Sistema

SANtricity 11.5

NetApp
February 12, 2024

Tabla de contenidos

Sistema

Configuración de cabina de almacenamiento

Conceptos

Rendimiento y configuración de la caché

La memoria caché es un área de almacenamiento volátil temporal en la controladora que tiene un tiempo de acceso menor que los medios con unidades.

Con el almacenamiento en caché, es posible aumentar el rendimiento de I/o de la siguiente manera:

- Los datos solicitados desde el host para una lectura pueden estar ya en la caché debido a una operación anterior. Esto elimina la necesidad de acceder a la unidad.
- Los datos de escritura se escriben primero en la caché. Esto permite que la aplicación avance sin esperar que los datos se escriban en la unidad.

La configuración predeterminada de la caché cumple con los requisitos de la mayoría de los entornos, pero es posible modificarla si es necesario.

Configuración de la caché de la cabina de almacenamiento

Es posible especificar los siguientes valores en la página sistema para todos los volúmenes de la cabina de almacenamiento:

- **Iniciar valor para vaciar** — el porcentaje de datos no escritos en la caché que activan un vaciado de caché (escribir en disco). Cuando la caché alberga el porcentaje de inicio especificado de datos sin escribir, se activa un vaciado. De forma predeterminada, la controladora inicia el vaciado de la caché cuando la caché se encuentra un 80 % llena.
- **Tamaño de bloque de caché** — el tamaño máximo de cada bloque de caché, que es una unidad organizativa para la administración de caché. De forma predeterminada, el tamaño de bloque de caché es 8 KiB, pero se puede establecer en 4, 8, 16 o 32 KiB. Lo ideal es establecer el tamaño de bloque de caché en el tamaño de I/o predominante de las aplicaciones. Por lo general, los sistemas de archivos o las aplicaciones de bases de datos utilizan tamaños menores. Se recomiendan tamaños mayores para las aplicaciones de grandes transferencias de datos o I/o secuenciales

Configuración de la caché del volumen

Es posible especificar los siguientes valores en la página volúmenes para volúmenes individuales de la cabina de almacenamiento (menú:almacenamiento[volúmenes]):

- **Caché de lectura** — la caché de lectura es un búfer que almacena datos que se han leído desde las unidades. Es posible que los datos de una operación de lectura ya deban estar en la caché debido a una operación anterior, por lo tanto, no es necesario acceder a las unidades. Los datos se conservan en la caché de lectura hasta que esta se vacía.
  - **Captura previa de caché de lectura dinámica**: La captura previa de lectura de caché dinámica permite a la controladora copiar otros bloques de datos secuenciales en la caché mientras lee bloques de datos de una unidad en la caché. Ese almacenamiento en caché aumenta la posibilidad de que se puedan cumplir futuras solicitudes de datos de la caché. La captura previa de lectura de la caché dinámica es importante para las aplicaciones multimedia que utilizan I/o secuencial La cantidad y la

velocidad de las capturas previas de los datos en la caché se ajustan automáticamente según la velocidad y el tamaño de solicitud de las lecturas del host. El acceso aleatorio no provoca la captura previa de los datos en la caché. Esta función no se aplica cuando el almacenamiento en caché de lectura está deshabilitado.

- **Almacenamiento en caché de escritura** — la caché de escritura es un búfer que almacena datos del host que todavía no se han escrito en las unidades. Los datos permanecen en la caché de escritura hasta que se escriben en las unidades. El almacenamiento en caché de escritura puede aumentar el rendimiento de I/O.

  Posible pérdida de datos — Si activa la opción almacenamiento en caché de escritura sin baterías y no dispone de una fuente de alimentación universal de protección, puede perder datos. Además, es posible perder datos si la controladora no tiene baterías y se habilita la opción almacenamiento en caché de escritura sin baterías.

  - **Almacenamiento en caché de escritura sin baterías** — la configuración de almacenamiento en caché de escritura sin baterías permite que el almacenamiento en caché de escritura continúe incluso cuando las baterías faltan, fallan, están completamente descargadas o no están totalmente cargadas. Por lo general, no se recomienda elegir el almacenamiento en caché de escritura sin baterías porque se pueden perder los datos en caso de interrupción del suministro eléctrico. Comúnmente, la controladora desactiva en forma temporal el almacenamiento en caché de escritura hasta que se cargan las baterías o se reemplaza una batería con errores.
  - **Almacenamiento en caché de escritura con duplicación** — el almacenamiento en caché de escritura con duplicación se produce cuando los datos escritos en la memoria caché de un controlador también se escriben en la memoria caché del otro controlador. Por lo tanto, si una controladora falla, la otra puede completar todas las operaciones de escritura pendientes. El mirroring de la caché de escritura está disponible solo si el almacenamiento en caché de escritura está habilitado y existen dos controladoras. El almacenamiento en caché de escritura con mirroring es la configuración predeterminada cuando se crea un volumen.

Información general sobre equilibrio de carga automático

La función Automatic Load Balancing ofrece una gestión de recursos de I/o mejorada, ya que reacciona dinámicamente a los cambios de carga con el tiempo y ajusta automáticamente la propiedad de la controladora de volumen para corregir cualquier problema de desequilibrio de carga cuando las cargas de trabajo son distintas de una controladora a otra.

La carga de trabajo de cada controladora se supervisa continuamente y, con la colaboración de los controladores multivía instalados en los hosts, es posible establecer automáticamente el equilibrio cada vez que sea necesario. Una vez que la carga de trabajo se vuelve a equilibrar de forma automática en todas las controladoras, el administrador de almacenamiento queda liberado de la carga que supone ajustar manualmente la propiedad de la controladora de volumen para admitir cambios de carga en la cabina de almacenamiento.

