Gestión del almacenamiento san

ONTAP 9

NetApp
April 20, 2024

Tabla de contenidos

Gestión del almacenamiento san

Conceptos de SAN

Aprovisionamiento SAN con iSCSI

En entornos SAN, los sistemas de almacenamiento son destinos que tienen dispositivos de almacenamiento objetivo. Para iSCSI y FC, los dispositivos de almacenamiento de destino se denominan LUN (unidades lógicas). Para la memoria no volátil rápida (NVMe) sobre Fibre Channel, los dispositivos de destino de almacenamiento se denominan espacios de nombres.

El almacenamiento se configura mediante la creación de LUN para iSCSI y FC, o bien mediante la creación de espacios de nombres para NVMe. Posteriormente, se accede a los LUN o espacios de nombres en hosts con redes de protocolos de interfaz de sistemas pequeños de Internet (iSCSI) o Fibre Channel (FC).

Para conectarse a redes iSCSI, los hosts pueden utilizar adaptadores de red Ethernet (NIC) estándar, tarjetas TOE (motor de descarga TCP) con iniciadores de software, adaptadores de red convergente (CNA) o adaptadores de bus de host (HBA) iSCSI dedicados.

Para conectarse a redes FC, los hosts requieren HBA o CNA FC.

Los protocolos FC compatibles incluyen:

- FC
- FCoE
- NVMe

Nombres y conexiones de red del nodo de destino iSCSI

Los nodos de destino iSCSI pueden conectarse a la red de varias maneras:

- Mediante interfaces Ethernet, que utilizan software integrado en ONTAP.
- En múltiples interfaces del sistema, con una interfaz usada para iSCSI que también puede transmitir tráfico para otros protocolos, como SMB y NFS.
- Mediante un adaptador de objetivo unificado (UTA) o un adaptador de red convergente (CNA).

Cada nodo iSCSI debe tener un nombre de nodo.

Los dos formatos, o designadores de tipo, para los nombres de nodo iSCSI son *IQN* y *eui*. El destino iSCSI de SVM siempre usa el indicador de tipo IQN. El iniciador puede usar el tipo IQN o el indicador de tipo eui.

Nombre del nodo del sistema de almacenamiento

Cada SVM que ejecuta iSCSI tiene un nombre de nodo predeterminado basado en un nombre de dominio inverso y un número de codificación único.

El nombre del nodo se muestra en el formato siguiente:

iqn.1992-08.com.netapp:sn.*unique-encoding-number*

En el ejemplo siguiente se muestra el nombre de nodo predeterminado para un sistema de almacenamiento con un número de codificación único:

```
iqn.1992-08.com.netapp:sn.812921059e6c11e097b3123478563412:vs.6
```

Puerto TCP para iSCSI

El protocolo iSCSI está configurado en ONTAP para utilizar el puerto TCP con el número 3260.

ONTAP no admite cambiar el número de puerto para iSCSI. El número de puerto 3260 se registra como parte de la especificación iSCSI y no puede utilizarlo ninguna otra aplicación o servicio.

Información relacionada

"Documentación de NetApp: Configuración de host SAN de ONTAP"

Gestión de servicios iSCSI

Gestión de servicios iSCSI

Puede gestionar la disponibilidad del servicio iSCSI en las interfaces lógicas iSCSI de la máquina virtual de almacenamiento (SVM) mediante el `vserver iscsi interface enable` o. `vserver iscsi interface disable` comandos.

De forma predeterminada, el servicio iSCSI está habilitado en todas las interfaces lógicas iSCSI.

Cómo se implementa iSCSI en el host

ISCSI se puede implementar en el host mediante hardware o software.

Es posible implementar iSCSI de una de las siguientes maneras:

- Utiliza el software Initiator que utiliza las interfaces Ethernet estándar del host.
- A través de un adaptador de bus de host (HBA) iSCSI: Un HBA iSCSI aparece al sistema operativo host como un adaptador de disco SCSI con discos locales.
- Con un adaptador DE motor de descarga TCP (TOE) que libera el procesamiento TCP/IP.

  El procesamiento del protocolo iSCSI se sigue realizando mediante el software del host.

Cómo funciona la autenticación iSCSI

Durante la fase inicial de una sesión iSCSI, el iniciador envía una solicitud de inicio de sesión al sistema de almacenamiento para iniciar una sesión iSCSI. A continuación, el sistema de almacenamiento permite o rechaza la solicitud de inicio de sesión o determina que no es necesario iniciar sesión.

Los métodos de autenticación iSCSI son los siguientes:

- Primero: Protocolo de autenticación por desafío mutuo (CHAP): El iniciador inicia sesión con un nombre de usuario y una contraseña CHAP.

Es posible especificar una contraseña CHAP o generar una contraseña secreta hexadecimal. Existen dos tipos de nombres de usuario y contraseñas CHAP:

- Entrante: El sistema de almacenamiento autentica el iniciador.

  Es necesario configurar de entrada si se utiliza la autenticación CHAP.

- Saliente: Esta es una opción para permitir que el iniciador autentique el sistema de almacenamiento.

  Es posible utilizar la configuración saliente únicamente si se define un nombre de usuario y una contraseña entrantes en el sistema de almacenamiento.

- Denegar: El iniciador no tiene acceso al sistema de almacenamiento.
- Ninguno: El sistema de almacenamiento no requiere autenticación para el iniciador.

Puede definir la lista de iniciadores y sus métodos de autenticación. También puede definir un método de autenticación predeterminado que se aplique a los iniciadores que no aparecen en esta lista.

Información relacionada

"Opciones de múltiples rutas de Windows con Data ONTAP: Fibre Channel e iSCSI"

Gestión de seguridad del iniciador iSCSI

ONTAP ofrece una serie de funciones para gestionar la seguridad de los iniciadores de iSCSI. Puede definir una lista de iniciadores iSCSI y el método de autenticación predeterminado para cada uno, mostrar los iniciadores y los métodos de autenticación asociados en la lista de autenticación, añadir y quitar iniciadores de la lista de autenticación, y definir el método de autenticación del iniciador iSCSI predeterminado para los iniciadores que no están en la lista.

Aislamiento de extremos iSCSI

A partir de la versión 9.1 de ONTAP se mejoraron los comandos de seguridad iSCSI existentes para aceptar un rango de direcciones IP o varias direcciones IP.

Todos los iniciadores de iSCSI deben proporcionar direcciones IP de origen al establecer una sesión o conexión con un destino. Esta nueva funcionalidad evita que un iniciador inicie sesión en el clúster si la dirección IP de origen no es compatible o desconocida, lo cual proporciona un esquema de identificación único. Los iniciadores originados por una dirección IP no compatible o desconocida serán rechazados su inicio de sesión en la capa de sesión iSCSI, lo que impide que el iniciador acceda a cualquier LUN o volumen del clúster.

Implemente esta nueva funcionalidad con dos comandos nuevos para ayudar a gestionar entradas preexistentes.

Añada un rango de direcciones del iniciador

Mejore la gestión de seguridad del iniciador de iSCSI añadiendo un rango de direcciones IP o varias direcciones IP con el `vserver iscsi security add-initiator-address-range` comando.

```
cluster1::> vserver iscsi security add-initiator-address-range
```

Quite el rango de direcciones del iniciador

Quite un rango de direcciones IP o varias direcciones IP con el `vserver iscsi security remove-initiator-address-range` comando.

```
cluster1::> vserver iscsi security remove-initiator-address-range
```

Qué es la autenticación CHAP

El protocolo de autenticación por desafío mutuo (CHAP) permite la comunicación autenticada entre iniciadores y destinos iSCSI. Cuando se utiliza la autenticación CHAP, se definen los nombres de usuario y las contraseñas CHAP tanto en el iniciador como en el sistema de almacenamiento.

Durante la fase inicial de una sesión iSCSI, el iniciador envía una solicitud de inicio de sesión al sistema de almacenamiento para iniciar la sesión. La solicitud de inicio de sesión incluye el nombre de usuario CHAP del iniciador y el algoritmo CHAP. El sistema de almacenamiento responde con un desafío CHAP. El iniciador proporciona una respuesta CHAP. El sistema de almacenamiento verifica la respuesta y autentica el iniciador. La contraseña CHAP se utiliza para calcular la respuesta.

Directrices para usar la autenticación CHAP

Debe seguir ciertas directrices al utilizar la autenticación CHAP.

- Si define un nombre de usuario y una contraseña entrantes en el sistema de almacenamiento, debe usar el mismo nombre de usuario y contraseña para la configuración de CHAP saliente en el iniciador. Si también define un nombre de usuario y una contraseña de salida en el sistema de almacenamiento para habilitar la autenticación bidireccional, debe usar el mismo nombre de usuario y la misma contraseña para la configuración de CHAP entrante en el iniciador.
- No es posible usar el mismo nombre de usuario y contraseña para la configuración de entrada y salida en el sistema de almacenamiento.
- Los nombres de usuario CHAP pueden tener entre 1 y 128 bytes.

  No se permite un nombre de usuario nulo.

- Las contraseñas CHAP (secretos) pueden tener entre 1 y 512 bytes.

  Las contraseñas pueden ser cadenas o valores hexadecimales. Para valores hexadecimales, debe introducir el valor con un prefijo "'0x'" o "'0X'". No se permite una contraseña nula.

> ONTAP permite el uso de caracteres especiales, letras no inglesas, números y espacios para las contraseñas de CHAP (secretos). Sin embargo, esto está sujeto a restricciones de host. Si un host específico no permite alguno de estos, no se pueden usar.
>
> Por ejemplo, el iniciador de software iSCSI de Microsoft requiere que las contraseñas CHAP de iniciador y destino tengan al menos 12 bytes si no se está utilizando el cifrado IPsec. La longitud máxima de la contraseña es de 16 bytes independientemente de si se usa IPsec.
>
> Para ver más restricciones, debería consultar la documentación del iniciador.

La forma en que se utilizan las listas de acceso de interfaz iSCSI para limitar las interfaces de iniciador puede aumentar el rendimiento y la seguridad

Las listas DE acceso de interfaz ISCSI se pueden usar para limitar el número de LIF en una SVM a la que puede acceder un iniciador, con lo que aumenta el rendimiento y la seguridad.

Cuando un iniciador inicia una sesión de detección con un iSCSI `SendTargets` Comando, recibe las direcciones IP asociadas con la LIF (interfaz de red) que está en la lista de acceso. De forma predeterminada, todos los iniciadores tienen acceso a todas las LIF iSCSI de la SVM. Puede utilizar la lista de acceso para restringir el número de LIF en una SVM a la que tiene acceso un iniciador.

Servicio de nombres de almacenamiento de Internet (iSNS)

El servicio de nombres de almacenamiento de Internet (iSNS) es un protocolo que permite la detección y gestión automatizadas de dispositivos iSCSI en una red de almacenamiento TCP/IP. Un servidor iSNS mantiene información sobre dispositivos iSCSI activos en la red, incluidas sus direcciones IP, los nombres de nodos iSCSI IQN y los grupos de portales.

Puede obtener un servidor iSNS de un proveedor tercero. Si posee un servidor iSNS en la red configurado y habilitado para su uso por parte del iniciador y el destino, puede usar la LIF de gestión para una máquina virtual de almacenamiento (SVM) para registrar todos los LIF iSCSI para esa SVM en el servidor iSNS. Una vez completado el registro, el iniciador de iSCSI puede consultar el servidor iSNS para detectar todas las LIF de esa SVM en particular.

Si decide utilizar un servicio iSNS, debe asegurarse de que las máquinas virtuales de almacenamiento (SVM) estén registradas correctamente en un servidor de servicio de nombres de almacenamiento de Internet (iSNS).

Si no tiene un servidor iSNS en la red, debe configurar manualmente cada objetivo para que sea visible para el host.

Lo que hace un servidor iSNS

Un servidor iSNS utiliza el protocolo de servicio de nombres de almacenamiento de Internet (iSNS) para mantener información sobre los dispositivos iSCSI activos en la red, incluidas sus direcciones IP, nombres de nodos iSCSI (IQN) y grupos de portales.

El protocolo iSNS permite la detección y gestión automatizadas de dispositivos iSCSI en una red de almacenamiento IP. Un iniciador de iSCSI puede consultar el servidor iSNS para detectar dispositivos de destino iSCSI.

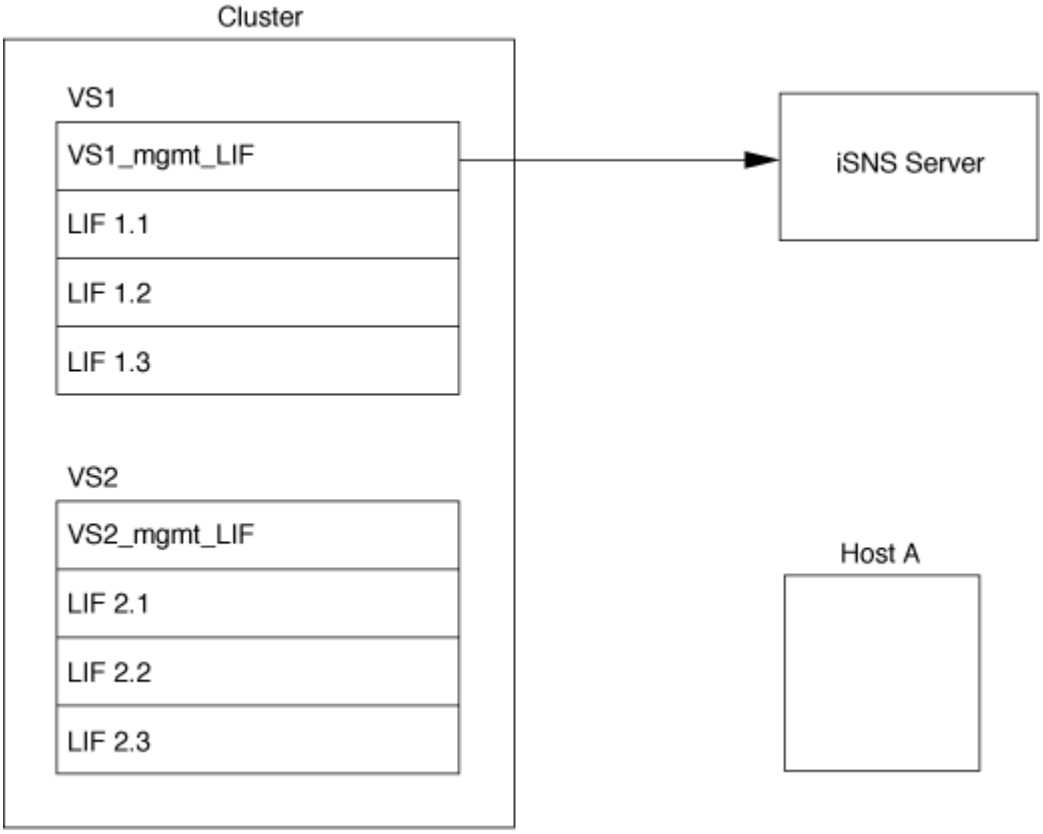
NetApp no suministra ni distribuye servidores iSNS. Puede obtener estos servidores de un proveedor con soporte de NetApp.

Cómo interactúan las SVM con un servidor iSNS

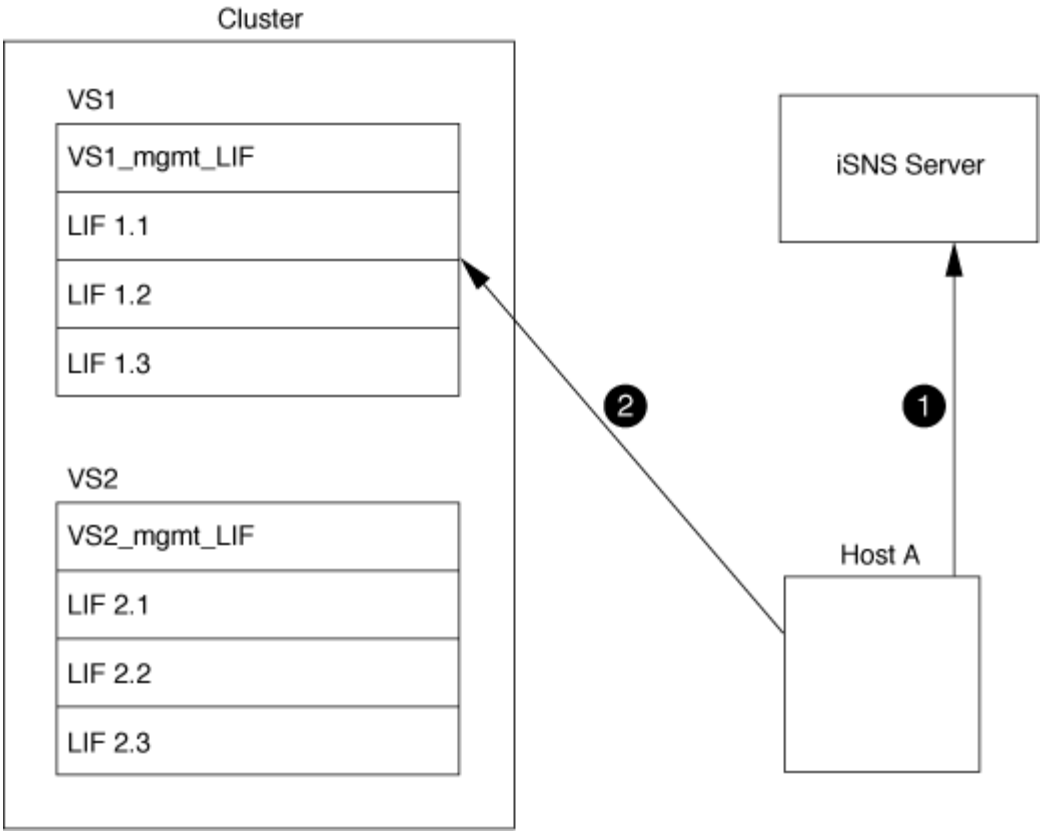
El servidor iSNS se comunica con cada máquina virtual de almacenamiento (SVM) a través de la LIF de gestión de SVM. La LIF de gestión registra toda la información de portal, alias y nombre del nodo de destino de iSCSI con el servicio iSNS para una SVM específica.

En el siguiente ejemplo, SVM «`VS1`» utiliza la LIF de gestión de SVM «`VS1_mgmt_lif`» para registrarse en el

servidor iSNS. Durante el registro de iSNS, una SVM envía todas las LIF de iSCSI a través de la LIF de gestión de SVM al servidor iSNS. Una vez completado el registro de iSNS, el servidor iSNS tendrá una lista de todas las LIF que sirven iSCSI en «`VS1`». Si un clúster contiene varias SVM, cada SVM debe registrarse individualmente con el servidor iSNS para utilizar el servicio iSNS.



En el siguiente ejemplo, después de que el servidor iSNS complete el registro con el destino, el Host A puede detectar todas las LIF para 'VS1' a través del servidor iSNS como se indica en el Paso 1. Una vez que el Host A completa el descubrimiento de las LIF para «`VS1`», el Host A puede establecer una conexión con cualquiera de las LIF en «`VS1`», tal como se muestra en el Paso 2. El host A no tiene en cuenta ninguna de las LIF incluidas en «`VS2`» hasta que la LIF de gestión «`VS2_mgmt_LIF`» para registros «`VS2`» en el servidor iSNS.



Sin embargo, si define las listas de acceso de interfaz, el host solo puede usar las LIF definidas en la lista de acceso de interfaz para acceder al destino.

Una vez que se configura inicialmente iSNS, ONTAP actualiza automáticamente el servidor iSNS cuando cambian las opciones de configuración de SVM.

Es posible que se produzca una demora de unos minutos entre el momento en que realiza cambios en la configuración y la hora en que ONTAP envía la actualización al servidor iSNS. Forzar una actualización inmediata de la información de iSNS en el servidor iSNS: `vserver iscsi isns update`

Comandos para gestionar iSNS

ONTAP proporciona comandos para gestionar el servicio iSNS.

Si desea…	Se usa este comando…
Configure un servicio iSNS	`vserver iscsi isns create`
Inicie un servicio iSNS	`vserver iscsi isns start`
Modifique un servicio iSNS	`vserver iscsi isns modify`
Muestra la configuración de servicio iSNS	`vserver iscsi isns show`
Fuerza una actualización de la información de iSNS registrada	`vserver iscsi isns update`

Detenga un servicio iSNS	`vserver iscsi isns stop`
Quite un servicio iSNS	`vserver iscsi isns delete`
Vea la página man de un comando	`man` *`command name`*

Consulte la página de manual de cada comando para obtener más información.

Aprovisionamiento DE SAN con FC

Debe conocer los conceptos importantes necesarios para comprender cómo implementa ONTAP UNA SAN FC.

Cómo se conectan los nodos de destino de FC a la red

Los sistemas de almacenamiento y hosts cuentan con adaptadores para que se puedan conectar a switches FC con cables.

Cuando un nodo está conectado a LA SAN FC, cada SVM registra el nombre de puerto WWPN de su LIF con el servicio de nombres de estructura del switch. ONTAP asigna automáticamente el WWNN de la SVM y el nombre de puerto WWPN de cada LIF.

> No se admite la conexión directa a nodos de hosts con FC, se requiere NPIV y esto requiere que se utilice un switch.con sesiones iSCSI, la comunicación funciona con conexiones que están enrutadas de red o de conexión directa. Sin embargo, ONTAP admite ambos métodos.

Cómo se identifican los nodos FC

Cada SVM configurada con FC se identifica con un nombre de nodo WWNN.

Cómo se utilizan los WWPN

Los WWPN identifican cada LIF en una SVM configurada para admitir FC. Estos LIF utilizan puertos FC físicos en cada nodo del clúster, que pueden ser tarjetas objetivo FC, UTA o UTA2 configurados como FC o FCoE en los nodos.

- Crear un iGroup

  Los WWPN de los HBA del host se usan para crear un iGroup. Un igroup se utiliza para controlar el acceso del host a una LUN específica. Puede crear un igroup especificando una colección de WWPN de iniciadores en una red de FC. Cuando asigna una LUN en un sistema de almacenamiento a un igroup, puede conceder a todos los iniciadores de ese grupo el acceso a esa LUN. Si el WWPN de un host no está en un igroup que se asigna a una LUN, ese host no tiene acceso a la LUN. Esto significa que los LUN no aparecen como discos en ese host.

  También puede crear conjuntos de puertos para que una LUN sea visible solo en puertos de destino específicos. Un conjunto de puertos consta de un grupo de puertos de destino FC. Es posible enlazar un igroup con un conjunto de puertos. Cualquier host del igroup solo puede acceder a las LUN mediante la conexión a los puertos de destino del puerto establecido.

- Identificación exclusiva de LIF FC

Los WWPN identifican de forma única cada interfaz lógica de FC. El sistema operativo del host utiliza la combinación del WWNN y el WWPN para identificar SVM y LIF de FC. Algunos sistemas operativos requieren un enlace persistente para garantizar que la LUN aparece con el mismo ID objetivo en el host.

Cómo funcionan las asignaciones de nombres en todo el mundo

Los nombres de todo el mundo se crean secuencialmente en ONTAP. Sin embargo, debido a la forma en que ONTAP los asigna, puede parecer que están asignados en un orden no secuencial.

Cada adaptador tiene un WWPN y un WWNN preconfigurados, pero ONTAP no usa estos valores preconfigurados. En su lugar, ONTAP asigna sus propios WWPN o WWN, según las direcciones MAC de los puertos Ethernet internos.

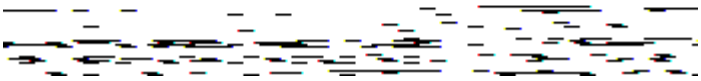
Puede parecer que los nombres internacionales no son secuenciales cuando se asignan por los siguientes motivos:

- Los nombres mundiales se asignan en todos los nodos y las máquinas virtuales de almacenamiento (SVM) del clúster.
- Los nombres liberados en todo el mundo se reciclan y se añaden al grupo de nombres disponibles.

Cómo se identifican los switches FC

Los switches Fibre Channel tienen un nombre de nodo WWNN del dispositivo mismo, y un nombre de puerto WWPN para cada uno de sus puertos.

Por ejemplo, el siguiente diagrama muestra cómo se asignan los WWPN a cada uno de los puertos de un switch Brocade de 16 puertos. Para obtener detalles sobre cómo están numerados los puertos de un switch determinado, consulte la documentación suministrada por el proveedor de ese switch.



Puerto **0**, WWPN 20:**00**:00:60:69:51:06:B4

Puerto **1**, WWPN 20:**01**:00:60:69:51:06:B4

Puerto **14**, WWPN 20:**0e**:00:60:69:51:06:b4

Puerto **15**, WWPN 20:**0f**:00:60:69:51:06:B4

Aprovisionamiento DE SAN con NVMe

A partir de ONTAP 9.4, NVMe/FC es compatible con el entorno SAN. NVMe/FC permite a los administradores de almacenamiento aprovisionar espacios de nombres y subsistemas y, a continuación, asignar los espacios de nombres a subsistemas de, de modo similar al modo en que se aprovisionan y asignan los LUN a iGroups para FC e iSCSI.

Un espacio de nombres NVMe es una cantidad de memoria no volátil que se puede formatear en bloques

lógicos. Los espacios de nombres son el equivalente de LUN para los protocolos FC e iSCSI, y un subsistema NVMe es análogo a un igroup. Los iniciadores asociados pueden acceder a un subsistema NVMe con iniciadores para que los espacios de nombres dentro del subsistema puedan acceder a ellos.

> Si bien son análogos en la función, los espacios de nombres de NVMe no admiten todas las funciones compatibles con los LUN.

A partir de ONTAP 9.5 se requiere una licencia para admitir el acceso a datos que mira el host con NVMe. Si se habilita NVMe en ONTAP 9.4, se concede un periodo de gracia de 90 días para adquirir la licencia antes de actualizar a ONTAP 9.5. Si lo tiene "ONTAP One", Las licencias NVMe están incluidas. Puede habilitar la licencia mediante el siguiente comando:

```
system license add -license-code NVMe_license_key
```

Información relacionada

"Informe técnico de NetApp 4684: Implementación y configuración de San modernas con NVMe/FC"

Volúmenes SAN

Información general sobre SAN Volumes

ONTAP proporciona tres opciones básicas de aprovisionamiento de volúmenes: Aprovisionamiento ligero, aprovisionamiento ligero y aprovisionamiento ligero. Cada opción utiliza diferentes formas de gestionar el espacio de volumen y los requisitos de espacio para las tecnologías de uso compartido de bloques de ONTAP. Comprender cómo funcionan las opciones le permite elegir la mejor opción para su entorno.

> No se recomienda colocar LUN DE SAN y recursos compartidos de NAS en el mismo volumen de FlexVol. Debería aprovisionar volúmenes FlexVol independientes específicamente para sus LUN DE SAN y debería aprovisionar volúmenes FlexVol independientes específicamente para sus recursos compartidos NAS. Esto simplifica la gestión y la replicación y es similar a la forma en la que los volúmenes de FlexVol son compatibles con Active IQ Unified Manager (anteriormente, Unified Manager de OnCommand).

Aprovisionamiento ligero para volúmenes

Cuando se crea un volumen con Thin Provisioning, ONTAP no reserva ningún espacio adicional cuando se crea el volumen. A medida que se escriben datos en el volumen, el volumen solicita el almacenamiento que necesita del agregado para acomodar la operación de escritura. El uso de volúmenes con aprovisionamiento ligero le permite comprometer en exceso su agregado, lo que introduce la posibilidad de que el volumen no pueda asegurar el espacio que necesita cuando el agregado se queda sin espacio libre.

Para crear un volumen de FlexVol con aprovisionamiento fino, debe configurar su `-space-guarantee` opción a. `none`.

Aprovisionamiento grueso para volúmenes

Cuando se crea un volumen con aprovisionamiento grueso, ONTAP reserva suficiente almacenamiento del agregado para garantizar que cualquier bloque del volumen se pueda escribir en cualquier momento. Cuando configura un volumen para utilizar este tipo de aprovisionamiento, puede emplear cualquiera de las funcionalidades de eficiencia del almacenamiento de ONTAP, como la compresión y la deduplicación, para compensar los mayores requisitos de almacenamiento inicial.

Para crear un volumen FlexVol con aprovisionamiento grueso, configure su `-space-slo` (objetivo de nivel de servicio) opción a. `thick`.

Aprovisionamiento para volúmenes semigruesos

Cuando se crea un volumen que utiliza aprovisionamiento grueso, ONTAP establece un espacio de almacenamiento aparte del agregado para tener en cuenta el tamaño del volumen. Si el volumen se está quedando sin espacio libre porque las tecnologías de uso compartido de bloques lo están utilizando, ONTAP realiza un esfuerzo para eliminar objetos de datos de protección (copias Snapshot y archivos FlexClone y LUN) para liberar el espacio en el que se encuentran. Siempre que ONTAP pueda eliminar los objetos de datos de protección con la rapidez suficiente como para responder al ritmo del espacio requerido para las sobrescrituras, las operaciones de escritura siguen teniendo éxito. Esto se denomina «mejor esfuerzo».

Nota: no se admite la siguiente funcionalidad en volúmenes que utilizan aprovisionamiento semi-grueso:

- tecnologías de eficiencia del almacenamiento como la deduplicación, la compresión y la compactación
- Transferencia de datos descargados (ODX) de Microsoft

Para crear un volumen de FlexVol con aprovisionamiento semigrueso, establezca su configuración `-space -slo` (objetivo de nivel de servicio) opción a. `semi-thick`.

Utilice con archivos y LUN reservados en el espacio

Un archivo o LUN con reserva de espacio es uno para el cual se asigna el almacenamiento cuando se crea. Históricamente, NetApp ha utilizado el término «LUN aprovisionada mediante thin provisioning» para indicar una LUN para la que se ha deshabilitado la reserva de espacio (LUN sin reservar espacio).

Nota: los archivos sin espacio reservado no se denominan normalmente «ficheros con Thin-Provisioning».

En la tabla siguiente se resumen las principales diferencias en cómo pueden utilizarse las tres opciones de aprovisionamiento de volúmenes con archivos y LUN con espacio reservado:

Aprovisionamiento de volúmenes	Reserva de espacio de archivos/LUN	Sobrescrituras	Datos de protección 2	Eficiencia del almacenamiento 3
Grueso	Compatible	Garantizado 1	Garantizado	Compatible
Fino	Sin efecto	Ninguno	Garantizado	Compatible
Semi-grueso	Compatible	Mejor esfuerzo 1	El mejor esfuerzo	No admitido

Notas

1. La capacidad para garantizar sobrescrituras o proporcionar una garantía de sobrescritura de mejor esfuerzo requiere que la reserva de espacio esté habilitada en la LUN o el archivo.
2. Los datos de protección incluyen copias Snapshot, y los archivos FlexClone y LUN marcados para su eliminación automática (clones de backup).
3. La eficiencia del almacenamiento incluye deduplicación, compresión, cualquier archivo FlexClone y LUN no marcados para su eliminación automática (clones activos), y subarchivos FlexClone (utilizados para la descarga de copia).

Compatibilidad con LUN aprovisionados mediante thin provisioning de SCSI

ONTAP admite LUN T10 SCSI con thin provisioning, así como LUN con thin provisioning de NetApp. El thin provisioning SCSI T10 permite que las aplicaciones host admitan funciones SCSI como la reclamación de espacio de LUN y las funcionalidades de supervisión de espacio de LUN para entornos de bloques. El thin provisioning SCSI T10 debe ser compatible con su software host SCSI.

Se utiliza ONTAP `space-allocation` Configuración para habilitar o deshabilitar la compatibilidad con thin provisioning T10 en una LUN. Se utiliza ONTAP `space-allocation enable` Configuración para habilitar thin provisioning SCSI T10 en una LUN.

La `[-space-allocation {enabled|disabled}]` En el manual de referencia de comandos de la ONTAP encontrará más información para habilitar o deshabilitar la compatibilidad con el thin provisioning T10 y para habilitar el aprovisionamiento ligero SCSI T10 en una LUN.

"Comandos de ONTAP 9"

Configure las opciones de aprovisionamiento del volumen

Puede configurar un volumen para thin provisioning, thick provisioning o semi-thick provisioning.

Acerca de esta tarea

Ajuste de `-space-slo` opción a. `thick` garantiza lo siguiente:

- El volumen completo se preasigna en el agregado. No puede utilizar el `volume create` o. `volume modify` para configurar el volumen `-space-guarantee` opción.
- se reserva el 100% del espacio requerido para sobrescrituras. No puede utilizar el `volume modify` para configurar el volumen `-fractional-reserve` opción

Ajuste de `-space-slo` opción a. `semi-thick` garantiza lo siguiente:

- El volumen completo se preasigna en el agregado. No puede utilizar el `volume create` o. `volume modify` para configurar el volumen `-space-guarantee` opción.
- No hay espacio reservado para sobrescrituras. Puede utilizar el `volume modify` para configurar el volumen `-fractional-reserve` opción.
- La eliminación automática de copias Snapshot está habilitada.

Paso

1. Configure las opciones de aprovisionamiento del volumen:

   `volume create -vserver` *`vserver_name`* `-volume` *`volume_name`* `-aggregate` *`aggregate_name`* `-space-slo none|thick|semi-thick -space-guarantee none|volume`

   La `-space-guarantee` de forma predeterminada, la opción es `none` Para sistemas AFF y volúmenes DP distintos de AFF. De lo contrario, se establece de forma predeterminada en `volume`. Para los volúmenes de FlexVol existentes, utilice `volume modify` para configurar las opciones de aprovisionamiento.

   El siguiente comando configura vol1 en SVM vs1 para thin provisioning:

```
cluster1::> volume create –vserver vs1 -volume vol1 -space-guarantee
none
```

El siguiente comando configura vol1 en SVM vs1 para el aprovisionamiento grueso:

```
cluster1::> volume create –vserver vs1 -volume vol1 -space-slo thick
```

El siguiente comando configura vol1 en SVM vs1 para un aprovisionamiento semigrueso:

```
cluster1::> volume create –vserver vs1 -volume vol1 -space-slo semi-
thick
```

Opciones de configuración de volúmenes SAN

Debe configurar varias opciones en el volumen que contiene el LUN. La manera en que establece las opciones de volumen determina la cantidad de espacio disponible para las LUN del volumen.

Crecimiento automático

Puede activar o desactivar Autofila. Si se habilita esta función, el crecimiento automático permite que ONTAP aumente automáticamente el tamaño del volumen hasta un tamaño máximo que se determine previamente. Debe haber espacio disponible en el agregado contenedor para admitir el crecimiento automático del volumen. Por lo tanto, si se habilita el crecimiento automático, se debe supervisar el espacio libre en el agregado que contiene y agregar más cuando se necesite.

No se puede activar el crecimiento automático para admitir la creación de copias Snapshot. Si se intenta crear una copia de Snapshot y hay espacio insuficiente en el volumen, se produce un error en la creación de Snapshot, incluso con el crecimiento automático habilitado.

Si se deshabilita el crecimiento automático, el tamaño del volumen seguirá siendo el mismo.

Autohrink

Puede activar o desactivar la función de reducción automática. Si lo habilita, la función de reducción automática permite a ONTAP reducir automáticamente el tamaño total de un volumen cuando la cantidad de espacio consumido en el volumen disminuye un umbral predeterminado. Esto aumenta la eficiencia de almacenamiento al activar los volúmenes para liberar automáticamente espacio libre no utilizado.

Eliminación automática de Snapshot

La eliminación automática de Snapshot elimina automáticamente las copias Snapshot si se produce alguna de las siguientes situaciones:

- El volumen está casi lleno.
- El espacio de reserva de Snapshot está casi lleno.
- El espacio de reserva de sobrescritura está lleno.

Es posible configurar la eliminación automática de Snapshot para eliminar copias de Snapshot de las más antiguas a las más nuevas, o de las más nuevas a las más antiguas. La eliminación automática de Snapshot no elimina las copias de Snapshot vinculadas a las copias de Snapshot en volúmenes o LUN clonados.

Si el volumen necesita espacio adicional y se habilitó el crecimiento automático y la eliminación automática de Snapshot, de manera predeterminada, ONTAP intenta adquirir el espacio necesario mediante la activación del crecimiento automático por primera vez. Si no se adquiere suficiente espacio a través del crecimiento automático, se activa la eliminación automática de Snapshot.

Reserva de Snapshot

La reserva de Snapshot define la cantidad de espacio en el volumen reservado para las copias de Snapshot. El espacio asignado a la reserva de Snapshot no se puede utilizar con ningún otro fin. Si se utiliza todo el espacio asignado a la reserva de Snapshot, las copias snapshot empiezan a consumir espacio adicional en el volumen.

Requisito para mover volúmenes en entornos SAN

Antes de mover un volumen que contiene LUN o espacios de nombres, debe cumplir ciertos requisitos.

- Para los volúmenes que contienen una o más LUN, debe tener un mínimo de dos rutas por LUN (LIF) conectadas a cada nodo del clúster.

  De este modo, se eliminan los puntos únicos de error y el sistema puede sobrevivir a fallos de componentes.

- Para los volúmenes que contienen espacios de nombres, el clúster debe ejecutar ONTAP 9.6 o una versión posterior.

  La transferencia de volúmenes no es compatible con configuraciones de NVMe que ejecuten ONTAP 9.5.

Consideraciones para establecer la reserva fraccionaria

La reserva fraccionaria, también denominada *LUN overwrite reserve*, le permite desactivar la reserva de sobrescritura para archivos y LUN reservados de espacio en un volumen de FlexVol. Esto puede ayudarle a maximizar el uso del almacenamiento, pero si su entorno se ve afectado negativamente por errores en las operaciones de escritura debido a la falta de espacio, debe comprender los requisitos que impone esta configuración.

La configuración de reserva fraccionaria se expresa como un porcentaje; los únicos valores válidos son `0` y.. `100` porcentaje. La configuración de reserva fraccionaria es un atributo del volumen.

Estableciendo la reserva fraccionaria en `0` aumenta la utilización del almacenamiento. Sin embargo, una aplicación que acceda a los datos del volumen puede sufrir una interrupción del servicio de los datos si el volumen no tiene espacio libre, incluso con la garantía de volumen establecida en `volume`. Sin embargo, con una configuración de volumen y un uso adecuados, se puede minimizar la posibilidad de que falle la escritura. ONTAP proporciona una garantía de escritura «"best effort"» para volúmenes con reserva fraccionaria establecida en `0` cuando se cumplan *all* de los siguientes requisitos:

- La deduplicación no se está utilizando

- La compresión no se está utilizando
- No se utilizan subarchivos FlexClone
- Todos los archivos de FlexClone y LUN de FlexClone están habilitados para la eliminación automática

  Esta no es la configuración predeterminada. Debe habilitar de forma explícita la eliminación automática, ya sea en el momento de la creación o modificando el archivo FlexClone o la LUN de FlexClone después de crearla.

- No se están utilizando la descarga de copias ODX y FlexClone
- La garantía de volumen se establece en `volume`
- La reserva de espacio de la LUN o el archivo es `enabled`
- La reserva de copias Snapshot de volumen se establece en `0`
- La eliminación automática de copias Snapshot de volumen es `enabled` con un nivel de compromiso de `destroy`, una lista de destrucción de `lun_clone,vol_clone,cifs_share,file_clone,sfsr`, y un disparador de `volume`

  Esta configuración también garantiza que los archivos FlexClone y las LUN de FlexClone se eliminen cuando sea necesario.

Tenga en cuenta que si la tasa de cambios es alta, en raras ocasiones la eliminación automática de la copia snapshot podría quedarse atrás, lo que dará como resultado que el volumen se quede sin espacio, incluso con todas las opciones de configuración requeridas anteriores en uso.

Además, tiene la opción de usar la funcionalidad de crecimiento automático de volumen para reducir la probabilidad de que las copias de snapshot del volumen deban eliminarse automáticamente. Si se habilita la funcionalidad de crecimiento automático, se debe supervisar el espacio libre en el agregado asociado. Si el agregado está lo suficientemente lleno como para evitar que el volumen crezca, es probable que se eliminen más copias snapshot a medida que se agota el espacio libre del volumen.

Si no puede satisfacer todos los requisitos de configuración anteriores y es necesario garantizar que el volumen no se quede sin espacio, debe establecer el valor de reserva fraccionaria del volumen en `100`. Esto requiere más espacio libre de antemano, pero garantiza que las operaciones de modificación de datos tendrán éxito incluso cuando las tecnologías enumeradas anteriormente estén en uso.

El valor predeterminado y los valores permitidos para la configuración de reserva fraccionaria dependen de la garantía del volumen:

Garantía de volumen	Reserva fraccionaria predeterminada	Valores permitidos
Volumen	100	0, 100
Ninguno	0	0, 100

Gestión del espacio del host DE SAN

En un entorno con thin provisioning, la gestión del espacio del host completa el proceso de gestión del espacio desde el sistema de almacenamiento que se ha liberado en el sistema de ficheros host.

El sistema de archivos de host contiene metadatos para realizar un seguimiento de los bloques disponibles para almacenar datos nuevos y qué bloques contienen datos válidos que no deben sobrescribirse. Estos metadatos se almacenan en el LUN. Cuando se elimina un archivo en el sistema de archivos host, los metadatos del sistema de archivos se actualizan para marcar los bloques del archivo como espacio libre. El espacio libre total del sistema de archivos se vuelve a calcular para incluir los bloques recién liberados. Para el sistema de almacenamiento, estas actualizaciones de metadatos no aparecen diferentes de cualquier otra escritura que realice el host. Por lo tanto, el sistema de almacenamiento no es consciente de que se han producido eliminaciones.

Esto crea una discrepancia entre la cantidad de espacio libre notificada por el host y la cantidad de espacio libre notificada por el sistema de almacenamiento subyacente. Por ejemplo, suponga que tiene un LUN de 200 GB recién aprovisionado asignado al host mediante el sistema de almacenamiento. Tanto el host como el sistema de almacenamiento informan de 200 GB de espacio libre. Luego, el host escribe 100 GB de datos. En este momento, tanto el host como el sistema de almacenamiento informan de 100 GB de espacio usado y 100 GB de espacio no utilizado.

A continuación, elimina 50 GB de datos del host. En este momento, su host informará de 50 GB de espacio usado y 150 GB de espacio no utilizado. Sin embargo, el sistema de almacenamiento informará de 100 GB de espacio usado y 100 GB de espacio sin utilizar.

La gestión del espacio en el host utiliza diversos métodos para conciliar la diferencia de espacio entre el host y el sistema de almacenamiento.

Gestión de hosts simplificada con SnapCenter

Es posible utilizar el software SnapCenter para simplificar algunas de las tareas de gestión y protección de datos asociadas con el almacenamiento iSCSI y FC. SnapCenter es un paquete de gestión opcional para los hosts Windows y UNIX.

Puede utilizar el software SnapCenter para crear fácilmente discos virtuales a partir de pools de almacenamiento que pueden distribuirse entre varios sistemas de almacenamiento y para automatizar las tareas de aprovisionamiento del almacenamiento y simplificar el proceso de creación de copias Snapshot y clones a partir de copias Snapshot consistentes con los datos del host.

Consulte la documentación de productos de NetApp para obtener más información acerca de "SnapCenter".

Enlaces relacionados

"Activar la asignación de espacio para LUN con Thin Provisioning de SCSI"

Acerca de iGroups

Los iGroups son tablas de nombres de WWPN de host de protocolo FC o de nodos de host iSCSI. Puede definir iGroups y asignarlas a LUN para controlar qué iniciadores tienen acceso a las LUN.

Generalmente, desea que todos los puertos de iniciador o iniciadores de software del host tengan acceso a una LUN. Si utiliza software multivía o tiene hosts en clúster, cada puerto iniciador o iniciador de software de cada host en clúster necesita rutas redundantes a la misma LUN.

Es posible crear iGroups para especificar qué iniciadores tienen acceso a las LUN antes o después de crear las LUN, pero debe crear iGroups antes de poder asignar una LUN a un igroup.

Los iGroups pueden tener varios iniciadores, y varios iGroups pueden tener el mismo iniciador. Sin embargo, no puede asignar una LUN a varios iGroups que tengan el mismo iniciador. Un iniciador no puede ser

miembro de iGroups de tipos de configuración distintos.

Ejemplo de cómo los iGroups proporcionan acceso a LUN

Es posible crear varios iGroups para definir qué LUN están disponibles para sus hosts. Por ejemplo, si tiene un clúster de hosts, puede utilizar iGroups para garantizar que determinadas LUN sean visibles solo para un host del clúster o para todos los hosts del clúster.

La siguiente tabla muestra cómo cuatro iGroups dan acceso a las LUN para cuatro hosts diferentes que acceden al sistema de almacenamiento. Los hosts en clúster (Host3 y Host4) son miembros del mismo igroup (group3) y pueden acceder a las LUN asignadas a este igroup. El igroup denominado group4 contiene los WWPN de Host4 para almacenar información local que su socio no debe ver.

Hosts con WWPN de HBA, IQN o EUIs	grupos de iniciadores	WWPN, IQN, EUIs añadidos a iGroups	LUN asignadas a iGroups
Host1, ruta única (iniciador de software iSCSI) iqn.1991-05.com.microsoft:host1	grupo1	iqn.1991-05.com.microsoft:host1	`/vol/vol2/lun1`
Host2, multivía (dos HBA) 10:00:00:00:c9:2b:6b:3c 10:00:00:00:c9:2b:02:3c	grupo 2	10:00:00:00:c9:2b:6b:3c 10:00:00:00:c9:2b:02:3c	`/vol/vol2/lun2`
Host3, multivía, agrupado con host 4 10:00:00:00:c9:2b:32:1b 10:00:00:00:c9:2b:41:02	grupo 3	10:00:00:00:c9:2b:32:1b 10:00:00:00:c9:2b:41:02 10:00:00:00:c9:2b:51:2c 10:00:00:00:c9:2b:47:a2	`/vol/vol2/qtree1/lun3`
Host4, multivía, agrupado (no visible para Host3) 10:00:00:00:c9:2b:51:2c 10:00:00:00:c9:2b:47:a2	grupo 4	10:00:00:00:c9:2b:51:2c 10:00:00:00:c9:2b:47:a2	`/vol/vol2/qtree2/lun4` `/vol/vol2/qtree1/lun5`

Especifique WWPN de iniciador y los nombres de nodo iSCSI para un igroup

Puede especificar los nombres de nodo iSCSI y los WWPN de los iniciadores cuando crea un igroup, o bien puede añadirlos más adelante. Si opta por especificar los nombres de nodo iSCSI y los WWPN de iniciador cuando crea la LUN, pueden eliminarse más adelante, si fuera necesario.

Siga las instrucciones de la documentación de Host Utilities para obtener los WWPN y para encontrar los

nombres de los nodos iSCSI asociados con un host específico. En el caso de los hosts que ejecutan el software ESX, utilice Virtual Storage Console.

