Gestione los puertos iSCSI

SANtricity software

NetApp
November 03, 2025

This PDF was generated from https://docs.netapp.com/es-es/e-series-santricity/sm-hardware/configure-iscsi-ports-hardware.html on November 03, 2025. Always check docs.netapp.com for the latest.

Tabla de contenidos

Gestione los puertos iSCSI . . . 1
- Configurar puertos iSCSI en SANtricity System Manager . . . 1
- Configurar la autenticación iSCSI en SANtricity System Manager . . . 3
- Habilitar la configuración de detección de iSCSI en SANtricity System Manager . . . 5
- Ver paquetes de estadísticas iSCSI en SANtricity System Manager . . . 6
- Ver sesiones iSCSI en SANtricity System Manager . . . 7
- Finalizar la sesión iSCSI en SANtricity System Manager . . . 11
- Configurar iSER sobre puertos InfiniBand en SANtricity System Manager . . . 11
- Ver estadísticas de iSER sobre InfiniBand en SANtricity System Manager . . . 12

Gestione los puertos iSCSI

Configurar puertos iSCSI en SANtricity System Manager

Si la controladora incluye una conexión de host iSCSI, los ajustes del puerto iSCSI se pueden configurar desde la página hardware.

Antes de empezar

- La controladora debe incluir puertos iSCSI; de lo contrario, la configuración de iSCSI no estará disponible.
- Se debe conocer la velocidad de la red (la tasa de transferencia de datos entre los puertos y el host).

> La configuración y las funciones iSCSI solamente aparecen si la cabina de almacenamiento es compatible con iSCSI.

Pasos

1. Seleccione **hardware**.
2. Si el gráfico muestra las unidades, haga clic en la pestaña * Controladores y componentes *.

   El gráfico cambia y muestra las controladoras en lugar de las unidades.

3. Haga clic en la controladora con los puertos iSCSI que desea configurar.

   Aparece el menú contextual de la controladora.

4. Seleccione **Configurar puertos iSCSI**.

   > La opción **Configurar puertos iSCSI** aparece sólo si System Manager detecta puertos iSCSI en la controladora.

   Se abre el cuadro de diálogo Configurar puertos iSCSI.

5. En la lista desplegable, seleccione el puerto que desea configurar y, a continuación, haga clic en **Siguiente**.
6. Seleccione los valores del puerto de configuración y, a continuación, haga clic en **Siguiente**.

   Para ver todas las configuraciones de puerto, haga clic en el enlace **Mostrar más opciones de puerto** situado a la derecha del cuadro de diálogo.

Detalles del campo

Opción de configuración de puertos	Descripción
Velocidad del puerto ethernet configurada (aparece solamente en ciertos tipos de tarjetas de interfaz del host)	Seleccione la velocidad que coincida que la capacidad de velocidad del SFP en el puerto.
Modo de corrección de errores de reenvío (FEC) (sólo aparece para determinados tipos de tarjetas de interfaz del sistema principal)	Si lo desea, seleccione uno de los modos FEC para el puerto de host especificado. El modo Reed Solomon no admite la velocidad de puerto de 25 Gbps.
Habilite IPv4/Habilitar IPv6	Seleccione una o ambas opciones para habilitar la compatibilidad con las redes IPv4 e IPv6. Si desea deshabilitar el acceso al puerto, cancele la selección de las dos casillas de comprobación.
Puerto de escucha TCP (disponible haciendo clic en **Mostrar más opciones de puerto**).	De ser necesario, introduzca un nuevo número de puerto. El puerto de escucha es el número de puerto TCP que la controladora utiliza para escuchar inicios de sesión iSCSI de iniciadores iSCSI del host. El puerto de escucha predeterminado es 3260. Debe introducir 3260 o un valor entre 49 49152 y 65 65535.
Tamaño de MTU (disponible haciendo clic en **Mostrar más opciones de puerto**).	De ser necesario, introduzca un nuevo tamaño en bytes para la unidad de transmisión máxima (MTU). El tamaño de MTU predeterminado es de 1500 bytes por trama. Debe introducir un valor entre 1500 y 9000.
Habilite las respuestas PING de ICMP PING	Seleccione esta opción para habilitar el protocolo de mensajes de control de Internet (ICMP). Los sistemas operativos de equipos en red usan ese protocolo para enviar mensajes. Esos mensajes ICMP determinan si es posible acceder a un host y cuánto tiempo debe transcurrir para enviar y recibir los paquetes de ese host.

