivos. Esta vista sólo está disponible para sistemas de archivos.

Recursos compartidos: acceso al directorio raíz

Controla el acceso básico a la raíz del sistema de archivos. 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 sólo lectura, ya que requieren el cambio de metadatos del directorio raíz del sistema de archivos.

Recursos compartidos: 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 el servicio “Asignación de identidad” [266]. En el caso del acceso a NFS basado en Unix, esto se puede cambiar desde el cliente con el comando `chown`.

Recursos compartidos: 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 el

servicio “Asignación de identidad” [266]. En el caso del acceso a NFS basado en Unix, esto se puede cambiar desde el cliente con el comando `chgrp`.

Recursos compartidos: 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.

TABLA 12-14 Usuarios de recursos compartidos

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.

TABLA 12-15 Permisos de recursos compartidos

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.

- A partir de la versión de software 2011.1, el siguiente comportamiento adicional se asocia con el permiso "write" (escritura) para todos los directorios:
- Los archivos secundarios del directorio se pueden suprimir (igual que el permiso ACL D), a menos que el indicador sticky bit esté configurado en el directorio, en cuyo caso los archivos secundarios sólo se podrán suprimir si lo solicita el propietario del archivo.
- Se pueden cambiar los horarios asociados con un archivo o directorio (al igual que el permiso ACL A).

- Se pueden crear atributos extendidos y las escrituras se pueden incluir en el directorio de atributos extendidos (al igual que el permiso ACL W).

Para seleccionar permisos en la BUI, se debe hacer clic en los cuadros individuales. De manera alternativa, si hace clic en la etiqueta ("user" [usuario], "group" [grupo] u "other" [otro]), se seleccionarán todos los permisos dentro de la etiqueta o se anulará su selección. En la CLI, los permisos se especifican como un valor octal de Unix estándar, donde cada dígito corresponde a las opciones usuario, grupo y otro, en ese orden. Cada dígito es el resultado de la suma de lectura (4), escritura (2) y ejecución (1). Por lo tanto, el valor de permisos de `743` sería el equivalente del usuario RWX, grupo R, otro WX.

Como alternativa a la configuración de bits de permisos POSIX en la hora de creación del recurso compartido, los administradores en cambio pueden seleccionar la opción "Use Windows Default Permissions" (Usar permisos predeterminados de Windows), que aplicará una ACL según se describe en la sección de “ACL del directorio raíz” [344] a continuación. Se trata de un atajo utilizado para simplificar la administración en entornos gestionados de manera exclusiva o predominante por usuarios con operaciones de Windows en segundo plano y tiene como finalidad proporcionar un comportamiento similar a la creación de recursos compartidos en un servidor de Windows.

Recursos compartidos: comportamiento de la ACL

Para obtener información sobre las ACL y su funcionamiento, consulte la documentación de “ACL del directorio raíz” [344].

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.

TABLA 12-16 Valores de cambio de modo

Valor de la BUI	Valor de la CLI	Descripción
Descartar ACL	discard	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	mask	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

Valor de la BUI	Valor de la CLI	Descripción
		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 la ACL	passthrough	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.

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 sólo 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`.

TABLA 12-17 Valores de comportamiento heredados de ACL

Valor de la BUI	Valor de la CLI	Descripción
Do not inherit entries	discard	No se heredan entradas de la ACL. El archivo o directorio se crea según el cliente y el protocolo que se utiliza.
Only inherit deny entries	noallow	Sólo se heredan las entradas de ACL que especifican permisos de "denegación".
Inherit all but "write ACL" and "change owner"	restricted	Elimina los permisos "write_acl" y "write_owner" cuando se hereda la entrada de ACL, pero en caso contrario, deja intactas las entradas de ACL heredables. Este es el valor por defecto.
Inherit all entries	passthrough	Se heredan todas las entradas de ACL heredables. Generalmente, el modo "passthrough" se utiliza para crear todos los archivos de "datos" con el mismo modo en un

Valor de la BUI	Valor de la CLI	Descripción
		árbol de directorio. El administrador configura la herencia de la ACL para crear todos los archivos con un modo, por ejemplo, 0664 o 0666.
Inherit all but "execute" when not specified	passthrough-x	Igual que "passthrough", excepto que las entradas de ACL de propietario, grupo y todos heredan el permiso de ejecución sólo si el modo de creación de archivos también solicita el bit de ejecución. La configuración "passthrough" funciona como se espera para los archivos de datos, pero posiblemente desee incluir de manera opcional el bit de ejecución del modo de creación de archivos en la ACL heredada. Un ejemplo es el archivo de salida que se genera a partir de herramientas, como "cc" o "gcc". 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 chmod(1) para cambiar los permisos del archivo.

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.

Todos los comportamientos anteriores están sujetos a cambios en versiones futuras.

ACL del 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 ZFSSA admite ACL de estilo NFSv4, 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 sólo afecta el directorio raíz del sistema de archivos. Las ACL se pueden controlar mediante la gestión de protocolos en banda, pero la BUI ofrece una manera de configurar la ACL sólo para el directorio raíz del sistema de archivos. No hay manera de configurar la ACL del directorio raíz mediante la CLI. 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). Cada ACE describe un tipo/destino, un modo, un conjunto de permisos e indicadores de herencia. 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 12-18 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 nombrado	Usuario designado por el campo de destino. 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 designado por el campo de destino. 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 12-19 Recursos compartidos: modos de ACL

Modo	Descripción
Allow	Los permisos se otorgan de manera explícita al destino de la ACE.

Modo	Descripción
Deny	Los permisos se deniegan de manera explícita al destino de la ACE.

TABLA 12-20 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)	Execute File/Traverse Directory (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 `ls` y `stat`.
(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. 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 sólo 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.

	Permiso	Descripción
(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, sólo el propietario del archivo puede suprimir el archivo secundario.
(A)	Escribir atributos	Permiso para cambiar los horarios asociados con un archivo o directorio.
(W)	Escribir atributos extendidos	Permiso para crear atributos extendidos o escribir en el directorio de atributos extendidos.
	Administración	
(c)	Leer ACL/permisos	Permiso para leer la ACL.
(C)	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: "Apply to Files" (Aplicar a archivos) o "Apply to Directories" (Aplicar a directorios).
(n)	No aplicar elementos secundarios pasados	La ACE actual sólo debe heredar un nivel de los tres hacia los elementos secundarios inmediatos. Este indicador requiere la configuración de una de las siguientes opciones: "Apply to Files" (Aplicar a archivos) o "Apply to Directories" (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 12-21 Entidades de directorio raíz de recursos compartidos

Tipo	Acción	Acceso
Propietario	Permitir	Control completo
Grupo	Permitir	Leer y ejecutar
Todos	Permitir	Leer y ejecutar

Recursos compartidos: instantáneas

Las instantáneas son copias de sólo lectura de un sistema de archivos en un punto dado en el tiempo. Para obtener más información sobre las instantáneas y sobre cómo funcionan, consulte la página de “conceptos” [300].

Propiedades de instantánea de recursos compartidos

.zfs/snapshot visible

Se puede 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. Este directorio contiene una lista de todas las instantáneas del sistema de archivos; se puede acceder a ellas del mismo modo que a los datos del sistema de archivos normal (en modo de sólo lectura). De forma predeterminada, el directorio '.zfs' no está visible en la lista de contenidos del directorio, pero se puede acceder a éste 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.

TABLA 12-22 Valores de instantánea

Valor de la BUI	Valor de la CLI	Descripción
Hidden	hidden	El directorio .zfs no está visible al mostrar el contenido del directorio en la raíz del sistema de archivos. Éste es el valor predeterminado.
Visible	visible	El directorio .zfs aparece como cualquier otro directorio en el sistema de archivos.

Etiqueta de instantáneas programada

Esta propiedad opcional anexa 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 instantáneas pueden ayudar a identificar el proyecto o el recurso compartido para el cual se tomó una instantánea, por ejemplo, "project1:share1" puede indicar una instantánea programada tomada en share1 dentro de project1. Las etiquetas pueden tener hasta 35 caracteres alfanuméricos e incluir caracteres especiales _ - . :

Visualización de instantáneas con la BUI

La lista de instantáneas activas del recurso compartido se encuentra en la ficha "snapshots" (Instantáneas). La lista se divide en dos fichas: la ficha "Snapshots" (Instantáneas) se utiliza para examinar y gestionar instantáneas. La ficha "Schedules" (Programas) gestiona programas de instantáneas automáticas. Dentro de la ficha "Snapshots", puede elegir entre ver todas las instantáneas, sólo instantáneas manuales o sólo instantáneas programadas. Para cada instantánea, se muestran los siguientes campos:

Campo	Descripción
Name	Nombre de la instantánea. Hay dos tipos de instantáneas: manual y automática.
	Instantáneas manuales: "Name" (Nombre) es el nombre proporcionado al crear la instantánea. Para cambiar el nombre de las instantáneas manuales, se debe hacer clic en el nombre e introducir un valor nuevo.
	Instantáneas automáticas: Hay tres tipos y el nombre no se puede cambiar:
	- .auto: instantáneas configuradas por el usuario con políticas de retención personalizadas (consulte “Instantáneas programadas” [352]).
	- .ndmp: se utilizan para la copia de seguridad de NDMP y se eliminan automáticamente.
	- .rr: se utilizan para la replicación remota y se eliminan automáticamente.
Creation	Fecha y hora de creación de la instantánea.
Unique	Cantidad de espacio único utilizado por la instantánea. Inicialmente, las instantáneas hacen referencia a los mismos bloques que el sistema de archivos o el propio LUN. A medida que el sistema de archivos se desvía, los bloques modificados en el recurso compartido activo pueden permanecer retenidos por una o varias

Campo	Descripción
	instantáneas. Cuando un bloque forma parte de varias instantáneas, se registrará en el uso de la instantánea del recurso compartido, pero no aparecerá en el espacio único de ninguna instantánea en particular. El espacio único se compone de bloques que sólo son mantenidos por una instantánea en particular, y representa la cantidad de espacio que se liberaría si se destruyera la instantánea.
Total	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	Muestran la cantidad de “clones” [300] de la instantánea. Cuando se pasa el mouse sobre una fila de instantáneas con una cantidad de clones distinta de cero, aparecerá el enlace "Show..." (Mostrar...). Al hacer clic en este enlace, aparecerá un cuadro de diálogo que muestra la lista completa de todos los clones.

Instantáneas manuales con la BUI

Hay dos tipos de instantáneas: de nivel de proyecto y de nivel de recurso compartido/LUN.

▼ Creación de una instantánea de nivel de proyecto

1. **Abra el proyecto del cual desea crear una instantánea.**
2. **Haga clic en la ficha Snapshots (Instantáneas).**
3. **Haga clic en el ícono  . Aparece la lista de instantáneas.**
4. **En el cuadro de diálogo, escriba un nombre para la instantánea.**
5. **Para crear la instantánea, haga clic en "apply" (Aplicar).**

▼ Creación de una instantánea de nivel de recurso compartido/LUN

1. **Abra el recurso compartido/LUN del cual desea crear una instantánea.**

2. **Haga clic en la ficha Snapshots (Instantáneas).**

3. **Haga clic en el ícono . Aparece la lista de instantáneas.**

4. **En el cuadro de diálogo, escriba un nombre para la instantánea.**

5. **Para crear la instantánea, haga clic en "apply" (Aplicar).**

   No hay límite para la cantidad de instantáneas que se pueden tomar, pero cada instantánea consume memoria, de modo que la creación de una gran cantidad de instantáneas puede disminuir la velocidad del sistema. El límite práctico para la cantidad de instantáneas en todo el sistema depende de la configuración del sistema, pero debería ser de más de cien mil.

▼ Cambio de nombre de una instantánea (BUI)

1. **Para cambiar el nombre de una instantánea, haga clic en el nombre, en la lista de instantáneas activas. De esta manera, se activará un cuadro de entrada de texto.**

2. **Después de actualizar el nombre en la entrada de texto, presione la tecla de retorno o cambie el enfoque para confirmar los cambios.**

▼ Destrucción de una instantánea (BUI)

1. **Para destruir una instantánea, haga clic en el ícono cuando se encuentre sobre la fila de la instantánea de destino.**

2. **Para destruir una instantánea, deberá destruir los clones y sus descendientes. En ese caso, aparecerá una lista de los clones que se verán afectados.**

▼ Reversión de una instantánea (BUI)

1. **Para revertir un sistema de archivos, haga clic en el ícono correspondiente a la instantánea de destino.**

2. **Aparecerá un cuadro de diálogo de confirmación y, si existen clones de la instantánea, instantáneas más recientes o descendientes de ellas, se mostrarán y se indicará que serán destruidos como parte de dicho proceso.**

Además de usarse para tener acceso a los datos de un directorio de instantáneas del sistema de archivos, las instantáneas también se pueden utilizar para volver una instancia anterior del sistema de archivos o LUN. Para ello, se deben destruir las instantáneas más recientes y sus clones, y de esta manera el contenido de los recursos compartidos se revertirá al estado en que se encontraba en el momento en que se tomó la instantánea. Esto no afecta ninguna configuración de propiedad del recurso compartido, aunque se perderán los cambios en el acceso al directorio raíz del sistema de archivos, ya que esto forma parte de los datos del sistema de archivos.

▼ Clonación de una instantánea (BUI)

- **Para crear un clon, haga clic en el ícono  correspondiente a la instantánea de origen. Aparecerá un cuadro de diálogo para los siguientes valores.**

  - Project (Proyecto): proyecto de destino. De manera predeterminada, los clones se crean dentro del proyecto actual, pero también se pueden crear en proyectos diferentes (o moverse entre proyectos).
  - Name (Nombre): escriba un nombre para el clon.
  - Mountpoint (Punto de montaje): para usar este valor, haga clic en el ícono del candado. Establezca el punto de montaje para el clon. Cuando se usa la opción Retain Other Local Settings (Conservar otras propiedades locales), se debe asignar un punto de montaje diferente al clon, ya que los recursos compartidos no pueden guardar el mismo punto de montaje.
  - Resource Name (Nombre del recurso): para usar este valor, haga clic en el ícono del candado. Introduzca el recurso que desea usar para el clon.
  - Retain Other Local Settings (Conservar otras propiedades locales): de manera predeterminada, todas las propiedades heredadas actualmente del sistema de archivos se heredarán del proyecto de destino en el clon. Siempre se conserva la configuración local. Al configurar esta propiedad, las propiedades heredadas se preservan como configuración local en el clon nuevo.

  Un “clon” [300] es una copia modificable de una instantánea y se gestiona como cualquier otro recurso compartido. Al igual que las instantáneas de los sistemas de archivos, inicialmente no consume espacio adicional. A medida que cambien los datos del clon, éste consumirá más espacio. La instantánea original no se puede destruir sin destruir también el clon. Las instantáneas programadas se pueden clonar de manera segura y las instantáneas programadas con clones se ignorarán si se deben destruir de todos modos.

Instantáneas programadas con la BUI

Además de las instantáneas manuales, puede configurar instantáneas automáticas según la siguiente tabla. Estas instantáneas se denominan ".auto-<registro de hora>", y se pueden tomar con programas con frecuencia cada media hora, cada hora, diaria, semanal o mensual. Un programa es una lista de intervalos y políticas de retención.

Las horas se muestran en 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.

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.

Versiones anteriores del software permitían instantáneas automáticas con una frecuencia de un minuto. Se comprobó que esto generaba una tensión innecesaria en el sistema y, en general, no resultaba útil. Para ayudar a los usuarios a evitar generar una tensión innecesaria en el sistema, esta característica se eliminó en la versión 2010.Q3. Ahora las instantáneas sólo se pueden especificar para un período de una vez cada media hora o un período mayor. Los períodos en minutos existentes se conservarán si se realiza una reversión del software, y las instancias anteriores caducarán según el programa existente, pero no se tomarán nuevas instantáneas. Se emitirá una alerta, si se encuentra un recurso compartido o proyecto con esta frecuencia.

▼

- **Para agregar un nuevo intervalo, haga clic en el ícono mientras visualiza la ficha "Schedules" (Programas). Cada intervalo tiene las siguientes propiedades.**

Propiedad	Descripción
Frequency	Una de "half hour" (media hora), "hour" (hora), "day" (día), "week" (semana), o "month" (mes). Esto indica con qué frecuencia se toma la instantánea.
Offset	Especifica un desplazamiento dentro de la frecuencia. Por ejemplo, al seleccionar una frecuencia de hora, se pueden tomar instantáneas en un desplazamiento en minutos explícito de la hora. En el caso de las instantáneas diarias, el desplazamiento puede especificar horas y minutos, y en el caso de las instantáneas

Propiedad	Descripción
	semanales o mensuales, el desfase puede especificar días, horas y minutos.
Keep at most	Controla la política de retención de las instantáneas. 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. Este límite suprimirá las instantáneas automáticas para el intervalo determinado, si éstas son más antiguas que la política de retención. Esto en realidad se aplica según el horario en que fueron tomadas las instantáneas y no según un recuento absoluto. Por consiguiente, si tiene instantáneas por hora y el dispositivo ZFSSA no está en funcionamiento durante un día, cuando vuelva a funcionar, se suprimirán todas las instantáneas por hora. Las instantáneas que forman parte de intervalos múltiples se destruyen sólo cuando ningún intervalo especifica que se deben mantener.

Instantáneas manuales con la CLI

Para acceder a las instantáneas de los recursos compartidos, navegue hasta el recurso compartido y el contexto de instantáneas.

```
clownfish:> shares select default select builds
clownfish:shares default/builds> snapshots
clownfish:shares default/builds snapshots>
```

Visualización de instantáneas (CLI)

Las instantáneas se pueden mostrar con los comandos de la CLI estándar.

```
clownfish:shares default/builds snapshots> list
today
yesterday
clownfish:shares default/builds snapshots>
```

Toma de instantáneas manuales (CLI)

Para tomar una instantánea de nivel de proyecto, navegue hasta el nodo del proyecto o instantánea y use el comando `snapshot`:

```
clownfish:cd /
```

```
clownfish:shares select myproject snapshots
clownfish:shares myproject snapshots> snapshot cob_monday
```

Para tomar una instantánea manual de nivel de recurso compartido de un recurso compartido individual, navegue hasta ese recurso compartido y use el comando snapshot allí:

```
clownfish:cd /
clownfish:shares select myproject select share1 snapshots
clownfish:snapshot lunchtime
```

Cambio de nombre de una instantánea (CLI)

Para cambiar el nombre de una instantánea, utilice el comando `rename`:

```
clownfish:shares default/builds snapshots> rename test test2
clownfish:shares default/builds snapshots>
```

Destrucción de una instantánea (CLI)

Para destruir una instantánea, utilice el comando `destroy`:

```
clownfish:shares default/builds snapshots> select test2
clownfish:shares default/builds@test2> destroy
This will destroy this snapshot. Are you sure? (Y/N)
clownfish:shares default/builds snapshots>
```

También puede utilizar el comando `destroy` desde el contexto del recurso compartido sin seleccionar una instantánea individual:

```
clownfish:shares default/builds snapshots> destroy test2
This will destroy this snapshot. Are you sure? (Y/N)
clownfish:shares default/builds snapshots>
```

Reversión de una instantánea (CLI)

Para revertir a una instantánea, seleccione la instantánea de destino y ejecute el comando `rollback`:

```
clownfish:shares default/builds snapshots> select today
clownfish:shares default/builds@today> rollback
Rolling back will revert data to snapshot, destroying newer data. Active
initiators will be disconnected.

Continue? (Y/N)
clownfish:shares default/builds@today>
```

Clonación de una instantánea (CLI)

Para clonar una instantánea, utilice el comando `clone`. Este comando lo llevará a un contexto de recurso compartido no confirmado idéntico al que se utiliza para crear recursos compartidos. Desde aquí, podrá ajustar las propiedades según sea necesario antes de confirmar los cambios para crear el clon.

```
clownfish:shares default/builds snapshots> select today
clownfish:shares default/builds@today> clone testbed
clownfish:shares default/testbed (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)
                      sharedav = 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)
clownfish:shares default/testbed (uncommitted clone)> set quota=10G
                         quota = 10G (uncommitted)
clownfish:shares default/testbed (uncommitted clone)> commit
clownfish:shares default/builds@today>
```

El comando además admite un primer argumento opcional, que es el proyecto en el cual se creará el clon. De manera predeterminada, el clon se crea en el mismo proyecto que el recurso compartido que se está clonando.

Visualización de clones dependientes con la CLI

Para visualizar una lista de todos los clones creados a partir de una instantánea en particular (clones dependientes), navegue hasta la instantánea , a continuación, use el comando list clones.

```
clonefish:shares default/builds> snapshots
clonefish:shares default/builds snapshots> select today
```

```
clonefish:shares default/builds@today> list clones

Clones: 2 total

PROJECT          SHARE
default          testbed
default          production
clonefish:shares default/builds@today>
```

El resultado muestra los nombres de los clones y el proyecto en el que reside cada clon.

Instantáneas programadas con la CLI

Las instantáneas automáticas programadas se pueden configurar con el comando `automatic` del contexto de instantáneas en el nivel de proyecto de un recurso compartido individual. Una vez que se encuentra en este contexto, puede agregar y eliminar nuevos intervalos con los comandos `create` y `destroy`. Cada intervalo tiene un conjunto de propiedades que se asignan a la vista de la BUI de la frecuencia, el desplazamiento y la cantidad de instantáneas que se mantendrán. Los programas se mantienen en formato UTC.

```
clownfish:shares default/builds snapshots> automatic
clownfish:shares default/builds snapshots automatic> create
clownfish:shares default/builds snapshots automatic (uncommitted)> set frequency=day
                     frequency = day (uncommitted)
clownfish:shares default/builds snapshots automatic (uncommitted)> set hour=14
                          hour = 14 (uncommitted)
clownfish:shares default/builds snapshots automatic (uncommitted)> set minute=30
                        minute = 30 (uncommitted)
clownfish:shares default/builds snapshots automatic (uncommitted)> set keep=7
                          keep = 7 (uncommitted)
clownfish:shares default/builds snapshots automatic (uncommitted)> get
                     frequency = day (uncommitted)
                           day = (unset)
                          hour = 14 (uncommitted)
                        minute = 30 (uncommitted)
                          keep = 7 (uncommitted)
clownfish:shares default/builds snapshots automatic (uncommitted)> commit
clownfish:shares default/builds snapshots automatic> list
NAME                 FREQUENCY            DAY                  HH:MM KEEP
automatic-000        day                  -                    14:30    7
clownfish:shares default/builds snapshots automatic> done
clownfish:shares default/builds snapshots>
```

Configuración de la etiqueta de instantáneas programadas con la CLI

En la BUI, la propiedad "scheduled snapshot label" (Etiqueta de instantánea programada) se puede configurar para proyectos o recursos compartidos. Del mismo modo, en la CLI, la etiqueta se puede definir navegando primero al contexto del proyecto o del recurso compartido. Para crear una etiqueta de instantánea programada, use el comando `set snaplabel`:

```
clownfish:shares project1/share1> set snaplabel=project1:share1
```

Proyectos

Los recursos compartidos, los sistemas de archivos y los LUN se pueden agrupar en proyectos. Un proyecto define un punto de control administrativo común para la gestión de recursos compartidos. Los recursos compartidos de un proyecto pueden compartir configuraciones en común, y se pueden aplicar cuotas en el nivel del proyecto además del nivel de recursos compartidos. 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.

De forma predeterminada, el dispositivo ZFSSA genera un único proyecto *predeterminado* cuando se configura por primera vez una agrupación de almacenamiento. Es posible generar todos los recursos compartidos dentro de este proyecto predeterminado, aunque en el caso de entornos de tamaño razonable, se recomienda generar proyectos adicionales, aunque sólo sea con fines organizativos.

Trabajo con proyectos en la BUI

Para acceder a la UI de proyectos , se utiliza Shares (Recursos compartidos) -> Projects (Proyectos). Se presentará una lista de todos los proyectos del sistema, aunque los proyectos se pueden seleccionar mediante el panel del proyecto o haciendo clic en el nombre del proyecto mientras se edita un recurso compartido dentro de un proyecto.

Campos del proyecto

Después de navegar a la vista del proyecto, aparecerá una lista de los proyectos del sistema. De manera alternativa, puede navegar hasta la pantalla de recursos compartidos y abrir el panel del proyecto obtener un acceso directo a los proyectos. El panel no escala bien con grandes cantidades de proyectos y no reemplaza la lista completa de proyectos. Se muestran los siguientes campos para cada proyecto:

TABLA 12-23 Campos del proyecto

Campo	Descripción
Name	Nombre del recurso compartido. El nombre del recurso compartido es un campo de texto editable. Al hacer clic en el nombre, podrá introducir un nombre nuevo para el proyecto. Para confirmar el cambio, debe presionar la tecla de retorno o alejar el enfoque del nombre. Se le solicitará que confirme la acción, ya que para

Campo	Descripción
	cambiar el nombre de los recursos compartidos, se deben desconectar los clientes activos.
Size	El tamaño total de todos los recursos compartidos dentro del proyecto y la reserva sin uso.

Las siguientes herramientas están disponibles para cada proyecto:

TABLA 12-24 Íconos del proyecto

Ícono	Descripción
	Permite editar un proyecto individual (al que también se puede acceder haciendo doble clic en la fila).
	Permite destruir el proyecto. Se le solicitará que confirme la acción, ya que destruirá todos los datos del recurso compartido y esta acción no se puede deshacer.

Edición de un proyecto

Para editar un proyecto, haga clic en el ícono de lápiz o haga doble clic en la fila de la lista de proyectos, o bien, haga clic en el nombre en el panel de proyectos. De esta manera, seleccionará el proyecto y tendrá diferentes fichas entre las que podrá elegir para editar las propiedades del proyecto.

El nombre del proyecto se presenta en la esquina superior izquierda, a la derecha del panel del proyecto. Para cambiar el nombre del proyecto, también puede hacer clic en el nombre del proyecto y escribir el nuevo texto. Se le solicitará que confirme la acción, ya que será necesario desconectar los clientes activos del proyecto.

Estadísticas de uso

A la izquierda de la vista (debajo del panel del proyecto expandido), hay una tabla en la que se explican las estadísticas de uso del espacio actual. Si hay propiedades con el valor cero, se excluyen de la tabla. La mayoría de estas propiedades son idénticas entre proyectos y recursos compartidos, aunque existen algunas estadísticas que solo tienen sentido para los proyectos.

- Available space (Espacio disponible): consulte “Shares (Recursos compartidos) > Shares (Recursos compartidos)” [314].
- Referenced data (Datos de referencia): suma de todos los datos de referencia para todos los recursos compartidos dentro del proyecto, además de una pequeña cantidad de sobrecarga del proyecto. Consulte “Shares (Recursos compartidos) > Shares (Recursos compartidos)” [314] para obtener más información acerca de la manera en que se calculan los datos de referencia para los recursos compartidos.

- Snapshot data (Datos de instantánea): suma de todos datos de instantáneas para todos los recursos compartidos, y cualquier sobrecarga de instantáneas del proyecto. Consulte “Shares (Recursos compartidos) > Shares (Recursos compartidos)” [314] para obtener más información acerca de la manera en que se calculan los datos de las instantáneas para los recursos compartidos.
- Unused Reservation (Reserva sin uso): reserva sin uso del proyecto. Solo comprende datos que en la actualidad no se utilizan para la reserva de nivel de proyecto. No comprende reservas sin uso de los recursos compartidos incluidos en el proyecto.
- Unused Reservation of shares (Reserva sin uso de recursos compartidos): suma de las reservas sin uso de todos los recursos compartidos. Consulte “Shares (Recursos compartidos) > Shares (Recursos compartidos)” [314] para obtener más información acerca de la manera en que se calculan las reservas sin uso para los recursos compartidos.
- Total space (Espacio total): suma de los datos de referencia, los datos de instantáneas, la reserva sin uso y la reserva sin uso de recursos compartidos.

Propiedades estáticas

El lado izquierdo de la vista de recursos compartidos también muestra las propiedades estáticas al editar un proyecto en particular. Estas propiedades son de solo lectura y no se pueden modificar.

- Compression ratio (Ratio de compresión): consulte la descripción completa en “Shares (Recursos compartidos) > Shares (Recursos compartidos)” [314].

▼ Creación de proyectos

1. **Para crear un proyecto, visualice la lista de proyectos y haga clic en el botón  .**
2. **De manera alternativa, al hacer clic en el botón "Add..." (Agregar) en el panel del proyecto, se presentará el mismo cuadro de diálogo. Introduzca el nombre del proyecto y haga clic en Aplicar para crear el proyecto.**

Trabajo con proyectos en la CLI

La CLI de proyectos se encuentra en `shares`.

Navegación

Para seleccionar un proyecto, utilice el comando `select`:

```
clownfish:> shares
clownfish:shares> select default
clownfish:shares default> get
                    aclinherit = restricted
                       aclmode = discard
                         atime = true
                      checksum = fletcher4
                   compression = off
                  compressratio = 100
                        copies = 1
                      creation = Thu Oct 23 2009 17:30:55 GMT+0000 (UTC)
                    mountpoint = /export
                         quota = 0
                      readonly = false
                    recordsize = 128K
                   reservation = 0
                 secondarycache = all
                          nbmand = false
                      sharesmb = off
                      sharenfs = on
                       snapdir = hidden
                     snaplabel = project1:share1
                         vscan = false
                      sharedav = off
                      shareftp = off
                 default_group = other
           default_permissions = 700
                default_sparse = false
                  default_user = nobody
          default_volblocksize = 8K
               default_volsize = 0
                    space_data = 43.9K
              space_unused_res = 0
       space_unused_res_shares = 0
               space_snapshots = 0
               space_available = 12.0T
                   space_total = 43.9K
clownfish:shares default>
```

Operaciones de los proyectos

Para crear un proyecto, se utiliza el comando `project`. Las propiedades se pueden modificar según sea necesario antes de confirmar los cambios:

```
clownfish:shares> project home
clownfish:shares home (uncommitted)> get
                    mountpoint = /export (default)
                         quota = 0 (default)
                   reservation = 0 (default)
                      sharesmb = off (default)
                      sharenfs = on (default)
```

```
                    sharedav = off (default)
                    shareftp = off (default)
                 default_group = other (default)
           default_permissions = 700 (default)
                default_sparse = true (default)
                  default_user = nobody (default)
          default_volblocksize = 8K (default)
               default_volsize = 0 (default)
                    aclinherit = (default)
                       aclmode = (default)
                         atime = (default)
                      checksum = (default)
                   compression = (default)
                        copies = (default)
                      readonly = (default)
                    recordsize = (default)
                secondarycache = (default)
                         nbmand = (default)
                        snapdir = (default)
                     snaplabel = project1:share1
                         vscan = (default)
                custom:contact = (default)
             custom:department = (default)
clownfish:shares home (uncommitted)> set sharenfs=off
                    sharenfs = off (uncommitted)
clownfish:shares home (uncommitted)> commit
clownfish:shares>
```

Para destruir un proyecto, se utiliza el comando `destroy`:

```
clownfish:shares> destroy home
This will destroy all data in "home"! Are you sure? (Y/N)
clownfish:shares>
```

Este comando también se puede ejecutar desde el contexto del proyecto después de seleccionar un proyecto.

Para cambiar el nombre de un proyecto, se utiliza el comando `rename`:

```
clownfish:shares> rename default home
clownfish:shares>
```

Selección de una agrupación en un cluster

En una configuración de cluster activo/activo, un nodo puede controlar ambas agrupaciones durante un failover. En este caso, el contexto de la CLI mostrará la agrupación actual entre paréntesis. Para cambiar las agrupaciones, debe utilizar el comando `set` desde el contexto de recursos compartidos de nivel superior:

```
clownfish:shares (pool-0)> set pool=pool-1
clownfish:shares (pool-1)>
```

Una vez que se ha seleccionado el contexto de la agrupación, los proyectos y los recursos compartidos se gestionan dentro de esa agrupación mediante las interfaces de la CLI estándar.