Virtualización del almacenamiento con la copia de datos descargados de VMware y Microsoft

Información general sobre la descarga de copias de VMware y Microsoft mediante la virtualización del almacenamiento

VMware y Microsoft admiten operaciones de descarga de copias para aumentar el rendimiento y el rendimiento de la red. Debe configurar su sistema para que cumpla los requisitos de los entornos de sistema operativo VMware y Windows para utilizar sus respectivas funciones de descarga de copias.

Al utilizar la descarga de copias de VMware y Microsoft en entornos virtualizados, deben alinearse los LUN. Las LUN desalineadas pueden degradar el rendimiento.

Ventajas de usar un entorno SAN virtualizado

La creación de un entorno virtualizado mediante LIF y máquinas virtuales de almacenamiento (SVM) le permite expandir su entorno SAN a todos los nodos del clúster.

- Gestión distribuida

  Puede iniciar sesión en cualquier nodo de la SVM para administrar todos los nodos de un clúster.

- Mayor acceso a los datos

  Con MPIO y ALUA, tendrá acceso a los datos a través de cualquier LIF iSCSI o FC activa para la SVM.

- Acceso de LUN controlado

  Si utiliza SLM y conjuntos de puertos, puede limitar qué LIF puede utilizar un iniciador para acceder a las LUN.

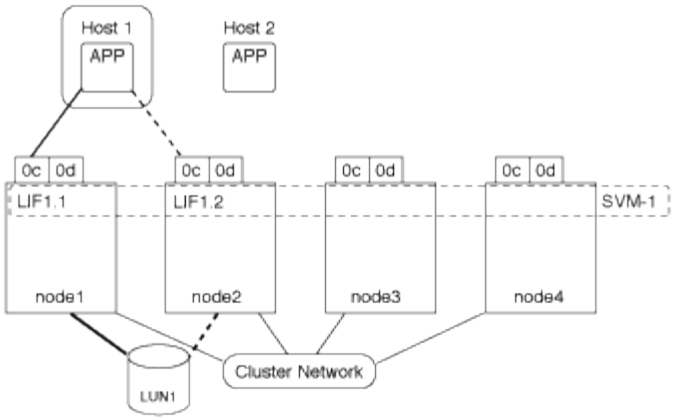
Cómo funciona el acceso de LUN en un entorno virtualizado

En un entorno virtualizado, las LIF permiten que los hosts (clientes) accedan a las LUN a través de rutas optimizadas y sin optimizar.

Una LIF es una interfaz lógica que conecta la SVM a un puerto físico. Aunque varias SVM pueden tener varios LIF en el mismo puerto, un LIF pertenece a una SVM. Puede acceder a las LUN a través de las LIF de SVM.

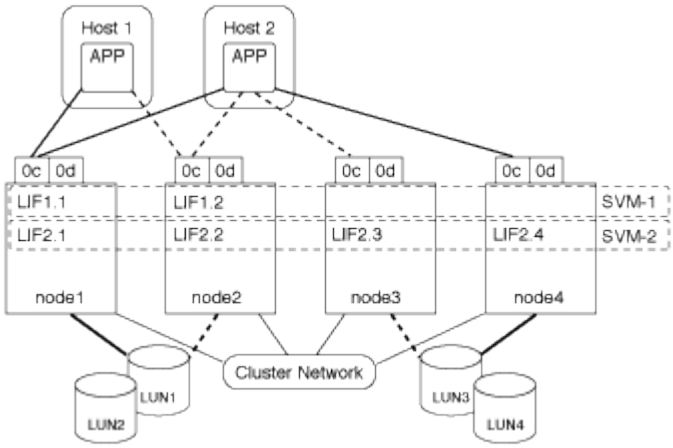
Ejemplo de acceso de LUN con una única SVM en un clúster

En el siguiente ejemplo, el host 1 se conecta a LIF1.1 y LIF1.2 en SVM-1 para acceder a LUN1. LIF1.1 utiliza el puerto físico 1:0c y LIF1.2:0c. LIF1.1 y LIF1.2 sólo pertenecen a SVM-1. Si se crea una nueva LUN en el nodo 1 o en el nodo 2, para SVM-1, puede usar estas mismas LIF. Si se crea una nueva SVM, pueden crearse nuevas LIF con los puertos físicos 0c o 0d de ambos nodos.



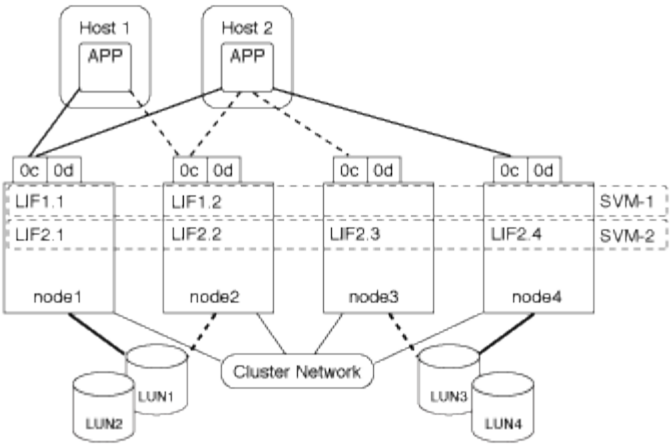
Ejemplo de acceso de la LUN con varias SVM en un clúster

Un puerto físico puede admitir varios LIF que sirven a diferentes SVM. Dado que los LIF están asociados con una SVM determinada, los nodos del clúster pueden enviar el tráfico de datos entrantes a la SVM correcta. En el ejemplo siguiente, cada nodo del 1 al 4 tiene una LIF para SVM-2 utilizando el puerto físico 0c de cada nodo. El host 1 se conecta a LIF1.1 y LIF1.2 en SVM-1 para acceder a LUN1. El host 2 se conecta al LIF2-1 y al LIF2-2 en la SVM-2 para acceder a LUN2. Ambas SVM comparten el puerto físico 0c en los nodos 1 y 2. SVM-2 tiene LIF adicionales que utiliza el host 2 para acceder a las LUN 3 y 4. Estos LIF están utilizando el puerto físico 0c en los nodos 3 y 4. Varias SVM pueden compartir los puertos físicos en los nodos.



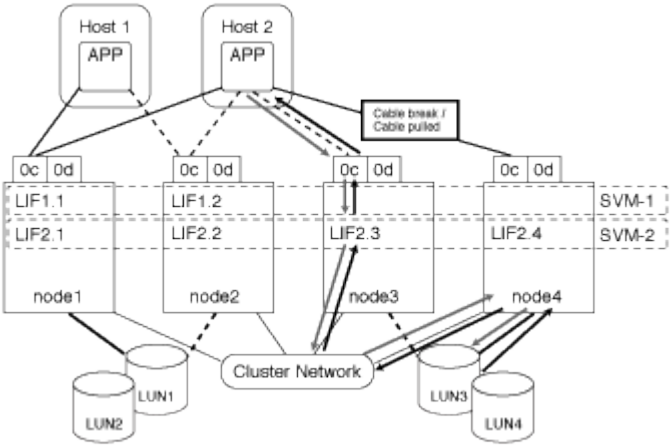
Ejemplo de una ruta activa o optimizada a una LUN desde un sistema host

En una ruta activa o optimizada, el tráfico de datos no viaja a través de la red de clúster; viaja por la ruta más directa a la LUN. La ruta activa o optimizada a LUN1 se realiza a través de LIF1.1 en el nodo 1, utilizando 0c de puerto físico. El host 2 tiene dos rutas activas o optimizadas, una ruta al nodo 1, LIF2.1, que comparte el puerto físico 0c y la otra ruta al nodo 4, LIF2.4, que utiliza el puerto físico 0c.



Ejemplo de una ruta de acceso activa o no optimizada (indirecta) a una LUN desde un sistema host

En una ruta de ruta activa o no optimizada (indirecta), el tráfico de datos viaja por la red de clúster. Este problema se produce solo si todas las rutas activas o optimizadas de un host no están disponibles para manejar el tráfico. Si se pierde la ruta desde el host 2 a la SVM-2 LIF2.4, el acceso a LUN3 y LUN4 atraviesa la red de clúster. El acceso desde el host 2 utiliza LIF2.3 en el nodo 3. A continuación, el tráfico entra en el switch de red de clúster y realiza una copia de seguridad de hasta node4 para acceder a LUN3 y LUN4. A continuación, volverá a atravesar el switch de red del clúster y, a continuación, volverá a pasar por LIF2.3 al host 2. Esta ruta activa o no optimizada se utiliza hasta que se restaura la ruta al LIF2.4 o se establece un nuevo LIF para SVM-2 en otro puerto físico del nodo 4.



=
:allow-uri-read:

Mejore el rendimiento de VMware VAAI para los hosts ESX

ONTAP admite algunas funciones de VMware vStorage APIs for Array Integration (VAAI) cuando el host ESX ejecuta ESX 4.1 o posterior. Estas funciones ayudan a descargar las operaciones del host ESX al sistema de almacenamiento y aumentan el rendimiento de la red. El host ESX habilita las funciones automáticamente en el entorno correcto.

La función VAAI admite los siguientes comandos SCSI:

- `EXTENDED_COPY`

  Esta función permite que el host inicie la transferencia de datos entre las LUN o dentro de una LUN sin

implicar al host en la transferencia de datos. El resultado es guardar los ciclos de CPU de ESX y aumentar el rendimiento de la red. La función de copia ampliada, también conocida como "descarga de copias", se utiliza en situaciones como el clonado de una máquina virtual. Cuando el host ESX lo invoca, la función de descarga de copias copia copia copia copia copia copia los datos del sistema de almacenamiento en lugar de pasar por la red host. La descarga de copias transfiere datos de las siguientes formas:

  - Dentro de una LUN
  - Entre las LUN de un volumen
  - Entre LUN en diferentes volúmenes dentro de una máquina virtual de almacenamiento (SVM)
  - Entre LUN de diferentes SVM dentro de un clúster
    Si no se puede invocar esta función, el host ESX utiliza automáticamente los comandos READ y WRITE estándar para la operación de copia.

- `WRITE_SAME`

  Esta función libera el trabajo de escribir un patrón repetido, como todos los ceros, a una cabina de almacenamiento. El host ESX utiliza esta función en operaciones como rellenar un archivo sin ceros.

- `COMPARE_AND_WRITE`

  Esta función omite ciertos límites de concurrencia de acceso a archivos, lo que acelera operaciones como el arranque de máquinas virtuales.

Requisitos para usar el entorno VAAI

Las funciones VAAI forman parte del sistema operativo ESX y las invoca automáticamente el host ESX cuando se configura el entorno correcto.

Los requisitos del entorno son los siguientes:

- El host ESX debe ejecutar ESX 4.1 o una versión posterior.
- El sistema de almacenamiento de NetApp que aloja el almacén de datos de VMware debe ejecutar ONTAP.
- (Solo copia de liberación de sobrecarga) el origen y el destino de la operación de copia de VMware se deben alojar en el mismo sistema de almacenamiento dentro del mismo clúster.

> La función de descarga de copias no admite en este momento la copia de datos entre almacenes de datos VMware alojados en diferentes sistemas de almacenamiento.

Determinar si ESX admite las funciones de VAAI

Para confirmar si el sistema operativo ESX admite las funciones VAAI, puede comprobar vSphere Client o utilizar cualquier otro medio para acceder al host. ONTAP admite los comandos SCSI de forma predeterminada.

Puede comprobar la configuración avanzada del host ESX para determinar si las funciones de VAAI están habilitadas. La tabla indica qué comandos SCSI corresponden a los nombres de control ESX.

Comando SCSI	Nombre del control ESX (función VAAI)
EXTENDED_COPY	`HardwareAcceleratedMove`
WRITE_SAME	`HardwareAcceleratedInit`
COMPARE_Y_WRITE	`HardwareAcceleratedLocking`

Transferencia de datos descargados (ODX) de Microsoft

La transferencia de datos descargados (ODX) de Microsoft, también conocida como *copy fload*, permite transferir datos directamente dentro de un dispositivo de almacenamiento o entre dispositivos de almacenamiento compatibles sin transferir los datos a través del equipo host.

ONTAP admite ODX para los protocolos SMB Y SAN.

En las transferencias de archivos que no tienen ODX, los datos se leen del origen y se transfieren por la red al host. El host transfiere los datos a través de la red al destino. En la transferencia de archivos ODX, los datos se copian directamente del origen al destino sin pasar por el host.

Como las copias descargadas de ODX se realizan directamente entre el origen y el destino, se obtienen importantes beneficios de rendimiento si se realizan copias dentro del mismo volumen, incluido un tiempo de copia más rápido para copias de mismo volumen, reducción del uso de CPU y memoria en el cliente y reducción del uso de ancho de banda de I/O de red. Si las copias se realizan entre volúmenes, es posible que no haya un aumento significativo del rendimiento en comparación con las copias basadas en host.

Para entornos SAN, ODX solo está disponible cuando es compatible tanto con el host como con el sistema de almacenamiento. Los equipos cliente compatibles con ODX y que tengan habilitada ODX automáticamente y de forma transparente utilizan la transferencia de archivos descargados cuando se mueven o copian archivos. ODX se utiliza independientemente de si arrastra y suelta archivos a través del Explorador de Windows o utiliza comandos de copia de archivos de la línea de comandos, o si una aplicación cliente inicia solicitudes de copia de archivos.

Requisitos para usar ODX

Si planea utilizar ODX para descargas de copias, debe estar familiarizado con las consideraciones de compatibilidad de volúmenes, los requisitos del sistema y los requisitos de funcionalidad de software.

Para utilizar ODX, el sistema debe tener lo siguiente:

- ONTAP

  ODX se habilita automáticamente en las versiones compatibles de ONTAP.

- Volumen de origen mínimo de 2 GB

  Para obtener un rendimiento óptimo, el volumen de origen debe ser mayor que 260 GB.

- Compatibilidad con ODX en el cliente Windows

  Windows Server 2012 o posterior admite ODX y Windows 8 o versiones posteriores. La matriz de

interoperabilidad contiene la información más reciente sobre los clientes Windows compatibles.

"Herramienta de matriz de interoperabilidad de NetApp"

- Compatibilidad con aplicaciones de copia para ODX

  La aplicación que realiza la transferencia de datos debe ser compatible con ODX. Las operaciones de aplicaciones compatibles con ODX incluyen lo siguiente:

  - Las operaciones de gestión de Hyper-V, como la creación y conversión de discos duros virtuales (VHD), la gestión de copias Snapshot y la copia de archivos entre máquinas virtuales
  - Operaciones del Explorador de Windows
  - Comandos de copia de Windows PowerShell
  - Comandos de copia en el símbolo del sistema de Windows
    La biblioteca de Microsoft TechNet contiene más información sobre las aplicaciones ODX compatibles en servidores y clientes Windows.
- Si se utilizan volúmenes comprimidos, el tamaño del grupo de compresión debe ser de 8 KB.

  No se admite el tamaño del grupo de compresión de 32 KB.

ODX no funciona con los siguientes tipos de volúmenes:

- Volúmenes de origen con capacidades inferiores a 2 GB
- Volúmenes de solo lectura
- "Volúmenes de FlexCache"

  ODX es compatible con los volúmenes de origen FlexCache.

- "Volúmenes semigruesos aprovisionados"

Requisitos especiales de archivo del sistema

Es posible eliminar los archivos ODX que se encuentran en qtrees. No debe quitar ni modificar ningún otro archivo del sistema ODX a menos que el soporte técnico le indique que lo haga.

Cuando se usa la función ODX, existen archivos del sistema ODX en todos los volúmenes del sistema. Estos archivos permiten una representación puntual de los datos utilizados durante la transferencia ODX. Los siguientes archivos del sistema se encuentran en el nivel raíz de cada volumen que contiene LUN o archivos en los que se ha descargado datos:

- `.copy-offload` (un directorio oculto)
- `.tokens` (archivo debajo del oculto `.copy-offload` directorio)

Puede utilizar el `copy-offload delete-tokens -path dir_path -node` *`node_name`* Comando para eliminar un qtree que contiene un archivo ODX.

Casos de uso para ODX

Debe conocer los casos de uso de ODX en SVM para poder determinar en qué circunstancias le proporciona ventajas en rendimiento.

Los servidores y los clientes de Windows que admiten ODX utilizan la descarga de copias como forma predeterminada de copiar datos en servidores remotos. Si el cliente o el servidor Windows no son compatibles con ODX o se produce un error en cualquier momento, la operación de copia o movimiento vuelve a las lecturas y escrituras tradicionales para la operación de copia o movimiento.

Los siguientes casos de uso admiten el uso de copias y movimientos ODX:

- Volumen interno

  Los archivos o LUN de origen y destino están dentro del mismo volumen.

- Entre volúmenes, mismo nodo, misma SVM

  Los archivos de origen y de destino o las LUN se encuentran en distintos volúmenes ubicados en el mismo nodo. Los datos son propiedad de la misma SVM.

- Entre volúmenes, distintos nodos, misma SVM

  Los archivos de origen y de destino o las LUN se encuentran en volúmenes distintos que se encuentran en nodos diferentes. Los datos son propiedad de la misma SVM.

- Entre SVM, mismo nodo

  El archivo de origen y los LUN de destino se encuentran en distintos volúmenes ubicados en el mismo nodo. Los datos son propiedad de diferentes SVM.

- Entre SVM, diferentes nodos

  El archivo o las LUN de origen y destino se encuentran en distintos volúmenes ubicados en nodos diferentes. Los datos son propiedad de diferentes SVM.

- Entre clústeres

  Las LUN de origen y de destino se encuentran en distintos volúmenes ubicados en distintos nodos en varios clústeres. Solo se admite en SAN y no funciona para SMB.

Existen algunos casos de uso especiales adicionales:

- Con la implementación de ODX de ONTAP, se puede utilizar ODX para copiar archivos entre recursos compartidos de SMB y unidades virtuales asociadas a FC o iSCSI.

  Puede utilizar el Explorador de Windows, la CLI de Windows o PowerShell, Hyper-V u otras aplicaciones que admiten ODX para copiar o mover archivos sin problemas mediante la descarga de la copia ODX entre recursos compartidos de SMB y LUN conectados, siempre y cuando los recursos compartidos y las LUN del SMB estén en el mismo clúster.

- Hyper-V proporciona algunos casos de uso adicionales para la descarga de copias ODX:

  - Se puede utilizar la transferencia de la copia ODX mediante Hyper-V para copiar datos dentro o a través de archivos de disco duro virtual (VHD), o bien copiar datos entre recursos compartidos de SMB asignados y LUN iSCSI conectados dentro del mismo clúster.

    Esto permite que las copias de sistemas operativos invitados pasen al almacenamiento subyacente.

  - Al crear discos duros virtuales de tamaño fijo, ODX se utiliza para inicializar el disco con ceros,

empleando un token de cero conocido.

- La descarga de copias ODX se utiliza para la migración de almacenamiento de máquinas virtuales si el almacenamiento de origen y destino está en el mismo clúster.

> Para aprovechar los casos de uso de un paso a través de la descarga de copias ODX mediante Hyper-V, el sistema operativo invitado debe ser compatible con ODX, mientras que los discos del sistema operativo invitado deben ser discos SCSI respaldados por almacenamiento (tanto SMB COMO SAN) que sean compatibles con ODX. Los discos IDE del sistema operativo invitado no admiten el paso a través de ODX.

Administración de SAN

Aprovisionamiento SAN

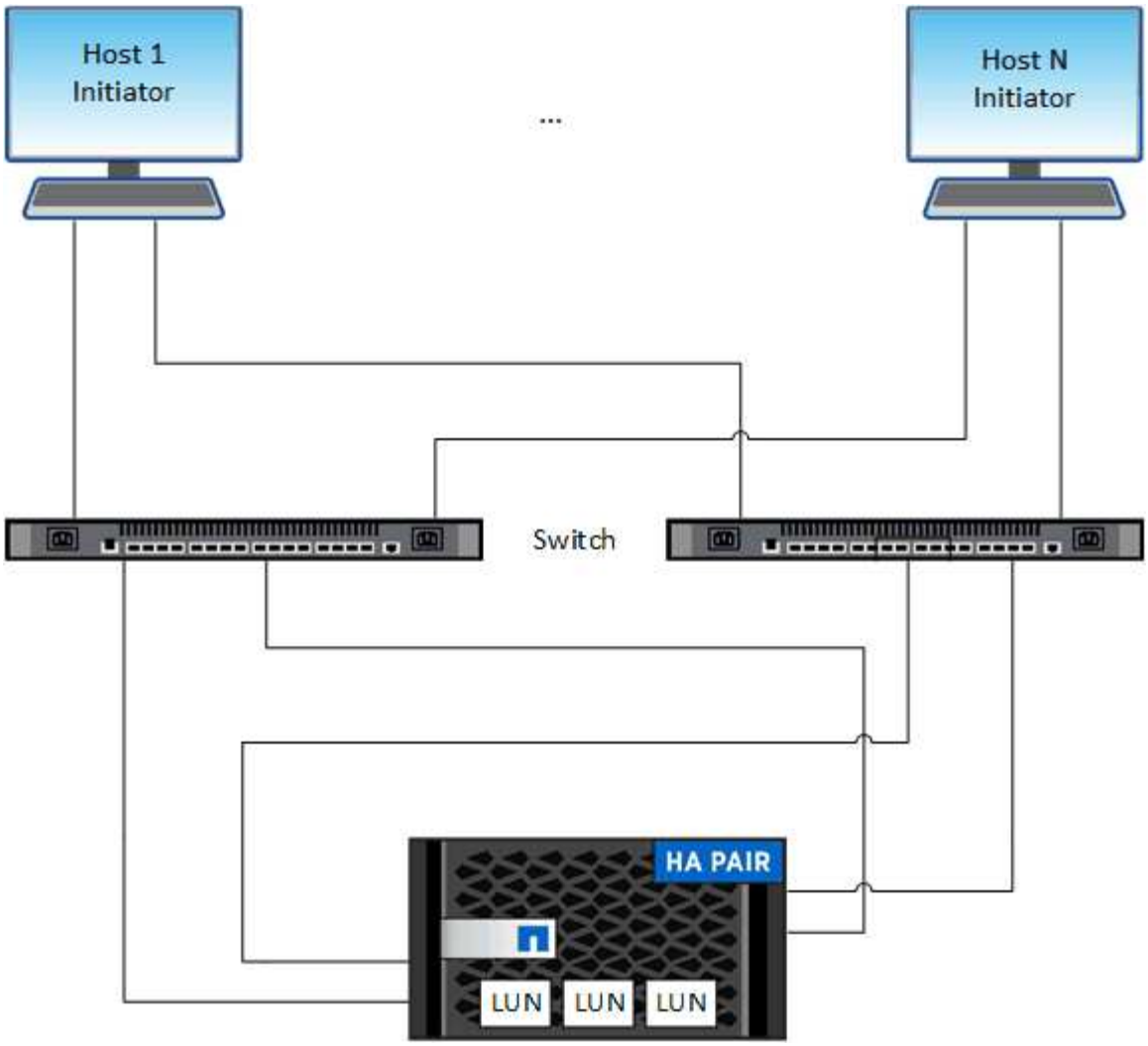
Información general de gestión de San

El contenido de esta sección muestra cómo configurar y gestionar entornos SAN con la interfaz de línea de comandos (CLI) de ONTAP y System Manager en ONTAP 9.7 y versiones posteriores.

Si utiliza la versión clásica de System Manager (disponible solo en ONTAP 9.7 y versiones anteriores), consulte los temas siguientes:

- "Protocolo iSCSI"
- "Protocolo FC/FCoE"

Puede utilizar los protocolos iSCSI y FC para proporcionar almacenamiento en un entorno SAN.



Con iSCSI y FC, los destinos de almacenamiento se denominan LUN (unidades lógicas) y se presentan a los hosts como dispositivos de bloque estándar. Puede crear LUN y, a continuación, asignarlas a iGroups. Los iGroups son tablas de WWN de host FC y nombres de nodos de host iSCSI; además, controlan qué iniciadores tienen acceso a qué LUN.

Los destinos FC se conectan a la red a través de switches FC y adaptadores del lado del host y se identifican por nombres de puerto WWPN. Los destinos iSCSI se conectan a la red a través de adaptadores de red Ethernet (NIC) estándar, tarjetas del motor de descarga TCP (TOE) con iniciadores de software, adaptadores de red convergentes (CNA) o adaptadores de host busto (HBA) dedicados y se identifican mediante nombres completos de iSCSI (IQN).

Configurar los switches para FCoE

Debe configurar los switches de FCoE para que el servicio FC pueda ejecutarse en la infraestructura Ethernet existente.

Lo que necesitará

- Debe ser compatible con la configuración SAN.

  Para obtener más información acerca de las configuraciones admitidas, consulte "Herramienta de matriz de interoperabilidad de NetApp".

- Se debe instalar un adaptador de objetivo unificado (UTA) en el sistema de almacenamiento.

  Si utiliza un UTA2, debe configurarse en `cna` modo.

- Se debe instalar un adaptador de red convergente (CNA) en el host.

Pasos

1. Use la documentación de su switch para configurar los switches para FCoE.
2. Compruebe que los ajustes de DCB para cada nodo del cluster se han configurado correctamente.

   ```
   run -node node1 -command dcb show
   ```

   Los ajustes de DCB se configuran en el switch. Si los ajustes no son correctos, consulte la documentación del switch.

3. Compruebe que el inicio de sesión FCoE funciona cuando el estado en línea del puerto de destino de FC es `true`.

   ```
   fcp adapter show -fields node,adapter,status,state,speed,fabric-
   established,physical-protocol
   ```

   Si el estado en línea del puerto de destino FC es `false`, consulte la documentación del conmutador.

Información relacionada

- "Herramienta de matriz de interoperabilidad de NetApp"
- "Informe técnico de NetApp 3800: Guía de implementación integral de Fibre Channel sobre Ethernet (FCoE)"
- "Guías de configuración de software de Cisco MDS 9000 NX-OS y SAN-OS"
- "Productos Brocade"

Requisitos del sistema

La configuración de LUN implica crear una LUN, crear un igroup y asignar la LUN al igroup. El sistema debe cumplir con ciertos requisitos previos antes de poder configurar las LUN.

- La matriz de interoperabilidad debe incluir la configuración DE SAN como compatible.
- El entorno SAN debe cumplir con los límites DE configuración de host SAN y controladora especificados en "Hardware Universe de NetApp" Para su versión del software ONTAP.
- Se debe instalar una versión compatible de Host Utilities.

  La documentación de Host Utilities proporciona más información.

- Debe tener LIF SAN en el nodo propietario de LUN y el partner de alta disponibilidad del nodo propietario.

Información relacionada

- "Herramienta de matriz de interoperabilidad de NetApp"
- "Configuración de host SAN ONTAP"
- "Informe técnico de NetApp 4017: Prácticas recomendadas de SAN Fibre Channel"

Qué debe saber antes de crear una LUN

Por qué el tamaño real de las LUN varía ligeramente

Debe tener en cuenta lo siguiente con respecto al tamaño de sus LUN.

- Cuando crea una LUN , el tamaño real de la LUN puede variar ligeramente en función del tipo de SO de la LUN. El tipo de SO LUN no se puede modificar una vez que se crea la LUN.
- Si crea una LUN en el tamaño máximo de LUN, tenga en cuenta que el tamaño real de la LUN puede ser ligeramente menor. ONTAP redondea el límite para ser ligeramente menor.
- Los metadatos de cada LUN requieren aproximadamente 64 KB de espacio en el agregado que lo contiene. Cuando crea una LUN, debe asegurarse de que el agregado que contiene tenga suficiente espacio para los metadatos de la LUN. Si el agregado no contiene espacio suficiente para los metadatos de la LUN, es posible que algunos hosts no puedan acceder a la LUN.

Directrices para asignar ID de LUN

Normalmente, el ID de LUN predeterminado comienza con 0 y se asigna en incrementos de 1 para cada LUN asignada adicional. El host asocia el ID de LUN con la ubicación y el nombre de ruta de la LUN. El rango de números de ID de LUN válidos depende del host. Para obtener información detallada, consulte la documentación proporcionada con las utilidades de host.

Directrices para asignar las LUN a iGroups

- Solo puede asignar una LUN una vez a un igroup.
- Como práctica recomendada, debe asignar una LUN a un solo iniciador específico a través del igroup.
- Puede agregar un solo iniciador a varios iGroups, pero el iniciador solo se puede asignar a una LUN.
- No puede utilizar el mismo ID de LUN para dos LUN asignadas al mismo igroup.
- Debe utilizar el mismo tipo de protocolo para iGroups y conjuntos de puertos.

Compruebe y añada su licencia de protocolo FC o iSCSI

Para poder habilitar el acceso en bloque para una máquina virtual de almacenamiento (SVM) con FC o iSCSI, debe tener una licencia. Las licencias FC e iSCSI están incluidas con "ONTAP One".

Ejemplo 1. Pasos

System Manager

Si no tiene ONTAP One, verifique y añada su licencia FC o iSCSI con System Manager de ONTAP (9,7 y posterior).

1. En System Manager, seleccione **Clúster > Configuración > Licencias**
2. Si la licencia no aparece en la lista, seleccione + Add e introduzca la clave de licencia.
3. Seleccione **Agregar**.

CLI

Si no tiene ONTAP One, verifique y añada su licencia FC o iSCSI con la CLI de ONTAP.

1. Compruebe que tiene una licencia activa para FC o iSCSI.

```
system license show
```

```
Package           Type    Description           Expiration
 ---------------- ------- ---------------------
--------------------
 Base              site    Cluster Base License  -
 NFS               site    NFS License           -
 CIFS              site    CIFS License          -
 iSCSI             site    iSCSI License         -
 FCP               site    FCP License           -
```

2. Si no tiene una licencia activa para FC o iSCSI, añada el código de licencia.

```
license add -license-code <your_license_code>
```

Aprovisionar el almacenamiento SAN

Este procedimiento crea nuevas LUN en una máquina virtual de almacenamiento existente que ya tiene configurado el protocolo FC o iSCSI.

Si necesita crear una máquina virtual de almacenamiento nueva y configurar el protocolo FC o iSCSI, consulte "Configure una SVM para FC" o. "Configure una SVM para iSCSI".

Si la licencia de FC no está habilitada, aparecen las LIF y SVM en línea pero el estado operativo está inactivo.

Las LUN aparecen como dispositivos de disco para el host.

El acceso asimétrico de unidad lógica (ALUA, Asymmetric Logical Unit Access) siempre está habilitado durante la creación de una LUN. No se puede cambiar la configuración de ALUA.

Debe usar la división en zonas de iniciador único para todas las LIF FC de la SVM a fin de alojar los iniciadores.

A partir de ONTAP 9.8, cuando se aprovisiona el almacenamiento, la calidad de servicio se habilita de forma predeterminada. Puede deshabilitar la calidad de servicio o seleccionar una política de calidad de servicio personalizada durante el proceso de aprovisionamiento o más adelante.

Ejemplo 2. Pasos

System Manager

Crear LUN para proporcionar almacenamiento para un host SAN mediante el protocolo FC o iSCSI con el Administrador del sistema de ONTAP (9.7 y versiones posteriores).

Para completar esta tarea mediante System Manager Classic (disponible con 9.7 y versiones anteriores), consulte "Configuración iSCSI para Red Hat Enterprise Linux"

Pasos

1. Instale el adecuado "Utilidades host SAN" en el host.
2. En System Manager, haga clic en **almacenamiento > LUN** y, a continuación, haga clic en **Agregar**.
3. Introduzca la información necesaria para crear la LUN.
4. Puede hacer clic en **más opciones** para realizar cualquiera de las siguientes acciones, dependiendo de su versión de ONTAP.

Opción	Disponible empezando por
• Asigne una política de calidad de servicio a las LUN en lugar de al volumen principal ◦ **Más opciones > almacenamiento y optimización** ◦ Seleccione **nivel de servicio de rendimiento**. ◦ Para aplicar la política QoS a LUN individuales en lugar de todo el volumen, seleccione **aplicar estos límites de rendimiento a cada LUN**. De forma predeterminada, los límites de rendimiento se aplican a nivel de volumen.	ONTAP 9.10.1
• Cree un nuevo iGroup mediante los iGroups existentes ◦ **Más Opciones > INFORMACIÓN de HOST** ◦ Seleccione **Nuevo iGroup utilizando los iGroups existentes**. **NOTA**: El tipo de SO para un igroup que contiene otros grupos de iniciadores no se puede cambiar después de que se haya creado.	ONTAP 9.9.1
• Añada una descripción a su igroup o iniciador de host La descripción sirve como alias del igroup o el iniciador del host. ◦ **Más Opciones > INFORMACIÓN de HOST**	ONTAP 9.9.1

• Cree el LUN en un volumen existente De manera predeterminada, se crea un nuevo LUN en un volumen nuevo. ◦ **Más Opciones > Agregar LUN** ◦ Seleccione **Grupo de LUN**.	ONTAP 9.9.1
• Deshabilite QoS o elija una política de calidad de servicio personalizada ◦ **Más opciones > almacenamiento y optimización** ◦ Seleccione **nivel de servicio de rendimiento**. **NOTA**: En ONTAP 9.9.1 y posterior, si selecciona una política de QoS personalizada, también puede seleccionar la colocación manual en un nivel local específico.	ONTAP 9,8

5. Para FC, dividir los switches de FC en zonas mediante WWPN. Use una zona por iniciador e incluya todos los puertos de destino en cada zona.
6. Detectar las LUN en el host.

   Para VMware vSphere, utilice Virtual Storage Console (VSC) para detectar e inicializar los LUN.

7. Inicialice las LUN y, opcionalmente, cree sistemas de archivos.
8. Compruebe que el host puede escribir y leer datos en la LUN.

CLI

Cree LUN para proporcionar almacenamiento para un host SAN mediante el protocolo FC o iSCSI con la CLI de ONTAP.

1. Compruebe que dispone de una licencia para FC o iSCSI.

```
system license show
```

```
Package           Type    Description           Expiration
 ----------------- ------- ---------------------
--------------------
 Base              site    Cluster Base License  -
 NFS               site    NFS License           -
 CIFS              site    CIFS License          -
 iSCSI             site    iSCSI License         -
 FCP               site    FCP License           -
```

2. Si no tiene una licencia para FC o iSCSI, utilice `license add` comando.

```
license add -license-code <your_license_code>
```

3. Habilite el servicio de protocolo en la SVM:

   Para iSCSI:

   ```
   vserver iscsi create -vserver <svm_name> -target-alias <svm_name>
   ```

   Para FC:

   ```
   vserver fcp create -vserver <svm_name> -status-admin up
   ```

4. Cree dos LIF para las SVM en cada nodo:

   ```
   network interface create -vserver <svm_name> -lif <lif_name> -role
   data -data-protocol <iscsi|fc> -home-node <node_name> -home-port
   <port_name> -address <ip_address> -netmask <netmask>
   ```

   NetApp admite un mínimo de un LIF iSCSI o FC por nodo para cada SVM que sirve datos. Sin embargo, se necesitan dos LIF por nodo para redundancia. Para iSCSI, se recomienda configurar un mínimo de dos LIF por nodo en redes Ethernet independientes.

5. Compruebe que sus LIF se han creado y que su estado operativo es `online`:

   ```
   network interface show -vserver <svm_name> <lif_name>
   ```

6. Cree sus LUN:

   ```
   lun create -vserver <svm_name> -volume <volume_name> -lun <lun_name>
   -size <lun_size> -ostype linux -space-reserve <enabled|disabled>
   ```

   El nombre de la LUN no puede superar los 255 caracteres y no puede contener espacios.

   > La opción NVFAIL se habilita automáticamente cuando se crea una LUN en un volumen.

7. Cree sus iGroups:

   ```
   igroup create -vserver <svm_name> -igroup <igroup_name> -protocol
   <fcp|iscsi|mixed> -ostype linux -initiator <initiator_name>
   ```

8. Asigne sus LUN a iGroups:

```
lun mapping create -vserver <svm__name> -volume <volume_name> -lun
<lun_name> -igroup <igroup_name>
```

9. Compruebe que sus LUN están configuradas correctamente:

```
lun show -vserver <svm_name>
```

10. Opcionalmente, "Cree un conjunto de puertos y enlace a un igroup".
11. Siga los pasos de la documentación de host para habilitar el acceso en bloque en los hosts específicos.
12. Use las utilidades de host para completar la asignación de FC o iSCSI y para detectar las LUN en el host.

Información relacionada

- "Información general sobre la administración de SAN"
- "Configuración de host SAN ONTAP"
- "Consulte y gestione los iGroups SAN en System Manager"
- "Informe técnico de NetApp 4017: Prácticas recomendadas de SAN Fibre Channel"

Aprovisionamiento de NVMe

Descripción general de NVMe

Es posible usar el protocolo de memoria no volátil rápida (NVMe) para proporcionar almacenamiento en un entorno SAN. El protocolo NVMe está optimizado para el rendimiento con el almacenamiento de estado sólido.

Para NVMe, los destinos de almacenamiento se denominan espacios de nombres. Un espacio de nombres NVMe es una cantidad de almacenamiento no volátil que se puede formatear en bloques lógicos y presentarla a un host como dispositivo de bloques estándar. Se crean espacios de nombres y subsistemas y, a continuación, se asignan los espacios de nombres a los subsistemas de, de modo similar al modo en que se aprovisionan las LUN y se asignan a iGroups para FC e iSCSI.

Los destinos NVMe se conectan a la red a través de una infraestructura FC estándar que utiliza switches FC o una infraestructura TCP estándar que utiliza switches Ethernet y adaptadores del lado del host.

La compatibilidad con NVMe varía según su versión de ONTAP. Consulte "Compatibilidad y limitaciones de NVMe" para obtener más detalles.

Qué es NVMe

El protocolo exprés de memoria no volátil (NVMe) es un protocolo de transporte que se utiliza para acceder a medios de almacenamiento no volátiles.

NVMe over Fabrics (NVMeoF) es una extensión definida por las especificaciones para NVMe que permite la

comunicación basada en NVMe mediante conexiones distintas de PCIe. Esta interfaz permite conectar gabinetes de almacenamiento externos a un servidor.

NVMe se ha diseñado para proporcionar un acceso eficiente a dispositivos de almacenamiento creados con memoria no volátil, desde la tecnología flash hasta las tecnologías de memoria persistente de mayor rendimiento. De este modo, no tiene las mismas limitaciones que los protocolos de almacenamiento diseñados para las unidades de disco duro. Los dispositivos flash y de estado sólido (SSD) son un tipo de memoria no volátil (NVM). NVM es un tipo de memoria que conserva su contenido durante una interrupción de la alimentación. NVMe es un modo de acceder a esa memoria.

Entre las ventajas de NVMe se incluyen mayores velocidades, productividad, rendimiento y capacidad para la transferencia de datos. Entre las características específicas se encuentran las siguientes:

- NVMe está diseñado para tener hasta 64 000 colas.

  Cada cola puede tener hasta 64 000 comandos simultáneos.

- NVMe es compatible con varios proveedores de hardware y software
- NMVe es más productivo con las tecnologías Flash que permiten tiempos de respuesta más rápidos
- NVMe permite solicitudes de datos múltiples para cada «misión» enviada al SSD.

  NVMe tarda menos tiempo en decodificar una «misión» y no requiere bloqueo de subprocesos en un programa multiproceso.

- NVMe admite una funcionalidad que evita cuellos de botella a nivel de CPU y posibilita una escalabilidad masiva conforme aumentan los sistemas.

Acerca de los espacios de nombres de NVMe

Un espacio de nombres NVMe es una cantidad de memoria no volátil (NVM) que se puede formatear en bloques lógicos. Los espacios de nombres se usan cuando una máquina virtual de almacenamiento se configura con el protocolo NVMe y es el equivalente de LUN para protocolos FC e iSCSI.

Uno o más espacios de nombres se aprovisionan y están conectados a un host NVMe. Cada espacio de nombres puede admitir distintos tamaños de bloque.

El protocolo NVMe ofrece acceso a los espacios de nombres mediante varias controladoras. El uso de controladores NVMe, que son compatibles con la mayoría de los sistemas operativos, los espacios de nombres de unidades de estado sólido (SSD) aparecen como dispositivos de bloque estándar en los cuales los sistemas de archivos y las aplicaciones se pueden implementar sin ninguna modificación.

Un identificador de espacio de nombres (NSID) es un identificador que utiliza una controladora para proporcionar acceso a un espacio de nombres. Al configurar el NSID para un host o un grupo de hosts, también se puede configurar la accesibilidad a un volumen en un host. Un bloque lógico solo se puede asignar a un único grupo de hosts a la vez, y un grupo de hosts determinado no tiene ningún NSID duplicado.

Acerca de los subsistemas NVMe

Un subsistema NVMe incluye una o más controladoras NVMe, espacios de nombres, puertos del subsistema NVM, un medio de almacenamiento NVM y una interfaz entre la controladora y el medio de almacenamiento NVM. Cuando crea un espacio de nombres NVMe, de forma predeterminada no se asigna a un subsistema. También puede optar por asignarlo a un subsistema nuevo o existente.

Información relacionada

- "Aprovisione el almacenamiento NVMe"
- "Asignar un espacio de nombres NVMe a un subsistema"
- "Configuración de los hosts SAN y los clientes de cloud"

Requisitos para la licencia de NVMe

A partir de ONTAP 9.5, se requiere una licencia para admitir NVMe. Si se habilita NVMe en ONTAP 9.4, se concede un periodo de gracia de 90 días para adquirir la licencia antes de actualizar a ONTAP 9.5.

Puede habilitar la licencia mediante el siguiente comando:

```
system license add -license-code NVMe_license_key
```

Configuración, compatibilidad y limitaciones de NVMe

A partir de ONTAP 9,4, el "Memoria no volátil rápida (NVMe)" el protocolo está disponible para los entornos SAN. FC-NVMe utiliza la misma práctica de configuración física y división en zonas que las redes FC tradicionales pero permite un mayor ancho de banda, un aumento de IOPS y una latencia reducida que FC-SCSI.

Las limitaciones y la compatibilidad de NVMe varían en función de la versión de ONTAP, su plataforma y la configuración. Para obtener detalles sobre su configuración específica, consulte "Herramienta de matriz de interoperabilidad de NetApp". Para conocer los límites admitidos, consulte "Hardware Universe".

> El número máximo de nodos por clúster está disponible en Hardware Universe bajo **Mezcla de plataformas soportada**.

Configuración

- Puede establecer su configuración NVMe con una sola estructura o multiestructura.
- Debe configurar una LIF de gestión para cada SVM compatible con SAN.
- No se admite el uso de estructuras heterogéneas de switches FC, a excepción de los switches blade integrados.

  Las excepciones específicas se enumeran en la "Herramienta de matriz de interoperabilidad de NetApp".

- Las estructuras en cascada, malla parcial, malla completa, núcleo-borde y director son métodos estándar en el sector para conectar switches FC a una estructura, y todos son compatibles.

  Una estructura puede estar compuesta por uno o varios switches y las controladoras de almacenamiento se pueden conectar a varios switches.

Funciones

Las siguientes funciones de NVMe se admiten según la versión de ONTAP.

Iniciando con ONTAP…	Compatibilidad con NVMe

9.12.1	Configuraciones IP de MetroCluster de 4 nodos en NVMe/FC. • Las configuraciones de MetroCluster no son compatibles con NVMe antes de la versión 9.12.1. • Las configuraciones de MetroCluster no son compatibles con NVMe/TCP.
9.10.1	Cambiar el tamaño de un espacio de nombres
9.9.1	• Los espacios de nombres y LUN coexisten en el mismo volumen.
9,8	• Coexistencia con protocolos Pueden existir los protocolos SCSI, NAS y NVMe en la misma máquina virtual de almacenamiento (SVM). Antes de ONTAP 9,8, NVMe puede ser el único protocolo en la SVM. *
9,6	• bloques de 512 bytes y bloques de 4096 bytes para espacios de nombres 4096 es el valor predeterminado. 512 solo se debe utilizar si el sistema operativo del host no admite bloques de 4096 bytes. • Movimiento de volúmenes con espacios de nombres asignados
9,5	Conmutación/retorno al nodo primario de la pareja de HA de múltiples rutas.

Protocolos

Se admiten los siguientes protocolos NVMe.

Protocolo	Iniciando con ONTAP…	Permitido por…
TCP	9.10.1	Predeterminado
FC	9,4	Predeterminado

A partir de ONTAP 9,8, puede configurar los protocolos SCSI, NAS y NVMe en la misma máquina virtual de almacenamiento (SVM).
En ONTAP 9,7 y versiones anteriores, NVMe puede ser el único protocolo en la SVM.

Espacios de nombres

Cuando trabaje con espacios de nombres de NVMe, debe tener en cuenta lo siguiente:

- Si pierde datos en una LUN, no se pueden restaurar desde un espacio de nombres o viceversa.
- La garantía de espacio para espacios de nombres es la misma que la garantía de espacio del volumen que contiene.
- No se puede crear un espacio de nombres en una transición de volúmenes desde Data ONTAP en 7-Mode.
- Los espacios de nombres no admiten lo siguiente:
  - Cambio de nombre
  - Movimiento entre volúmenes
  - Copia entre volúmenes
  - Copiar bajo demanda

Limitaciones adicionales

Las configuraciones de NVMe no admiten las siguientes funciones de ONTAP:

- Sincr
- Consola de almacenamiento virtual

Lo siguiente solo se aplica a nodos que ejecutan ONTAP 9.4:

- Las LIF y los espacios de nombres de NVMe deben alojarse en el mismo nodo.
- Debe crearse el servicio NVMe antes de crear la LIF NVMe.

Información relacionada

"Prácticas recomendadas para SAN modernas"

Configure una máquina virtual de almacenamiento para NVMe

Si desea usar el protocolo NVMe en un nodo, debe configurar la SVM específicamente para NVMe.

Antes de empezar

Sus adaptadores FC o Ethernet deben ser compatibles con NVMe. Los adaptadores admitidos figuran en la "Hardware Universe de NetApp".

Ejemplo 3. Pasos

System Manager

Configure una máquina virtual de almacenamiento para NVMe con ONTAP System Manager (9.7 y posterior).

Para configurar NVMe en una nueva máquina virtual de almacenamiento	Para configurar NVMe en una máquina virtual de almacenamiento existente
1. En System Manager, haga clic en **almacenamiento > Storage VMs** y, a continuación, haga clic en **Agregar**. 2. Escriba un nombre para la máquina virtual de almacenamiento. 3. Seleccione **NVMe** para el **Protocolo de acceso**. 4. Seleccione **Activar NVMe/FC** o **Activar NVMe/TCP** y **Guardar**.	1. En System Manager, haga clic en **almacenamiento > Storage VMs**. 2. Haga clic en la máquina virtual de almacenamiento que desee configurar. 3. Haga clic en la ficha **Configuración** y, a continuación, haga clic en Junto al protocolo NVMe. 4. Seleccione **Activar NVMe/FC** o **Activar NVMe/TCP** y **Guardar**.