Si seleccionó **Activar IPv4**, se abre un cuadro de diálogo para seleccionar la configuración IPv4 después de hacer clic en **Siguiente**. Si seleccionó **Activar IPv6**, se abre un cuadro de diálogo para seleccionar la configuración de IPv6 después de hacer clic en **Siguiente**. Si seleccionó ambas opciones, primero se abre el cuadro de diálogo de configuración IPv4 y después de hacer clic en **Siguiente**, se abre el cuadro de diálogo de configuración de IPv6.

7. Configure los valores para IPv4 o IPv6 de forma automática o manual. Para ver todas las opciones de configuración de puertos, haga clic en el enlace **Mostrar más valores** situado a la derecha del cuadro de diálogo.

Detalles del campo

Opción de configuración de puertos	Descripción
Obtener configuración automáticamente	Seleccione esta opción para obtener automáticamente la configuración.
Especificar manualmente la configuración estática	Seleccione esta opción e introduzca una dirección estática en los campos. (Si lo desea, puede cortar y pegar direcciones en los campos.) En el caso de IPv4, incluya la máscara de subred y la puerta de enlace. En el caso de IPv6, incluya la dirección IP enrutable y la dirección IP del enrutador.
Active la compatibilidad con VLAN (disponible haciendo clic en **Mostrar más opciones**).	Seleccione esta opción para habilitar una VLAN e introducir su ID. Una red de área local virtual (VLAN) es una red lógica que se comporta como si estuviese físicamente separada de otras redes de área local virtuales y físicas (LAN) admitidas por los mismos switches, los mismos enrutadores, o ambos.
Activar prioridad ethernet (disponible haciendo clic en **Mostrar más valores**).	Seleccione esta opción para habilitar el parámetro que determina la prioridad de acceso a la red. Use la barra deslizante para seleccionar una prioridad entre 1 (más baja) y 7 (más alta). En un entorno de red de área local (LAN) compartida, como Ethernet, es posible que muchas estaciones compitan por el acceso a la red. El acceso se otorga por orden de llegada. Es posible que dos estaciones intenten acceder a la red al mismo tiempo, lo que provoca que ambas estaciones se apagen y esperen antes de volver a intentarlo. Este proceso se minimiza para Ethernet con switch, donde existe una sola estación conectada a un puerto del switch.

8. Haga clic en **Finalizar**.

Configurar la autenticación iSCSI en SANtricity System Manager

Para obtener seguridad adicional en una red iSCSI, se puede establecer la autenticación entre controladoras (objetivos) y hosts (iniciadores).

System Manager usa el método de protocolo de autenticación por desafío mutuo (CHAP), que valida la identidad de los destinos e iniciadores durante el enlace inicial. La autenticación se basa en una clave de seguridad compartida denominada *CHAP Secret*.

Antes de empezar

Es posible establecer el secreto CHAP para los iniciadores (hosts iSCSI) antes o después de haber

establecido el secreto CHAP para los objetivos (controladoras). Antes de seguir las instrucciones de esta tarea, primero debe esperar a que los hosts hayan establecido una conexión iSCSI y, a continuación, configurar el secreto CHAP en los hosts individuales. Una vez realizadas las conexiones, los nombres IQN de los hosts y los secretos CHAP se enumeran en el cuadro de diálogo de autenticación iSCSI (que se describe en esta tarea), y no es necesario introducirlos manualmente.