Propiedades del proyecto

Las siguientes propiedades están disponibles en la CLI, con su equivalente en la BUI. Las propiedades se pueden configurar mediante los comandos CLI estándar `get` y `set`. Además, las propiedades se pueden heredar del proyecto principal mediante el comando `unset`.

Nombre de la CLI	"Tipo" [300]	Nombre de la BUI	Ubicación de la BUI
aclinherit	inherited	"Acceso del proyecto" [372]	Acceso
aclmode	inherited	"Acceso del proyecto" [372]	Acceso
atime	inherited	"General de proyecto" [369]	General
checksum	inherited	"General de proyecto" [369]	General
compression	inherited	"General de proyecto" [369]	General
compressratio	read-only	"Proyectos" [362]	Estática
copies	inherited	"General de proyecto" [369]	General
creation	read-only	-	-
dedup	inherited	"General de proyecto" [369]	General
default_group	creation default	"General de proyecto" [369]	General
default_permissions	creation default	"General de proyecto" [369]	General
default_sparse	creation default	"General de proyecto" [369]	General
default_user	creation default	"General de proyecto" [369]	General
default_volblocksize	creation default	"General de proyecto" [369]	General
default_volsize	creation default	"General de proyecto" [369]	General

Nombre de la CLI	"Tipo" [300]	Nombre de la BUI	Ubicación de la BUI
mountpoint	inherited	"General de proyecto" [369]	General
nbmand	inherited	"General de proyecto" [369]	General
quota	space management	"General de proyecto" [369]	General
readonly	inherited	"General de proyecto" [369]	General
recordsize	inherited	"General de proyecto" [369]	General
reservation	space management	"General de proyecto" [369]	General
secondary cache	inherited	"General de proyecto" [369]	General
sharedav	inherited	"Protocolos del proyecto" [371]	Protocolos
shareftp	inherited	"Protocolos del proyecto" [371]	Protocolos
sharenfs	inherited	"Protocolos del proyecto" [371]	Protocolos
sharesmb	inherited	"Protocolos del proyecto" [371]	Protocolos
snapdir	inherited	"Instantáneas de proyecto" [372]	Instantáneas
snaplabel	inherited	"Instantáneas de proyecto" [372]	Instantáneas
space_available	read-only	"Proyectos" [362]	Uso
space_data	read-only	"Proyectos" [362]	Uso
space_snapshots	read-only	"Proyectos" [362]	Uso
space_total	read-only	"Proyectos" [362]	Uso
space_unused_res	read-only	"Proyectos" [362]	Uso
space_unused_res_shares	read-only	"Proyectos" [362]	Uso
vscan	inherited	"General de proyecto" [369]	General

General de proyecto

Propiedades generales de proyectos

Esta sección de la BUI controla los valores de configuración generales del proyecto que son independientes de cualquier protocolo específico y no se relacionan con las instantáneas ni el control de acceso. Si bien la CLI agrupa todas las propiedades en una única lista, en esta sección, se describe el comportamiento de las propiedades en ambos contextos.

Para obtener más información sobre cómo se asignan estas propiedades a la CLI, consulte la sección “CLI de proyectos”.

Uso de espacio de proyectos

El espacio dentro de la agrupación de almacenamiento se comparte entre todos los recursos compartidos. Los sistemas de archivos pueden crecer o reducirse dinámicamente según sea necesario, aunque también es posible aplicar restricciones de espacio a cada recurso compartido. Para obtener más información sobre el almacenamiento agrupado, consulte la página de “conceptos” [300].

Cuota de proyectos

Determina un límite máximo sobre la cantidad total de espacio consumido por todos los sistemas de archivos y LUN dentro del proyecto. Para obtener más información, consulte la “sección de recursos compartidos” [327]. A diferencia de los sistemas de archivos, las cuotas de proyectos no pueden excluir las instantáneas y sólo se pueden aplicar a todos los recursos compartidos y sus instantáneas.

Reserva de proyectos

Garantiza una cantidad mínima de espacio para utilizar en todos los sistemas de archivos y LUN dentro del proyecto. Para obtener más información, consulte la “sección de recursos compartidos” [327]. A diferencia de los sistemas de archivos, la reserva del proyecto no puede excluir las instantáneas y sólo se puede aplicar a todos los recursos compartidos y sus instantáneas.

Propiedades heredadas de proyectos

Son propiedades estándar que pueden ser heredadas por recursos compartidos dentro del proyecto. El comportamiento de estas propiedades es idéntico al del nivel de recursos compartidos; para obtener más documentación, consulte la sección de recursos compartidos.

- "Mountpoint" [327]
- "Sólo lectura" [327]
- "Update access time on read" [327]
- "Non-blocking mandatory locking" [327]
- "Data compression" [327]
- "Data deduplication" [327]
- "Suma de comprobación" [327]
- "Cache device usage" [327]
- "Database record size" [327]
- "Additional replication" [327]
- "Virus scan" [327]

Propiedades personalizadas de proyectos

Se pueden agregar propiedades personalizadas según sea necesario para anexar etiquetas definidas por el usuario a proyectos y recursos compartidos. Para obtener más información, consulte "Esquemas" [374].

Valores predeterminados para la creación sistemas de archivos

Estos valores de configuración se utilizan para completar los valores predeterminados al crear un sistema de archivos. Su cambio no afecta los sistemas de archivos existentes. Para obtener más información, consulte la sección correspondiente de recursos compartidos.

- "User" [344]
- "Group" [344]
- "Permissions" [344]

Valores predeterminados para la creación de LUN

Estos valores de configuración se utilizan para completar los valores predeterminados al crear un LUN. Su cambio no afecta los LUN existentes. Para obtener más información, consulte la sección correspondiente de recursos compartidos.

- "Volume size" [327]
- "Thin provisioned" [327]
- "Shares (Recursos compartidos) > Shares (Recursos compartidos)" [314]

Protocolos del proyecto

Cada proyecto tiene propiedades específicas del protocolo que definen el comportamiento de protocolos diferentes para ese recurso compartido dentro del proyecto. En general, los "shares" [336] heredan propiedades específicas de protocolos de manera directa. Aquí se incluyen las excepciones y los casos especiales.

- NFS: las propiedades de los recursos compartidos de "NFS" [208] se heredan normalmente y se describen en la "documentación de recursos compartidos" [336].
- SMB
  - Resource name (Nombre de recurso): nombre mediante el cual los clientes "SMB" [214] hacen referencia a este recurso compartido.
  - Enable Access-based Enumeration (Activar enumeración basada en el acceso): opción mediante la cual se realiza una enumeración basada en el acceso, cuando está activada. La enumeración basada en el acceso filtra las entradas de directorio según las credenciales del cliente. Cuando el cliente no tiene acceso a un archivo o directorio, ese archivo no se incluye en la lista de entradas devueltas al cliente. Esta opción no está activada de forma predeterminada.

    No puede haber dos recursos compartidos "SMB" [214] en el mismo sistema que compartan el mismo nombre de recurso. Cuando los sistemas de archivos heredan nombres de recursos de un proyecto, el nombre de recurso del recurso compartido se crea conforme a estas reglas:
  - off (desactivado): los sistemas de archivos incluidos no se exportan mediante "SMB" [214].
  - on (activado): los sistemas de archivos incluidos se exportan mediante "SMB" [214] con el nombre del sistema de archivos como nombre de recurso.
  - Cualquier otro distinto de "off" u "on": para cada sistema de archivos, se crea un nombre de recurso con el formato *<nombre de recurso del proyecto>_<nombre del sistema de archivos>*.
- iSCSI: las propiedades de "iSCSI" [213] no se heredan.
- HTTP: las propiedades de los recursos compartidos de "HTTP" [234] se heredan normalmente y se describen en la "documentación de recursos compartidos" [336].
- FTP: las propiedades de los recursos compartidos de "FTP" [232] se heredan normalmente y se describen en la "documentación de recursos compartidos" [336].
- SFTP: las propiedades de los recursos compartidos de "SFTP" [246] se heredan normalmente y se describen en la "documentación de recursos compartidos" [336].
- NFS: las propiedades de los recursos compartidos de "NFS" [208] se heredan normalmente y se describen en la "documentación de recursos compartidos" [336].
- SMB
  - Resource name (Nombre de recurso): nombre mediante el cual los clientes "SMB" [214] hacen referencia a este recurso compartido.
  - Enable Access-based Enumeration (Activar enumeración basada en el acceso): opción mediante la cual se realiza una enumeración basada en el acceso, cuando

está activada. La enumeración basada en el acceso filtra las entradas de directorio según las credenciales del cliente. Cuando el cliente no tiene acceso a un archivo o directorio, ese archivo no se incluye en la lista de entradas devueltas al cliente. Esta opción no está activada de forma predeterminada.

No puede haber dos recursos compartidos "SMB" [214] en el mismo sistema que compartan el mismo nombre de recurso. Cuando los sistemas de archivos heredan nombres de recursos de un proyecto, el nombre de recurso del recurso compartido se crea conforme a estas reglas:

- Off (desactivado): los sistemas de archivos incluidos no se exportan mediante "SMB" [214].
- On (activado): los sistemas de archivos incluidos se exportan mediante "SMB" [214] con el nombre del sistema de archivos como nombre de recurso.
- Cualquier otro distinto de off u on: para cada sistema de archivos, se crea un nombre de recurso con el formato *<nombre de recurso del proyecto>_<nombre del sistema de archivos>*.

- iSCSI: las propiedades de "iSCSI" [213] no se heredan.

Acceso del proyecto

- Access Control (Control de acceso): esta vista proporciona control sobre las propiedades heredables que afectan el comportamiento de la "ACL" [344].
- Inherited ACL Behavior (Comportamiento de la ACL heredada): estas propiedades se comportan de la misma manera que en el nivel de recursos compartidos. El cambio de estas propiedades cambiará el comportamiento correspondiente de los sistemas de archivos que en la actualidad heredan las propiedades.
  - "ACL behavior on mode change" [344]
  - "ACL inheritance behavior" [344]

Instantáneas de proyecto

Las instantáneas son copias de sólo lectura de un sistema de archivos en un punto dado en el tiempo. Para obtener más información sobre las instantáneas y sobre cómo funcionan, consulte la página de "conceptos" [300]. Las instantáneas de los proyectos se componen de instantáneas de cada sistema de archivos y LUN del proyecto, todas con nombres idénticos. Los recursos compartidos pueden suprimir las instantáneas de manera individual y, si bien se admite la creación de una instantánea con el mismo nombre que la instantánea de un proyecto, esto podría provocar un comportamiento indefinido, ya que la instantánea se considerará parte de la instantánea del proyecto con el mismo nombre.

Propiedades de instantáneas de proyecto

.zfs/snapshot visible

Se puede 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. Este directorio contiene una lista de todas las instantáneas del sistema de archivos; se puede acceder a ellas del mismo modo que a los datos del sistema de archivos normal (en modo de sólo lectura). De forma predeterminada, el directorio '.zfs' no está visible en la lista de contenidos del directorio, pero se puede acceder a éste 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.

TABLA 12-25 Valores de instantánea de proyecto

Valor de la BUI	Valor de la CLI	Descripción
Hidden	hidden	El directorio .zfs no está visible al mostrar el contenido del directorio en la raíz del sistema de archivos. Éste es el valor predeterminado.
Visible	visible	El directorio .zfs aparece como cualquier otro directorio en el sistema de archivos.

Etiqueta de instantáneas programada

Esta propiedad opcional anexa 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 instantáneas pueden ayudar a identificar el proyecto o el recurso compartido para el cual se tomó una instantánea, por ejemplo, "project1:share1" puede indicar una instantánea programada tomada en share1 dentro de project1. Las etiquetas pueden tener hasta 35 caracteres alfanuméricos e incluir caracteres especiales _ - . :

Las instantáneas de nivel de proyecto se administran de la misma manera que las instantáneas de nivel de recurso compartido. Para obtener más información acerca de instantáneas, consulte “Recursos compartidos: Instantáneas” [352]

Las instantáneas del proyecto no admiten operaciones de reversión ni clonación. Para obtener más información acerca de instantáneas, consulte “Recursos compartidos: Instantáneas” [352]

Para acceder a las instantáneas de un proyecto, navegue hasta el proyecto y ejecute el comando `snapshots`.

```
clownfish:> shares select default
clownfish:shares default> snapshots
clownfish:shares default snapshots>
```

Desde este punto, las instantáneas se administran de la misma manera que las instantáneas de nivel de recurso compartido. Para obtener más información acerca de instantáneas, consulte “Recursos compartidos: Instantáneas” [352]

Las instantáneas del proyecto no admiten operaciones de reversión ni clonación. Para obtener más información acerca de instantáneas, consulte “Recursos compartidos: Instantáneas” [352]

Esquemas

Propiedades personalizadas de uso compartido

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.

Trabajo con esquemas en la BUI

Para definir propiedades personalizadas, ingrese al elemento de navegación Shares (Recursos compartidos) -> Schema (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 12-26 Campos de propiedades de esquemas

Campo	Descripción
NAME	El nombre de la CLI para esta propiedad. Debe contener sólo caracteres alfanuméricos o los caracteres ".:_\".
DESCRIPTION	El nombre de la BUI para esta propiedad. Puede contener caracteres arbitrarios y se utiliza en la sección de ayuda de la CLI.
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 los siguientes:

TABLA 12-27 Tipos válidos para las propiedades

Tipo de BUI	Tipo de CLI	Descripción
String	String	Datos de cadenas arbitrarias. Es el equivalente de la falta de validación.
Integer	Integer	Un número entero positivo o negativo.
Positive Integer	PositiveInteger	Un número entero positivo.
Boolean	Boolean	Un valor verdadero/falso. En la BUI esto se presenta como una casilla de verificación, mientras que en la CLI debe tener los valores "true" (verdadero) o "false" (falso).
Email Address	EmailAddress	Una dirección de correo electrónico. Sólo se realiza una validación sintáctica mínima.
Hostname or 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” [327], 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. Si a una propiedad se la elimina 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 es 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.

▼ Configuración de esquemas con la BUI

1. **Navegue hasta la vista Shares (Recursos compartidos) -> Schema (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" [contacto]).**
4. **Introduzca una descripción de la propiedad ("Owner Contact" [Contacto del propietario]).**

5. **Elija un tipo para la nueva propiedad ("Email Address" [Dirección de correo electrónico]).**
6. **Haga clic en el botón "Apply" (Aplicar).**
7. **Navegue hasta el proyecto o el recurso compartido existente.**
8. **Cambie la propiedad "Owner Contact" (Contacto del propietario) en la sección "Custom Properties" (Propiedades personalizadas).**

Trabajo con esquemas en la CLI

El contexto del esquema se encuentra en shares (recursos compartidos) -> schema (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 que se definen las propiedades personalizadas, se puede acceder a ellas como a cualquier otra propiedad con el nombre "custom:<propiedad>":

```
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
```

▼ Configuración de esquemas con la CLI

1. **Navegue 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. **Navegue hasta el proyecto o el recurso compartido existente.**
7. **Configure la propiedad "custom:contact".**

♦ ♦ ♦ CAPÍTULO 13

Replicación

AVISO DE LICENCIAS: *Las funciones de replicación remota y clonación se pueden evaluar sin cargo, pero para poder usarlas en producción se debe adquirir una licencia independiente por separado. Después del período de evaluación, se debe adquirir la licencia correspondiente para estas funciones o se las debe desactivar. Oracle se reserva el derecho de realizar auditorías en cualquier momento para controlar la existencia de las licencias necesarias. Para obtener información detallada, consulte "Acuerdo de licencia de software (SLA) de Oracle y derecho de sistemas de hardware con opciones de software integrado".*

Descripción general de la replicación

Los dispositivos Oracle ZFS Storage Appliance admiten la replicación basada en instantáneas de proyectos y recursos compartidos desde un dispositivo ZFSSA de origen hacia cualquier cantidad de dispositivos ZFSSA de destino de forma manual, programada o continua. La replicación comprende datos y metadatos. La replicación remota (o simplemente "replicación") es una función de finalidad general optimizada para los siguientes casos de uso:

- Recuperación en caso de desastre. La replicación se puede utilizar para reflejar un dispositivo ZFSSA en caso de recuperación ante desastres. En caso de un desastre que afecte el servicio del dispositivo ZFSSA principal (o incluso un centro de datos entero), los administradores activan el servicio en el sitio de recuperación ante desastres, que toma el control mediante los datos replicados más recientemente. Cuando se ha restaurado el sitio principal, los datos que se cambiaron mientras estaba en servicio el sitio de recuperación ante desastres se pueden migrar hacia el sitio principal, y se restaurará el servicio normal. Dichos casos se pueden probar por completo antes de que se produzca un desastre.
- Distribución de datos. La replicación se puede utilizar para distribuir datos (por ejemplo, medios o imágenes de máquinas virtuales) hacia sistemas remotos en todo el mundo, en situaciones donde los clientes del dispositivo ZFSSA de destino normalmente no podrían llegar directamente al dispositivo ZFSSA de origen, o donde dicha configuración podría resultar poco eficaz en cuanto a la alta latencia. Un ejemplo utiliza este esquema para el almacenamiento en la caché local para mejorar la latencia de los datos de sólo lectura (como los documentos).
- Copia de seguridad disco a disco. La replicación se puede utilizar como solución de copias de seguridad para entornos en donde no son factibles las copias de seguridad en cinta. Las

copias de seguridad en cinta no son factibles, por ejemplo, en casos donde el ancho de banda disponible es insuficiente o donde la latencia de recuperación es demasiado alta.

- Migración de datos. La replicación se puede utilizar para migrar datos y configuración entre dispositivos ZFSSA al actualizar el hardware o volver a equilibrar el almacenamiento. La migración shadow también se puede utilizar para esta finalidad.

La función de replicación remota tiene varias propiedades importantes:

- Basada en instantáneas. El subsistema de replicación toma una instantánea como parte de cada operación de actualización. Para una actualización completa, se envía el contenido de todo el proyecto hasta la instantánea. En el caso de una actualización incremental, sólo se envían los cambios desde la última instantánea de replicación para la misma acción.
- 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.
- Asíncrono. Dado que la replicación toma instantáneas y luego las envía, es necesario que los datos estén 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.
- Incluye metadatos. El flujo de replicación subyacente serializa los datos de usuario y los metadatos de ZFS, incluida la mayoría de las propiedades configuradas en la pantalla Shares (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. Consulte información detallada en “Gestión de paquetes de replicación ” [393].
- Protegido. El protocolo de control de replicación utilizado con los dispositivos ZFS Storage Appliance está protegido con SSL. De manera opcional, los datos también pueden estar protegidos con SSL. Los dispositivos sólo se pueden replicar hacia/desde otros dispositivos ZFSSA después del proceso de autenticación manual inicial; consulte “Creación y edición de destinos” [386].

La replicación tiene las siguientes limitaciones conocidas:

- Si se cambia la dirección IP del destino, se interrumpe la replicación
- No es posible mover acciones entre agrupaciones
- Las operaciones de E/S se limitan a un máximo de 200 MB/seg. por replicación de nivel de proyecto

Explicación de la replicación

Terminología de replicación

- Par de replicación (o simplemente par en este contexto): dispositivo ZFS Storage Appliance que se configuró como origen o destino de replicación.
- Origen de replicación (o simplemente origen): par (dispositivo ZFSSA) que contiene datos para replicar hacia otro par (dispositivo ZFSSA, el *destino*). Los dispositivos ZFSSA individuales pueden actuar como origen y destino, pero actuarán sólo como uno de ellos en el contexto de una *acción* de replicación en particular.
- Destino de replicación (o simplemente destino): par (dispositivo ZFSSA) que recibe y almacena datos replicados desde otro par (dispositivo ZFSSA, el *origen*). Este término también hace referencia a un objeto de configuración en el dispositivo ZFSSA que permite que este replique en otro dispositivo ZFSSA.
- Grupo de replicación (o simplemente grupo): el conjunto de conjuntos de datos (exactamente un proyecto y algunos recursos compartidos) replicados como unidad. Consulte “Replicación de nivel de proyecto frente a replicación de nivel de recurso compartido ” [385].
- Acción de replicación (o simplemente acción): objeto de configuración en un dispositivo ZFSSA de origen que especifica un proyecto o recurso compartido, un dispositivo ZFSSA de destino y opciones de políticas (incluso con qué frecuencia se deben enviar actualizaciones, si se deben cifrar datos en el cable, etc.).
- Paquete: elemento análogo del lado del destino de una acción; objeto de configuración en el dispositivo ZFSSA de destino que gestiona los datos replicados como parte de una acción en particular desde un origen en particular. Cada acción de un dispositivo ZFSSA de origen está asociada con un paquete, exactamente, en un dispositivo ZFSSA de destino y viceversa. En caso de pérdida de cualquiera de los objetos, se deberá crear un nuevo par de acción/paquete (y una actualización de replicación completa).
- Sincronización completa (o actualización completa): operación de replicación que envía todos los contenidos de un proyecto y algunos de sus recursos compartidos.
- Actualización incremental: operación de replicación que envía sólo las diferencias de un proyecto y sus recursos compartidos desde la actualización anterior (independientemente de si dicha actualización era completa o incremental).

Destinos de replicación de proyecto

Antes de poder replicar un dispositivo ZFSSA de origen a uno de destino, los dos sistemas deben configurar una conexión de pares de replicación que permita a los dispositivos ZFSSA identificarse entre sí de manera segura para las comunicaciones futuras. Para configurar esta conexión, los administradores crean un nuevo destino de replicación en la pantalla Configuration (Configuración) > Services (Servicios) > Remote Replication (Replicación

remota) del dispositivo ZFSSA de origen. Para crear un nuevo destino, los administradores especifican tres campos:

- Nombre (utilizado sólo para identificar el destino en la CLI y la BUI del dispositivo ZFSSA de origen)
- Nombre de host o dirección de red (para establecer contacto con el dispositivo ZFSSA de destino)
- Contraseña de usuario root del dispositivo ZFSSA de destino (para autorizar al administrador a configurar la conexión en el dispositivo ZFSSA de destino)

Luego, los dispositivos ZFSSA intercambian claves utilizadas para identificarse entre sí de manera segura en las comunicaciones posteriores. Estas claves se almacenan de manera continua como parte de la configuración del dispositivo ZFSSA y se conservan tras los reinicios y las actualizaciones. Se perderán en caso de que se produzca una reinstalación o restablecimiento de fábrica del dispositivo ZFSSA. La contraseña de usuario root nunca se almacena de manera continua; por lo tanto, no es necesario realizar cambios en la configuración de replicación si se cambia la contraseña de usuario root en alguno de los dispositivos ZFSSA. La contraseña nunca se transmite sin codificar porque este intercambio de identidad inicial (como todas las operaciones de control de replicación) está protegido con SSL.

De forma predeterminada, la conexión del destino de replicación no es bidireccional. Si un administrador configura la replicación desde el origen A hacia el destino B, entonces B no podrá utilizar A automáticamente como destino. Sin embargo, el sistema admite la reversión de la dirección de la replicación, que crea automáticamente un destino para A en B (si es que ya no existe) de manera que B se pueda replicar hacia A.

NOTA: Cuando un origen de replicación usa los servicios NIS o LDAP para asignar usuarios o grupos de usuarios que están incluidos en una configuración de recursos compartidos en el origen (por ejemplo. en 'Share Level ACL' [ACL de nivel de recurso compartido] o 'Share Space Usage' [Uso de espacio de recursos compartidos]), esos usuarios o grupos de usuarios deben estar disponibles en el destino de replicación (por ejemplo, se deben usar los mismos servidores NIS o LDAP) porque de lo contrario se pueden producir errores en las operaciones de servidor y reversión de la replicación.

Para configurar destinos de replicación, consulte “Configuración de replicación de proyectos ” [386].

Acciones y paquetes de replicación de proyectos

Los destinos representan una conexión entre dispositivos ZFSSA que les permite comunicarse de manera segura para la replicación; sin embargo, los destinos no especifican lo que se replicará, la frecuencia ni las opciones. Para ello, los administradores deben definir las *acciones* de replicación en el dispositivo ZFSSA de origen. Las acciones constituyen el punto de control administrativo principal para la replicación; cada una especifica:

- un grupo de replicación (un proyecto y una cantidad de recursos compartidos)

- ZFSSA de destino
- agrupación de almacenamiento en el dispositivo ZFSSA de destino (usada únicamente durante la instalación inicial)
- una frecuencia (que puede ser manual, programada o continua)
- opciones adicionales, por ejemplo, si se debe cifrar el flujo de datos en el cable

El grupo es especificado de manera implícita por el proyecto o recurso compartido en donde se configura la acción (consulte “Replicación de nivel de proyecto frente a replicación de nivel de recurso compartido ” [385]). La agrupación de almacenamiento y el dispositivo ZFSSA de destino no se pueden cambiar después de crear la acción; sin embargo, las otras acciones se pueden modificar en cualquier momento. En general, si la actualización de replicación está en curso cuando se cambia una opción, el nuevo valor sólo tendrá efecto cuando comience la siguiente actualización.

Las acciones son la unidad principal de la configuración de replicación del dispositivo ZFSSA. Cada acción corresponde a un *paquete* en el dispositivo ZFSSA de destino que 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. Los administradores configuran la frecuencia y otras opciones de actualizaciones de replicación mediante la modificación de propiedades de la acción correspondiente. La creación de la acción en el dispositivo ZFSSA de origen crea el paquete en el dispositivo ZFSSA de destino, en la agrupación de almacenamiento especificada; por lo tanto, el origen debe poder comunicarse con el destino cuando se crea inicialmente la acción.

La primera actualización de cada acción de replicación envía una *sincronización completa* (o *actualización completa*): todos los contenidos de los recursos compartidos y el proyecto de la acción se envían al dispositivo ZFSSA de destino. Una vez que finaliza la sincronización inicial, las actualizaciones de replicaciones posteriores son *incrementales*: sólo se envían los cambios desde la actualización anterior. La acción (en el origen) y el paquete (en el destino) realizan un seguimiento de los cambios que se han replicado al destino mediante instantáneas de replicación con nombre. En general, siempre que se haya enviado al menos una sincronización completa para acción y la conexión de acción/paquete no esté dañada debido a un fallo de software o una acción administrativa, las actualizaciones de replicación serán incrementales.

La acción y el paquete están vinculados entre sí. Si el paquete se daña o se destruye de alguna manera, la acción no podrá 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). La BUI y la CLI advierten a los administradores que intentan realizar operaciones que pueden destruir la conexión entre la acción y el paquete. 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, los administradores deben cortar o destruir el paquete y la acción, y generar una nueva acción en el origen.

NOTA: El dispositivo ZFSSA evita la destrucción de datos en el destino, a menos que el administrador lo solicite explícitamente. 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 ZFSSA no podrá sobrescribir los datos antes recibidos. Para resolver esta situación, los administradores deben destruir el paquete y la acción existentes, crear un nuevo paquete y una nueva acción e iniciar nuevamente la replicación.

En las versiones de software anteriores a 2010.Q1, la configuración de la acción y la réplica (como la configuración de destino) se almacenaba en el controlador en lugar de formar parte de la configuración del proyecto y el recurso compartido en la agrupación de almacenamiento. Como resultado, el restablecimiento de fábrica destruía la configuración. En 2010.Q1 y versiones posteriores, la configuración de la acción y el paquete se almacena en la agrupación de almacenamiento con los proyectos y recursos compartidos correspondientes y, por lo tanto, está disponible incluso después del restablecimiento de fábrica. Sin embargo, se perderá la información de destino, y las acciones con destinos faltantes no se podrán configurar para apuntar hacia un nuevo destino.

Agrupaciones de almacenamiento de replicación de proyectos

Cuando la acción 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 creación de la acción crea un paquete vacío en el destino en la agrupación de almacenamiento especificada y, después de esta operación, el origen no tendrá información 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 nodo principal propietario de la dirección IP utilizada por el origen de la replicación porque sólo 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 (NFS y 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 forma de mover los paquetes entre agrupaciones de almacenamiento.

Replicación de nivel de proyecto frente a replicación de nivel de recurso compartido

El dispositivo ZFSSA permite a los administradores configurar la replicación remota en el nivel de proyecto y en el nivel de recurso compartido. Al igual que otras propiedades configurables en la pantalla Shares (Recursos compartidos), cada recurso compartido puede heredar o sustituir la configuración de su proyecto principal. Heredar la configuración no sólo 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 sólo 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 que tenemos lo siguiente:

- un proyecto `home` y recursos compartidos `bill`, `cindi` y `dave`
- `home` tiene una replicación configurada con una determinada cantidad 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 una determinada cantidad 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`

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 las secciones “Gestión de paquetes de replicación ” [393] y “ Replicación de clones ” [415].

Configuración de replicación de proyectos

Asegúrese de leer y comprender las secciones anteriores relacionadas con paquetes, acciones y destinos de replicación antes de configurar la replicación.

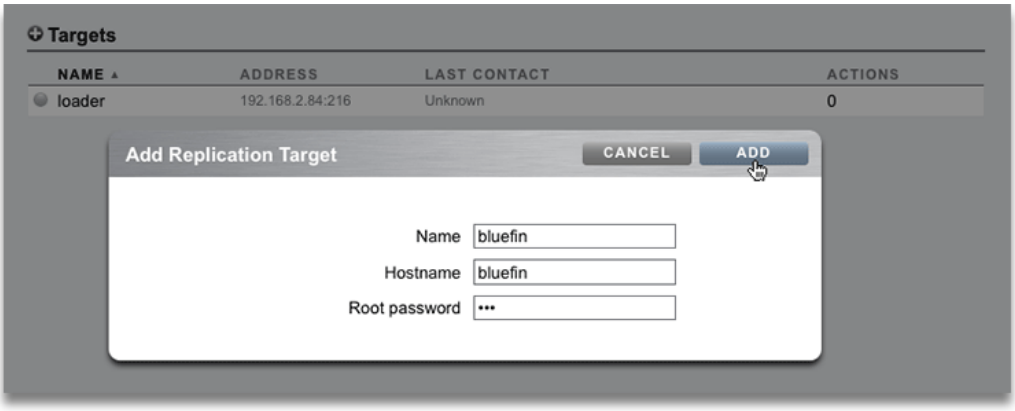
Creación y edición de destinos

En esta sección se describe la creación y la edición de destinos.