CLI

Configure una máquina virtual de almacenamiento para NVMe con la interfaz de línea de comandos de ONTAP.

1. Si no quiere usar una SVM existente, cree una:

   ```
   vserver create -vserver <SVM_name>
   ```

   a. Compruebe que la SVM se ha creado:

      ```
      vserver show
      ```

2. Compruebe que tiene instalados adaptadores compatibles con NVMe o TCP en el clúster:

   Para NVMe:

   ```
   network fcp adapter show -data-protocols-supported fc-nvme
   ```

   Para TCP:

   ```
   network port show
   ```

3. Si utiliza ONTAP 9.7 o una versión anterior, quite todos los protocolos de la SVM:

```
vserver remove-protocols -vserver <SVM_name> -protocols
iscsi,fcp,nfs,cifs,ndmp
```

A partir de ONTAP 9.8, no es necesario quitar otros protocolos al añadir NVMe.

4. Añada el protocolo NVMe a la SVM:

```
vserver add-protocols -vserver <SVM_name> -protocols nvme
```

5. Si ejecuta ONTAP 9.7 o una versión anterior, compruebe que NVMe sea el único protocolo permitido en la SVM:

```
vserver show -vserver <SVM_name> -fields allowed-protocols
```

NVMe debe ser el único protocolo que se muestra en la `allowed protocols` columna.

6. Cree el servicio NVMe:

```
vserver nvme create -vserver <SVM_name>
```

7. Compruebe que el servicio NVMe se ha creado:

```
vserver nvme show -vserver <SVM_name>
```

La `Administrative Status` De la SVM debe aparecer como `up`.

8. Cree una LIF NVMe/FC:
   - Para ONTAP 9.9.1 o anterior, FC:

     ```
     network interface create -vserver <SVM_name> -lif <lif_name>
     -role data -data-protocol fc-nvme -home-node <home_node> -home
     -port <home_port>
     ```

   - Para ONTAP 9.10.1 o posterior, FC o TCP:

```
network interface create -vserver <SVM_name> -lif <lif_name>
-service-policy <default-data-nvme-tcp | default-data-nvme-fc>
-data-protocol <fcp | fc-nvme | nvme-tcp> -home-node <home_node>
-home-port <home_port> -status-admin up -failover-policy disabled
-firewall-policy data -auto-revert false -failover-group
<failover_group> -is-dns-update-enabled false
```

9. Cree una LIF NVMe/FC en el nodo del partner de alta disponibilidad:
   - Para ONTAP 9.9.1 o anterior, FC:

     ```
     network interface create -vserver <SVM_name> -lif <lif_name>
     -role data -data-protocol fc-nvme -home-node <home_node> -home
     -port <home_port>
     ```

   - Para ONTAP 9.10.1 o posterior, FC o TCP:

     ```
     network interface create -vserver <SVM_name> -lif <lif_name>
     -service-policy <default-data-nvme-tcp | default-data-nvme-fc>
     -data-protocol <fcp | fc-nvme | nvme-tcp> -home-node <home_node>
     -home-port <home_port> -status-admin up -failover-policy disabled
     -firewall-policy data -auto-revert false -failover-group
     <failover_group> -is-dns-update-enabled false
     ```

10. Compruebe que se han creado los LIF NVMe/FC:

    ```
    network interface show -vserver <SVM_name>
    ```

11. Cree volúmenes en el mismo nodo que el LIF:

    ```
    vol create -vserver <SVM_name> -volume <vol_name> -aggregate
    <aggregate_name> -size <volume_size>
    ```

    Si aparece un mensaje de advertencia acerca de la política de eficiencia automática, puede ignorarlo de forma segura.

Aprovisione el almacenamiento NVMe

Utilice estos pasos para crear espacios de nombres y aprovisionar almacenamiento para cualquier host compatible con NVMe en una máquina virtual de almacenamiento existente.

A partir de ONTAP 9.8, cuando se aprovisiona el almacenamiento, la calidad de servicio se habilita de forma predeterminada. Puede deshabilitar la calidad de servicio o seleccionar una política de calidad de servicio personalizada durante el proceso de aprovisionamiento o más adelante.

Antes de empezar

La máquina virtual de almacenamiento debe configurarse para NVMe, y ya se debe configurar el transporte FC o TCP.

System Manager

Con System Manager de ONTAP (9.7 y versiones posteriores), cree espacios de nombres para ofrecer almacenamiento mediante el protocolo NVMe.

Pasos

1. En System Manager, haga clic en **almacenamiento > espacios de nombres NVMe** y, a continuación, haga clic en **Agregar**.

   Si necesita crear un subsistema nuevo, haga clic en **más opciones**.

2. Si está ejecutando ONTAP 9.8 o posterior y desea desactivar QoS o elegir una directiva de QoS personalizada, haga clic en **más opciones** y, a continuación, en **almacenamiento y optimización** seleccione **nivel de servicio de rendimiento**.
3. Dividir los switches de FC en zonas mediante WWPN. Use una zona por iniciador e incluya todos los puertos de destino en cada zona.
4. En el host, detecte los nuevos espacios de nombres.
5. Inicialice el espacio de nombres y formatee el sistema de archivos.
6. Verificar que el host puede escribir y leer datos en el espacio de nombres.

CLI

Si usa la interfaz de línea de comandos de ONTAP, cree espacios de nombres para ofrecer almacenamiento con el protocolo NVMe.

Este procedimiento crea un espacio de nombres y un subsistema NVMe en una máquina virtual de almacenamiento existente que ya se configuró para el protocolo NVMe y luego asigna el espacio de nombres al subsistema para permitir el acceso a los datos desde el sistema host.

Si necesita configurar la máquina virtual de almacenamiento para NVMe, consulte "Configure una SVM para NVMe".

Pasos

1. Compruebe que la SVM esté configurada para NVMe:

   ```
   vserver show -vserver <svm_name> -fields allowed-protocols
   ```

   `NVMe` debe aparecer debajo de la `allowed-protocols` columna.

2. Cree el espacio de nombres NVMe:

   ```
   vserver nvme namespace create -vserver <svm_name> -path <path> -size
   <size_of_namespace> -ostype <OS_type>
   ```

3. Cree el subsistema NVMe:

```
vserver nvme subsystem create -vserver <svm_name> -subsystem
<name_of_subsystem> -ostype <OS_type>
```

El nombre del subsistema NVMe distingue mayúsculas de minúsculas. Debe contener de 1 a 96 caracteres. Se permiten caracteres especiales.

4. Compruebe que se ha creado el subsistema:

```
vserver nvme subsystem show -vserver <svm_name>
```

La `nvme` el subsistema debe aparecer debajo de `Subsystem` columna.

5. Obtenga el NQN del host.
6. Añada el NQN del host al subsistema:

```
vserver nvme subsystem host add -vserver <svm_name> -subsystem
<subsystem_name> -host-nqn <Host_NQN>
```

7. Asigne el espacio de nombres al subsistema:

```
vserver nvme subsystem map add -vserver <svm_name> -subsystem
<subsystem_name> -path <path>
```

Un espacio de nombres solo se puede asignar a un subsistema único.

8. Compruebe que el espacio de nombres está asignado al subsistema:

```
vserver nvme namespace show -vserver <svm_name> -instance
```

El subsistema debe aparecer como `Attached subsystem`.

Asignar un espacio de nombres NVMe a un subsistema

La asignación de un espacio de nombres NVMe a un subsistema permite el acceso a los datos desde el host. Es posible asignar un espacio de nombres NVMe a un subsistema al aprovisionar almacenamiento, o bien puede hacerlo después de que se ha aprovisionado el almacenamiento.

A partir de ONTAP 9.14.1, puede priorizar la asignación de recursos para hosts específicos. De forma predeterminada, cuando se añade un host al subsistema NVMe, se da prioridad regular. Puede usar la interfaz de línea de comandos (CLI) de ONTAP para cambiar manualmente la prioridad predeterminada de regular a alta. Los hosts a los que se asigna una prioridad alta se asignan números de colas de I/O de mayor tamaño y

profundidades de cola.

> Si desea dar una prioridad alta a un host que se añadió a un subsistema en ONTAP 9.13.1 o versiones anteriores, puede cambie la prioridad del host.

Antes de empezar

El espacio de nombres y el subsistema ya deben crearse. Si necesita crear un espacio de nombres y un subsistema, consulte "Aprovisione el almacenamiento NVMe".

Pasos

1. Obtenga el NQN del host.
2. Añada el NQN del host al subsistema:

```
vserver nvme subsystem host add -vserver <SVM_name> -subsystem
<subsystem_name> -host-nqn <Host_NQN_:subsystem._subsystem_name>
```

   Si desea cambiar la prioridad predeterminada del host de normal a alta, use el `-priority high` opción. Esta opción está disponible a partir de ONTAP 9.14.1.

3. Asigne el espacio de nombres al subsistema:

```
vserver nvme subsystem map add -vserver <SVM_name> -subsystem
<subsystem_name> -path <path>
```

   Un espacio de nombres solo se puede asignar a un subsistema único.

4. Compruebe que el espacio de nombres está asignado al subsistema:

```
vserver nvme namespace show -vserver <SVM_name> -instance
```

   El subsistema debe aparecer como `Attached subsystem`.

Gestionar las LUN

Editar el grupo de políticas de calidad de servicio de la LUN

A partir de ONTAP 9.10.1, puede usar System Manager para asignar o quitar políticas de calidad de servicio (QoS) en varias LUN a la vez.

> Si se asigna la política de calidad de servicio en el nivel del volumen, se debe cambiar en el nivel del volumen. Solo puede editar la política de calidad de servicio en el nivel de LUN si originalmente se asignó en el nivel de LUN.

Pasos

1. En System Manager, haga clic en **almacenamiento > LUN**.

2. Seleccione la LUN o los LUN que desee editar.

   Si edita más de una LUN a la vez, las LUN deben pertenecer a la misma máquina virtual de almacenamiento (SVM). Si selecciona los LUN que no pertenecen a la misma SVM, no se muestra la opción para editar el grupo de políticas de calidad de servicio.

3. Haga clic en **más** y seleccione **Editar grupo de políticas QoS**.

Convertir una LUN en un espacio de nombres

A partir de ONTAP 9.11.1, es posible utilizar la interfaz de línea de comandos de ONTAP para convertir sin movimiento un LUN existente a un espacio de nombres NVMe.

Lo que necesitará

- La LUN especificada no debe tener ningún mapa existente en un igroup.
- El LUN no debe estar en una SVM configurada por MetroCluster ni en una relación de SM-BC.
- La LUN no debe ser un extremo de protocolo ni estar vinculada a un extremo de protocolo.
- La LUN no debe tener un prefijo distinto de cero ni un flujo de sufijo.
- La LUN no debe formar parte de una copia Snapshot ni en el lado destino de la relación de SnapMirror como LUN de solo lectura.

Paso

1. Convertir una LUN en un espacio de nombres NVMe:

```
vserver nvme namespace convert-from-lun -vserver -lun-path
```

Desconectar una LUN

A partir de ONTAP 9.10.1, puede utilizar System Manager para desconectar las LUN. Antes de ONTAP 9.10.1, debe utilizar la CLI de ONTAP para desconectar las LUN.

System Manager

Pasos

1. En System Manager, haga clic en **almacenamiento>LUN**.
2. Desconectar una única LUN o varias

Si desea…	Haga esto…
Desconectar una única LUN	Junto al nombre de la LUN, haga clic en ⋮ Y seleccione **desconectar**.
Desconectar varias LUN	1. Seleccione las LUN que desea desconectar. 2. Haga clic en **más** y seleccione **desconectar**.

CLI

Solo puede desconectar una LUN a la vez al utilizar la CLI.

Paso

1. Desconectar la LUN:

```
lun offline <lun_name> -vserver <SVM_name>
```

Cambiar el tamaño de una LUN

Puede aumentar o reducir el tamaño de una LUN.

No se puede cambiar el tamaño de las LUN de Solaris.

Aumentar el tamaño de una LUN

El tamaño al que puede aumentar su LUN varía en función de su versión de ONTAP.

Versión de ONTAP	Tamaño máximo de LUN
ONTAP 9.12.1P2 y posterior	128 TB para plataformas AFF, FAS y ASA
ONTAP 9,8 y versiones posteriores	• 128 TB para plataformas de cabinas All-Flash SAN (ASA • 16 TB para plataformas que no son ASA
ONTAP 9,5, 9,6 y 9,7	16 TB

ONTAP 9.4 o anterior	10 veces el tamaño original de la LUN, pero no superior a 16 TB, que es el tamaño máximo de LUN. Por ejemplo, si crea un LUN de 100 GB, solo puede ampliarlo a 1,000 GB. Es posible que el tamaño máximo real de la LUN no sea exactamente de 16 TB. ONTAP redondea el límite para ser ligeramente menor.

No es necesario desconectar la LUN para aumentar el tamaño. Sin embargo, después de haber aumentado el tamaño, debe volver a analizar el LUN en el host para que el host reconozca el cambio de tamaño.

Consulte la página Command Reference para el `lun resize` Comando para obtener más información acerca de cómo cambiar el tamaño de una LUN.

Ejemplo 4. Pasos

System Manager

Aumente el tamaño de una LUN con System Manager de ONTAP (9.7 y posterior).

1. En System Manager, haga clic en **almacenamiento > LUN**.
2. Haga clic en ⋮ Y seleccione **Editar**.
3. En **almacenamiento y optimización** aumente el tamaño de la LUN y **Guardar**.

CLI

Aumente el tamaño de una LUN con la CLI de ONTAP.

1. Aumentar el tamaño de la LUN:

```
lun resize -vserver <SVM_name> -volume <volume_name> -lun <lun_name>
-size <lun_size>
```

2. Compruebe que ha aumentado el tamaño de LUN:

```
lun show -vserver <SVM_name_>
```

Las operaciones de ONTAP completan el tamaño máximo real de la LUN, de modo que es ligeramente inferior al valor esperado. Además, el tamaño real de la LUN puede variar ligeramente según el tipo de SO de la LUN. Para obtener el valor de tamaño exacto, ejecute los siguientes comandos en el modo avanzado:

```
set -unit B

lun show -fields max-resize-size -volume volume_name -lun lun_name
```

1. Vuelva a analizar el LUN en el host.
2. Siga la documentación del host para hacer que el tamaño de LUN recién creado sea visible para el sistema de archivos del host.

Reducir el tamaño de una LUN

Antes de reducir el tamaño de una LUN, el host necesita migrar los bloques que contienen los datos de la LUN al límite del tamaño de la LUN más pequeño. Debe utilizar una herramienta como SnapCenter para garantizar que la LUN se disminuye correctamente sin truncar los bloques que contengan datos de LUN. No se recomienda reducir manualmente el tamaño del LUN.

Después de reducir el tamaño del LUN, ONTAP notifica automáticamente al iniciador que el tamaño del LUN ha disminuido. Sin embargo, es posible que se requieran pasos adicionales en el host para que el host reconozca el nuevo tamaño de LUN. Consulte la documentación del host para obtener información específica sobre cómo reducir el tamaño de la estructura del archivo host.

Mover una LUN

Puede mover un LUN entre volúmenes dentro de una máquina virtual de almacenamiento (SVM), pero no puede mover un LUN entre varias SVM. Las LUN movidas entre volúmenes dentro de un SVM se mueven inmediatamente y sin pérdida de conectividad.

Lo que necesitará

Si el LUN utiliza una asignación de LUN selectiva (SLM), debería "Modifique la lista SLM Reporting-Nodes" Para incluir el nodo de destino y su partner de alta disponibilidad antes de mover el LUN.

Acerca de esta tarea

Las funciones de eficiencia del almacenamiento, como la deduplicación, la compresión y la compactación, no se conservan durante un movimiento de LUN. Se deben volver a aplicar una vez que se haya completado el movimiento de LUN.

La protección de datos mediante copias Snapshot se produce en el nivel de volumen. Por lo tanto, al mover una LUN, ésta se encuentra bajo el esquema de protección de datos del volumen de destino. Si no tiene establecidas copias de Snapshot para el volumen de destino, no se crean copias de Snapshot de la LUN. Además, todas las copias Snapshot de la LUN se conservan en el volumen original hasta que se eliminan dichas copias.

No se puede mover una LUN a los siguientes volúmenes:

- Un volumen de destino de SnapMirror
- El volumen raíz de SVM

No puede mover los siguientes tipos de LUN:

- LUN creada a partir de un archivo
- Una LUN que tiene el estado NVFAIL
- LUN en una relación de uso compartido de carga
- LUN de clase de extremo de protocolo

Para los LUN de Solaris os_TYPE que tienen 1 TB o más, es posible que se agote el tiempo de espera del host durante el movimiento de la LUN. Para este tipo de LUN, tiene que desmontar la LUN antes de iniciar la transición.

Ejemplo 5. Pasos

System Manager

Mueva una LUN con System Manager de ONTAP (9.7 y posterior).

A partir de ONTAP 9.10.1, se puede usar System Manager para crear un volumen nuevo al mover una sola LUN. En ONTAP 9.8 y 9.9.1, el volumen al que se mueve el LUN debe existir antes de iniciar el movimiento de LUN.

Pasos

1. En System Manager, haga clic en **almacenamiento>LUN**.
2. Haga clic con el botón derecho en la LUN que desea mover y, a continuación, haga clic en ⋮ Y seleccione **mover LUN**.

   En ONTAP 9.10.1, seleccione para mover el LUN a **un volumen existente** o a **Nuevo volumen**.

   Si selecciona crear un nuevo volumen, proporcione las especificaciones del volumen.

3. Haga clic en **mover**.

CLI

Mueva una LUN con la CLI de ONTAP.

1. Mover la LUN:

   ```
   lun move start
   ```

   Durante un período muy breve, la LUN puede verse tanto en el volumen de origen como en el de destino. Esto es normal y se resuelve al finalizar el traslado.

2. Realice un seguimiento del estado de la transferencia y compruebe que la finalización es correcta:

   ```
   lun move show
   ```

Información relacionada

- "Asignación de LUN selectiva"

Eliminar las LUN

Es posible eliminar una LUN de una máquina virtual de almacenamiento (SVM) si ya no se necesita la LUN.

Lo que necesitará

Se debe quitar la asignación de la LUN de su igroup para poder eliminarla.

Pasos

1. Compruebe que la aplicación o el host no están utilizando la LUN.
2. Desasigne la LUN del igroup:

```
lun mapping delete -vserver <SVM_name> -volume <volume_name> -lun
<LUN_name> -igroup <igroup_name>
```

3. Elimine la LUN:

```
lun delete -vserver <SVM_name> -volume <volume_name> -lun <LUN_name>
```

4. Compruebe que ha eliminado la LUN:

```
lun show -vserver <SVM_name>
```

```
Vserver   Path              State    Mapped  Type     Size
--------- ----------------- -------- ------- -------- ------
vs5       /vol/vol16/lun8   online   mapped  windows  10.00GB
```

Qué debe saber antes de copiar las LUN

Debe ser consciente de ciertas cosas antes de copiar una LUN.

Los administradores de clúster pueden copiar una LUN en máquinas virtuales de almacenamiento (SVM) del clúster mediante el `lun copy` comando. Los administradores de clústeres deben establecer la relación entre iguales de las máquinas virtuales de almacenamiento (SVM) mediante el `vserver peer create` Antes de ejecutar una operación de copia de LUN entre SVM. Debe haber suficiente espacio en el volumen de origen para un clon SIS.

Las LUN de las copias Snapshot se pueden usar como LUN de origen del `lun copy` comando. Cuando se copia una LUN mediante `lun copy` Comando, la copia LUN está disponible inmediatamente para acceso de lectura y escritura. La LUN de origen no se modifica por la creación de una copia LUN. Tanto la LUN de origen como la copia LUN existen como LUN únicas con diferentes números de serie de LUN. Los cambios realizados en la LUN de origen no se reflejan en la copia LUN, y los cambios realizados en la copia LUN no se reflejan en la LUN de origen. La asignación de la LUN de origen no se copia en la nueva LUN; es necesario asignar la copia LUN.

La protección de datos mediante copias Snapshot se produce en el nivel de volumen. Por lo tanto, si copia una LUN en un volumen distinto del volumen de la LUN de origen, la LUN de destino cae en el esquema de protección de datos del volumen de destino. Si no tiene establecidas copias de Snapshot para el volumen de destino, no se crean copias de Snapshot de la copia de LUN.

La copia de LUN es una operación no disruptiva.

No se pueden copiar los siguientes tipos de LUN:

- LUN creada a partir de un archivo
- Una LUN con el estado NVFAIL
- LUN en una relación de uso compartido de carga
- LUN de clase de extremo de protocolo

Examine el espacio configurado y usado de una LUN

Conocer el espacio configurado y el espacio real usado para las LUN puede ayudar a determinar la cantidad de espacio que se puede recuperar al hacer la reclamación de espacio, la cantidad de espacio reservado que contiene datos, y el tamaño total configurado en comparación con el tamaño real usado para una LUN.

Paso

1. Vea el espacio configurado en comparación con el espacio real usado para una LUN:

   ```
   lun show
   ```

   En el siguiente ejemplo, se muestra el espacio configurado en comparación con el espacio real utilizado por las LUN en la máquina virtual de almacenamiento (SVM) vs3:

   ```
   lun show -vserver vs3 -fields path, size, size-used, space-reserve
   ```

   ```
   vserver path                    size    space-reserve size-used
   ------- -----------------       ------- ------------- ---------
   vs3     /vol/vol0/lun1          50.01GB disabled      25.00GB
   vs3     /vol/vol0/lun1_backup   50.01GB disabled      32.15GB
   vs3     /vol/vol0/lun2          75.00GB disabled      0B
   vs3     /vol/volspace/lun0      5.00GB  enabled       4.50GB
   4 entries were displayed.
   ```

Activar la asignación de espacio para LUN con Thin Provisioning de SCSI

Si el host admite thin provisioning de SCSI, puede habilitar la asignación de espacio para LUN de SCSI con Thin Provisioning en ONTAP. Cuando se habilita la asignación de espacio, ONTAP notifica al host cuando el volumen se ha quedado sin espacio y el LUN del volumen no puede aceptar escrituras. ONTAP también recupera espacio automáticamente cuando el host elimina datos.

En los hosts que no admiten thin provisioning SCSI, cuando el volumen que contiene LUN se queda sin espacio y no se puede aumentar automáticamente, ONTAP desconecta la LUN. En los hosts compatibles con el thin provisioning SCSI, ONTAP no desconecta la LUN cuando se queda sin espacio. La LUN permanece en línea en modo de solo lectura, y se le notifica al host que la LUN ya no puede aceptar escrituras.

Además, cuando se eliminan datos en un host que admite thin provisioning SCSI, la gestión de espacio en el host identifica los bloques de datos eliminados en el sistema de archivos del host y emite automáticamente

uno o más `SCSI UNMAP` los comandos para liberar los bloques correspondientes en el sistema de almacenamiento.

Antes de empezar

Para permitir la asignación de espacio, el host debe admitir thin provisioning de SCSI. El thin provisioning de SCSI utiliza el aprovisionamiento de bloques lógicos tal como se define en el estándar SCSI SBC-3. Solo los hosts que admiten este estándar pueden utilizar thin provisioning SCSI en ONTAP.

Los siguientes hosts actualmente admiten thin provisioning de SCSI cuando habilita la asignación de espacio:

- Citrix XenServer 6,5 y posterior
- ESXi 5,0 y versiones posteriores
- Kernel UEK de Oracle Linux 6,2 o posterior
- RHEL 6,2 y posterior
- SLES11 y posterior
- Solaris 11,1 y posterior
- Windows

Acerca de esta tarea

De manera predeterminada, la asignación de espacio está deshabilitada para todas las LUN. Debe desconectar la LUN para permitir la asignación de espacio; después debe realizar la detección en el host para que el host reconozca que se ha habilitado la asignación de espacio.

Pasos

1. Desconecte la LUN.

```
lun modify -vserver vserver_name -volume volume_name -lun lun_name
-state offline
```

2. Activar asignación de espacio:

```
lun modify -vserver _vserver_name_ -volume _volume_name_ -lun _lun_name_
-space-allocation enabled
```

3. Compruebe que la asignación de espacio está activada:

```
lun show -vserver _vserver_name_ -volume _volume_name_ -lun _lun_name_
-fields space-allocation
```

4. Conectar la LUN:

```
lun modify -vserver _vserver_name_ -volume _volume_name_ -lun _lun_name_
-state online
```

5. En el host, vuelva a analizar todos los discos para garantizar que el cambio en el `-space-allocation` la opción se detecta correctamente.

Controle y supervise el rendimiento de I/o de las LUN utilizando la calidad de servicio de almacenamiento

Puede controlar el rendimiento de entrada/salida (I/o) a las LUN asignando LUN a los grupos de políticas de calidad de servicio de almacenamiento. Es posible controlar el rendimiento de I/o para garantizar que las cargas de trabajo alcancen objetivos de rendimiento específicos o reducir una carga de trabajo que afecte negativamente a otras cargas de trabajo.

Acerca de esta tarea

Los grupos de directivas aplican un límite máximo de rendimiento (por ejemplo, 100 MB/s). Puede crear un grupo de políticas sin especificar un rendimiento máximo, lo que permite supervisar el rendimiento antes de controlar la carga de trabajo.

También puede asignar máquinas virtuales de almacenamiento (SVM) con volúmenes de FlexVol y LUN a grupos de políticas.

Tenga en cuenta los siguientes requisitos sobre la asignación de una LUN a un grupo de políticas:

- La LUN debe estar contenida en la SVM a la que pertenece el grupo de políticas.

  La SVM se especifica al crear el grupo de políticas.

- Si asigna un LUN a un grupo de políticas, no puede asignar el volumen o la SVM que contiene el LUN a un grupo de políticas.

Para obtener más información acerca de cómo usar la calidad de servicio de almacenamiento, consulte "Referencia de administración del sistema".

Pasos

1. Utilice la `qos policy-group create` comando para crear un grupo de políticas.
2. Utilice la `lun create` o el `lun modify` con el `-qos-policy-group` Parámetro para asignar una LUN a un grupo de políticas.
3. Utilice la `qos statistics` comandos para ver datos de rendimiento.
4. Si es necesario, utilice `qos policy-group modify` comando para ajustar el límite máximo de rendimiento del grupo de políticas.

Herramientas disponibles para supervisar sus LUN de forma efectiva

Hay herramientas disponibles para ayudarle a supervisar de forma efectiva las LUN y evitar quedarse sin espacio.

- Active IQ Unified Manager es una herramienta gratuita que le permite gestionar todo el almacenamiento en todos los clústeres del entorno.
- System Manager es una interfaz gráfica de usuario integrada en ONTAP que le permite gestionar manualmente las necesidades de almacenamiento en el nivel del clúster.
- OnCommand Insight presenta una única vista de la infraestructura de almacenamiento y le permite

configurar la supervisión automática, alertas e informes cuando sus LUN, volúmenes y agregados se están quedando sin espacio de almacenamiento.

Funcionalidades y restricciones de los LUN convertidos

En un entorno SAN, es necesario interrumpir el servicio durante la transición de un volumen de 7-Mode a ONTAP. Debe apagar los hosts para completar la transición. Después de la transición, debe actualizar las configuraciones de host para poder empezar a servir datos en ONTAP

Debe programar una ventana de mantenimiento durante la cual puede apagar los hosts y completar la transición.

Las LUN que se han realizado la transición de Data ONTAP en 7-Mode a ONTAP tienen ciertas funcionalidades y restricciones que afectan a la forma en que se pueden gestionar las LUN.

Puede hacer lo siguiente con las LUN convertidas:

- Vea la LUN mediante `lun show` comando
- Vea el inventario de LUN convertidos desde el volumen de 7-Mode con el `transition 7-mode show` comando
- Restaure un volumen a partir de una copia de Snapshot de 7-Mode

  Al restaurar el volumen, se realiza la transición de todas las LUN capturadas en la copia Snapshot

- Restaure un único LUN de una copia Snapshot de 7-Mode mediante la `snapshot restore-file` comando
- Crear un clon de una LUN en una copia Snapshot de 7-Mode
- Restaure un rango de bloques a partir de una LUN capturada en una copia Snapshot de 7-Mode
- Cree un FlexClone del volumen mediante una copia snapshot de 7-Mode

No se puede hacer lo siguiente con las LUN convertidas:

- Acceda a los clones de LUN respaldados por copias de Snapshot capturados en el volumen

Información relacionada

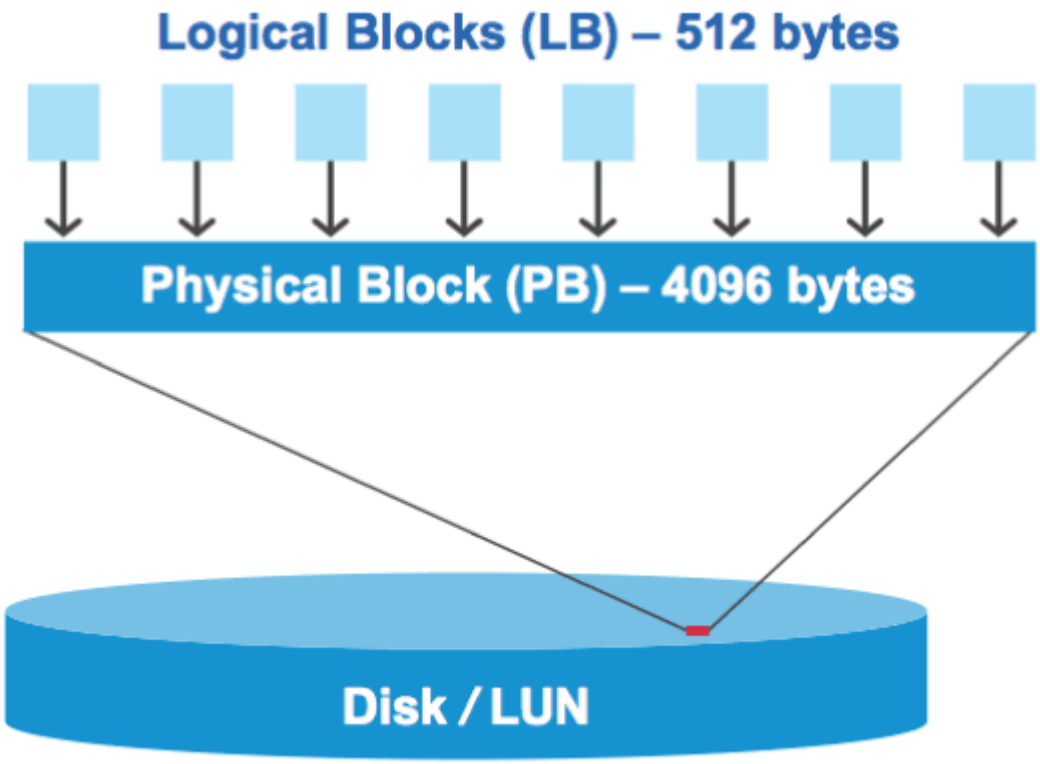
"Transición basada en copias"

Alineación incorrecta de I/o en la descripción general de las LUN alineadas correctamente

ONTAP podría informar de desalineación de I/o en LUN alineadas correctamente. En general, estas advertencias de mala alineación pueden ignorarse mientras tenga la confianza de que su LUN está correctamente aprovisionada y que la tabla de particiones es correcta.

Los LUN y los discos duros proporcionan almacenamiento como bloques. Como el tamaño de bloque de los discos del host es de 512 bytes, los LUN presentan bloques de ese tamaño al host a la vez que utilizan bloques de más grandes de 4 KB para almacenar datos. El bloque de datos de 512 bytes que usa el host se conoce como un bloque lógico. El bloque de datos de 4 KB que utiliza la LUN para almacenar datos se conoce como un bloque físico. Esto significa que hay ocho bloques lógicos de 512 bytes en cada bloque físico de 4

KB.



El sistema operativo host puede iniciar una operación de I/o de lectura o escritura en cualquier bloque lógico. Las operaciones de I/o solo se consideran alineadas cuando comienzan en el primer bloque lógico del bloque físico. Si una operación de I/o se inicia en un bloque lógico que no es también el inicio de un bloque físico, la I/o se considera mal alineada. ONTAP detecta automáticamente los errores de alineación y los informa en la LUN. Sin embargo, la presencia de I/o mal alineadas no significa necesariamente que la unidad lógica tampoco esté alineada. Es posible que se notifique una I/o mal alineada en las LUN alineadas correctamente.

Si necesita más investigación, consulte el artículo de la base de conocimientos "¿Cómo identificar las I/o no alineadas en las LUN?"

Para obtener más información sobre las herramientas para corregir problemas de alineación, consulte la siguiente documentación: +

- "Utilidades unificadas de host de Windows 7.1"
- "Guía de instalación y administración de Virtual Storage Console para VMware vSphere"

Alinear las operaciones de I/o con los tipos de SO de LUN

Para ONTAP 9,7 o anterior, debe usar la LUN de ONTAP recomendada `ostype` Valor que mejor se adapta a su sistema operativo para lograr una alineación de E/S con el esquema de particiones de SO.

El esquema de partición empleado por el sistema operativo host es un factor importante que contribuye a los desalineamientos de E/S. Algunas LUN de ONTAP `ostype` los valores utilizan un desplazamiento especial denominado «'prefix'» para habilitar la alineación del esquema de partición predeterminado utilizado por el sistema operativo host.

En algunas circunstancias, puede que se requiera una tabla de particiones personalizadas para lograr la alineación de las operaciones de I/O. Sin embargo, para `ostype` valores con un valor de «'prefijo'» mayor que `0`, Es posible que una partición personalizada cree E/S mal alineadas

Para obtener más información acerca de las LUN aprovisionadas en ONTAP 9,7 o versiones anteriores, consulte el artículo de la base de conocimientos "Cómo identificar las I/O no alineadas en las LUN".

De forma predeterminada, las nuevas LUN que se aprovisionan en ONTAP 9,8 o una versión posterior tienen un tamaño de prefijo y sufijo de cero para todos los tipos de sistema operativo de LUN. De forma predeterminada, las I/O deben alinearse con el SO del host compatible.

Consideraciones especiales sobre la alineación de E/S para Linux

Las distribuciones de Linux ofrecen una amplia variedad de formas de usar un LUN, como dispositivos sin formato para bases de datos, varios administradores de volúmenes y sistemas de archivos. No es necesario crear particiones en un LUN cuando se usa como dispositivo sin configurar o como volumen físico en un volumen lógico.

Para RHEL 5 y versiones anteriores y SLES 10 y anteriores, si la LUN se utilizará sin un administrador de volúmenes, debe realizar particiones en la LUN para tener una partición que comienza en un desplazamiento alineado, que es un sector que es un múltiplo de ocho bloques lógicos.

Consideraciones especiales sobre la alineación de I/o para las LUN de Solaris

Es necesario tener en cuenta varios factores a la hora de determinar si se debe usar el `solaris` ostype o la `solaris_efi` ostype.

Consulte "Guía de instalación y administración de Solaris Host Utilities" para obtener información detallada.

Los LUN de arranque de ESX no están alineados

ONTAP suele informar de las LUN utilizadas como LUN de arranque de ESX como mal alineadas. ESX crea varias particiones en el LUN de arranque, por lo que es muy difícil realizar una alineación. Las LUN de arranque de ESX mal alineadas no suelen ser un problema de rendimiento, ya que la cantidad total de I/o mal alineadas es pequeña. Suponiendo que la LUN se provisionara correctamente con VMware `ostype`, no se necesita ninguna acción.

Información relacionada

"Alineación de disco/partición del sistema de archivos de máquina virtual invitada para VMware vSphere, otros entornos virtuales y los sistemas de almacenamiento de NetApp"

Formas de abordar problemas cuando las LUN se desconectan

Cuando no hay espacio disponible para las escrituras, las LUN se desconectan para conservar la integridad de los datos. Las LUN pueden quedarse sin espacio y desconectarse por varios motivos, y hay varias formas de abordar el problema.

Si…	Le permite…
El agregado está lleno	• Añada más discos. • Utilice la `volume modify` comando para reducir un volumen que tiene espacio disponible. • Si tiene volúmenes con garantía de espacio que tienen espacio disponible, cambie la garantía de espacio de volumen a. `none` con la `volume modify` comando.
El volumen está lleno, pero hay espacio disponible en el agregado que contiene	• Para los volúmenes de garantía de espacio, utilice `volume modify` comando para aumentar el tamaño del volumen. • Para volúmenes con Thin Provisioning, utilice `volume modify` comando para aumentar el tamaño máximo del volumen. Si no se habilita el crecimiento automático de un volumen, se debe usar `volume modify -autogrow-mode` para habilitar la función. • Elimine copias Snapshot manualmente con el `volume snapshot delete` o utilice el `volume snapshot autodelete modify` Comando para eliminar automáticamente copias Snapshot.

Información relacionada

"Gestión de discos y niveles locales (agregado)"

"Gestión de almacenamiento lógico"

Solucione problemas de LUN iSCSI que no están visibles en el host

Los LUN de iSCSI aparecen como discos locales para el host. Si los LUN del sistema de almacenamiento no están disponibles como discos en el host, debe comprobar los ajustes de configuración.

Ajuste de configuración	Qué hacer
Cableado	Compruebe que los cables entre el host y el sistema de almacenamiento estén conectados correctamente.

Ajuste de configuración	Qué hacer
Conectividad de la red	Compruebe que hay conectividad TCP/IP entre el host y el sistema de almacenamiento. • Desde la línea de comandos del sistema de almacenamiento, haga ping a las interfaces del host que se utilizan para iSCSI: `ping –node` *`node_name`* `-destination` *`host_ip_address_for_iSCSI`* • En la línea de comandos del host, realice una ping en las interfaces del sistema de almacenamiento que se utilizan para iSCSI: `ping –node` *`node_name`* `-destination` *`host_ip_address_for_iSCSI`*
Requisitos del sistema	Compruebe que los componentes de su configuración están cualificados. Además, compruebe que tiene el nivel correcto de paquete de servicio, la versión del iniciador, la versión de ONTAP y otros requisitos del sistema operativo host. La matriz de interoperabilidad contiene los requisitos del sistema más actualizados.
Tramas gigantes	Si utiliza tramas gigantes en la configuración, compruebe que se hayan habilitado tramas gigantes en todos los dispositivos de la ruta de red: La NIC Ethernet del host, el sistema de almacenamiento y todos los switches.
Estado del servicio iSCSI	Compruebe que el servicio iSCSI tiene licencia y se ha iniciado en el sistema de almacenamiento.
Inicio de sesión del iniciador	Compruebe que el iniciador ha iniciado sesión en el sistema de almacenamiento. Si la `iscsi initiator show` el resultado del comando no muestra ningún iniciador con sesión iniciada. compruebe la configuración del iniciador en el host. Compruebe también que el sistema de almacenamiento está configurado como destino del iniciador.
Nombres de nodos iSCSI (IQN)	Compruebe que está usando los nombres de nodo iniciador correctos en la configuración de igroup. En el host, puede usar las herramientas y los comandos del iniciador para mostrar el nombre del nodo iniciador. Los nombres de los nodos del iniciador configurados en el igroup y el host deben coincidir.
Asignaciones de LUN	Compruebe que las LUN se han asignado a un igroup. En la consola del sistema de almacenamiento, puede usar uno de los siguientes comandos: • `lun mapping show` Muestra todas las LUN y los iGroups a los que se les han asignado. • `lun mapping show -igroup` Muestra las LUN asignadas a un igroup específico.

Ajuste de configuración	Qué hacer
Los LIF iSCSI permiten	Compruebe que las interfaces lógicas iSCSI están habilitadas.

Información relacionada

"Herramienta de matriz de interoperabilidad de NetApp"

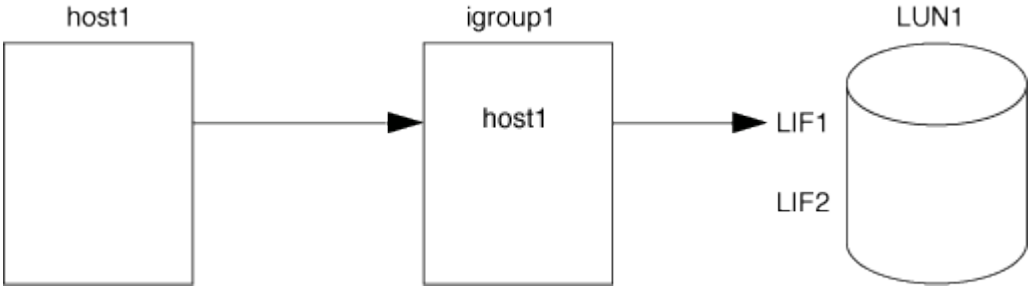
Gestione iGroups y conjuntos de puertos

Formas de limitar el acceso LUN con conjuntos de puertos e iGroups

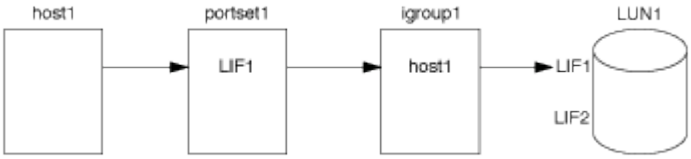
Además de utilizar la asignación de LUN selectiva (SLM), puede limitar el acceso a sus LUN a través de iGroups y conjuntos de puertos.

Los conjuntos de puertos se pueden utilizar con SLM para restringir aún más el acceso de ciertos destinos a ciertos iniciadores. Cuando se utiliza SLM con conjuntos de puertos, se podrá acceder a los LUN en el conjunto de puertos del nodo que posee la LUN y en el partner de alta disponibilidad de ese nodo.

En el ejemplo siguiente, initiator1 no tiene un conjunto de puertos. Sin un conjunto de puertos, initiator1 puede acceder a LUN1 a través de LIF1 y LIF2.



Puede limitar el acceso a LUN1 mediante un conjunto de puertos. En el ejemplo siguiente, initiator1 sólo puede acceder a LUN1 a través de LIF1. Sin embargo, initiator1 no puede acceder a LUN1 a través de LIF2 porque LIF2 no está en portset1.



Información relacionada

- Asignación de LUN selectiva
- Cree un conjunto de puertos y enlace a un igroup

Consulte y gestione iniciadores E iGroups SAN

Es posible usar System Manager para ver y gestionar los iGroups y los iniciadores.

Acerca de esta tarea

- Los iGroups identifican qué hosts pueden acceder a LUN específicas del sistema de almacenamiento.
- Después de crear un iniciador e iGroups, también puede editarlos o eliminarlos.

- Para gestionar los iniciadores y los grupos de iniciadores SAN, puede realizar las tareas siguientes:
  - [view-manage-san-igroups]
  - [view-manage-san-inits]

Consulte y gestione los iGroups SAN

Puede usar System Manager para ver una lista de iGroups. En la lista, es posible ejecutar operaciones adicionales.

Pasos

1. En el Administrador del sistema, haga clic en **hosts > grupos de iniciadores DE SAN**.

   La página muestra una lista de iGroups. Si la lista es grande, puede ver páginas adicionales de la lista haciendo clic en los números de página en la esquina inferior derecha de la página.

   Las columnas muestran información diversa sobre los iGroups. A partir de 9.11.1, también se muestra el estado de conexión del igroup. Pase el ratón sobre las alertas de estado para ver detalles.

2. (Opcional): Puede realizar las siguientes tareas haciendo clic en los iconos de la esquina superior derecha de la lista:
   - **Buscar**
   - **Descargar** la lista.
   - **Mostrar** o **Ocultar** columnas en la lista.
   - **Filtrar** los datos de la lista.
3. Es posible realizar operaciones de la lista:
   - Haga clic en + Add para añadir un igroup.
   - Haga clic en el nombre del igroup para ver la página **Overview** que muestra detalles sobre el igroup.

     En la página **Overview**, puede ver las LUN asociadas con el igroup, y puede iniciar las operaciones para crear las LUN y asignarlas. Haga clic en **All SAN Initiators** para volver a la lista principal.

   - Pase el ratón sobre el igroup y, a continuación, haga clic en ⋮ junto al nombre de un igroup para editar o eliminar el igroup.
   - Pase el ratón sobre el área que se encuentra a la izquierda del nombre del igroup y, a continuación, active la casilla de comprobación. Si hace clic en **+Agregar al iGroup**, puede añadir ese igroup a otro igroup.
   - En la columna **Storage VM**, haga clic en el nombre de una VM de almacenamiento para ver detalles sobre ella.

Consulte y gestione iniciadores DE SAN

Puede usar System Manager para ver una lista de iniciadores. En la lista, es posible ejecutar operaciones adicionales.

Pasos

1. En el Administrador del sistema, haga clic en **hosts > grupos de iniciadores DE SAN**.

   La página muestra una lista de iGroups.

2. Para ver los iniciadores, realice lo siguiente:
   - Haga clic en la ficha **iniciadores FC** para ver una lista de iniciadores FC.
   - Haga clic en la ficha **iSCSI Initiators** para ver una lista de iniciadores iSCSI.

     Las columnas muestran diversa información sobre los iniciadores.

   A partir de 9.11.1, se muestra también el estado de conexión del iniciador. Pase el ratón sobre las alertas de estado para ver detalles.

3. (Opcional): Puede realizar las siguientes tareas haciendo clic en los iconos de la esquina superior derecha de la lista:
   - **Buscar** la lista de iniciadores en particular.
   - **Descargar** la lista.
   - **Mostrar** o **Ocultar** columnas en la lista.
   - **Filtrar** los datos de la lista.

Cree un igroup anidado

A partir de ONTAP 9.9.1, es posible crear un igroup que esté compuesto por otros iGroups existentes.

1. En el Administrador del sistema, haga clic en **Host > grupos de iniciadores SAN** y, a continuación, haga clic en **Agregar**.
2. Introduzca el igroup **Nombre** y **Descripción**.

   La descripción sirve como alias del igroup.

3. Seleccione **Storage VM** y **Host System**.

   El tipo de sistema operativo de un igroup anidado no se puede cambiar una vez que se crea el igroup.

4. En **Miembros del iGroup** seleccione **Grupo iniciador existente**.

   Puede utilizar **Buscar** para buscar y seleccionar los iGroups que desea agregar.

Asigne iGroups a varias LUN

A partir de ONTAP 9.9.1, puede asignar iGroups a dos o más LUN simultáneamente.

1. En System Manager, haga clic en **almacenamiento > LUN**.
2. Seleccione las LUN que desea asignar.
3. Haga clic en **más** y, a continuación, haga clic en **asignar a iGroups**.

Los iGroups seleccionados se agregan a las LUN seleccionadas. Las asignaciones preexistentes no se sobrescriben.