Cuando la función Automatic Load Balancing está habilitada, ejecuta las siguientes funciones:

- Supervisa y equilibra automáticamente la utilización de recursos de la controladora.
- Ajusta automáticamente la propiedad de la controladora de volumen cuando es necesario y así, optimiza el ancho de banda de I/o entre los hosts y la cabina de almacenamiento.

Habilitar y deshabilitar Automatic Load Balancing

La función Automatic Load Balancing está habilitada de forma predeterminada en todas las cabinas de almacenamiento.

Puede ser conveniente deshabilitar Automatic Load Balancing en la cabina de almacenamiento por las siguientes razones:

- No se desea cambiar automáticamente la propiedad de una controladora de volumen para equilibrar la carga de trabajo.
- Se trabaja en un entorno altamente optimizado donde la distribución de carga se configura intencionalmente para lograr una distribución específica entre las controladoras.

Los tipos de hosts compatibles con la función Automatic Load Balancing

Aunque la función Automatic Load Balancing está habilitada en el nivel de la cabina de almacenamiento, el tipo de host que se selecciona para un host o clúster de hosts tiene una influencia directa sobre la forma en que opera la función.

Cuando se equilibra la carga de trabajo de la cabina de almacenamiento en varias controladoras, la función Automatic Load Balancing intenta mover volúmenes a los que pueden acceder ambas controladoras y que solo se asignan a un host o clúster de hosts compatible con la función Automatic Load Balancing.

Este comportamiento evita que un host pierda acceso a un volumen debido al proceso de equilibrio de carga; sin embargo, la presencia de volúmenes asignados a hosts no compatibles con Automatic Load Balancing afecta a la capacidad para equilibrar la carga de trabajo que posee la cabina de almacenamiento. Para que Automatic Load Balancing equilibre la carga de trabajo, el controlador multivía debe ser compatible con TPGS, y debe incluirse el tipo de host en la siguiente tabla.

> Para que un clúster de hosts se considere compatible con Automatic Load Balancing, todos los hosts de ese grupo deben ser compatibles con Automatic Load Balancing.

Tipo de host compatible con Automatic Load Balancing	Con este controlador multivía
Windows o Windows almacenado en clúster	MPIO con DSM E-Series de NetApp
Linux DM-MP (Kernel 3.10 o posterior)	DM-MP con `scsi_dh_alua` controlador de dispositivos
VMware	Complemento nativo multivía (NMP) con `VMW_SATP_ALUA Storage Array Type` plugin

> Salvo excepciones menores, los tipos de hosts no compatibles con Automatic Load Balancing siguen funcionando normalmente más allá de que la función esté habilitada o no. Una excepción es cuando un sistema conmuta al nodo de respaldo y las cabinas de almacenamiento mueven volúmenes sin asignar nuevamente a la controladora a la que pertenecen cuando la ruta de datos regresa. No se mueve ninguno de los volúmenes asignados a hosts no compatibles con Automatic Load Balancing.

Consulte "Herramienta de matriz de interoperabilidad" Para acceder a información de compatibilidad para controladores multivía específicos, nivel de sistema operativo y compatibilidad con soportes de controladoras-

unidades.

Comprobación de la compatibilidad del sistema operativo con la función Automatic Load Balancing

Compruebe la compatibilidad del sistema operativo con la función Automatic Load Balancing antes de configurar un sistema nuevo o migrar uno existente.

1. Vaya a la "Herramienta de matriz de interoperabilidad" para encontrar la solución y verificar la compatibilidad.

   Si el sistema operativo es Red Hat Enterprise Linux 6 o SUSE Linux Enterprise Server 11, póngase en contacto con el servicio de asistencia técnica.

2. Actualice y configure el `/etc/multipath.conf file`.
3. Asegúrese de que ambos `retain_attached_device_handler` y.. `detect_prio` se establecen en `yes` para el proveedor y el producto correspondientes, o utilice la configuración predeterminada.

Tipo de sistema operativo del host predeterminado

La cabina de almacenamiento utiliza el tipo de host predeterminado cuando se conectan inicialmente los hosts. Define la manera en que funcionan las controladoras en la cabina de almacenamiento con el sistema operativo del host cuando se accede a los volúmenes. Es posible cambiar el tipo de host si hay una necesidad de cambiar la manera en que opera la cabina de almacenamiento en relación con los hosts que están conectados con ella.

En general, se debe cambiar el tipo de host predeterminado antes de conectar hosts a la cabina de almacenamiento o al añadir hosts adicionales.

Tenga en cuenta estas directrices:

- Si todos los hosts que piensa conectar a la cabina de almacenamiento tienen el mismo sistema operativo (entorno de host homogéneo), cambie el tipo de host para que coincida con el sistema operativo.
- Si hay hosts con diferentes sistemas operativos que piensa conectar a la cabina de almacenamiento (entorno de host heterogéneo), cambie el tipo de host para que coincida con la mayoría de los sistemas operativos de los hosts.

  Por ejemplo, si va a conectar ocho hosts diferentes a la cabina de almacenamiento y seis de ellos tienen un sistema operativo Windows, debe seleccionar Windows como tipo de sistema operativo de host predeterminado.

- Si la mayoría de los hosts conectados poseen una combinación de sistemas operativos diferentes, cambie el tipo de host a opción predeterminada de fábrica.

  Por ejemplo, si va a conectar ocho hosts diferentes a la cabina de almacenamiento y dos de ellos tienen un sistema operativo Windows, tres tienen HP-UX, Y otros tres ejecutan un sistema operativo Linux, debe seleccionar opción predeterminada de fábrica como el tipo de sistema operativo del host predeterminado.

Procedimientos

Edite el nombre de la cabina de almacenamiento

Es posible cambiar el nombre de la cabina de almacenamiento que aparece en la barra de título de SANtricity System Manager.