▼ Creación y edición de destinos en la BUI

1. **Para crear destinos de replicación remota en la BUI, vaya a Configuration (Configuración) > Services (Servicios) > Remote Replication (Replicación remota) > Targets (Destinos). Haga clic en  Targets (Destinos) y configure los valores de Name (Nombre), Hostname (Nombre de host) y Password (Contraseña).**

2. **Para editar destinos de replicación remota en la BUI, vaya a Configuration (Configuración) > Services (Servicios) > Remote Replication (Replicación remota) > Targets (Destinos). Para el destino que desea editar, mueva el cursor sobre el nombre del destino, haga clic en el ícono de lápiz y configure el valor de Name (Nombre) o Hostname (Nombre de host). El nombre de host debe indicar el mismo dispositivo ZFSSA que antes (verificado mediante el número de serie del dispositivo). Si desea indicar un dispositivo ZFSSA diferente al que se configuró antes, debe crear un nuevo destino para autenticarlo con el nuevo dispositivo ZFSSA.**



▼ Creación y edición de destinos en la CLI

1. **En la CLI, navegue hacia el nodo `targets` para configurar o anular la configuración del destino `hostname`, `root_password` y `label`.**

```
knife:> configuration services replication targets
```

2. **Desde este contexto, los administradores pueden:**

   - Agregar nuevos destinos
   - Ver las acciones configuradas con el destino existente
   - Editar el identificador único (etiqueta) o nombre de host para el destino
   - Destruir un destino, si ninguna acción lo está utilizando

3. **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 esto, pero no puede garantizar que no existen acciones en las agrupaciones de almacenamiento exportadas que utilizan un destino dado.**

Creación y edición de acciones

Las acciones de replicación tienen las siguientes propiedades, que se presentan ligeramente diferentes en la BUI y la CLI:

FIGURA 13-1 Agregación de acción de replicación

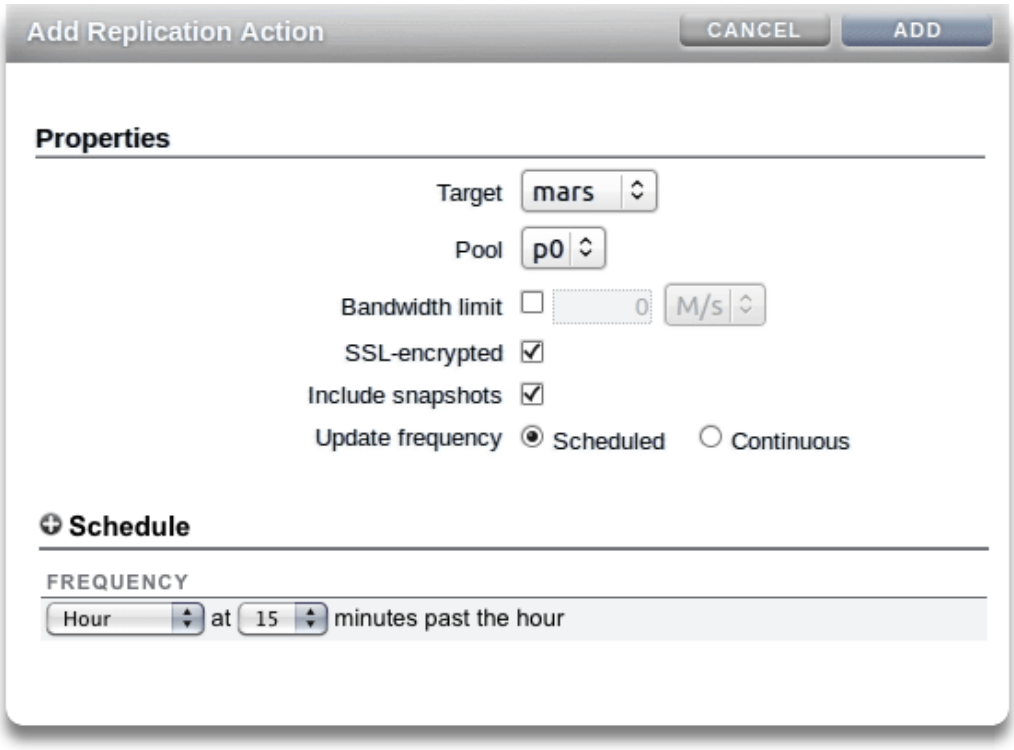


TABLA 13-1 Propiedades de la CLI para la acción de replicación

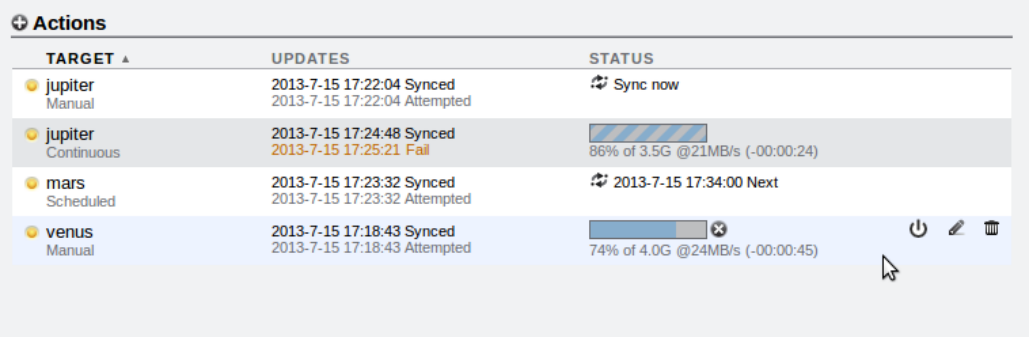
Propiedad (nombre de la CLI)	Descripción
Target	Identificador único del sistema de destino de replicación. Esta propiedad se especifica cuando se configura inicialmente una acción y se mantiene inmutable en lo sucesivo.
Pool	Agrupación de almacenamiento en el destino donde se replicará este proyecto. Esta propiedad se especifica cuando se configura inicialmente una acción y no se muestra en lo sucesivo.
Mode (CLI: continuous) and schedule	Indica si la acción se replica continuamente o en intervalos manuales o programados. Consulte “Modos de replicación: programados o continuos ” [392] para obtener información detallada.
Include Snapshots	Indica si las actualizaciones de replicación incluyen instantáneas de no replicación. Consulte “Replicación:

Propiedad (nombre de la CLI)	Descripción
	inclusión de las instantáneas intermedias ” [392] para obtener información detallada.
Limit bandwidth	Especifica una velocidad máxima para esta actualización de replicación (en términos de cantidad de datos transferidos por la red por segundo). Los cambios que se hagan a esta propiedad durante una actualización de replicación entran en efecto en la siguiente actualización.
Bytes sent	Propiedad de sólo lectura que describe la cantidad de bytes enviados al destino.
Estimated size	Propiedad de sólo lectura que describe el tamaño estimado de los datos que se replicarán.
Estimated time left	Propiedad de sólo lectura que describe el tiempo restante estimado hasta la finalización.
Average throughput	Propiedad de sólo lectura que describe el rendimiento promedio de la replicación.
Use SSL	Indica si se deben cifrar datos en el cable mediante SSL. El uso de esta función puede tener un impacto significativo sobre el rendimiento de la replicación por acción.
State	Propiedad de sólo lectura que describe si la acción está actualmente inactiva, está enviando una actualización o está cancelando una actualización.
Last sync	Propiedad de sólo lectura que describe la última vez que se envió con éxito una actualización. Este valor puede ser desconocido si el sistema no ha enviado una actualización exitosa desde el inicio.
Last attempt	Propiedad de sólo lectura que describe la última vez que se intentó realizar una actualización. Este valor puede ser desconocido si el sistema no ha intentado enviar una actualización desde el inicio.
Next update	Propiedad de sólo lectura que describe cuándo se realizará el siguiente intento. Este valor podría ser una fecha (para una actualización programada), "manual" o "continua".

▼ Creación y edición de acciones en la BUI

1. **Después de configurar al menos un destino de replicación, los administradores pueden configurar acciones en un recurso compartido o proyecto local; para ello, deben navegar hacia éste en la BUI y hacer clic en la ficha Replication (Replicación) o navegar hacia éste en la CLI y seleccionar el nodo "replication". Estas interfaces muestran el estado de las acciones existentes configuradas**

en el proyecto o el recurso compartido e información sobre el progreso de la replicación, y permiten a los administradores crear nuevas acciones:



2. **Al realizar una replicación a un destino, se muestran dos filas de información de estado. La primera fila muestra el nombre del destino, la fecha y hora de la última sincronización exitosa y una barra de progreso, o una barra de progreso a rayas si la replicación es continua. La segunda fila muestra el tipo de replicación (programada, manual o continua), la fecha y hora del último intento de sincronización o de la última sincronización fallida y detalles de estado. Para las replicaciones en curso, los detalles de estado incluyen el porcentaje de finalización, el tamaño estimado de los datos que se replicarán, el rendimiento promedio de la replicación y el tiempo estimado hasta la finalización. Cuando la replicación no está en curso, la columna Estado muestra la próxima replicación programada o el mensaje "Sync now" (Sincronizar ahora), según corresponda para el tipo de replicación.**

▼ Creación y edición de acciones en la CLI

1. **En la CLI, se puede visualizar la misma información de progreso y se muestra el estado `sending` para una replicación en curso:**

```
otoro:shares otoro-proj-01 action-000> show
Properties:
                    id = 80a96f4f-93fe-4abd-eb54-fb82e7f8c69f
                target = chutoro
            continuous = false
         include_snaps = true
         max_bandwidth = unlimited
            bytes_sent = 505M
        estimated_size = 3.0G
  estimated_time_left = 00:00:41
   average_throughput = 63MB/s
```

```
            use_ssl = false
              state = sending
    state_description = Sending update
          next_update = Sync now
            last_sync = Sun Jul 14 2013 06:04:38 GMT+0000 (UTC)
             last_try = Sun Jul 14 2013 06:04:38 GMT+0000 (UTC)
          last_result = success
```

2. **Nota: La replicación puede demorar mucho tiempo en completarse, según el tamaño de los datos que se están replicando. Use la información de progreso para determinar el estado de la actualización. Es importante no interrumpir la replicación inicial, por ejemplo, no reiniciar el dispositivo ZFSSA ni cancelar la actualización; de lo contrario, se deberá reiniciar toda la replicación inicial.**

3. **La información del destino de replicación se puede mostrar en la CLI con el estado `actions`:**

```
otoro:configuration services replication targets> show

Targets:
     TARGET        LABEL            ACTIONS
     target-000    oakmeal          1

otoro:configuration services replication targets> select target-000

otoro:configuration services replication target-000> show
Properties:
               address = 10.153.34.167:216
                 label = oakmeal
              hostname = oakmeal-7320-167
                   asn = 4913649f-7549-6d2a-866b-987ddbc4e163
               actions = 1

oakmeal-7320-167:configuration services replication target-000> actions
     POOL          PROJECT          SHARE
     pool1         project1         (multiple)
```

4. **Al usar la CLI, puede resultar útil saber el identificador de la nueva acción de replicación. El identificador se usa más adelante para seleccionar el nodo de acción de replicación correcto. Para ver el identificador de la nueva acción, use el comando `last` para navegar hasta el nodo de la nueva acción de replicación. A continuación, use el comando `get id` para recuperar el identificador de la acción:**

```
otoro:> shares
otoro:shares> select p1
otoro:shares p1> replication
otoro:shares p1 replication> create
otoro:shares p1 action (uncommitted)> set target=oakmeal
                       target = oakmeal (uncommitted)
otoro:shares p1 action (uncommitted)> set pool=p
                         pool = p (uncommitted)
```

```
otoro:shares p1 action (uncommitted)> set use_ssl=false
                      use_ssl = false (uncommitted)
otoro:shares p1 action (uncommitted)> commit
otoro:shares p1 replication> last
otoro:shares p1 action-001> get id
                           id = fb1bb3fd-3361-42e1-e4a1-b06c426172fb
otoro:shares p1 action-001> done
otoro:shares p1 replication>
```

Modos de replicación: programados o continuos

Las acciones de replicación se pueden configurar para enviar actualizaciones de forma manual, programada o continua. El proceso de actualización de replicación en sí mismo es igual en ambos casos. Esta propiedad sólo controla el intervalo.

Debido a que las acciones de replicación continua envían actualizaciones con la mayor frecuencia posible, se envía 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 los realmente necesarios. 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.

La replicación continua sigue siendo asíncrona. En la actualidad, los dispositivos ZFS Storage Appliance no admiten la replicación síncrona, la cual no considera los datos confirmados en el almacenamiento estable hasta que estén confirmados en el almacenamiento estable de los sistemas de almacenamiento principales y secundarios.

Replicación: inclusión de las instantáneas intermedias

Cuando la propiedad "Include Snapshots" (Incluir instantáneas) es verdadera, 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). Ello incluye instantáneas automáticas e instantáneas creadas por el administrador. Esta propiedad se puede desactivar para omitir estas instantáneas y enviar sólo los cambios ocurridos entre las instantáneas de replicación con cada actualización.

Replicación: envío y cancelación de actualizaciones

En el caso de destinos configurados con replicación manual o programada, los administradores pueden enviar de inmediato una actualización de replicación; para ello, deben hacer clic en

el botón  en la BUI o utilizar el comando `sendupdate` en la CLI. Esta función no está disponible (o no funcionará) si en la actualidad se está enviando una actualización en forma activa. Asegúrese de tener espacio en disco suficiente en el destino para replicar todo el proyecto antes de enviar una actualización.

Si la actualización está actualmente activa, la BUI mostrará una barra de progreso y la CLI mostrará el estado `sending`. Para cancelar la actualización, haga clic en el botón  o utilice el comando `cancelupdate`. Esto puede demorar varios segundos antes de finalizar la cancelación.

Gestión de paquetes de replicación

Los paquetes son contenedores de los recursos compartidos y los proyectos replicados. Cada acción de replicación en un dispositivo ZFSSA de origen corresponde a un paquete en el dispositivo ZFSSA de destino, como se describe más arriba. La BUI y la CLI permiten a los administradores explorar propiedades, instantáneas, recursos compartidos y proyectos replicados de manera similar a los recursos compartidos y proyectos locales. Sin embargo, debido a que los recursos compartidos replicados deben coincidir exactamente con sus contrapartes en el dispositivo ZFSSA de origen, no se permite realizar diversas operaciones de gestión dentro de los paquetes de replicación, entre ellos, la creación, la destrucción y el cambio de nombre de proyectos y recursos compartidos, la creación y el cambio de nombre de instantáneas, y la modificación de la mayoría de las propiedades de proyectos y recursos compartidos. Las instantáneas diferentes a aquellas utilizadas como base de la replicación incremental se pueden destruir en paquetes de replicación. No recomendamos esta práctica, pero se puede utilizar cuando fuera necesario tener espacio libre adicional.

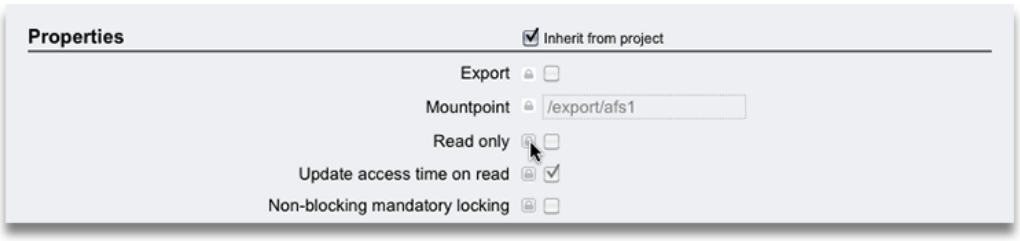
En la versión de software 2009.Q3 y versiones anteriores, no se podían cambiar las propiedades en recursos compartidos replicados. La versión 2010.Q1 (con las actualizaciones diferidas asociadas) agrega compatibilidad limitada para la modificación de propiedades de recursos compartidos replicados a fin de implementar políticas diferentes en los dispositivos ZFSSA de origen y destino. Estas modificaciones de propiedades persisten en las actualizaciones de replicaciones. Sólo se pueden modificar las siguientes propiedades de recursos compartidos y proyectos replicados:

- Reserva, compresión, copias, anulación de duplicación 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 dispositivo ZFSSA de destino desde el origen.
- Propiedades de punto de montaje y uso compartido (por ejemplo, sharenfs, nombre de recurso SMB, etc.). Estas propiedades controlan de qué manera se exportan los recursos compartidos a los clientes NAS y cómo se pueden cambiar para afectar diferentes políticas de protección o seguridad en el dispositivo ZFSSA de destino desde el origen.
- Políticas de instantáneas automáticas. Las políticas de instantáneas automáticas se pueden cambiar en el sistema de destino, pero estos cambios no tendrán efecto hasta cortar el

paquete. Las instantáneas automáticas no se toman ni se destruyen en recursos compartidos y proyectos replicados.

La BUI y la CLI no permiten a los administradores cambiar propiedades inmutables. En el caso de los recursos compartidos, se utiliza un ícono diferente para indicar que la herencia de la propiedad no se puede cambiar:

FIGURA 13-2 Gestión de propiedades de paquetes de replicación



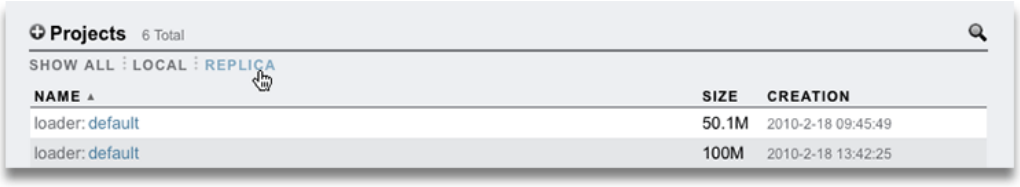
Las actualizaciones diferidas proporcionadas con la versión 2010.Q1 se deben aplicar en los destinos de replicación para modificar las propiedades de esos destinos. El sistema no permitirá a los administradores modificar las propiedades dentro de los paquetes de replicación en sistemas que no hayan aplicado las actualizaciones diferidas de la versión 2010.Q1.

La versión actual no admite la configuración de la replicación "en cadena" (es decir, la replicación de recursos compartidos replicados en otro dispositivo ZFSSA).

Gestión de paquetes de replicación en la BUI

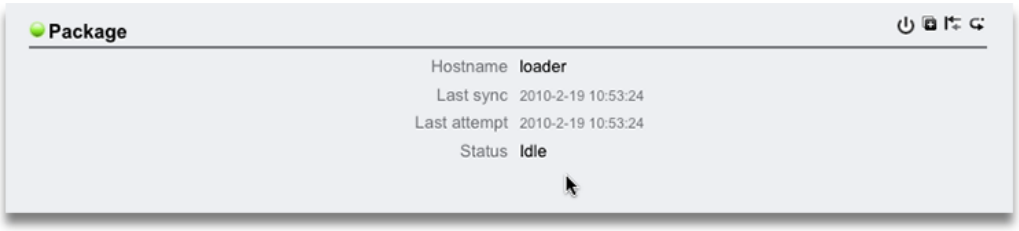
Los paquetes de replicación se muestran en la BUI como proyectos con el filtro "Replica" (Réplica):

FIGURA 13-3 Filtro Replica (Réplica)



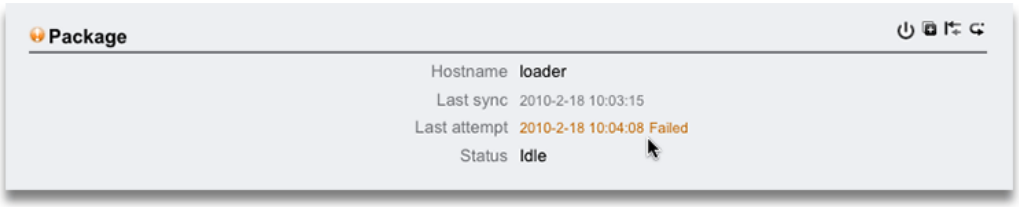
La selección de un paquete de replicación para edición lleva al administrador a la vista Shares (Recursos compartidos) correspondiente al proyecto del paquete. Desde aquí, los administradores pueden gestionar los recursos compartidos replicados de manera similar a los recursos compartidos locales con las excepciones descritas anteriormente. Las propiedades de los paquetes (incluido el estado) se pueden modificar en la ficha Replicación:

FIGURA 13-4 Vista de recursos compartidos del proyecto del paquete



El ícono de estado a la izquierda cambia cuando se ha producido un fallo en la replicación:

FIGURA 13-5 El ícono de estado indica error



Los paquetes sólo se muestran en la BUI 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.

Gestión de paquetes de replicación en la CLI

Los paquetes de replicación están organizados en la CLI por origen en `shares replication sources`. Los administradores primero deben seleccionar un origen y, luego, un paquete. Las operaciones de nivel de paquete se pueden llevar a cabo en este nodo o se puede seleccionar

el proyecto para gestionar recursos compartidos y propiedades del proyecto al igual que los recursos compartidos y proyectos locales, con las excepciones descritas anteriormente. Por ejemplo:

```
loader:> shares replication sources
loader:shares replication sources> show
Sources:

source-000 ayu
            PROJECT    STATE       LAST UPDATE
package-000 oldproj    idle        unknown
package-001 aproj1     receiving   Sun Feb 21 2010 22:04:35 GMT+0000 (UTC)

loader:shares replication sources> select source-000
loader:shares replication source-000> select package-001
loader:shares replication source-000 package-001> show
Properties:
                     enabled = true
                       state = receiving
            state_description = Receiving update
                    last_sync = Sun Feb 21 2010 22:04:40 GMT+0000 (UTC)
                     last_try = Sun Feb 21 2010 22:04:40 GMT+0000 (UTC)

Projects:
                      aproj1

loader:shares replication source-000 package-001> select aproj1
loader:shares replication source-000 package-001 aproj1> get mountpoint
                    mountpoint = /export
loader:shares replication source-000 package-001 aproj1> get sharenfs
                     sharenfs = on
```

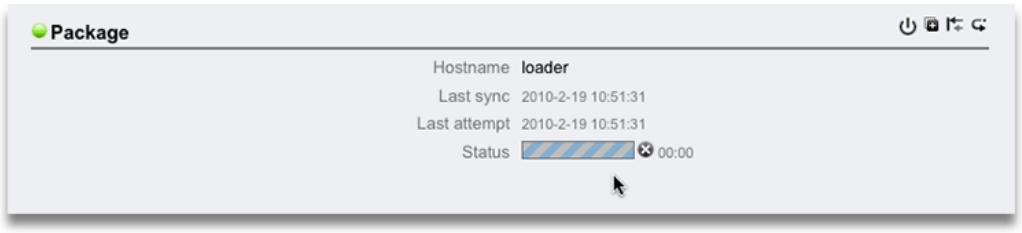
También puede visualizar orígenes de replicación desde `replicación de servicios de configuración`. Por ejemplo:

```
loader:configuration services replication> show
Properties:
                    <status> = online
Children:
                        targets => Configure replication targets
                        sources => View and manage replication packages
```

Cancelación de actualizaciones de replicación

Para cancelar las actualizaciones de replicación en curso en el destino con la BUI, navegue hasta el paquete de replicación (consulte la información que se muestra arriba) y, luego, haga clic en la ficha Replicación. Si hay una actualización en curso, verá una barra de progreso a rayas con un botón para cancelar () junto a dicha barra tal como se muestra a continuación:

FIGURA 13-6 Cancelación de replicación



Haga clic en este botón para cancelar la actualización.

Para cancelar las actualizaciones de replicación en progreso en el destino con la CLI, navegue hasta el paquete de replicación (consulte la información que se muestra arriba) y, luego, utilice el comando `cancelupdate`.

No es posible iniciar actualizaciones desde el destino. Los administradores deben iniciar sesión en el sistema de origen para iniciar una actualización manual.

Desactivación de un paquete

En el caso de las actualizaciones de replicación de un paquete, es posible desactivarlas completamente, cancelar cualquier actualización en curso y anular todas las nuevas actualizaciones del dispositivo ZFSSA de origen.

Para alternar entre la desactivación de un paquete desde la BUI, navegue hasta el paquete (consulte la información que se muestra arriba), luego, haga clic en la ficha Replication (Replicación) y, luego, haga clic en el ícono . El ícono de estado de la izquierda debería cambiar para indicar el estado del paquete (activado, desactivado o con errores). El paquete seguirá desactivado hasta que el administrador lo active explícitamente con el mismo botón o mediante la CLI.

Para alternar entre la desactivación de un paquete de la CLI, navegue hasta el paquete (consulte la información que se muestra arriba), modifique la propiedad `enabled` y confirme los cambios.

Clonación de un paquete o recursos compartidos individuales

Un *clon* de un paquete replicado es un proyecto local y mutable que puede ser gestionado como cualquier otro proyecto en el sistema. Los recursos compartidos del clon son clones de los

recursos compartidos replicados en la instantánea recibida más recientemente. Estos clones comparten el almacenamiento con las instantáneas de origen de la misma manera que los clones de las instantáneas de recursos compartidos (consulte “Clonación de una instantánea” [352]). 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.

Utilice el botón  en la BUI o el comando de la CLI `clone` (en el contexto del paquete) para crear un clon de paquete basado en la instantánea de replicación recibida más recientemente. En la interfaz de la CLI y la BUI, el administrador debe especificar un nombre para el proyecto del clon nuevo y debe permitir al administrador sustituir el punto de montaje del proyecto o sus recursos compartidos para asegurarse de que no entren en conflicto con otros recursos compartidos del sistema.

En la versión 2009.Q3 y anteriores, la clonación de un proyecto replicado era la única manera de acceder a los datos y, por consiguiente, la única manera de implementar el failover de la recuperación ante desastres. En la versión 2010.Q1 y posteriores, los sistemas de archivos individuales se pueden exportar como sólo lectura sin crear un clon. Además, los paquetes de replicación se pueden convertir directamente en proyectos locales modificables como parte de la operación de failover. Como resultado, la clonación de un paquete ya no será necesaria ni recomendada, ya que estas alternativas ofrecen una funcionalidad similar con operaciones más simples y sin necesidad de gestionar clones y sus dependencias.

En particular, 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 por 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 tiene clones, se cambiará el nombre a dicha instantánea con un nombre único (normalmente, `recv-XXX`).

Los administradores también pueden clonar instantáneas de recursos compartidos replicados individuales mediante las interfaces de la CLI y la BUI normal.

Exportación de sistemas de archivos replicados

Los sistemas de archivos replicados se pueden exportar en formato de sólo 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 ZFSSA de origen).

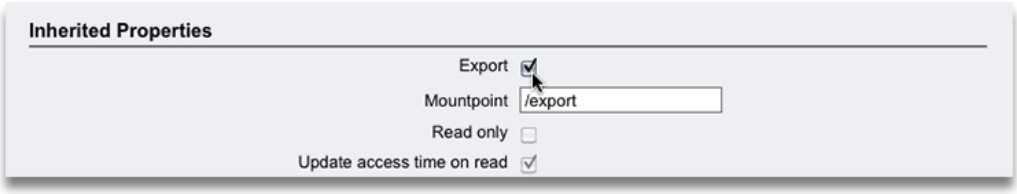
El contenido del sistema de archivos siempre coincide con la instantánea de replicación recibida más recientemente para ese sistema de archivos. Es posible que sea más nueva que la instantánea recibida más recientemente para todo el paquete, y que no coincida con la

instantánea más reciente para otros recursos compartidos del mismo paquete. Para obtener más información, consulte “ Instantáneas y coherencia de datos ” [413].

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 interfaz de usuario basada en explorador (BUI) o la interfaz de línea de comandos (CLI):

FIGURA 13-7 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.

Corte de replicación

Un paquete de replicación se puede convertir en un proyecto local modificable 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 replicación. Después de esta operación, el paquete ya no puede recibir actualizaciones de replicación. Por lo tanto, las actualizaciones de replicación posteriores del mismo proyecto desde el origen necesitarán enviar una actualización completa con una nueva acción (en un nuevo paquete). Las actualizaciones de replicación posteriores que utilicen la misma acción presentarán errores porque el paquete correspondiente ya no existe en el destino.

Esta opción es principalmente útil cuando se utiliza la replicación para migrar datos entre dispositivos ZFSSA o en otros casos que no impliquen replicar los datos recibidos nuevamente en el origen como parte de un plan típico de recuperación ante desastres de dos sistemas.

Para cortar la replicación desde la BUI, se debe navegar hasta el paquete de replicación (ver más arriba) y, a continuación, hacer clic en la ficha Replication (Replicación) y en el botón  . El cuadro de diálogo que aparece permite que el administrador especifique el nombre del nuevo proyecto local.

Para cortar la replicación desde la CLI, se debe navegar hasta el paquete de replicación (ver más arriba) y, a continuación, utilizar el comando `sever`. Este comando toma un argumento opcional que especifica el nombre del nuevo proyecto local. Si no se especifica ningún argumento, se utiliza el nombre original.

Dado que se exportan todos los recursos compartidos locales, todos los recursos compartidos del paquete se exportan cuando se corta el paquete, independientemente de que se hayan exportado previamente (ver más arriba). 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 corte. Estos conflictos se deben resolver antes de realizar el corte mediante la reconfiguración los puntos de montaje de los recursos compartidos correspondientes.

Reversión de la dirección de la replicación

Se puede invertir la dirección de la replicación para admitir los planes típicos de recuperación ante desastres de dos sistemas. Esta operación es similar a la operación de corte descrita anteriormente, pero, además, configura una acción de replicación en el nuevo proyecto local para realizar una replicación incremental en el sistema de origen. No se efectúan cambios en el sistema de origen cuando se completa esta operación, sino que el primer intento de actualización con esta acción convertirá el proyecto original del sistema de origen en un paquete de replicación y revertirá los cambios efectuados desde la última actualización de replicación exitosa de ese sistema.

Esta función no redirige automáticamente cargas de trabajo de producción ni direcciones IP de failover, ni realiza otras actividades relacionadas con el failover de la recuperación ante desastres, aparte de modificar el estado de lectura y escritura de las copias de datos principales y secundarios.

Como parte de la conversión del proyecto de origen original en un paquete de replicación en el sistema 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 revirtiendo 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.

Después de establecer la replicación de nivel de recurso compartido de un dispositivo ZFSSA a otro, la reversión de esa replicación en el dispositivo ZFSSA de destino destruye el cronograma de replicación. Luego, se crea una acción de replicación en el nivel de proyecto, que contiene el dispositivo ZFSSA de destino correcto sin un cronograma.

Como mencionamos anteriormente, esta característica generalmente se utiliza para implementar una configuración de recuperación ante desastres de dos sistemas, en la cual un sistema *principal* proporciona datos de producción y los replica a un sistema *secundario* o *DR* (por lo general, en otro centro de datos) en espera para tomar el control del tráfico de producción en caso de que se produzca un desastre en el sitio principal. Si se produce un desastre en el sitio principal, la copia del sitio secundario se debe convertir en "principal" y, para ello, se debe convertir en modificable y el tráfico de producción se debe redirigir al sitio secundario. Cuando se repara el sitio principal, los cambios acumulados en el sitio secundario se pueden replicar nuevamente en el sitio principal y ese sitio puede reanudar el mantenimiento de la carga de trabajo de producción.

A continuación, se describe una secuencia típica de eventos con ese plan:

- El sistema principal abastece la carga de trabajo de producción y se ocupa de la replicación al sistema secundario.
- Se produce un desastre, que posiblemente representa una falla total del sistema en el sitio principal. Los administradores revierten la dirección de la replicación en el sitio secundario; para ello, exportan los recursos compartidos replicados de un nuevo proyecto configurado para realizar la replicación nuevamente en el sitio principal cuando se restaure dicho servicio principal. Mientras tanto, la carga de trabajo de producción se redirige al sitio secundario.
- Cuando el sitio principal vuelve a estar en línea, el administrador inicia una actualización de replicación desde el sitio secundario hacia el sitio principal. Esto permite convertir la copia del sitio principal en un paquete de replicación, lo cual revierte los cambios realizados desde la última actualización exitosa del destino (antes de la falla). Cuando la copia del sitio principal está actualizada, la dirección de la replicación se revierte nuevamente, lo que convierte la copia del sitio principal en modificable. El tráfico de producción se redirige nuevamente al sitio principal. Se reanuda la replicación del sitio principal al secundario, lo cual restaura la relación inicial entre las copias principal y secundaria.

Para revertir la dirección de la replicación de un paquete, se recomienda a los administradores que, antes de hacerlo, detengan la replicación de ese proyecto desde el 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 dispositivo ZFSSA de destino anterior (que ahora es el dispositivo ZFSSA de origen).

Para revertir la replicación desde la BUI, se debe navegar hasta el paquete de replicación (ver más arriba) y, a continuación, hacer clic en la ficha Replication (Replicación) y en el botón  . El cuadro de diálogo que aparece permite que el administrador especifique el nombre del nuevo proyecto local.

Para revertir la replicación desde la CLI, se debe navegar hasta el paquete de replicación (ver más arriba) y, a continuación, utilizar el comando `reverse`. Este comando toma un argumento opcional que especifica el nombre del nuevo proyecto local. Si no se especifica ningún argumento, se utiliza el nombre original.

Dado que se exportan todos los recursos compartidos locales, todos los recursos compartidos del paquete se exportan cuando se revierte el paquete, independientemente de que se hayan exportado previamente (ver más arriba). 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 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.