Cree un conjunto de puertos y enlace a un igroup

Además de utilizar "Asignación de LUN selectiva (SLM)", Puede crear un conjunto de puertos y enlazar el conjunto de puertos a un igroup para limitar aún más qué LIF puede usar un iniciador para acceder a una LUN.

Si no se vincula un conjunto de puertos a un igroup, todos los iniciadores del igroup pueden acceder a las LUN asignadas a través de todas las LIF del nodo al que pertenece la LUN y al partner de alta disponibilidad del nodo propietario.

Lo que necesitará

Debe tener al menos un LIF y un igroup.

A menos que utilice grupos de interfaces, se recomiendan dos LIF para redundancia tanto de iSCSI como de FC. Solo se recomienda un LIF para los grupos de interfaces.

Acerca de esta tarea

Es ventajoso utilizar conjuntos de puertos con SLM cuando tiene más de dos LIF en un nodo y desea restringir un iniciador determinado a un subconjunto de LIF. Sin conjuntos de puertos, todos los destinos del nodo podrán acceder a ellos con acceso a la LUN a través del nodo al que pertenece la LUN y del partner de alta disponibilidad del nodo propietario.

Ejemplo 6. Pasos

System Manager

A partir de ONTAP 9.10.1, es posible usar System Manager para crear conjuntos de puertos y vincularlos a iGroups.

Si necesita crear un conjunto de puertos y vincularlo a un igroup en una versión de ONTAP anterior a 9.10.1, debe usar el procedimiento de la CLI de ONTAP.

1. En System Manager, haga clic en **Red > Descripción general > Portsets** y, a continuación, en **Agregar**.
2. Introduzca la información del nuevo conjunto de puertos y haga clic en **Agregar**.
3. Haga clic en **hosts > grupos de iniciadores SAN**.
4. Para enlazar el conjunto de puertos con un nuevo igroup, haga clic en **Add**.

   Para enlazar el conjunto de puertos a un igroup existente, seleccione el igroup, haga clic en ⋮Y, a continuación, haga clic en **Editar iGroup**.

Información relacionada

"Consulte y gestione los iniciadores y los iGroups"

CLI

1. Cree un conjunto de puertos que contenga las LIF correspondientes:

   `portset create -vserver vserver_name -portset portset_name -protocol protocol -port-name port_name`

   Si usa FC, especifique el `protocol` parámetro como `fcp`. Si utiliza iSCSI, especifique el `protocol` parámetro como `iscsi`.

2. Enlace el igroup al conjunto de puertos:

   `lun igroup bind -vserver vserver_name -igroup igroup_name -portset portset_name`

3. Compruebe que sus conjuntos de puertos y LIF son correctos:

   `portset show -vserver vserver_name`

```
Vserver   Portset   Protocol Port Names    Igroups
--------- --------- -------- ------------- --------
vs3       portset0  iscsi    lif0,lif1     igroup1
```

Gestionar conjuntos de puertos

Además de "Asignación de LUN selectiva (SLM)", Puede utilizar conjuntos de puertos para limitar aún más qué LIF puede utilizar un iniciador para acceder a una LUN.

A partir de ONTAP 9.10.1, es posible usar System Manager para cambiar las interfaces de red asociadas con los conjuntos de puertos y eliminar los conjuntos de puertos.

Cambiar las interfaces de red asociadas a un conjunto de puertos

1. En System Manager, seleccione **Network > Overview > Portsets**.
2. Seleccione el conjunto de puertos que desea editar luego ⋮, Luego seleccione **Editar Portset**.

Eliminar un conjunto de puertos

1. En System Manager, haga clic en **Red > Descripción general > Portsets**.
2. Para eliminar un solo conjunto de puertos, seleccione el conjunto de puertos y, a continuación, seleccione ⋮ Y, a continuación, seleccione **Eliminar conjuntos de puertos**.

   Para eliminar varios conjuntos de puertos, seleccione los conjuntos de puertos y haga clic en **Eliminar**.

Información general sobre asignación de LUN selectiva

La asignación selectiva de LUN (SLM) reduce el número de rutas desde el host hacia el LUN. Con SLM, cuando se crea una nueva asignación de LUN, el LUN solo se puede acceder a través de las rutas del nodo al que pertenece la LUN y su partner de alta disponibilidad.

SLM permite gestionar un solo igroup por host y también admite operaciones de movimiento de LUN no disruptivas que no requieren manipulación del conjunto de puertos o reasignación de LUN.

"Conjuntos de puertos" Se puede utilizar con SLM para restringir aún más el acceso de determinados destinos a determinados iniciadores. Cuando se utiliza SLM con conjuntos de puertos, se podrá acceder a los LUN en el conjunto de puertos del nodo que posee la LUN y en el partner de alta disponibilidad de ese nodo.

SLM está habilitado de forma predeterminada en todos los mapas de LUN nuevos.

Determinar si SLM está habilitado en una asignación de LUN

Si su entorno tiene una combinación de LUN creadas en una versión de ONTAP 9 y LUN que han realizado la transición desde versiones anteriores, puede que deba determinar si la asignación de LUN selectiva (SLM) está habilitada en una LUN concreta.

Puede utilizar la información que se muestra en el resultado del `lun mapping show -fields reporting-nodes, node` Comando para determinar si SLM está habilitado en la asignación de LUN. Si SLM no está habilitado, se muestra “-” en las celdas bajo la columna “nodos de portabilidad” de la salida del comando. Si SLM está habilitado, la lista de nodos que se muestran bajo la columna "nodos" se duplica en la columna "nodos de portabilidad".

Modifique la lista nodos de informes de SLM

Si mueve un LUN o un volumen que contiene LUN a otra pareja de alta disponibilidad (ha) dentro del mismo clúster, debe modificar la lista de nodos de generación de informes de asignación de LUN selectiva (SLM) antes de iniciar el movimiento para garantizar que se mantengan las rutas de LUN activas y optimizadas.

Pasos

1. Añada el nodo de destino y su nodo asociado a la lista Reporting-Nodes del volumen o del agregado:

```
lun mapping add-reporting-nodes -vserver _vserver_name_ -path _lun_path_
-igroup _igroup_name_ [-destination-aggregate _aggregate_name_|-
destination-volume _volume_name_]
```

Si tiene una convención de nomenclatura coherente, puede modificar varias asignaciones de LUN al mismo tiempo mediante *igroup_prefix** en lugar de *igroup_name*.

2. Vuelva a analizar el host para detectar las rutas recién añadidas.
3. Si el sistema operativo lo requiere, añada las rutas nuevas a la configuración de I/o de red multivía (MPIO).
4. Ejecute el comando para la operación de movimiento necesaria y espere a que finalice la operación.
5. Compruebe que se está prestando servicio a E/S a través de la ruta activa/optimizada:

```
lun mapping show -fields reporting-nodes
```

6. Elimine el propietario anterior de la LUN y su nodo asociado de la lista de nodos de generación de informes:

```
lun mapping remove-reporting-nodes -vserver _vserver_name_ -path
_lun_path_ -igroup _igroup_name_ -remote-nodes
```

7. Compruebe que la LUN se ha eliminado del mapa de LUN existente:

```
lun mapping show -fields reporting-nodes
```

8. Elimine las entradas obsoletas del dispositivo para el sistema operativo host.
9. Si es necesario, cambie los archivos de configuración de accesos múltiples.
10. Vuelva a analizar el host para verificar la eliminación de las rutas antiguas.
    Consulte la documentación del host para ver los pasos específicos para volver a analizar los hosts.

Gestionar el protocolo iSCSI

Configure su red para obtener el mejor rendimiento

Las redes Ethernet varían en gran medida en cuanto al rendimiento. Se puede maximizar el rendimiento de la red utilizada para iSCSI mediante la selección de valores de configuración específicos.

Pasos

1. Conecte los puertos de host y de almacenamiento a la misma red.

   Se recomienda conectarse a los mismos conmutadores. No se debe usar el enrutamiento.

2. Seleccione los puertos de mayor velocidad disponibles y dedicarlos a iSCSI.

   Los puertos de 10 GbE son los mejores. Los puertos de 1 GbE son el mínimo.

3. Desactive el control de flujo Ethernet para todos los puertos.

   Debería ver "Gestión de redes" Para utilizar la CLI para configurar el control de flujo del puerto Ethernet.

4. Habilitar tramas gigantes (normalmente MTU de 9000).

   Todos los dispositivos de la ruta de datos, incluidos los iniciadores, los destinos y los switches, deben admitir tramas gigantes. De lo contrario, al habilitar tramas gigantes se reduce realmente el rendimiento de red considerablemente.

Configure una SVM para iSCSI

Para configurar una máquina virtual de almacenamiento (SVM) para iSCSI, debe crear LIF para la SVM y asignar el protocolo iSCSI a esas LIF.

Acerca de esta tarea

Necesita un mínimo de un LIF iSCSI por nodo para cada SVM que sirva datos con el protocolo iSCSI. Para redundancia, debe crear al menos dos LIF por nodo.

Ejemplo 7. Pasos

System Manager

Configuración de una máquina virtual de almacenamiento para iSCSI con ONTAP System Manager (9.7 y posterior).

Para configurar iSCSI en un nuevo equipo virtual de almacenamiento	Para configurar iSCSI en un equipo virtual de almacenamiento existente
1. En System Manager, haga clic en **almacenamiento > Storage VMs** y, a continuación, haga clic en **Agregar**. 2. Escriba un nombre para la máquina virtual de almacenamiento. 3. Seleccione **iSCSI** para el **Protocolo de acceso**. 4. Haga clic en **Activar iSCSI** e introduzca la dirección IP y la máscara de subred de la interfaz de red. + cada nodo debe tener al menos dos interfaces de red. 5. Haga clic en **Guardar**.	1. En System Manager, haga clic en **almacenamiento > Storage VMs**. 2. Haga clic en la máquina virtual de almacenamiento que desee configurar. 3. Haga clic en la ficha **Configuración** y, a continuación, haga clic en Junto al protocolo iSCSI. 4. Haga clic en **Activar iSCSI** e introduzca la dirección IP y la máscara de subred de la interfaz de red. + cada nodo debe tener al menos dos interfaces de red. 5. Haga clic en **Guardar**.

CLI

Configuración de una máquina virtual de almacenamiento para iSCSI con la interfaz de línea de comandos de ONTAP.

1. Habilite las SVM para que escuche el tráfico de iSCSI:

   ```
   vserver iscsi create -vserver vserver_name -target-alias vserver_name
   ```

2. Cree una LIF para las SVM de cada nodo que utilice para iSCSI:
   - Para ONTAP 9,6 y versiones posteriores:

     ```
     network interface create -vserver vserver_name -lif lif_name -data
     -protocol iscsi -service-policy default-data-iscsi -home-node node_name
     -home-port port_name -address ip_address -netmask netmask
     ```

   - Para ONTAP 9,5 y versiones anteriores:

     ```
     network interface create -vserver vserver_name -lif lif_name -role data
     -data-protocol iscsi -home-node node_name -home-port port_name -address
     ip_address -netmask netmask
     ```

3. Compruebe que ha configurado las LIF correctamente:

   ```
   network interface show -vserver vserver_name
   ```

4. Compruebe que iSCSI esté en funcionamiento y que el IQN objetivo para esa SVM:

```
vserver iscsi show -vserver vserver_name
```

5. Desde el host, cree sesiones iSCSI con sus LIF.

Información relacionada

"Informe técnico de NetApp 4080: Prácticas recomendadas para SAN moderno"

Definir un método de política de seguridad para un iniciador

Puede definir una lista de iniciadores y sus métodos de autenticación. También puede modificar el método de autenticación predeterminado que se aplica a los iniciadores que no tienen un método de autenticación definido por el usuario.

Acerca de esta tarea

Puede generar contraseñas únicas utilizando algoritmos de directivas de seguridad en el producto o especificar manualmente las contraseñas que desea utilizar.

> No todos los iniciadores admiten contraseñas secretas CHAP hexadecimales.

Pasos

1. Utilice la `vserver iscsi security create` comando para crear un método de política de seguridad para un iniciador.

   ```
   vserver iscsi security create -vserver vs2 -initiator iqn.1991-
   05.com.microsoft:host1 -auth-type CHAP -user-name bob1 -outbound-user-name
   bob2
   ```

2. Siga los comandos de la pantalla para añadir las contraseñas.

   Crea un método de directiva de seguridad para el iniciador iqn.1991-05.com.microsoft:host1 con nombres de usuario y contraseñas CHAP entrantes y salientes.

Información relacionada

- Cómo funciona la autenticación iSCSI
- Autenticación CHAP

Eliminar un servicio iSCSI para una SVM

Es posible eliminar un servicio iSCSI para una SVM si ya no se necesita.

Lo que necesitará

El estado de administración del servicio iSCSI debe estar en el estado «inactivo» antes de poder eliminar un servicio iSCSI. Puede mover el estado de administración a hacia abajo con `vserver iscsi modify` comando.

Pasos

1. Utilice la `vserver iscsi modify` Comando para detener la actividad de I/o de la LUN.

   ```
   vserver iscsi modify -vserver vs1 -status-admin down
   ```

2. Utilice la `vserver iscsi delete` Comando para quitar el servicio iscsi de la SVM.

   ```
   vserver iscsi delete -vserver vs_1
   ```

3. Utilice la `vserver iscsi show command` Para verificar si ha eliminado el servicio iSCSI de la SVM.

   ```
   vserver iscsi show -vserver vs1
   ```

Obtenga más detalles en las recuperaciones de errores de sesión iSCSI

Al aumentar el nivel de recuperación de errores de la sesión iSCSI, es posible recibir información más detallada sobre las recuperaciones de errores de iSCSI. El uso de un nivel de recuperación de errores más alto puede provocar una reducción menor en el rendimiento de la sesión iSCSI.

Acerca de esta tarea

De manera predeterminada, ONTAP se configura para utilizar el nivel de recuperación de errores 0 para sesiones iSCSI. Si está usando un iniciador cualificado para el nivel de recuperación de errores 1 o 2, puede optar por aumentar el nivel de recuperación de errores. El nivel de recuperación de error de sesión modificado afecta solo a las sesiones recién creadas y no afecta a las sesiones existentes.

A partir de ONTAP 9,4, el `max-error-recovery-level` la opción no es compatible con `iscsi show` y.. `iscsi modify` comandos.

Pasos

1. Entrar al modo avanzado:

   ```
   set -privilege advanced
   ```

2. Compruebe la configuración actual mediante la `iscsi show` comando.

   ```
   iscsi show -vserver vs3 -fields max-error-recovery-level
   ```

   ```
   vserver max-error-recovery-level
   ------- ------------------------
   vs3     0
   ```

3. Cambie el nivel de recuperación de error mediante el `iscsi modify` comando.

   ```
   iscsi modify -vserver vs3 -max-error-recovery-level 2
   ```

Registre la SVM en un servidor iSNS

Puede utilizar el `vserver iscsi isns` Comando para configurar la máquina virtual de almacenamiento (SVM) para registrarse en un servidor iSNS.

Acerca de esta tarea

La `vserver iscsi isns create` El comando configura la SVM para registrarse en el servidor iSNS. La

SVM no proporciona comandos que permitan configurar o gestionar el servidor iSNS. Para gestionar el servidor iSNS, puede usar las herramientas de administración del servidor o la interfaz que proporcione el proveedor para el servidor iSNS.

Pasos

1. En el servidor iSNS, asegúrese de que el servicio iSNS esté activo y disponible para su servicio.
2. Cree la LIF de gestión de SVM en un puerto de datos:

   ```
   network interface create -vserver SVM_name -lif lif_name -role data -data
   -protocol none -home-node home_node_name -home-port home_port -address
   IP_address -netmask network_mask
   ```

3. Cree un servicio iSCSI en la SVM si todavía no existe ninguno:

   ```
   vserver iscsi create -vserver SVM_name
   ```

4. Compruebe que el servicio iSCSI se ha creado correctamente:

   ```
   iscsi show -vserver SVM_name
   ```

5. Compruebe que existe una ruta predeterminada para la SVM:

   ```
   network route show -vserver SVM_name
   ```

6. Si no hay ninguna ruta predeterminada para la SVM, cree una ruta predeterminada:

   ```
   network route create -vserver SVM_name -destination destination -gateway
   gateway
   ```

7. Configure la SVM para registrarse con el servicio iSNS:

   ```
   vserver iscsi isns create -vserver SVM_name -address IP_address
   ```

   Se admiten las familias de direcciones IPv4 e IPv6. La familia de direcciones del servidor iSNS debe ser la misma que la de la LIF de gestión de SVM.

   Por ejemplo, no puede conectar una LIF de gestión anSVM con una dirección IPv4 a un servidor iSNS con una dirección IPv6.

8. Compruebe que el servicio iSNS esté en ejecución:

   ```
   vserver iscsi isns show -vserver SVM_name
   ```

9. Si el servicio iSNS no está en ejecución, inícielo:

   ```
   vserver iscsi isns start -vserver SVM_name
   ```

Resuelva los mensajes de error de iSCSI en el sistema de almacenamiento

Hay varios mensajes de error comunes relacionados con iSCSI que se pueden ver con el `event log show` comando. Debe saber qué significan estos mensajes y qué puede hacer para resolver los problemas que identifican.

La siguiente tabla contiene los mensajes de error más comunes e instrucciones para resolverlos:

Mensaje	Explicación	Qué hacer
`ISCSI: network interface identifier disabled for use; incoming connection discarded`	El servicio iSCSI no está habilitado en la interfaz.	Puede utilizar el `iscsi interface enable` Comando para habilitar el servicio iSCSI en la interfaz. Por ejemplo: `iscsi interface enable -vserver vs1 -lif lif1`
`ISCSI: Authentication failed for initiator nodename`	CHAP no está configurado correctamente para el iniciador especificado.	Debe comprobar la configuración de CHAP; no puede usar el mismo nombre de usuario y contraseña para la configuración de entrada y salida en el sistema de almacenamiento: • Las credenciales entrantes en el sistema de almacenamiento deben coincidir con las credenciales salientes en el iniciador. • Las credenciales salientes en el sistema de almacenamiento deben coincidir con las credenciales entrantes del iniciador.

Habilitar o deshabilitar la recuperación tras fallos automática de LIF de iSCSI

Después de actualizar a ONTAP 9.11.1 o una versión posterior, debe habilitar manualmente la conmutación por error automática de LIF en todas las LIF de iSCSI creadas en ONTAP 9.10.1 o una versión anterior.

A partir de ONTAP 9.11.1, puede habilitar la recuperación automática tras fallos de LIF para LIF iSCSI en plataformas de cabinas SAN all-flash. Si se produce una recuperación tras fallos de almacenamiento, el LIF de iSCSI se migra automáticamente desde su nodo o puerto principal a su puerto o nodo de alta disponibilidad asociado y, a continuación, una vez finalizada la recuperación tras fallos. O bien, si el puerto para LIF iSCSI deja de estar en buen estado, la LIF se migra automáticamente a un puerto en buen estado de su nodo inicial actual y de nuevo a su puerto original cuando el estado del puerto vuelve a estar en buen estado. El habilita las cargas de trabajo SAN que se ejecutan en iSCSI para reanudar el servicio de I/O más rápido después de que se experimenta una conmutación al nodo de respaldo.

En ONTAP 9.11.1 y versiones posteriores, de forma predeterminada, los LIF iSCSI recién creados se habilitan para la conmutación automática por error de LIF si se cumple alguna de las siguientes condiciones:

- No hay ningún LIF de iSCSI en la SVM
- Todos los LIF de iSCSI en la SVM están habilitados para la conmutación al respaldo automática de LIF

Activar recuperación tras fallos automática de LIF iSCSI

De manera predeterminada, las LIF de iSCSI creadas en ONTAP 9.10.1 y versiones anteriores no están habilitadas para la conmutación automática por error de LIF. Si hay LIF de iSCSI en la SVM que no están habilitados para la conmutación automática al respaldo de LIF, los LIF creados recientemente no se habilitarán para la conmutación automática por error de LIF. Si la recuperación tras fallos automática de LIF no está habilitada y existe un evento de recuperación tras fallos, los LIF de iSCSI no migrarán.

Más información acerca de "Recuperación tras fallos y restauración de LIF".

Paso

1. Habilitar la recuperación automática tras fallos en una LIF iSCSI:

```
network interface modify -vserver SVM_name -lif iscsi_lif -failover-
policy sfo-partner-only -auto-revert true
```

   Para actualizar todos los LIF iSCSI en la SVM, utilice `-lif*` en lugar de `lif`.

Desactive la recuperación tras fallos automática de LIF de iSCSI

Si anteriormente habilitó conmutación por error automática de LIF de iSCSI en LIF iSCSI creadas en ONTAP 9.10.1 o una versión anterior, tiene la opción de deshabilitarla.

Paso

1. Desactive la recuperación automática tras fallos para una LIF iSCSI:

```
network interface modify -vserver SVM_name -lif iscsi_lif -failover-
policy disabled -auto-revert false
```

   Para actualizar todos los LIF iSCSI en la SVM, utilice `-lif*` en lugar de `lif`.

Información relacionada

- "Cree una LIF"
- Manualmente "Migre una LIF"
- Manualmente "Revierte una LIF a su puerto de inicio"
- "Configure los ajustes de recuperación tras fallos en un LIF"

Gestione el protocolo FC

Configure una SVM para FC

Para configurar una máquina virtual de almacenamiento (SVM) para FC, debe crear LIF para la SVM y asignar el protocolo FC a esas LIF.

Antes de empezar

Debe tener una licencia de FC ("Incluido con ONTAP One") y debe estar activado. Si la licencia de FC no está habilitada, aparecen las LIF y SVM en línea pero el estado operativo es `down`. Para que los LIF y SVM estén

operativos, el servicio FC debe estar habilitado. Debe usar la división en zonas de iniciador único para todas las LIF FC de la SVM a fin de alojar los iniciadores.

Acerca de esta tarea

NetApp admite un mínimo de un LIF de FC por nodo para cada SVM que sirve datos con el protocolo FC. Debe usar dos LIF por nodo y dos estructuras, con un LIF por nodo conectado. De este modo se proporciona redundancia en la capa del nodo y en la estructura.

Ejemplo 8. Pasos

System Manager

Configuración de una máquina virtual de almacenamiento para iSCSI con ONTAP System Manager (9.7 y posterior).

Para configurar FC en un nuevo equipo virtual de almacenamiento	Para configurar FC en una máquina virtual de almacenamiento existente
1. En System Manager, haga clic en **almacenamiento > Storage VMs** y, a continuación, haga clic en **Agregar**. 2. Escriba un nombre para la máquina virtual de almacenamiento. 3. Seleccione **FC** para **Protocolo de acceso**. 4. Haga clic en **Habilitar FC**. + los puertos FC se asignan automáticamente. 5. Haga clic en **Guardar**.	1. En System Manager, haga clic en **almacenamiento > Storage VMs**. 2. Haga clic en la máquina virtual de almacenamiento que desee configurar. 3. Haga clic en la ficha **Configuración** y, a continuación, haga clic en ⚙ Junto al protocolo FC. 4. Haga clic en **Activar FC** e introduzca la dirección IP y la máscara de subred de la interfaz de red. + los puertos FC se asignan automáticamente. 5. Haga clic en **Guardar**.

CLI

1. Habilite el servicio FC en la SVM:

   ```
   vserver fcp create -vserver vserver_name -status-admin up
   ```

2. Cree dos LIF para las SVM en cada nodo que sirva FC:
   - Para ONTAP 9,6 y versiones posteriores:

     ```
     network interface create -vserver vserver_name -lif lif_name -data
     -protocol fcp -service-policy default-data-fcp -home-node node_name
     -home-port port_name -address ip_address -netmask netmask -status-admin
     up
     ```

   - Para ONTAP 9,5 y versiones anteriores:

     ```
     network interface create -vserver vserver_name -lif lif_name -role data
     -data-protocol fcp -home-node node_name -home-port port
     ```

3. Compruebe que sus LIF se han creado y que su estado operativo es `online`:

   ```
   network interface show -vserver vserver_name lif_name
   ```

Información relacionada

"Soporte de NetApp"

"Herramienta de matriz de interoperabilidad de NetApp"

Eliminar un servicio de FC para una SVM

Es posible eliminar un servicio de FC para una SVM si ya no se necesita.

Lo que necesitará

El estado de administración debe ser «inactivo» antes de poder eliminar un servicio FC para una SVM. Puede establecer el estado de administración en inactivo con cualquiera de los dos `vserver fcp modify` o el `vserver fcp stop` comando.

Pasos

1. Utilice la `vserver fcp stop` Comando para detener la actividad de I/o de la LUN.

   ```
   vserver fcp stop -vserver vs_1
   ```

2. Utilice la `vserver fcp delete` Comando para quitar el servicio de la SVM.

   ```
   vserver fcp delete -vserver vs_1
   ```

3. Utilice la `vserver fcp show` Para verificar si ha eliminado el servicio FC de la SVM:

   ```
   vserver fcp show -vserver vs_1
   ```

Configuraciones de MTU recomendadas para tramas gigantes de FCoE

Para Fibre Channel sobre Ethernet (FCoE), las tramas gigantes para la porción del adaptador Ethernet de la CNA deben configurarse en 9000 MTU. Las tramas gigantes para la parte del adaptador FCoE de CNA se deben configurar en más de 1500 MTU. Solo configure las tramas gigantes si el iniciador, el destino y todos los switches intermedios admiten y están configurados para tramas gigantes.

Gestione el protocolo NVMe

Inicie el servicio NVMe para una SVM

Para poder utilizar el protocolo NVMe en la máquina virtual de almacenamiento (SVM), se debe iniciar el servicio NVMe en la SVM.

Antes de empezar

Debe permitirse NVMe como protocolo en el sistema.

Se admiten los siguientes protocolos NVMe:

Protocolo	Comenzando con …	Permitido por…
TCP	ONTAP 9.10.1	Predeterminado
FCP	ONTAP 9,4	Predeterminado

Pasos

1. Cambie la configuración del privilegio a avanzado:

   ```
   set -privilege advanced
   ```

2. Compruebe que NVMe se permite como protocolo:

   ```
   vserver nvme show
   ```

3. Cree el servicio de protocolo NVMe:

   ```
   vserver nvme create
   ```

4. Inicie el servicio de protocolo NVMe en la SVM:

   ```
   vserver nvme modify -status -admin up
   ```

Elimine el servicio NVMe de una SVM

Si es necesario, puede eliminar el servicio NVMe de su máquina virtual de almacenamiento (SVM).

Pasos

1. Cambie la configuración del privilegio a avanzado:

   ```
   set -privilege advanced
   ```

2. Detenga el servicio NVMe en la SVM:

   ```
   vserver nvme modify -status -admin down
   ```

3. Elimine el servicio NVMe:

   ```
   vserver nvme delete
   ```

Cambiar el tamaño de un espacio de nombres

A partir de ONTAP 9.10.1, se puede utilizar la interfaz de línea de comandos ONTAP para aumentar o reducir el tamaño de un espacio de nombres NVMe. Es posible usar System Manager para aumentar el tamaño de un espacio de nombres NVMe.

Aumentar el tamaño de un espacio de nombres

System Manager

1. Haga clic en **almacenamiento > espacios de nombres NVMe**.
2. Hoover el espacio de nombres que desea aumentar, haga clic en ⋮Y, a continuación, haga clic en **Editar**.
3. En **CAPACIDAD**, cambie el tamaño del espacio de nombres.

CLI

1. Introduzca el siguiente comando: `vserver nvme namespace modify -vserver SVM_name -path path -size new_size_of_namespace`

Reducir el tamaño de un espacio de nombres

Se debe usar la CLI de ONTAP para reducir el tamaño de un espacio de nombres NVMe.

1. Cambie la configuración del privilegio a avanzado:

   ```
   set -privilege advanced
   ```

2. Reducir el tamaño del espacio de nombres:

   ```
   vserver nvme namespace modify -vserver SVM_name -path namespace_path -size
   new_size_of_namespace
   ```

Convertir un espacio de nombres en una LUN

A partir de ONTAP 9.11.1, se puede utilizar la interfaz de línea de comandos de ONTAP para convertir un espacio de nombres NVMe existente en una LUN.

Antes de empezar

- El espacio de nombres NVMe especificado no debe tener ningún mapa existente a un subsistema.
- El espacio de nombres no debe formar parte de una copia Snapshot ni de la relación de SnapMirror en el lado de destino como espacio de nombres de solo lectura.
- Dado que los espacios de nombres de NVMe solo son compatibles con plataformas y tarjetas de red específicas, esta función solo funciona con hardware específico.

Pasos

1. Introduzca el siguiente comando para convertir un espacio de nombres NVMe en una LUN:

   ```
   lun convert-from-namespace -vserver -namespace-path
   ```

Configure la autenticación en banda a través de NVMe

A partir de ONTAP 9.12.1, se puede utilizar la interfaz de línea de comandos (CLI) de ONTAP para configurar la autenticación en banda (segura), bidireccional y unidireccional entre un host NVMe y una controladora mediante los protocolos NVME/TCP y NVMe/FC mediante la autenticación DH-HMAC-CHAP. A partir de ONTAP 9.14.1, la autenticación

en banda se puede configurar en System Manager.

Para configurar la autenticación en banda, cada host o controladora debe estar asociado con una clave DH-HMAC-CHAP que es una combinación de NQN del host o controladora NVMe y un secreto de autenticación configurado por el administrador. Para que un host o una controladora NVMe autentiquen a su par, deben conocer la clave asociada con el par.

En la autenticación unidireccional, se configura una clave secreta para el host, pero no para la controladora. En la autenticación bidireccional, se configura una clave secreta para el host y la controladora.

SHA-256 es la función hash predeterminada y 2048 bits es el grupo DH predeterminado.

System Manager

A partir de ONTAP 9.14.1, se puede usar System Manager para configurar la autenticación en banda mientras se crea o actualiza un subsistema NVMe, se crean o clonan espacios de nombres NVMe, o bien se añaden grupos de coherencia con nuevos espacios de nombres NVMe.

Pasos

1. En el Administrador del sistema, haga clic en **Hosts > Subsistema NVMe** y, a continuación, haga clic en **Agregar**.
2. Añada el nombre del subsistema NVMe y seleccione la máquina virtual de almacenamiento y el sistema operativo del host.
3. Introduzca el NQN del host.
4. Seleccione **Usar autenticación en banda** junto al Host NQN.
5. Proporcione el secreto del host y el secreto de la controladora.

   La clave DH-HMAC-CHAP es una combinación del NQN del host o controladora NVMe y un secreto de autenticación configurado por el administrador.

6. Seleccione la función hash y el grupo DH preferidos para cada host.

   Si no selecciona una función hash y un grupo DH, SHA-256 se asigna como función hash predeterminada y 2048 bits se asigna como grupo DH predeterminado.

7. Opcionalmente, haga clic en **Agregar** y repita los pasos según sea necesario para agregar más host.
8. Haga clic en **Guardar**.
9. Para verificar que la autenticación en banda está habilitada, haga clic en **System Manager > Hosts > Subsistema NVMe > Grid > Vista Peek**.

   Un icono de clave transparente junto al nombre del host indica que el modo unidireccional está activado. Una clave opaca junto al nombre del host indica que el modo bidireccional está activado.

CLI

Pasos

1. Añada la autenticación DH-HMAC-CHAP al subsistema NVMe:

   ```
   vserver nvme subsystem host add -vserver <svm_name> -subsystem
   <subsystem> -host-nqn <host_nqn> -dhchap-host-secret
   <authentication_host_secret> -dhchap-controller-secret
   <authentication_controller_secret> -dhchap-hash-function <sha-
   256|sha-512> -dhchap-group <none|2048-bit|3072-bit|4096-bit|6144-
   bit|8192-bit>
   ```

2. Compruebe que el protocolo de autenticación CHAP DH-HMAC se ha agregado al host:

   ```
   vserver nvme subsystem host show
   ```

```
  [ -dhchap-hash-function {sha-256|sha-512} ]  Authentication Hash
Function
  [ -dhchap-dh-group {none|2048-bit|3072-bit|4096-bit|6144-bit|8192-
bit} ]
                                               Authentication
Diffie-Hellman
                                               Group
  [ -dhchap-mode {none|unidirectional|bidirectional} ]
                                               Authentication Mode
```

3. Compruebe que la autenticación CHAP DH-HMAC se ejecutó durante la creación de la controladora NVMe:

```
vserver nvme subsystem controller show
```

```
 [ -dhchap-hash-function {sha-256|sha-512} ]  Authentication Hash
Function
 [ -dhchap-dh-group {none|2048-bit|3072-bit|4096-bit|6144-bit|8192-
bit} ]
                                               Authentication
Diffie-Hellman
                                               Group
 [ -dhchap-mode {none|unidirectional|bidirectional} ]
                                               Authentication Mode
```

Deshabilite la autenticación en banda sobre NVMe

Si configuró la autenticación en banda a través de NVMe mediante DH-HMAC-CHAP, puede optar por deshabilitarla en cualquier momento.

Si va a revertir desde ONTAP 9.12.1 o posterior a ONTAP 9.12.0 o una versión anterior, debe deshabilitar la autenticación en banda antes de revertir. Si la autenticación en banda con DH-HMAC-CHAP no está desactivada, se producirá un error en la reversión.

Pasos

1. Quite el host del subsistema para deshabilitar la autenticación DH-HMAC-CHAP:

```
vserver nvme subsystem host remove –vserver <svm_name> -subsystem
<subsystem> -host-nqn <host_nqn>
```

2. Compruebe que el protocolo de autenticación DH-HMAC-CHAP se ha eliminado del host:

```
vserver nvme subsystem host show
```

3. Vuelva a agregar el host al subsistema sin autenticación:

```
vserver nvme subsystem host add vserver <svm_name> -subsystem
<subsystem> -host-nqn <host_nqn>
```

Cambiar la prioridad del host de NVMe

A partir de ONTAP 9.14.1, puede configurar su subsistema NVMe para priorizar la asignación de recursos para hosts específicos. De forma predeterminada, cuando se agrega un host al subsistema, se le asigna una prioridad regular. Los hosts a los que se asigna una prioridad alta se asignan números de colas de I/O de mayor tamaño y profundidades de cola.

Puede usar la interfaz de línea de comandos (CLI) de ONTAP para cambiar manualmente la prioridad predeterminada de regular a alta. Para cambiar la prioridad asignada a un host, debe eliminar el host del subsistema y volver a añadirlo.

Pasos

1. Compruebe que la prioridad de host se ha establecido en Regular:

```
vserver nvme show-host-priority
```

2. Elimine el host del subsistema:

```
vserver nvme subsystem host remove –vserver <svm_name> -subsystem
<subsystem> -host-nqn <host_nqn>
```

3. Compruebe que el host se ha eliminado del subsistema:

```
vserver nvme subsystem host show
```

4. Vuelva a agregar el host al subsistema con prioridad alta:

```
vserver nvme subsystem host add -vserver <SVM_name> -subsystem
<subsystem_name> -host-nqn <Host_NQN_:subsystem._subsystem_name>
-priority high
```

Gestionar la detección automática de hosts de controladoras NVMe/TCP

A partir de ONTAP 9.14.1, la detección de host de las controladoras con el protocolo NVMe/TCP se automatiza de forma predeterminada en las estructuras basadas en IP.

Habilite la detección de host automatizada de las controladoras NVMe/TCP

Si deshabilitó la detección de hosts automatizada anteriormente, pero sus necesidades cambiaron, es posible volver a habilitarla.

Pasos

1. Entre en el modo de privilegio avanzado:

```
set -privilege advanced
```

2. Habilitar detección automatizada:

```
vserver nvme modify -vserver <vserver_name> -mdns-service-discovery
-enabled true
```

3. Compruebe que la detección automatizada de controladoras NVMe/TCP está habilitada.

```
vserver nvme show
```

Deshabilite la detección automática de host de las controladoras NVMe/TCP

Si no necesita controladoras NVMe/TCP para que el host lo detecte automáticamente y detecta el tráfico de multidifusión no deseado en la red, debe deshabilitar esta funcionalidad.

Pasos

1. Entre en el modo de privilegio avanzado:

```
set -privilege advanced
```

2. Desactivar la detección automatizada:

```
vserver nvme modify -vserver <vserver_name> -mdns-service-discovery
-enabled false
```

3. Verifique que la detección automatizada de las controladoras NVMe/TCP está deshabilitada.

```
vserver nvme show
```

Deshabilitar identificador de máquina virtual de host NVMe

A partir de ONTAP 9.14.1, de forma predeterminada, ONTAP admite la capacidad de los hosts NVMe/FC para identificar las máquinas virtuales con un identificador único y para que los hosts NVMe/FC supervisen la utilización de los recursos de las máquinas virtuales. Esto mejora la generación de informes y la solución de problemas del host.

Puede utilizar el arranque para desactivar esta funcionalidad.

Paso

1. Desactive el identificador de la máquina virtual:

```
bootargs set fct_sli_appid_off <port>, <port>
```

En el ejemplo siguiente se deshabilita el VMID en el puerto 0g y en el puerto 0i.

```
bootargs set fct_sli_appid_off 0g,0i

fct_sli_appid_off == 0g,0i
```

Gestione sistemas con adaptadores de FC

Gestione sistemas con adaptadores de FC

Hay comandos disponibles para gestionar los adaptadores FC integrados y las tarjetas adaptadoras FC. Estos comandos se pueden utilizar para configurar el modo del adaptador, mostrar información del adaptador y cambiar la velocidad.

La mayoría de los sistemas de almacenamiento tienen adaptadores FC integrados que se pueden configurar como iniciadores o destinos. También puede utilizar tarjetas adaptadoras de FC configuradas como iniciadores o destinos. Los iniciadores se conectan a las bandejas de discos del back-end y posiblemente a cabinas de almacenamiento externas (FlexArray). Los destinos se conectan solo a switches FC. Tanto los puertos HBA de destino FC como la velocidad del puerto del switch deben configurarse con el mismo valor y no deben configurarse en modo automático.

Información relacionada

"CONFIGURACIÓN DE SAN"

Comandos para gestionar adaptadores de FC

Puede usar comandos FC para gestionar adaptadores de destino FC, adaptadores de iniciador FC y adaptadores de FC integrados para su controladora de almacenamiento. Los mismos comandos se utilizan para gestionar adaptadores de FC para el protocolo FC y el protocolo FC-NVMe.

Los comandos de adaptador del iniciador de FC solo funcionan en el nivel del nodo. Debe utilizar el `run -node` *`node_name`* Antes de poder utilizar los comandos del adaptador del iniciador de FC.

Comandos para gestionar los adaptadores de destino de FC

Si desea…	Se usa este comando…
Muestra información del adaptador de FC en un nodo	`network fcp adapter show`
Modifique los parámetros del adaptador de destino FC	`network fcp adapter modify`
Muestra información sobre el tráfico del protocolo FC	`run -node node_name sysstat -f`
Muestra el tiempo que se ha ejecutado el protocolo FC	`run -node node_name uptime`
Mostrar la configuración y el estado del adaptador	`run -node node_name sysconfig -v adapter`
Compruebe qué tarjetas de expansión están instaladas y si hay algún error de configuración	`run -node node_name sysconfig -ac`
Ver una página de manual de un comando	`man command_name`

Comandos para gestionar los adaptadores de iniciador de FC

Si desea…	Se usa este comando…
Muestra información de todos los iniciadores y sus adaptadores en un nodo	`run -node node_name storage show adapter`
Mostrar la configuración y el estado del adaptador	`run -node node_name sysconfig -v adapter`
Compruebe qué tarjetas de expansión están instaladas y si hay algún error de configuración	`run -node node_name sysconfig -ac`

Comandos para gestionar los adaptadores de FC internos

Si desea…	Se usa este comando…
Muestra el estado de los puertos FC internos	`run -node node_name system hardware unified-connect show`

Configure los adaptadores de FC

Cada puerto FC integrado se puede configurar de forma individual como iniciador o destino. Los puertos en determinados adaptadores de FC también se pueden configurar de forma individual como un puerto de destino o como un puerto iniciador, al igual que

los puertos FC integrados. Hay disponible una lista de adaptadores que se pueden configurar para el modo de destino en "Hardware Universe de NetApp".

El modo de destino se utiliza para conectar los puertos a iniciadores FC. El modo iniciador se usa para conectar los puertos a unidades de cinta, bibliotecas de cintas o almacenamiento de terceros con la virtualización de FlexArray o con importación de LUN externa (FLI).

Los mismos pasos se utilizan cuando se configuran los adaptadores de FC para el protocolo FC y el protocolo FC-NVMe. Sin embargo, solo ciertos adaptadores de FC admiten FC-NVMe. Consulte "Hardware Universe de NetApp" Para obtener una lista de los adaptadores que admiten el protocolo FC-NVMe.

Configure los adaptadores de FC para el modo de destino

Pasos

1. Desconectar el adaptador:

   ```
   node run -node node_name storage disable adapter adapter_name
   ```

   Si el adaptador no se desconecta, también puede quitar el cable del puerto de adaptador correspondiente del sistema.

2. Cambie el adaptador del iniciador al destino:

   ```
   system hardware unified-connect modify -t target -node node_name adapter
   adapter_name
   ```

3. Reinicie el nodo que aloja el adaptador que cambió.
4. Compruebe que el puerto de destino tiene la configuración correcta:

   ```
   network fcp adapter show -node node_name
   ```

5. Conectar su adaptador:

   ```
   network fcp adapter modify -node node_name -adapter adapter_port -state up
   ```

Configure los adaptadores de FC para el modo iniciador

Lo que necesitará

- Las LIF del adaptador deben eliminarse de cualquier conjunto de puertos de los que pertenezcan.
- Todas las LIF de todas las máquinas virtuales de almacenamiento (SVM) que utilizan el puerto físico que se va a modificar deben migrarse o destruirse antes de cambiar la personalidad del puerto físico de destino a iniciador.

> NVMe/FC no admite el modo iniciador.

Pasos

1. Quite todas las LIF del adaptador:

   ```
   network interface delete -vserver SVM_name -lif LIF_name,LIF_name
   ```

2. Desconectar el adaptador:

```
network fcp adapter modify -node node_name -adapter adapter_port -status-admin
down
```

Si el adaptador no se desconecta, también puede quitar el cable del puerto de adaptador correspondiente del sistema.

3. Cambie el adaptador del destino al iniciador:

```
system hardware unified-connect modify -t initiator adapter_port
```

4. Reinicie el nodo que aloja el adaptador que cambió.
5. Compruebe que los puertos FC estén configurados en estado correcto para la configuración:

```
system hardware unified-connect show
```

6. Vuelva a conectar el adaptador:

```
node run -node node_name storage enable adapter adapter_port
```

Ver la configuración de adaptador

Puede utilizar comandos específicos para ver información sobre sus adaptadores FC/UTA.

Adaptador de destino FC

Paso

1. Utilice la `network fcp adapter show` comando para mostrar información del adaptador: `network fcp adapter show -instance -node node1 -adapter 0a`

   El resultado muestra información de configuración del sistema y información del adaptador para cada ranura que se utiliza.

Adaptador de destino unificado (UTA) X1143A-R6

Pasos

1. Arranque la controladora sin los cables conectados.
2. Ejecute el `system hardware unified-connect show` comando para ver la configuración del puerto y los módulos.
3. Consulte la información del puerto antes de configurar el CNA y los puertos.

Cambie el puerto UTA2 del modo CNA al modo FC

Debe cambiar el puerto UTA2 del modo adaptador de red convergente (CNA) al modo Fibre Channel (FC) para admitir el iniciador de FC y el modo de destino de FC. Debe cambiar la personalidad del modo CNA al modo FC cuando necesite cambiar el medio físico que conecta el puerto a su red.

Pasos

1. Desconectar el adaptador:

```
network fcp adapter modify -node node_name -adapter adapter_name -status-admin
down
```

2. Cambie el modo de puerto:

```
ucadmin modify -node node_name -adapter adapter_name -mode fcp
```

3. Reinicie el nodo y a continuación, active el adaptador:

```
network fcp adapter modify -node node_name -adapter adapter_name -status-admin
up
```

4. Notifique a su administrador o VIF Manager que elimine o quite el puerto, según corresponda:

   - Si el puerto se utiliza como puerto de inicio de una LIF, es miembro de un grupo de interfaces (ifgrp) o una VLAN de host, un administrador debe hacer lo siguiente:

     i. Mueva las LIF, quite el puerto del ifgrp o elimine las VLAN respectivamente.

     ii. Elimine manualmente el puerto ejecutando el `network port delete` comando.

     Si la `network port delete` error del comando, el administrador debe solucionar los errores y volver a ejecutar el comando.

   - Si el puerto no se usa como puerto de inicio de una LIF, no es miembro de un ifgrp y no aloja VLAN, el gestor VIF debería eliminar el puerto de sus registros en el momento del reinicio.

     Si el administrador VIF no quita el puerto, el administrador debe quitarlo manualmente después del reinicio usando la `network port delete` comando.

```
net-f8040-34::> network port show

    Node: net-f8040-34-01
                                                          Speed(Mbps) Health
    Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
    --------- ------------ ---------------- ---- ---- -----------
--------
    ...
    e0i       Default      Default          down 1500  auto/10    -
    e0f       Default      Default          down 1500  auto/10    -
    ...

    net-f8040-34::> ucadmin show
                               Current  Current    Pending  Pending
Admin
    Node            Adapter   Mode     Type       Mode     Type
Status
    ------------    -------   -------  ---------  -------  ---------
-----------
    net-f8040-34-01   0e       cna      target     -        -
offline
```

```
    net-f8040-34-01   0f       cna      target     -        -
offline
    ...

    net-f8040-34::> network interface create -vs net-f8040-34 -lif m
-role
node-mgmt-home-node net-f8040-34-01 -home-port e0e -address 10.1.1.1
-netmask 255.255.255.0


    net-f8040-34::> network interface show -fields home-port, curr-port

    vserver lif                   home-port curr-port
    ------- --------------------- --------- ---------
    Cluster net-f8040-34-01_clus1 e0a       e0a
    Cluster net-f8040-34-01_clus2 e0b       e0b
    Cluster net-f8040-34-01_clus3 e0c       e0c
    Cluster net-f8040-34-01_clus4 e0d       e0d
    net-f8040-34
            cluster_mgmt          e0M       e0M
    net-f8040-34
            m                     e0e       e0i
    net-f8040-34
            net-f8040-34-01_mgmt1 e0M       e0M
    7 entries were displayed.

    net-f8040-34::> ucadmin modify local 0e fc

    Warning: Mode on adapter 0e and also adapter 0f will be changed to
fc.
    Do you want to continue? {y|n}: y
    Any changes will take effect after rebooting the system. Use the
"system node reboot" command to reboot.

    net-f8040-34::> reboot local
      (system node reboot)

    Warning: Are you sure you want to reboot node "net-f8040-34-01"?
    {y|n}: y
```

5. Compruebe que tiene instalado el SFP+ correcto:

   ```
   network fcp adapter show -instance -node -adapter
   ```

   Para CNA, se debe usar un SFP Ethernet de 10 GB. Para FC, se debe usar un SFP de 8 GB o un SFP de 16 GB antes de cambiar la configuración en el nodo.

