Conceptos de SAN

ONTAP 9

NetApp
April 20, 2024

This PDF was generated from https://docs.netapp.com/es-es/ontap/san-admin/san-host-provisioning-concept.html on April 20, 2024. Always check docs.netapp.com for the latest.

Tabla de contenidos

Conceptos de SAN . . . 1
Aprovisionamiento SAN con iSCSI . . . 1
Gestión de servicios iSCSI . . . 2
Aprovisionamiento DE SAN con FC . . . 8
Aprovisionamiento DE SAN con NVMe . . . 9
Volúmenes SAN . . . 10
Gestión del espacio del host DE SAN . . . 16
Acerca de iGroups . . . 17
Especifique WWPN de iniciador y los nombres de nodo iSCSI para un igroup . . . 18
Virtualización del almacenamiento con la copia de datos descargados de VMware y Microsoft . . . 18

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.

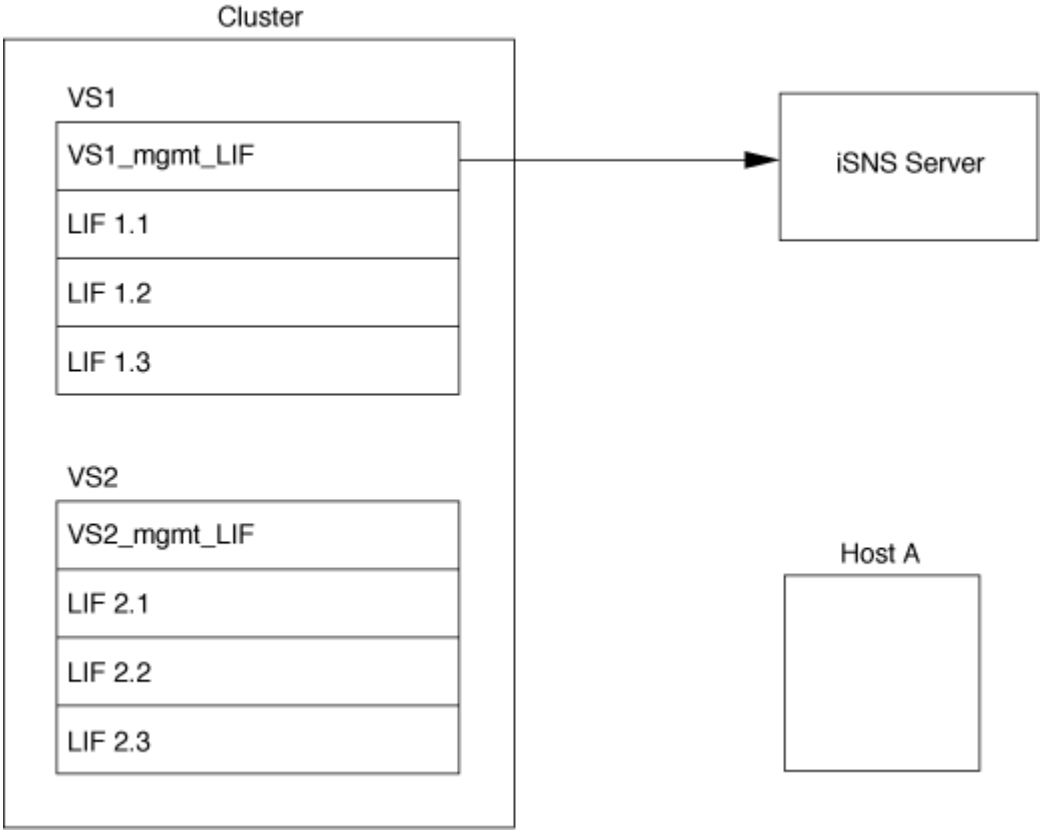
El protocolo iSNS permite la detección y gestión automatizadas de dispositivos iSCSI en una red de almacenamiento IP. Un iniciador de iSCSI puede consultar el servidor iSNS para detectar dispositivos de destino iSCSI.