Pasos

1. Seleccione MENU:Settings[System].
2. En **General**, busque el campo **Nombre:**.

   Si no se definió un nombre de cabina de almacenamiento, este campo muestra el texto "Unknown".

3. Haga clic en el icono **Editar** (lápiz) ubicado junto al nombre de la cabina de almacenamiento.

   Ahora el campo puede editarse.

4. Introduzca un nombre nuevo.

   Un nombre puede contener letras, números y los caracteres especiales subrayado (_), guión (-) y signo numeral (#). Un nombre no puede contener espacios. Un nombre puede contener un máximo de 30 caracteres. El nombre debe ser único.

5. Haga clic en el icono **Guardar** (Marca de verificación).

   Si desea cerrar el campo editable sin realizar cambios, haga clic en el icono Cancelar (X).

Resultado

El nuevo nombre aparecerá en la barra de título de SANtricity System Manager.

Encender luces de localización en cabina de almacenamiento

Para encontrar la ubicación física de una cabina de almacenamiento en un armario, se pueden encender las luces (LED) localizadoras.

Pasos

1. Seleccione MENU:Settings[System].
2. En **General**, haga clic en **encender las luces localizadoras de la matriz de almacenamiento**.

   Se abre el cuadro de diálogo **encender las luces localizadoras de la matriz de almacenamiento** y se encienden las luces localizadoras de la matriz de almacenamiento correspondiente.

3. Cuando haya localizado físicamente la cabina de almacenamiento, regrese al cuadro de diálogo y seleccione **Apagar**.

Resultados

Las luces localizadoras se apagan y el cuadro de diálogo se cierra.

Sincronice los relojes de la cabina de almacenamiento

Si el protocolo de tiempo de redes (NTP) no está habilitado, los relojes de las controladoras se pueden configurar manualmente, de manera que queden sincronizados con el cliente de gestión (el sistema que se utiliza para ejecutar el explorador que accede

a System Manager de SANtricity).

Acerca de esta tarea

La sincronización garantiza que las marcas de tiempo del evento del registro de eventos coincidan con las marcas de tiempo escritas en los archivos de registro del host. Durante el proceso de sincronización, las controladoras siguen estando disponibles y siguen siendo operativas.

> Si la opción NTP se encuentra habilitada en System Manager, no se debe usar esta opción para sincronizar los relojes. En cambio, NTP sincroniza automáticamente los relojes con un host externo que utiliza el protocolo de tiempo de redes simple (SNTP).

> Una vez que se realiza la sincronización, se puede observar que las estadísticas de rendimiento se pierden o se alteran, las programaciones se ven afectadas (ASUP, snapshots, etc.) y las marcas de tiempo de los datos de registro se alteran. Para evitar este problema, se puede usar NTP.

Pasos

1. Seleccione MENU:Settings[System].
2. En **General**, haga clic en **Sincronizar relojes de cabinas de almacenamiento**.

   Se abre el cuadro de diálogo **Sincronizar relojes de cabinas de almacenamiento**. Muestra la fecha y hora actuales de la controladora y el equipo que se usa como cliente de gestión.

   > Para las cabinas de almacenamiento simples, solo se muestra una controladora.

3. Si las horas que aparecen en el cuadro de diálogo no coinciden, haga clic en **Sincronizar**.

Resultados

Una vez que la sincronización se haya realizado correctamente, las marcas de tiempo del evento serán las mismas para el registro de eventos y los registros de host.

Guarde la configuración de la cabina de almacenamiento

Es posible guardar la información de configuración de una cabina de almacenamiento en un archivo de script para ahorrar tiempo al configurar cabinas de almacenamiento adicionales con las mismas opciones.

Antes de empezar

La cabina de almacenamiento no debe estar sujeta a ninguna operación por la que se modifique su configuración lógica. Algunos ejemplos de estas operaciones son crear o eliminar volúmenes, descargar firmware de controladora, asignar o modificar unidades de repuesto, o añadir capacidad (unidades) a un grupo de volúmenes.

Acerca de esta tarea

Al guardar la configuración de una cabina de almacenamiento, se genera un script de interfaz de línea de comandos (CLI) con las opciones de la cabina de almacenamiento, la configuración de los volúmenes, la configuración de los hosts o las asignaciones de host a volumen para la cabina de almacenamiento. Se puede usar este script de CLI generado para replicar una configuración a otra cabina de almacenamiento con la misma configuración de hardware.

No obstante, no se debe usar este script de CLI para la recuperación ante desastres. En lugar de eso, para

restaurar el sistema, utilice el archivo de backup de base de datos de configuración que creó manualmente o póngase en contacto con el soporte técnico para obtener estos datos de los datos de AutoSupport más recientes.

Esta operación *not* guarda estos valores:

- Duración de la batería
- Hora del día de la controladora
- Opciones de la memoria estática de acceso aleatorio no volátil (NVSRAM)
- Funciones excepcionales
- Contraseña de la cabina de almacenamiento
- Estado operativo y estados de los componentes de hardware
- Estado operativo (excepto que sea óptimo) y estados de los grupos de volúmenes
- Servicios de copia, como el mirroring y la copia de volumen

Riesgo de errores en la aplicación — no utilice esta opción si la matriz de almacenamiento está sufriendo una operación que cambiará cualquier configuración lógica. Algunos ejemplos de estas operaciones son crear o eliminar volúmenes, descargar firmware de controladora, asignar o modificar unidades de repuesto, o añadir capacidad (unidades) a un grupo de volúmenes.