Cambie los módulos ópticos del adaptador de destino CNA/UTA2

Debe cambiar los módulos ópticos del adaptador de destino unificado (CNA/UTA2) para admitir el modo de personalidad seleccionado para el adaptador.

Pasos

1. Verifique el SFP+ actual utilizado en la tarjeta. A continuación, reemplace el SFP+ actual por el SFP+ adecuado para la personalidad preferida (FC o CNA).
2. Retire los módulos ópticos actuales del adaptador X1143A-R6.
3. Inserte los módulos correctos para la óptica del modo de personalidad preferido (FC o CNA).
4. Compruebe que tiene instalado el SFP+ correcto:

   ```
   network fcp adapter show -instance -node -adapter
   ```

   Los módulos SFP+ admitidos y los cables de cobre (Twinax) de la Marca Cisco se enumeran en el *Hardware Universe*.

Información relacionada

"Hardware Universe de NetApp"

Configuraciones de puertos compatibles para los adaptadores X1143A-R6

El modo de destino FC es la configuración predeterminada para los puertos de adaptador X1143A-R6. Sin embargo, los puertos de este adaptador se pueden configurar como puertos Ethernet y FCoE de 10 GB o como puertos FC de 16 GB.

Cuando se configura para Ethernet y FCoE, los adaptadores X1143A-R6 admiten el tráfico de destino NIC y FCoE simultáneo en el mismo puerto de 10 GBE. Cuando se configura para FC, cada par de dos puertos que comparte el mismo ASIC se puede configurar individualmente para modo iniciador FC o destino FC. Esto significa que un solo adaptador X1143A-R6 puede admitir el modo objetivo FC en un par de dos puertos y el modo iniciador de FC en otro par de dos puertos.

Información relacionada

"Hardware Universe de NetApp"

"CONFIGURACIÓN DE SAN"

Configure los puertos

Para configurar el adaptador de objetivo unificado (X1143A-R6), debe configurar los dos puertos adyacentes en el mismo chip en el mismo modo Personality.

Pasos

1. Configure los puertos según sea necesario para Fibre Channel (FC) o el adaptador de red convergente (CNA) mediante el `system node hardware unified-connect modify` comando.
2. Conecte los cables adecuados para FC o Ethernet de 10 GB.
3. Compruebe que tiene instalado el SFP+ correcto:

   ```
   network fcp adapter show -instance -node -adapter
   ```

Para CNA, se debe usar un SFP Ethernet de 10 GB. Para FC, se debe usar un SFP de 8 GB o un SFP de 16 GB, a partir de la estructura de FC al que se está conectando.

Evite la pérdida de conectividad cuando utilice el adaptador X1133A-R6

Puede evitar la pérdida de conectividad durante un error en el puerto configurando el sistema con rutas redundantes en HBA X1133A-R6 independientes.

El HBA X1133A-R6 es un adaptador FC de 4 puertos y 16 GB que consta de dos pares de dos puertos. El adaptador X1133A-R6 se puede configurar como modo de destino o modo de iniciador. Cada par de 2 puertos se admite con un único ASIC (por ejemplo, el puerto 1 y el puerto 2 en ASIC 1 y el puerto 3 y el puerto 4 en ASIC 2). Ambos puertos en un único ASIC deben configurarse para funcionar en el mismo modo, tanto en modo objetivo como en modo iniciador. Si se produce un error con el ASIC que admite un par, ambos puertos del par se desconectan.

Para evitar esta pérdida de conectividad, puede configurar el sistema con rutas redundantes para separar los HBA X1133A-R6, o con rutas redundantes a los puertos compatibles con diferentes ASIC en el HBA.

Administre LIF para todos los protocolos SAN

Administre LIF para todos los protocolos SAN

Los iniciadores deben usar I/O multivía (MPIO) y el acceso asimétrico de unidades lógicas (ALUA) para la capacidad de conmutación por error para los clústeres de un entorno SAN. Si falla un nodo, los LIF no migran ni asumen las direcciones IP del nodo del compañero que ha fallado. En su lugar, el software MPIO, mediante ALUA en el host, es responsable de seleccionar las rutas adecuadas para el acceso de las LUN a través de LIF.

Debe crear una o varias rutas iSCSI desde cada nodo de una pareja de ha, utilizando interfaces lógicas (LIF) para permitir el acceso a las LUN a las que presta servicio el par de alta disponibilidad. Debe configurar un LIF de gestión para cada máquina virtual de almacenamiento (SVM) compatible con SAN.

La conexión directa o el uso de switches Ethernet es compatible con la conectividad. Debe crear LIF para ambos tipos de conectividad.

- Debe configurar un LIF de gestión para cada máquina virtual de almacenamiento (SVM) compatible con SAN.
  Puede configurar dos LIF por nodo, uno para cada estructura que se usa con FC y para separar redes Ethernet para iSCSI.

Una vez creadas las LIF, pueden eliminarse de conjuntos de puertos, moverse a diferentes nodos en una máquina virtual de almacenamiento (SVM) y eliminarse.

Información relacionada

- "Configurar LIF overveiw"
- "Cree una LIF"

Configure una LIF NVMe

Deben satisfacerse ciertos requisitos al configurar las LIF de NVMe.

Antes de empezar

El adaptador de FC en el que se crea la LIF debe admitir NVMe. Los adaptadores admitidos se enumeran en "Hardware Universe".

Acerca de esta tarea

A partir de ONTAP 9.12.1 y versiones posteriores, puede configurar dos LIF NVMe por nodo en un máximo de 12 nodos. En ONTAP 9.11.1 y versiones anteriores, puede configurar dos LIF NVMe por nodo en un máximo de dos nodos.

Se aplican las siguientes reglas al crear una LIF NVMe:

- NVMe puede ser el único protocolo de datos en las LIF de datos.
- Debe configurar una LIF de gestión para cada SVM que sea compatible con SAN.
- Para ONTAP 9,5 y versiones posteriores, debe configurar un LIF NVMe en el nodo que contiene el espacio de nombres y en el partner de alta disponibilidad del nodo.
- Solo para ONTAP 9.4:
  - Las LIF y los espacios de nombres de NVMe deben alojarse en el mismo nodo.
  - Solo se puede configurar un LIF de datos NVMe por SVM.

Pasos

1. Cree la LIF:

```
network interface create -vserver <SVM_name> -lif <LIF_name> -role
<LIF_role> -data-protocol {fc-nvme|nvme-tcp} -home-node <home_node>
-home-port <home_port>
```

   NVME/TCP está disponible a partir de ONTAP 9.10.1 y versiones posteriores.

2. Compruebe que la LIF se ha creado:

```
network interface show -vserver <SVM_name>
```

Después de la creación, las LIF NVMe/TCP reciben la detección en el puerto 8009.

Qué debe saber antes de mover una LIF SAN

Solo debe realizar un movimiento LIF si está cambiando el contenido del clúster, por ejemplo, agregar nodos al clúster o eliminar nodos del clúster. Si realiza un movimiento de LIF, no necesita volver a crear una zona de la estructura de FC ni crear nuevas sesiones iSCSI entre los hosts conectados del clúster y la nueva interfaz de destino.

No puede mover un LIF DE SAN mediante el `network interface move` comando. El movimiento de LIF DE SAN debe realizarse desconectando el LIF, trasladando el LIF a otro nodo o puerto raíz y, a continuación, volviendo a conectarlo en su nueva ubicación. El acceso asimétrico de Unidad lógica (ALUA, Asymmetric Logical Unit Access) proporciona rutas redundantes y selección automática de rutas como parte de cualquier solución SAN de ONTAP. Por lo tanto, no se produce ninguna interrupción de I/o cuando se desconecta el LIF

para dicho movimiento. El host simplemente reintenta y, a continuación, mueve I/o a otra LIF.

Con el movimiento LIF, puede hacer lo siguiente de forma no disruptiva:

- Sustituya un par de alta disponibilidad de un clúster por un par de alta disponibilidad actualizado de manera que los hosts que acceden a los datos de las LUN sean transparentes
- Actualizar una tarjeta de interfaz de destino
- Traslade los recursos de una máquina virtual de almacenamiento (SVM) de un conjunto de nodos de un clúster a otro conjunto de nodos del clúster

Quite una LIF DE SAN de un conjunto de puertos

Si la LIF que desea eliminar o mover está en un conjunto de puertos, debe quitar la LIF del conjunto de puertos antes de poder eliminar o mover la LIF.

Acerca de esta tarea

Debe realizar el Paso 1 del siguiente procedimiento sólo si hay un LIF en el conjunto de puertos. No puede quitar la última LIF de un conjunto de puertos si el conjunto de puertos está vinculado a un iGroup. De lo contrario, puede empezar con Paso 2 si hay varias LIF en el conjunto de puertos.

Pasos

1. Si solo hay una LIF en el conjunto de puertos, utilice `lun igroup unbind` comando para desvincular el puerto establecido del igroup.

   > Cuando se desvincula un iGroup de un conjunto de puertos, todos los iniciadores del iGroup tienen acceso a todas las LUN de destino asignadas al iGroup en todas las interfaces de red.

   ```
   cluster1::>lun igroup unbind -vserver vs1 -igroup ig1
   ```

2. Utilice la `lun portset remove` Comando para quitar la LIF del conjunto de puertos.

   ```
   cluster1::> port set remove -vserver vs1 -portset ps1 -port-name lif1
   ```

Mover un LIF SAN

Si un nodo tiene que desconectarse, puede mover un LIF SAN para conservar la información de configuración, como su WWPN, y evitar volver a dividir en zonas la estructura de switches. Como hay que desconectar un LIF SAN antes de trasladarlo, el tráfico del host debe depender de software multivía del host para ofrecer un acceso no disruptivo a la LUN. Puede mover LIF SAN a cualquier nodo de un clúster, pero no puede mover estas entre máquinas virtuales de almacenamiento (SVM).

Lo que necesitará

Si el LIF es miembro de un conjunto de puertos, es necesario haber eliminado el LIF del conjunto de puertos antes de poder mover el LIF a un nodo diferente.

Acerca de esta tarea

El nodo de destino y el puerto físico de un LIF que desee mover deben estar en la misma estructura de FC o red Ethernet. Si mueve un LIF a otra estructura que no haya tenido una zona adecuada o si mueve un LIF a

una red Ethernet que no tenga conectividad entre un iniciador iSCSI y un destino, no será posible acceder a la LUN cuando vuelva a estar en línea.

Pasos

1. Vea el estado administrativo y operativo de la LIF:

   ```
   network interface show -vserver vserver_name
   ```

2. Cambie el estado de la LIF a. `down` (sin conexión):

   ```
   network interface modify -vserver vserver_name -lif LIF_name -status-admin
   down
   ```

3. Asigne a la LIF un nodo y un puerto nuevos:

   ```
   network interface modify -vserver vserver_name -lif LIF_name -home-node
   node_name -home-port port_name
   ```

4. Cambie el estado de la LIF a. `up` (en línea):

   ```
   network interface modify -vserver vserver_name -lif LIF_name -status-admin up
   ```

5. Compruebe los cambios:

   ```
   network interface show -vserver vserver_name
   ```

Eliminar una LIF en un entorno SAN

Antes de eliminar una LIF, debe asegurarse de que el host conectado a la LIF pueda acceder a las LUN a través de otra ruta.

Lo que necesitará

Si la LIF que desea eliminar es miembro de un conjunto de puertos, primero debe quitar la LIF del conjunto de puertos antes de poder eliminar la LIF.

System Manager

Elimine una LIF con el Administrador del sistema de ONTAP (9.7 y posterior).

Pasos

1. En System Manager, haga clic en **Red > Descripción general** y, a continuación, seleccione **interfaces de red**.
2. Seleccione la máquina virtual de almacenamiento desde la que desea eliminar la LIF.
3. Haga clic en ⋮ Y seleccione **Eliminar**.

CLI

Elimine una LIF con la CLI de ONTAP.

Pasos

1. Compruebe el nombre de la LIF y el puerto actual que se va a eliminar:

   ```
   network interface show –vserver vserver_name
   ```

2. Elimine la LIF:

   ```
   network interface delete

   network interface delete -vserver vs1 -lif lif1
   ```

3. Compruebe que ha eliminado la LIF:

   ```
   network interface show

   network interface show -vserver vs1
   ```

   ```
   Logical Status     Network                     Current   Current Is
   Vserver Interface  Admin/Oper Address/Mask     Node      Port
   Home
   ------- ---------- ---------- ---------------- --------- -------
   ----
   vs1
           lif2       up/up      192.168.2.72/24  node-01   e0b
   true
           lif3       up/up      192.168.2.73/24  node-01   e0b
   true
   ```

Requisitos de LIF de SAN para añadir nodos a un clúster

Debe tener en cuenta determinadas consideraciones al añadir nodos a un clúster.

- Debe crear LIF en los nuevos nodos del modo que corresponda antes de crear LUN en esos nuevos nodos.

- Debe detectar estas LIF desde los hosts según lo dictado por la pila del host y el protocolo.
- Debe crear LIF en los nodos nuevos de modo que los movimientos de la LUN y los volúmenes sean posibles sin utilizar la red de interconexión de clúster.

Configure LIF iSCSI para devolver el FQDN al host iSCSI SendTargets Discovery Operation

A partir de ONTAP 9, las LIF iSCSI se pueden configurar para que devuelvan un nombre de dominio completo (FQDN) cuando un sistema operativo host envía una operación de detección SendTargets iSCSI. Devolver un FQDN es útil cuando hay un dispositivo de traducción de direcciones de red (NAT) entre el sistema operativo host y el servicio de almacenamiento.

Acerca de esta tarea

Las direcciones IP de un lado del dispositivo NAT no tienen sentido en el otro lado, pero FQDN puede tener significado en ambos lados.

> El límite de interoperabilidad del valor FQDN es de 128 caracteres en todo el sistema operativo host.

Pasos

1. Cambie la configuración del privilegio a avanzado:

   ```
   set -privilege advanced
   ```

2. Configure los LIF iSCSI para devolver el FQDN:

   ```
   vserver iscsi interface modify -vserver SVM_name -lif iscsi_LIF_name
   -sendtargets_fqdn FQDN
   ```

   En el ejemplo siguiente, los LIF iSCSI están configurados para devolver storagehost-005.example.com como el FQDN.

   ```
   vserver iscsi interface modify -vserver vs1 -lif vs1_iscsi1 -sendtargets-fqdn
   storagehost-005.example.com
   ```

3. Compruebe que sendTargets sea el FQDN:

   ```
   vserver iscsi interface show -vserver SVM_name -fields sendtargets-fqdn
   ```

   En este ejemplo, storagehost-005.example.com se muestra en el campo de salida sendTargets-fqdn.

   ```
   cluster::vserver*> vserver iscsi interface show -vserver vs1 -fields
   sendtargets-fqdn
   vserver lif        sendtargets-fqdn
   ------- ---------- ---------------------------
   vs1     vs1_iscsi1 storagehost-005.example.com
   vs1     vs1_iscsi2 storagehost-006.example.com
   ```

Información relacionada

"Comandos de ONTAP 9"

Combinaciones de configuración recomendadas de volúmenes y archivos o LUN

Información general de las combinaciones de configuración de volúmenes y archivos o LUN recomendadas

Existen combinaciones específicas de configuraciones de volumen y archivo de FlexVol o LUN que puede utilizar, en función de sus requisitos de aplicación y administración. Comprender los beneficios y los costos de estas combinaciones puede ayudarlo a determinar la combinación adecuada de configuración de volúmenes y LUN para su entorno.

Se recomiendan las siguientes combinaciones de configuración de volúmenes y LUN:

- Archivos reservados de espacio o LUN con aprovisionamiento de volumen grueso
- Archivos sin espacio reservado o LUN con thin provisioning de volumen
- Archivos reservados de espacio o LUN con aprovisionamiento de volumen grueso

Puede utilizar thin provisioning SCSI en sus LUN junto con cualquiera de estas combinaciones de configuración.

Archivos reservados de espacio o LUN con aprovisionamiento de volumen grueso

Beneficios:

- Se garantizan todas las operaciones de escritura en los archivos con espacio reservado; no se producen errores debido a la falta de espacio.
- No existen restricciones sobre las tecnologías de eficiencia del almacenamiento y protección de datos en el volumen.

Costos y limitaciones:

- Debe reservar espacio suficiente desde el agregado hacia delante para admitir el volumen considerablemente aprovisionado.
- El espacio es igual al doble del tamaño de la LUN se asigna desde el volumen en el momento de creación de la LUN.

Archivos sin espacio reservado o LUN con thin provisioning de volumen

Beneficios:

- No existen restricciones sobre las tecnologías de eficiencia del almacenamiento y protección de datos en el volumen.
- El espacio se asigna solo como se utiliza.

Costos y restricciones:

- No se garantizan las operaciones de escritura; pueden fallar si el volumen se queda sin espacio libre.
- Debe gestionar eficazmente el espacio libre del agregado para evitar que el agregado se quede sin espacio libre.

Archivos reservados de espacio o LUN con aprovisionamiento de volumen grueso

Beneficios:

Se reserva menos espacio inicial que para el aprovisionamiento de volúmenes gruesos y se ofrece una garantía de escritura de mejor esfuerzo.

Costos y restricciones:

- Las operaciones de escritura pueden fallar con esta opción.

  Puede mitigar este riesgo equilibrando correctamente el espacio libre en el volumen frente a la volatilidad de los datos.

- No puede confiar en la retención de objetos de protección de datos como copias Snapshot, archivos FlexClone y LUN.
- No se pueden utilizar funcionalidades de eficiencia del almacenamiento con uso compartido de bloques de ONTAP que no se pueden eliminar automáticamente, incluida la deduplicación, la compresión y la descarga ODX/copia.

Determinar la combinación correcta de configuración de volumen y LUN para su entorno

Responder a algunas preguntas básicas acerca de su entorno puede ayudarle a determinar la mejor configuración de LUN y volumen FlexVol para su entorno.

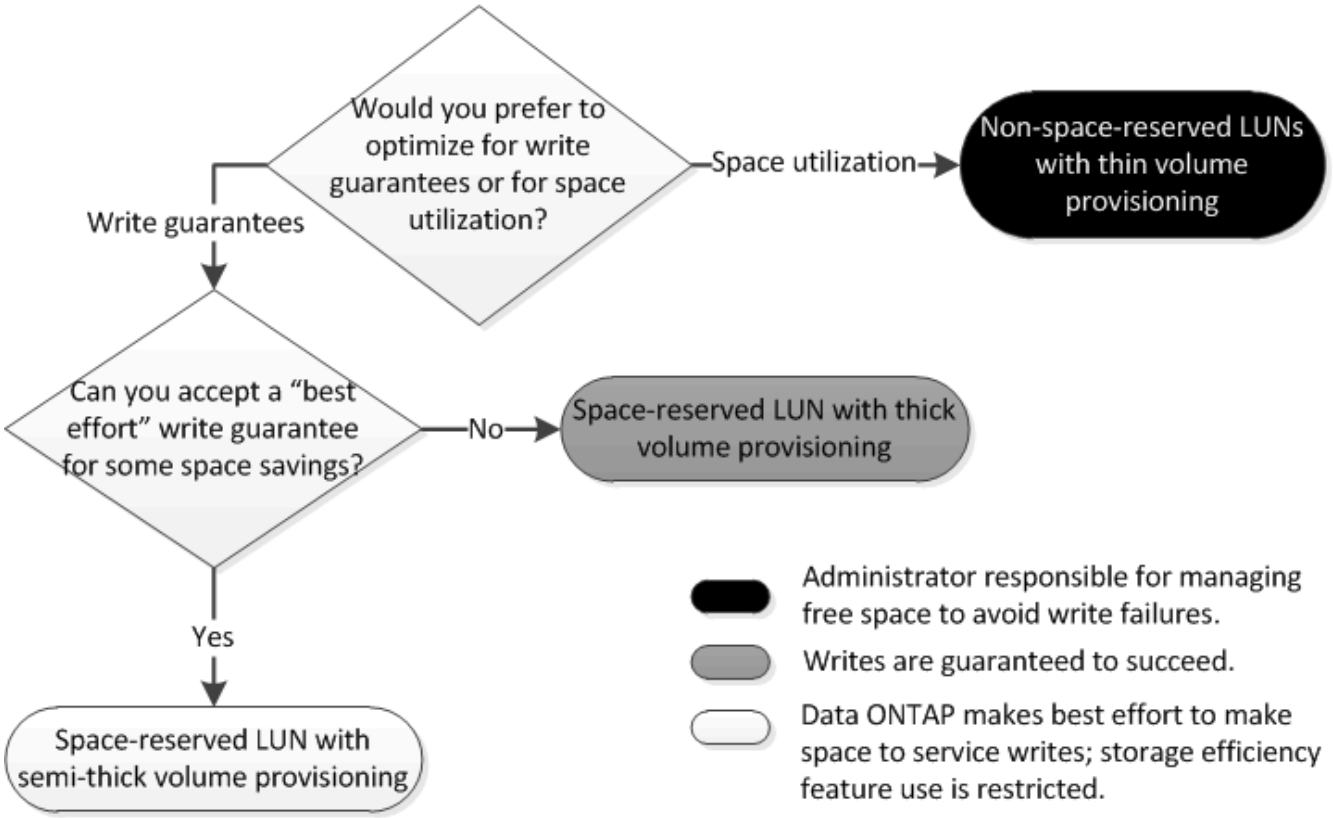
Acerca de esta tarea

Puede optimizar su configuración de LUN y volúmenes para un uso máximo del almacenamiento o para la seguridad de garantías de escritura. En función de sus requisitos de utilización del almacenamiento y su capacidad para supervisar y reponer espacio libre rápidamente, debe determinar el volumen de FlexVol y los volúmenes LUN adecuados para su instalación.

> No es necesario un volumen separado para cada LUN.

Paso

1. Use el siguiente árbol de decisiones para determinar la mejor combinación de configuración de volumen y LUN para su entorno:



Calcule la tasa de crecimiento de datos de las LUN

Necesita conocer la velocidad a la que crecen sus datos de LUN con el tiempo para determinar si debe utilizar LUN reservadas para el espacio o LUN no reservadas para el espacio.

Acerca de esta tarea

Si tiene una tasa alta y constante de crecimiento de datos, puede que las LUN con reserva de espacio sean una mejor opción. Si tiene una tasa baja de crecimiento de datos, debe plantearse poner en marcha LUN sin reservar espacio.

Puede utilizar herramientas como OnCommand Insight para calcular la tasa de crecimiento de datos o puede calcularla manualmente. Los siguientes pasos son para el cálculo manual.

Pasos

1. Configure un LUN con reserva de espacio.
2. Supervise los datos en la LUN durante un período establecido, como una semana.

   Asegúrese de que el período de monitorización sea lo suficientemente largo como para formar una muestra representativa de los aumentos que se producen regularmente en el crecimiento de datos. Por ejemplo, es posible que usted tenga constantemente un gran crecimiento de datos a final de cada mes.

3. Cada día, registre en GB cuánto crecen sus datos.
4. Al final de su período de monitoreo, agregue los totales para cada día juntos, y luego divida por el número de días en su período de monitoreo.

   Este cálculo genera la tasa media de crecimiento.

Ejemplo

En este ejemplo, necesita una LUN de 200 GB. Decide supervisar la LUN durante una semana y registrar los siguientes cambios diarios en sus datos:

- Domingo: 20 GB
- Lunes: 18 GB
- Martes: 17 GB
- Miércoles: 20 GB
- Jueves: 20 GB
- Viernes: 23 GB
- Sábado: 22 GB

En este ejemplo, la tasa de crecimiento es (20+18+17+20+20+23+22) / 7 = 20 GB al día.

Opción de configuración para archivos reservados espacio o LUN con volúmenes aprovisionados con thick-Provisioning

Esta combinación de configuración de volumen y archivo de FlexVol o LUN ofrece la capacidad de utilizar tecnologías de eficiencia del almacenamiento y no le requiere supervisar de forma activa el espacio libre, ya que se asigna suficiente espacio de antemano.

Las siguientes opciones de configuración son necesarias para configurar un archivo o LUN con espacio reservado en un volumen mediante el aprovisionamiento grueso:

Ajuste del volumen	Valor
Garantizado	Volumen
Reserva fraccionaria	100
Reserva de Snapshot	Cualquiera
Eliminación automática de Snapshot	Opcional
Crecimiento automático	Opcional; si está habilitado, el espacio libre del agregado debe supervisarse de forma activa.

Configuración de archivo o LUN	Valor
Reserva de espacio	Activado

Configuración para archivos que no estén reservados espacio o LUN con volúmenes con thin provisioning

Esta combinación de configuración de volumen y archivo FlexVol o LUN requiere la cantidad más pequeña de almacenamiento que se asigne de antemano, pero requiere la

gestión activa del espacio libre para evitar errores debido a la falta de espacio.

Los siguientes ajustes de configuración son necesarios para configurar un LUN o archivos sin espacio reservado en un volumen con thin provisioning:

Ajuste del volumen	Valor
Garantizado	Ninguno
Reserva fraccionaria	0
Reserva de Snapshot	Cualquiera
Eliminación automática de Snapshot	Opcional
Crecimiento automático	Opcional

Configuración de archivo o LUN	Valor
Reserva de espacio	Deshabilitado

Consideraciones adicionales

Cuando el volumen o el agregado se queda sin espacio, se puede producir un error en las operaciones de escritura en el archivo o la LUN.

Si no desea supervisar activamente el espacio libre tanto del volumen como del agregado, debe habilitar la fila automática para el volumen y establecer el tamaño máximo para el volumen en el tamaño del agregado. En esta configuración, se debe supervisar el espacio libre del agregado de forma activa, pero no es necesario supervisar el espacio libre del volumen.

Configuración para archivos reservados espacio o LUN con aprovisionamiento de volúmenes semigruesos

Esta combinación de configuración de volumen y archivo o LUN de FlexVol requiere que haya menos almacenamiento que la combinación completamente aprovisionada, pero impone restricciones sobre las tecnologías de eficiencia que se pueden utilizar para el volumen. Las sobrescrituras se realizan de acuerdo con el mejor esfuerzo posible para esta combinación de configuración.

Las siguientes opciones de configuración son necesarias para configurar un LUN con reserva de espacio en un volumen mediante el aprovisionamiento semi-grueso:

Ajuste del volumen	Valor
Garantizado	Volumen
Reserva fraccionaria	0

Ajuste del volumen	Valor
Reserva de Snapshot	0
Eliminación automática de Snapshot	Activado, con un nivel de compromiso de destrucción, una lista de destrucción que incluye todos los objetos, el activador establecido en volumen y todos los LUN y archivos FlexClone habilitados para la eliminación automática.
Crecimiento automático	Opcional; si está habilitado, el espacio libre del agregado debe supervisarse de forma activa.

Configuración de archivo o LUN	Valor
Reserva de espacio	Activado

Restricciones tecnológicas

No se pueden usar las siguientes tecnologías de eficiencia del almacenamiento de volumen para esta combinación de configuración:

- Compresión
- Deduplicación
- Descarga de copias ODX y FlexClone
- LUN y archivos de FlexClone no marcados para eliminación automática (clones activos)
- Subarchivos FlexClone
- ODX/descarga de copias

Consideraciones adicionales

Al emplear esta combinación de configuración deben tenerse en cuenta los siguientes hechos:

- Cuando el volumen que admite que la LUN se ejecuta con poco espacio, se destruyen los datos de protección (LUN y archivos de FlexClone, copias Snapshot).
- Es posible que se agote el tiempo de espera de las operaciones de escritura y se produzca un error en ellas cuando el volumen se queda sin espacio libre.

De forma predeterminada, la compresión se habilita para las plataformas AFF. Debe deshabilitar explícitamente la compresión en cualquier volumen para el que desee utilizar aprovisionamiento de media en una plataforma AFF.

Protección de DATOS SAN

Información general sobre los métodos de protección de datos en entornos SAN

Puede proteger sus datos realizando copias de ellos para que estén disponibles para su restauración en caso de eliminación accidental, fallos en las aplicaciones, daños en los

datos o desastres. En función de sus necesidades de backup y protección de datos, ONTAP ofrece una variedad de métodos que le permiten proteger sus datos.

Continuidad del negocio de SnapMirror (SM-BC)

A partir de la disponibilidad general de ONTAP 9.9.1, proporciona un objetivo de tiempo de recuperación cero (objetivo de tiempo de recuperación nulo) o conmutación por error de aplicaciones transparente (TAF) para permitir la recuperación automática tras fallos de aplicaciones vitales para el negocio en entornos SAN. SM-BC requiere la instalación de ONTAP Mediator 1,2 en una configuración con dos clústeres AFF o dos clústeres de cabina SAN all-flash (ASA).

"Documentación de NetApp: Continuidad empresarial de SnapMirror"

Copia Snapshot

Le permite crear, programar y mantener manualmente o de forma automática varios backups de sus LUN. Las copias Snapshot utilizan solo una cantidad mínima de espacio en el volumen adicional y no tienen ningún coste de rendimiento. Si sus datos de LUN se modifican o eliminan por error, esos datos pueden restaurarse de forma rápida y sencilla a partir de una de las copias Snapshot más recientes.

LUN de FlexClone (se requiere licencia de FlexClone)

Proporciona copias puntuales editables de otra LUN en un volumen activo o en una copia Snapshot. Un clon y su primario se pueden modificar de forma independiente sin que se vean afectados.

SnapRestore (se requiere licencia)

Le permite realizar una recuperación de datos bajo solicitud y rápida, que gestiona el espacio de manera eficiente desde copias Snapshot en todo un volumen. Puede utilizar SnapRestore para restaurar una LUN a un estado conservado anterior sin reiniciar el sistema de almacenamiento.

Copias de mirroring para la protección de datos (se requiere licencia de SnapMirror)

Ofrece recuperación ante desastres asíncrona, ya que le permite crear periódicamente copias Snapshot de los datos del volumen, copiar estas copias Snapshot a través de una red de área local o de área amplia a un volumen asociado, normalmente en otro clúster, y conservar dichas copias Snapshot. La copia reflejada del volumen de partner proporciona disponibilidad y restauración de datos desde el momento de la última copia de Snapshot, si los datos del volumen de origen se pierden o se dañan.

Backups de SnapVault (se requiere licencia de SnapMirror)

Ofrece un almacenamiento eficiente y retención de backups a largo plazo. Las relaciones de SnapVault permiten realizar un backup de las copias de Snapshot seleccionadas de los volúmenes en un volumen de destino y conservar los backups.

Si realiza backups a cinta y operaciones de archivado, puede ponerlas en marcha en los datos de los que ya se ha realizado un backup en el volumen secundario de SnapVault.

SnapDrive para Windows o UNIX (se requiere una licencia de SnapDrive)

Configura el acceso a las LUN, gestiona las LUN y gestiona las copias snapshot del sistema de almacenamiento directamente desde hosts de Windows o UNIX.

Backup y recuperación en cinta nativos

ONTAP admite la mayoría de las unidades de cinta existentes, así como un método para que los proveedores de cintas añadan dinámicamente soporte para nuevos dispositivos. ONTAP también es compatible con el protocolo de cinta magnética remota (RMT), lo que permite la copia de seguridad y la recuperación en cualquier sistema capaz.

Información relacionada

"Documentación de NetApp: SnapDrive para UNIX"

"Documentación de NetApp: SnapDrive para Windows (versiones actuales)"

"Protección de datos mediante backup en cinta"

Efecto de mover o copiar una LUN en copias Snapshot

Efecto de mover o copiar una LUN en la información general sobre copias Snapshot

Las copias Snapshot se crean en el nivel de los volúmenes. Si copia o mueve una LUN a otro volumen, la política de copia de Snapshot del volune de destino se aplica al volumen copiado o movido. Si no se establecen copias Snapshot para el volumen de destino, no se crearán copias Snapshot de la LUN movida o copiada.

Restaure un solo LUN de una copia Snapshot

Puede restaurar un único LUN a partir de una copia Snapshot sin restaurar todo el volumen que contiene la única LUN. Puede restaurar el LUN en su lugar o a una nueva ruta en el volumen. La operación restaura solo el LUN único sin que se vean afectados otros archivos o LUN del volumen. También puede restaurar archivos con secuencias.

Lo que necesitará

- Debe tener suficiente espacio en el volumen para completar la operación de restauración:
  - Si va a restaurar una LUN con la reserva de espacio donde la reserva fraccionaria es 0%, necesitará un tamaño más que el de la LUN restaurada.
  - Si va a restaurar una LUN con la reserva de espacio donde la reserva fraccionaria es del 100%, necesitará el doble del tamaño de la LUN restaurada.
  - Si va a restaurar una LUN que no tiene espacio reservado, solo necesita el espacio real utilizado para la LUN restaurada.
- Se debe haber creado una copia Snapshot de la LUN de destino.

  Si la operación de restauración falla, es posible que la LUN de destino se trunque. En estos casos, puede usar la copia Snapshot para evitar la pérdida de datos.

- Se debe haber creado una copia Snapshot de la LUN de origen.

  En raras ocasiones, la restauración de LUN puede generar un error y, con ello, la LUN de origen no se puede utilizar. Si esto sucede, puede usar la copia Snapshot para devolver la LUN al estado justo antes del intento de restauración.

- La LUN de destino y la LUN de origen deben tener el mismo tipo de SO.

Si la LUN de destino tiene un tipo de sistema operativo diferente de la LUN de origen, el host puede perder el acceso a los datos a la LUN de destino después de la operación de restauración.

Pasos

1. Desde el host, detenga todo el acceso del host a la LUN.
2. Desmonte la LUN en su host para que el host no pueda acceder a la LUN.
3. Desasigne la LUN:

   ```
   lun mapping delete -vserver vserver_name -volume volume_name -lun lun_name
   -igroup igroup_name
   ```

4. Determine la copia Snapshot en la que desea restaurar la LUN:

   ```
   volume snapshot show -vserver vserver_name -volume volume_name
   ```

5. Cree una copia Snapshot de la LUN antes de restaurar la LUN:

   ```
   volume snapshot create -vserver vserver_name -volume volume_name -snapshot
   snapshot_name
   ```

6. Restaure el LUN especificado en un volumen:

   ```
   volume snapshot restore-file -vserver vserver_name -volume volume_name
   -snapshot snapshot_name -path lun_path
   ```

7. Siga los pasos de la pantalla.
8. Si es necesario, conectar la LUN:

   ```
   lun modify -vserver vserver_name -path lun_path -state online
   ```

9. Si es necesario, reasigne la LUN:

   ```
   lun mapping create -vserver vserver_name -volume volume_name -lun lun_name
   -igroup igroup_name
   ```

10. Desde el host, vuelva a montar la LUN.
11. Desde el host, reinicie el acceso a la LUN.

Restaure todas las LUN de un volumen a partir de una copia Snapshot

Puede utilizar `volume snapshot restore` Comando para restaurar todas las LUN de un volumen especificado desde una copia Snapshot.

Pasos

1. Desde el host, detenga todo el acceso del host a las LUN.

   El uso de SnapRestore sin detener todo el acceso de host a las LUN del volumen puede provocar daños en los datos y errores del sistema.

2. Desmonte las LUN de ese host para que el host no pueda acceder a las LUN.

3. Desasigne sus LUN:

   ```
   lun mapping delete -vserver vserver_name -volume volume_name -lun lun_name
   -igroup igroup_name
   ```

4. Para determinar la copia Snapshot en la que desea restaurar el volumen:

   ```
   volume snapshot show -vserver vserver_name -volume volume_name
   ```

5. Cambie la configuración de privilegios a avanzada:

   ```
   set -privilege advanced
   ```

6. Restaure sus datos:

   ```
   volume snapshot restore -vserver vserver_name -volume volume_name -snapshot
   snapshot_name
   ```

7. Siga las instrucciones que aparecen en pantalla.
8. Reasigne sus LUN:

   ```
   lun mapping create -vserver vserver_name -volume volume_name -lun lun_name
   -igroup igroup_name
   ```

9. Compruebe que sus LUN están en línea:

   ```
   lun show -vserver vserver_name -path lun_path -fields state
   ```

10. Si sus LUN no están en línea, conectarlos:

    ```
    lun modify -vserver vserver_name -path lun_path -state online
    ```

11. Cambie la configuración de privilegio a admin:

    ```
    set -privilege admin
    ```

12. Desde el host, vuelva a montar las LUN.
13. Desde el host, reinicie el acceso a sus LUN.

Elimine una o más copias Snapshot existentes de un volumen

Puede eliminar manualmente una o varias copias Snapshot existentes del volumen. Se recomienda hacerlo si se necesita más espacio en el volumen.

Pasos

1. Utilice la `volume snapshot show` Comando para verificar qué copias de Snapshot desea eliminar.

```
cluster::> volume snapshot show -vserver vs3 -volume vol3

                                                  ---Blocks---
Vserver  Volume  Snapshot                 Size   Total% Used%
-------- ------- ----------------------- -----  ------ -----
vs3      vol3
                 snap1.2013-05-01_0015   100KB   0%    38%
                 snap1.2013-05-08_0015   76KB   0%    32%
                 snap2.2013-05-09_0010   76KB   0%    32%
                 snap2.2013-05-10_0010   76KB   0%    32%
                 snap3.2013-05-10_1005   72KB   0%    31%
                 snap3.2013-05-10_1105   72KB   0%    31%
                 snap3.2013-05-10_1205   72KB   0%    31%
                 snap3.2013-05-10_1305   72KB   0%    31%
                 snap3.2013-05-10_1405   72KB   0%    31%
                 snap3.2013-05-10_1505   72KB   0%    31%
10 entries were displayed.
```

2. Utilice la `volume snapshot delete` Comando para eliminar copias Snapshot.

Si desea…	Introduzca este comando…
Elimine una sola copia Snapshot	`volume snapshot delete -vserver` *`svm_name`* `-volume` *`vol_name`* `-snapshot` *`snapshot_name`*
Elimine varias copias Snapshot	`volume snapshot delete -vserver` *`svm_name`* `-volume` *`vol_name`* `-snapshot` *`snapshot_name1`*`[,`*`snapshot_name2`*`,…]`
Elimine todas las copias Snapshot	`volume snapshot delete -vserver` *`svm_name`* `-volume` *`vol_name`* `-snapshot *`

En el siguiente ejemplo se eliminan todas las copias Snapshot del volumen vol3.

```
cluster::> volume snapshot delete -vserver vs3 -volume vol3 *

10 entries were acted on.
```

Use LUN FlexClone para proteger sus datos

Use LUN FlexClone para proteger la descripción general de sus datos

Una LUN FlexClone es una copia puntual modificable de otra LUN en un volumen activo

o en una copia Snapshot. El clon y su primario se pueden modificar de forma independiente sin que se vean afectados.

Una LUN FlexClone comparte espacio inicialmente con su LUN principal. De forma predeterminada, la LUN FlexClone hereda el atributo de espacio reservado de la LUN principal. Por ejemplo, si la LUN principal no está reservada a espacio, la LUN FlexClone también está sin la reserva de espacio de forma predeterminada. Sin embargo, puede crear una LUN FlexClone sin reservar espacio desde un elemento principal que es una LUN con reserva de espacio.

Cuando se clona una LUN, el uso compartido de bloques se produce en segundo plano y no se puede crear una copia de Snapshot de volumen hasta que haya finalizado el uso compartido de bloques.

Debe configurar el volumen para habilitar la función de eliminación automática de LUN de FlexClone con el `volume snapshot autodelete modify` comando. De lo contrario, si desea que las LUN de FlexClone se eliminen automáticamente pero el volumen no está configurado para la eliminación automática de FlexClone, no se elimina ninguna de las LUN de FlexClone.

Al crear una LUN de FlexClone, la función de eliminación automática de la LUN de FlexClone está deshabilitada de manera predeterminada. Debe habilitarla manualmente en cada LUN de FlexClone antes de que esa LUN de FlexClone se pueda eliminar de forma automática. Si utiliza aprovisionamiento de volúmenes semigruesos y desea obtener la garantía de escritura «mejor esfuerzo» proporcionada por esta opción, debe poner a disposición LUN de *all* FlexClone para su eliminación automática.

> Cuando crea una LUN de FlexClone a partir de una copia Snapshot, la LUN se divide automáticamente de la copia Snapshot con un proceso en segundo plano con gestión eficiente del espacio, de modo que la LUN no siga dependiendo de la copia Snapshot o consuma espacio adicional. Si no ha finalizado esta división en segundo plano y esta copia snapshot se elimina automáticamente, esa LUN de FlexClone se elimina aunque haya deshabilitado la función de eliminación automática de FlexClone para esa LUN de FlexClone. Una vez finalizada la división en segundo plano, la LUN de FlexClone no se elimina ni siquiera si se elimina esa copia snapshot.

Información relacionada

"Gestión de almacenamiento lógico"

Razones para utilizar LUN de FlexClone

Puede utilizar las LUN FlexClone para crear varias copias de lectura/escritura de una LUN.

Se recomienda hacerlo por los siguientes motivos:

- Debe crear una copia temporal de una LUN para fines de pruebas.
- Debe realizar una copia de sus datos disponibles a usuarios adicionales sin tener que darles acceso a los datos de producción.
- Desea crear un clon de una base de datos para operaciones de manipulación y proyección, al mismo tiempo que se conservan los datos originales sin alterarlos.
- Desea acceder a un subconjunto específico de los datos de una LUN (un volumen lógico o un sistema de archivos específicos de un grupo de volúmenes, O un archivo específico o un conjunto de archivos en un sistema de archivos) y cópielos en la LUN original, sin restaurar el resto de datos de la LUN original. Esto funciona en sistemas operativos que son compatibles con el montaje de las LUN y un clon de la LUN al mismo tiempo. SnapDrive para UNIX lo admite con el `snap connect` comando.

- Necesita varios hosts DE arranque SAN con el mismo sistema operativo.

Cómo un volumen de FlexVol puede reclamar espacio libre con la configuración de eliminación automática

Puede activar la configuración de eliminación automática de un volumen FlexVol para eliminar automáticamente archivos FlexClone y LUN FlexClone. Al habilitar la eliminación automática, se puede recuperar una cantidad de espacio libre objetivo en el volumen cuando un volumen está casi lleno.

Puede configurar un volumen para que comience a eliminar automáticamente archivos FlexClone y LUN FlexClone cuando el espacio libre en el volumen disminuya por debajo de un valor de umbral determinado y deje de eliminar automáticamente clones cuando se reclame una cantidad de espacio libre objetivo en el volumen. Aunque, no puede especificar el valor de umbral que inicia la eliminación automática de clones, puede especificar si un clon es apto para su eliminación y puede especificar la cantidad de espacio libre objetivo para un volumen.

Un volumen elimina automáticamente los archivos FlexClone y las LUN FlexClone cuando el espacio libre en el volumen disminuye por debajo de un umbral determinado y cuando se cumplen los siguientes requisitos:

- La función de eliminación automática está habilitada para el volumen que contiene los archivos FlexClone y las LUN FlexClone.

  Para habilitar la funcionalidad de eliminación automática para un volumen de FlexVol, se puede usar la `volume snapshot autodelete modify` comando. Debe configurar el `-trigger` parámetro a. `volume` o. `snap_reserve` Para que un volumen elimine automáticamente archivos FlexClone y LUN FlexClone.

- La función de eliminación automática está activada para los archivos de FlexClone y las LUN de FlexClone.

  Puede activar la eliminación automática para un archivo FlexClone o una LUN FlexClone mediante el `file clone create` con el `-autodelete` parámetro. Como resultado, puede conservar algunos archivos FlexClone y LUN FlexClone deshabilitando la eliminación automática de los clones y asegurándose de que otras opciones de configuración del volumen no anulen la configuración del clon.

Configurar un volumen FlexVol para que elimine automáticamente archivos FlexClone y LUN FlexClone

Es posible habilitar un volumen FlexVol para eliminar automáticamente archivos de FlexClone y LUN FlexClone con la eliminación automática habilitada cuando el espacio libre en el volumen disminuye por debajo de un umbral en particular.

Lo que necesitará

- El volumen FlexVol debe contener archivos FlexClone y LUN FlexClone, y debe estar en línea.
- El volumen FlexVol no debe ser un volumen de solo lectura.

Pasos

1. Permita la eliminación automática de archivos de FlexClone y LUN de FlexClone en el volumen de FlexVol mediante el `volume snapshot autodelete modify` comando.
   - Para la `-trigger` parámetro, puede especificar `volume` o. `snap_reserve`.

- Para la `-destroy-list` parámetro, debe especificar siempre `lun_clone,file_clone` independientemente de si desea eliminar solo un tipo de clon.

  El siguiente ejemplo muestra cómo puede habilitar volume vol1 para activar la eliminación automática de archivos FlexClone y LUN de FlexClone para la reclamación de espacio hasta que el 25% del volumen esté compuesto por espacio libre:

```
cluster1::> volume snapshot autodelete modify -vserver vs1 -volume
vol1 -enabled true -commitment disrupt -trigger volume -target-free
-space 25 -destroy-list lun_clone,file_clone

Volume modify successful on volume:vol1
```

> Al habilitar la eliminación automática de volúmenes de FlexVol, si establece el valor de `-commitment` parámetro a. `destroy`, Todos los archivos FlexClone y las LUN FlexClone con `-autodelete` parámetro establecido en `true` puede eliminarse cuando el espacio libre en el volumen disminuya por debajo del valor de umbral especificado. Sin embargo, los archivos FlexClone y las LUN FlexClone con el `-autodelete` parámetro establecido en `false` no se eliminará.

2. Compruebe que la eliminación automática de archivos FlexClone y LUN de FlexClone está activada en el volumen de FlexVol mediante el `volume snapshot autodelete show` comando.

   El siguiente ejemplo muestra que el volumen vol1 está activado para la eliminación automática de archivos FlexClone y LUN FlexClone:

```
cluster1::> volume snapshot autodelete show -vserver vs1 -volume vol1

         Vserver Name: vs1
          Volume Name: vol1
          Enabled: true
           Commitment: disrupt
         Defer Delete: user_created
         Delete Order: oldest_first
  Defer Delete Prefix: (not specified)*
    Target Free Space: 25%
              Trigger: volume
     Destroy List: lun_clone,file_clone
Is Constituent Volume: false
```

3. Asegúrese de que la eliminación automática esté habilitada para los archivos de FlexClone y las LUN FlexClone del volumen que desea eliminar siguiendo estos pasos:

   a. Permitir la eliminación automática de un archivo FlexClone o una LUN FlexClone concretos mediante el `volume file clone autodelete` comando.

      Puede forzar la eliminación automática de un archivo FlexClone o una LUN de FlexClone mediante la

`volume file clone autodelete` con el `-force` parámetro.