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, mediante el comando de destrucción del nodo `shares replication sources`.

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.

Tareas de replicación

Las siguientes tareas constituyen ejemplos de los procedimientos de replicación.

Reversión de la replicación: establecimiento de la replicación

A continuación, se muestra un ejemplo de reversión de la replicación para admitir una recuperación ante desastres típica de dos sistemas. En este ejemplo, M11 es el sistema de producción y M5 es el sistema de recuperación.

Replicación inversa

1. **En el sistema de producción M11, navegue hasta Configuration (Configuración) > Services (Servicios).**
2. **En la línea SMB debajo de Data Services (Servicio de datos), si el estado es Disabled (Desactivado), haga clic en Enable service (Activar servicio).**
3. **Navegue hasta Configuration (Configuración) > Services (Servicios) > Remote Replication (Replicación remota).**
4. **Haga clic en Targets (Destinos) y configure los valores de nombre, nombre de host y contraseña. Name=M5, Host name=192.168.1.17, Root password=pppp $1234.**
5. **Seleccione Pool=Pool1.**
6. **Navegue hasta Shares (Recursos compartidos) > Projects (Proyectos).**
7. **Haga clic en Projects (Proyectos). Name=P1.**
8. **Navegue hasta Shares (Recursos compartidos) > Projects (Proyectos) > P1 > Protocols (Protocolos).**
9. **En la sección SMB, configure Resource Name=on.**
10. **Navegue hasta Shares (Recursos compartidos) > Projects (Proyectos) > P1 > Shares (Recursos compartidos).**
11. **Haga clic en FileSystems (Sistemas de archivos). Name=S1, User=root, Group=other, Permissions=RWX RWX RWX.**
12. **Navegue hasta Shares (Recursos compartidos) > Projects (Proyectos) > P1 > Shares (Recursos compartidos) > S1 > Protocols (Protocolos). La sección SMB muestra que se puede llegar a S1 mediante SMB en \\192.168.1.7\S1.**
13. **Navegue hasta Shares (Recursos compartidos) > Projects (Proyectos) > P1 > Replication (Replicación).**
14. **Haga clic en Actions (Acciones) y configure el destino y la agrupación. Target=M5, Pool=Pool1.**

15. **Haga clic en  Schedule (Cronograma) y configure la frecuencia. Frequency=Half-Hour at 00 minutes past the hour.**

16. **En el sistema cliente SMB, asigne la unidad de red \\192.168.1.7\S1 (user=root, password=pppp$1234).**

17. **Cree el archivo F1.txt.**

18. **En el sistema de producción M11, navegue hasta Shares (Recursos compartidos) > Projects (Proyectos) > P1 > Replication (Replicación).**

19. **En la línea de acción TARGET=M5, haga clic en Update now (Actualizar ahora).**

20. **Después de finalizar la replicación, haga clic en Disable (Desactivar), el estado pasará a desactivado.**

Reversión de la replicación: simulación de la recuperación ante desastres

Para simular una recuperación antes desastres que previene el acceso al sistema de producción, use el sistema de recuperación para revertir la replicación. Cuando se revierte la replicación, el paquete de replicación presente en el destino se convierte en un proyecto local y, además, se configura una acción de replicación para este proyecto local para realizar una replicación incremental en el sistema de origen original. Esta acción de replicación no está activada de forma predeterminada. El administrador debe enviar la actualización manualmente.

▼ Replicación inversa

1. **Para simular la pérdida de contacto con el sistema principal M11 en el sistema cliente SMB, seleccione Disconnect network drive (Desconectar unidad de red).**

2. **En el sistema de recuperación ante desastres M5, seleccione Pool=Pool1.**

3. **Navegue hasta Shares (Recursos compartidos) > Projects (Proyectos) > Replica (Réplica). Se muestra el proyecto M11:P1.**

4. **Navegue hasta Shares (Recursos compartidos) > Projects (Proyectos) > Replica (Réplica) > M11:P1 > Replication (Replicación). El estado del paquete es Status=Idle.**

5. **Haga clic en Reverse the direction of replication (Revertir dirección de replicación) y defina el nuevo nombre del proyecto. New Project Name=P1.**

6. **Navegue hasta Shares (Recursos compartidos) > Projects (Proyectos) > Replica (Réplica). El proyecto M11:P1 ya no aparece porque el paquete de replicación presente en el destino se convirtió a un proyecto local.**

7. **Navegue hasta Configuration (Configuración) > Services (Servicios).**

8. **En la línea SMB debajo de Data Services (Servicio de datos), si el estado es Disabled (Desactivado), haga clic en Enable service (Activar servicio).**

9. **Navegue hasta Shares (Recursos compartidos) > Projects (Proyectos) > Local. Se muestra el proyecto P1.**

10. **Navegue hasta Shares (Recursos compartidos) > Projects (Proyectos) > P1 > Protocols (Protocolos).**

11. **En la sección SMB, configure Resource Name=on.**

12. **Navegue hasta Shares (Recursos compartidos) > Projects (Proyectos) > P1 > Shares (Recursos compartidos) > S1 > Protocols (Protocolos). La sección SMB muestra que se puede llegar a S1 mediante SMB en \\192.168.1.17\S1.**

13. **En el sistema cliente SMB, asigne la unidad de red \\192.168.1.17\S1 (user=root, password=pppp$1234).**

14. **Edite el archivo F1.txt y guárdelo como F2.txt. NOTA: Durante una secuencia de recuperación ante desastres real, una vez que se restauran las comunicaciones con el sistema de producción M11, tendrá la oportunidad de activar actualizaciones manuales, programadas o continuas mientras las aplicaciones siguen accediendo a los datos en el sistema de recuperación antes desastres M5.**

15. **Para preparar la transición nuevamente al sistema de producción, seleccione Disconnect network drive (Desconectar unidad de red).**

16. **En el sistema de recuperación ante desastres M5, navegue hasta Shares (Recursos compartidos) > Projects (Proyectos) > P1 > Replication (Replicación).**

17. **En la línea de acción TARGET=M11, haga clic en Update now (Actualizar ahora).**

18. **Después de finalizar la replicación, haga clic en Disable (Desactivar).**

Reversión de la replicación: reanudación de la replicación desde el sistema de producción

Cada vez que se revierte la replicación, debe proporcionar un nuevo nombre de proyecto que se utilizará cuando el paquete de replicación se convierte en un nuevo proyecto local. Si desea usar el mismo nombre y una reversión de replicación anterior dejó un proyecto local vacío con ese nombre, debe suprimir el proyecto vacío existente de modo que la próxima reversión pueda crear un proyecto con el mismo nombre.

▼ Replicación inversa

1. **En el sistema de producción M11, navegue hasta Shares (Recursos compartidos) > Projects (Proyectos) > Local > P1. P1 está vacío porque la primera actualización del nuevo sistema de origen (el destino original) convierte el proyecto original del sistema de origen original en un paquete de replicación. En este ejemplo, se utiliza una acción de replicación de nivel de proyecto que replica todos los recursos compartidos en el proyecto. Por lo tanto, todos los recursos compartidos presentes en este proyecto local ahora están presentes en el paquete de replicación, lo cual deja vacío el proyecto local.**
2. **Navegue hasta Shares (Recursos compartidos) > Projects (Proyectos) > Local.**
3. **Suprima P1. Es seguro suprimir este proyecto vacío porque el contenido se movió al paquete de replicación como resultado de la reversión de la replicación desde el destino original.**
4. **Navegue hasta Shares (Recursos compartidos) > Projects (Proyectos) > Replica (Réplica) > M5:P1 > Replication (Replicación).**
5. **Haga clic en Reverse the direction of replication (Revertir dirección de replicación) y defina el nombre del proyecto. New Project Name=P1.**
6. **En el sistema cliente SMB, asigne la unidad de red \\192.168.1.7\S1 (user=root, password=pppp$1234). Se muestran los archivos F1.txt y F2.txt.**
7. **En el sistema de producción M11, navegue hasta Shares (Recursos compartidos) > Projects (Proyectos) > P1 > Replication (Replicación).**
8. **En la línea de acción TARGET=M5, haga clic en Edit entry (Editar entrada).**
9. **Haga clic en  Schedule (Cronograma) y configure la frecuencia. Frequency=Half-Hour at 00 minutes past the hour.**

10. **En la línea de acción TARGET=M5, haga clic en Update now (Actualizar ahora). Esto dirige el sistema de recuperación ante desastres M5 para convertir el proyecto local P1 nuevamente en el paquete de replicación M11:P1.**

11. **Supervise la columna ACTUALIZACIONES en la línea de acción TARGET=M5 y espere hasta que finalice la actualización de replicación.**

12. **En el sistema de recuperación ante desastres M5, navegue hasta Shares (Recursos compartidos) > Projects (Proyectos) > Local > P1. P1 está vacío porque el proyecto se volvió a convertir en un paquete de replicación.**

13. **Navegue hasta Shares (Recursos compartidos) > Projects (Proyectos) > Local.**

14. **Para permitir que la siguiente reversión convierta el paquete de replicación en un proyecto denominado P1, suprima P1.**

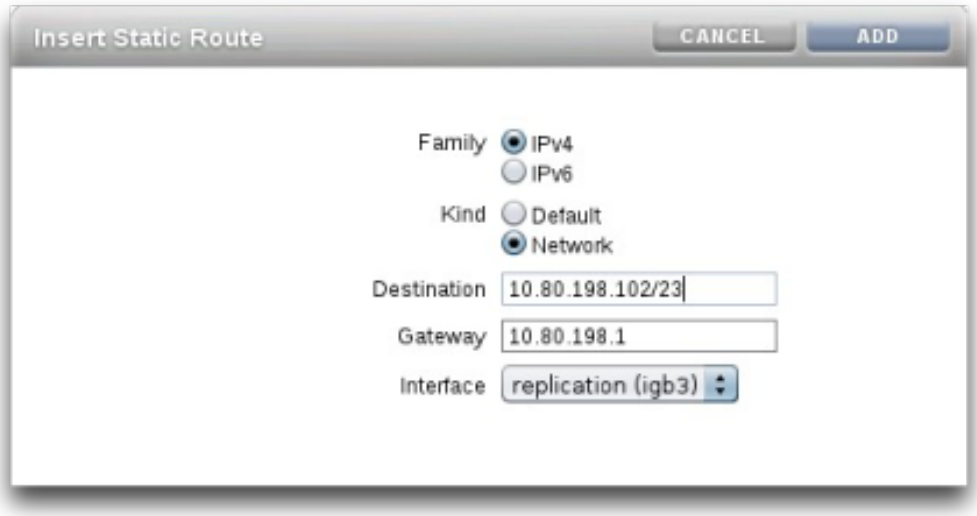
Uso forzoso de una ruta estática al replicar

Para consolidar el tráfico de la replicación en una interfaz de red específica, debe conectar los dispositivos ZFSSA de origen y destino mediante rutas estáticas. Para establecer las rutas estáticas, siga los pasos que se indican a continuación.

▼ Uso forzoso de una ruta estática al replicar

1. **Para establecer una ruta estática, en la página Configuration (Configuración) > Network (Red) > Routing (Enrutamiento), haga clic en el ícono para agregar  .**

2. **En el cuadro Insert Static Route (Insertar ruta estática), seleccione los valores para Family (Familia) y Kind (Clase) y, a continuación, introduzca los valores de Destination IP (IP de destino), Gateway (Puerta de enlace) e Interface (Interfaz).**



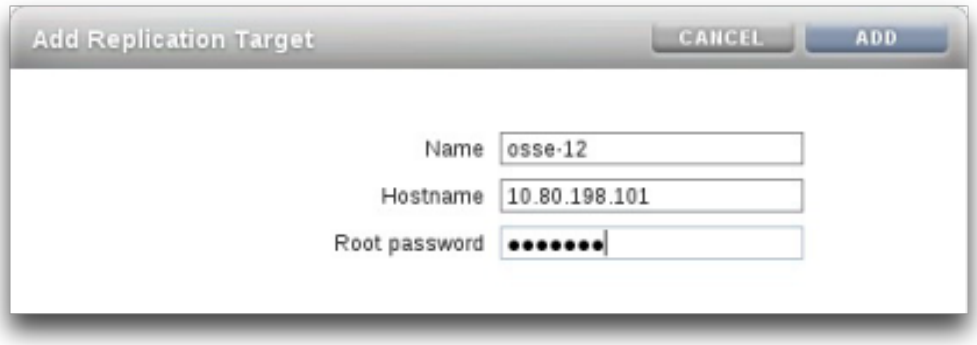
3. **Haga clic en Add (Agregar).**

4. **Para asegurarse de que se esté redireccionando tanto el tráfico del origen como el del destino, use `traceroute` en la CLI. Para obtener información acerca del uso de `traceroute`, consulte "Configuración del enrutamiento de red" [81]. En el ejemplo, se usa `10.80.219.124 @ igb0` para identificar que igb0 es la interfaz. Es una manera rápida de verificar que se esté usando la interfaz correcta.**

```
brmv01sn02:> traceroute poc7330-050
traceroute: Warning: Multiple interfaces found; using 10.80.219.124 @ igb0 traceroute
 to poc7330-050 (10.80.219.117), 30 hops max, 40 byte packets
 1  poc7330-050.us.oracle.com (10.80.219.117)  0.446 ms  0.115 ms  0.104 ms
```

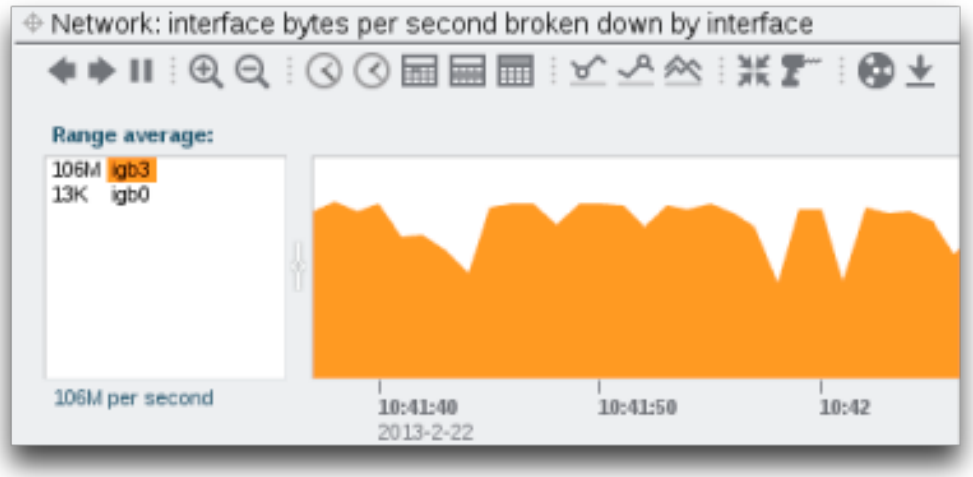
5. **Para agregar un nuevo destino de replicación, en la página Configuration (Configuración) > Services (Servicios) > Replication (Replicación), haga clic en el ícono para agregar .**

6. **En el cuadro Add Replication Target (Agregar destino de replicación), escriba un nombre para el destino, la dirección IP del nombre de host correspondiente a la interfaz de red y la contraseña.**



7. **Haga clic en Add (Agregar).**

8. **Para garantizar que el tráfico se transmita por la ruta estática definida, después de que se haya iniciado la replicación use "Bytes de interfaz de red" de "Guía de análisis de Oracle ZFS Storage Appliance ".**



9. **En la página Preferences (Preferencias), asegúrese de que la opción "Propiedades de preferencias" [149] esté activada.**

10. **Después de verificar que la replicación del origen al destino use la interfaz correcta, revierta la replicación. Para obtener información acerca de la reversión de replicaciones, consulte “ Reversión de la dirección de la replicación ” [400].**

Clonación de un proyecto de replicación recibido

En el siguiente ejemplo de la CLI, se muestra la clonación de un proyecto de replicación recibido donde se sustituye el punto de montaje del proyecto y de un recurso compartido:

```
perch:> shares
perch:shares> replication
perch:shares replication> sources
perch:shares replication sources> select source-000
perch:shares replication source-000> select package-000
perch:shares replication source-000 package-000> clone
perch:shares replication source-000 package-000 clone> set target_project=my_clone
               target_project = my_clone
perch:shares replication source-000 package-000 clone> list
CLONE PARAMETERS
               target_project = my_clone
          original_mountpoint = /export
          override_mountpoint = false
                   mountpoint =

    SHARE                          MOUNTPOINT
    bob                            (inherited)
    myfs1                          (inherited)
perch:shares replication source-000 package-000 clone> set override_mountpoint=true
          override_mountpoint = true
perch:shares replication source-000 package-000 clone> set mountpoint=/export/my_clone
                   mountpoint = /export/my_clone
perch:shares replication source-000 package-000 clone> select bob
perch:shares replication source-000 package-000 clone bob> set override_mountpoint=true
          override_mountpoint = true
perch:shares replication source-000 package-000 clone bob> set mountpoint=/export/bob
                   mountpoint = /export/bob
perch:shares replication source-000 package-000 clone bob> done
perch:shares replication source-000 package-000 clone> commit
CLONE PARAMETERS
               target_project = my_clone
          original_mountpoint = /export
          override_mountpoint = true
                   mountpoint = /export/my_clone

    SHARE                          MOUNTPOINT
    bob                            /export/bob (overridden)
    myfs1                          (inherited)
Are you sure you want to clone this project?
There are no conflicts.
perch:shares replication source-000 package-000 clone>
```

Detalles de la replicación remota

Autorizaciones

Además del filtro de replicación remota del ámbito de servicios que permite a los administradores detener, iniciar y reiniciar el servicio de replicación, el subsistema de replicación proporciona dos “Autorizaciones de usuarios” [140] en el ámbito de proyectos y recursos compartidos:

Autorización	Detalles
rrsource	Permite a los administradores crear, editar y destruir las acciones y los destinos de replicación, y enviar y cancelar actualizaciones para las acciones de replicación.
rrtarget	Permite a los administradores gestionar paquetes replicados, incluidos la desactivación de la replicación en el nivel del paquete, la clonación de un paquete o de sus miembros, la modificación de propiedades de conjuntos 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 ZFSSA, aun cuando se configura en la pantalla de servicio Remote Replication (Replicación remota). Para obtener ayuda relacionada con las autorizaciones, consulte “Autorizaciones de usuarios” [140].

Alertas

El sistema publica alertas cuando se produce alguno de los siguientes eventos:

- La actualización de replicación manual o programada comienza o finaliza correctamente (en el origen y el destino).
- Se produce un error en cualquier actualización de replicación, incluso como resultado de la cancelación explícita del administrador (en el origen y destino).
- Se omite la actualización de replicación programada porque ya hay otra actualización en curso para la misma acción (ver más arriba).
- Cuando una replicación continua se inicia por primera vez.

- Cuando falla una replicación continua.
- Cuando una replicación continua se inicia por primera vez, falla o se reanuda después de un fallo.

Eventos de auditoría de replicación

El sistema audita los siguientes eventos de replicación y los registra en "Logs" de "Manual de servicio del cliente de Oracle ZFS Storage Appliance ".

- 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

Replicación y agrupación en clusters

La replicación se puede configurar de cualquier dispositivo ZFS Storage Appliance a cualquier otro dispositivo ZFS Storage Appliance, independientemente de si cada uno forma parte de un cluster y de si el par de cluster del dispositivo ZFSSA tiene una replicación configurada en cualquier dirección, excepto las siguientes limitaciones:

- No se admite la configuración de la replicación de ambos pares de un cluster al mismo destino de replicación, pero se puede obtener una configuración similar mediante dos direcciones IP diferentes para el mismo dispositivo ZFSSA de destino. Los administradores pueden utilizar múltiples direcciones IP del dispositivo ZFSSA de destino para crear un destino de replicación en cada nodo principal de cluster para ser utilizado por dicho cabezal.

- Cuando configure una replicación entre pares de clusters, configure la replicación con ambos controladores en estado En cluster. No utilice direcciones de redes privadas y utilice destinos de replicación separados para las agrupaciones de cada controlador.

Las siguientes reglas rigen el comportamiento de la replicación en las configuraciones agrupadas en cluster:

- 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 actualizaciones de replicaciones 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 nodo principal con esta dirección IP siempre tendrá la agrupación

de almacenamiento que contiene la réplica importada. Para garantizarlo, se asigna la agrupación y los recursos de dirección IP al mismo nodo principal durante la configuración del cluster.

- Se producirá un error en las actualizaciones de replicación (desde y hacia el dispositivo ZFSSA) que estén en curso cuando un dispositivo ZFSSA 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 conmutación por recuperación no se verán afectadas por la operación.

Para obtener más información sobre la agrupación en clusters y la terminología relacionada con los clusters, consulte el Capítulo 10, Configuración de cluster.

Instantáneas y coherencia de datos

El dispositivo ZFSSA replica instantáneas y cada instantánea se recibe automáticamente en el destino; por lo tanto, el contenido de la réplica de un recurso compartido en el destino siempre coincide con el contenido del recurso compartido en el origen en el momento en que se toma la instantánea. Dado que las instantáneas de todos los recursos compartidos enviadas en un grupo en particular se obtienen en el mismo momento (ver más arriba), 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 (cuando comenzó la actualización de replicación).

Sin embargo, las instantáneas de cada recurso compartido se replican por separado (y en serie); por lo tanto, es posible que algunos recursos compartidos dentro de un paquete se hayan actualizado con una instantánea más reciente que la de otros recursos compartidos del mismo paquete. Esto ocurre durante una actualización de replicación (después de la actualización de algunos recursos compartidos y antes de la actualización de otros) y después de una actualización de replicación con errores (después de la cual se han actualizado algunos recursos compartidos, pero otros no).

En resumen:

- Cada recurso compartido siempre es coherente con el momento del destino (coherente en sí mismo).
- 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 (coherente con los paquetes).
- 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.

Gestión de instantáneas

Las instantáneas son la base de la replicación incremental. 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 se trata de una actualización incremental o completa según si se ha intentado replicar esta acción antes y si el destino ya tiene la instantánea que necesita 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 “gestión del espacio” [304] en el dispositivo ZFSSA, en particular “su aplicación a las instantáneas” [304].
- Para obtener información acerca de la gestión del espacio para replicar LUN, consulte “Gestión de espacio para replicación de LUN” [304].

Replicación de la configuración de iSCSI

Como se describió anteriormente, 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. Cuando 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. Sólo es necesario que los grupos existan con el mismo nombre y no que tengan la misma configuración. Si esto no se cumple, la clonación y exportación de LUN replicados puede fallar.

El GUID SCSI asociado a un LUN se replica con el LUN. Como resultado, el LUN del dispositivo ZFSSA de destino tendrá el mismo GUID SCSI que el LUN del dispositivo ZFSSA 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).

Replicación de clones

La replicación en 2009.Q3 y versiones anteriores era sólo de nivel de proyecto y explícitamente prohibía la replicación de proyectos que contuvieran clones cuyas instantáneas de origen residieran fuera del proyecto. Con la replicación de nivel de recurso compartido en 2010.Q1 y versiones posteriores, esta restricción se ha flexibilizado, pero los administradores aún deben considerar las instantáneas de origen de los clones que se replican. En particular, la replicación inicial de un clon requiere que la instantánea de origen ya se haya replicado al destino o se esté replicando como parte de la misma actualización. Esta restricción no es aplicada por el software de gestión del dispositivo ZFSSA, pero si se intenta replicar un clon cuando la instantánea de origen no existe en el destino, se producirá un error.

En la práctica, existen diversas maneras de garantizar el éxito de la replicación de un clon:

- Si la instantánea de origen de un clon está en el mismo proyecto, simplemente utilice la replicación de nivel de proyecto.
- Si la instantánea de origen del clon no está en el mismo proyecto o si, por otros motivos, no se desea realizar una replicación de nivel de proyecto que incluya el origen, utilice la replicación de nivel de recurso compartido para replicar el recurso compartido de

origen primero y, luego, utilice la replicación de nivel de recurso compartido o de nivel de proyecto para replicar el clon.

- No destruya el origen del clon en el sistema de destino, a menos que también desee destruir el clon.

En todos los casos, la propiedad "include snapshots" (incluir instantáneas) debe ser verdadera en la acción del origen para garantizar que la instantánea de origen se envíe realmente al destino.

Observación de la replicación

Los siguientes "Análisis" de "Guía de análisis de Oracle ZFS Storage Appliance " están disponibles para replicación:

- "Operaciones de replicación de movimiento de datos" de "Guía de análisis de Oracle ZFS Storage Appliance "
- "Bytes de replicación de movimiento de datos" de "Guía de análisis de Oracle ZFS Storage Appliance "
- También hay disponibles "Estadísticas" de "Guía de análisis de Oracle ZFS Storage Appliance "

Fallos de replicación

Se pueden producir fallos en las actualizaciones de replicaciones individuales por diversos motivos. Cuando es posible, el dispositivo ZFSSA informa el motivo del fallo mediante alertas publicadas en el dispositivo ZFSSA de origen o de destino, o en la pantalla Replication (Replicación) de la acción que produjo el error. Para obtener información detallada sobre el fallo, debe hacer clic en el ícono de alerta naranja que representa el estado de la acción. A continuación, se muestran los tipos de fallos más comunes:

Error	Detalles
Cancelado	La actualización de replicación fue cancelada por el administrador. La replicación se puede cancelar en el origen o destino y es posible que un par no se dé cuenta que el otro par ha cancelado la operación.
Error de conectividad de red	El dispositivo ZFSSA no pudo establecer conexión con el dispositivo ZFSSA de destino debido a un problema de la red. Es posible que haya una configuración errónea en el origen, el destino o la red.
Error de verificación de par	El dispositivo ZFSSA 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

Error	Detalles
	destino de replicación en el dispositivo ZFSSA 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 de proyecto ” [381].
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 dispositivo ZFSSA de destino ejecuta software incompatible. Para obtener información detallada, consulte “ Actualización de la versión 2009.Q3 y versiones anteriores ” [419].
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. También es posible observar este error 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 dispositivo ZFSSA de destino.
Hay un paquete que no está vacío	Se produjo un error en la replicación porque el paquete de destino contiene datos de una actualización de replicación errónea anterior. Este error se produce cuando se intenta enviar una actualización de replicación para una acción cuya primera actualización de replicación falló después de replicar algunos datos. El dispositivo ZFSSA de destino no destruirá datos sin una indicación administrativa explícita; por lo tanto, no sobrescribirá los datos recibidos parcialmente. El administrador debe eliminar el paquete y la acción existentes, crear una nueva acción en el origen e iniciar nuevamente la replicación.
Desactivado	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 replicaciones 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, éstas se acumularán hasta que los recursos estén disponibles.
Sin espacio	Se produjo un error en la replicación porque el sistema de origen no tenía suficiente espacio para crear una

Error	Detalles
	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 excedería la cuota debido a reservaciones que no incluyen instantáneas.
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. Verifique las notas de la versión correspondientes a la versión del software del sistema de origen, para obtener una lista de las actualizaciones diferidas y para saber si éstas afectan la replicación remota.
Otro	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. La implementación actual replica los recursos compartidos dentro de un proyecto en serie y no revierte los cambios de las actualizaciones en las que se ha producido un error. Como resultado, cuando se produce un error en una actualización, es posible que algunos recursos compartidos del destino estén actualizados y otros no. Para obtener más información, consulte "Instantáneas y coherencia de datos" más arriba.

Si bien algunos datos se pueden haber replicado con éxito como parte de una actualización con errores, la implementación actual vuelve a enviar todos los datos enviados como parte de la actualización previa (con errores). Es decir que las actualizaciones con errores no retomarán donde dejaron, sino que comenzarán desde donde se produjo el error de la actualización.

Cuando se producen errores en las actualizaciones manuales o programadas, el sistema no vuelve a intentar automáticamente hasta la siguiente actualización programada (si la hubiera). Cuando se producen errores en la replicación continua, el sistema aguarda algunos minutos y vuelve a intentar. El sistema continuará intentando las replicaciones continuas con errores de manera indefinida.

Cuando hay una actualización de replicación en curso y hay otra actualización programada, la última actualización se omite por completo en lugar de iniciarse inmediatamente después de la finalización de la actualización anterior. La siguiente actualización se enviará sólo en el momento en que se ha programado la siguiente actualización. El sistema publica una alerta cuando se omite una actualización por este motivo.

Compatibilidad de replicación

Antes de realizar una actualización de replicación, el servicio de replicación verifica que el sistema de destino sea compatible con los nuevos datos del origen.

- Si, en el origen, hay funciones en uso que no son compatibles con el destino, y las funciones se pueden desactivar de forma segura, el servicio de replicación desactivará la funciones, realizará la actualización y emitirá una advertencia.
- Si, en el origen, hay funciones en uso que no son compatibles con el destino y no se pueden desactivar, el servicio de replicación no realizará la actualización y emitirá un error.

NOTA: Siempre es mejor actualizar el destino lo antes posible.

Las actualizaciones que anulan la compatibilidad de replicación se entregan como actualizaciones diferidas. Para ver la lista actual y una descripción, consulte "Actualizaciones" de "Manual de servicio del cliente de Oracle ZFS Storage Appliance " y las notas de la versión de Oracle ZFS Storage Appliance para su versión actual.

Actualización de la versión 2009.Q3 y versiones anteriores

La implementación de la replicación ha cambiado significativamente entre las versiones 2009.Q3 y 2010.Q1. Se recomienda suspender la replicación desde y hacia un dispositivo ZFSSA antes de iniciar una actualización desde la versión 2009.Q3 o anterior. Esto es obligatorio en clusters que utilizan la actualización gradual.

Existen tres cambios importantes visibles para el usuario y relacionados con la actualización a la versión 2010.Q1 o posteriores:

- El protocolo de red utilizado para la replicación ha sido mejorado. Los sistemas de la versión 2009.Q3 se pueden replicar en sistemas que ejecuten cualquier versión (incluida la versión 2010.Q1, y posteriores), mientras que los sistemas que ejecutan la versión 2010.Q1, o posterior, sólo pueden replicarse en otros sistemas que ejecuten la versión 2010.Q1, o posterior. En la práctica, esto significa que los destinos de replicación se deben actualizar antes o al mismo tiempo que los orígenes de replicación, para evitar errores derivados de versiones de protocolos no compatibles.
- La configuración de la acción de replicación ahora se almacena en la agrupación de almacenamiento en lugar de hacerlo en el sistema principal. Como resultado, después de actualizar desde la versión 2009.Q3, o anterior, a 2010.Q1, los administradores deben aplicar las actualizaciones diferidas para migrar su configuración de replicación.
- * Hasta que se apliquen estas actualizaciones, se producirán errores en las actualizaciones de replicación entrantes para las réplicas existentes, y las actualizaciones de replicación no se enviarán para las acciones configuradas en la versión 2009.Q3, o anteriores. Además, se

utilizará espacio de la agrupación de almacenamiento para las réplicas no migradas, que no se puedan gestionar desde la BUI o la CLI.

- * Cuando se apliquen estas actualizaciones, de la misma manera que sucede con todas las actualizaciones diferidas, la reversión del software del sistema tendrá resultados indefinidos. Con la versión anterior posiblemente no se podrá acceder a los datos replicados, se dejarán de configurar todas las acciones de replicación y las actualizaciones de replicaciones entrantes serán actualizaciones completas.
- Las autorizaciones de replicación han pasado del ámbito anterior al ámbito de proyectos y recursos compartidos. Todas las autorizaciones de replicación configuradas en la versión 2009.Q3 o anteriores ya no existirán en 2010.Q1. Los administradores que utilicen control de acceso específico para la replicación deberán delegar las nuevas autorizaciones de replicación a los administradores adecuados después de la actualización.

♦ ♦ ♦ CAPÍTULO 14

Migración shadow

En esta sección se describe la migración shadow para ZFSSA.