Acerca de esta tarea

Se puede seleccionar uno de los siguientes métodos de autenticación:

- **Autenticación unidireccional** — Utilice esta opción para permitir que el controlador autentique la identidad de los hosts iSCSI (autenticación unidireccional).
- **Autenticación bidireccional** — Utilice este ajuste para permitir que tanto el controlador como los hosts iSCSI lleven a cabo la autenticación (autenticación bidireccional). Esta opción aporta un segundo nivel de seguridad, ya que permite que la controladora autentique la identidad de los hosts iSCSI y, a su vez, que los hosts iSCSI autentiquen la identidad de la controladora.

> La configuración y las funciones de iSCSI solo aparecen en la página Configuración si la cabina de almacenamiento es compatible con iSCSI.

Pasos

1. Seleccione MENU:Settings[System].
2. En Configuración de iSCSI, haga clic en **Configurar autenticación**.

   Se muestra el cuadro de diálogo Configurar autenticación, donde se indica el método actualmente seleccionado. También muestra si alguno de los hosts tiene secretos CHAP configurados.

3. Seleccione una de las siguientes opciones:
   - **Sin autenticación** — Si no desea que el controlador autentique la identidad de los hosts iSCSI, seleccione esta opción y haga clic en **Finalizar**. El cuadro de diálogo se cierra y la configuración está lista.
   - **Autenticación unidireccional** — para permitir que el controlador autentique la identidad de los hosts iSCSI, seleccione esta opción y haga clic en **Siguiente** para abrir el cuadro de diálogo Configurar CHAP de destino.
   - **Autenticación bidireccional** — para permitir que tanto el controlador como los hosts iSCSI lleven a cabo la autenticación, seleccione esta opción y haga clic en **Siguiente** para abrir el cuadro de diálogo Configurar CHAP de destino.
4. Tanto para la autenticación unidireccional como para la bidireccional, introduzca o confirme el secreto CHAP de la controladora (el objetivo). El secreto CHAP debe tener entre 12 y 57 caracteres ASCII imprimibles.

   > Si el secreto CHAP de la controladora se configuró anteriormente, los caracteres que aparecen en el campo se muestran enmascarados. Si es necesario, puede reemplazar los caracteres existentes (los caracteres nuevos no están enmascarados).

5. Debe realizar una de las siguientes acciones:
   - Si está configurando la autenticación *unidireccional*, haga clic en **Finalizar**. El cuadro de diálogo se cierra y la configuración está lista.
   - Si está configurando la autenticación *bidireccional*, haga clic en **Siguiente** para abrir el cuadro de diálogo Configurar CHAP del iniciador.

6. En el caso de la autenticación bidireccional, introduzca o confirme un secreto CHAP de cualquiera de los hosts iSCSI (los iniciadores), que pueden tener entre 12 y 57 caracteres ASCII imprimibles. Si no desea configurar la autenticación bidireccional de un host en particular, deje en blanco el campo Secreto CHAP del iniciador.

> Si el secreto CHAP de un host se configuró con anterioridad, los caracteres del campo están enmascarados. Si es necesario, puede reemplazar los caracteres existentes (los caracteres nuevos no están enmascarados).

7. Haga clic en **Finalizar**.

Resultados

La autenticación sucede durante la secuencia de inicio de sesión iSCSI, entre las controladoras y los hosts iSCSI, a menos que no se haya especificado ninguna autenticación.

Habilitar la configuración de detección de iSCSI en SANtricity System Manager

Es posible habilitar la configuración relacionada con la detección de dispositivos de almacenamiento en una red iSCSI.

La configuración de detección de objetivos permite registrar la información de iSCSI de la cabina de almacenamiento con el protocolo de servicio de nombres de almacenamiento de Internet (iSNS), y también determinar si se deben permitir las sesiones de detección sin nombre.

Antes de empezar

Si el servidor iSNS utiliza una dirección IP estática, esa dirección debe estar disponible para registrarse en iSNS. Se admiten tanto IPv4 como IPv6.