El ejemplo siguiente muestra que la eliminación automática de la LUN de FlexClone lun1_clone contenida en el volumen vol1 está habilitada:

```
cluster1::> volume file clone autodelete -vserver vs1 -clone-path
/vol/vol1/lun1_clone -enabled true
```

Puede activar la eliminación automática cuando crea archivos FlexClone y LUN de FlexClone.

b. Compruebe que el archivo FlexClone o la LUN de FlexClone están activados para eliminación automática mediante la `volume file clone show-autodelete` comando.

El ejemplo siguiente muestra que la LUN de FlexClone lun1_clone está habilitada para eliminación automática:

```
cluster1::> volume file clone show-autodelete -vserver vs1 -clone
-path vol/vol1/lun1_clone
                                                          Vserver
Name: vs1
                                                          Clone
Path: vol/vol1/lun1_clone

**Autodelete Enabled: true**
```

Para obtener más información acerca del uso de los comandos, consulte las páginas man correspondientes.

Clonar las LUN de un volumen activo

Para crear copias de sus LUN, debe clonar las LUN en el volumen activo. Estas LUN FlexClone son copias legibles y editables de las LUN originales en el volumen activo.

Lo que necesitará

Debe instalar una licencia de FlexClone. Esta licencia se incluye con "ONTAP One".

Acerca de esta tarea

Un LUN FlexClone con reserva de espacio requiere tanto espacio como la LUN principal con reserva de espacio. Si la LUN FlexClone no está reservada para el espacio, debe asegurarse de que el volumen tenga suficiente espacio para acomodar los cambios en la LUN FlexClone.

Pasos

1. Debe haber verificado que las LUN no están asignadas a un igroup o que se escriben en antes de crear el clon.
2. Utilice la `lun show` Comando para comprobar que la LUN existe.

   ```
   lun show -vserver vs1
   ```

```
Vserver  Path                 State     Mapped    Type     Size
-------- ----------------- --------- --------- -------- -------
vs1      /vol/vol1/lun1    online   unmapped  windows  47.07MB
```

3. Utilice la `volume file clone create` Comando para crear la LUN FlexClone.

   `volume file clone create -vserver vs1 -volume vol1 -source-path lun1 -destination-path/lun1_clone`

   Si necesita que la LUN de FlexClone esté disponible para su eliminación automática, tendrá que incluir `-autodelete true`. Si crea este LUN FlexClone en un volumen mediante el aprovisionamiento semi-grueso, debe habilitar la eliminación automática para todas las LUN de FlexClone.

4. Utilice la `lun show` Comando para verificar que ha creado una LUN.

   `lun show -vserver vs1`

```
Vserver  Path                     State    Mapped   Type     Size
-------- ----------------------- -------- -------- -------- ------
vs1      /vol/volX/lun1          online   unmapped windows  47.07MB
vs1      /vol/volX/lun1_clone    online   unmapped windows  47.07MB
```

Crear LUN FlexClone a partir de una copia snapshot en un volumen

Puede usar una copia snapshot del volumen para crear copias FlexClone de las LUN. Las copias FlexClone de las LUN son legibles y editables.

Lo que necesitará

Debe instalar una licencia de FlexClone. Esta licencia se incluye con "ONTAP One".

Acerca de esta tarea

La LUN FlexClone hereda el atributo de reservas de espacio de la LUN principal. Un LUN FlexClone con reserva de espacio requiere tanto espacio como la LUN principal con reserva de espacio. Si la LUN FlexClone no está reservada para el espacio, el volumen debe tener espacio suficiente para acomodar los cambios en el clon.

Pasos

1. Compruebe que la LUN no está asignada ni se está escribiendo en.
2. Cree una copia Snapshot del volumen que contenga las LUN:

   `volume snapshot create -vserver` *`vserver_name`* `-volume` *`volume_name`* `-snapshot` *`snapshot_name`*

   Debe crear una copia Snapshot (la copia Snapshot que realiza la copia) de la LUN que desea clonar.

3. Cree la LUN FlexClone a partir de la copia Snapshot:

```
file clone create -vserver vserver_name -volume volume_name -source-path
source_path -snapshot-name snapshot_name -destination-path destination_path
```

Si necesita que la LUN de FlexClone esté disponible para su eliminación automática, tendrá que incluir `-autodelete true`. Si crea este LUN FlexClone en un volumen mediante el aprovisionamiento semi-grueso, debe habilitar la eliminación automática para todas las LUN de FlexClone.

4. Compruebe que la LUN de FlexClone es correcta:

```
lun show -vserver vserver_name
```

```
Vserver Path                      State    Mapped    Type     Size
------- ----------------------    -------- --------- -------- -------
vs1     /vol/vol1/lun1_clone      online   unmapped windows   47.07MB
vs1     /vol/vol1/lun1_snap_clone online   unmapped windows   47.07MB
```

Evitar que se elimine automáticamente un archivo FlexClone o una LUN de FlexClone específica

Si configura un volumen FlexVol para eliminar automáticamente archivos FlexClone y LUN FlexClone, es posible eliminar cualquier clon que se ajuste a los criterios que especifique. Si tiene archivos FlexClone o LUN FlexClone específicos que desea conservar, puede excluirlos del proceso automático de eliminación de FlexClone.

Lo que necesitará

Debe instalar una licencia de FlexClone. Esta licencia se incluye con "ONTAP One".

Acerca de esta tarea

Cuando se crea un archivo FlexClone o una LUN de FlexClone, se deshabilita de forma predeterminada la configuración de eliminación automática del clon. Los archivos FlexClone y las LUN FlexClone con eliminación automática desactivada se conservan cuando se configura un volumen FlexVol para eliminar automáticamente los clones para reclamar espacio en el volumen.

> Si establece la `commitment` nivele el volumen a. `try` o. `disrupt`, Puede conservar de forma individual archivos de FlexClone o LUN de FlexClone desactivando la eliminación automática de dichos clones. Sin embargo, si establece la `commitment` nivele el volumen a. `destroy` y las listas de destrucción incluyen `lun_clone,file_clone`, La configuración de volumen anula la configuración de clon y todos los archivos FlexClone y las LUN FlexClone se pueden eliminar independientemente de la configuración de eliminación automática de los clones.

Pasos

1. Evite que un archivo FlexClone o una LUN de FlexClone específicos se eliminen automáticamente mediante el `volume file clone autodelete` comando.

   El ejemplo siguiente muestra cómo puede deshabilitar la eliminación automática para FlexClone LUN lun1_clone contenido en vol1:

```
cluster1::> volume file clone autodelete -vserver vs1 -volume vol1
-clone-path lun1_clone -enable false
```

No se puede eliminar automáticamente un archivo FlexClone o una LUN FlexClone con la eliminación automática para reclamar espacio en el volumen.

2. Compruebe que la eliminación automática está deshabilitada para el archivo FlexClone o la LUN FlexClone mediante el `volume file clone show-autodelete` comando.

   El ejemplo siguiente muestra que la eliminación automática es falsa para la LUN FlexClone lun1_clone:

```
cluster1::> volume file clone show-autodelete -vserver vs1 -clone-path
vol/vol1/lun1_clone
                                                                Vserver
Name: vs1
                                                                Clone Path:
vol/vol1/lun1_clone
                                                                Autodelete
Enabled: false
```

Configuración y uso de backups de SnapVault en un entorno SAN

Configuración y uso de los backups de SnapVault en una descripción general del entorno SAN

La configuración y el uso de SnapVault en un entorno SAN son muy similares a la configuración y el uso en un entorno NAS, pero para restaurar las LUN en un entorno SAN se requieren procedimientos especiales.

Los backups de SnapVault contienen un conjunto de copias de solo lectura de un volumen de origen. En un entorno SAN, siempre realiza un backup de volúmenes completos en el volumen secundario de SnapVault, no de LUN individuales.

El procedimiento para crear e inicializar la relación de SnapVault entre un volumen primario que contiene LUN y un volumen secundario que actúa como un backup de SnapVault es idéntico al procedimiento utilizado con los volúmenes FlexVol utilizados para protocolos de archivos. Este procedimiento se describe detalladamente en "Protección de datos".

Es importante garantizar que las LUN de las que se realiza el backup tengan un estado coherente antes de que se creen y copien al volumen secundario de SnapVault. Automatizar la creación de copias Snapshot con SnapCenter garantiza que la aplicación original pueda usar las LUN de backup.

Existen tres opciones básicas para restaurar LUN a partir de un volumen secundario de SnapVault:

- Puede asignar un LUN directamente desde el volumen secundario de SnapVault y conectar un host a la LUN para acceder al contenido de dicha LUN.

  La LUN es de solo lectura y solo se puede asignar de la copia Snapshot más reciente en el backup de SnapVault. Se pierden las reservas persistentes y otros metadatos de los LUN. Si lo desea, puede utilizar

un programa de copia en el host para copiar el contenido de la LUN nuevamente en la LUN original si aún está accesible.

La LUN tiene un número de serie diferente a la LUN de origen.

- Es posible clonar cualquier copia Snapshot en el volumen secundario SnapVault en un nuevo volumen de lectura y escritura.

  A continuación, puede asignar cualquiera de las LUN del volumen y conectar un host a la LUN para acceder al contenido del LUN. Si lo desea, puede utilizar un programa de copia en el host para copiar el contenido de la LUN nuevamente en la LUN original si aún está accesible.

- Puede restaurar todo el volumen que contiene el LUN desde cualquier copia Snapshot en el volumen secundario de SnapVault.

  La restauración de todo el volumen sustituye a todas las LUN y todos los archivos del volumen. Se pierden todas las nuevas LUN creadas desde que se creó la copia Snapshot.

  Las LUN conservan su asignación, números de serie, UUID y reservas persistentes.

Acceda a una copia de LUN de solo lectura desde un backup de SnapVault

Puede acceder a una copia de solo lectura de una LUN de la última copia de Snapshot de un backup de SnapVault. El ID de LUN, la ruta y el número de serie son diferentes de la LUN de origen y deben asignarse primero. Las reservas persistentes, las asignaciones de LUN y los iGroups no se replican en el volumen secundario de SnapVault.

Lo que necesitará

- Debe inicializarse la relación de SnapVault y la última copia Snapshot del volumen secundario de SnapVault debe contener la LUN deseada.
- La máquina virtual de almacenamiento (SVM) que contiene el backup de SnapVault debe tener una o varias LIF con el protocolo SAN deseado accesible desde el host utilizado para acceder a la copia de LUN.
- Si piensa acceder a las copias de LUN directamente desde el volumen secundario de SnapVault, debe crear los iGroups en la SVM de SnapVault con antelación.

  Es posible acceder a un LUN directamente desde el volumen secundario de SnapVault sin tener que restaurar o clonar primero el volumen que contiene la LUN.

Acerca de esta tarea

Si una nueva copia Snapshot se añade al volumen secundario SnapVault mientras tiene una LUN asignada de una copia Snapshot anterior, el contenido de la LUN asignada cambia. La LUN sigue asignada con los mismos identificadores, pero los datos se toman de la nueva copia Snapshot. Si cambia el tamaño de LUN, algunos hosts detectan automáticamente el cambio de tamaño; los hosts Windows requieren que se vuelva a analizar el disco para recoger cualquier cambio de tamaño.

Pasos

1. Ejecute el `lun show` Comando para enumerar los LUN disponibles en el volumen secundario de SnapVault.

   En este ejemplo, puede ver tanto las LUN originales en el volumen primario srcvola como las copias en el volumen secundario de SnapVault dstvolB:

```
cluster::> lun show

Vserver   Path                  State   Mapped   Type          Size
--------  ------------------    ------  -------  --------      -------
vserverA  /vol/srcvolA/lun_A  online  mapped   windows  300.0GB
vserverA  /vol/srcvolA/lun_B  online  mapped   windows  300.0GB
vserverA  /vol/srcvolA/lun_C  online  mapped   windows  300.0GB
vserverB  /vol/dstvolB/lun_A  online  unmapped windows  300.0GB
vserverB  /vol/dstvolB/lun_B  online  unmapped windows  300.0GB
vserverB  /vol/dstvolB/lun_C  online  unmapped windows  300.0GB

6 entries were displayed.
```

2. Si el igroup del host deseado no existe en la SVM que contiene el volumen secundario de SnapVault, ejecute el `igroup create` comando para crear un igroup.

   Este comando crea un igroup para un host Windows que utiliza el protocolo iSCSI:

```
cluster::> igroup create -vserver vserverB -igroup temp_igroup
  -protocol iscsi -ostype windows
  -initiator iqn.1991-05.com.microsoft:hostA
```

3. Ejecute el `lun mapping create` Comando para asignar la copia LUN deseada al igroup.

```
cluster::> lun mapping create -vserver vserverB -path /vol/dstvolB/lun_A
  -igroup temp_igroup
```

4. Conecte el host a la LUN y acceda al contenido de la LUN como desee.

Restaure un solo LUN a partir de un backup de SnapVault

Es posible restaurar un solo LUN a una nueva ubicación o a la ubicación original. Puede restaurar desde cualquier copia Snapshot en el volumen secundario de SnapVault. Para restaurar la LUN en la ubicación original, primero debe restaurarla en una nueva ubicación y, a continuación, copiarla.

Lo que necesitará

- Debe inicializarse la relación de SnapVault, y el volumen secundario de SnapVault debe contener una copia Snapshot adecuada para restaurar.
- La máquina virtual de almacenamiento (SVM) que contiene el volumen secundario de SnapVault debe tener una o más LIF con el protocolo SAN deseado a los que se puede acceder desde el host que se utiliza para acceder a la copia de LUN.
- Los iGroups ya deben existir en la SVM de SnapVault.

Acerca de esta tarea

El proceso incluye crear un clon de volumen de lectura y escritura a partir de una copia Snapshot en el volumen secundario de SnapVault. Puede utilizar la LUN directamente desde el clon, o bien puede copiar de nuevo el contenido de la LUN a su ubicación original.

La LUN del clon tiene una ruta y un número de serie diferentes a la LUN original. No se conservan las reservas persistentes.

Pasos

1. Ejecute el `snapmirror show` Comando para verificar el volumen secundario que contiene el backup de SnapVault.

```
cluster::> snapmirror show

Source          Dest     Mirror  Relation  Total             Last
Path     Type   Path     State   Status    Progress  Healthy Updated
-------- ---- --------- ------- --------- --------- ------- -------
vserverA:srcvolA
         XDP  vserverB:dstvolB
                          Snapmirrored
                                  Idle       -         true    -
```

2. Ejecute el `volume snapshot show` Comando para identificar la copia Snapshot desde la que desea restaurar la LUN.

```
cluster::> volume snapshot show

Vserver  Volume  Snapshot                 State Size   Total% Used%
-------- ------- ---------------------- ----- ------ ------ -----
vserverB
         dstvolB
                 snap2.2013-02-10_0010  valid  124KB     0%    0%
                 snap1.2013-02-10_0015 valid  112KB     0%    0%
                 snap2.2013-02-11_0010  valid  164KB     0%    0%
```

3. Ejecute el `volume clone create` Comando para crear un clon de lectura y escritura a partir de la copia Snapshot que desea.

   El clon de volumen se crea en el mismo agregado que el backup de SnapVault. Debe haber suficiente espacio en el agregado para almacenar el clon.

```
cluster::> volume clone create -vserver vserverB
  -flexclone dstvolB_clone -type RW -parent-volume dstvolB
  -parent-snapshot daily.2013-02-10_0010
[Job 108] Job succeeded: Successful
```

4. Ejecute el `lun show` Comando para mostrar las LUN del clon del volumen.

```
cluster::> lun show -vserver vserverB -volume dstvolB_clone

Vserver   Path                        State   Mapped   Type
--------- ------------------------  ------- -------- --------
vserverB  /vol/dstvolB_clone/lun_A  online  unmapped windows
vserverB  /vol/dstvolB_clone/lun_B  online  unmapped windows
vserverB  /vol/dstvolB_clone/lun_C  online  unmapped windows

3 entries were displayed.
```

5. Si el igroup del host deseado no existe en la SVM que contiene el backup de SnapVault, ejecute el `igroup create` comando para crear un igroup.

   En este ejemplo, se crea un igroup para un host Windows que utiliza el protocolo iSCSI:

```
cluster::> igroup create -vserver vserverB -igroup temp_igroup
  -protocol iscsi -ostype windows
  -initiator iqn.1991-05.com.microsoft:hostA
```

6. Ejecute el `lun mapping create` Comando para asignar la copia LUN deseada al igroup.

```
cluster::> lun mapping create -vserver vserverB
  -path /vol/dstvolB_clone/lun_C -igroup temp_igroup
```

7. Conecte el host a la LUN y acceda al contenido de la LUN, según lo desee.

   La LUN es de lectura y escritura y se puede utilizar en lugar de la LUN original. Dado que el número de serie de la LUN es diferente, el host lo interpreta como un LUN diferente al original.

8. Use un programa de copia en el host para copiar el contenido de la LUN nuevamente en la LUN original.

Restaurar todos los LUN de un volumen a partir de un backup de SnapVault

Si necesita restaurar uno o varios LUN de un volumen desde un backup de SnapVault, puede restaurar el volumen completo. La restauración del volumen afecta a todos los LUN del volumen.

Lo que necesitará

Debe inicializarse la relación de SnapVault, y el volumen secundario de SnapVault debe contener una copia Snapshot adecuada para restaurar.

Acerca de esta tarea

Si se restaura un volumen completo, este volverá al estado que tenía cuando se hizo la copia Snapshot. Si se agregó una LUN al volumen después de la copia Snapshot, esa LUN se elimina durante el proceso de

restauración.

Después de restaurar el volumen, las LUN siguen asignadas a los iGroups a los que se asignaron justo antes de la restauración. La asignación de LUN puede ser diferente del mapa en el momento de la copia Snapshot. Se conservan las reservas persistentes en los LUN de clústeres de hosts.

Pasos

1. Detenga las operaciones de I/o en todos los LUN del volumen.
2. Ejecute el `snapmirror show` Comando para verificar el volumen secundario que contiene el volumen secundario de SnapVault.

```
cluster::> snapmirror show

Source          Dest     Mirror  Relation  Total             Last
Path     Type   Path     State   Status    Progress  Healthy Updated
-------- ---- --------- ------- --------- --------- ------- -------
vserverA:srcvolA
         XDP  vserverB:dstvolB
                          Snapmirrored
                                  Idle       -         true    -
```

3. Ejecute el `volume snapshot show` Comando para identificar la copia Snapshot desde la que desea restaurar.

```
cluster::> volume snapshot show

Vserver  Volume  Snapshot                State Size   Total% Used%
-------- ------- ---------------------- ----- ------ ------ -----
vserverB
         dstvolB
                 snap2.2013-02-10_0010  valid  124KB     0%    0%
                 snap1.2013-02-10_0015 valid  112KB     0%    0%
                 snap2.2013-02-11_0010  valid  164KB     0%    0%
```

4. Ejecute el `snapmirror restore` y especifique el `-source-snapshot` Opción para especificar la copia Snapshot que se usará.

   El destino que se especifica para la restauración es el volumen original al que se va a restaurar.

```
cluster::> snapmirror restore -destination-path vserverA:srcvolA
  -source-path vserverB:dstvolB -source-snapshot daily.2013-02-10_0010

Warning: All data newer than Snapshot copy hourly.2013-02-11_1205 on
volume vserverA:src_volA will be deleted.
Do you want to continue? {y|n}: y
[Job 98] Job is queued: snapmirror restore from source
"vserverB:dstvolB" for the snapshot daily.2013-02-10_0010.
```

5. Si va a compartir LUN en un clúster de hosts, restaure las reservas persistentes en los LUN de los hosts afectados.

Restaurar un volumen a partir de un backup de SnapVault

En el siguiente ejemplo, la LUN llamada lun_D se agregó al volumen después de crear la copia Snapshot. Después de restaurar todo el volumen a partir de la copia Snapshot, lun_D ya no aparece.

En la `lun show` Resultado del comando, puede ver las LUN en el srcvolA del volumen primario y las copias de solo lectura de esas LUN en el volumen secundario de SnapVault dstvolB. No hay copia de lun_D en el backup de SnapVault.

```
cluster::> lun show
Vserver   Path                  State   Mapped   Type          Size
--------- ------------------    ------- -------- --------      -------
vserverA  /vol/srcvolA/lun_A  online  mapped   windows  300.0GB
vserverA  /vol/srcvolA/lun_B  online  mapped   windows  300.0GB
vserverA  /vol/srcvolA/lun_C  online  mapped   windows  300.0GB
vserverA  /vol/srcvolA/lun_D  online  mapped   windows  250.0GB
vserverB  /vol/dstvolB/lun_A  online  unmapped windows  300.0GB
vserverB  /vol/dstvolB/lun_B  online  unmapped windows  300.0GB
vserverB  /vol/dstvolB/lun_C  online  unmapped windows  300.0GB

7 entries were displayed.

cluster::>snapmirror restore -destination-path vserverA:srcvolA
  -source-path vserverB:dstvolB
  -source-snapshot daily.2013-02-10_0010

Warning: All data newer than Snapshot copy hourly.2013-02-11_1205
on volume vserverA:src_volA will be deleted.
Do you want to continue? {y|n}: y
[Job 98] Job is queued: snapmirror restore from source
"vserverB:dstvolB" for the snapshot daily.2013-02-10_0010.

cluster::> lun show
Vserver   Path                  State   Mapped   Type          Size
--------- ------------------    ------- -------- --------      -------
vserverA  /vol/srcvolA/lun_A  online  mapped   windows  300.0GB
vserverA  /vol/srcvolA/lun_B  online  mapped   windows  300.0GB
vserverA  /vol/srcvolA/lun_C  online  mapped   windows  300.0GB
vserverB  /vol/dstvolB/lun_A  online  unmapped windows  300.0GB
vserverB  /vol/dstvolB/lun_B  online  unmapped windows  300.0GB
vserverB  /vol/dstvolB/lun_C  online  unmapped windows  300.0GB

6 entries were displayed.
```

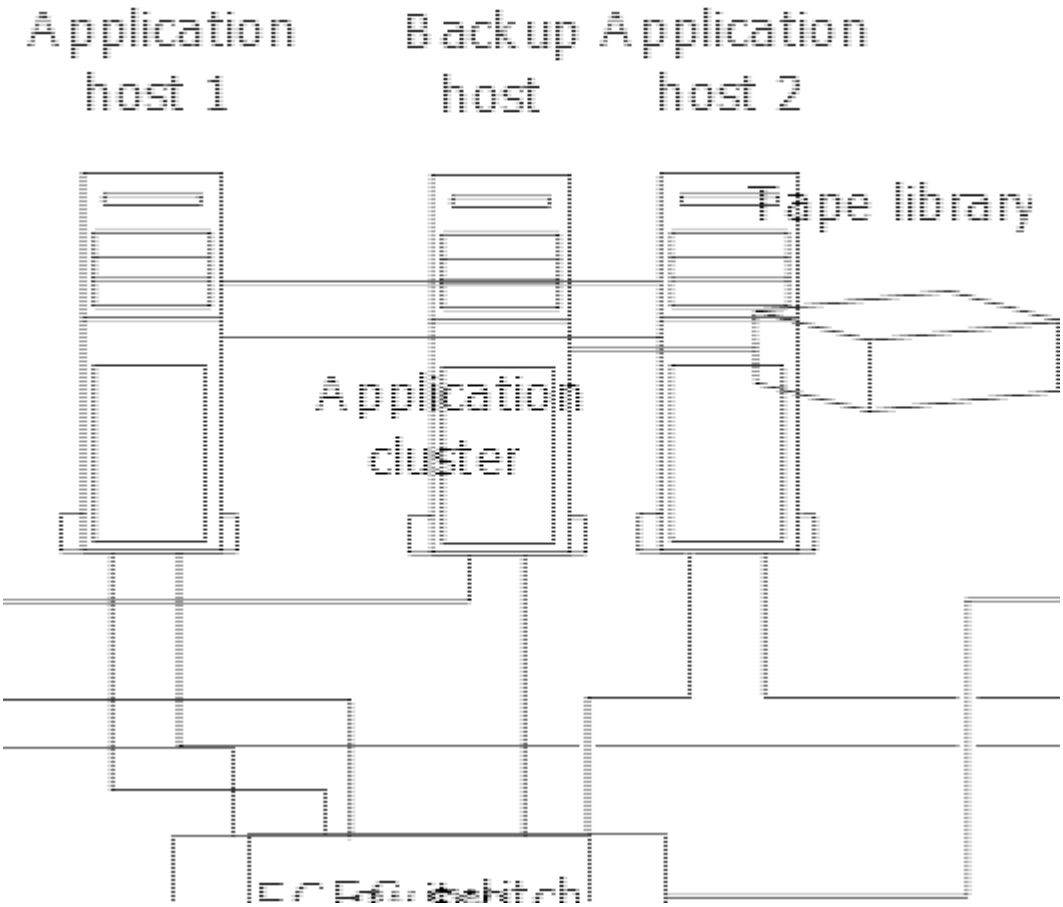
Una vez que se restaura el volumen secundario del SnapVault, el volumen de origen ya no contiene lun_D. No es necesario volver a asignar las LUN en el volumen de origen después de la restauración porque estas se siguen asignando.

Cómo se puede conectar un sistema de backup de host al sistema de almacenamiento primario

Se puede lanzar backups de sistemas SAN a cinta a través de un host de backup independiente para evitar que el rendimiento se resienta en el host de aplicaciones.

Es imprescindible mantener separados los datos DE SAN y NAS con fines de backup. La siguiente figura

muestra la configuración física recomendada para un sistema de backup host al sistema de almacenamiento principal. Debe configurar los volúmenes como solo SAN. Las LUN pueden quedar limitadas a un único volumen o las LUN pueden propagarse por varios volúmenes o sistemas de almacenamiento.



Los volúmenes de un host pueden consistir en una única LUN asignada desde el sistema de almacenamiento o de varias LUN mediante un gestor de volúmenes, como VxVM en sistemas HP-UX.

Realice un backup de una LUN a través de un sistema de backup del host

Es posible usar un LUN clonado de una copia Snapshot como datos de origen para el sistema de backup host.

Lo que necesitará

Debe haber una LUN de producción y asignarse a un igroup que incluya el nombre de nodo WWPN o iniciador del servidor de aplicaciones. La LUN también se debe formatear y es accesible para el host

Pasos

1. Guarde el contenido de los búferes del sistema de archivos del host en el disco.

   Se puede utilizar el comando provisto por el sistema operativo del host, o bien se puede utilizar SnapDrive para Windows y SnapDrive para UNIX. También puede optar por hacer que este paso forme parte de su script de procesamiento previo de la copia DE seguridad DE SAN.

2. Utilice la `volume snapshot create` Comando para crear una copia Snapshot de la LUN de producción.

   ```
   volume snapshot create -vserver vs0 -volume vol3 -snapshot vol3_snapshot
   ```

```
-comment "Single snapshot" -foreground false
```

3. Utilice la `volume file clone create` Comando para crear un clon de la LUN de producción.

   ```
   volume file clone create -vserver vs3 -volume vol3 -source-path lun1 -snapshot
   -name snap_vol3 -destination-path lun1_backup
   ```

4. Utilice la `lun igroup create` Comando para crear un igroup que incluye el WWPN del servidor de backup.

   ```
   lun igroup create -vserver vs3 -igroup igroup3 -protocol fc -ostype windows
   -initiator 10:00:00:00:c9:73:5b:91
   ```

5. Utilice la `lun mapping create` Comando para asignar el clon de LUN que creó en el paso 3 al host de backup.

   ```
   lun mapping create -vserver vs3 -volume vol3 -lun lun1_backup -igroup igroup3
   ```

   Puede optar por hacer que este paso forme parte de la secuencia de comandos de posprocesamiento de su aplicación DE backup SAN.

6. Desde el host, detectar el nuevo LUN y hacer que el sistema de archivos esté disponible para el host.

   Puede optar por hacer que este paso forme parte de la secuencia de comandos de posprocesamiento de su aplicación DE backup SAN.

7. Realice un backup de los datos del clon LUN desde el host de backup a cinta con la aplicación de backup SAN.
8. Utilice la `lun modify` Comando para desconectar el clon de la LUN.

   ```
   lun modify -vserver vs3 -path /vol/vol3/lun1_backup -state offline
   ```

9. Utilice la `lun delete` Para quitar el clon LUN.

   ```
   lun delete -vserver vs3 -volume vol3 -lun lun1_backup
   ```

10. Utilice la `volume snapshot delete` Comando para quitar la copia Snapshot.

    ```
    volume snapshot delete -vserver vs3 -volume vol3 -snapshot vol3_snapshot
    ```

Referencia para la configuración DE SAN

Información general de la configuración DE SAN

Una red de área de almacenamiento (SAN) consta de una solución de almacenamiento conectada a los hosts a través de un protocolo de transporte SAN como iSCSI o FC. Puede configurar el SAN para que su solución de almacenamiento se conecte a los hosts mediante uno o varios switches. Si utiliza iSCSI, también puede configurar su SAN de modo que su solución de almacenamiento se conecte directamente al host sin necesidad de switch.

En una SAN, varios hosts, mediante diferentes sistemas operativos, como Windows, Linux o UNIX, pueden acceder a la solución de almacenamiento a la vez. Puede utilizar "Asignación de LUN selectiva" y.. "conjuntos de puertos" limitar el acceso a los datos entre los hosts y el almacenamiento.

Para iSCSI, la topología de red entre la solución de almacenamiento y los hosts se denomina red. Para FC, FC/NVMe y FCoE La topología de red entre la solución de almacenamiento y los hosts se conoce como estructura. Para crear redundancia, que le proteja de la pérdida de acceso a los datos, debería configurar la SAN con parejas de alta disponibilidad en una configuración multired o multiestructura. Las configuraciones que utilizan nodos únicos o redes/estructuras únicas no son totalmente redundantes, por lo que no se recomiendan.

Después de configurar la SAN, puede "Aprovisione almacenamiento para iSCSI o FC", o usted puede "Aprovisione almacenamiento para FC/NVMe". Luego puede conectarse a los hosts para comenzar a reparar datos.

La compatibilidad con el protocolo SAN varía en función de la versión de ONTAP, su plataforma y la configuración. Para obtener detalles sobre su configuración específica, consulte "Herramienta de matriz de interoperabilidad de NetApp".

Información relacionada

- "Descripción de la administración de San"
- "Configuración, compatibilidad y limitaciones de NVMe"

Configuraciones de iSCSI

Formas de configurar hosts SAN iSCSI

Debe configurar la configuración de iSCSI con parejas de alta disponibilidad (HA) que se conecten directamente a sus hosts SAN iSCSI o que se conecten a los hosts a través de uno o más switches IP.

"Parejas de HA" Se definen como los nodos de generación de informes para las rutas Active/Optimized y Active/Unoptimizadas que usarán los hosts para acceder a las LUN. Varios hosts, utilizando diferentes sistemas operativos, como Windows, Linux o UNIX, pueden acceder al almacenamiento al mismo tiempo. Los hosts requieren que se instale y configure una solución multivía compatible con ALUA. Los sistemas operativos compatibles y las soluciones multivía se pueden verificar en el "Herramienta de matriz de interoperabilidad de NetApp".

En una configuración de varias redes, existen dos o más switches que conectan los hosts con el sistema de almacenamiento. Se recomiendan las configuraciones de varias redes porque son totalmente redundantes. En una configuración de red única, hay un switch que conecta los hosts al sistema de almacenamiento. Las configuraciones de red única no son totalmente redundantes.

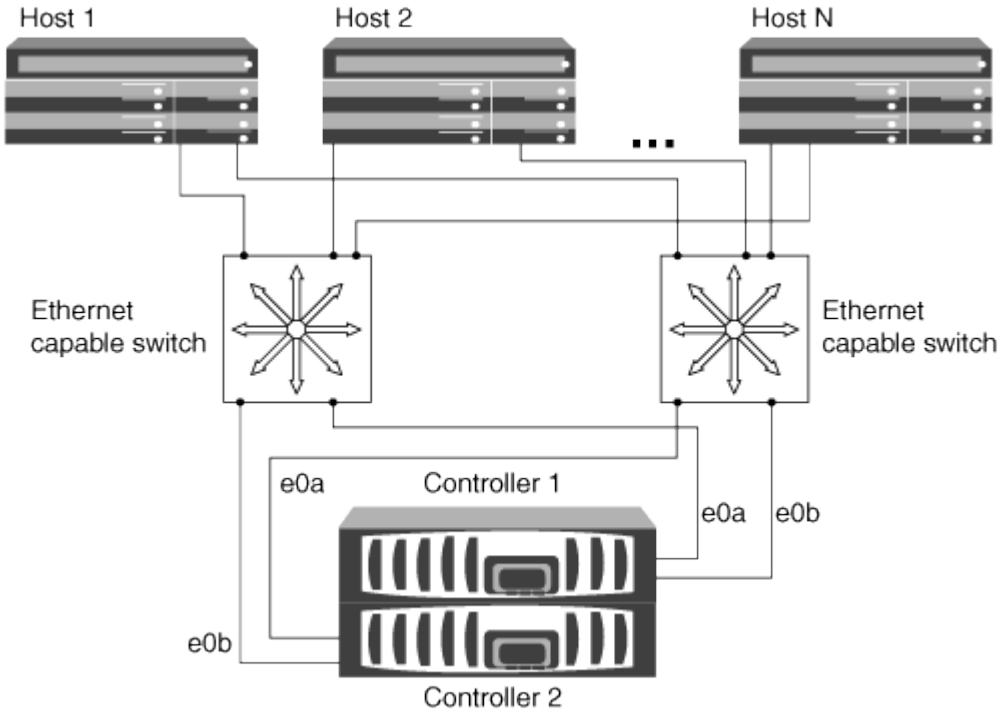
> "Configuraciones de nodo único" no se recomiendan porque no proporcionan la redundancia necesaria para admitir tolerancia a fallos y operaciones no disruptivas.

Información relacionada

- Vea cómo "Asignación de LUN selectiva (SLM)" Limita las rutas que se utilizan para acceder a las LUN que pertenece a una pareja de alta disponibilidad.
- Descubra "LIF SAN".
- Obtenga más información sobre "Ventajas de las VLAN en iSCSI".

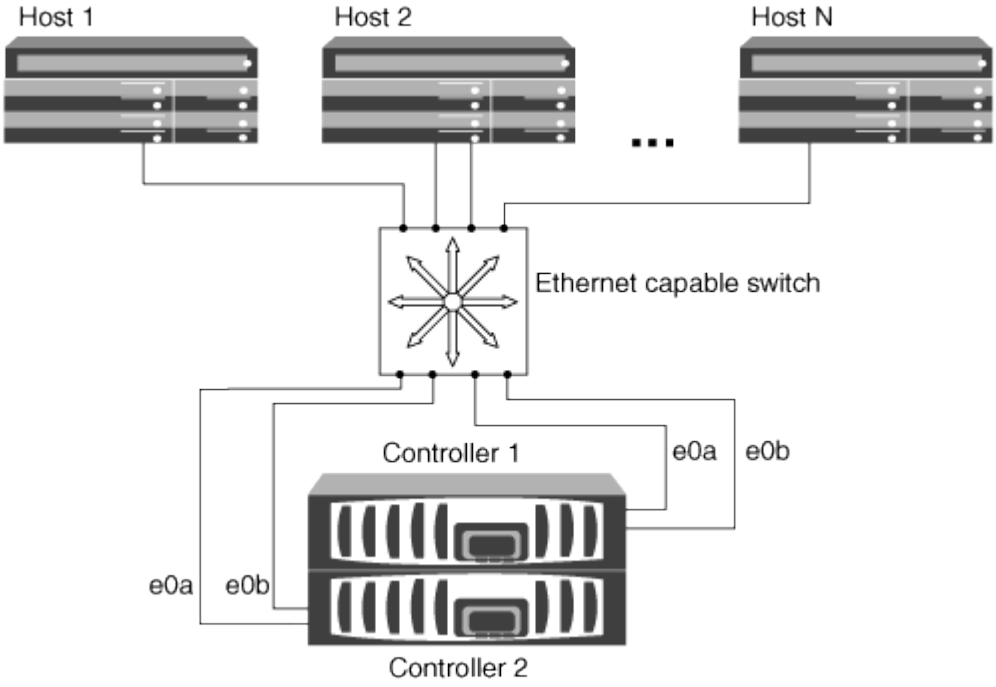
Configuraciones iSCSI multired

En las configuraciones de pares de alta disponibilidad de varias redes, dos o más switches conectan el par de alta disponibilidad con uno o más hosts. Dado que hay varios switches, esta configuración es completamente redundante.



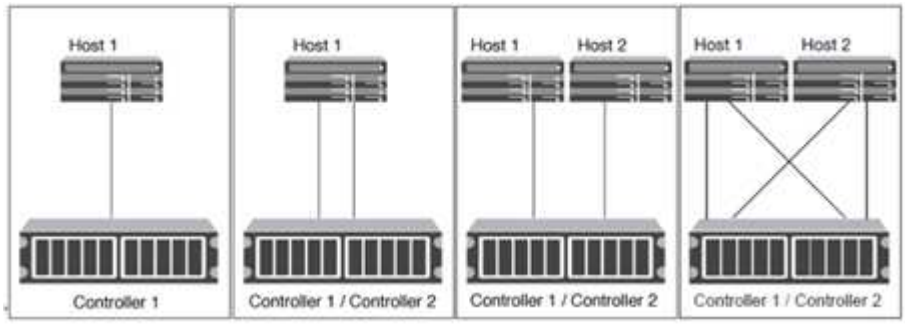
Configuraciones iSCSI de red única

En las configuraciones de pares de alta disponibilidad de red única, un switch conecta el par de alta disponibilidad a uno o varios hosts. Dado que hay un único switch, esta configuración no es completamente redundante.



Configuración iSCSI de conexión directa

En una configuración de conexión directa, uno o varios hosts están conectados directamente a las controladoras.



Ventajas de usar VLAN en configuraciones iSCSI

Una VLAN consta de un grupo de puertos switch agrupados en un dominio de difusión. Una VLAN puede estar en un único switch o puede abarcar varios chasis de switch. Las VLAN estáticas y dinámicas le permiten aumentar la seguridad, aislar problemas y limitar las rutas disponibles en la infraestructura de red IP.

Cuando se implementan VLAN en infraestructuras de redes IP grandes, se obtienen las siguientes ventajas:

- Mayor seguridad.

  VLAN le permite aprovechar la infraestructura existente a la vez que proporciona una seguridad mejorada porque limitan el acceso entre diferentes nodos de una red Ethernet o SAN IP.

- Fiabilidad mejorada de la red Ethernet y SAN IP mediante el aislamiento de los problemas.
- Reducción del tiempo de resolución de problemas limitando el espacio del problema.
- Reducción del número de rutas disponibles a un puerto de destino iSCSI en particular.
- Reducción del número máximo de rutas que utiliza un host.

  El hecho de tener demasiadas rutas ralentiza los tiempos de reconexión. Si un host no tiene una solución multivía, puede utilizar VLAN para permitir solo una ruta.

VLAN dinámicas

Las VLAN dinámicas se basan en direcciones MAC. Puede definir una VLAN especificando la dirección MAC de los miembros que desea incluir.

Las VLAN dinámicas proporcionan flexibilidad y no requieren la asignación a los puertos físicos en los que el dispositivo está conectado físicamente al conmutador. Puede mover un cable de un puerto a otro sin tener que configurar la VLAN de nuevo.

VLAN estáticas

Las VLAN estáticas se basan en puertos. El switch y el puerto del switch se utilizan para definir la VLAN y sus miembros.

Las VLAN estáticas ofrecen una seguridad mejorada porque no es posible romper las VLAN mediante la

suplantación de control de acceso a medios (MAC). Sin embargo, si alguien tiene acceso físico al switch, el reemplazo de un cable y la reconfiguración de la dirección de red puede permitir el acceso.

En algunos entornos, es más fácil crear y gestionar VLAN estáticas que las VLAN dinámicas. Esto es debido a que las VLAN estáticas requieren que solo se especifique el switch y el identificador de puerto, en lugar de la dirección MAC de 48 bits. Además, puede etiquetar los rangos de puertos del switch con el identificador de VLAN.

Configuraciones de FC

Formas de configurar los hosts SAN FC y FC-NVMe

Es recomendable configurar sus hosts SAN FC y FC-NVMe usando pares de alta disponibilidad y un mínimo de dos switches. Esto proporciona redundancia en las capas de la estructura y del sistema de almacenamiento para admitir tolerancia a fallos y operaciones no disruptivas. No puede conectar directamente hosts SAN FC o FC-NVMe a parejas de alta disponibilidad sin utilizar un switch.

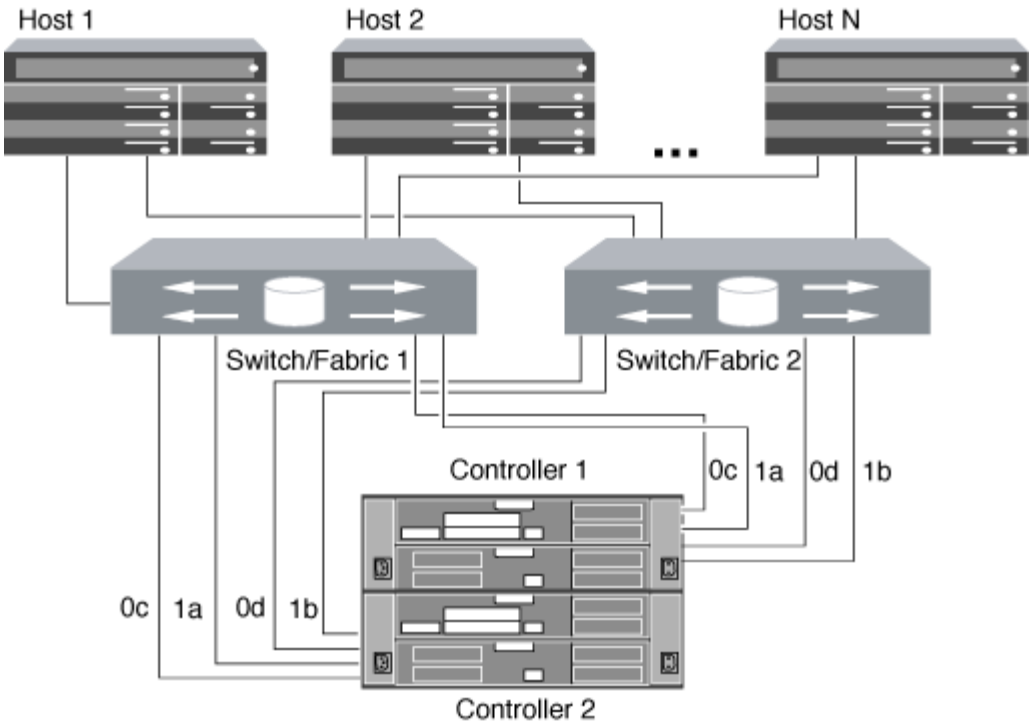
Las estructuras en cascada, malla parcial, malla completa, núcleo-borde y director son métodos estándar en el sector para conectar switches FC a una estructura, y todos son compatibles. No se admite el uso de estructuras heterogéneas de switches FC, a excepción de los switches blade integrados. Las excepciones específicas se enumeran en la "Herramienta de matriz de interoperabilidad". Una estructura puede estar compuesta por uno o varios switches y las controladoras de almacenamiento se pueden conectar a varios switches.

Varios hosts, utilizando diferentes sistemas operativos, como Windows, Linux o UNIX, pueden acceder a las controladoras de almacenamiento al mismo tiempo. Los hosts requieren que se instale y configure una solución multivía compatible. Los sistemas operativos compatibles y las soluciones multivía se pueden verificar en la herramienta de matriz de interoperabilidad.

Configuraciones FC y FC-NVMe multiestructura

En las configuraciones de par de alta disponibilidad multiestructura, existen dos o más switches que conectan pares de alta disponibilidad a uno o varios hosts. Para mayor simplicidad, la siguiente figura de par de alta disponibilidad multiestructura solo muestra dos estructuras, pero puede tener dos o más estructuras en cualquier configuración de estructura múltiple.

Los números de puerto de destino FC (0C, 0d, 1a, 1b) que aparecen en las ilustraciones son ejemplos. Los números de puerto reales varían según el modelo de su nodo de almacenamiento y si usa adaptadores de expansión.

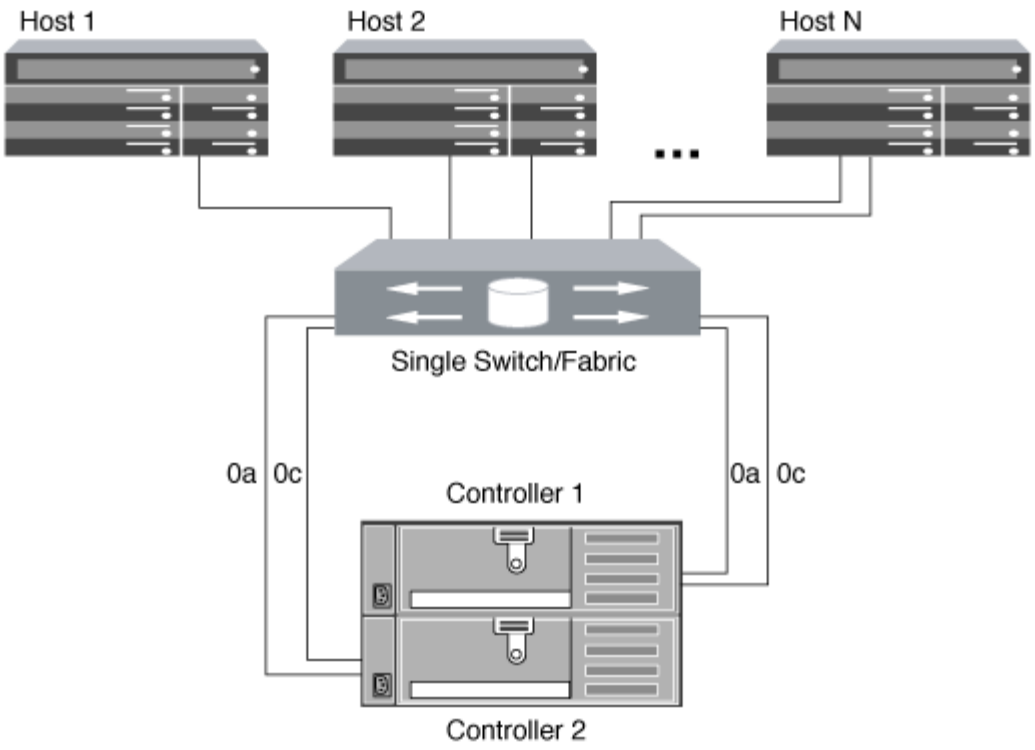


Configuraciones FC y FC-NVMe de estructura única

En configuraciones de pareja de alta disponibilidad de estructura única, existe una estructura que conecta ambas controladoras en el par de alta disponibilidad a uno o varios hosts. Dado que los hosts y las controladoras están conectados a través de un único switch, las configuraciones de par de alta disponibilidad de estructura única no son totalmente redundantes.