Migración de datos

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 ZFSSA tiene dos soluciones integradas para migrar los datos relacionados con los casos de uso más comunes. La primera, Capítulo 13, Replicación, tiene como finalidad replicar datos entre uno o varios dispositivos ZFSSA, y se trata por separado. 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 ZFSSA 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, como los que se describen a continuación.

Migración tradicional de datos

La migración tradicional de archivos normalmente funciona de una de las dos maneras siguientes: sincronización repetida o interposición externa.

Migración mediante sincronización

Este método funciona mediante la adopción de un host activo X y la migración de datos al nuevo host Y, mientras X permanece activo. Los clientes aún pueden leer y modificar datos en el host original mientras esta migración está en curso. Una vez que se realiza la migración inicial de los datos, se envían cambios incrementales de manera reiterada hasta que el archivo

delta es suficientemente pequeño para ser enviado dentro de una única ventana de inactividad. En este momento, el recurso compartido original pasa a ser de sólo lectura, el archivo delta final se envía al nuevo host y todos los clientes se actualizan para apuntar a la nueva ubicación. La manera más común de lograr esto es mediante la herramienta rsync, aunque existen otras herramientas integradas. Este mecanismo tiene diversas desventajas:

- Si bien el tiempo de inactividad anticipado es breve, no se puede cuantificar con facilidad. Si un usuario confirma una gran cantidad cambios inmediatamente antes del tiempo de inactividad programado, puede aumentar el período de inactividad.
- Durante la migración, el nuevo servidor está inactivo. Dado que los nuevos servidores generalmente contienen nuevas características o mejoras de rendimiento, representan un desperdicio de recursos durante un período de migración potencialmente extenso.
- La coordinación entre varios sistemas de archivos es incómoda. Cuando se migran docenas o cientos de sistemas de archivos, cada migración tardará una cantidad diferente de tiempo y se deberá programar el tiempo de inactividad de la unión de todos los sistemas de archivos.

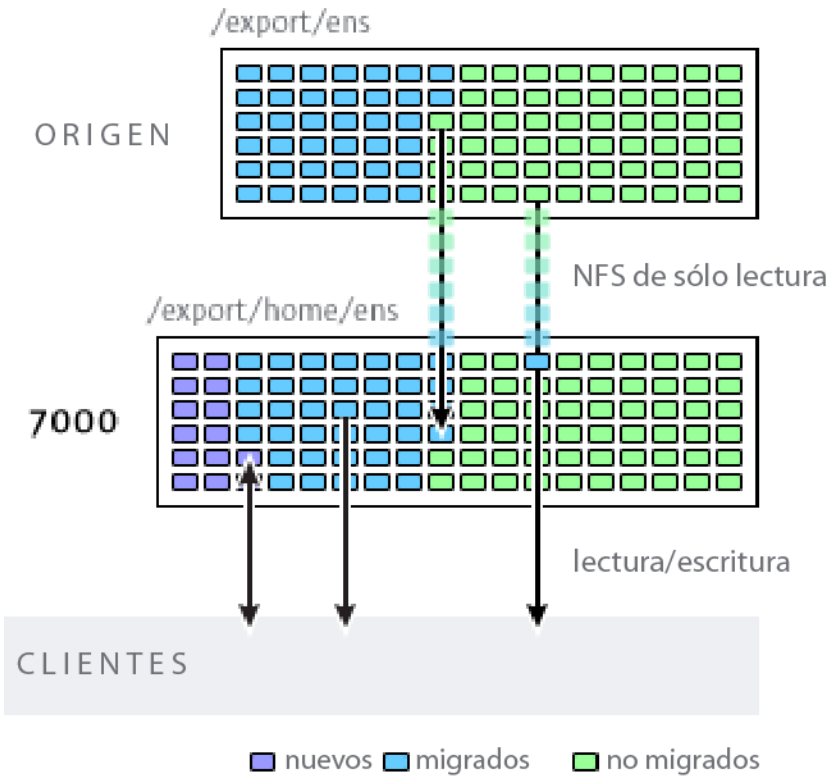
Migración mediante interposición externa

Este método funciona mediante la adopción de un host activo X y la inserción de un nuevo dispositivo ZFSSA M que migra datos a un nuevo host Y. Todos los clientes se actualizan a la vez para apuntar a M, y los datos se migran automáticamente en segundo plano. Esto ofrece más flexibilidad para las opciones de migración (como la capacidad de migrar a un nuevo servidor en el futuro sin tiempo de inactividad) y permite aprovechar el nuevo servidor para datos ya migrados, pero también tiene desventajas significativas:

- El dispositivo de migración ZFSSA representa un nuevo equipo físico, con costos asociados (inversión inicial, costos de asistencia, energía y enfriamiento) y sobrecarga de gestión adicional.
- El dispositivo de migración ZFSSA representa un nuevo punto de error en el sistema.
- El dispositivo de migración ZFSSA se interpone en datos ya migrados e incurre en latencia adicional, generalmente, en forma permanente. Estos dispositivos ZFSSA normalmente quedan en su lugar, aunque sería posible programar otro período de inactividad y retirar el dispositivo de migración ZFSSA.

Migración shadow

FIGURA 14-1 Migración shadow



La migración shadow utiliza la interposición, pero está integrada en el dispositivo ZFSSA y no requiere un equipo físico aparte. Cuando se generan recursos compartidos, 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 ZFSSA de origen X se coloca en modo de sólo lectura, se crea un recurso compartido con la propiedad shadow configurada y los clientes se actualizan para apuntar al nuevo recurso compartido del dispositivo Sun Storage 7000 ZFSSA. A continuación, los clientes pueden acceder al dispositivo ZFSSA en modo lectura y escritura.

Una vez que está configurada la propiedad shadow, los datos se migran de manera transparente en segundo plano desde el dispositivo ZFSSA de origen localmente. Si una solicitud proviene de un cliente para un archivo que aún no se ha migrado, el dispositivo ZFSSA 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 ZFSSA 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 sólo en un host. Por lo tanto, es extremadamente importante que antes de realizar cualquier migración entre dos hosts ésta 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.

Comportamiento de la migración shadow

Restricciones del origen shadow

- Para migrar datos correctamente, el directorio o sistema de archivos de origen *debe ser de sólo 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 irrecuperables en el dispositivo ZFSSA.
- La migración shadow admite la migración sólo de orígenes NFS. Los recursos compartidos NFSv4 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.

Semántica del sistema de archivos shadow 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:

- En el caso de los directorios, se bloquean las solicitudes de clientes hasta que finalice la migración de todo el directorio. En el caso de los archivos, sólo 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 ZFSSA, 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 en múltiples sistemas de archivos a un único sistema de archivos, mediante el uso de montajes de clientes automáticos NFSv4 (en ocasiones denominados "montajes reflejados") o montajes locales anidados.

Migración de identidad y ACL

Para migrar correctamente la información de identidad de los archivos, incluidas las ACL, se debe cumplir con las siguientes reglas:

- Los dispositivos ZFSSA de origen y de destino de la migración deben tener la misma configuración de servicio de nombres.
- Los dispositivos ZFSSA de origen y de destino de la migración deben tener el mismo dominio mapid NFSv4.
- El origen de la migración debe admitir NFSv4. 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 ZFSSA.

Si observa archivos o directorios cuyo propietario es "nobody" (nadie), probablemente signifique que el dispositivo ZFSSA no tiene servicios de nombres configurados correctamente, o que el dominio mapid NFSv4 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.

Gestión de migración shadow

Creación de un sistema de archivos shadow

El origen de la migración shadow sólo se puede configurar cuando se crea un sistema de archivos. En el caso de la BUI, está 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, éste automáticamente comienza a migrar en segundo plano, además de responder las solicitudes en línea. Esta migración es controlada por el “servicio de migración shadow” [245]. 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 sólo 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 éste 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 sólo 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

La supervisión del progreso de una migración shadow es difícil debido al contexto en el cual se ejecuta la operación. Un único sistema de archivos puede realizar una migración shadow de un sistema de archivos entero, de una parte de él o de varios sistemas de archivos con puntos de montaje anidados. Por lo tanto, no existe manera de solicitar estadísticas sobre el origen y tener la seguridad de que sean correctas. Además, incluso con la migración de un único sistema de archivos, los métodos utilizados para calcular el tamaño disponible no son coherentes en los sistemas. Por ejemplo, el sistema de archivos remoto puede utilizar compresión, y puede, o no, incluir sobrecarga de metadatos. Por estos motivos, es imposible mostrar una barra de progreso precisa para cualquier migración en particular.

El dispositivo ZFSSA proporciona la siguiente información y garantiza que es precisa:

- Tamaño local del sistema de archivos local hasta el momento

- Tamaño lógico de los datos copiados hasta el momento
- Tiempo dedicado a la migración de datos hasta el momento

Estos valores están disponibles en la BUI y la CLI mediante las propiedades del sistemas de archivos estándar y las propiedades del nodo de migración shadow (o panel de la interfaz de usuario). Si conoce el tamaño del sistema de archivos remoto, lo puede utilizar para calcular el progreso. El tamaño de los datos copiados sólo se compone de contenido de archivos sin formato que se debe migrar desde el origen. Los directorios, los metadatos y los atributos extendidos no están incluidos en este cálculo. Si bien el tamaño de los datos migrados hasta ahora sólo incluye los datos migrados en forma remota, la reanudación de la migración en segundo plano podría recorrer partes del sistema de archivos que ya se han migrado. Como consecuencia, podría ejecutarse bastante rápidamente mientras procesa estos directorios iniciales y bajar la velocidad una vez que alcanza las porciones del sistema de archivos que aún no se han migrado.

Si bien no existe una medición precisa del progreso, el dispositivo ZFSSA intenta calcular los datos restantes en función de la hipótesis de un árbol de directorio relativamente uniforme. Este cálculo puede ser bastante preciso o no tener ningún valor según el conjunto de datos, y sólo se realiza con fines informativos. Por ejemplo, se podría tener un árbol de sistema de archivos relativamente superficial, pero contar con una gran cantidad de datos en un único directorio que se visitó por última vez. En este caso, la migración parecerá estar casi completa y, luego, se reducirá rápidamente a un porcentaje muy bajo cuando se detecte este nuevo árbol. En cambio, si el directorio grande se procesa primero, el cálculo puede suponer que todos los demás directorios tienen una cantidad de datos similarmente grande y, cuando los encuentra mayormente vacíos, el cálculo rápidamente aumenta de un porcentaje pequeño a casi completo. La mejor manera de medir el progreso consiste en configurar una migración de prueba, ejecutarla y dejarla finalizar, y utilizar ese valor para calcular el progreso del sistema de archivos de tamaño y diseño similar.

Cancelación de migración

La migración se puede cancelar, pero esto sólo 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`.

Instantáneas de sistemas de archivo 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, éstas no se pueden revertir ni pueden ser el origen de un clon. Esto refleja el estado incoherente de los datos en el disco durante la migración.

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 sólo 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, éste 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 sólo 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 una conmutación por error 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 una conmutación por error en el destino, el administrador puede observar los errores y corregir la configuración de shadow según sea necesario para el nuevo entorno.

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 "Análisis" de "Guía de análisis de Oracle ZFS Storage Appliance ". El análisis de migración shadow está disponible en la categoría de movimiento de datos. Existen dos 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 conjuntos 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.

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 ZFSSA. 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 sólo 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.

Tareas de migración shadow

Antes de intentar llevar a cabo una migración completa, es importante probar dicha migración para asegurarse de que el dispositivo ZFSSA 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 recursos compartidos para la migración final.

▼ Prueba de la posible migración shadow

1. **Configure el origen de manera que el dispositivo ZFSSA 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 sólo 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 sólo 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

1. **Programe 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 ZFSSA 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 sólo 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 SS7000.**

   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 recursos compartidos durante un único tiempo de inactividad programado mediante la secuencia de comandos de la CLI.

♦ ♦ ♦ CAPÍTULO 15

Secuencias de comandos de la CLI

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

Automatización del acceso

Puede usar “Comandos por lotes” [433] o “Creación de secuencias de comandos” [434] (o alguna combinación de ellos), pero en cualquiera de los casos la infraestructura automatizada requiere acceso al dispositivo. Para ello se debe utilizar Capítulo 7, Configuración de usuario, “Autorizaciones de usuarios” [140] y “Configuración de claves SSH públicas con la CLI” [150].

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@dory < 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@dory << 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.

Creación de secuencias de comandos

Si bien el uso de comandos por lotes es suficiente para las operaciones más simples, puede ser tedioso utilizarlo con 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

Entorno de secuencia de comandos

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

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

Como indicador de entorno de secuencia de comandos, puede escribir la secuencia de comandos y finalizar con "`.`" en una línea para ejecutarla:

```
dory:> 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!
```

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:

```
dory:> script print("It is now " + new Date())
It is now Tue Oct 14 2009 05:33:01 GMT+0000 (UTC)
```

Interacción con el sistema

Desde luego, las secuencias de comandos sirven de poco si no pueden interactuar con el sistema en general. Hay varias funciones incorporadas que permiten a las secuencias de comandos interactuar con el sistema:

TABLA 15-1 Funciones incorporadas para admitir interacciones entre sistemas

Función	Descripción
`get`	Permite obtener el valor de la propiedad especificada. Tenga en cuenta que esta función devuelve el valor en forma nativa, por ejemplo, las fechas se devuelven como objetos Fecha.
`list`	Devuelve una matriz de tokens que corresponden a los objetos secundarios dinámicos del contexto actual.
`run`	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.
`props`	Devuelve una matriz de los nombres de las propiedades para el nodo actual.
`set`	Toma dos argumentos de cadena y configura la propiedad especificada con el valor especificado.
`choices`	Devuelve una selección de los valores válidos de cualquier propiedad para la cual se conoce el conjunto de valores y se puede enumerar.

Función run

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

```
dory:> configuration version script dump(run('get boot_time'))
'                     boot_time = 2009-10-12 07:02:17\n'
```

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:

```
dory:> configuration version script dump(run('get boot_time').split(/\s+/))
[&amp;#39;', 'boot_time', '=', '2009-10-12', '07:02:17', &amp;#39;']
```

Función get

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 robusta, use la función "`get`" incorporada. 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. 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': '');
```

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

```
% ssh root@dory < 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; para solucionar el problema al que hace referencia este mensaje se puede especificar la opción "-T" para ssh.

Función list

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. Por ejemplo, a continuación, se

muestra una secuencia de comandos que 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 ..');
       }
```

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

```
% ssh root@koi < 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
...
```

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 ..');
}
```

Y ésta es la salida de la ejecución de esta nueva secuencia de comandos, suponiendo que se le asignó el nombre "prettyspace.aksh":

```
% ssh root@koi < 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
...
```

Función children

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. 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");
        }
```

Ésta es la salida de la ejecución de la secuencia de comandos, suponiendo que se haya guardado en un archivo llamado "svcinfo.aksh":

```
% ssh root@koi < space.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
```

Función choices

La función choices devuelve una selección de los valores válidos de cualquier propiedad para la cual se conoce el conjunto 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.

```
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 ..');
        }
}
```

Esta es la salida de la ejecución de la secuencia de comandos:

```
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
```

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 15-2 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.

Errores

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:

```
dory:> 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:

```
dory:> 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@dory <<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
```

♦ ♦ ♦ CAPÍTULO 16

Flujos de trabajo de mantenimiento

Un flujo de trabajo es una Capítulo 15, Secuencias de comandos de la CLI que se carga y se gestiona mediante el propio dispositivo ZFSSA. 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 de manera opcional como Capítulo 9, Configuración de alertas o en un momento designado. Así, los flujos de trabajo permiten que el dispositivo ZFSSA se *extienda* para capturar políticas y procedimientos específicos y se pueden usar (por ejemplo) para codificar formalmente las prácticas recomendadas para una organización o aplicación en particular.

Uso de los flujos de trabajo

Los flujos de trabajo se incluyen en un archivo ECMAscript válido que contiene una única variable global, `workflow`. Es un objeto que debe contener al menos tres miembros:

TABLA 16-1 Miembros objeto requeridos

Miembro obligatorio	Tipo	Descripción
`name`	String	Nombre del flujo de trabajo.
`description`	String	Descripción del flujo de trabajo.
`execute`	Function	Función que ejecuta el flujo de trabajo.

Este es el flujo de trabajo canónicamente trivial:

```
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"; la ejecución del flujo de trabajo genera la salida "hello world!".

Contexto de ejecución de flujos de trabajo

Los flujos de trabajo se ejecutan de manera asíncrona en el shell del dispositivo ZFSSA, y utilizan (de manera predeterminada) el usuario que ejecuta el flujo de trabajo. Así, los flujos de trabajo tienen a su disposición la Capítulo 15, Secuencias de comandos de la CLI y pueden interaccionar con el dispositivo ZFSSA como cualquier otra instancia del shell del dispositivo ZFSSA. Es decir, los flujos de trabajo pueden ejecutar comandos, analizar salidas, modificar el estado, etc. Este es un ejemplo más complicado que 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] + '%');
       }
};
```

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 16-2 Miembros de parámetros de flujo de trabajo requeridos

Miembro obligatorio	Tipo	Descripción
`label`	String	Etiqueta para adornar la entrada del parámetro del flujo de trabajo.
`type`	String	Tipo de parámetro de flujo de trabajo.

El miembro `type` debe ser de uno de estos tipos:

TABLA 16-3 Nombres de tipos de miembros

Nombre del tipo	Descripción
`Boolean`	Valor booleano

Nombre del tipo	Descripción
`ChooseOne`	Un valor de una serie de valores especificados
`EmailAddress`	Dirección de correo electrónico
`File`	Archivo que se transfiere al dispositivo ZFSSA
`Host`	Host válido, como nombre o decimal con punto
`HostName`	Nombre de host válido
`HostPort`	Puerto válido disponible
`Integer`	Número entero
`NetAddress`	Dirección de red
`NodeName`	Nombre de nodo de red
`NonNegativeInteger`	Número entero mayor o igual que cero
`Number`	Cualquier número, incluido el punto flotante
`Password`	Contraseña
`Permissions`	Permisos de POSIX
`Port`	Número de puerto
`Size`	Tamaño
`String`	Cadena
`StringList`	Lista de cadenas

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

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 16-4 Miembros requeridos de parámetros restringidos

Miembro obligatorio	Tipo	Descripción
`options`	Array	Matriz de cadenas que especifica las opciones válidas.
`optionlabels`	Array	Matriz de cadenas que especifica las etiquetas asociadas con las opciones especificadas en `options`.

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 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 16-5 Miembros requeridos para parámetros opcionales

Miembro opcional	Tipo	Descripción
`optional`	Boolean	Si se configura con el valor `true`, 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. 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. 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 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.

Generación de informes de ejecución de flujos de trabajo

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 16-6 Miembros requeridos para la generación de informes de ejecución

Miembro obligatorio	Tipo	Descripción
`step`	String	Cadena que denota el nombre del paso de ejecución.
`execute`	Function	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. 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); }
};
```

Control de versiones

El control de versiones tiene dos aspectos relevantes para los flujos de trabajo: el primero es la expresión de la versión del software del dispositivo ZFSSA 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 16-7 Miembros opcionales para el control de versiones

Miembro opcional	Tipo	Descripción
`required`	String	Versión mínima requerida del software del dispositivo ZFSSA para poder ejecutar el flujo de trabajo, incluidos el año, mes, día, compilación y rama.
`version`	String	Versión de este flujo de trabajo, en notación decimal con punto (principal.menor.micro).

Control de versiones de dispositivo

Para expresar una versión de software del dispositivo ZFSSA mínima requerida, agregue el campo opcional `required` al flujo de trabajo. Las versiones del dispositivo ZFSSA

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 "2009.04.10,12-0" sería la compilación doce del software originalmente desarrollado el 10 de abril de 2009. Para obtener la versión del software actual del dispositivo ZFSSA, ejecute el comando "`configuration version get version`" de la CLI o consulte el campo "Version" (Versión) de "Sistema" de "Manual de servicio del cliente de Oracle ZFS Storage Appliance " en la BUI. A continuación se presenta un ejemplo del uso del campo `required`:

```
var workflow = {
 name: 'Configure FC',
 description: 'Configures fibre channel target groups',
        required: '2009.12.25,1-0',
        ...
```

Si un flujo de trabajo requiere una versión de software que es más reciente que la versión cargada en el dispositivo ZFSSA, 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 ZFSSA, 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".

Flujos de trabajo como acciones de alerta

De manera opcional, los flujos de trabajo se pueden ejecutar como Capítulo 9, Configuración de alertas. Para que un flujo de trabajo pueda ser elegible como acción de alerta, la acción `alert` del flujo de trabajo debe estar configurada con el valor `true`.

Contexto de ejecución de las acciones de alerta

Cuando se ejecutan como acciones de alerta, los flujos de trabajo asumen la identidad del usuario que los creó. Por este motivo, todo flujo de trabajo que deba ser elegible como acción de alerta debe tener el parámetro `setid` configurado con el valor `true`. Las acciones de alerta tienen un parámetro de objeto único que tiene los siguientes miembros:

TABLA 16-8 Miembros requeridos para el contexto de ejecución de las alertas

Miembro obligatorio	Tipo	Descripción
`class`	String	Clase de alerta.
`code`	String	Código de alerta.
`items`	Object	Objeto que describe la alerta.
`timestamp`	Date	Fecha/hora de la alerta.

El miembro `items` del objeto de parámetros tiene los siguientes miembros:

TABLA 16-9 Miembros requeridos para el miembro de elementos

Miembro obligatorio	Tipo	Descripción
`url`	String	Dirección URL de la página web en donde se describe la alerta.
`action`	String	Acción que debe realizar el usuario en respuesta a la alerta.
`impact`	String	Impacto del evento que generó la alerta.
`description`	String	Cadena en lenguaje natural en donde se describe la alerta.
`severity`	String	Gravedad del evento que generó la alerta.

Auditoría de acciones de alerta

Los flujos de trabajo que se ejecutan como acciones de alerta pueden utilizar la función `audit` para generar entradas de log de auditoría. Se recomienda generar toda la información de depuración relevante para el log de auditoría mediante la función `audit`. Por ejemplo, en el siguiente flujo de trabajo, se ejecuta el failover si se tiene el estado de cluster, pero se realiza una auditoría de 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) {
               /*
                * To failover, we first confirm that clustering is configured
                * and that we are in the clustered state.  We then reboot,
                * which will force our peer to takeover.  Note that we're
                * being very conservative by only rebooting if in the
```

```
                 * AKCS_CLUSTERED state:  there are other states in which it
                 * may well be valid to failback (e.g., we are in AKCS_OWNER,
                 * and our peer is AKCS_STRIPPED), but those states may also
                 * indicate aberrent operation, and we therefore refuse to
                 * failback.  (Even in an active/passive clustered config, a
                 * FAILBACK should always be performed to transition the
                 * cluster peers from OWNER/STRIPPED to CLUSTERED/CLUSTERED.)
                 */
                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');
        }
};
```

Uso de flujos de trabajo programados

Los flujos de trabajo se pueden iniciar mediante un evento de temporizador, para lo que se debe configurar un programa. Se debe agregar la propiedad "scheduled" al objeto "workflow" y se debe configurar en "true". Los programas se pueden crear desde la CLI una vez que el flujo de trabajo se haya cargado en el dispositivo ZFSSA, o se puede agregar una propiedad de tipo de matriz llamada "schedule" al objeto "workflow".

Uso de la CLI

Después de haber cargado un flujo de trabajo en el dispositivo ZFSSA, se puede definir un programa para el flujo de trabajo desde la interfaz CLI de la siguiente manera:

```
dory:> maintenance workflows
dory:maintenance workflows> "select workflow-002'''
dory:maintenance workflow-002> schedules
```

```
dory:maintenance workflow-002 schedules>create
dory:maintenance workflow-002 schedule (uncommitted)> set frequency=day
                   frequency = day (uncommitted)
dory:maintenance workflow-002 schedule (uncommitted)> set hour=10
                        hour = 10 (uncommitted)
dory:maintenance workflow-002 schedule (uncommitted)> set minute=05
                      minute = 05 (uncommitted)
dory:maintenance workflow-002 schedule (uncommitted)> commit
dory:maintenance workflow-002 schedules> list
NAME                 FREQUENCY            DAY                  HH:MM
schedule-001         day                  -                    10:05
dory:maintenance workflow-002 schedules> create
dory:maintenance workflow-002 schedule (uncommitted)> set frequency=week
                   frequency = week (uncommitted)
dory:maintenance workflow-002 schedule (uncommitted)> set day=Monday
                         day = Monday (uncommitted)
dory:maintenance workflow-002 schedule (uncommitted)> set hour=13
                        hour = 13 (uncommitted)
dory:maintenance workflow-002 schedule (uncommitted)> set minute=15
                      minute = 15 (uncommitted)
dory:maintenance workflow-002 schedule (uncommitted)> commit
dory:maintenance workflow-002 schedules> list
NAME                 FREQUENCY            DAY                  HH:MM
schedule-001         day                              -                       10:05
schedule-002         week                     Monday               13:15
dory:maintenance workflow-002 schedules>
```

Cada entrada del programa tiene las siguientes propiedades:

TABLA 16-10 Propiedades de programa

Propiedad	Tipo	Descripción
`NAME`	String	Nombre del programa, generado por el sistema.
`frequency`	String	Minuto, media hora, hora, día, semana, mes.
`day`	String	Especifica el día y se puede configurar con los valores: Monday, Tuesday, Wednesday, Thursday, Friday, Saturday o Sunday (lunes, martes, miércoles, jueves, viernes, sábado o domingo). Se puede configurar cuando la frecuencia es semanal o mensual.
`hour`	String	00-23; especifica la parte correspondiente a la hora del programa y se puede configurar cuando la frecuencia es diaria, semanal o mensual.
`minute`	String	00-59; especifica la parte correspondiente a los minutos del programa.

Codificación del programa

Los programas también se pueden especificar en el código del flujo de trabajo como propiedad del objeto "workflow". La sintaxis usada para las propiedades difiere de la utilizada para crear el programa en la CLI. Aquí se utilizan tres propiedades:

TABLA 16-11 Propiedades de programa

Propiedad	Tipo	Descripción
`offset`	Number	Determina el punto inicial del período definido.
`period`	Number	Define la frecuencia del programa.
`unit`	String	Especifica si se utilizan segundos o meses como unidad en la definición del período y el desplazamiento.

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 del objeto "MySchedules" especifican el tipo de unidades utilizado para las propiedades "offset" y "period". Se pueden configurar con el valor de segundos o mes. La propiedad "period" especifica la frecuencia del evento, mientras que

"offset" especifica las unidades dentro del período. En el ejemplo anterior, el período del segundo programa está definido para una semana, a partir del segundo día, a las 4:30. 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 recurrencias del programa, que también se expresa en las unidades definidas por la propiedad "units."
- units: se puede definir en segundos o meses.

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 un jueves.

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 am. El programa tiene una recurrencia semanal indefinida cada sábado a las 4:30 am. A continuación se puede ver el programa como se lo visualiza en la CLI.

```
<small>dory:> maintenance workflows
dory:maintenance workflows> list
WORKFLOW     NAME                        OWNER SETID ORIGIN               VERSION
workflow-000 Configure for Oracle Solaris Cluster NFS root  false Oracle Corporation   1.0.0
workflow-001 Unconfigure Oracle Solaris Cluster NFS root  false Oracle Corporation   1.0.0
workflow-002 Configure for Oracle Enterprise Manager Monitoring root  false Sun Microsystems, Inc.
 1.1
workflow-003 Unconfigure Oracle Enterprise Manager Monitoring root  false Sun Microsystems, Inc.
 1.0</small>
```

dory:maintenance workflow-002 schedules>

```
NAME                FREQUENCY           DAY                 HH:MM
schedule-000        halfhour            -                   --:00
schedule-001        week                Saturday            04:30
```

Ejemplo: selección de tipo de dispositivo

El siguiente ejemplo es un flujo de trabajo que crea una hoja de trabajo basada en un tipo de unidad especificada:

```
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 ../..');
```

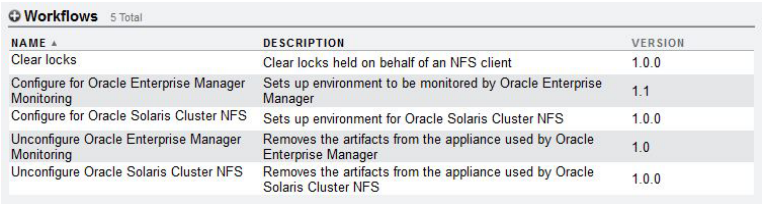
```
 }

 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); }
};
```

BUI

Para cargar los flujos de trabajo en el dispositivo ZFSSA, haga clic en el ícono del signo más; para ejecutarlos, haga clic en la fila en la que se especifica el flujo de trabajo.

FIGURA 16-1



CLI

Los flujos de trabajo se manipulan en la sección `maintenance workflows` de la CLI.

Descarga de flujos de trabajo

Los flujos de trabajo se descargan al dispositivo ZFSSA mediante el comando `download`, que es similar al "Sistema" de "Manual de servicio del cliente de Oracle ZFS Storage Appliance ":

```
dory:maintenance workflows> download
dory:maintenance workflows download (uncommitted)> get
                          url = (unset)
                         user = (unset)
                     password = (unset)
```

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.

```
dory:maintenance workflows download (uncommitted)> set url=
   ftp://foo/example1.akwf
                          url = ftp://foo/example1.akwf
dory:maintenance workflows download (uncommitted)> set user=bmc
                         user = bmc
dory:maintenance workflows download (uncommitted)> set password
Enter password:
                     password = ********
dory:maintenance workflows download (uncommitted)> commit
Transferred 138 of 138 (100%) ... done
```

Visualización de flujos de trabajo

Para ver una lista de los flujos de trabajo, use el comando `list` desde el contexto `maintenance workflows`:

```
<small>dory:maintenance workflows> list
WORKFLOW     NAME                        OWNER SETID ORIGIN               VERSION
workflow-000 Configure for Oracle Solaris Cluster NFS root  false Oracle Corporation   1.0.0
workflow-001 Unconfigure Oracle Solaris Cluster NFS root  false Oracle Corporation   1.0.0
workflow-002 Configure for Oracle Enterprise Manager Monitoring root  false Sun Microsystems, Inc.
 1.1
workflow-003 Unconfigure Oracle Enterprise Manager Monitoring root  false Sun Microsystems, Inc.
 1.0</small>
```

Para ver una lista de los flujos de trabajo, use el comando `show` desde el contexto `maintenance workflows`:

```
dory:maintenance workflows> select workflow-001
dory:maintenance workflow-001> show
Properties:
                          name = Configure for Oracle Solaris Cluster NFS
                   description = Sets up environment for Oracle Solaris Cluster NFS
                         owner = root
                        origin = Oracle Corporation
                         setid = false
                         alert = false
                       version = 1.0.0
                     scheduled = false
```

Para seleccionar un flujo de trabajo, use el comando `select`:

```
dory:maintenance workflows> select workflow-000
dory:maintenance workflow-000>
```

Para obtener las propiedades de un flujo de trabajo, use el comando `get` desde el contexto del flujo de trabajo seleccionado:

```
dory:maintenance workflow-000> get
```

```
        name = Hello world
 description = Bids a greeting to the world
       owner = root
      origin = <local>
       setid = false
       alert = false
   scheduled = false
```

Ejecución de flujos de trabajo

Para ejecutar un flujo de trabajo, use el comando `execute` desde el contexto del flujo de trabajo seleccionado. Si el flujo de trabajo no tiene parámetros, simplemente se ejecutará:

```
dory:maintenance workflow-000> execute
hello world!
```

Si el flujo de trabajo tiene parámetros, el contexto pasará a ser un contexto cautivo en el que se deben especificar los parámetros:

```
dory:maintenance workflow-000> execute
dory:maintenance workflow-000 execute (uncommitted)> get
                        type = (unset)
                   overwrite = (unset)
```

Todo intento de confirmar la ejecución del flujo de trabajo sin antes haber definido los parámetros requeridos generará un fallo explícito:

```
dory:maintenance workflow-000 execute (uncommitted)> commit
error: cannot execute workflow without setting property "type"
```

Para ejecutar el flujo de trabajo, defina los parámetros especificados y, a continuación, use el comando `commit`:

```
dory:maintenance workflow-000 execute (uncommitted)> set type=system
                        type = system
dory:maintenance workflow-000 execute (uncommitted)> set overwrite=true
                   overwrite = true
dory:maintenance workflow-000 execute (uncommitted)> commit
```

Si el flujo de trabajo tiene pasos especificados, se mostrarán mediante la CLI, por ejemplo:

```
dory:maintenance workflow-000 execute (uncommitted)> commit
Checking for existing worksheet ... done
Finding disks of specified type ... done
Creating worksheet ... done
```

♦ ♦ ♦ CAPÍTULO 17

Integración

Los dispositivos Oracle ZFS Storage Appliance ofrecen un conjunto completo de protocolos de datos para comunicarse con una amplia variedad de hosts de aplicaciones. Para mejorar el rendimiento de la aplicación o integrarla de manera más estrecha a su entorno de aplicación, siga las mejores prácticas descriptas en Resúmenes de soluciones y notas del producto que se encuentra en la página de documentación de almacenamiento NAS.