Acerca de esta tarea

Es posible habilitar la siguiente configuración relacionada con la detección de iSCSI:

- **Activar el servidor iSNS para registrar un destino** — cuando está activado, la cabina de almacenamiento registra la información de su nombre completo iSCSI (IQN) y su puerto del servidor iSNS. Esta opción permite la detección de iSNS para que un iniciador pueda recuperar la información de IQN y puerto del servidor iSNS.
- **Activar sesiones de detección sin nombre** — cuando las sesiones de detección sin nombre están habilitadas, el iniciador (host iSCSI) no necesita proporcionar el IQN del destino (controladora) durante la secuencia de inicio de sesión para una conexión de tipo de detección. Cuando se deshabilitan, los hosts deben proporcionar el IQN para establecer una sesión de detección con la controladora. Sin embargo, siempre se requiere el IQN objetivo durante una sesión normal (con I/o). Al deshabilitar esta opción, se puede evitar que los hosts iSCSI no autorizados se conecten a la controladora mediante esta dirección IP solamente.

> La configuración y las funciones de iSCSI solo aparecen en la página Configuración si la cabina de almacenamiento es compatible con iSCSI.

Pasos

1. Seleccione MENU:Settings[System].
2. En **Configuración de iSCSI**, haga clic en **Ver/editar configuración de detección de objetivos**.

Se muestra el cuadro de diálogo Configuración de detección de objetivos. Debajo del **Activar servidor iSNS**… campo, el cuadro de diálogo indica si la controladora ya está registrada.

3. Para registrar el controlador, seleccione **Activar servidor iSNS para registrar mi destino** y, a continuación, seleccione una de las siguientes opciones:
   - **Obtener automáticamente la configuración del servidor DHCP** — Seleccione esta opción si desea configurar el servidor iSNS usando un servidor DHCP (Dynamic Host Configuration Protocol). Tenga en cuenta que, si usa esta opción, todos los puertos iSCSI en la controladora también deben configurarse para usar DHCP. Si es necesario, actualice el puerto iSCSI de la controladora para habilitar esta opción.

     Para que el servidor DHCP proporcione la dirección del servidor iSNS, debe configurar el servidor DHCP para que utilice la opción 43 — ""Información específica del proveedor"." Esta opción debe incluir la dirección IPv4 del servidor iSNS en los bytes de datos 0xa-0xd (10-13).

   - **Especificar manualmente la configuración estática** — Seleccione esta opción si desea introducir una dirección IP estática para el servidor iSNS. (Si lo desea, puede cortar y pegar direcciones en los campos.) En el campo, introduzca una dirección IPv4 o IPv6. Si configuró ambas, IPv4 es la predeterminada. Introduzca además un puerto de escucha TCP (utilice 3205, que es el predeterminado, o especifique un valor entre 49 49152 y 65 65535).
4. Para permitir que la cabina de almacenamiento participe en sesiones de detección sin nombre, seleccione **Habilitar sesiones de detección sin nombre**.
   - Cuando se habilita esta opción, no se requiere que los iniciadores de iSCSI especifiquen el IQN objetivo para recuperar la información de la controladora.
   - Cuando se deshabilita, se impiden las sesiones de detección a menos que el iniciador proporcione el IQN objetivo. Al deshabilitar las sesiones de detección sin nombre, se obtiene seguridad adicional.
5. Haga clic en **Guardar**.

Resultados

Se muestra una barra de progreso cuando System Manager intenta registrar la controladora en el servidor iSNS. Este proceso puede llevar hasta cinco minutos.

Ver paquetes de estadísticas iSCSI en SANtricity System Manager

Es posible ver datos sobre las conexiones iSCSI con la cabina de almacenamiento.

Acerca de esta tarea

En System Manager, se muestran los siguientes tipos de estadísticas de iSCSI. Todas las estadísticas son de solo lectura y no pueden configurarse.

Los tipos de estadísticas que se muestran en System Manager se basan en las estadísticas disponibles para la cabina de almacenamiento.

- **Estadísticas de MAC Ethernet** — proporciona estadísticas para el control de acceso a medios (MAC). MAC también proporciona un mecanismo de direccionamiento denominado dirección física o dirección MAC. La dirección MAC es una dirección única que se asigna a cada adaptador de red. La dirección MAC ayuda a entregar paquetes de datos a un destino dentro de la subred.