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

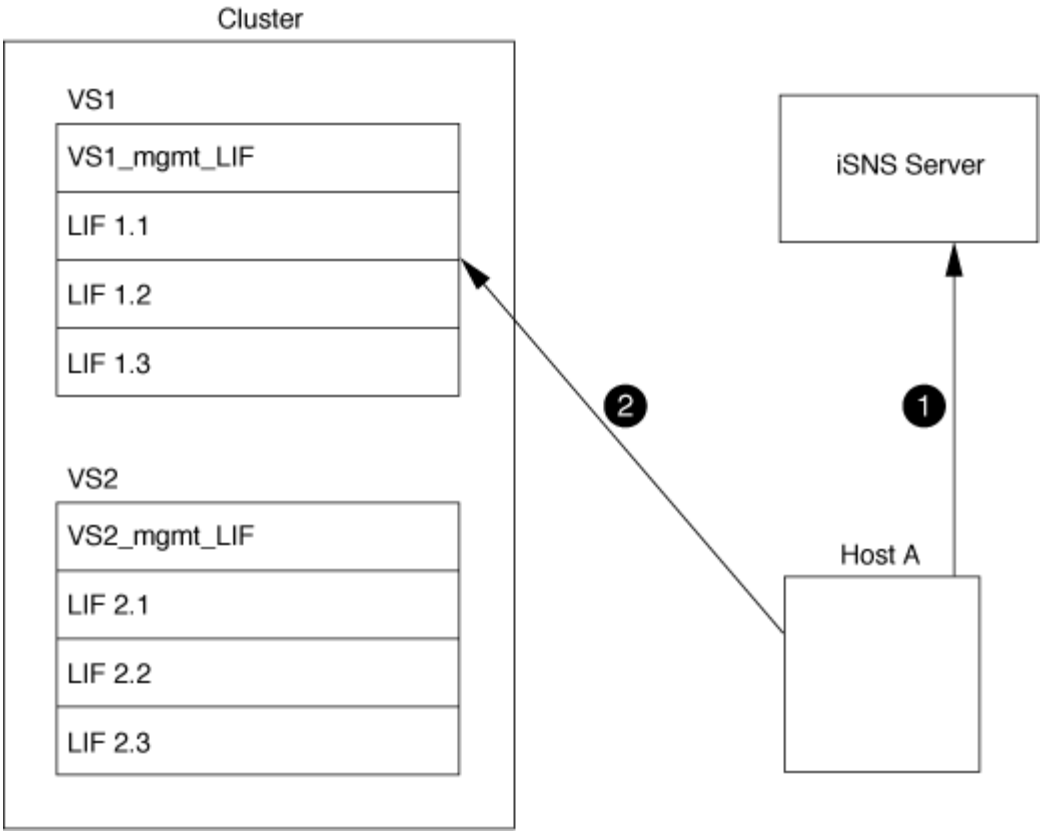
Cómo interactúan las SVM con un servidor iSNS

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.

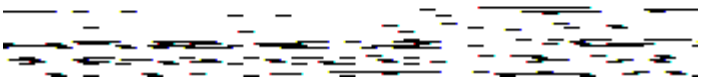
Puede parecer que los nombres internacionales no son secuenciales cuando se asignan por los siguientes motivos:

- 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`

Hosts con WWPN de HBA, IQN o EUIs	grupos de iniciadores	WWPN, IQN, EUIs añadidos a iGroups	LUN asignadas a iGroups
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.

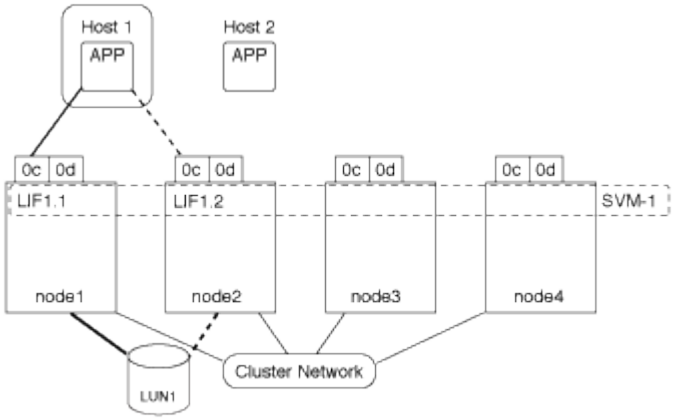
Cómo funciona el acceso de LUN en un entorno virtualizado

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.

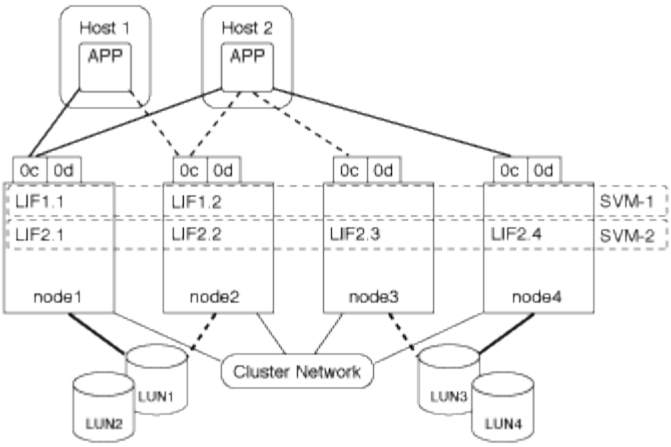
Ejemplo de acceso de LUN con una única SVM en un clúster

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.



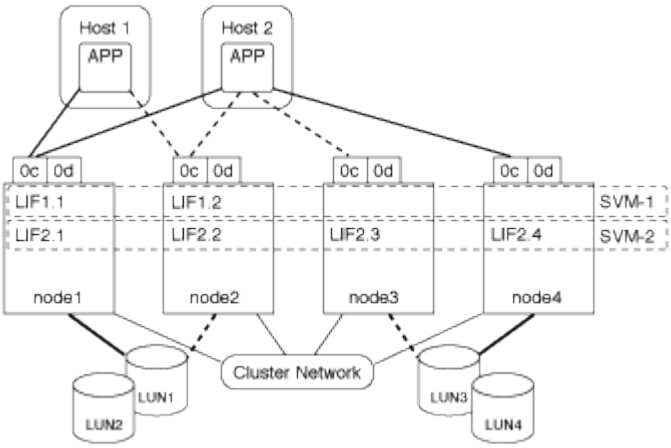
Ejemplo de acceso de la LUN con varias SVM en un clúster

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.