Pasos

1. Seleccione MENU:Settings[System].
2. Seleccione **Guardar configuración de la matriz de almacenamiento**.
3. Seleccione los elementos de la configuración que desea guardar:
   - **Configuración de la matriz de almacenamiento**
   - **Configuración de volumen**
   - **Configuración del host**
   - **Asignaciones de host a volumen**

   Si selecciona el elemento **asignaciones de host a volumen**, el elemento **Configuración de volumen** y el elemento **Configuración de host** también se seleccionan de forma predeterminada. No puede guardar **asignaciones de host a volumen** sin guardar también **Configuración de volumen** y **Configuración de host**.
4. Haga clic en **Guardar**.

   El archivo se guarda en la carpeta de descargas del explorador con el nombre `storage-array-configuration.cfg`.

Después de terminar

Para cargar una configuración de cabina de almacenamiento en otra cabina de almacenamiento, use Unified Manager de SANtricity.

Borrar la configuración de la cabina de almacenamiento

Use la operación Clear Configuration cuando desee eliminar todos los pools, los grupos

de volúmenes, los volúmenes, las definiciones de hosts y las asignaciones de hosts de la cabina de almacenamiento.

Antes de empezar

- Antes de borrar la configuración de la cabina de almacenamiento, realice un backup de los datos.

Acerca de esta tarea

Clear Storage Array Configuration contiene dos opciones:

- **Volumen**: Normalmente, puede utilizar la opción volumen para volver a configurar una matriz de almacenamiento de prueba como una matriz de almacenamiento de producción. Por ejemplo, puede configurar una cabina de almacenamiento para pruebas y después, una vez terminadas las pruebas, eliminar la configuración de prueba y configurar la cabina de almacenamiento para un entorno de producción.
- **Storage Array**: Normalmente, puede utilizar la opción Storage Array para mover una matriz de almacenamiento a otro departamento o grupo. Por ejemplo, puede que utilice una cabina de almacenamiento en Engineering y ahora Engineering consigue una nueva cabina de almacenamiento, por lo que desea mover la cabina de almacenamiento actual a Administración para volver a configurarla.

  La opción cabina de almacenamiento elimina algunas opciones de configuración adicionales.

	Volumen	Cabina de almacenamiento
Elimina pools y grupos de volúmenes	X	X
Elimina volúmenes	X	X
Elimina hosts y clústeres de hosts	X	X
Elimina asignaciones de hosts	X	X
Elimina el nombre de la cabina de almacenamiento		X
Restablece la configuración de caché de la cabina de almacenamiento a su valor predeterminado		X

Riesgo de pérdida de datos — esta operación elimina todos los datos de la matriz de almacenamiento. (No ejecuta un borrado seguro.) No es posible cancelar esta operación una vez que se inicia. Realice esta operación solo cuando el soporte técnico se lo indique.

Pasos

1. Seleccione MENU:Settings[System].
2. Seleccione **Borrar configuración de la matriz de almacenamiento**.
3. En la lista desplegable, seleccione **volumen** o **matriz de almacenamiento**.

4. **Opcional**: Si desea guardar la configuración (no los datos), utilice los vínculos del cuadro de diálogo.
5. Confirme que desea llevar a cabo la operación.

Resultados

- La configuración actual se elimina y se destruyen todos los datos existentes de la cabina de almacenamiento.
- Todas las unidades quedan sin asignar.

Configure el banner de inicio de sesión

Puede crear un banner de inicio de sesión que se presente a los usuarios antes de que puedan establecer sesiones en System Manager de SANtricity. El banner puede incluir un aviso de asesoría y un mensaje de consentimiento.

Acerca de esta tarea

Al crear un banner, este aparece antes de la pantalla de inicio de sesión en un cuadro de diálogo.

Pasos

1. Seleccione MENU:Settings[System].
2. En la sección **General**, seleccione **Configurar banner de inicio de sesión**.

   Se abre el cuadro de diálogo **Configurar banner de inicio de sesión**.

3. Introduzca el texto que desea que aparezca en el banner de inicio de sesión.

   No use formato HTML ni otras etiquetas de marcado.

4. Haga clic en **Guardar**.

Resultado

La próxima vez que los usuarios inicien sesión en System Manager, el texto se abrirá en un cuadro de diálogo. Los usuarios deben hacer clic en **Aceptar** para continuar con la pantalla de inicio de sesión.

Gestionar los tiempos de espera de sesión

Es posible configurar los tiempos de espera en SANtricity System Manager para que las sesiones inactivas de los usuarios se desconecten después de un periodo especificado.

Acerca de esta tarea

De manera predeterminada, el tiempo de espera de sesión para System Manager es de 30 minutos. Es posible ajustar el tiempo, o bien directamente pueden deshabilitarse los tiempos de espera de sesión.

Si se configura Access Management con las funcionalidades del lenguaje de marcado de aserción de seguridad (SAML) integradas en la cabina, es posible que se agote el tiempo de espera de sesión cuando la sesión SSO del usuario alcance su límite máximo. Esto puede ocurrir antes del tiempo de espera de sesión de System Manager.

Pasos

1. Seleccione MENU:Settings[System].

2. En la sección **General**, seleccione **Habilitar/deshabilitar tiempo de espera de la sesión**.

   Se abre el cuadro de diálogo **Activar/Desactivar tiempo de espera de sesión**.

3. Utilice los controles de desplazamiento para aumentar o disminuir el tiempo en minutos.

   El tiempo de espera mínimo que puede configurarse para System Manager es de 15 minutos.

   > Para desactivar los tiempos de espera de sesiones, anule la selección de la casilla de verificación **establecer el lapso…**.

4. Haga clic en **Guardar**.

Modifique la configuración de caché para la cabina de almacenamiento

Se puede ajustar la configuración de la memoria caché para el vaciado y el tamaño del bloque de todos los volúmenes de la cabina de almacenamiento.