- “Symantec DMP/Storage Foundation”

Para algunas aplicaciones, la instalación del software en el host de la aplicación mejora la interoperabilidad. Los siguientes artículos ofrecen una descripción general de la manera en que la integración del software puede proporcionar una mejor experiencia para los administradores de almacenamiento. Cada descarga contiene un paquete con la documentación completa.

- “Sun ZFS Storage Appliance Plug-in for Oracle Solaris Cluster Geographic Edition” [498]
- “Complemento de sistema de archivos de red de dispositivo Sun ZFS Storage para Oracle Solaris Cluster” [498]
- “Sun ZFS Storage Appliance Provider For Volume Shadow Copy Service Software” [501]
- “Sun ZFS Storage Management Plug-In for Oracle Enterprise Manager Grid Controller” [499]
- “Oracle Virtual Machine Storage Connect Plug-in for the Sun ZFS Storage Appliance” [501]
- “Sun ZFS Storage 7000 Storage Replication Adapter for VMware Site Recovery Manager” [503]
- “ Oracle Intelligent Storage Protocol ” [497]

El dispositivo se ha diseñado además de manera exclusiva para integrarse sin problemas con otros productos de Oracle. Por ejemplo, en las siguientes secciones, se describe cómo configurar Sun ZFS Storage Appliance como destino de copia de seguridad para Oracle Exadata Database Machine y Oracle SPARC SuperCluster.

- “Copia de seguridad de Oracle Exadata Database Machine” [464]
- “Configuración de Oracle SPARC SuperCluster para copia de seguridad con ZFS Storage Appliance” [493]

Para obtener más información, visite la página de documentación de almacenamiento NAS.

Copia de seguridad de Oracle Exadata Database Machine

Cuando está equipado con QDR InfiniBand nativo y opciones de conectividad Ethernet de 10 Gb, el dispositivo ZFS Storage Appliance es ideal para realizar copias de seguridad de Oracle Exadata de manera confiable. Se proporciona el producto Oracle Exadata Backup Configuration Utility para su implementación mediante una herramienta de línea de comandos, o bien, se puede configurar el dispositivo en forma manual con las instrucciones de las siguientes secciones:

- “Configuración manual de un dispositivo Sun ZFS Storage Appliance” [464]
- “Configuración de Oracle Exadata para un dispositivo Sun ZFS Storage Appliance” [468]

La utilidad incluye la documentación completa, incluidas las instrucciones sobre cómo ejecutar una copia de seguridad desde Oracle Exadata. Independientemente de que se realice en forma manual o mediante la utilidad, la configuración de las agrupaciones de almacenamiento y la conexión de red en el dispositivo es necesaria para cualquier de los dos métodos.

Para obtener más información sobre cómo utilizar el dispositivo ZFS Storage Appliance como destino de copia de seguridad para Oracle Exadata, consulte las notas del producto Protección de Oracle Exadata mediante el dispositivo Sun ZFS Storage Appliance: mejores prácticas de configuración, en la página de documentación de almacenamiento NAS. También está disponible el cluster Oracle ZFS Storage ZS3-4, que se ofrece ya montado en el bastidor con estantes de discos como el dispositivo Oracle ZFS Storage ZS3-BA para minimizar la complejidad de instalación. La integración de este dispositivo con Oracle Exadata es idéntica al proceso descrito anteriormente.

Configuración manual de un dispositivo Sun ZFS Storage Appliance

En esta sección, se brindan las directrices generales para configurar manualmente un dispositivo ZFS Storage Appliance para usar con Oracle Exadata. Para obtener información detallada, consulte las notas del producto Protección de Oracle Exadata mediante el dispositivo Sun ZFS Storage Appliance: mejores prácticas de configuración, en la página de documentación de almacenamiento NAS.

Configuración de redes, agrupaciones y recursos compartidos

En las siguientes secciones, se resumen las mejores prácticas para optimizar las configuraciones de redes, agrupaciones de almacenamiento y recursos compartidos de ZFS Storage Appliance para admitir las operaciones de copia de seguridad y restauración.

Configuración de red

En esta sección, se describe cómo configurar los grupos de rutas múltiples de red IP (IPMP) y cómo configurar el enrutamiento en el dispositivo ZFS Storage Appliance.

Nota: Si ha utilizado Oracle Exadata Backup Configuration Utility, configure la red según se describe en esta sección. Para obtener más información, consulte las notas del producto Mejores prácticas.

Para los clientes que buscan mayor conectividad IB, se pueden instalar y configurar más HCA IB. Para obtener más información, consulte la Guía de instalación de Oracle ZFS Storage Appliance.

Los principios de esta sección se pueden aplicar a una implementación Ethernet de 10 Gb al aplicar la configuración de red a las interfaces ixgbe en lugar de las interfaces ibp. La implementación Ethernet de 10Gb se puede configurar como IPMP activa/activa. Si el dispositivo ZFS Storage Appliance está en una subred distinta de Oracle Exadata, podría ser necesario crear rutas estáticas de ZFS Storage Appliance a Oracle Exadata. Para obtener más información, consulte al administrador de la red.

▼ Configuración de red básica

1. **Asegúrese de que el dispositivo ZFS Storage Appliance esté conectado a Oracle Exadata.**
2. **Configure `ibp0`, `ibp1`, `ibp2` y `ibp3` con dirección `0.0.0.0/8` (necesario para IPMP), modo conectado y clave de partición `ffff`. Para identificar la clave de partición utilizada por el sistema Oracle Exadata, ejecute el siguiente comando como usuario root:
`# cat /sys/class/net/ib0/pkey`.**
3. **Configure el grupo IPMP activo/en espera mediante `ibd0` y `ibd3`, con `ibd0` activo y `ibd3` en espera.**
4. **Configure el grupo IPMP activo/en espera mediante `ibd1` y `ibd2`, con `ibd2` activo y `ibd1` en espera.**

5. **Active el enrutamiento adaptable para garantizar que la carga del tráfico esté equilibrada correctamente cuando existen múltiples direcciones IP en la misma subred que son propiedad del mismo nodo principal. Esto ocurre después de que se produce un failover en el cluster.**

Configuración de agrupaciones

En esta sección, se describen las consideraciones de diseño necesarias para determinar la configuración de agrupaciones más adecuada para las operaciones de copia de seguridad y restauración de ZFS Storage Appliance for Oracle Recovery Manager (RMAN) basadas en los requisitos de rendimiento y protección de datos.

Nota: Si ha utilizado Oracle Exadata Backup Configuration Utility, configure la agrupación según se describe en esta sección. Para obtener más información, consulte las notas del producto Mejores prácticas.

El planificador del sistema debe considerar la protección de la agrupación en función de las siguientes directrices:

- Utilice la protección basada en la paridad para sistemas de uso general y de capacidad optimizada:
- * RAID-Z para protección contra fallos de una sola unidad en sistemas sujetos a cargas de trabajo aleatorias.
- * RAID-Z2 para protección contra fallos de dos unidades en sistemas con cargas de trabajo de transmisión solamente.
- Utilice el reflejo para un alto rendimiento con copias de seguridad aplicadas de manera incremental.
- Configure las agrupaciones en función de los requisitos de rendimiento:
- * Configure una única agrupación para sistemas de gestión optimizada.
- * Configure dos agrupaciones para sistemas de rendimiento optimizado. Los sistemas de dos agrupaciones se deben configurar utilizando la mitad de las unidades de cada bandeja.
- Configure la protección de los dispositivos de log:
- * Segmente los dispositivos de log para configuraciones de agrupaciones reflejadas y RAID-Z.
- * Refleje los dispositivos de log para configuraciones de agrupaciones RAID-Z2.

Nota: Si ha utilizado Oracle Exadata Backup Configuration Utility, pase al siguiente tema: “Configuración de Oracle Exadata para un dispositivo Sun ZFS Storage Appliance” [468].

Configuración de recursos compartidos

Las opciones predeterminadas de recursos compartidos de ZFS Storage Appliance proporcionan un buen punto de partida para las cargas de trabajo de uso general. Los recursos compartidos

de ZFS Storage Appliance se pueden optimizar para operaciones de copia de seguridad y restauración de Oracle RMAN de la siguiente manera:

- Cree un proyecto para almacenar todos los recursos compartidos relacionados con la copia de seguridad y la recuperación de una base de datos única. En el caso de una implementación de dos agrupaciones, cree dos proyectos, uno para cada agrupación.
- Configure los recursos compartidos que admiten las cargas de trabajo de copia de seguridad y restauración de Oracle RMAN con los siguientes valores:
- * Tamaño de registro de la base de datos (`recordsize`): 128kB
- * Desviación de escritura síncrona (`logbias`): Throughput (Rendimiento) (para el procesamiento de conjuntos de copia de seguridad y copias de imágenes) o Latency (Latencia) (para copias de seguridad aplicadas de manera incremental).
- * Uso del dispositivo de la caché (`secondary cache`): None (Ninguno) (para conjuntos de copia de seguridad) o All (Todos) (cuando se admiten copias de seguridad aplicadas de manera incremental u operaciones de clones de base de datos)
- * Compresión de datos (`compression`): Off (Apagado) para sistemas de rendimiento optimizado, LZJB o gzip-2 para sistemas de capacidad optimizada
- * Cantidad de recursos compartidos por agrupación: 1 para sistemas de gestión optimizada, 2 o 4 para sistemas de rendimiento optimizado

Se pueden aplicar opciones adicionales de configuración de recursos compartidos, como compresión o replicación de alto nivel `gzip`, a los recursos compartidos utilizados para admitir la copia de seguridad y restauración de Oracle Exadata, como mandato de requisitos del cliente.

Los clientes que implementen servicios de datos adicionales de ZFS Storage Appliance deben considerar llevar a cabo pruebas específicas de la implementación para verificar las implicancias de las desviaciones de las prácticas descritas anteriormente.

Configuración de Oracle RMAN y la instancia de Oracle Database

Oracle RMAN es un componente esencial para proteger el contenido de Oracle Exadata. Oracle RMAN se puede utilizar para generar conjuntos de copias de seguridad, copias de imágenes y copias de seguridad actualizadas incrementalmente de contenido de Oracle Exadata en dispositivos ZFS Storage Appliance. Para optimizar el rendimiento de las copias de seguridad de Oracle RMAN de Oracle Exadata a un dispositivo ZFS Storage Appliance, el administrador de la base de datos debe aplicar las siguientes mejores prácticas:

- Equilibrar la carga de los canales Oracle RMAN de manera uniforme en todos los nodos de la máquina de base de datos.
- Equilibrar la carga de los canales de Oracle RMAN de manera uniforme en todos los controladores y recursos compartidos del dispositivo ZFS Storage Appliance.

Para optimizar el almacenamiento en búfer del canal de Oracle RMAN al dispositivo ZFS Storage Appliance, puede ajustar los valores de diversos parámetros de instancia ocultos. En el caso de Oracle Database 11*g* versión 2, se pueden sintonizar los siguientes parámetros:

- Para el conjunto de copias de seguridad y restauración:
- * _backup_disk_bufcnt=64
- * _backup_disk_bufsz=1048576
- Para la copia de seguridad y restauración de copias de imágenes:
- * _backup_file_bufcnt=64
- * _backup_file_bufsz=1048576

Para obtener más información sobre la sintonización de estos parámetros y de parámetros equivalentes de versiones anteriores del software Oracle Database, consulte el ID del artículo 1072545.1: *Sintonización de rendimiento de RMAN mediante parámetros de memoria de búfer*) en http://support.oracle.com (http://support.oracle.com.).

Oracle Direct NFS (dNFS) es un cliente NFS de alto rendimiento que ofrece un rendimiento excepcional para las operaciones de copia de seguridad y restauración de Oracle RMAN. dNFS se debe configurar para aquellos clientes que buscan el máximo rendimiento para operaciones de copia de seguridad y restauración.

Pasos siguientes

"Configuración de Oracle Exadata para un dispositivo Sun ZFS Storage Appliance" [468]

Configuración de Oracle Exadata para un dispositivo Sun ZFS Storage Appliance

En esta sección, se incluyen secuencias de comandos de ejemplo, que muestran cómo conectar un dispositivo ZFS Storage Appliance a Oracle Exadata. Estas secuencias de comandos fueron diseñadas para admitir una base de datos denominada `dbname` en una configuración de dispositivo ZFS Storage Appliance de una agrupación y de dos agrupaciones.

Configuración de Oracle Exadata para un dispositivo Sun ZFS Storage Appliance

Pasos de implementación generales

Los pasos de implementación son los siguientes:

1. Configure la estructura del directorio (puntos de montaje) para montar los recursos compartidos en el host.
2. Actualice `/etc/fstab` para montar los recursos compartidos exportados del dispositivo ZFS Storage Appliance a los puntos de montaje adecuados.
3. Cree un servicio `init.d` para automatizar el proceso de montar y desmontar los recursos compartidos.
4. Actualice el archivo `oranfstab` para acceder a los recursos compartidos exportados del dispositivo ZFS Storage Appliance o configure el montaje en el inicio en `/etc/fstab`.
5. Monte los recursos compartidos en el host.
6. Cambie los permisos de los recursos compartidos montados para hacerlos coincidir con la configuración de permisos de `ORACLE_HOME`.
7. De manera opcional, reinicie la instancia de Oracle Database para aplicar los cambios del archivo `oranfstab`.

Nota: Si ha utilizado Oracle Exadata Backup Configuration Utility, ya se han realizado automáticamente todos los pasos, excepto los pasos 4 y 7. En la sección siguiente, "Pasos de implementación detallados," tiene la opción de llevar a cabo la Actualización de oranfstab para acceder a las exportaciones del dispositivo Sun ZFS Storage Appliance y el paso 2 de Configuración de la propiedad de los recursos compartidos montados.

Pasos de implementación detallados

Temas de esta sección:

- Configuración de la estructura de directorio para montar los recursos compartidos en el host
- Actualización del archivo /etc/fstab
- Creación de un servicio init.d
- Actualización de oranfstab para acceder a las exportaciones de ZFS Storage Appliance
- Montaje de los recursos compartidos en el host
- Configuración de la propiedad de los recursos compartidos montados

Configuración de la estructura de directorio para montar los recursos compartidos en el host

Configure los puntos de montaje de los recursos compartidos en el host como se muestra a continuación:

```
mkdir -p /zfssa/dbname/backup1
mkdir -p /zfssa/dbname/backup2
mkdir -p /zfssa/dbname/backup3
mkdir -p /zfssa/dbname/backup4
```

Actualización del archivo /etc/fstab

Para actualizar el archivo `/etc/fstab`, utilice una de las siguientes opciones.

Nota: El carácter de escape de nueva línea de UNIX (\) indica que una única línea de código se ha ajustado a una segunda línea en el listado a continuación. Cuando introduzca una línea ajustada a `fstab`, elimine el carácter \ y combine los dos segmentos de línea, separados por un espacio, en una única línea.

Para una configuración de una agrupación:

```
192.168.36.200:/export/dbname/backup1 /zfssa/dbname/backup1 nfs \<br/>
 rw,bg,hard,nointr,rsize=1048576,wsize=1048576,tcp,nfsvers= \<br/>   3,timeo=600 0 0
192.168.36.200:/export/dbname/backup2 /zfssa/dbname/backup2 nfs \<br/>
 rw,bg,hard,nointr,rsize=1048576,wsize=1048576,tcp,nfsvers= \<br/>   3,timeo=600 0 0
192.168.36.200:/export/dbname/backup3 /zfssa/dbname/backup3 nfs \<br/>
 rw,bg,hard,nointr,rsize=1048576,wsize=1048576,tcp,nfsvers= \<br/>   3,timeo=600 0 0
192.168.36.200:/export/dbname/backup4 /zfssa/dbname/backup4 nfs \<br/>
 rw,bg,hard,nointr,rsize=1048576,wsize=1048576,tcp,nfsvers= \<br/>   3,timeo=600 0 0
```

Para una configuración de dos agrupaciones:

```
192.168.36.200:/export/dbname/backup1 /zfssa/dbname/backup1 nfs \<br/>
 rw,bg,hard,nointr,rsize=1048576,wsize=1048576,tcp,nfsvers= \<br/>   3,timeo=600 0 0
192.168.36.201:/export/dbname/backup2 /zfssa/dbname/backup2 nfs \<br/>
 rw,bg,hard,nointr,rsize=1048576,wsize=1048576,tcp,nfsvers= \<br/>   3,timeo=600 0 0
192.168.36.200:/export/dbname/backup3 /zfssa/dbname/backup3 nfs \<br/>
 rw,bg,hard,nointr,rsize=1048576,wsize=1048576,tcp,nfsvers= \<br/>   3,timeo=600 0 0
192.168.36.201:/export/dbname/backup4 /zfssa/dbname/backup4 nfs \<br/>
 rw,bg,hard,nointr,rsize=1048576,wsize=1048576,tcp,nfsvers= \<br/>   3,timeo=600 0 0
```

Creación de un servicio init.d

Cree un servicio init.d mediante la siguiente opción adecuada.

```
# !/bin/sh
#
# zfssa_dbname: Mount ZFSSA project dbname for database dbname
#
# chkconfig: 345 61 19
# description: mounts ZFS Storage Appliance shares
#


start()
{
  mount /zfssa/dbname/backup1
  mount /zfssa/dbname/backup2
  mount /zfssa/dbname/backup3
  mount /zfssa/dbname/backup4
```

```
  echo "Starting $prog: "
}


stop()
{
  umount /zfssa/dbname/backup1
  umount /zfssa/dbname/backup2
  umount /zfssa/dbname/backup3
  umount /zfssa/dbname/backup4
  echo "Stopping $prog: "
}


case "$1" in
  start)
     start
     ;;
  stop)
     stop
     ;;
  restart)
     stop
     start
     ;;
  status)
     mount
     ;;
   *)
      echo "Usage: $0 {start|stop|restart|status}"
     exit 1
esac
```

(Opcional) Active el servicio `init.d` para el inicio al iniciar; para ello, introduzca:

```
# chkconfig zfssa_dbname on
```

(Opcional) Inicie y detenga el servicio manualmente con los comandos de servicio:

```
# service zfssa_dbname start<br/># service zfssa_dbname stop
```

Actualización de oranfstab para acceder a las exportaciones de ZFS Storage Appliance

Para actualizar el archivo `oranfstab` para acceder a las exportaciones del dispositivo ZFS Storage Appliance, utilice la siguiente opción adecuada.

Nota: Si ha utilizado Oracle Exadata Backup Configuration Utility, tiene la opción de llevar a cabo este procedimiento.

Para una configuración de una agrupación:

```
server: 192.168.36.200
path: 192.168.36.200
export: /export/dbname/backup1 mount: /zfssa/dbname/backup1
export: /export/dbname/backup2 mount: /zfssa/dbname/backup2
export: /export/dbname/backup3 mount: /zfssa/dbname/backup3
export: /export/dbname/backup4 mount: /zfssa/dbname/backup4
```

Para una configuración de dos agrupaciones:

```
server: 192.168.36.200
path: 192.168.36.200
export: /export/dbname/backup1 mount: /zfssa/dbname-2pool/backup1
export: /export/dbname/backup3 mount: /zfssa/dbname-2pool/backup3
server: 192.168.36.201
path: 192.168.36.201
export: /export/dbname/backup2 mount: /zfssa/dbname-2pool/backup2
export: /export/dbname/backup4 mount: /zfssa/dbname-2pool/backup4
```

Montaje de los recursos compartidos en el host

Para montar los recursos compartidos en el host, introduzca una de las siguientes dos opciones:

```
# service mount_dbname start
```

O

```
# dcli -l root -g /home/oracle/dbs_group service mount_dbname start
```

Configuración de la propiedad de los recursos compartidos montados

Cambie la configuración de permisos de los recursos compartidos montados para hacerlos coincidir con la configuración de permisos de `ORACLE_HOME`. En este ejemplo, las propiedades de usuario y grupo están configuradas como `oracle:dba`.

Nota: Si ha utilizado Oracle Exadata Backup Configuration Utility, tiene la opción de llevar a cabo el paso 2; el paso 1 ya se ha realizado automáticamente.

1. Introduzca una de las siguientes dos opciones:
`# chown oracle:dba /zfssa/dbname/*`
o
`# dcli -l root -g /home/oracle/dbs_group chown oracle:dba/zfssa/dbname/*`.
2. Reinicie la instancia de Oracle Database para aplicar los cambios realizados en el archivo `oranfstab` mediante una de las siguientes opciones:

- Reinicie una instancia a la vez (actualización gradual), por ejemplo:

- :$ srvctl stop instance -d dbname -i dbname1
- :$ srvctl start instance -d dbname -i dbname1
- :$ srvctl stop instance -d dbname -i dbname2
- :$ srvctl start instance -d dbname -i dbname2
- :$ srvctl stop instance -d dbname -i dbname3
- :$ srvctl start instance -d dbname -i dbname3
- :$ srvctl stop instance -d dbname -i dbname4
- :$ srvctl start instance -d dbname -i dbname4
- :$ srvctl stop instance -d dbname -i dbname5
- :$ srvctl start instance -d dbname -i dbname5
- :$ srvctl stop instance -d dbname -i dbname6
- :$ srvctl start instance -d dbname -i dbname6
- :$ srvctl stop instance -d dbname -i dbname7
- :$ srvctl start instance -d dbname -i dbname7
- :$ srvctl stop instance -d dbname -i dbname8
- :$ srvctl start instance -d dbname -i dbname8
- Reinicie toda la base de datos, por ejemplo:
- :$ srvctl stop database -d dbname
- :$ srvctl start database -d dbname

Copia de seguridad de Oracle SPARC SuperCluster

Cuando está equipado con QDR InfiniBand nativo y opciones de conectividad Ethernet de 10 Gb, el dispositivo ZFS Storage Appliance es ideal para realizar copias de seguridad de Oracle SPARC SuperCluster. Use las instrucciones de las siguientes secciones para configurar el sistema:

- “Configuración del dispositivo ZFS Storage Appliance para copias de seguridad”
- “Configuración de Oracle SPARC SuperCluster para copia de seguridad con ZFS Storage Appliance”

Para obtener información detallada acerca del uso del dispositivo ZFS Storage Appliance como destino de copia de seguridad para Oracle SPARC SuperCluster, consulte la documentación técnica Configuración de dispositivos Sun ZFS Backup Appliance con Oracle SPARC SuperCluster en la página de documentación de almacenamiento NAS. También está disponible el cluster Oracle ZFS Storage ZS3-4, que se ofrece ya montado en el bastidor con estantes de discos como el dispositivo Oracle ZFS Storage ZS3-BA para minimizar la complejidad de instalación. La integración de este dispositivo con Oracle SPARC SuperCluster es idéntica al proceso descrito anteriormente.

Configuración de dispositivos ZFS Storage Appliance para copias de seguridad

En esta sección, se brindan las directrices generales para configurar un dispositivo ZFS Storage Appliance para usar en copias de seguridad con Oracle SPARC SuperCluster. Para obtener información detallada, consulte la documentación técnica Configuración de dispositivos Sun ZFS Backup Appliance con Oracle SPARC SuperCluster en la página de documentación de almacenamiento NAS. Los ejemplos representan un dispositivo ZFS Storage Appliance con dos controladores (cabezales) y cuatro estantes de discos.

Temas de esta sección:

Configuración de enlaces de datos InfiniBand en dispositivos ZFS Storage Appliance

Los pasos detallados en esta sección permiten configurar cada una de las conexiones InfiniBand del dispositivo ZFS Storage Appliance. Los ocho GUID correspondientes a los puertos InifiniBand del HBA que se registran durante este procedimiento se usan para configurar los conmutadores InfiniBand de Oracle SPARC SuperCluster en el siguiente procedimiento.

1. Conecte el dispositivo ZFS Storage Appliance con Oracle SPARC SuperCluster como se describe en el documento técnico Configuración de dispositivos Sun ZFS Backup Appliance con Oracle SPARC SuperCluster en la página de documentación de almacenamiento NAS.

2. Inicie sesión en la interfaz de usuario basada en explorador (BUI) del cabezal 1 y navegue hasta Configuration (Configuración) > Network (Red).

3. Haga clic en el ícono más junto a Enlaces de datos. Se abre el cuadro de diálogo Network Datalink (Enlace de datos de red).

4. Complete el cuadro de diálogo del siguiente modo:

- Seleccione la casilla `IB Partition` (Partición de IB).
- Introduzca un nombre significativo para el enlace de datos.
- Configure `Partition Key` (Clave de partición) con el valor `8503`.
- En Link Mode (Modo de enlace), seleccione Connected Mode (Modo conectado).
- No seleccione la casilla `LACP Aggregation` (Agregación de LACP).
- Seleccione `Partition Device` `ibp0`.
- Tome nota del número de GUID (por ejemplo, `21280001ef43bb`) y haga clic en Apply (Aplicar).

5. Repita los pasos 3 y 4 para cada una de las interfaces de InfiniBand restantes (`ibp1`, `ibp2` y `ibp3`).

6. Repita los pasos 2 a 5 para el cabezal 2.

Configuración de los conmutadores InfiniBand de Oracle SPARC SuperCluster para agregar el dispositivo ZFS Storage Appliance

En este procedimiento, se agregan los GUID de los puertos InifiniBand del HBA de ZFS Storage Appliance a la configuración de InfiniBand existente de Oracle SPARC SuperCluster. Al agregar estos puertos y usar la clave de partición 8503, se puede establecer la comunicación entre los dos dispositivos.

1. Inicie sesión en el conmutador de tapas InfiniBand de Oracle SPARC SuperCluster como root. De manera predeterminada, el conmutador de tapas recibe el nombre de host `<sscid>sw-ib1`, donde `<sscid>` es el nombre del prefijo asignado al sistema Oracle SPARC SuperCluster. En el siguiente ejemplo, `<sscid>` es `aiessc`.

```
login as: root
root@aiesscsw-ib1's password:
Last login: Tue Sep 25 08:19:01 2013 from dhcp-brm-bl5-204-3e
```

```
east-10-135-75-254.usdhcp.oraclecorp.com
```

2. Introduzca el comando `enablesm` para verificar que el conmutador esté ejecutando el gestor de subred (si no se está ejecutando, el comando sirve para iniciarlo).

```
[root@aiesscsw-ib1 ~]# enablesm
opensm (pid 15906) is already running...
Starting partitiond daemon
/usr/local/util/partitiond is already running
(You may also perform a 'restart' if wanted)
```

3. Introduzca el comando `getmaster` para verificar que éste sea el conmutador maestro de la configuración. Si el conmutador maestro no se está ejecutando en el conmutador de tapas, cierre sesión e inicie sesión en el conmutador maestro designado para llevar a cabo el resto de este procedimiento.

```
[root@aiesscsw-ib1 ~]# getmaster
Local SM enabled and running
20130913 10:16:51 Master SubnetManager on sm lid 13 sm guid
0x2128e8ac27a0a0 : SUN DCS 36P QDR aiesscsw-ib1.us.oracle.com
[root@aiesscsw-ib1 ~]#
```

4. Use los procedimientos de copia de seguridad documentados (http://docs.oracle.com/cd/E26698_01/index.html (http://docs.oracle.com/cd/E26698_01/index.html)) para hacer la copia de seguridad de la configuración del conmutador.

5. Introduzca el comando `smpartition list active` para verificar que la clave de partición 0x0503 esté asignada al nombre de partición "sto" (`sto = 0x0503`).
 La clave de partición se configuró con el valor 8503 en los enlaces de datos del dispositivo ZFS Storage Appliance, pero el conmutador de InfiniBand indica 0503. Esto es intencional porque el protocolo InfiniBand reserva el bit más importante (0x8000) de la clave de partición (pkey) hexadecimal para su propio uso. Por lo tanto, las pkey 0x8503 y 0x0503 son iguales.

```
[root@aiesscsw-ib1 ~]# smpartition list active
# Sun DCS IB partition config file
# This file is generated, do not edit
#! version_number : 11
Default=0x7fff, ipoib : ALL_CAS=full, ALL_SWITCHES=full, SELF=
full;
SUN_DCS=0x0001, ipoib : ALL_SWITCHES=full;
ic1s10 = 0x0501,ipoib,defmember=full:
0x0021280001ef30f7,
0x0021280001ef33bf,
0x0021280001ef30b7,
0x0021280001ef314b;
ic2s10 = 0x0502,ipoib,defmember=full:
0x0021280001ef30f8,
0x0021280001ef33c0,
0x0021280001ef30b8,
0x0021280001ef314c;
sto = 0x0503,ipoib,defmember=full:
0x0021280001ef43f8,
```

```
0x0021280001ef43b7,
0x0021280001cf90c0,
0x0021280001ef43bb,
...more...
```

6. Agregue el dispositivo ZFS Storage Appliance a la configuración de InfiniBand:

- Introduzca el comando `smpartition start` para iniciar una sesión de reconfiguración.

```
# smpartition start<br/>
[root@aiesscsw-ib1 ~]# smpartition start
```

- Introduzca el comando `smpartition add` para agregar los ocho nuevos GUID a la configuración.

```
# smpartition add -n sto -port <GUID1> <GUID2> <GUID3> ...  <GUID8><br/>
[root@aiesscsw-ib1 ~]# smpartition add -n sto -port
21280001ef43bb 21280001ef43bc 21280001cf90bf 21280001cf90c0
21280001ef43f7 21280001ef43f8 21280001ef43b7 21280001ef43b8
```

- Introduzca el comando `smpartition list modified` para verificar que los nuevos GUID se hayan agregado correctamente.

```
# smpartition list modified<br/>
[root@aiesscsw-ib1 ~]# smpartition list modified
# Sun DCS IB partition config file
<nowki># This file is generated, do not edit
#! version_number : 11
Default=0x7fff, ipoib : ALL_CAS=full, ALL_SWITCHES=full, SELF=
full;
SUN_DCS=0x0001, ipoib : ALL_SWITCHES=full;
ic1s10 = 0x0501,ipoib,defmember=full:
0x0021280001ef30f7,
0x0021280001ef33bf,
0x0021280001ef30b7,
0x0021280001ef314b;
ic2s10 = 0x0502,ipoib,defmember=full:
0x0021280001ef30f8,
0x0021280001ef33c0,
0x0021280001ef30b8,
0x0021280001ef314c;
sto = 0x0503,ipoib,defmember=full:
0x0021280001ef43f8,
0x0021280001ef43b7,
0x0021280001cf90c0,
0x0021280001ef43bb,
0x0021280001ef43bc,
0x0021280001cf90bf,
0x0021280001ef43b8,
0x0021280001ef43f7,
0x0021280001ef3048,
0x0021280001ef30af,
```

```
0x0021280001ef30f8,
0x0021280001ef30f7,
0x0021280001ef33c0,
0x0021280001ef33bf,
0x0021280001ef30cc,
0x0021280001ef342b,
0x0021280001ef30b8,
0x0021280001ef30b7,
0x0021280001ef314c,
0x0021280001ef314b,
0x0021280001efec65,
0x0021280001efec66,
0x0021280001efecb1,
0x0021280001efecb2;
```

- Introduzca el comando `smpartition commit` para aplicar la nueva configuración y propagar los cambios de configuración a todos los conmutadores InfiniBand de la configuración.

```
# smpartition commit<br/>
[root@aiesscsw-ib1 ~]# smpartition commit
[root@aiesscsw-ib1 ~]#
```

7. Cierre la sesión del conmutador InfiniBand.

8. Use los procedimientos de copia de seguridad documentados (http://docs.oracle.com/cd/E26698_01/index.html (http://docs.oracle.com/cd/E26698_01/index.html)) para hacer la copia de seguridad de la configuración de InfiniBand.