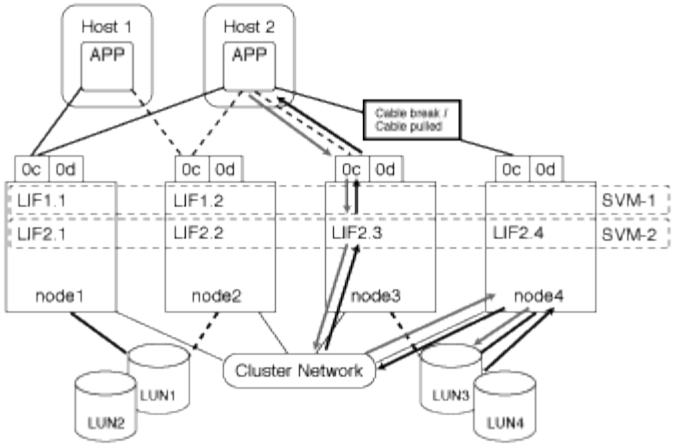
Ejemplo de una ruta activa o optimizada a una LUN desde un sistema host

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.

Información de copyright

Copyright © 2024 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

El software derivado del material de NetApp con copyright está sujeto a la siguiente licencia y exención de responsabilidad:

ESTE SOFTWARE LO PROPORCIONA NETAPP «TAL CUAL» Y SIN NINGUNA GARANTÍA EXPRESA O IMPLÍCITA, INCLUYENDO, SIN LIMITAR, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN CONCRETO, CUYA RESPONSABILIDAD QUEDA EXIMIDA POR EL PRESENTE DOCUMENTO. EN NINGÚN CASO NETAPP SERÁ RESPONSABLE DE NINGÚN DAÑO DIRECTO, INDIRECTO, ESPECIAL, EJEMPLAR O RESULTANTE (INCLUYENDO, ENTRE OTROS, LA OBTENCIÓN DE BIENES O SERVICIOS SUSTITUTIVOS, PÉRDIDA DE USO, DE DATOS O DE BENEFICIOS, O INTERRUPCIÓN DE LA ACTIVIDAD EMPRESARIAL) CUALQUIERA SEA EL MODO EN EL QUE SE PRODUJERON Y LA TEORÍA DE RESPONSABILIDAD QUE SE APLIQUE, YA SEA EN CONTRATO, RESPONSABILIDAD OBJETIVA O AGRAVIO (INCLUIDA LA NEGLIGENCIA U OTRO TIPO), QUE SURJAN DE ALGÚN MODO DEL USO DE ESTE SOFTWARE, INCLUSO SI HUBIEREN SIDO ADVERTIDOS DE LA POSIBILIDAD DE TALES DAÑOS.

NetApp se reserva el derecho de modificar cualquiera de los productos aquí descritos en cualquier momento y sin aviso previo. NetApp no asume ningún tipo de responsabilidad que surja del uso de los productos aquí descritos, excepto aquello expresamente acordado por escrito por parte de NetApp. El uso o adquisición de este producto no lleva implícita ninguna licencia con derechos de patente, de marcas comerciales o cualquier otro derecho de propiedad intelectual de NetApp.

Es posible que el producto que se describe en este manual esté protegido por una o más patentes de EE. UU., patentes extranjeras o solicitudes pendientes.

LEYENDA DE DERECHOS LIMITADOS: el uso, la copia o la divulgación por parte del gobierno están sujetos a las restricciones establecidas en el subpárrafo (b)(3) de los derechos de datos técnicos y productos no comerciales de DFARS 252.227-7013 (FEB de 2014) y FAR 52.227-19 (DIC de 2007).

Los datos aquí contenidos pertenecen a un producto comercial o servicio comercial (como se define en FAR 2.101) y son propiedad de NetApp, Inc. Todos los datos técnicos y el software informático de NetApp que se proporcionan en este Acuerdo tienen una naturaleza comercial y se han desarrollado exclusivamente con fondos privados. El Gobierno de EE. UU. tiene una licencia limitada, irrevocable, no exclusiva, no transferible, no sublicenciable y de alcance mundial para utilizar los Datos en relación con el contrato del Gobierno de los Estados Unidos bajo el cual se proporcionaron los Datos. Excepto que aquí se disponga lo contrario, los Datos no se pueden utilizar, desvelar, reproducir, modificar, interpretar o mostrar sin la previa aprobación por escrito de NetApp, Inc. Los derechos de licencia del Gobierno de los Estados Unidos de América y su Departamento de Defensa se limitan a los derechos identificados en la cláusula 252.227-7015(b) de la sección DFARS (FEB de 2014).

Información de la marca comercial

NETAPP, el logotipo de NETAPP y las marcas que constan en http://www.netapp.com/TM son marcas comerciales de NetApp, Inc. El resto de nombres de empresa y de producto pueden ser marcas comerciales de sus respectivos propietarios.