Acerca de esta tarea

La memoria caché es un área de almacenamiento volátil temporal en la controladora que tiene un tiempo de acceso más rápido que la unidad. Para ajustar el rendimiento de la caché, se pueden modificar las siguientes opciones de configuración:

Configuración de caché	Descripción
Inicio de vaciado de caché bajo demanda	La opción Iniciar purga de caché según demanda especifica el porcentaje de datos sin escribir de la caché que activan el vaciado de caché (escritura en disco). De forma predeterminada, el vaciado de caché comienza cuando los datos sin escribir alcanzan un 80 % de la capacidad. Un porcentaje mayor es una buena opción en entornos que tienen principalmente operaciones de escritura, de manera que las solicitudes de escritura nuevas se pueden procesar mediante la caché sin tener que ir al disco. Los valores de configuración más bajos son mejores para los entornos con operaciones de I/o erráticas (con ráfagas de datos), de manera que el sistema vacía la caché con frecuencia entre las ráfagas de datos. No obstante, un porcentaje inicial inferior al 80 % puede disminuir el rendimiento.

Configuración de caché	Descripción
Tamaño del bloque de caché	El tamaño de bloque de la caché determina el tamaño máximo de cada bloque de la caché, que es una unidad organizativa para la gestión de la caché. De manera predeterminada, el tamaño de bloque es de 8 KiB. System Manager permite un tamaño de bloque de caché de 4, 8, 16 o 32 KiBs. Las aplicaciones utilizan distintos tamaños de bloques, que pueden afectar al rendimiento del almacenamiento. Un tamaño menor es una buena opción para los sistemas de archivos o las aplicaciones de bases de datos. Un tamaño mayor es ideal para aplicaciones que generan operaciones de I/o secuenciales, por ejemplo, multimedia.

Pasos

1. Seleccione MENU:Settings[System].
2. Desplácese hacia abajo hasta **Configuración adicional** y, a continuación, haga clic en **Cambiar configuración de caché**.

   Se abre el cuadro de diálogo Cambiar configuración de caché.

3. Ajuste los siguientes valores:
   - Iniciar purga de caché según demanda: Elija un porcentaje adecuado para la I/o que se utiliza en el entorno. Si elige un valor inferior a 80 %, es posible que note una disminución de rendimiento.
   - Tamaño del bloque de caché — Seleccione un tamaño que sea adecuado para sus aplicaciones.
4. Haga clic en **Guardar**.

Establezca la generación de informes de conectividad de host

Es posible habilitar la generación de informes de conectividad de host para que la cabina de almacenamiento supervise constantemente la conexión entre las controladoras y los hosts configurados, y emita alertas si se interrumpe la conexión. Esta función está habilitada de forma predeterminada.

Acerca de esta tarea

Si se deshabilita la generación de informes de conectividad de host, el sistema ya no supervisa la conectividad ni los problemas de los controladores multivía con un host conectado a la cabina de almacenamiento.

> Al deshabilitar la generación de informes de conectividad de host, también se deshabilita el equilibrio de carga automático que supervisa y equilibra la utilización de recursos de la controladora.

Pasos

1. Seleccione MENU:Settings[System].
2. Desplácese hasta **Configuración adicional** y, a continuación, haga clic en **Activar/Desactivar generación de informes de conectividad de host**.

El texto debajo de esta opción indica si se encuentra habilitada o deshabilitada.

Se mostrará un cuadro de diálogo de confirmación.

3. Haga clic en **Sí** para continuar.

   Al seleccionar esta opción, es posible alternar entre habilitar o deshabilitar la función.

Establecer equilibrio de carga automático

La función **equilibrio de carga automático** garantiza que el tráfico de E/S entrante de los hosts se gestione dinámicamente y se equilibre entre ambas controladoras. Esta función está habilitada de forma predeterminada, pero se puede deshabilitar desde System Manager.

Acerca de esta tarea

Cuando la función Automatic Load Balancing está habilitada, ejecuta las siguientes funciones:

- Supervisa y equilibra automáticamente la utilización de recursos de la controladora.
- Ajusta automáticamente la propiedad de la controladora de volumen cuando es necesario y así, optimiza el ancho de banda de I/o entre los hosts y la cabina de almacenamiento.

Puede ser conveniente deshabilitar Automatic Load Balancing en la cabina de almacenamiento por las siguientes razones:

- No se desea cambiar automáticamente la propiedad de una controladora de volumen para equilibrar la carga de trabajo.
- Se trabaja en un entorno altamente optimizado donde la distribución de carga se configura intencionalmente para lograr una distribución específica entre las controladoras.

Pasos

1. Seleccione MENU:Settings[System].
2. Desplácese hasta **Configuración adicional** y, a continuación, haga clic en **Habilitar/deshabilitar equilibrio de carga automático**.

   El texto debajo de esta opción indica si la función se encuentra habilitada o deshabilitada.

   Se mostrará un cuadro de diálogo de confirmación.

3. Confirme haciendo clic en **Sí** para continuar.

   Al seleccionar esta opción, es posible alternar entre habilitar o deshabilitar la función.

> Cuando esta función pasa de estar deshabilitada a habilitada, también se habilita la función Host Connectivity Reporting.

Cambiar el tipo de host predeterminado

Use la opción de configuración Cambiar el sistema operativo del host predeterminado para cambiar el tipo de host predeterminado en el nivel de la cabina de almacenamiento.

En general, se debe cambiar el tipo de host predeterminado antes de conectar hosts a la cabina de almacenamiento o al añadir hosts adicionales.

Acerca de esta tarea

Tenga en cuenta estas directrices:

- Si todos los hosts que piensa conectar a la cabina de almacenamiento tienen el mismo sistema operativo (entorno de host homogéneo), cambie el tipo de host para que coincida con el sistema operativo.
- Si hay hosts con diferentes sistemas operativos que piensa conectar a la cabina de almacenamiento (entorno de host heterogéneo), cambie el tipo de host para que coincida con la mayoría de los sistemas operativos de los hosts.