Configuración de la red del dispositivo ZFS Storage Appliance para conexión mediante una única dirección IP

Esta configuración se utiliza solamente con sistemas Oracle SPARC SuperCluster T5 sin conmutadores de hoja externos. Para obtener el mejor rendimiento y failover posibles, use la configuración activo-activo (sección siguiente) para todas las demás configuraciones.

Configure los puertos InfiniBand del dispositivo ZFS Storage Appliance para conectividad de red y failover simple en el cluster; para ello, use el siguiente procedimiento para configurar el puerto 1 con la dirección IP deseada.

1. Inicie sesión en la BUI del cabezal 1 y navegue hasta Configuration (Configuración) > Network (Red).

2. Haga clic en el ícono más junto a Interfaces. Se abre el cuadro de diálogo Network Interface (Interfaz de red).

3. Complete el cuadro de diálogo del siguiente modo:

- Introduzca un nombre significativo para la interfaz de red.
- Verifique que esté seleccionada la opción `Enable Interface` (Activar interfaz).
- Verifique que esté seleccionada la opción `Allow Administration` (Permitir administración).
- Verifique que esté seleccionada la opción `Use IPv4 Protocol` (Usar protocolo IPv4).
- Verifique que la selección del menú `Configure with` (Configurar con) sea `Static Address List` (Lista de direcciones estáticas).
- En el cuadro que se encuentra debajo, introduzca la dirección IP deseada con la máscara de red apropiada.
- Verifique que no esté seleccionada la opción `Use IPv6 Protocol` (Usar protocolo IPv6).
- Seleccione el enlace de datos para `ibp0` y haga clic en Apply (Aplicar).

4. Repita los pasos 1 a 3 en el cabezal 2 con `ibp2` como enlace de datos.

Configuración de la red del dispositivo ZFS Storage Appliance para configuraciones activo-activo

Configure los puertos InfiniBand del dispositivo ZFS Storage Appliance para rutas múltiples de IP. Se necesitan cuatro direcciones IP, en la subred de almacenamiento privada, para cada cabezal del dispositivo ZFS Storage Appliance (por lo tanto, se necesitan ocho direcciones en total) porque las interfaces ejecutan una configuración activo-activo.

1. Configure cada enlace de datos de InfiniBand como su propia interfaz de red.

- Inicie sesión en la BUI del cabezal 1 y navegue hasta Configuration (Configuración) > Network (Red).
- Haga clic en el ícono más junto a Interfaces. Se abre el cuadro de diálogo Network Interface (Interfaz de red).
- Complete el cuadro de diálogo del siguiente modo:
- * Introduzca un nombre significativo para la interfaz de red.
- * Verifique que esté seleccionada la opción `Enable Interface` (Activar interfaz).
- * Verifique que esté seleccionada la opción `Allow Administration` (Permitir administración).
- * Verifique que esté seleccionada la opción `Use IPv4 Protocol` (Usar protocolo IPv4).
- * Verifique que la selección del menú Configure with (Configurar con) sea Static Address List (Lista de direcciones estáticas).
- * En el cuadro que se encuentra debajo, introduzca `0.0.0.0/8`.
- * Verifique que no esté seleccionada la opción `Use IPv6 Protocol` (Usar protocolo IPv6).

- * Seleccione el enlace de datos para `ibp0` y haga clic en Apply (Aplicar).
- Repita los pasos 2 y 3 para cada uno de los enlaces de datos restantes (`ibp1`, `ibp2` y `ibp3`).
- Repita los pasos 1 a 4 para el cabezal 2.

2. Configure la interfaz IPMP en el cabezal 1.

- Inicie sesión en la BUI del cabezal 1 y navegue hasta Configuration (Configuración) > Network (Red).
- Haga clic en el ícono más junto a Interfaces. Se abre el cuadro de diálogo Network Interface (Interfaz de red).
- Complete el cuadro de diálogo del siguiente modo:
- * Introduzca un nombre significativo para la interfaz de red IPMP.
- * Verifique que esté seleccionada la opción `Enable Interface` (Activar interfaz).
- * Verifique que esté seleccionada la opción `Allow Administration` (Permitir administración).
- * Verifique que esté seleccionada la opción `Use IPv4 Protocol` (Usar protocolo IPv4).
- * Verifique que la selección del menú `Configure with` (Configurar con) sea `Static Address List` (Lista de direcciones estáticas).
- * Haga clic tres veces en el signo más que se encuentra al lado de la casilla vacía, de manera que aparezcan cuatro casillas vacías.
- * En cada casilla vacía, introduzca una de las direcciones IP reservadas para las conexiones InfiniBand con su designación de máscara de red /24 respectiva. Como práctica recomendada, no use direcciones IP consecutivas del bloque, es mejor ir salteándose una (por ejemplo, todas pares o todas impares).
- * Verifique que no esté seleccionada la opción `Use IPv6 Protocol` (Usar protocolo IPv6).
- * Seleccione la casilla `IP MultiPathing Group` (Grupo de rutas múltiples IP).
- * Seleccione las casillas que se encuentran al lado de las interfaces correspondientes a los enlaces de datos `ibp0` e `ibp3`.
- * Verifique que cada una de las dos interfaces esté configurada con el valor `Active` (Activo) y haga clic en Apply (Aplicar).
- Desde Configuration (Configuración) > Network (Red), haga clic en Routing (Enrutamiento).
- Haga clic en el modelo de multiorigen correspondiente a `Adaptive` (Adaptable).

3. Configure la interfaz IPMP en el cabezal 2.

- Inicie sesión en la BUI del cabezal 2 y navegue hasta Configuration (Configuración) > Network (Red).
- Haga clic en el ícono más junto a Interfaces. Se abre el cuadro de diálogo Network Interface (Interfaz de red).
- Complete el cuadro de diálogo del siguiente modo:
- * Introduzca un nombre significativo para la interfaz de red IPMP.

- * Verifique que esté seleccionada la opción `Enable Interface` (Activar interfaz).
- * Verifique que esté seleccionada la opción `Allow Administration` (Permitir administración).
- * Verifique que esté seleccionada la opción `Use IPv4 Protocol` (Usar protocolo IPv4).
- * Verifique que la selección del menú `Configure with` (Configurar con) sea `Static Address List` (Lista de direcciones estáticas).
- * Haga clic tres veces en el signo más que se encuentra al lado de la casilla vacía, de manera que aparezcan cuatro casillas vacías.
- * En cada casilla vacía, introduzca una de las cuatro direcciones IP restantes reservadas para las conexiones InfiniBand con su designación de máscara de red /24 respectiva. Deben ser las que no se usaron en el cabezal 1.
- * Verifique que no esté seleccionada la opción `Use IPv6 Protocol` (Usar protocolo IPv6).
- * Seleccione la casilla `IP MultiPathing Group` (Grupo de rutas múltiples IP).
- * Seleccione las casillas que se encuentran al lado de las interfaces correspondientes a los enlaces de datos `ibp1` e `ibp2`.
- * Verifique que cada una de las dos interfaces esté configurada con el valor `Active` (Activo) y haga clic en Apply (Aplicar).
- Desde Configuration (Configuración) > Network (Red), haga clic en Routing (Enrutamiento).
- Haga clic en el modelo de multiorigen correspondiente a `Adaptive` (Adaptable).

4. Verifique la conectividad con los nodos de Oracle SPARC SuperCluster. Verifique que cada uno de los nodos pueda hacer ping a cada una de las ocho direcciones usadas en los grupos IPMP del dispositivo ZFS Storage Appliance. Agregue estas direcciones IP a la tabla `/etc/inet/hosts` de cada nodo.

Configuración de la agrupación de almacenamiento del dispositivo ZFS Storage Appliance

La configuración de agrupaciones asigna recursos de unidades de disco físicas a agrupaciones de almacenamiento lógicas para almacenamiento de datos de copias de seguridad. Para maximizar el rendimiento del sistema, configure dos agrupaciones de almacenamiento de igual tamaño; para ello, asigne la mitad de las unidades físicas de cada una de las bandejas de unidades a cada agrupación de almacenamiento.

El software de gestión del dispositivo ZFS Storage Appliance presenta un mensaje de advertencia acerca de la eficiencia cuando se configuran dos agrupaciones con el mismo perfil de protección RAID. Si se está configurando para una solución de copia de seguridad de Oracle RMAN de alto rendimiento, se puede ignorar este mensaje.

Configuración de los recursos compartidos del dispositivo ZFS Storage Appliance

La configuración de recursos compartidos es el proceso de configurar y ejecutar los puntos de montaje de NFS para el acceso de los clientes. Se deben crear dos proyectos para la configuración de Oracle SPARC SuperCluster: un proyecto por agrupación. Un proyecto es una entidad que proporciona un punto de interfaz de gestión de nivel superior para un conjunto de recursos compartidos. Para optimizar la gestión de los recursos compartidos, actualice el punto de montaje predeterminado de los recursos compartidos incluidos en el proyecto de manera de hacer referencia al nombre de la base de datos, por ejemplo, `/export/dbname`. Para optimizar el rendimiento del sistema, cree cuatro recursos compartidos para cada proyecto en cada agrupación, lo que genera un total de ocho recursos compartidos (cuatro por cabezal). Para configurar un proyecto, haga lo siguiente:

1. Inicie sesión en la BUI del cabezal 1 y navegue hasta Shares (Recursos compartidos) > Projects (Proyectos).

2. Haga clic en el ícono del signo más que se encuentra al lado de Projects (Proyectos), introduzca un nombre significativo para el proyecto y, a continuación, haga clic en Apply (Aplicar). Como se creará un proyecto similar en el otro cabezal, asigne un nombre único al proyecto del cabezal 1, por ejemplo, `H1-mydb`.

3. Haga clic en el ícono del lápiz que se encuentra al lado del nombre del nuevo proyecto para editar el proyecto.

4. Haga clic en General y complete las propiedades de la siguiente manera:

- Cambie el parámetro `Mountpoint` (Punto de montaje) de manera de incluir el nombre de la base de datos (por ejemplo, `/export/H1-mydb`).
- Cambie el valor de `Synchronous write bias` (Desviación de escritura síncrona) de `Latency` (Latencia) a `Throughput` (Rendimiento) y haga clic en Apply (Aplicar).

5. Haga clic en Protocols (Protocolos) y agregue una excepción de NFS de la siguiente manera:

- Haga clic en el ícono más junto a NFS Exceptions (Excepciones de NFS).
- Cambie el valor de `Type` (Tipo) a `Network` (Red).
- Introduzca la subred y la máscara de red (por ejemplo, /24) de la red InfiniBand.
- Cambie el valor de `Access Mode` (Modo de acceso) a `Read/Write` (Lectura y escritura).
- Verifique que `Charset` (Juego de caracteres) esté configurado con el valor `default` (Predeterminado).
- Seleccione la casilla `Root Access` (Acceso root) y haga clic en Apply (Aplicar).

6. Haga clic en Shares (Recursos compartidos), al lado de General.

7. Cree cuatro sistemas de archivos para el cabezal 1 y asígneles nombres únicos para que sean diferentes de los nombres del cabezal 2. Para intercalar los flujos de copia de seguridad y

distribuir los datos entre los dos cabezales, lo que resulta en un mejor rendimiento, use nombres con números impares para el cabezal 1, por ejemplo, `backup1`, `backup3`, `backup5` y `backup7` y use nombres con números pares para el cabezal 2, por ejemplo, `backup2`, `backup4`, `backup6` y `backup8`. Para crear los sistemas de archivos, haga clic en el ícono del signo más que se encuentra al lados de Filesystems (Sistemas de archivos), introduzca el nombre del sistema de archivos (`backup1`) y haga clic en Apply (Aplicar). Repita este paso para crear los tres sistemas de archivos restantes (`backup3`, `backup5` y `backup7`).

8. Repita los pasos 2 a 7 para el cabezal 1. Recuerde usar un nombre de proyecto único (por ejemplo, `H2-mydb`) y especificar identificadores de copia de seguridad con números pares (`backup2`, `backup4`, `backup6` y `backup8`) para los nombres de los sistemas de archivos.

Configuración de análisis DTrace del dispositivo ZFS Storage Appliance

El dispositivo ZFS Storage Appliance incluye una herramienta de análisis de rendimiento completa llamada DTrace Analytics. DTrace Analytics es una estructura que supervisa estadísticas de contabilidad de rendimiento importantes del subsistema. Para proporcionar datos completos sobre la eficacia y el rendimiento de las cargas de trabajo de copia de seguridad y restauración de Oracle RMAN, se debe supervisar un subconjunto de las estadísticas de contabilidad disponibles.

Los siguientes análisis están disponibles si se configura la opción de análisis avanzados en el dispositivo ZFS Storage Appliance (Configuration [Configuración] > Preferences [Preferencias] > Enable Advanced Analytics [Activar análisis avanzado]):

- CPU: porcentaje de utilización desglosado por modo de CPU
- Disco: cantidad promedio de operaciones de E/S desglosadas por estado de operación
- Disco: bytes de E/S por segundo desglosados por tipo de operación
- Disco: operaciones de E/S por segundo desglosadas por latencia
- Disco: discos con utilización de al menos 95% desglosados por disco
- Red: bytes de interfaz por segundo desglosados por dirección
- Red: bytes de interfaz por segundo desglosados por interfaz
- Protocolo: operaciones de NFSv3 por segundo desglosadas por tamaño
- Protocolo: operaciones de NFSv3 por segundo desglosadas por tipo de operación
- Protocolo: operaciones de NFSv3 por segundo de tipo lectura desglosadas por latencia
- Protocolo: operaciones de NFSv3 por segundo de tipo escritura desglosadas por latencia
- Protocolo: operaciones de NFSv3 por segundo de tipo lectura desglosadas por tamaño
- Protocolo: operaciones de NFSv3 por segundo de tipo escritura desglosadas por tamaño

La implementación de estas estadísticas de contabilidad permite a los usuarios finales tener un conocimiento cuantitativo del consumo de recursos instantáneo e histórico y la calidad del servicio (QoS) correspondiente a su implementación específica.

Configuración de montajes de cliente NFS

Al configurar el dispositivo ZFS Storage Appliance, los servidores que tienen acceso al dispositivo, incluidos los nodos de Oracle SPARC SuperCluster, se consideran como clientes. La configuración del montaje de clientes NFS incluye la creación de la estructura de directorios de destino para acceder al dispositivo ZFS Storage Appliance, así como a las opciones específicas de montaje NFS necesarias para un rendimiento óptimo del sistema. Las opciones de montaje para los clientes Solaris son:

```
rw,bg,hard,nointr,rsize=1048576,wsize=1048576,proto=tcp,vers=3,forcedirectio
```

Los puntos de montaje de los directorios creados en el dispositivo ZFS Storage Appliance se deben crear en cada uno de los nodos de Oracle SPARC SuperCluster y se deben agregar a la tabla `/etc/inet/hosts` correspondiente.

Ajuste de la red y el núcleo de Solaris 11

Se deben agregar las siguientes entradas al archivo `/etc/system` de cada uno de los nodos de Oracle SPARC SuperCluster:

```
set rpcmod:clnt_max_conns = 8
set nfs:nfs3_bsize = 131072
```

Asimismo, se deben ejecutar los siguientes comandos en cada nodo de Oracle SPARC SuperCluster cada vez que se lo reinicie:

```
/usr/sbin/ndd -set /dev/tcp tcp_max_buf 2097152
/usr/sbin/ndd -set /dev/tcp tcp_xmit_hiwat 1048576
/usr/sbin/ndd -set /dev/tcp tcp_recv_hiwat 1048576
```

Puede ser necesario hacer ajustes adicionales para lograr un rendimiento óptimo. Consulte la información más reciente en el documento 1474401.1 de parámetros ajustables de Oracle SPARC SuperCluster, disponible en http://support.oracle.com (http://support.oracle.com). Además, la versión QFSDP de enero de 2013 agregó una herramienta "ssctuner" que configura automáticamente los parámetros ajustables. Consulte las notas de la versión de Oracle SPARC SuperCluster para obtener información adicional.

Configuración de Oracle Direct NFS (dNFS)

En cada nodo de Oracle SPARC SuperCluster, configure dNFS de la siguiente manera:

1. Cierre la instancia en ejecución del software de base de datos de Oracle.

2. Cambie el directorio a `$ORACLE_HOME/rdbms/lib`.

3. Active dNFS:

```
make -f $ORACLE_HOME/rdbms/lib/ins_rdbms.mk dnfs_on
```

4. Actualice el archivo `oranfstab` (se encuentra en `/$ORACLE_HOME/dbs`) con los nombres del servidor, la ruta y la exportación específicos para la configuración, donde:

- El parámetro server (Servidor) hace referencia al nombre local del cabezal del dispositivo ZFS Storage Appliance en la red InfiniBand.
- Los parámetros path (ruta) deben reflejar las direcciones correspondientes al cabezal especificado durante la configuración.
- Los parámetros export (exportar) deben reflejar los puntos de montaje similares a las entradas creadas en `/etc/vfstab`. Las entradas deben tener un aspecto similar al siguiente.

Para la configuración de IP única (sólo Oracle SPARC SuperCluster T5 sin conmutadores de hoja externos):

```
server: aie-zba-h1-stor
path: 192.168.30.100
export: /export/test1/backup1 mount: /zba/test1/backup1
export: /export/test1/backup3 mount: /zba/test1/backup3
export: /export/test1/backup5 mount: /zba/test1/backup5
export: /export/test1/backup7 mount: /zba/test1/backup7
server: aie-zba-h2-stor
path: 192.168.30.101
export: /export/test1/backup2 mount: /zba/test1/backup2
export: /export/test1/backup4 mount: /zba/test1/backup4
export: /export/test1/backup6 mount: /zba/test1/backup6
export: /export/test1/backup8 mount: /zba/test1/backup8<br/>
```

Para la configuración de grupos IPMP (todos los demás):

```
server: aie-zba-h1-stor
path: 192.168.30.100
path: 192.168.30.102
path: 192.168.30.104
path: 192.168.30.106
export: /export/test1/backup1 mount: /zba/test1/backup1
export: /export/test1/backup3 mount: /zba/test1/backup3
export: /export/test1/backup5 mount: /zba/test1/backup5
export: /export/test1/backup7 mount: /zba/test1/backup7
server: aie-zba-h2-stor
path: 192.168.30.101
path: 192.168.30.103
path: 192.168.30.105
path: 192.168.30.107
export: /export/test1/backup2 mount: /zba/test1/backup2
export: /export/test1/backup4 mount: /zba/test1/backup4
```

```
export: /export/test1/backup6 mount: /zba/test1/backup6
export: /export/test1/backup8 mount: /zba/test1/backup8
```

5. Reinicie la instancia del software de base de datos de Oracle.

Ajuste de la instancia de Oracle Database para copia de seguridad y restauración de Oracle RMAN

La optimización de las operaciones de copia de seguridad y restauración de ancho de banda alto con Oracle RMAN y el dispositivo ZFS Storage Appliance requiere el ajuste de los parámetros de la instancia que controla el almacenamiento en búfer de E/S. Para obtener información acerca del procedimiento para ajustar estos parámetros, consulte el artículo ID 1072545.1: Sintonización de rendimiento de RMAN mediante parámetros de memoria de búfer en http://support.oracle.com (http://support.oracle.com.).

Para Oracle SPARC SuperCluster, se debe considerar el ajuste de los siguientes cuatro parámetros:

- `_backup_disk_bufcnt`: cantidad de búferes utilizados para procesar conjuntos de copia de seguridad
- `_backup_disk_bufsz`: tamaño de los búferes utilizados para procesar conjuntos de copia de seguridad
- `_backup_file_bufcnt`: cantidad de búferes utilizados para procesar copias de imágenes
- `_backup_file_bufsz`: tamaño de los búferes utilizados para procesar copias de imágenes

Para las operaciones de copia de seguridad y restauración en conjuntos de copia de seguridad y copias de imágenes, configure la cantidad de búferes con el valor 64 y el tamaño de búfer con el valor 1 MB:

```
SQL> alter system set “_backup_disk_bufcnt”=64;
SQL> alter system set “_backup_file_bufcnt”=64;
SQL> alter system set “_backup_disk_bufsz”=1048576;
SQL> alter system set “_backup_file_bufsz”=1048576;
```

Estos comandos se pueden configurar de manera persistente, para lo que debe agregarlos a `SPFILE`, o se pueden definir de manera dinámica en el bloque de ejecución de Oracle RMAN utilizado para ejecutar las operaciones de copia de seguridad y restauración.

Los siguientes fragmentos de código muestran cómo ajustar los tamaños y las cantidades de búferes dinámicamente para las operaciones de copia de seguridad y restauración.

- Copia de seguridad de conjuntos de copia de seguridad:

```
run
{<br/>
   sql 'alter system set “_backup_disk_bufcnt”=64';<br/>
   sql 'alter system set “_backup_disk_bufsz”=1048576';<br/>
   allocate channel...
...<br/>
   backup as backupset database;
}
```

- Restauración de conjuntos de copia de seguridad:

```
run
{<br/>
   sql 'alter system set “_backup_disk_bufcnt”=64';<br/>
   sql 'alter system set “_backup_disk_bufsz”=1048576';<br/>
   allocate channel...
...<br/>
   restore database;
}
```

- Copia de seguridad de copia de imágenes:

```
run
{<br/>
   sql 'alter system set “_backup_file_bufcnt”=64';<br/>
   sql 'alter system set “_backup_file_bufsz”=1048576';<br/>
   allocate channel...
...<br/>
   backup as copy database;
}
```

- Restauración de copia de imágenes:

```
run
{<br/>
   sql 'alter system set “_backup_file_bufcnt”=64';<br/>
   sql 'alter system set “_backup_file_bufsz”=1048576';<br/>
   allocate channel...
...<br/>
   restore database;
}
```

Para realizar copias de seguridad aplicadas de manera incremental se requiere la lectura de un conjunto de copia de seguridad incremental y la escritura en una copia de imágenes. Para ajustar los búferes para copias de seguridad aplicadas de manera incremental, ejecute lo siguiente:

```
run
{<br/>
   sql 'alter system set “_backup_disk_bufcnt”=64';<br/>
   sql 'alter system set “_backup_disk_bufsz”=1048576';<br/>
   sql 'alter system set “_backup_file_bufcnt”=64';<br/>
   sql 'alter system set “_backup_file_bufsz”=1048576';<br/>
```

```
   allocate channel...
...<br/>
   recover copy of database;
}
```

Creación de servicios dedicados para operaciones de Oracle RMAN

Es posible configurar dos servicios dedicados al procesamiento de Oracle RMAN para optimizar la gestión del equilibrio de carga, la alta disponibilidad y las actualizaciones. La carga de estos servicios se puede distribuir de manera uniforme entre todos los nodos del sistema Oracle SPARC SuperCluster. Para optimizar la disponibilidad y el rendimiento, los servicios se deben configurar para ejecutarse en una instancia preferida y se los debe preparar para realizar failover a cualquiera de las instancias del cluster. Si se configuran estos servicios, la actualización de la cuarta parte o la mitad de un bastidor del sistema Oracle SPARC SuperCluster no requiere que se modifique la cadena de conexión del bloque de ejecución de Oracle RMAN.

La utilidad `srvctl` se usa para instalar servicios para el procesamiento de Oracle RMAN. El siguiente fragmento de código muestra cómo crear dos servicios distribuidos de manera uniforme en un cluster de cuatro nodos que están configurados para realizar failover a cualquiera de los otros nodos del cluster. En este ejemplo, los servicios están instalados para una base de datos llamada dbname y se denominan `dbname_bkup`.

```
srvctl add service -d dbname -r dbname1 -a dbname2 -s dbname_bkup1
srvctl start service -d dbname -s dbname_bkup1
srvctl add service -d dbname -r dbname2 -a dbname1 -s dbname_bkup2
srvctl start service -d dbname -s dbname_bkup2
```

Configuración de Oracle RMAN

La configuración del canal y el paralelismo de Oracle RMAN incluye la especificación de los destinos del sistema de archivos para los canales de copia de seguridad de Oracle RMAN y la cantidad total de canales utilizados para las operaciones de copia de seguridad y restauración. Si se configuran 16 canales de Oracle RMAN distribuidos entre los recursos compartidos disponibles del dispositivo ZFS Storage Appliance se pueden mejorar el rendimiento. Configure los canales de Oracle RMAN de manera que estén distribuidos de manera uniforme tanto entre las instancias de la base de datos de Oracle y los nodos del cluster de RAC como entre los recursos compartidos exportados desde el dispositivo ZFS Storage Appliance.

Los siguientes fragmentos de código muestran bloques de ejecución modelo de Oracle RMAN para realizar operaciones de copia de seguridad y restauración para conjuntos de copias de seguridad y copias de imágenes, así como para aplicar fusiones incrementales a las copias de las imágenes. El código modelo se basa en la siguiente configuración de base de datos:

- Nombre de base de datos: `dbname`
- Inicio de sesión en SYSDBA: `sys/welcome`
- Dirección de análisis: `ad01-scan`
- Nombres de servicios para la copia de seguridad: `dbname_bkup`

El dispositivo ZFS Storage Appliance se puede configurar en una configuración de una agrupación en la que el dispositivo exporta ocho recursos compartidos que se usan como ocho puntos de montaje.

Los bloques de ejecución de Oracle RMAN para la copia de seguridad y la restauración que usan conjuntos de copias de seguridad y copias de imágenes se muestran en los ejemplos de las secciones siguientes. En estos ejemplos, se accede a los puntos de montaje de la configuración de cuatro recursos compartidos como `/zfssa/dbname/backup1` a `/zfssa/dbname/backup4`. Asimismo, los ejemplos corresponden a una configuración en la que el dispositivo ZFS Storage Appliance exporta cuatro recursos compartidos usados como cuatro puntos de montaje para 16 canales de Oracle RMAN.

Copia de seguridad de nivel 0 de conjunto de copias de seguridad:

```
run
{<br/>
   sql ’alter system set "_backup_disk_bufcnt"=64 scope=memory’;<br/>
   sql ’alter system set "_backup_disk_bufsz"=1048576 scope=memory’;<br/>
   allocate channel ch01 device type disk connect ’sys/welcome@ad01-<br/>
   scan/dbname_bkup1’ format ’/zfssa/dbname/backup1/%U’;<br/>
   allocate channel ch02 device type disk connect ’sys/welcome@ad01-<br/>
   scan/dbname_bkup2’ format ’/zfssa/dbname/backup2/%U’;<br/>
   allocate channel ch03 device type disk connect ’sys/welcome@ad01-<br/>
   scan/dbname_bkup1’ format ’/zfssa/dbname/backup3/%U’;<br/>
   allocate channel ch04 device type disk connect ’sys/welcome@ad01-<br/>
   scan/dbname_bkup2’ format ’/zfssa/dbname/backup4/%U’;<br/>
   allocate channel ch05 device type disk connect ’sys/welcome@ad01-<br/>
   scan/dbname_bkup1’ format ’/zfssa/dbname/backup1/%U’;<br/>
   allocate channel ch06 device type disk connect ’sys/welcome@ad01-<br/>
   scan/dbname_bkup2’ format ’/zfssa/dbname/backup2/%U’;<br/>
   allocate channel ch07 device type disk connect ’sys/welcome@ad01-<br/>
   scan/dbname_bkup1’ format ’/zfssa/dbname/backup3/%U’;<br/>
   allocate channel ch08 device type disk connect ’sys/welcome@ad01-<br/>
   scan/dbname_bkup2’ format ’/zfssa/dbname/backup4/%U’;<br/>
   allocate channel ch09 device type disk connect ’sys/welcome@ad01-<br/>
   scan/dbname_bkup1’ format ’/zfssa/dbname/backup2/%U’;<br/>
   allocate channel ch10 device type disk connect ’sys/welcome@ad01-<br/>
   scan/dbname_bkup2’ format ’/zfssa/dbname/backup1/%U’;<br/>
   allocate channel ch11 device type disk connect ’sys/welcome@ad01-<br/>
   scan/dbname_bkup1’ format ’/zfssa/dbname/backup4/%U’;<br/>
   allocate channel ch12 device type disk connect ’sys/welcome@ad01-<br/>
   scan/dbname_bkup2’ format ’/zfssa/dbname/backup3/%U’;<br/>
   allocate channel ch13 device type disk connect ’sys/welcome@ad01-<br/>
   scan/dbname_bkup1’ format ’/zfssa/dbname/backup2/%U’;<br/>
   allocate channel ch14 device type disk connect ’sys/welcome@ad01-<br/>
   scan/dbname_bkup2’ format ’/zfssa/dbname/backup1/%U’;<br/>
   allocate channel ch15 device type disk connect ’sys/welcome@ad01-<br/>
```

```
   scan/dbname_bkup1’ format ’/zfssa/dbname/backup4/%U’;<br/>
   allocate channel ch16 device type disk connect ’sys/welcome@ad01-<br/>
   scan/dbname_bkup2’ format ’/zfssa/dbname/backup3/%U’;<br/>
   configure snapshot controlfile name to<br/>
   ’/zfssa/dbname/backup1/snapcf_dbname.f’;<br/>
   backup as backupset incremental level 0 section size 32g database<br/>
   tag ’FULLBACKUPSET_L0’ plus archivelog tag ’FULLBACKUPSET_L0’;
}
```