- **Ethernet TCP/IP statistics** — proporciona estadísticas para TCP/IP, que es el Protocolo de control de transmisión (TCP) y el Protocolo de Internet (IP) para el dispositivo iSCSI. Con TCP, las aplicaciones en hosts en red pueden crean conexiones entre sí, mediante las cuales pueden intercambiar datos en paquetes. El IP es un protocolo orientado a datos que comunica datos por una interred conmutada por paquetes. Las estadísticas de IPv4 e IPv6 se muestran por separado.
- **Ethernet Kernel statistics** — Proporciona estadísticas para los controladores del kernel de la plataforma del dispositivo iSCSI. Las estadísticas del núcleo muestran datos de red similares a la opción de estadísticas TCP/IP. Sin embargo, los datos estadísticos del núcleo se recopilan de los controladores del núcleo de la plataforma en lugar de directamente del hardware iSCSI.
- **Estadísticas de destino local/iniciador (protocolo)**: Muestra estadísticas para el destino iSCSI, que proporciona acceso a nivel de bloque a sus medios de almacenamiento y muestra las estadísticas de iSCSI para la matriz de almacenamiento cuando se utiliza como iniciador en operaciones de mirroring asíncrono.
- **Estadísticas de Estados operativos de DCBX** — muestra los estados operativos de las diversas funciones de Data Center Bridging Exchange (DCBX).
- **LLDP TLV statistics** — muestra las estadísticas de tipo-longitud-valor (TLV) del protocolo de detección de nivel de vínculo (LLDP).
- **Estadísticas TLV de DCBX** — muestra la información que identifica los puertos de host de la matriz de almacenamiento en un entorno de protocolo de puente del centro de datos (DCB). Esta información se comparte con los colegas de red para fines de identificación y funcionalidad.

Es posible ver cada una de las estadísticas como estadísticas sin configurar o estadísticas de base. Las estadísticas sin configurar son todas las estadísticas recogidas desde que se iniciaron las controladoras. Las estadísticas de base son las estadísticas de un momento específico que se recogen desde el establecimiento de la hora de la línea de base.

Pasos

1. Seleccione menú:ficha Soporte[Centro de soporte > Diagnóstico].
2. Seleccione **Ver paquetes de estadísticas iSCSI**.
3. Haga clic en una pestaña para ver los diferentes conjuntos de estadísticas.
4. Para establecer la línea de base, haga clic en **establecer nueva línea de base**.

   La configuración de la línea de base establece un nuevo punto de partida para la recogida de estadísticas. La misma línea de base se usa para todas las estadísticas de iSCSI.

Ver sesiones iSCSI en SANtricity System Manager

Es posible ver información detallada sobre las conexiones iSCSI a la cabina de almacenamiento. Se pueden realizar sesiones iSCSI con hosts o cabinas de almacenamiento remotas en una relación de reflejo asíncrono.

Pasos

1. Seleccione MENU:Settings[System].
2. Seleccione **Ver/finalizar sesiones iSCSI**.

   Se muestra una lista de las sesiones iSCSI actuales.

3. **Opcional:** para ver información adicional acerca de una sesión iSCSI específica, seleccione una sesión y,

a continuación, haga clic en **Ver detalles**.

Detalles del campo

Elemento	Descripción
Identificador de sesión (SSID)	La cadena hexadecimal que identifica una sesión entre un iniciador de iSCSI y un destino iSCSI. El SSID está compuesto por ISID y TPGT.
Identificador de sesión del iniciador (ISID)	La parte del iniciador del identificador de sesión. El iniciador especifica el ISID durante el inicio de sesión.
Grupo de portal de destino	El destino iSCSI.
Etiqueta del grupo de portal de destino (TPGT)	La parte del destino del identificador de sesión. Identificador numérico de 16 bits para un grupo de portales de destino iSCSI.
Nombre iSCSI del iniciador	El nombre WWN único del iniciador.
Etiqueta de iSCSI del iniciador	La etiqueta de usuario configurada en System Manager.
Alias del iniciador de iSCSI	Un nombre que también puede asociarse a un nodo iSCSI. El alias permite a una organización asociar una cadena intuitiva al nombre iSCSI. Sin embargo, el alias no es un sustituto del nombre iSCSI. El alias del iniciador de iSCSI solo puede configurarse en el host, no en System Manager
Host	El servidor que envía entrada y salida a la cabina de almacenamiento.
Identificador de conexión (CID)	Nombre único para una conexión dentro de la sesión entre el iniciador y el destino. El iniciador genera este ID y lo presenta al destino durante las solicitudes de inicio de sesión. El ID de conexión también se presenta durante los cierres de sesión que cierran las conexiones.
Identificador de puerto	El puerto de la controladora asociado a la conexión.
Dirección IP del iniciador	La dirección IP del iniciador.
Parámetros de inicio de sesión negociados	Los parámetros que se negocian durante el inicio de sesión de la sesión iSCSI.
Método de autenticación	La técnica para autenticar usuarios que desean acceder a la red iSCSI. Los valores válidos son **CHAP** y **Ninguno**.