  Por ejemplo, si va a conectar ocho hosts diferentes a la cabina de almacenamiento y seis de ellos tienen un sistema operativo Windows, debe seleccionar Windows como tipo de sistema operativo de host predeterminado.

- Si la mayoría de los hosts conectados poseen una combinación de sistemas operativos diferentes, cambie el tipo de host a opción predeterminada de fábrica.

  Por ejemplo, si va a conectar ocho hosts diferentes a la cabina de almacenamiento y dos de ellos tienen un sistema operativo Windows, tres tienen HP-UX, Y otros tres ejecutan un sistema operativo Linux, debe seleccionar opción predeterminada de fábrica como el tipo de sistema operativo del host predeterminado.

Pasos

1. Seleccione MENU:Settings[System].
2. Desplácese hasta **Configuración adicional** y, a continuación, haga clic en **Cambiar el tipo de sistema operativo del host** predeterminado.
3. Seleccione el tipo de sistema operativo de host que desea usar como predeterminado.
4. Haga clic en **Cambiar**.

Habilitar o deshabilitar la interfaz de gestión heredada

Es posible habilitar o deshabilitar la interfaz de gestión heredada (Symbol), que es un método de comunicación entre la cabina de almacenamiento y el cliente de gestión. De manera predeterminada, la interfaz de gestión heredada está activada. Si se desactiva, la cabina de almacenamiento y su cliente de gestión utilizan un método más seguro de comunicación (API DE REST a través de https); sin embargo, ciertas herramientas y tareas pueden verse afectadas si se deshabilita la cabina.

Acerca de esta tarea

La configuración afecta a las operaciones de la siguiente manera:

- **Activado** (predeterminado): Es la configuración necesaria para la duplicación, para los comandos de la CLI que funcionan sólo en las matrices de almacenamiento E5700 y E5600, y para otras herramientas como la utilidad QuickConnect y el adaptador OCI.
- **Off** — Configuración requerida para reforzar la confidencialidad en las comunicaciones entre la matriz de almacenamiento y el cliente de administración, y para acceder a herramientas externas. Opción recomendada para configurar un servidor de directorio (LDAP).

Pasos

1. Seleccione MENU:Settings[System].
2. Desplácese hacia abajo hasta **Configuración adicional** y, a continuación, haga clic en **Cambiar interfaz de administración**.
3. En el cuadro de diálogo, haga clic en **Sí** para continuar.

Preguntas frecuentes

¿Qué es la caché de la controladora?

La caché de la controladora es un espacio de memoria física que optimiza dos tipos de operaciones de I/o (entrada/salida): Entre las controladoras y los hosts, y entre las controladoras y los discos.

En el caso de las transferencias de datos de lectura y escritura, los hosts y las controladoras se comunican a través de conexiones de alta velocidad. Sin embargo, la comunicación del back-end de la controladora a los discos es más lenta debido a que los discos son dispositivos relativamente lentos.

Cuando la caché de la controladora recibe los datos, la controladora reconoce qué aplicaciones host son las que ahora tienen los datos. De este modo, las aplicaciones host no necesitan esperar a que se escriban las operaciones de I/o en el disco. En cambio, las aplicaciones pueden continuar con sus operaciones. Los datos en caché también están a disposición de las aplicaciones de servidor, lo que elimina la necesidad de lecturas adicionales del disco para acceder a los datos.

La caché de la controladora afecta al rendimiento general de la cabina de almacenamiento de diversas maneras:

- La caché actúa como un búfer, de modo que las transferencias de datos entre disco y host no necesitan sincronizarse.
- Los datos de una operación de escritura o lectura del host pueden estar en caché desde una operación anterior, lo que elimina la necesidad de acceder al disco.
- Si se utiliza el almacenamiento en caché de escritura, el host puede enviar comandos de escritura posteriores antes de que los datos de una operación de escritura anterior se escriban en el disco.
- Si la captura previa de caché está habilitada, el acceso de lectura secuencial se optimiza. La captura previa de caché hace que una operación de lectura tenga más probabilidades de encontrar los datos en la caché, en lugar de leer los datos del disco.

> **Posible pérdida de datos** — Si activa la opción **almacenamiento en caché de escritura sin baterías** y no dispone de una fuente de alimentación universal de protección, podría perder datos. Además, puede perder datos si no tiene baterías de controlador y activa la opción **almacenamiento en caché de escritura sin baterías**.

¿Qué es el vaciado de la caché?

Cuando la cantidad de datos no guardados que se encuentra en la caché llega a cierto nivel, la controladora guarda periódicamente en una unidad los datos en caché. Este proceso de guardado se denomina "vaciado".

La controladora utiliza dos algoritmos para vaciar la caché: En función de la demanda y en función de la antigüedad. La controladora utiliza un algoritmo en función de la demanda hasta que la cantidad de datos en caché desciende por debajo del umbral de vaciado de caché. De manera predeterminada, un vaciado

comienza cuando está en uso el 80 % de la caché.

En System Manager, puede configurar el umbral «Iniciar purga de caché a demanda» para que admita mejor el tipo de I/o utilizado en su entorno. En un entorno principalmente compuesto por operaciones de escritura, debe establecer un porcentaje alto de «Iniciar purga de caché de demanda» para aumentar la probabilidad de que cualquier solicitud de escritura nueva se pueda procesar mediante la caché sin tener que ir al disco. La configuración de un porcentaje alto limita la cantidad de vaciados de caché a fin de que más datos permanezcan en la caché, lo que aumenta la posibilidad de más aciertos en caché.