Los números de puerto de destino FC (0A, 0C) que aparecen en las ilustraciones son ejemplos. Los números de puerto reales varían según el modelo de su nodo de almacenamiento y si usa adaptadores de expansión.

Todas las plataformas que admiten las configuraciones FC admiten configuraciones de par de alta disponibilidad de estructura única.



"Configuraciones de nodo único" no se recomiendan porque no proporcionan la redundancia necesaria para admitir tolerancia a fallos y operaciones no disruptivas.

Información relacionada

- Vea cómo "Asignación de LUN selectiva (SLM)" Limita las rutas que se utilizan para acceder a las LUN que pertenece a una pareja de alta disponibilidad.
- Descubra "LIF SAN".

Prácticas recomendadas para la configuración del switch FC

Para obtener el mejor rendimiento, debe tener en cuenta ciertas prácticas recomendadas al configurar el switch de FC.

Una configuración permanente de la velocidad es la mejor práctica para las configuraciones de switch FC, especialmente en grandes estructuras, porque ofrece el mejor rendimiento para recompilaciones de estructuras y puede ahorrar mucho tiempo. Aunque la autonegociación ofrece la mayor flexibilidad, la configuración del switch de FC no siempre funciona del modo esperado y añade tiempo a la secuencia general de compilación de estructura.

Todos los switches que están conectados a la estructura deben ser compatibles con la virtualización de N_Port ID (NPIV) y deben tener NPIV habilitado. ONTAP utiliza NPIV para presentar destinos de FC a una estructura.

Para obtener más detalles sobre qué entornos se admiten, consulte "Herramienta de matriz de interoperabilidad de NetApp".

Para ver las prácticas recomendadas para FC e iSCSI, consulte "Informe técnico de NetApp 4080: Prácticas recomendadas para SAN moderno".

Número admitido de saltos de FC

El número máximo de saltos de FC admitidos entre un host y el sistema de almacenamiento depende del proveedor de switch y de la compatibilidad del sistema de almacenamiento para las configuraciones de FC.

Los saltos son el número de switches presentes en la ruta que va del iniciador (host) al destino (sistema de almacenamiento). Cisco también se refiere a este valor como el *diámetro de LA estructura DE SAN*.

Cambiar proveedor	Número de saltos admitidos
Brocade	7 GbE para FC, 5 GbE para FCoE
Cisco	7 para FC, hasta 3 de los switches pueden ser switches FCoE.

Información relacionada

"Descargas de NetApp: Documentos de matriz de escalabilidad de Brocade"

"Descargas de NetApp: Documentos de matriz de escalabilidad de Cisco"

Velocidades admitidas en el puerto de destino FC

Los puertos de destino FC pueden configurarse para que funcionen a diferentes velocidades. Debe configurar la velocidad del puerto de destino para que coincida con la velocidad del dispositivo al que se conecta. Todos los puertos de destino utilizados por un host determinado deben configurarse con la misma velocidad.

Los puertos de destino FC se pueden utilizar para las configuraciones FC-NVMe exactamente del mismo modo que se utilizan para las configuraciones FC.

Debe configurar la velocidad del puerto de destino para que coincida con la velocidad del dispositivo al que se conecta en vez de utilizar la autonegociación. Un puerto configurado para la autonegociación puede tardar más en volver a conectarse después de una toma de control/devolución u otra interrupción.

Puede configurar los puertos internos y los adaptadores de expansión para que se ejecuten a la velocidad siguiente. Cada controladora y puerto del adaptador de expansión se pueden configurar de forma individual para diferentes velocidades según sea necesario.

Puertos de 4 GB	Puertos de 8 GB	Puertos de 16 GB	Puertos de 32 GB
• 4 GB • 2 GB • 1 GB	• 8 GB • 4 GB • 2 GB	• 16 GB • 8 GB • 4 GB	• 32 GB • 16 GB • 8 GB

Los puertos UTA2 pueden utilizar un adaptador SFP+ de 8 GB para admitir velocidades de 8, 4 y 2 GB, si fuera necesario.

Recomendaciones de configuración de los puertos de destino FC

Para obtener el mejor rendimiento y la mayor disponibilidad, debe usar la configuración recomendada de puertos de destino FC.

En la siguiente tabla, se muestra el orden de uso de puertos preferido para los puertos de destino FC y FC-NVMe integrados. Para los adaptadores de expansión, los puertos FC deben propagarse para no usar el mismo ASIC para la conectividad. El orden de ranura preferido se muestra en la "Hardware Universe de NetApp" Para la versión del software ONTAP que utiliza el controlador.

FC-NVMe es compatible con los siguientes modelos:

- AFF A300

  Los puertos internos de AFF A300 no son compatibles con FC-NVMe.

- AFF A700
- AFF A700s
- AFF A800

Los sistemas FAS2520 no tienen puertos FC integrados y no admiten adaptadores complementarios.

Controladora	Pares de puertos con ASIC compartido	Número de puertos de destino: Puertos preferidos
FAS9000, AFF A700, AFF A700s y AFF A800	Ninguno	Todos los puertos de datos están en adaptadores de expansión. Consulte "Hardware Universe de NetApp" si quiere más información.
8080, 8060 y 8040	0e+0f 0g+0h	1: 0e 2: 0e, 0g 3: 0e, 0g, 0h 4: 0e, 0g, 0f, 0h
FAS8200 y AFF A300	0g+0h	1: 0g 2: 0g, 0h
8020	0c+0d	1: 0c 2: 0c, 0d

Controladora	Pares de puertos con ASIC compartido	Número de puertos de destino: Puertos preferidos
62xx	0a+0b 0c+0d	1: 0a 2: 0a, 0c 3: 0a, 0c, 0b 4: 0a, 0c, 0b, 0d
32xx	0c+0d	1: 0c 2: 0c, 0d
FAS2554, FAS2552, FAS2600 series,FAS2720,FAS2750, AFF A200 y AFF A220	0c+0d 0e+0f	1: 0c 2: 0c, 0e 3: 0c, 0e, 0d 4: 0c, 0e, 0d, 0f

Gestione sistemas con adaptadores de FC

Información general sobre la gestión de sistemas con adaptadores de FC

Hay comandos disponibles para gestionar los adaptadores FC integrados y las tarjetas adaptadoras FC. Estos comandos se pueden utilizar para configurar el modo del adaptador, mostrar información del adaptador y cambiar la velocidad.

La mayoría de los sistemas de almacenamiento tienen adaptadores FC integrados que se pueden configurar como iniciadores o destinos. También puede utilizar tarjetas adaptadoras de FC configuradas como iniciadores o destinos. Los iniciadores se conectan a las bandejas de discos del back-end y posiblemente a cabinas de almacenamiento externas (FlexArray). Los destinos se conectan solo a switches FC. Tanto los puertos HBA de destino FC como la velocidad del puerto del switch deben configurarse con el mismo valor y no deben configurarse en modo automático.

Comandos para gestionar adaptadores de FC

Puede usar comandos FC para gestionar adaptadores de destino FC, adaptadores de iniciador FC y adaptadores de FC integrados para su controladora de almacenamiento. Los mismos comandos se utilizan para gestionar adaptadores de FC para el protocolo FC y el protocolo FC-NVMe.

Los comandos de adaptador del iniciador de FC solo funcionan en el nivel del nodo. Debe utilizar el `run -node` *`node_name`* Antes de poder utilizar los comandos del adaptador del iniciador de FC.

Comandos para gestionar los adaptadores de destino de FC

Si desea…	Se usa este comando…
Muestra información del adaptador de FC en un nodo	`network fcp adapter show`
Modifique los parámetros del adaptador de destino FC	`network fcp adapter modify`
Muestra información sobre el tráfico del protocolo FC	`run -node node_name sysstat -f`
Muestra el tiempo que se ha ejecutado el protocolo FC	`run -node node_name uptime`
Mostrar la configuración y el estado del adaptador	`run -node node_name sysconfig -v adapter`
Compruebe qué tarjetas de expansión están instaladas y si hay algún error de configuración	`run -node node_name sysconfig -ac`
Ver una página de manual de un comando	`man command_name`

Comandos para gestionar los adaptadores de iniciador de FC

Si desea…	Se usa este comando…
Muestra información de todos los iniciadores y sus adaptadores en un nodo	`run -node node_name storage show adapter`
Mostrar la configuración y el estado del adaptador	`run -node node_name sysconfig -v adapter`
Compruebe qué tarjetas de expansión están instaladas y si hay algún error de configuración	`run -node node_name sysconfig -ac`

Comandos para gestionar los adaptadores de FC internos

Si desea…	Se usa este comando…
Muestra el estado de los puertos FC internos	`system node hardware unified-connect show`

Configure los adaptadores de FC para el modo iniciador

Puede configurar puertos FC individuales de adaptadores integrados y determinadas tarjetas adaptadoras FC para el modo iniciador. El modo iniciador se usa para conectar los puertos a unidades de cinta, bibliotecas de cintas o almacenamiento de terceros con la virtualización de FlexArray o con importación de LUN externa (FLI).

Lo que necesitará

- Las LIF del adaptador deben eliminarse de cualquier conjunto de puertos de los que pertenezcan.
- Todas las LIF de todas las máquinas virtuales de almacenamiento (SVM) que utilizan el puerto físico que se va a modificar deben migrarse o destruirse antes de cambiar la personalidad del puerto físico de destino a iniciador.

Acerca de esta tarea

Cada puerto FC integrado se puede configurar de forma individual como iniciador o destino. Los puertos en determinados adaptadores de FC también se pueden configurar de forma individual como un puerto de destino o como un puerto iniciador, al igual que los puertos FC integrados. Hay disponible una lista de adaptadores que se pueden configurar para el modo de destino en "Hardware Universe de NetApp".

NVMe/FC no admite el modo iniciador.

Pasos

1. Quite todas las LIF del adaptador:

   ```
   network interface delete -vserver SVM_name -lif lif_name,lif_name
   ```

2. Desconectar el adaptador:

   ```
   network fcp adapter modify -node node_name -adapter adapter_port -status-admin
   down
   ```

   Si el adaptador no se desconecta, también puede quitar el cable del puerto de adaptador correspondiente del sistema.

3. Cambie el adaptador del destino al iniciador:

   ```
   system hardware unified-connect modify -t initiator adapter_port
   ```

4. Reinicie el nodo que aloja el adaptador que cambió.
5. Compruebe que los puertos FC estén configurados en estado correcto para la configuración:

   ```
   system hardware unified-connect show
   ```

6. Vuelva a conectar el adaptador:

   ```
   node run -node node_name storage enable adapter adapter_port
   ```

Configure los adaptadores de FC para el modo de destino

Puede configurar puertos FC individuales de adaptadores integrados y determinadas tarjetas adaptadoras FC para el modo destino. El modo de destino se utiliza para conectar los puertos a iniciadores FC.

Acerca de esta tarea

Cada puerto FC integrado se puede configurar de forma individual como iniciador o destino. Los puertos en determinados adaptadores de FC también se pueden configurar de forma individual como un puerto de destino o como un puerto iniciador, al igual que los puertos FC integrados. Hay disponible una lista de adaptadores que se pueden configurar para el modo de destino en "Hardware Universe de NetApp".

Los mismos pasos se utilizan cuando se configuran los adaptadores de FC para el protocolo FC y el protocolo FC-NVMe. Sin embargo, solo ciertos adaptadores de FC admiten FC-NVMe. Consulte "Hardware Universe de NetApp" Para obtener una lista de los adaptadores que admiten el protocolo FC-NVMe.

Pasos

1. Desconectar el adaptador:

   ```
   node run -node node_name storage disable adapter adapter_name
   ```

   Si el adaptador no se desconecta, también puede quitar el cable del puerto de adaptador correspondiente del sistema.

2. Cambie el adaptador del iniciador al destino:

   ```
   system node hardware unified-connect modify -t target -node node_name adapter
   adapter_name
   ```

3. Reinicie el nodo que aloja el adaptador que cambió.
4. Compruebe que el puerto de destino tiene la configuración correcta:

   ```
   network fcp adapter show -node node_name
   ```

5. Conectar su adaptador:

   ```
   network fcp adapter modify -node node_name -adapter adapter_port -state up
   ```

Muestra información sobre un adaptador de destino de FC

Puede utilizar el `network fcp adapter show` Comando para mostrar la información de la configuración del sistema y del adaptador de cualquier adaptador de FC en el sistema.

Paso

1. Muestra información sobre el adaptador de FC mediante el `network fcp adapter show` comando.

   El resultado muestra información de configuración del sistema y información del adaptador para cada ranura que se utiliza.

   ```
   network fcp adapter show -instance -node node1 -adapter 0a
   ```

Cambie la velocidad del adaptador de FC

Debe configurar la velocidad del puerto de destino del adaptador para que coincida con la velocidad del dispositivo al que se conecta, en vez de utilizar la autonegociación. Un puerto configurado para la autonegociación puede tardar más tiempo en reconectar después de una toma de control/devolución u otra interrupción.

Lo que necesitará

Todos los LIF que utilizan este adaptador como puerto de inicio deben estar desconectados.

Acerca de esta tarea

Dado que esta tarea abarca todas las máquinas virtuales de almacenamiento (SVM) y todos los LIF de un clúster, debe utilizar el `-home-port` y.. `-home-lif` parámetros para limitar el alcance de esta operación. Si no utiliza estos parámetros, la operación se aplica a todas las LIF del clúster, lo que podría no ser deseable.

Pasos

1. Desconecte todas las LIF de este adaptador:

   ```
   network interface modify -vserver * -lif * { -home-node node1 -home-port 0c }
   -status-admin down
   ```

2. Desconectar el adaptador:

   ```
   network fcp adapter modify -node node1 -adapter 0c -state down
   ```

   Si el adaptador no se desconecta, también puede quitar el cable del puerto de adaptador correspondiente del sistema.

3. Determine la velocidad máxima del adaptador de puerto:

   ```
   fcp adapter show -instance
   ```

   No puede modificar la velocidad del adaptador más allá de la velocidad máxima.

4. Cambie la velocidad del adaptador:

   ```
   network fcp adapter modify -node node1 -adapter 0c -speed 16
   ```

5. Conectar el adaptador:

   ```
   network fcp adapter modify -node node1 -adapter 0c -state up
   ```

6. Conectar todas las LIF del adaptador:

   ```
   network interface modify -vserver * -lif * { -home-node node1 -home-port 0c }
   -status-admin up
   ```

Puertos FC compatibles

El número de puertos FC integrados y puertos CNA/UTA2 configurados para FC varía según el modelo de la controladora. Los puertos FC también están disponibles mediante adaptadores de expansión de destino FC admitidos o tarjetas UTA2 adicionales configuradas con adaptadores FC SFP+.

Puertos FC, UTA y UTA2 integrados

- Los puertos integrados se pueden configurar de forma individual como puertos FC de destino o de iniciador.
- El número de puertos FC integrados varía según el modelo de la controladora.

  La "Hardware Universe de NetApp" Contiene una lista completa de puertos FC integrados en cada modelo de controladora.

- Los sistemas FAS2520 no son compatibles con FC.

Puertos FC de adaptador de ampliación de destino

- Los adaptadores de expansión de destino disponibles difieren según el modelo de la controladora.

  La "Hardware Universe de NetApp" contiene una lista completa de los adaptadores de expansión de destino para cada modelo de controladora.

- Los puertos de algunos adaptadores de ampliación de FC se configuran como iniciadores o destinos de fábrica y no se pueden cambiar.

  Los demás se pueden configurar de forma individual como puertos FC de destino o de iniciador, al igual que los puertos FC incorporados. Hay una lista completa disponible en "Hardware Universe de NetApp".

Evite la pérdida de conectividad cuando utilice el adaptador X1133A-R6

Puede evitar la pérdida de conectividad durante un error en el puerto configurando el sistema con rutas redundantes en HBA X1133A-R6 independientes.

El HBA X1133A-R6 es un adaptador FC de 4 puertos y 16 GB que consta de dos pares de dos puertos. El adaptador X1133A-R6 se puede configurar como modo de destino o modo de iniciador. Cada par de 2 puertos se admite con un único ASIC (por ejemplo, el puerto 1 y el puerto 2 en ASIC 1 y el puerto 3 y el puerto 4 en ASIC 2). Ambos puertos en un único ASIC deben configurarse para funcionar en el mismo modo, tanto en modo objetivo como en modo iniciador. Si se produce un error con el ASIC que admite un par, ambos puertos del par se desconectan.

Para evitar esta pérdida de conectividad, puede configurar el sistema con rutas redundantes para separar los HBA X1133A-R6, o con rutas redundantes a los puertos compatibles con diferentes ASIC en el HBA.

Gestione los adaptadores X1143A-R6

Información general sobre las configuraciones de puertos admitidas para los adaptadores X1143A-R6

De manera predeterminada, el adaptador X1143A-R6 se configura en el modo objetivo FC, pero puede configurar sus puertos como puertos Ethernet y FCoE de 10 GB (CNA) o como puertos de destino o iniciador FC de 16 GB. Esto requiere distintos adaptadores de SFP+.

Cuando se configura para Ethernet y FCoE, los adaptadores X1143A-R6 admiten el tráfico de destino NIC y FCoE simultáneo en el mismo puerto de 10 GBE. Cuando se configura para FC, cada par de dos puertos que comparte el mismo ASIC se puede configurar individualmente para modo iniciador FC o destino FC. Esto significa que un solo adaptador X1143A-R6 puede admitir el modo objetivo FC en un par de dos puertos y el modo iniciador de FC en otro par de dos puertos. Los pares de puertos conectados al mismo ASIC deben configurarse en el mismo modo.

En el modo FC, el adaptador X1143A-R6 se comporta como cualquier dispositivo FC existente con velocidades de hasta 16 Gbps. En el modo CNA, se puede utilizar el adaptador X1143A-R6 para el tráfico NIC y FCoE simultáneo que comparta el mismo puerto 10 GbE. El modo CNA solo admite el modo de destino FC para la función FCoE.

Configure los puertos

Para configurar el adaptador de objetivo unificado (X1143A-R6), debe configurar los dos puertos adyacentes en el mismo chip en el mismo modo Personality.

Pasos

1. Configure los puertos según sea necesario para Fibre Channel (FC) o el adaptador de red convergente (CNA) mediante el `system node hardware unified-connect modify` comando.
2. Conecte los cables adecuados para FC o Ethernet de 10 GB.
3. Compruebe que tiene instalado el SFP+ correcto:

   ```
   network fcp adapter show -instance -node -adapter
   ```

   Para CNA, se debe usar un SFP Ethernet de 10 GB. Para FC, se debe usar un SFP de 8 GB o un SFP de 16 GB, a partir de la estructura de FC al que se está conectando.

Cambie el puerto UTA2 del modo CNA al modo FC

Debe cambiar el puerto UTA2 del modo adaptador de red convergente (CNA) al modo Fibre Channel (FC) para admitir el iniciador de FC y el modo de destino de FC. Debe cambiar la personalidad del modo CNA al modo FC cuando necesite cambiar el medio físico que conecta el puerto a su red.

Pasos

1. Desconectar el adaptador:

   ```
   network fcp adapter modify -node node_name -adapter adapter_name -status-admin
   down
   ```

2. Cambie el modo de puerto:

   ```
   ucadmin modify -node node_name -adapter adapter_name -mode fcp
   ```

3. Reinicie el nodo y a continuación, active el adaptador:

   ```
   network fcp adapter modify -node node_name -adapter adapter_name -status-admin
   up
   ```

4. Notifique a su administrador o VIF Manager que elimine o quite el puerto, según corresponda:
   - Si el puerto se utiliza como puerto de inicio de una LIF, es miembro de un grupo de interfaces (ifgrp) o una VLAN de host, un administrador debe hacer lo siguiente:
     i. Mueva las LIF, quite el puerto del ifgrp o elimine las VLAN respectivamente.
     ii. Elimine manualmente el puerto ejecutando el `network port delete` comando.

     Si la `network port delete` error del comando, el administrador debe solucionar los errores y volver a ejecutar el comando.
   - Si el puerto no se usa como puerto de inicio de una LIF, no es miembro de un ifgrp y no aloja VLAN, el gestor VIF debería eliminar el puerto de sus registros en el momento del reinicio.

Si el administrador VIF no quita el puerto, el administrador debe quitarlo manualmente después del reinicio usando la `network port delete` comando.

```
net-f8040-34::> network port show

    Node: net-f8040-34-01
                                                          Speed(Mbps) Health
    Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
    --------- ------------ ---------------- ---- ---- -----------
--------
    ...
    e0i       Default      Default          down 1500  auto/10    -
    e0f       Default      Default          down 1500  auto/10    -
    ...

    net-f8040-34::> ucadmin show
                           Current  Current    Pending  Pending    Admin
    Node          Adapter  Mode     Type       Mode     Type
Status
    ------------  -------  -------  ---------  -------  ---------
-----------
    net-f8040-34-01
                  0e       cna      target     -        -
offline
    net-f8040-34-01
                  0f       cna      target     -        -
offline
    ...

    net-f8040-34::> network interface create -vs net-f8040-34 -lif m
-role
node-mgmt-home-node net-f8040-34-01 -home-port e0e -address 10.1.1.1
-netmask 255.255.255.0


    net-f8040-34::> network interface show -fields home-port, curr-port

    vserver lif                   home-port curr-port
    ------- --------------------- --------- ---------
    Cluster net-f8040-34-01_clus1 e0a       e0a
    Cluster net-f8040-34-01_clus2 e0b       e0b
    Cluster net-f8040-34-01_clus3 e0c       e0c
    Cluster net-f8040-34-01_clus4 e0d       e0d
    net-f8040-34
            cluster_mgmt          e0M       e0M
    net-f8040-34
```

```
            m                    e0e       e0i
    net-f8040-34
            net-f8040-34-01_mgmt1 e0M       e0M
    7 entries were displayed.

    net-f8040-34::> ucadmin modify local 0e fc

    Warning: Mode on adapter 0e and also adapter 0f will be changed to
fc.
    Do you want to continue? {y|n}: y
    Any changes will take effect after rebooting the system. Use the
"system node reboot" command to reboot.

    net-f8040-34::> reboot local
      (system node reboot)

    Warning: Are you sure you want to reboot node "net-f8040-34-01"?
    {y|n}: y
```

5. Compruebe que tiene instalado el SFP+ correcto:

   `network fcp adapter show -instance -node -adapter`

   Para CNA, se debe usar un SFP Ethernet de 10 GB. Para FC, se debe usar un SFP de 8 GB o un SFP de 16 GB antes de cambiar la configuración en el nodo.

Cambie los módulos ópticos del adaptador de destino CNA/UTA2

Debe cambiar los módulos ópticos del adaptador de destino unificado (CNA/UTA2) para admitir el modo de personalidad seleccionado para el adaptador.

Pasos

1. Verifique el SFP+ actual utilizado en la tarjeta. A continuación, reemplace el SFP+ actual por el SFP+ adecuado para la personalidad preferida (FC o CNA).
2. Retire los módulos ópticos actuales del adaptador X1143A-R6.
3. Inserte los módulos correctos para la óptica del modo de personalidad preferido (FC o CNA).
4. Compruebe que tiene instalado el SFP+ correcto:

   `network fcp adapter show -instance -node -adapter`

   Los módulos SFP+ compatibles y los cables de cobre de Marca Cisco (Twinax) se enumeran en la "Hardware Universe de NetApp".

Ver la configuración de adaptador

Para ver la configuración del adaptador de destino unificado (X1143A-R6), debe ejecutar el `system hardware unified-connect show` comando para mostrar todos los

módulos de la controladora.

Pasos

1. Arranque la controladora sin los cables conectados.
2. Ejecute el `system hardware unified-connect show` comando para ver la configuración del puerto y los módulos.
3. Consulte la información del puerto antes de configurar el CNA y los puertos.

Configuraciones de FCoE

Formas de configurar la información general sobre FCoE

FCoE puede configurarse de diversas formas mediante switches FCoE. FCoE no admite las configuraciones de conexión directa.

Todas las configuraciones de FCoE tienen estructura doble, son completamente redundantes y requieren un software multivía en el lado del host. En todas las configuraciones de FCoE, puede tener varios switches FCoE y FC en la ruta entre el iniciador y el destino, hasta el límite máximo de saltos. Para conectar los switches entre sí, deben ejecutar una versión de firmware que admita ISL de Ethernet. Cada host de cualquier configuración de FCoE se puede configurar con un sistema operativo diferente.

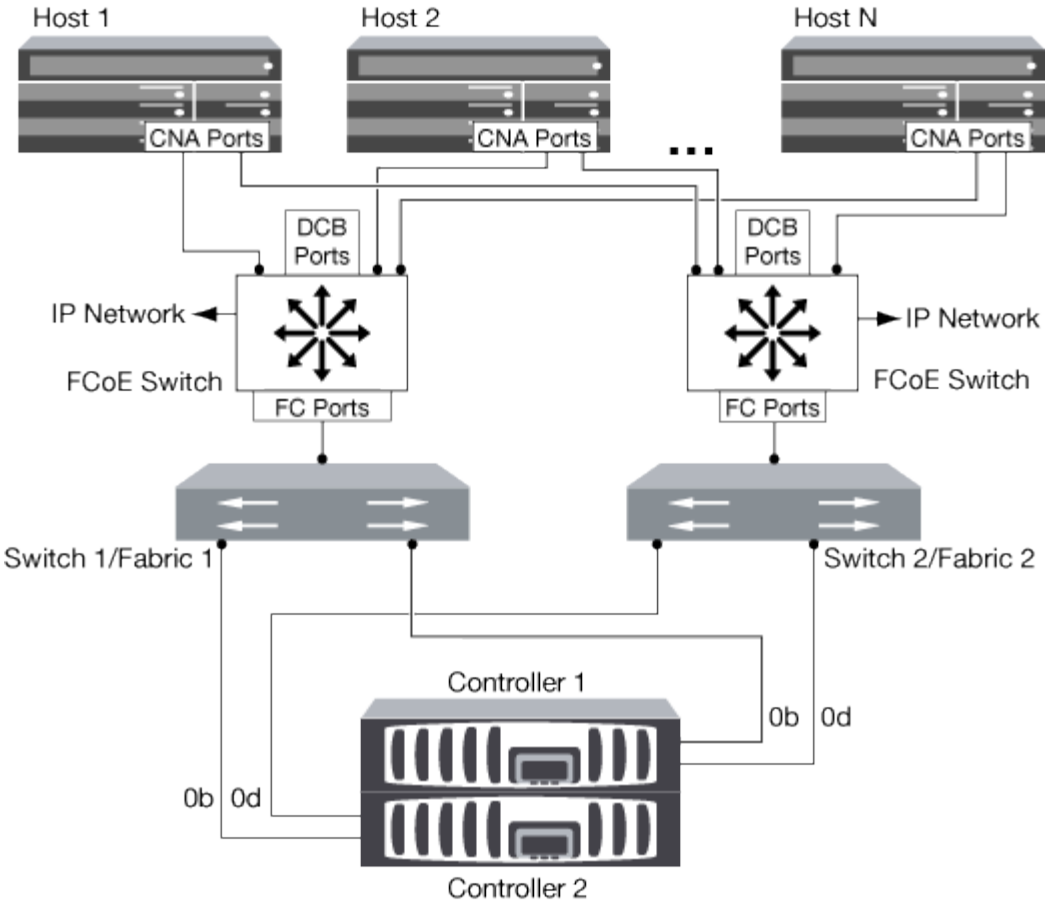
Las configuraciones de FCoE requieren switches Ethernet que admitan explícitamente las funciones de FCoE. Las configuraciones de FCoE se validan mediante el mismo proceso de interoperabilidad y garantía de calidad que los switches FC. Las configuraciones admitidas se muestran en la matriz de interoperabilidad. Algunos de los parámetros incluidos en estas configuraciones admitidas son el modelo de switch, el número de switches que puede ponerse en marcha en una sola estructura y la versión de firmware del switch compatible.

Los números de puertos del adaptador de ampliación de destino FC en las ilustraciones son ejemplos. Los números de puerto reales pueden variar, según las ranuras de expansión en las que se hayan instalado los adaptadores de expansión de destino FCoE.

Iniciador FCoE a destino FC

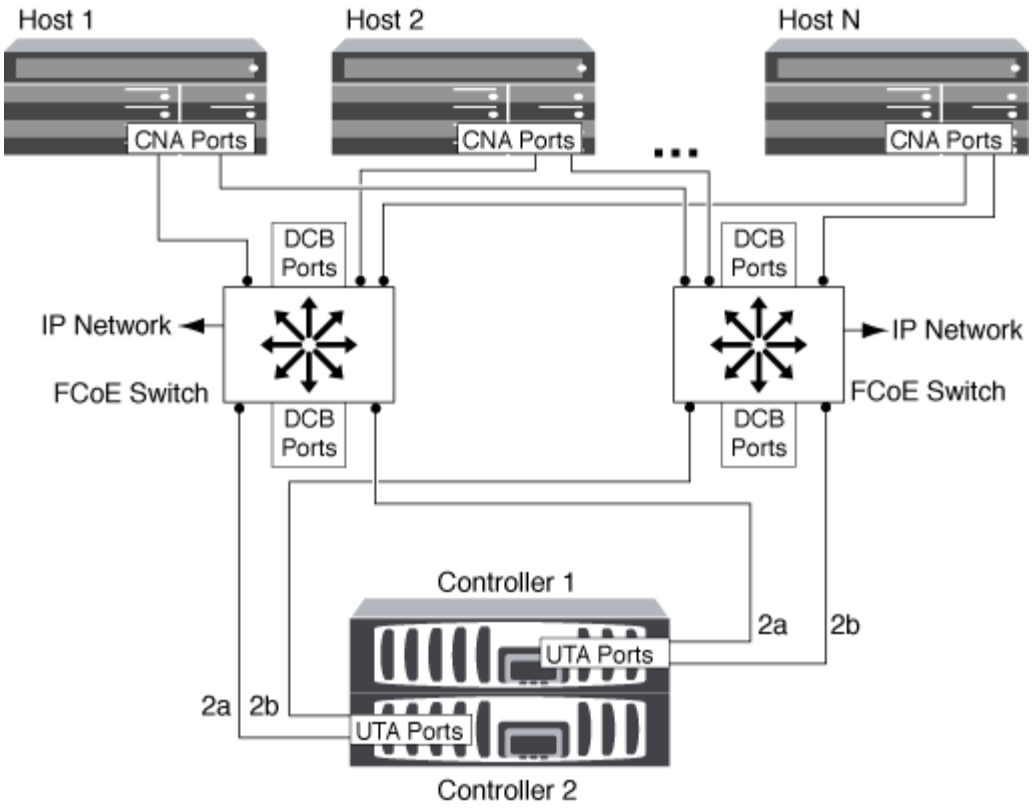
Con iniciadores FCoE (CNA) puede conectar hosts a ambas controladoras en un par de alta disponibilidad mediante switches FCoE a puertos de destino FC. El switch FCoE debe tener también puertos FC. El iniciador FCoE del host siempre se conecta al switch FCoE. El switch FCoE puede conectarse directamente al destino FC o conectarse al destino FC a través de switches FC.

En la siguiente ilustración, se muestran las CNA del host conectadas a un switch FCoE y luego a un switch de FC antes de conectarse al par de alta disponibilidad:



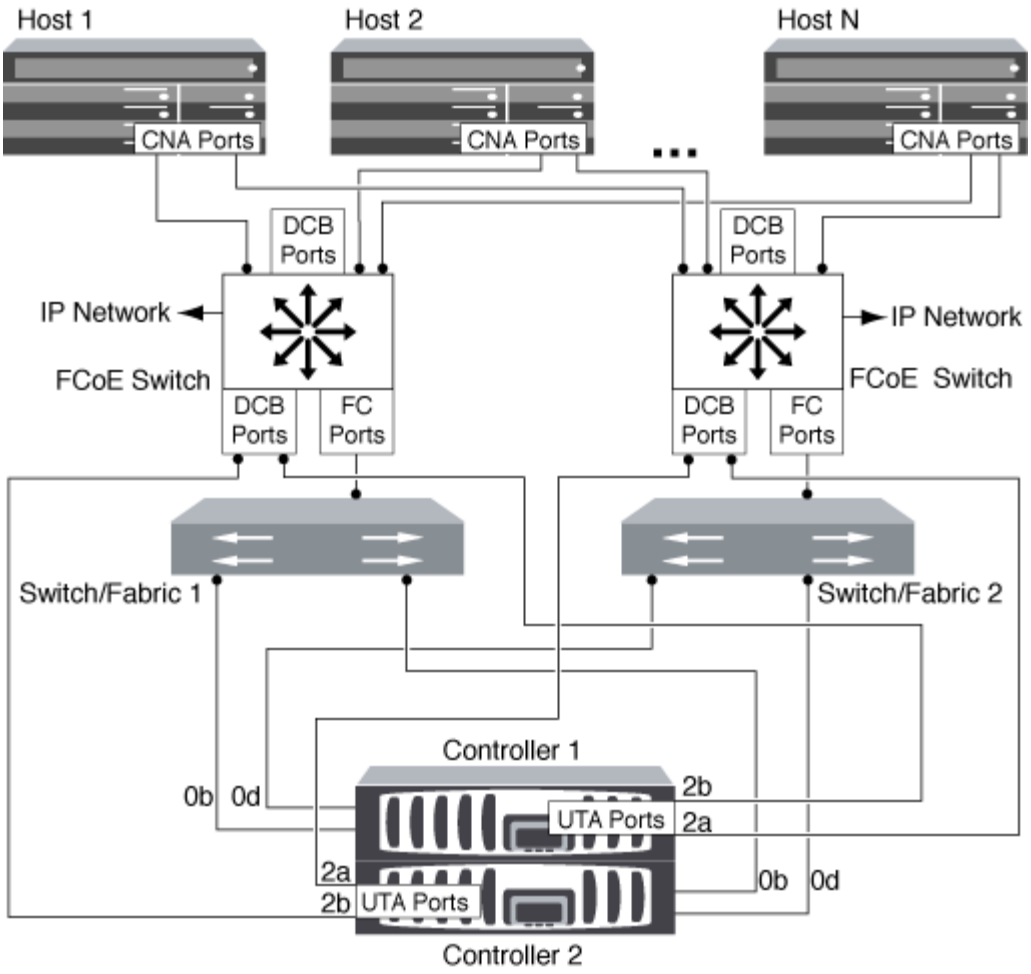
Iniciador de FCoE a destino de FCoE

Con los iniciadores FCoE del host (CNA) es posible conectar los hosts a ambas controladoras en una pareja de alta disponibilidad a los puertos de destino FCoE (también denominados UTA o 2 s) a través de los switches FCoE.



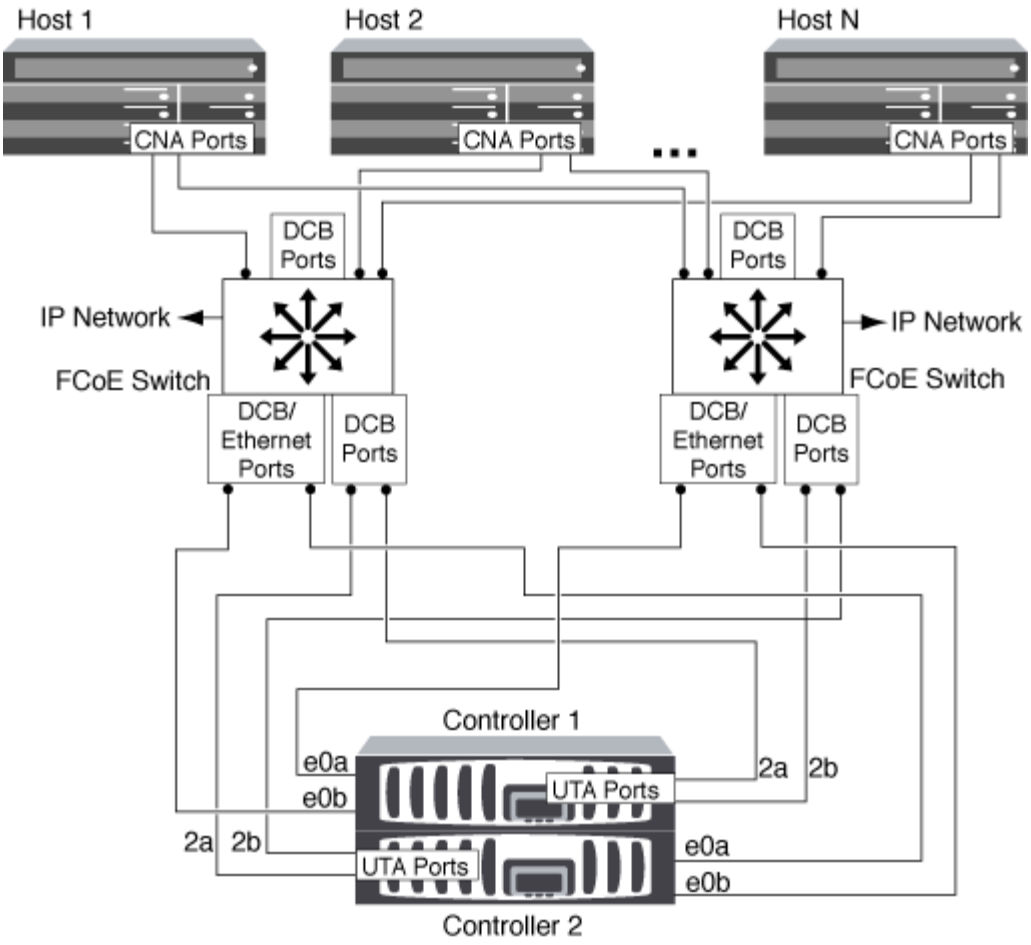
Iniciador FCoE para destinos de FCoE y FC

Con los iniciadores FCoE del host (CNA) es posible conectar los hosts a ambas controladoras en un par de alta disponibilidad a los puertos de destino FCoE y FC (también denominados UTA o UTA 2) a través de los switches FCoE.



Combinación de FCoE y los protocolos de almacenamiento IP

Con los iniciadores FCoE del host (CNA) es posible conectar los hosts a ambas controladoras en una pareja de alta disponibilidad a los puertos de destino FCoE (también denominados UTA o 2 s) a través de los switches FCoE. Los puertos FCoE no pueden usar la agregación tradicional de enlaces a un único switch. Los switches de Cisco admiten un tipo especial de agregación de enlaces (Virtual Port Channel) que admite FCoE. Un canal de puerto virtual agrega vínculos individuales a dos switches. También puede utilizar Canales de puerto virtual para otro tráfico Ethernet. Los puertos que se utilizan para el tráfico aparte de FCoE, como NFS, SMB, iSCSI y otro tráfico Ethernet, pueden utilizar puertos Ethernet habituales en los switches FCoE.



Combinaciones de iniciadores y objetivos de FCoE

Se admiten ciertas combinaciones de iniciadores y destinos FC tradicionales y FCoE.

Iniciadores FCoE

Es posible utilizar iniciadores de FCoE en equipos host con destinos FCoE y FC tradicionales en controladoras de almacenamiento. El iniciador FCoE del host debe conectarse a un switch FCoE DCB (Data Center Bridging); no se admite la conexión directa a un destino.

En la siguiente tabla se enumeran las combinaciones compatibles:

Iniciador	Destino	Compatible?
FC	FC	Sí
FC	FCoE	Sí
FCoE	FC	Sí
FCoE	FCoE	Sí

Destinos FCoE

Puede combinar puertos de destino FCoE con puertos FC de 4 GB, 8 GB o 16 GB en la controladora de almacenamiento, independientemente de si los puertos FC son adaptadores de destino adicionales o puertos integrados. Puede tener adaptadores de destino FCoE y FC en la misma controladora de almacenamiento.

> Aún se aplican las reglas para combinar los puertos FC internos y de ampliación.

Número de saltos admitidos por FCoE

El número máximo de saltos de Fibre Channel over Ethernet (FCoE) admitidos entre un host y el sistema de almacenamiento depende del proveedor de switches y de la compatibilidad del sistema de almacenamiento para las configuraciones FCoE.

Los saltos son el número de switches presentes en la ruta que va del iniciador (host) al destino (sistema de almacenamiento). La documentación de Cisco Systems también se refiere a este valor como el *diameter de LA estructura SAN*.

Para FCoE, puede tener switches FCoE conectados a switches FC.

Para las conexiones FCoE integrales, los switches FCoE deben ejecutar una versión de firmware que admita enlaces entre switches Ethernet (ISL).

En la siguiente tabla, se enumeran los números máximos de saltos admitidos:

Cambiar proveedor	Número de saltos admitidos
Brocade	7 para FC 5 para FCoE
Cisco	7 Hasta 3 switches pueden ser switches FCoE.

División en zonas de Fibre Channel y FCoE

Información general sobre la división en zonas de Fibre Channel y FCoE

Una zona FC, FC-NVMe o FCoE es una agrupación lógica de uno o varios puertos dentro de una estructura. Para que los dispositivos puedan verse entre sí, conectarse, crear sesiones entre sí y comunicarse, ambos puertos necesitan tener una pertenencia a una zona común. Se recomienda la división en zonas de un solo iniciador.

Motivos para dividir en zonas

- La división en zonas reduce o elimina la *comunicación entre zonas* entre los HBA del iniciador.

  Esto ocurre incluso en entornos pequeños y es uno de los mejores argumentos para implementar la zonificación. Los subconjuntos lógicos de la estructura creados por la división en zonas eliminan los problemas de la comunicación por zonas.

- La división en zonas reduce el número de rutas disponibles a un puerto FC, FC-NVMe o FCoE en particular y reduce el número de rutas entre un host y una LUN en particular que se puede ver.

  Por ejemplo, algunas soluciones multivía del SO del host tienen limitado el número de rutas que pueden gestionar. La división en zonas puede reducir el número de zonas que ve un controlador multivía de SO. Si un host no tiene una solución multivía instalada, debe verificar que solo pueda verse una ruta a un LUN mediante la división en zonas en la estructura o una combinación de asignación de LUN selectiva (SLM) y conjuntos de puertos en la SVM.

- La división en zonas aumenta la seguridad al limitar el acceso y la conectividad a los puntos finales que comparten una zona común.

  Los puertos que no tienen zonas en común no se pueden comunicar entre sí.

- La división en zonas mejora la fiabilidad DE SAN aislando los problemas que se producen y contribuye a reducir el tiempo de resolución de problemas limitando el espacio disponible.

Recomendaciones para la división en zonas

- Debe implementar la división en zonas en cualquier momento, si cuatro o más hosts están conectados a UNA SAN, o si SLM no se implementa en los nodos de una SAN.
- Aunque es posible aplicar la división en zonas de nombre de nodo WWNN con algunos proveedores de switch, se requiere la división en zonas de nombres de puerto WWPN para definir correctamente un puerto específico y utilizar NPIV con eficacia.
- Debe limitar el tamaño de la zona mientras mantiene la capacidad de gestión.

  Es posible superponer varias zonas para limitar el tamaño. Idealmente se debería definir una zona para cada host o cada clúster de hosts.

- Debe utilizar la división en zonas de un único iniciador para eliminar la comunicación entre zonas de los HBA del iniciador.

División en zonas basada en World Wide Name

La división en zonas basada en nombre WWN especifica el nombre WWN de los miembros que se incluirán en la zona. Al dividir en zonas en ONTAP, debe usar la división en zonas de nombre de puerto WWPN.

La división en zonas de nombres de puerto WWPN aporta flexibilidad porque el acceso no está determinado por el lugar físico de conexión entre el dispositivo y la estructura. Puede mover un cable de un puerto a otro sin tener que configurar las zonas de nuevo.

Para las rutas Fibre Channel a controladoras de almacenamiento que ejecutan ONTAP, asegúrese de que sus switches se dividen mediante los WWPN de las interfaces lógicas (LIF) objetivo, no los WWPN de los puertos físicos en el nodo. Para obtener más información acerca de las LIF, consulte la *Guía de gestión de redes ONTAP*.

"Gestión de redes"

Zonas individuales

En la configuración recomendada de la división por zonas, hay un iniciador de host por zona. La zona consta de un puerto de iniciador de host y uno o varios LIF de destino en

los nodos de almacenamiento que proporcionan acceso a las LUN hasta el número deseado de rutas por destino. Esto significa que los hosts que acceden a los mismos nodos no pueden ver los puertos del otro, pero cada iniciador puede acceder a cualquier nodo.

Debería añadir todas las LIF de la máquina virtual de almacenamiento (SVM) a la zona con el iniciador del host. Esto le permite mover volúmenes o LUN sin editar sus zonas existentes ni crear zonas nuevas.

Para las rutas Fibre Channel a los nodos que ejecutan ONTAP, asegúrese de que sus switches se dividen mediante los WWPN de las interfaces lógicas (LIF) objetivo, no los WWPN de los puertos físicos en el nodo. Los WWPN de los puertos físicos comienzan por «'50» y los WWPN de las LIF empiezan por «'20».

División en zonas de estructura única

En una configuración de estructura única, puede seguir conectando cada iniciador de host a cada nodo de almacenamiento. Se requiere un software multivía en el host para administrar varias rutas. Cada host debería tener dos iniciadores para que la multivía ofrezca resiliencia en la solución.

Cada iniciador debería tener como mínimo un LIF desde cada nodo a el que pueda acceder el iniciador. La división en zonas debe permitir al menos una ruta desde el iniciador de host al par de nodos del clúster para proporcionar una ruta para la conectividad de LUN. Esto significa que cada iniciador del host podría tener solo un LIF de destino por nodo en su configuración de zonas. Si hay algún requisito para la multivía en el mismo nodo o en varios nodos del clúster, cada nodo tendrá varias LIF por nodo en su configuración de zona. Esto permite que el host siga teniendo acceso a sus LUN si un nodo falla o se mueve un volumen que contiene la LUN a un nodo diferente. Esto también requiere que los nodos de generación de informes se establezcan correctamente.