Elemento	Descripción
Método de resumen del encabezado	La técnica para mostrar posibles valores de encabezados para la sesión iSCSI. HeaderDigest y DataDigest pueden ser **None** o **CRC32C**. El valor predeterminado para ambos es **Ninguno**.
Método de resumen de datos	La técnica para mostrar posibles valores de datos para la sesión iSCSI. HeaderDigest y DataDigest pueden ser **None** o **CRC32C**. El valor predeterminado para ambos es **Ninguno**.
Conexiones máximas	El mayor número de conexiones permitidas para la sesión iSCSI. El número máximo de conexiones puede ser de 1 a 4. El valor predeterminado es **1**.
Alias de destino	La etiqueta asociada al destino.
Alias del iniciador	La etiqueta asociada al iniciador.
Dirección IP de destino	La dirección IP del destino para la sesión iSCSI. Los nombres DNS no son compatibles.
R2T inicial	La inicial lista para transferir Estados. El estado puede ser **Sí** o **no**.
Longitud de ráfaga máxima	La carga útil máxima de SCSI en bytes para esta sesión iSCSI. La longitud máxima de ráfaga puede ser de 512 a 262,144 144 (256 KB). El valor predeterminado es **262,144 (256 KB)**.
Longitud de la primera ráfaga	La carga útil de SCSI en bytes para datos no solicitados para esta sesión iSCSI. La longitud de la primera ráfaga puede ser de 512 a 131,072 072 (128 KB). El valor predeterminado es **65,536 (64 KB)**.
Tiempo predeterminado de espera	La cantidad mínima de segundos que se deben esperar para intentar establecer una conexión después de la terminación o el restablecimiento de una conexión. El valor predeterminado de tiempo para esperar puede ser de 0 a 3600. El valor predeterminado es **2**.
Tiempo predeterminado de retención	La cantidad máxima de segundos durante los cuales aún puede establecerse una conexión después de la terminación o el restablecimiento de una conexión. El valor predeterminado de tiempo para retener puede ser de 0 a 3600. El valor predeterminado es **20**.
R2T pendiente máximo	La cantidad máxima de Estados listos para transferencia pendientes para esta sesión iSCSI. El valor máximo de Estados listos para transferencia pendientes puede ser de 1 a 16. El valor predeterminado es **1**.
Nivel de recuperación de errores	El nivel de recuperación de error para esta sesión iSCSI. El valor del nivel de recuperación de errores siempre está establecido en **0**.

Elemento	Descripción
Longitud máxima del segmento de datos de recepción	La cantidad máxima de datos que el iniciador o el destino pueden recibir en cualquier unidad de datos de carga útil de iSCSI (PDU).
Nombre de destino	El nombre oficial del destino (no el alias). El nombre de destino con formato *IQN*.
Nombre del iniciador	El nombre oficial del iniciador (no el alias). El nombre del iniciador que usa formato *IQN* o *eui*.

4. **Opcional:** para guardar el informe en un archivo, haga clic en **Guardar**.

   El archivo se guarda en la carpeta de descargas del explorador con el nombre de archivo `iscsi-session-connections.txt`.