En un entorno en el que las operaciones de I/o son erráticas (con picos de datos), es posible utilizar un vaciado de caché bajo para que el sistema vacíe la caché con frecuencia entre los picos de datos. En un entorno diverso de operaciones de I/o que procesa diferentes cargas, o cuando se desconoce el tipo de cargas, se puede configurar un umbral del 50 % como un buen punto de partida intermedio. Tenga en cuenta que, si selecciona un porcentaje de inicio inferior al 80 %, es posible que disminuya el rendimiento, ya que los datos necesarios para la lectura del host pueden no estar disponibles. Además, un porcentaje más bajo también aumenta la cantidad de escrituras de disco necesarias para mantener el nivel de caché, lo que aumenta la sobrecarga del sistema.

El algoritmo en función de la antigüedad especifica el periodo durante el cual los datos de escritura pueden permanecer en la caché antes de calificar para el vaciamiento a los discos. Las controladoras utilizan el algoritmo en función de la antigüedad hasta que se alcanza el umbral de vaciado de caché. El valor predeterminado es de 10 segundos, pero este lapso se considera solo en periodos de inactividad. No es posible modificar la configuración de tiempo de vaciado desde System Manager; en cambio, se debe utilizar el comando Set Storage Array en la interfaz de línea de comandos (CLI).

Posible pérdida de datos — Si activa la opción **almacenamiento en caché de escritura sin baterías** y no dispone de una fuente de alimentación universal de protección, podría perder datos. Además, puede perder datos si no tiene baterías de controlador y activa la opción **almacenamiento en caché de escritura sin baterías**.

¿Qué es el tamaño de bloque de caché?

La controladora de la cabina de almacenamiento organiza su caché en "bloques", que son fragmentos de memoria que pueden tener un tamaño de 4, 8, 16 o 32 KiBs. Todos los volúmenes del sistema de almacenamiento comparten el mismo espacio de caché; por lo tanto, los volúmenes solo pueden tener un tamaño de bloque de caché.

Los bloques de caché no son lo mismo que los bloques de 512 bytes que utiliza el sistema de bloques lógicos de los discos.

Las aplicaciones utilizan diferentes tamaños de bloque, lo que puede afectar el rendimiento del almacenamiento. De manera predeterminada, el tamaño de bloque en System Manager es 8 KiB, pero se puede modificar el valor a 4, 8, 16 o 32 KiBs. Un tamaño menor es una buena opción para los sistemas de archivos o las aplicaciones de bases de datos. Un tamaño mayor es una buena opción para aplicaciones que requieren grandes transferencias de datos, operaciones de I/o secuenciales o alto ancho de banda, como las aplicaciones multimedia.

¿Cuándo se deben sincronizar los relojes de la cabina de almacenamiento?

Se deben sincronizar manualmente los relojes de las controladoras en la cabina de almacenamiento si se observa que las marcas de tiempo que se muestran en System Manager no están alineadas con las marcas de tiempo del cliente de gestión (el

ordenador que accede a System Manager por medio del explorador). Esta tarea es necesaria solo si no se habilitó el protocolo de tiempo de redes (NTP) en System Manager.

> Se recomienda enfáticamente utilizar un servidor NTP en lugar de sincronizar manualmente los relojes. NTP sincroniza automáticamente los relojes con un servidor externo que utiliza el protocolo de tiempo de redes simple (SNTP).

Se puede comprobar el estado de sincronización desde el cuadro de diálogo **Sincronizar relojes de cabinas de almacenamiento**, que se encuentra disponible en la página sistema. Si las horas que aparecen en el cuadro de diálogo no coinciden, ejecute una sincronización. Puede ver este cuadro de diálogo periódicamente y verificar si las horas que muestran los relojes de las controladoras se distanciaron y ya no están sincronizadas.

¿Qué es la generación de informes de conectividad de host?

Cuando la opción de generación de informes de conectividad de host está habilitada, la cabina de almacenamiento supervisa continuamente la conexión entre las controladoras y los hosts configurados, y luego notifica si se interrumpió la conexión.

Pueden producirse interrupciones en la conexión si hay algún cable suelto, dañado o faltante, o si hay otro problema con el host. En estas situaciones, es posible que el sistema abra un mensaje de Recovery Guru:

- **Pérdida de redundancia del host** — se abre si alguno de los controladores no puede comunicarse con el host.
- **Tipo de host incorrecto** — se abre si el tipo de host se ha especificado incorrectamente en la matriz de almacenamiento, lo que podría dar lugar a problemas de conmutación por error.

Puede ser conveniente deshabilitar la generación de informes de conectividad de host cuando la operación de reinicio de una controladora puede demorar más que el tiempo de espera de conexión. Cuando se deshabilita esta función, se suprimen los mensajes de Recovery Guru.

> Además, al deshabilitar la generación de informes de conectividad de host también se deshabilita el equilibrio de carga automático, que supervisa y equilibra el uso de recursos de la controladora. Sin embargo, si se vuelve a habilitar la generación de informes de conectividad de host, la función de equilibrio de carga automático no se vuelve a habilitar automáticamente.

Configuración de iSCSI

Conceptos

Terminología de iSCSI

Conozca la forma en que los términos de iSCSI se aplican a su cabina de almacenamiento.