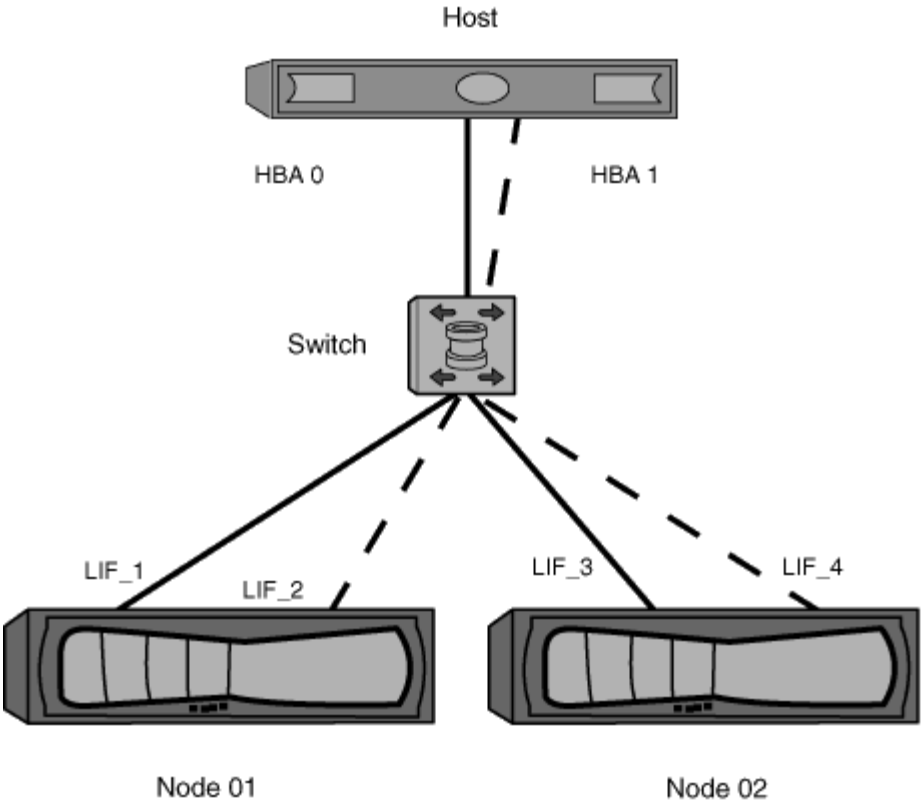
Se admiten las configuraciones de estructura única, pero no se consideran de alta disponibilidad. El error de un componente único puede provocar la pérdida del acceso a los datos.

En la figura siguiente, el host tiene dos iniciadores y está ejecutando un software multivía. Hay dos zonas:

> La convención de nomenclatura utilizada en esta figura es solo una recomendación de una posible convención de nomenclatura que puede usar para su solución de ONTAP.

- Zona 1: HBA 0, LIF_1 y LIF_3
- Zona 2: HBA 1, LIF_2 y LIF_4

Si la configuración incluía más nodos, las LIF de los nodos adicionales se incluirían en estas zonas.



En este ejemplo también puede tener las cuatro LIF en cada zona. En ese caso, las zonas serían las siguientes:

- Zona 1: HBA 0, LIF_1, LIF_2, LIF_3 y LIF_4
- Zona 2: HBA 1, LIF_1, LIF_2, LIF_3 y LIF_4

> El sistema operativo host y el software multivía deben ser compatibles con el número de rutas compatibles que se están utilizando para acceder a las LUN de los nodos. Para determinar el número de rutas utilizadas para acceder a las LUN de los nodos, consulte la sección límites de configuración DE SAN.

Información relacionada

"Hardware Universe de NetApp"

División en zonas de pares de alta disponibilidad de estructura doble

En configuraciones de estructura doble, puede conectar cada iniciador de host a cada nodo del clúster. Cada iniciador de host utiliza un switch diferente para acceder a los nodos del clúster. Se requiere un software multivía en el host para administrar varias rutas.

Las configuraciones de estructura doble se consideran de alta disponibilidad porque se mantiene el acceso a los datos en caso de que falle un único componente.

En la figura siguiente, el host tiene dos iniciadores y está ejecutando un software multivía. Hay dos zonas. SLM se configura de modo que todos los nodos se consideran nodos de generación de informes.

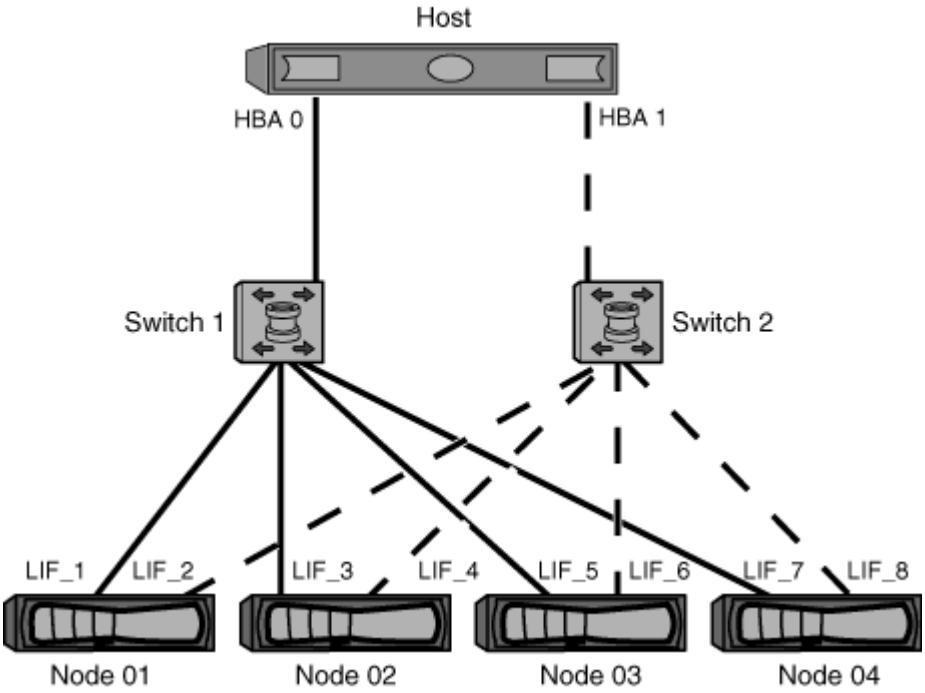
La convención de nomenclatura utilizada en esta figura es solo una recomendación de una posible convención de nomenclatura que puede usar para su solución de ONTAP.

- Zona 1: HBA 0, LIF_1, LIF_3, LIF_5 y LIF_7
- Zona 2: HBA 1, LIF_2, LIF_4, LIF_6 y LIF_8

Cada iniciador de host se zonas mediante un switch diferente. Se accede a la zona 1 a través del conmutador 1. Se accede a la zona 2 a través del conmutador 2.

Cada iniciador puede acceder a una LIF en todos los nodos. Esto permite que el host siga teniendo acceso a sus LUN si un nodo da error. Los SVM tienen acceso a todos los LIF iSCSI y FC de todos los nodos de una solución en clúster según el ajuste de asignación de LUN selectiva (SLM) y la configuración del nodo de generación de informes. Puede utilizar la división en zonas de SLM, conjuntos de puertos o switch de FC para reducir el número de rutas de una SVM al host y el número de rutas de una SVM a un LUN.

Si la configuración incluía más nodos, las LIF de los nodos adicionales se incluirían en estas zonas.



El sistema operativo host y el software multivía tienen que admitir el número de rutas que se están utilizando para acceder a las LUN en los nodos.

Información relacionada

"Hardware Universe de NetApp"

Restricciones de división en zonas para switches Cisco FC y FCoE

Cuando se usan switches Fibre Channel y FCoE de Cisco, una única zona estructural no debe contener más de un LIF de destino para el mismo puerto físico. Si hay varias LIF en el mismo puerto en la misma zona, es posible que los puertos LIF no puedan recuperarse de una pérdida de conexión.

Los switches FC normales se utilizan para el protocolo FC-NVMe exactamente del mismo modo que se

utilizan para el protocolo FC.

- Varios LIF para los protocolos FC y FCoE, pueden compartir puertos físicos en un nodo siempre y cuando se encuentren en zonas diferentes.
- FC-NVMe y FCoE no pueden compartir el mismo puerto físico.
- FC y FC-NVMe pueden compartir el mismo puerto físico de 32 GB.
- Los switches FC y FCoE de Cisco requieren que cada LIF de un puerto dado esté en una zona separada de los otros LIF de ese puerto.
- Una sola zona puede tener tanto LIF FC como FCoE. Una zona puede contener un LIF de todos los puertos de destino del clúster, pero tenga cuidado de no superar los límites de ruta del host y verificar la configuración de SLM.
- Los LIF de diferentes puertos físicos pueden estar en la misma zona.
- Los switches de Cisco requieren que se separen las LIF.

  Aunque no es necesario, se recomienda separar las LIF para todos los switches

Requisitos para configuraciones SAN compartidas

Las configuraciones DE SAN compartidas se definen como hosts conectados tanto a los sistemas de almacenamiento de ONTAP como a los de otros proveedores. Siempre que se cumplan varios requisitos, se admitirá el acceso a sistemas de almacenamiento de ONTAP y sistemas de almacenamiento de otros proveedores desde un único host.

Para todos los sistemas operativos host, se recomienda usar adaptadores independientes para conectarse a los sistemas de almacenamiento de cada proveedor. El uso de adaptadores independientes reduce las posibilidades de que existan conflictos entre controladores y configuraciones. En el caso de las conexiones con un sistema de almacenamiento ONTAP, el modelo de adaptador, la BIOS, el firmware y el controlador deben aparecer como compatibles con la herramienta de matriz de interoperabilidad de NetApp.

Debe configurar los valores de tiempo de espera necesarios o recomendados y otros parámetros de almacenamiento para el host. Debe instalar siempre el software de NetApp o aplicar en último lugar los ajustes de NetApp.

- Para AIX, debe aplicar los valores de la versión de AIX Host Utilities que se enumeran en la herramienta de matriz de interoperabilidad para la configuración.
- En el caso de ESX, debe aplicar la configuración del host mediante Virtual Storage Console para VMware vSphere.
- Para HP-UX, debe usar la configuración de almacenamiento predeterminada de HP-UX.
- Para Linux, debe aplicar los valores de la versión de Linux Host Utilities que se enumeran en la herramienta de matriz de interoperabilidad para la configuración.
- Para Solaris, debe aplicar los valores de la versión de Solaris Host Utilities que se enumeran en la herramienta de matriz de interoperabilidad para su configuración.
- Para Windows, debe instalar la versión de Windows Host Utilities que se muestra en la herramienta de matriz de interoperabilidad para la configuración.

Información relacionada

"Herramienta de matriz de interoperabilidad de NetApp"

Configuraciones SAN en un entorno MetroCluster

Configuraciones SAN en un entorno MetroCluster

Debe tener en cuenta determinados aspectos que se deben tener en cuenta al utilizar configuraciones DE SAN en un entorno de MetroCluster.

- Las configuraciones de MetroCluster no son compatibles con las configuraciones VSAN «enrutadas» de estructura FC de interfaz.
- A partir de ONTAP 9.12.1, las configuraciones IP de MetroCluster de cuatro nodos son compatibles con NVMe/FC. Las configuraciones de MetroCluster no son compatibles con NVMe/TCP. Las configuraciones de MetroCluster no son compatibles con NVMe antes de ONTAP 9.12.1.
- La configuración de MetroCluster admite otros protocolos SAN, como iSCSI, FC y FCoE.
- Al usar las configuraciones del cliente SAN, debe comprobar si se incluye alguna consideraciones especiales para las configuraciones de MetroCluster en las notas que se proporcionan en la "Herramienta de matriz de interoperabilidad de NetApp" (IMT).
- Los sistemas operativos y las aplicaciones deben proporcionar una resiliencia de I/o de 120 segundos para admitir la conmutación por cierre automática no planificada de MetroCluster y la conmutación de sitios iniciada por tiebreaker o de Mediator.
- MetroCluster utiliza los mismos WWPN en ambos lados de LA SAN front-end.

Información relacionada

- "Comprender la protección de datos y la recuperación ante desastres de MetroCluster"
- "Artículo de la base de conocimientos: ¿Cuáles son las consideraciones de compatibilidad del host AIX en una configuración de MetroCluster?"
- "Artículo de la base de conocimientos: Consideraciones de compatibilidad del host Solaris en una configuración de MetroCluster"

Evite la superposición de puertos entre la conmutación de sitios y la conmutación de estado

En un entorno SAN, puede configurar los switches de interfaz para evitar la superposición cuando el puerto antiguo se desconecta y el nuevo puerto se conecta.

Durante la conmutación de sitios, el puerto FC del sitio superviviente podría iniciar sesión en la estructura antes de que la estructura haya detectado que el puerto FC del sitio de desastre está sin conexión y ha eliminado este puerto de los servicios de nombre y directorio.

Si el puerto FC del desastre aún no se ha eliminado, el intento de inicio de sesión estructural del puerto FC del sitio superviviente podría ser rechazado debido a un WWPN duplicado. Este comportamiento de los switches FC puede cambiarse para respetar el inicio de sesión del dispositivo anterior y no el existente. Debe comprobar los efectos de este comportamiento en otros dispositivos de estructura. Póngase en contacto con el proveedor de switches para obtener más información.

Elija el procedimiento correcto según el tipo de interruptor.

Ejemplo 9. Pasos

Switch Cisco

1. Conéctese al switch e inicie sesión.
2. Entrar al modo de configuración:

```
switch# config t
switch(config)#
```

3. Sobrescribir la primera entrada del dispositivo en la base de datos del servidor de nombres con el nuevo dispositivo:

```
switch(config)# no fcns reject-duplicate-pwwn vsan 1
```

4. En los switches que ejecutan NX-OS 8.x, confirme que el tiempo de espera de inactividad de flogi está configurado en cero:

   a. Visualizar la temporeral de inactividad:

   ```
   switch(config)# show flogi interval info \| i quiesce
   ```

   ```
   Stats:  fs flogi quiesce timerval:  0
   ```

   b. Si la salida en el paso anterior no indica que el tiempo es cero, entonces configúrelo en cero:

   ```
   switch(config)# flogi scale enable
   ```

```
switch(config)$ flogi quiesce timeout 0
```

Switch Brocade

1. Conéctese al switch e inicie sesión.
2. Introduzca el `switchDisable` comando.
3. Introduzca el `configure` y pulse `y` en el prompt de.

```
 F-Port login parameters (yes, y, no, n): [no] y
```

4. Seleccione el ajuste 1:

```
- 0: First login take precedence over the second login (default)
- 1: Second login overrides first login.
- 2: the port type determines the behavior
Enforce FLOGI/FDISC login: (0..2) [0] 1
```

5. Responda a las preguntas restantes o pulse **Ctrl + D**.
6. Introduzca el `switchEnable` comando.

Información relacionada

"Realizar la conmutación de sitios para pruebas o mantenimiento"

Compatibilidad con host para accesos múltiples

Compatibilidad con host para información general sobre multivía

ONTAP siempre utiliza ALUA (Asymmetric Logical Unit Access) para las rutas FC e iSCSI. Asegúrese de utilizar configuraciones host que sean compatibles con ALUA para los protocolos FC e iSCSI.

A partir de la conmutación por error/retorno de una pareja de ha multivía de ONTAP 9.5, se admite la configuración de NVMe mediante Asynchronous Namespace Access (ANA). En ONTAP 9.4, NVMe solo admite una ruta desde el host al destino. El host de aplicación debe gestionar la conmutación por error en la ruta a su partner de alta disponibilidad (ha).

Para obtener información sobre qué configuraciones de host específicas admiten ALUA o ANA, consulte "Herramienta de matriz de interoperabilidad de NetApp" y.. "Configuración de host SAN ONTAP" para el sistema operativo del host.

Cuando se requiere un software multivía para el host

Si hay más de una ruta desde las interfaces lógicas (LIF) de la máquina virtual de almacenamiento hasta la estructura, se requiere un software multivía. Se requiere un software multivía en el host siempre que el host pueda acceder a una LUN a través de más de una ruta.

El software multivía presenta un disco único al sistema operativo para todas las rutas que se dirigen a una LUN. Sin un software multivía, el sistema operativo trataría cada una de las partes como un disco independiente, lo cual provocaría daños en los datos.

Se considera que su solución tiene varias rutas si dispone de alguna de las siguientes opciones:

- Un único puerto iniciador del host conectando varios LIF SAN en la SVM
- Varios puertos de iniciador conectando a un único LIF SAN en la SVM
- Varios puertos de iniciador conectando varios LIF SAN en la SVM

Se recomienda el software multivía en configuraciones de alta disponibilidad. Además de la asignación selectiva de LUN, se recomienda usar la división en zonas o los conjuntos de puertos de switch FC para limitar las rutas utilizadas para acceder a las LUN.

El software multivía también se conoce como software MPIO (I/o multivía).

Número recomendado de rutas desde el host a los nodos en el clúster

No debe exceder de ocho rutas desde el host a cada nodo del clúster, prestando atención al número total de rutas compatibles con el sistema operativo del host y la

multivía utilizada en el host.

Debe tener un mínimo de dos rutas por LUN conectadas a cada nodo de generación de informes a través de la asignación de LUN selectiva (SLM) que utiliza la máquina virtual de almacenamiento (SVM) del clúster. De este modo, se eliminan los puntos únicos de error y el sistema puede sobrevivir a fallos de componentes.

Si tiene cuatro o más nodos en el clúster o más de cuatro puertos de destino que utilizan las SVM en cualquiera de los nodos, Puede usar los siguientes métodos para limitar el número de rutas que se pueden utilizar para acceder a las LUN de los nodos de modo que no supere el máximo recomendado de ocho rutas.

- SLM

  SLM reduce el número de rutas entre el host y la LUN solo a rutas del nodo que posee el LUN y el partner de alta disponibilidad del nodo propietario. SLM está habilitado de forma predeterminada.

- Conjuntos de puertos para iSCSI
- Asignaciones de igroup de FC desde el host
- División en zonas de switches FC

Información relacionada

"Administración de SAN"

Límites de configuración

Determinar el número de nodos compatibles para las configuraciones SAN

El número de nodos por clúster que admite ONTAP varía en función de la versión de ONTAP, los modelos de controladora de almacenamiento del clúster y el protocolo de los nodos del clúster.

Acerca de esta tarea

Si alguno de los nodos del clúster está configurado para FC, FC-NVMe, FCoE o iSCSI, ese clúster se limita a los límites de nodos SAN. Los límites de nodos basados en las controladoras de su clúster se enumeran en *Hardware Universe*.

Pasos

1. Vaya a. "Hardware Universe de NetApp".
2. Haga clic en **plataformas** en la parte superior izquierda (junto al botón **Inicio**) y seleccione el tipo de plataforma.
3. Seleccione la casilla de verificación junto a su versión de ONTAP.

   Se mostrará una nueva columna para que pueda elegir sus plataformas.

4. Active las casillas junto a las plataformas utilizadas en su solución.
5. Anule la selección de la casilla de verificación **Seleccionar todo** en la columna **Seleccionar las especificaciones**.
6. Active la casilla de verificación **nodos máximos por clúster (NAS/SAN)**.
7. Haga clic en **Mostrar resultados**.

Información relacionada

"Hardware Universe de NetApp"

Determinar el número de hosts compatibles por clúster en configuraciones FC y FC-NVMe

El número máximo de hosts SAN que se pueden conectar a un clúster varía en gran medida según su combinación específica de varios atributos de clúster, como el número de hosts conectados a cada nodo del clúster, iniciadores por host, sesiones por host y nodos en el clúster.

Acerca de esta tarea

Para las configuraciones de FC y FC-NVMe, debe usar el número de anexos de destino del iniciador (ITN) en el sistema para determinar si puede añadir más hosts al clúster.

Un ITN representa una ruta desde el iniciador del host hasta el destino del sistema de almacenamiento. El número máximo de ITN por nodo en las configuraciones de FC y FC-NVMe es 2,048. Siempre que esté por debajo del número máximo de ITN, puede continuar agregando hosts al clúster.

Para determinar el número de ITN utilizados en su clúster, realice los siguientes pasos para cada nodo del clúster.

Pasos

1. Identificar todas las LIF de un nodo determinado.
2. Ejecute el siguiente comando para cada LIF en el nodo:

   ```
   fcp initiator show -fields wwpn, lif
   ```

   El número de entradas que se muestran en la parte inferior del resultado del comando representa el número de ITN para esa LIF.

3. Registre el número de ITN que se muestran para cada LIF.
4. Añada el número de ITN para cada LIF de todos los nodos del clúster.

   Este total representa el número de ITN de su clúster.

Determinar el número admitido de hosts en configuraciones iSCSI

El número máximo de hosts SAN que se pueden conectar en configuraciones iSCSI varía en gran medida en función de su combinación específica de varios atributos de clúster, como el número de hosts conectados a cada nodo del clúster, iniciadores por host, inicios de sesión por host y nodos en el clúster.

Acerca de esta tarea

El número de hosts que se pueden conectar directamente a un nodo o que se pueden conectar mediante uno o más switches depende del número de puertos Ethernet disponibles. El número de puertos Ethernet disponibles está determinado por el modelo de la controladora y el número y tipo de adaptadores instalados en la controladora. El número de puertos Ethernet admitidos para controladoras y adaptadores está disponible en *Hardware Universe*.

Para todas las configuraciones de clústeres multinodo, debe determinar el número de sesiones iSCSI por nodo para saber si puede añadir más hosts al clúster. Siempre que el clúster se encuentre por debajo del número máximo de sesiones iSCSI por nodo, puede continuar añadiendo hosts al clúster. El número máximo

de sesiones iSCSI por nodo varía en función de los tipos de controladoras del clúster.

Pasos

1. Identificar todos los grupos de portal de destino en el nodo.
2. Compruebe el número de sesiones iSCSI para cada grupo de portales de destino del nodo:

   ```
   iscsi session show -tpgroup tpgroup
   ```

   El número de entradas que se muestra en la parte inferior del resultado del comando representa el número de sesiones iSCSI para ese grupo de portales de destino.

3. Registre el número de sesiones iSCSI que se muestran para cada grupo de portales de destino.
4. Agregue el número de sesiones iSCSI para cada grupo de portales de destino en el nodo.

   El total representa la cantidad de sesiones iSCSI en el nodo.

Límites de configuración de switch de FC

Los switches de Fibre Channel tienen límites máximos de configuración, incluyendo el número de inicios de sesión compatibles por puerto, grupo de puertos, blade y switch. Los proveedores de switch documentan sus propios límites.

Cada interfaz lógica de FC (LIF) se registra en un puerto del switch de FC. El número total de inicios de sesión desde un único destino en el nodo es igual al número de LIF más un inicio de sesión para el puerto físico subyacente. No supere los límites de configuración del proveedor del switch para inicios de sesión u otros valores de configuración. Esto también contiene true para los iniciadores que se utilizan en el lado del host en entornos virtualizados con NPIV habilitado. No supere los límites de configuración del proveedor del switch para inicios de sesión para el destino o los iniciadores que se están utilizando en la solución.

Límites del switch Brocade

Encontrará los límites de configuración de los switches Brocade en las *Brocade Scalability Guidelines*.

Límites de switches de Cisco Systems

Puede encontrar los límites de configuración para switches de Cisco en la "Límites de configuración de Cisco" Guía para su versión del software de switch de Cisco.

Visión general de profundidad de cola

Es posible que deba ajustar la profundidad de la cola FC en el host para obtener los valores máximos de ITN por nodo y de «fan-in» de puertos FC. El número máximo de LUN y el número de HBA que pueden conectarse a un puerto de FC están limitados por la profundidad de cola disponible en los puertos de destino FC.

Acerca de esta tarea

La profundidad de cola es el número de solicitudes de I/o (comandos SCSI) que se pueden poner en cola a la vez en una controladora de almacenamiento. Cada solicitud de I/o del HBA del iniciador del host al adaptador de destino de la controladora de almacenamiento consume una entrada de cola. Normalmente, una mayor profundidad de cola equivale a un mejor rendimiento. Sin embargo, si se alcanza la profundidad máxima de cola del controlador de almacenamiento, ese controlador de almacenamiento rechaza los comandos entrantes

devolviendo una respuesta QFULL a ellos. Si un gran número de hosts acceden a un controlador de almacenamiento, debe planificar cuidadosamente para evitar las condiciones de QFULL, lo que reduce significativamente el rendimiento del sistema y puede provocar errores en algunos sistemas.

En una configuración con varios iniciadores (hosts), todos los hosts deben tener profundidades de cola similares. Debido a la desigualdad en la profundidad de cola entre los hosts conectados a la controladora de almacenamiento a través del mismo puerto objetivo, los hosts con profundidades de cola más pequeñas se ven privados del acceso a los recursos por parte de hosts con profundidades de cola más grandes.

Se pueden hacer las siguientes recomendaciones generales sobre las profundidades de cola de '"tuning'":

- Para sistemas pequeños y medianos, use una profundidad de cola HBA de 32.
- Para sistemas grandes, utilice una profundidad de cola de HBA de 128.
- Para casos excepcionales o pruebas de rendimiento, utilice una profundidad de cola de 256 para evitar posibles problemas de cola.
- Todos los hosts deben tener las profundidades de cola establecidas en valores similares para proporcionar un acceso igual a todos los hosts.
- Para evitar pérdidas de rendimiento o errores, no se debe exceder la profundidad de cola de puertos FC de destino de la controladora de almacenamiento.

Pasos

1. Cuente el número total de iniciadores de FC de todos los hosts que se conectan a un puerto de destino de FC.
2. Multiplique por 128.
   - Si el resultado es inferior a 2,048, establezca la profundidad de cola de todos los iniciadores en 128. Hay 15 hosts con un iniciador conectado a cada uno de los dos puertos de destino de la controladora de almacenamiento. 15 × 128 = 1,920. Como 1,920 es menor que el límite total de profundidad de cola de 2,048, puede establecer la profundidad de cola de todos los iniciadores en 128.
   - Si el resultado es superior a 2,048, vaya al paso 3.
     Tiene 30 hosts con un iniciador conectado a cada uno de dos puertos de destino de la controladora de almacenamiento. 30 x 128 = 3.840. Dado que 3,840 es mayor que el límite total de profundidad de cola de 2,048, debe elegir una de las opciones del paso 3 para la corrección.
3. Seleccione una de las siguientes opciones para añadir más hosts a la controladora de almacenamiento.
   - Opción 1:
     i. Añada más puertos de destino FC.
     ii. Redistribuya los iniciadores de FC.
     iii. Repita los pasos 1 y 2.

     La profundidad de cola deseada de 3,840 excede la profundidad de cola disponible por puerto. Para solucionarlo, puede añadir un adaptador de destino FC de dos puertos a cada controladora y volver a dividir los switches de FC de modo que 15 de sus 30 hosts se conecten a un conjunto de puertos y los 15 hosts restantes se conecten a un segundo conjunto de puertos. La profundidad de cola por puerto se reduce a 15 × 128 = 1,920.
   - Opción 2:
     i. Designar a cada huésped como «grande» o «centro comercial» basándose en su necesidad prevista de I/O.
     ii. Multiplique el número de iniciadores grandes por 128.

iii. Multiplique el número de iniciadores pequeños por 32.

iv. Añada los dos resultados juntos.

v. Si el resultado es inferior a 2,048, establezca la profundidad de cola de los hosts grandes en 128 y la profundidad de cola de los hosts pequeños en 32.

vi. Si el resultado es aún mayor que 2,048 por puerto, reduzca la profundidad de cola por iniciador hasta que la profundidad total de la cola sea inferior o igual a 2,048.

> Para estimar la profundidad de cola necesaria para obtener un determinado rendimiento de I/o por segundo, utilice esta fórmula:
>
> Profundidad de cola necesaria = (número de operaciones de I/o por segundo) × (tiempo de respuesta)
>
> Por ejemplo, si necesita 40,000 E/S por segundo con un tiempo de respuesta de 3 milisegundos, la profundidad de cola necesaria = 40,000 × (.003) = 120.

El número máximo de hosts que se pueden conectar a un puerto de destino es 64 si decide limitar la profundidad de cola a la recomendación básica de 32. Sin embargo, si decide tener una profundidad de cola de 128, puede haber un máximo de 16 hosts conectados a un puerto de destino. Cuanto mayor sea la profundidad de la cola, menos hosts serán compatibles con un único puerto de destino. Si su requisito es tal que no pueda comprometer la profundidad de cola, debería obtener más puertos de destino.

La profundidad de cola deseada de 3,840 excede la profundidad de cola disponible por puerto. Cuenta con 10 hosts «grandes» que tienen unas necesidades elevadas de I/o de almacenamiento y 20 hosts «de centros comerciales» con necesidades bajas de I/O. Configure la profundidad de la cola del iniciador en los hosts grandes en 128 y la profundidad de la cola del iniciador en los hosts pequeños en 32.

La profundidad total de la cola resultante es de (10 × 128) + (20 × 32) = 1,920.

Puede distribuir la profundidad de cola disponible de forma equitativa entre cada iniciador.

La profundidad de cola resultante por iniciador es de 2,048 ÷ 30 = 68.

Establecer profundidades de cola en hosts SAN

Es posible que deba cambiar las profundidades de cola del host para alcanzar los valores máximos de ITN por nodo y de fan-in de puertos FC.

Hosts AIX

Puede cambiar la profundidad de cola en los hosts AIX mediante el `chdev` comando. Cambios realizados mediante `chdev` el comando persiste durante todos los reinicios.

Ejemplos:

- Para cambiar la profundidad de cola del dispositivo hdisk7, utilice el siguiente comando:

  ```
  chdev -l hdisk7 -a queue_depth=32
  ```

- Para cambiar la profundidad de cola del HBA fcs0, utilice el siguiente comando:

  ```
  chdev -l fcs0 -a num_cmd_elems=128
  ```

El valor predeterminado para `num_cmd_elems` es 200. El valor máximo es 2.048.

> Es posible que sea necesario desconectar el HBA para cambiar `num_cmd_elems` a continuación, vuelva a conectarlo en línea mediante el `rmdev -l fcs0 -R` y.. `makdev -l fcs0 -P` comandos.

Hosts HP-UX

Puede cambiar la profundidad de la cola de dispositivos o LUN en hosts HP-UX mediante el parámetro kernel `scsi_max_qdepth`. Puede cambiar la profundidad de la cola del HBA mediante el parámetro kernel `max_fcp_reqs`.

- El valor predeterminado para `scsi_max_qdepth` es 8. El valor máximo es 255.

  `scsi_max_qdepth` puede cambiarse dinámicamente en un sistema en ejecución mediante el `-u` en la `kmtune` comando. El cambio será efectivo para todos los dispositivos del sistema. Por ejemplo, utilice el siguiente comando para aumentar la profundidad de la cola de LUN a 64:

  ```
  kmtune -u -s scsi_max_qdepth=64
  ```

  Es posible cambiar la profundidad de la cola para archivos de dispositivo individuales mediante `scsictl` comando. Cambios mediante `scsictl` el comando no persiste entre reinicios del sistema. Para ver y cambiar la profundidad de cola de un archivo de dispositivo concreto, ejecute el siguiente comando:

  ```
  scsictl -a /dev/rdsk/c2t2d0
  ```

  ```
  scsictl -m queue_depth=16 /dev/rdsk/c2t2d0
  ```

- El valor predeterminado para `max_fcp_reqs` es 512. El valor máximo es 1024.

  El kernel debe ser reconstruido y el sistema debe ser reiniciado para los cambios a. `max_fcp_reqs` para que surta efecto. Para cambiar la profundidad de cola del HBA a 256, por ejemplo, utilice el siguiente comando:

  ```
  kmtune -u -s max_fcp_reqs=256
  ```

Hosts Solaris

Puede establecer la profundidad de cola LUN y HBA para los hosts Solaris.

- Para profundidad de cola de LUN: El número de LUN en uso en un host multiplicado por el acelerador de por LUN (profundidad de cola de lun) debe ser menor o igual que el valor de profundidad de cola del GT en el host.
- Para profundidad de cola en una pila Sun: Los controladores nativos no permiten por LUN o por destino `max_throttle` Ajustes en el nivel del HBA. El método recomendado para establecer el `max_throttle` El valor de los controladores nativos se encuentra en el nivel VID_PID (por tipo de dispositivo) de la `/kernel/drv/sd.conf` y.. `/kernel/drv/ssd.conf` archivos. La utilidad de host establece este valor en 64 para configuraciones de MPxIO y 8 para configuraciones de Veritas DMP.

Pasos

1. `# cd/kernel/drv`

2. `# vi lpfc.conf`
3. Busque `/tft-queue (/tgt-queue)`

   ```
   tgt-queue-depth=32
   ```

   El valor predeterminado se establece en 32 durante la instalación.

4. Establezca el valor deseado en función de la configuración de su entorno.
5. Guarde el archivo.
6. Reinicie el host con el `sync; sync; sync; reboot -- -r` comando.

Hosts VMware para un HBA QLogic

Utilice la `esxcfg-module` Comando para cambiar la configuración de tiempo de espera de HBA. Actualizar manualmente la `esx.conf` no se recomienda el archivo.

Pasos

1. Inicie sesión en la consola de servicio como usuario raíz.
2. Utilice la `#vmkload_mod -l` Comando para verificar qué módulo Qlogic HBA está cargado actualmente.
3. Para una instancia única de un HBA Qlogic, ejecute el siguiente comando:

   ```
   #esxcfg-module -s ql2xmaxqdepth=64 qla2300_707
   ```

   En este ejemplo se utiliza el módulo qla2300_707. Utilice el módulo adecuado basado en la salida de `vmkload_mod -l`.

4. Guarde los cambios con el siguiente comando:

   ```
   #/usr/sbin/esxcfg-boot -b
   ```

5. Reinicie el servidor con el siguiente comando:

   ```
   #reboot
   ```

6. Confirme los cambios con los siguientes comandos:
   a. `#esxcfg-module -g qla2300_707`
   b. `qla2300_707 enabled = 1 options = 'ql2xmaxqdepth=64'`

VMware host para un HBA Emulex

Utilice la `esxcfg-module` Comando para cambiar la configuración de tiempo de espera de HBA. Actualizar manualmente la `esx.conf` no se recomienda el archivo.

Pasos

1. Inicie sesión en la consola de servicio como usuario raíz.
2. Utilice la `#vmkload_mod -l grep lpfc` Comando para verificar qué HBA de Emulex está cargado actualmente.

3. Para una única instancia de un HBA de Emulex, introduzca el siguiente comando:

   ```
   #esxcfg-module -s lpfc0_lun_queue_depth=16 lpfcdd_7xx
   ```

   > Dependiendo del modelo de HBA, el módulo puede ser lpfcdd_7xx o lpfcdd_732. El comando anterior utiliza el módulo lpfcdd_7xx. Debe utilizar el módulo adecuado en función del resultado de `vmkload_mod -l`.

   Si se ejecuta este comando, la profundidad de la cola de LUN es 16 para el HBA que representa lpfc0.

4. Para varias instancias de un HBA Emulex, ejecute el siguiente comando:

   ```
   a esxcfg-module -s "lpfc0_lun_queue_depth=16 lpfc1_lun_queue_depth=16"
   lpfcdd_7xx
   ```

   La profundidad de cola de LUN para lpfc0 y la profundidad de cola de LUN para lpfc1 está establecida en 16.

5. Introduzca el siguiente comando:

   ```
   #esxcfg-boot -b
   ```

6. Reinicie mediante `#reboot`.

Host Windows para un HBA Emulex

En hosts Windows, puede utilizar el `LPUTILNT` Utilidad para actualizar la profundidad de cola para los HBA de Emulex.

Pasos

1. Ejecute el `LPUTILNT` utilidad ubicada en `C:\WINNT\system32` directorio.
2. Seleccione **parámetros de accionamiento** en el menú de la derecha.
3. Desplácese hacia abajo y haga doble clic en **QueueDepth**.

   > Si está configurando **QueueDepth** superior a 150, también es necesario aumentar adecuadamente el siguiente valor del Registro de Windows:
   >
   > `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\lpxnds\Parameters\Device\NumberOfRequests`

Hosts Windows para un HBA Qlogic

En hosts Windows, puede utilizar el `SANsurfer` Utilidad HBA Manager para actualizar las profundidades de cola para HBA Qlogic.

Pasos

1. Ejecute el `SANsurfer` Utilidad del gestor de HBA.
2. Haga clic en **Puerto HBA** > **Ajustes**.
3. Haga clic en **Configuración avanzada del puerto HBA** en el cuadro de lista.

4. Actualice el `Execution Throttle` parámetro.

Hosts Linux para HBA Emulex

Puede actualizar las profundidades de cola de un HBA Emulex en un host Linux. Para que las actualizaciones sean persistentes entre reinicios, debe crear una nueva imagen de disco RAM y reiniciar el host.

Pasos

1. Identificar los parámetros de profundidad de cola que se van a modificar:

   ```
   modinfo lpfc|grep queue_depth
   ```

   Se muestra la lista de parámetros de profundidad de cola con su descripción. Dependiendo de la versión del sistema operativo, puede modificar uno o más de los siguientes parámetros de profundidad de cola:

   - `lpfc_lun_queue_depth`: Número máximo de comandos FC que se pueden poner en cola para una LUN específica (uint)
   - `lpfc_hba_queue_depth`: Número máximo de comandos FC que se pueden poner en cola en un HBA lpfc (uint)
   - `lpfc_tgt_queue_depth`: Número máximo de comandos FC que se pueden poner en cola en un puerto de destino específico (uint)

     La `lpfc_tgt_queue_depth` El parámetro sólo se aplica a sistemas Red Hat Enterprise Linux 7.x, sistemas SUSE Linux Enterprise Server 11 SP4 y sistemas 12.x.

2. Actualice las profundidades de cola agregando los parámetros de profundidad de cola al `/etc/modprobe.conf` Archivo para un sistema Red Hat Enterprise Linux 5.x y para `/etc/modprobe.d/scsi.conf` Archivo para un sistema Red Hat Enterprise Linux 6.x o 7.x, o SUSE Linux Enterprise Server 11.x o 12.x.

   Según la versión del sistema operativo, puede agregar uno o varios de los siguientes comandos:

   - `options lpfc lpfc_hba_queue_depth=new_queue_depth`
   - `options lpfc lpfc_lun_queue_depth=new_queue_depth`
   - `options lpfc_tgt_queue_depth=new_queue_depth`

3. Cree una nueva imagen de disco RAM y, a continuación, reinicie el host para que las actualizaciones persistan entre reinicios.

   Para obtener más información, consulte "Administración del sistema" Para su versión del sistema operativo Linux.

4. Compruebe que los valores de profundidad de cola se han actualizado para cada parámetro de profundidad de cola que haya modificado:

   ```
   root@localhost ~]#cat /sys/class/scsi_host/host5/lpfc_lun_queue_depth
         30
   ```

   Se muestra el valor actual de la profundidad de cola.

Hosts Linux para HBA QLogic

Puede actualizar la profundidad de la cola de dispositivos de un controlador QLogic en un host Linux. Para que las actualizaciones sean persistentes entre reinicios, debe crear una nueva imagen de disco RAM y reiniciar el host. Puede usar la GUI de gestión de HBA de QLogic o la interfaz de línea de comandos (CLI) para modificar la profundidad de la cola de HBA de QLogic.

Esta tarea muestra cómo utilizar la interfaz de línea de comandos del HBA QLogic para modificar la profundidad de la cola del HBA QLogic

Pasos

1. Identifique el parámetro de profundidad de cola del dispositivo que se va a modificar:

   ```
   modinfo qla2xxx | grep ql2xmaxqdepth
   ```

   Solo puede modificar la `ql2xmaxqdepth` Parámetro de profundidad de cola, que indica la profundidad máxima de cola que se puede establecer para cada LUN. El valor predeterminado es 64 para RHEL 7.5 y versiones posteriores. El valor predeterminado es 32 para RHEL 7.4 y anteriores.

   ```
   root@localhost ~]# modinfo qla2xxx|grep ql2xmaxqdepth
   parm:       ql2xmaxqdepth:Maximum queue depth to set for each LUN.
   Default is 64. (int)
   ```

2. Actualice el valor de profundidad de la cola del dispositivo:

   - Si desea que las modificaciones sean persistentes, realice los siguientes pasos:

     i. Actualice las profundidades de cola agregando el parámetro de profundidad de cola al `/etc/modprobe.conf` Archivo para un sistema Red Hat Enterprise Linux 5.x y para `/etc/modprobe.d/scsi.conf` Archivo para un sistema Red Hat Enterprise Linux 6.x o 7.x, o SUSE Linux Enterprise Server 11.x o 12.x: `options qla2xxx ql2xmaxqdepth=new_queue_depth`

     ii. Cree una nueva imagen de disco RAM y, a continuación, reinicie el host para que las actualizaciones persistan entre reinicios.

     Para obtener más información, consulte "Administración del sistema" Para su versión del sistema operativo Linux.

   - Si solo desea modificar el parámetro para la sesión actual, ejecute el siguiente comando:

     ```
     echo new_queue_depth > /sys/module/qla2xxx/parameters/ql2xmaxqdepth
     ```

     En el siguiente ejemplo, la profundidad de cola se establece en 128.

   ```
   echo 128 > /sys/module/qla2xxx/parameters/ql2xmaxqdepth
   ```

3. Compruebe que se actualizan los valores de profundidad de cola:

   ```
   cat /sys/module/qla2xxx/parameters/ql2xmaxqdepth
   ```

   Se muestra el valor actual de la profundidad de cola.

4. Modifique la profundidad de la cola del HBA QLogic actualizando el parámetro firmware `Execution Throttle` Desde el BIOS del HBA QLogic.

   a. Inicie sesión en la CLI de gestión de los HBA de QLogic:

      ```
      /opt/QLogic_Corporation/QConvergeConsoleCLI/qaucli
      ```

   b. En el menú principal, seleccione `Adapter Configuration` opción.

      ```
      [root@localhost ~]#
      /opt/QLogic_Corporation/QConvergeConsoleCLI/qaucli
      Using config file:
      /opt/QLogic_Corporation/QConvergeConsoleCLI/qaucli.cfg
      Installation directory: /opt/QLogic_Corporation/QConvergeConsoleCLI
      Working dir: /root

      QConvergeConsole

              CLI - Version 2.2.0 (Build 15)

          Main Menu

          1:  Adapter Information
          **2:  Adapter Configuration**
          3:  Adapter Updates
          4:  Adapter Diagnostics
          5:  Monitoring
          6:  FabricCache CLI
          7:  Refresh
          8:  Help
          9:  Exit


              Please Enter Selection: 2
      ```

   c. En la lista de parámetros de configuración del adaptador, seleccione `HBA Parameters` opción.

```
1:  Adapter Alias
    2:  Adapter Port Alias
    **3:  HBA Parameters**
    4:  Persistent Names (udev)
    5:  Boot Devices Configuration
    6:  Virtual Ports (NPIV)
    7:  Target Link Speed (iiDMA)
    8:  Export (Save) Configuration
    9:  Generate Reports
   10:  Personality
   11:  FEC
(p or 0: Previous Menu; m or 98: Main Menu; ex or 99: Quit)
        Please Enter Selection: 3
```

d. Seleccione el puerto HBA necesario de la lista de puertos HBA.

```
Fibre Channel Adapter Configuration

    HBA Model QLE2562 SN: BFD1524C78510
      1: Port   1: WWPN: 21-00-00-24-FF-8D-98-E0 Online
      2: Port   2: WWPN: 21-00-00-24-FF-8D-98-E1 Online
    HBA Model QLE2672 SN: RFE1241G81915
      3: Port   1: WWPN: 21-00-00-0E-1E-09-B7-62 Online
      4: Port   2: WWPN: 21-00-00-0E-1E-09-B7-63 Online


        (p or 0: Previous Menu; m or 98: Main Menu; ex or 99: Quit)
        Please Enter Selection: 1
```

Se muestran los detalles del puerto del HBA.

e. En el menú HBA Parameters, seleccione la `Display HBA Parameters` para ver el valor actual de `Execution Throttle` opción.

El valor predeterminado de `Execution Throttle` la opción es 65535.

```
HBA Parameters Menu

=========================================================
HBA            : 2 Port: 1
SN             : BFD1524C78510
HBA Model      : QLE2562
HBA Desc.      : QLE2562 PCI Express to 8Gb FC Dual Channel
FW Version     : 8.01.02
```

```
WWPN          : 21-00-00-24-FF-8D-98-E0
WWNN          : 20-00-00-24-FF-8D-98-E0
Link          : Online
=========================================================

    1:  Display HBA Parameters
    2:  Configure HBA Parameters
    3:  Restore Defaults


        (p or 0: Previous Menu; m or 98: Main Menu; x or 99: Quit)
        Please Enter Selection: 1
---------------------------------------------------------------------------
--------
HBA Instance 2: QLE2562 Port 1 WWPN 21-00-00-24-FF-8D-98-E0 PortID 03-
07-00
Link: Online
---------------------------------------------------------------------------
--------
Connection Options             : 2 - Loop Preferred, Otherwise Point-to-
Point
Data Rate                      : Auto
Frame Size                     : 2048
Hard Loop ID                   : 0
Loop Reset Delay (seconds)     : 5
Enable Host HBA BIOS           : Enabled
Enable Hard Loop ID            : Disabled
Enable FC Tape Support         : Enabled
Operation Mode                 : 0 - Interrupt for every I/O completion
Interrupt Delay Timer (100us)  : 0
**Execution Throttle             : 65535**
Login Retry Count              : 8
Port Down Retry Count          : 30
Enable LIP Full Login          : Enabled
Link Down Timeout (seconds)    : 30
Enable Target Reset            : Enabled
LUNs Per Target                : 128
Out Of Order Frame Assembly    : Disabled
Enable LR Ext. Credits         : Disabled
Enable Fabric Assigned WWN     : N/A

Press <Enter> to continue:
```

a. Pulse **Intro** para continuar.

b. En el menú HBA Parameters, seleccione la `Configure HBA Parameters` Opción para modificar los parámetros del HBA.

c. En el menú Configurar parámetros, seleccione `Execute Throttle` y actualice el valor de este parámetro.

```
Configure Parameters Menu

=======================================================
HBA           : 2 Port: 1
SN            : BFD1524C78510
HBA Model     : QLE2562
HBA Desc.     : QLE2562 PCI Express to 8Gb FC Dual Channel
FW Version    : 8.01.02
WWPN          : 21-00-00-24-FF-8D-98-E0
WWNN          : 20-00-00-24-FF-8D-98-E0
Link          : Online
=======================================================

    1:  Connection Options
    2:  Data Rate
    3:  Frame Size
    4:  Enable HBA Hard Loop ID
    5:  Hard Loop ID
    6:  Loop Reset Delay (seconds)
    7:  Enable BIOS
    8:  Enable Fibre Channel Tape Support
    9:  Operation Mode
   10:  Interrupt Delay Timer (100 microseconds)
   11:  Execution Throttle
   12:  Login Retry Count
   13:  Port Down Retry Count
   14:  Enable LIP Full Login
   15:  Link Down Timeout (seconds)
   16:  Enable Target Reset
   17:  LUNs per Target
   18:  Enable Receive Out Of Order Frame
   19:  Enable LR Ext. Credits
   20:  Commit Changes
   21:  Abort Changes


        (p or 0: Previous Menu; m or 98: Main Menu; x or 99: Quit)
        Please Enter Selection: 11
Enter Execution Throttle [1-65535] [65535]: 65500
```

d. Pulse **Intro** para continuar.

e. En el menú Configurar parámetros, seleccione `Commit Changes` opción para guardar los cambios.

f. Salga del menú.