Finalizar la sesión iSCSI en SANtricity System Manager

Es posible finalizar una sesión iSCSI que no se necesita. Se pueden realizar sesiones iSCSI con hosts o cabinas de almacenamiento remotas en una relación de reflejo asíncrono.

Acerca de esta tarea

Es posible que desee finalizar una sesión iSCSI por los siguientes motivos:

- **Acceso no autorizado** — Si un iniciador iSCSI está conectado y no debe tener acceso, puede finalizar la sesión iSCSI para forzar al iniciador iSCSI fuera de la matriz de almacenamiento. El iniciador de iSCSI puede haber iniciado sesión porque el método de autenticación Ninguno estaba disponible.
- **Tiempo de inactividad del sistema** — Si necesita desconectar una matriz de almacenamiento y observa que los iniciadores iSCSI todavía están conectados, puede finalizar las sesiones iSCSI para sacar los iniciadores iSCSI de la matriz de almacenamiento.

Pasos

1. Seleccione MENU:Settings[System].
2. Seleccione **Ver/finalizar sesiones iSCSI**.

   Se muestra una lista de las sesiones iSCSI actuales.

3. Seleccione la sesión que desea finalizar
4. Haga clic en **Finalizar sesión** y confirme que desea realizar la operación.

Configurar iSER sobre puertos InfiniBand en SANtricity System Manager

Si la controladora tiene un puerto Iser over InfiniBand, se puede configurar la conexión de red al host.

Antes de empezar

- La controladora debe tener un puerto Iser over InfiniBand; de lo contrario, las opciones de Iser over InfiniBand no estarán disponibles en System Manager.
- Se debe conocer la dirección IP de la conexión de host.

Pasos

1. Seleccione **hardware**.
2. Si el gráfico muestra las unidades, haga clic en la pestaña * Controladores y componentes *.

   El gráfico cambia y muestra las controladoras en lugar de las unidades.

3. Haga clic en la controladora que tenga el puerto Iser over InfiniBand que desea configurar.

   Aparece el menú contextual de la controladora.

4. Seleccione **Configurar puertos Iser over InfiniBand**.

   Se muestra el cuadro de diálogo Configurar puertos Iser over InfiniBand.

5. En el menú desplegable, seleccione el puerto HIC que desea configurar y después introduzca la dirección IP del host.
6. Haga clic en **Configurar**.
7. Complete la configuración y, a continuación, restablezca el puerto Iser over InfiniBand haciendo clic en **Sí**.

Ver estadísticas de iSER sobre InfiniBand en SANtricity System Manager

Si la controladora de la cabina de almacenamiento incluye un puerto Iser over InfiniBand, es posible ver datos sobre las conexiones del host.

Acerca de esta tarea

En System Manager, se muestran los siguientes tipos de estadísticas de Iser over InfiniBand. Todas las estadísticas son de solo lectura y no pueden configurarse.

- **Estadísticas de destino local (protocolo)** — proporciona estadísticas para el destino Iser over InfiniBand, que muestra el acceso de nivel de bloque a sus medios de almacenamiento.
- **Estadísticas de la interfaz Iser over InfiniBand** — proporciona estadísticas para todos los puertos Iser en la interfaz InfiniBand, que incluye estadísticas de rendimiento e información de errores de enlace asociados con cada puerto del switch.

Es posible ver cada una de las estadísticas como estadísticas sin configurar o estadísticas de base. Las estadísticas sin configurar son todas las estadísticas recogidas desde que se iniciaron las controladoras. Las estadísticas de base son las estadísticas de un momento específico que se recogen desde el establecimiento de la hora de la línea de base.

Pasos

1. Seleccione MENU:Settings[System].
2. Seleccione **Ver estadísticas de Iser over InfiniBand**.
3. Haga clic en una pestaña para ver los diferentes conjuntos de estadísticas.

4. **Opcional:** para establecer la línea de base, haga clic en **establecer nueva línea de base**.

   La configuración de la línea de base establece un nuevo punto de partida para la recogida de estadísticas. La misma línea de base se usa para todas las estadísticas de Iser over InfiniBand.

Información de copyright

Copyright © 2025 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.