Copia de seguridad de nivel 1 de conjunto de copias de seguridad:

```
run
{<br/>
   sql ’alter system set "_backup_disk_bufcnt"=64 scope=memory’;<br/>
   sql ’alter system set "_backup_disk_bufsz"=1048576 scope=memory’;<br/>
   allocate channel ch01 device type disk connect ’sys/welcome@ad01-<br/>
   scan/dbname_bkup1’ format ’/zfssa/dbname/backup1/%U’;<br/>
   allocate channel ch02 device type disk connect ’sys/welcome@ad01-<br/>
   scan/dbname_bkup2’ format ’/zfssa/dbname/backup2/%U’;<br/>
   allocate channel ch03 device type disk connect ’sys/welcome@ad01-<br/>
   scan/dbname_bkup1’ format ’/zfssa/dbname/backup3/%U’;<br/>
   allocate channel ch04 device type disk connect ’sys/welcome@ad01-<br/>
   scan/dbname_bkup2’ format ’/zfssa/dbname/backup4/%U’;<br/>
   allocate channel ch05 device type disk connect ’sys/welcome@ad01-<br/>
   scan/dbname_bkup1’ format ’/zfssa/dbname/backup1/%U’;<br/>
   allocate channel ch06 device type disk connect ’sys/welcome@ad01-<br/>
   scan/dbname_bkup2’ format ’/zfssa/dbname/backup2/%U’;<br/>
   allocate channel ch07 device type disk connect ’sys/welcome@ad01-<br/>
   scan/dbname_bkup1’ format ’/zfssa/dbname/backup3/%U’;<br/>
   allocate channel ch08 device type disk connect ’sys/welcome@ad01-<br/>
   scan/dbname_bkup2’ format ’/zfssa/dbname/backup4/%U’;<br/>
   allocate channel ch09 device type disk connect ’sys/welcome@ad01-<br/>
   scan/dbname_bkup1’ format ’/zfssa/dbname/backup2/%U’;<br/>
   allocate channel ch10 device type disk connect ’sys/welcome@ad01-<br/>
   scan/dbname_bkup2’ format ’/zfssa/dbname/backup1/%U’;<br/>
   allocate channel ch11 device type disk connect ’sys/welcome@ad01-<br/>
   scan/dbname_bkup1’ format ’/zfssa/dbname/backup4/%U’;<br/>
   allocate channel ch12 device type disk connect ’sys/welcome@ad01-<br/>
   scan/dbname_bkup2’ format ’/zfssa/dbname/backup3/%U’;<br/>
   allocate channel ch13 device type disk connect ’sys/welcome@ad01-<br/>
   scan/dbname_bkup1’ format ’/zfssa/dbname/backup2/%U’;<br/>
   allocate channel ch14 device type disk connect ’sys/welcome@ad01-<br/>
   scan/dbname_bkup2’ format ’/zfssa/dbname/backup1/%U’;<br/>
   allocate channel ch15 device type disk connect ’sys/welcome@ad01-<br/>
   scan/dbname_bkup1’ format ’/zfssa/dbname/backup4/%U’;<br/>
   allocate channel ch16 device type disk connect ’sys/welcome@ad01-<br/>
   scan/dbname_bkup2’ format ’/zfssa/dbname/backup3/%U’;<br/>
   configure snapshot controlfile name to<br/>
   ’/zfssa/dbname/backup1/snapcf_dbname.f’;<br/>
   backup as backupset incremental level 1 database tag<br/>
   ’FULLBACKUPSET_L1’ plus archivelog tag ’FULLBACKUPSET_L1’;
}
```

Copia de seguridad de copia de imágenes:

```
run
```

```
{<br/>
   sql ’alter system set "_backup_file_bufcnt"=64 scope=memory’;<br/>
   sql ’alter system set "_backup_file_bufsz"=1048576 scope=memory’;<br/>
   allocate channel ch01 device type disk connect ’sys/welcome@ad01-<br/>
   scan/dbname_bkup1’ format ’/zfssa/dbname/backup1/%U’;<br/>
   allocate channel ch02 device type disk connect ’sys/welcome@ad01-<br/>
   scan/dbname_bkup2’ format ’/zfssa/dbname/backup2/%U’;<br/>
   allocate channel ch03 device type disk connect ’sys/welcome@ad01-<br/>
   scan/dbname_bkup1’ format ’/zfssa/dbname/backup3/%U’;<br/>
   allocate channel ch04 device type disk connect ’sys/welcome@ad01-<br/>
   scan/dbname_bkup2’ format ’/zfssa/dbname/backup4/%U’;<br/>
   allocate channel ch05 device type disk connect ’sys/welcome@ad01-<br/>
   scan/dbname_bkup1’ format ’/zfssa/dbname/backup1/%U’;<br/>
   allocate channel ch06 device type disk connect ’sys/welcome@ad01-<br/>
   scan/dbname_bkup2’ format ’/zfssa/dbname/backup2/%U’;<br/>
   allocate channel ch07 device type disk connect ’sys/welcome@ad01-<br/>
   scan/dbname_bkup1’ format ’/zfssa/dbname/backup3/%U’;<br/>
   allocate channel ch08 device type disk connect ’sys/welcome@ad01-<br/>
   scan/dbname_bkup2’ format ’/zfssa/dbname/backup4/%U’;<br/>
   allocate channel ch09 device type disk connect ’sys/welcome@ad01-<br/>
   scan/dbname_bkup1’ format ’/zfssa/dbname/backup2/%U’;<br/>
   allocate channel ch10 device type disk connect ’sys/welcome@ad01-<br/>
   scan/dbname_bkup2’ format ’/zfssa/dbname/backup1/%U’;<br/>
   allocate channel ch11 device type disk connect ’sys/welcome@ad01-<br/>
   scan/dbname_bkup1’ format ’/zfssa/dbname/backup4/%U’;<br/>
   allocate channel ch12 device type disk connect ’sys/welcome@ad01-<br/>
   scan/dbname_bkup2’ format ’/zfssa/dbname/backup3/%U’;<br/>
   allocate channel ch13 device type disk connect ’sys/welcome@ad01-<br/>
   scan/dbname_bkup1’ format ’/zfssa/dbname/backup2/%U’;<br/>
   allocate channel ch14 device type disk connect ’sys/welcome@ad01-<br/>
   scan/dbname_bkup2’ format ’/zfssa/dbname/backup1/%U’;<br/>
   allocate channel ch15 device type disk connect ’sys/welcome@ad01-<br/>
   scan/dbname_bkup1’ format ’/zfssa/dbname/backup4/%U’;<br/>
   allocate channel ch16 device type disk connect ’sys/welcome@ad01-<br/>
   scan/dbname_bkup2’ format ’/zfssa/dbname/backup3/%U’;<br/>
   configure snapshot controlfile name to<br/>
   ’/zfssa/dbname/backup1/snapcf_dbname.f’;<br/>
   backup incremental level 1 for recover of copy with tag ’IMAGECOPY’<br/>
   database;
}
```

Fusión incremental con copia de imágenes:

```
run
{<br/>
   sql ’alter system set "_backup_disk_bufcnt"=64 scope=memory’;<br/>
   sql ’alter system set "_backup_disk_bufsz"=1048576 scope=memory’;<br/>
   sql ’alter system set "_backup_file_bufcnt"=64 scope=memory’;<br/>
   sql ’alter system set "_backup_file_bufsz"=1048576 scope=memory’;<br/>
   allocate channel ch01 device type disk connect ’sys/welcome@ad01-<br/>
   scan/dbname_bkup1’;<br/>
   allocate channel ch02 device type disk connect ’sys/welcome@ad01-<br/>
   scan/dbname_bkup2’;<br/>
   allocate channel ch03 device type disk connect ’sys/welcome@ad01-<br/>
   scan/dbname_bkup1’;<br/>
   allocate channel ch04 device type disk connect ’sys/welcome@ad01-<br/>
   scan/dbname_bkup2’;<br/>
```

```
   allocate channel ch05 device type disk connect 'sys/welcome@ad01-<br/>
   scan/dbname_bkup1';<br/>
   allocate channel ch06 device type disk connect 'sys/welcome@ad01-<br/>
   scan/dbname_bkup2';<br/>
   allocate channel ch07 device type disk connect 'sys/welcome@ad01-<br/>
   scan/dbname_bkup1';<br/>
   allocate channel ch08 device type disk connect 'sys/welcome@ad01-<br/>
   scan/dbname_bkup2';<br/>
   allocate channel ch09 device type disk connect 'sys/welcome@ad01-<br/>
   scan/dbname_bkup1';<br/>
   allocate channel ch10 device type disk connect 'sys/welcome@ad01-<br/>
   scan/dbname_bkup2';<br/>
   allocate channel ch11 device type disk connect 'sys/welcome@ad01-<br/>
   scan/dbname_bkup1';<br/>
   allocate channel ch12 device type disk connect 'sys/welcome@ad01-<br/>
   scan/dbname_bkup2';<br/>
   allocate channel ch13 device type disk connect 'sys/welcome@ad01-<br/>
   scan/dbname_bkup1';<br/>
   allocate channel ch14 device type disk connect 'sys/welcome@ad01-<br/>
   scan/dbname_bkup2';<br/>
   allocate channel ch15 device type disk connect 'sys/welcome@ad01-<br/>
   scan/dbname_bkup1';<br/>
   allocate channel ch16 device type disk connect 'sys/welcome@ad01-<br/>
   scan/dbname_bkup2';<br/>
   configure snapshot controlfile name to<br/>
   '/zfssa/dbname/backup1/snapcf_dbname.f';<br/>
   recover copy of database with tag 'IMAGECOPY';
}
```

Validación de restauración:

```
run
{<br/>
   sql 'alter system set "_backup_disk_bufcnt"=64 scope=memory';<br/>
   sql 'alter system set "_backup_disk_bufsz"=1048576 scope=memory';<br/>
   sql 'alter system set "_backup_file_bufcnt"=64 scope=memory';<br/>
   sql 'alter system set "_backup_file_bufsz"=1048576 scope=memory';<br/>
   allocate channel ch01 device type disk connect 'sys/welcome@ad01-<br/>
   scan/dbname_bkup1';<br/>
   allocate channel ch02 device type disk connect 'sys/welcome@ad01-<br/>
   scan/dbname_bkup2';<br/>
   allocate channel ch03 device type disk connect 'sys/welcome@ad01-<br/>
   scan/dbname_bkup1';<br/>
   allocate channel ch04 device type disk connect 'sys/welcome@ad01-<br/>
   scan/dbname_bkup2';<br/>
   allocate channel ch05 device type disk connect 'sys/welcome@ad01-<br/>
   scan/dbname_bkup1';<br/>
   allocate channel ch06 device type disk connect 'sys/welcome@ad01-<br/>
   scan/dbname_bkup2';<br/>
   allocate channel ch07 device type disk connect 'sys/welcome@ad01-<br/>
   scan/dbname_bkup1';<br/>
   allocate channel ch08 device type disk connect 'sys/welcome@ad01-<br/>
   scan/dbname_bkup2';<br/>
   allocate channel ch09 device type disk connect 'sys/welcome@ad01-<br/>
   scan/dbname_bkup1';<br/>
   allocate channel ch10 device type disk connect 'sys/welcome@ad01-<br/>
   scan/dbname_bkup2';<br/>
```

```
   allocate channel ch11 device type disk connect 'sys/welcome@ad01-<br/>
   scan/dbname_bkup1';<br/>
   allocate channel ch12 device type disk connect 'sys/welcome@ad01-<br/>
   scan/dbname_bkup2';<br/>
   allocate channel ch13 device type disk connect 'sys/welcome@ad01-<br/>
   scan/dbname_bkup1';<br/>
   allocate channel ch14 device type disk connect 'sys/welcome@ad01-<br/>
   scan/dbname_bkup2';<br/>
   allocate channel ch15 device type disk connect 'sys/welcome@ad01-<br/>
   scan/dbname_bkup1';<br/>
   allocate channel ch16 device type disk connect 'sys/welcome@ad01-<br/>
   scan/dbname_bkup2';<br/>
   configure snapshot controlfile name to<br/>
   '/zfssa/dbname/backup1/snapcf_dbname.f';<br/>
   restore validate database;
}
```

Pasos siguientes

"Copia de seguridad de Oracle SPARC SuperCluster" [473]

Configuración de Oracle SPARC SuperCluster para copia de seguridad con ZFS Storage Appliance

En esta sección, se incluyen secuencias de comandos de ejemplo, que muestran cómo conectar un dispositivo ZFS Storage Appliance a Oracle SPARC SuperCluster. Estas secuencias de comandos fueron diseñadas para admitir una base de datos denominada `dbname` en una configuración de dispositivo ZFS Storage Appliance de una agrupación y de dos agrupaciones.

Configuración de SCC: configuración de Oracle SPARC SuperCluster para copia de seguridad con ZFS Storage Appliance

Pasos de implementación generales

Los pasos de implementación son los siguientes:

1. Configure la estructura del directorio (puntos de montaje) para montar los recursos compartidos en el host.
2. Actualice `/etc/vfstab` para montar los recursos compartidos exportados del dispositivo ZFS Storage Appliance a los puntos de montaje adecuados.

3. Active los servicios de cliente de NFS para montar los recursos compartidos de NFS en el reinicio, de manera de automatizar el proceso de montaje y desmontaje de recursos compartidos.
4. Actualice el archivo `oranfstab` para acceder a los recursos compartidos exportados del dispositivo ZFS Storage Appliance.
5. Monte los recursos compartidos en el host.
6. Cambie los permisos de los recursos compartidos montados para hacerlos coincidir con la configuración de permisos de `ORACLE_HOME`.
7. Reinicie la instancia de Oracle Database para aplicar los cambios del archivo `oranfstab`.

Pasos de implementación detallados

Temas de esta sección:

Configuración de la estructura de directorio para montar los recursos compartidos en el host

Configure los puntos de montaje de los recursos compartidos en el host como se muestra a continuación:

```
mkdir -p /zfssa/dbname/backup1
mkdir -p /zfssa/dbname/backup2
mkdir -p /zfssa/dbname/backup3
mkdir -p /zfssa/dbname/backup4
```

Actualización del archivo /etc/vfstab

Para actualizar el archivo `/etc/vfstab`, utilice una de las siguientes opciones.

Nota: El carácter de escape de nueva línea de UNIX (\) indica que una única línea de código se ha ajustado a una segunda línea en el listado a continuación. Cuando introduzca una línea

ajustada a `fstab`, elimine el carácter \ y combine los dos segmentos de línea, separados por un espacio, en una única línea.

Para una configuración de una agrupación:

```
192.168.36.200:/export/dbname/backup1 - /zfssa/dbname/backup1 \<br/>
   nfs - yes rw,bg,hard,nointr,rsize=1048576,wsize=1048576,proto= \<br/>
   tcp,vers=3,forcedirectio
192.168.36.200:/export/dbname/backup2 - /zfssa/dbname/backup2 \<br/>
   nfs - yes rw,bg,hard,nointr,rsize=1048576,wsize=1048576,proto= \<br/>
   tcp,vers=3,forcedirectio
192.168.36.200:/export/dbname/backup3 - /zfssa/dbname/backup3 \<br/>
   nfs - yes rw,bg,hard,nointr,rsize=1048576,wsize=1048576,proto= \<br/>
   tcp,vers=3,forcedirectio
192.168.36.200:/export/dbname/backup4 - /zfssa/dbname/backup4 \<br/>
   nfs - yes rw,bg,hard,nointr,rsize=1048576,wsize=1048576,proto= \<br/>
   tcp,vers=3,forcedirectio
```

Para una configuración de dos agrupaciones:

```
192.168.36.200:/export/dbname/backup1 - /zfssa/dbname/backup1 \<br/>
   nfs - yes rw,bg,hard,nointr,rsize=1048576,wsize=1048576,proto= \<br/>
   tcp,vers=3,forcedirectio
192.168.36.201:/export/dbname/backup2 - /zfssa/dbname/backup2 \<br/>
   nfs - yes rw,bg,hard,nointr,rsize=1048576,wsize=1048576,proto= \<br/>
   tcp,vers=3,forcedirectio
192.168.36.200:/export/dbname/backup3 - /zfssa/dbname/backup3 \<br/>
   nfs - yes rw,bg,hard,nointr,rsize=1048576,wsize=1048576,proto= \<br/>
   tcp,vers=3,forcedirectio
192.168.36.201:/export/dbname/backup4 - /zfssa/dbname/backup4 \<br/>
   nfs - yes rw,bg,hard,nointr,rsize=1048576,wsize=1048576,proto= \<br/>
   tcp,vers=3,forcedirectio
```

Activación del servicio de cliente NFS

Use el siguiente comando para activar el servicio de cliente NFS en el host de Solaris 11:

```
svcadm enable -r nfs/client
```

Actualización de oranfstab para acceder a las exportaciones de ZFS Storage Appliance

Para actualizar el archivo `oranfstab` para acceder a las exportaciones del dispositivo ZFS Storage Appliance, utilice la siguiente opción adecuada.

Para una configuración de una agrupación:

```
server: 192.168.36.200
```

```
path: 192.168.36.200
path: 192.168.36.201
path: 192.168.36.202
path: 192.168.36.203
export: /export/dbname/backup1 mount: /zfssa/dbname/backup1
export: /export/dbname/backup2 mount: /zfssa/dbname/backup2
export: /export/dbname/backup3 mount: /zfssa/dbname/backup3
export: /export/dbname/backup4 mount: /zfssa/dbname/backup4
```

Para una configuración de dos agrupaciones:

```
server: 192.168.36.200
path: 192.168.36.200
path: 192.168.36.202
export: /export/dbname/backup1 mount: /zfssa/dbname-2pool/backup1
export: /export/dbname/backup3 mount: /zfssa/dbname-2pool/backup3
server: 192.168.36.201
path: 192.168.36.201
path: 192.168.36.203
export: /export/dbname/backup2 mount: /zfssa/dbname-2pool/backup2
export: /export/dbname/backup4 mount: /zfssa/dbname-2pool/backup4
```

Montaje de los recursos compartidos en el host

Con el comando estándar `mount` de Solaris, monte los recursos compartidos de manera manual:

```
# mount /zfssa/dbname/backup1
# mount /zfssa/dbname/backup2
# mount /zfssa/dbname/backup3
# mount /zfssa/dbname/backup4
```

Configuración de la propiedad de los recursos compartidos montados

Cambie la configuración de permisos de los recursos compartidos montados para hacerlos coincidir con la configuración de permisos de `ORACLE_HOME`. En este ejemplo, las propiedades de usuario y grupo están configuradas como `oracle:dba`.

1. Introduzca:
`chown oracle:dba /zfssa/dbname/*`
2. Reinicie la instancia de Oracle Database para aplicar los cambios realizados en el archivo `oranfstab` mediante una de las siguientes opciones:

- Reinicie una instancia a la vez (actualización gradual), por ejemplo:
- `:$ srvctl stop instance -d dbname -i dbname1`
- `:$ srvctl start instance -d dbname -i dbname1`
- `:$ srvctl stop instance -d dbname -i dbname2`

- `:$ srvctl start instance -d dbname -i dbname2`
- `:$ srvctl stop instance -d dbname -i dbname3`
- `:$ srvctl start instance -d dbname -i dbname3`
- `:$ srvctl stop instance -d dbname -i dbname4`
- `:$ srvctl start instance -d dbname -i dbname4`
- `:$ srvctl stop instance -d dbname -i dbname5`
- `:$ srvctl start instance -d dbname -i dbname5`
- `:$ srvctl stop instance -d dbname -i dbname6`
- `:$ srvctl start instance -d dbname -i dbname6`
- `:$ srvctl stop instance -d dbname -i dbname7`
- `:$ srvctl start instance -d dbname -i dbname7`
- `:$ srvctl stop instance -d dbname -i dbname8`
- `:$ srvctl start instance -d dbname -i dbname8`
- Reinicie toda la base de datos, por ejemplo:
- `:$ srvctl stop database -d dbname`
- `:$ srvctl start database -d dbname`

Oracle Intelligent Storage Protocol

Oracle Database tiene una arquitectura en capas que incluye Oracle Disk Manager (ODM). ODM proporciona un módulo de gestión de archivos que permite que Oracle Database utilice un sistemas de archivos local, una partición de disco sin procesar o un servidor NFS para almacenar información de bases de datos.

Para aumentar el rendimiento de las bases de datos, la interfaz de ODM permite que Oracle Database transmita información junto con cada solicitud de E/S. Esta información define varios atributos asociados con la E/S, como el tipo de archivo asociado con la solicitud de E/S. Esto permite gestionar de manera distinta las escrituras en archivos log de bases de datos y archivos de datos.

El nuevo OISP permite que el cliente NFSv4 de Oracle Database transmita información de optimización de ODM al servidor NFSv4 de ZFS Storage Appliance. ZFS Storage Appliance aprovecha la información de optimización de ODM para simplificar la configuración de las bases de datos y para aumentar aún más su rendimiento.

Oracle Intelligent Storage Protocol proporciona dos funciones:

- Definición automática del tamaño de registro de archivo óptimo para nuevos archivos de bases de datos
- Uso automático de la desviación de escritura óptima (rendimiento o latencia ZFS) para cada solicitud de escritura

Definición del tamaño de registro de archivo óptimo

El cliente Oracle dNFS envía el tamaño de registro óptimo a ZFS Storage Appliance para cada solicitud de escritura de NFSv4. El servidor NFSv4 de ZFS Storage Appliance envía el tamaño de registro al sistema de archivos ZFS con la solicitud de E/S. El sistema de archivos ZFS luego omite el tamaño de registro predeterminado del sistema de archivos y utiliza el valor de tamaño de registro enviado con la solicitud de E/S. El tamaño de registro solamente se puede definir para los archivos recién creados. Si ya existe un archivo, no se modificará el tamaño de registro.

Uso del modo de escritura de rendimiento o latencia ZFS para cada solicitud

El cliente Oracle dNFS envía la desviación de escritura óptima a ZFS Storage Appliance para cada solicitud de escritura de NFSv4. El servidor NFSv4 de ZFS Storage Appliance envía la desviación de escritura al sistema de archivos ZFS con la solicitud de E/S. El sistema de archivos ZFS luego omite la desviación de escritura predeterminada del sistema de archivos e intenta utilizar el valor de desviación de escritura enviado con la solicitud de E/S. Según el estado del sistema de archivos ZFS, es posible que se ignore la desviación de escritura enviada con la solicitud de E/S.

Complemento de sistema de archivos de red de dispositivo Sun ZFS Storage para Oracle Solaris Cluster

Oracle Solaris Cluster (OCS) es un producto de software de agrupación clusters de alta disponibilidad para el sistema operativo Solaris.

Sun ZFS Storage Appliance Network File System Plug In for Oracle Solaris Cluster admite OSC con Sun ZFS Storage Appliance mediante el protocolo NFS. El archivo Léame y el complemento están disponibles como parte de Sun ZFS Storage Appliance Network File System Plugin for Oracle Solaris Cluster en Oracle Technology Network.

Sun ZFS Storage Appliance Plug-in for Oracle Solaris Cluster Geographic Edition

El software Oracle Solaris Cluster Geographic Edition es una extensión en capas del software Oracle Solaris Cluster. El software Geographic Edition protege las aplicaciones contra las

interrupciones inesperadas. Para ello, utiliza varios clusters que están separados por distancias grandes y emplea una infraestructura redundante que replica los datos entre estos sitios de cluster. Este complemento coordina la replicación de datos entre sitios remotos de Oracle Solaris Cluster por medio del servicio de replicación remota de Sun ZFS Storage Appliance.

El paquete de complementos está disponible a través de la página de información de almacenamiento NAS de Oracle Technology Network.

Sun ZFS Storage Management Plug-In for Oracle Enterprise Manager Grid Controller

Sun ZFS Storage Management Plug-In for Oracle Enterprise Manager Grid Controller ofrece supervisión de nivel superior para el entorno del controlador de cuadrículas de la familia Sun ZFS Storage Appliance con capacidad para:

- Supervisar dispositivos Sun ZFS Storage Appliance.
- Recopilar información del sistema de almacenamiento, información de configuración e información de rendimiento de los componentes de almacenamiento disponibles.
- Activar alertas e infracciones en función de umbrales, y supervisar la información recopilada por la herramienta.
- Proporcionar informes integrados que complementan el análisis.
- Admitir la supervisión por parte de agentes remotos.

Una vez que se ha configurado el dispositivo para que lo supervise el controlador de cuadrículas, se crean conjuntos de datos y hojas de trabajo de análisis para ofrecer a la vista del administrador del controlador de cuadrículas un mayor nivel de detalle, proporcionado por el análisis en tiempo real disponible en el dispositivo.

El complemento de gestión está disponible en el siguiente enlace: Oracle Technology Network.

Incluye una guía de instalación que deben leer los administradores del controlador de cuadrículas y los administradores de almacenamiento de los dispositivos que se supervisan.

Con cada dispositivo se incluyen dos “flujos de trabajo” [443] que se utilizan respectivamente para preparar un sistema para supervisión o para quitar los artefactos creados para el entorno de supervisión:

- Configuración de la supervisión de Oracle Enterprise Manager
- Desconfiguración de la supervisión de Oracle Enterprise Manager

Se puede acceder a estos flujos de trabajo desde la página “Maintenance (Mantenimiento) > Workflows (Flujos de trabajo)” [443] de la interfaz de usuario basada en explorador.

Oracle Grid Controller Sun ZFS Storage Management Plug-In for Oracle Enterprise Manager Grid Controller

Configuración de la supervisión de Oracle Enterprise Manager

Este flujo de trabajo se utiliza para preparar un entorno para la supervisión o para restablecer el estado original de los artefactos creados por el flujo de trabajo, en caso de que el administrador de almacenamiento haya modificado los artefactos durante el funcionamiento. Al ejecutar este flujo de trabajo, se realizan los siguientes cambios en el sistema:

- Se generará un *oracle_agent*, "Propiedades de roles" [142], con acceso limitado al sistema, para permitir al agente de Oracle Enterprise Manager Grid Controller obtener la información necesaria para la supervisión, pero no para realizar cambios en el sistema. Se generará un *oracle_agent*, Capítulo 7, Configuración de usuario, y se le asignará este rol. El uso de este rol y usuario es fundamental para mantener registros de auditoría claros respecto del momento y la manera en que el agente accede al dispositivo.
- Se activará la herramienta de análisis avanzado, que pone a disposición de todos los usuarios de Sun ZFS Storage Appliance un amplio conjunto de estadísticas.
- Se generará la hoja de trabajo *Oracle Enterprise Manager*, que facilitará la comunicación entre el administrador del controlador de cuadrículas y el administrador de almacenamiento. Todas las métricas supervisadas por el controlador de cuadrículas están disponibles en esta hoja de trabajo.

Desconfiguración de la supervisión de Oracle Enterprise Manager

Este flujo de trabajo elimina los artefactos generados por la *Configuración de la supervisión de Oracle Enterprise Manager*. Concretamente:

- Elimina el rol y usuario *oracle_agent*.
- Elimina la hoja de trabajo de *Oracle Enterprise Manager*.

Este flujo de trabajo *no* desactivará la herramienta de análisis avanzado ni ninguno de los conjuntos de datos activados con fines de recopilación.

Oracle Virtual Machine Storage Connect Plug-in for the Sun ZFS Storage Appliance

Una de las diversas características introducidas en Oracle VM 3.0 es la estructura de Storage Connect. Esta estructura permite a Oracle VM 3.0 Manager acceder directamente a los servidores de almacenamiento y los recursos de aprovisionamiento. Con esta estructura, puede registrar servidores de almacenamiento, detectar recursos de almacenamiento existentes, crear y presentar discos físicos a las agrupaciones de servidores, y compartir repositorios de almacenamiento y máquinas virtuales.

Oracle Virtual Machine Storage Connect Plug-in for the Sun ZFS Storage Appliance es un componente del conjunto de programas de Oracle VM, que permite a Oracle VM aprovisionar y gestionar el dispositivo Sun ZFS Storage Appliance para la virtualización. El complemento está instalado en Oracle VM Server y se comunica con los servidores de almacenamiento mediante flujos de trabajo instalados en ZFSSA.

El archivo Léame y el complemento están disponibles en Oracle Technology Network.

Sun ZFS Storage Appliance Provider For Volume Shadow Copy Service Software

Volume Shadow Copy Services (VSS) para sistemas operativos Microsoft ofrece una estructura para permitir la realización de copias de seguridad de volúmenes mientras las aplicaciones del sistema continúan con la escritura en los volúmenes. VSS ofrece una interfaz uniforme que permite la coordinación entre aplicaciones de usuario que actualizan datos en el disco (escritores VSS) y aquellas que realizan copias de seguridad de las aplicaciones (solicitantes VSS). Específicamente, VSS ofrece:

- Una infraestructura de copia de seguridad que coordina las aplicaciones con las actividades del sistema de archivos.
- Una ubicación para generar un punto en el tiempo, copias fusionadas conocidas como *instantáneas*.

Sun ZFS Storage Appliance Provider For Volume Shadow Copy Service Software es un proveedor de hardware VSS que permite a Sun ZFS Storage Appliance tomar instantáneas coherentes para los hosts de Windows que utilizan destinos de bloque. VSS coordina las instantáneas para garantizar la coherencia de los datos de bloque. El proveedor se comunica con un conjunto de flujos de trabajo en el dispositivo para coordinar la toma de instantáneas como se ven desde la aplicación. Funciona con iSCSI y canal de fibra.

Sun ZFS Storage Appliance Provider For Volume Shadow Copy Service Software se instala en los hosts que requieren esta funcionalidad y coordinación entre las aplicaciones. La documentación completa para la integración de esta aplicación se incluye con los componentes

descargados en forma de un archivo ReadMe (Léame). El archivo Léame y el software del proveedor están disponibles como parte del parche de complementos y proveedores de software de Sun ZFS Storage 7000 en Oracle Technology Network. El sitio web de Microsoft contiene más información sobre VSS, incluida la siguiente descripción general: http://msdn.microsoft.com/en-us/library/aa384649 (http://msdn.microsoft.com/en-us/library/aa384649)%28VS.85%29.aspx.

Compatibilidad de FC con Symantec 'DMP'/Storage Foundation

- SF - Symantec Storage Foundation 5.1
- SF HA - Storage Foundation High Availability 5.1
- SFCFS/SF Oracle RAC - Storage Foundation Cluster File System/Storage Foundation for Oracle RAC 5.1
- SFCFS/SFCFS Oracle RAC - Storage Foundation Cluster File System/Storage Foundation Cluster File System for Oracle RAC 5.1

Compatibilidad de FC para Storage Foundation 5.1RP2 de Symantec y superior para las siguientes versiones de sistema operativo

- Solaris 10 SPARC
- Solaris 10 x86
- Linux RedHat5
- Oracle Enterprise Linux (OEL)

Consulte la lista de compatibilidad de hardware de Symantec en http://www.symantec.com/business/support/index?page=content&id=TECH74012 (http://www.symantec.com/business/support/index).

Tenga en cuenta las siguientes restricciones:

- Se deben instalar las ASL de la serie 7000 "requeridas" por Symantec, que se pueden descargar de: https://vos.symantec.com/asl.
- Symantec además requiere el nivel de parche SF 5.1 VM de 5.1RP2 o superior, que se puede descargar de: https://vos.symantec.com/patch/matrix.
- Symantec también requiere la siguiente configuración de parámetros de DMP (sólo para la serie 7000 "agrupada en clusters") de:
- `:dmp_health_time=0`

- `:dmp_path_age=0`
- `:dmp_lun_retry_timeout=200`

Consulte la nota técnica de hardware de Symantec, que hace referencia a la configuración de la serie 7000 'agrupada en cluster': http://www.symantec.com/business/support/index?page=content&id=TECH47728 (http://www.symantec.com/business/support/index)

Storage Foundation 5.1SP2 de Symantec para Windows admite conexiones de FC para la serie 7000 en las siguientes versiones de Windows:

- Windows Server 2003
- Windows Server 2008
- Windows Server 2008 R2

Consulte la lista de compatibilidad de hardware de SF 5.1SP2 en http://www.symantec.com/business/support/index?page=content&id=TECH138719 (http://www.symantec.com/business/support/index).

Sun ZFS Storage 7000 Storage Replication Adapter for VMware Site Recovery Manager

Sun ZFS Storage 7000 Storage Replication Adapter (SRA) for VMware vCenter Site Recovery Manager (SRM) integra los dispositivos Sun ZFS Storage 7000 a las implementaciones de VMware que se extienden a múltiples sitios y requieren una rápida recuperación en caso de una interrupción del servicio del sitio protegido. El SRA se conecta a los entornos existentes de VMware vCenter SRM y permite la gestión de los dispositivos Sun ZFS Storage 7000 mediante las secuencias de detección, prueba y failover de VMware vCenter SRM a medida que se prueba y se ejecuta el plan de recuperación. El uso del SRA se lleva a cabo completamente dentro de la aplicación VMware vCenter SRM.

El administrador de VMware deberá trabajar en estrecha colaboración con el administrador de dispositivos Sun ZFS Storage 7000 responsable del dispositivo que aloja los almacenes de datos de VMware. Para obtener más información, consulte la Guía de administración de Sun ZFS Storage 7000 SRA for VMware SRM incluida con el SRA.

NOTA: El SRA se puede descargar de Oracle Technology Network. Para obtener el SRA, es necesario tener un contrato de asistencia válido con Oracle para el dispositivo Sun ZFS Storage 7000.

Índice