Duración	Descripción
CHAP	El método de protocolo de autenticación por desafío mutuo (CHAP) valida la identidad de destinos e iniciadores durante el enlace inicial. La autenticación se basa en una clave de seguridad compartida denominada CHAP*secret*__.
Controladora	Una controladora consta de una placa, un firmware y un software. Controla las unidades e implementa las funciones de System Manager.
DHCP	El protocolo de configuración dinámica de hosts (DHCP) es un protocolo que se usa en las redes de protocolo de Internet (IP) para los parámetros de configuración de red de distribución dinámica, como las direcciones IP.
IB	InfiniBand (IB) es una norma de comunicación para la transmisión de datos entre servidores de alto rendimiento y sistemas de almacenamiento.
Respuesta ICMP PING	El protocolo de mensajes de control de Internet (ICMP) es un protocolo que usan los sistemas operativos de ordenadores conectados a una red para enviar mensajes. Los mensajes ICMP determinan si se puede acceder a un host y cuánto tiempo lleva trasladar paquetes desde o hacia ese host.
IQN	Un identificador de nombre completo de iSCSI (IQN) es un nombre único para un iniciador de iSCSI o un destino iSCSI.
Iser	Las extensiones de iSCSI para RDMA (Iser) conforman un protocolo que extiende el protocolo iSCSI para operaciones a través de transporte RDMA, como InfiniBand o Ethernet.
ISNS	El servicio de nombres de almacenamiento de Internet (iSNS) es un protocolo que permite la detección, gestión y configuración automatizada de dispositivos iSCSI y Fibre Channel en redes TCP/IP.
Dirección MAC	Ethernet utiliza identificadores de control de acceso de medios (direcciones MAC) para distinguir entre canales lógicos distintos que conectan dos puertos en la misma interfaz de red de transporte físico.
Cliente de gestión	Un cliente de gestión es el equipo donde se instala un explorador para acceder a System Manager.
MTU	Una unidad de transmisión máxima (MTU) es el paquete o el marco de mayor tamaño que se pueden enviar en una red.
RDMA	El acceso directo a memoria remota (RDMA) es una tecnología que les permite a los equipos en red intercambiar datos en la memoria principal sin la participación del sistema operativo de ninguno de los equipos.
Sesión de detección sin nombre	Cuando se habilita la opción de sesiones de detección sin nombre, no se requiere que los iniciadores de iSCSI especifiquen el IQN objetivo para recuperar la información de la controladora.

Procedimientos

Configure los puertos iSCSI

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

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).

Acerca de esta tarea

En esta tarea, se describe cómo acceder a la configuración del puerto iSCSI desde la página hardware. También puede acceder a la configuración desde la página sistema (menú:Configuración[sistema]).

> 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 **Mostrar parte posterior de la bandeja**.

   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 opciones de configuración de puertos, haga clic en el enlace Mostrar más opciones de puerto que se encuentra a la derecha del cuadro de diálogo.

Detalles del campo

Opción de configuración de puertos	Descripción
Habilite IPv4/Habilitar IPv6	Seleccione una o ambas opciones para habilitar la compatibilidad con las redes IPv4 e IPv6. NOTA: Si desea desactivar el acceso al puerto, anule la selección de las dos casillas de verificación.
Puerto de escucha TCP (disponible cuando se hace 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 cuando se hace 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 Habilitar IPv4, se abre un cuadro de diálogo para seleccionar la configuración de IPv4 después de hacer clic en Siguiente. Si seleccionó Habilitar IPv6, se abre un cuadro de diálogo para seleccionar la configuración de IPv6 después de hacer clic en Siguiente. Si seleccionó ambas opciones, se abre primero el cuadro de diálogo de configuración de 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.
Habilite la compatibilidad con VLAN (disponible cuando se hace 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.
Habilite la prioridad de ethernet (disponible cuando haga clic en Mostrar más opciones)	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**.

Configure la autenticación iSCSI

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 para 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**.

Resultado

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.

Habilite la configuración de detección de iSCSI

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**.

   Aparece el cuadro de diálogo **Configuración de detección de objetivos**. Debajo del servidor Habilitar 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 — "Vendor Specific Information". 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**.

Resultado

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 de iSCSI

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.

- **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.
- **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.

Finalice la sesión iSCSI

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 menú:ficha Soporte[Centro de soporte > Diagnóstico].
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.

Ver sesiones iSCSI

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 menú:ficha Soporte[Centro de soporte > Diagnóstico].
2. Seleccione **Ver/finalizar sesiones iSCSI**.

   Se muestra una lista de las sesiones iSCSI actuales.

3. Para ver información adicional sobre 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 Ethernet	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. 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`.

Configure los puertos Iser over InfiniBand

Si la controladora tiene un puerto Iser over InfiniBand, se puede configurar la conexión de red al host. Las opciones de configuración están disponibles en las páginas hardware o sistema.

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.

Acerca de esta tarea

Es posible acceder a la configuración de Iser over InfiniBand desde la página **hardware** o desde el menú:Configuración[sistema]. En esta tarea se describe cómo configurar los puertos desde la página **hardware**.

> La configuración y las funciones de Iser over InfiniBand aparecen solamente si la controladora de la cabina de almacenamiento contiene un puerto Iser over InfiniBand.

Pasos

1. Seleccione **hardware**.
2. Si el gráfico muestra las unidades, haga clic en **Mostrar parte posterior de la bandeja**.

   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 over InfiniBand

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.

Es posible acceder a estadísticas de Iser over InfiniBand desde la página sistema (MENU:Settings[System]) o desde la página Soporte. Estas instrucciones describen cómo acceder a las estadísticas desde la página Soporte.

Pasos

1. Seleccione menú:ficha Soporte[Centro de soporte > Diagnóstico].
2. Seleccione **Ver estadísticas de Iser over InfiniBand**.
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 Iser over InfiniBand.

Preguntas frecuentes

¿Qué sucede cuando utilizo un servidor iSNS para el registro?

Cuando se utiliza información del servidor de servicio de nombres de almacenamiento de Internet (iSNS), los hosts (iniciadores) pueden configurarse para consultar el servidor iSNS a fin de recuperar información del objetivo (controladoras).

Este registro proporciona al servidor iSNS la información del puerto y del nombre completo de iSCSI (IQN) de la controladora, y permite consultas entre los iniciadores (hosts iSCSI) y los objetivos (controladoras).

¿Qué métodos de registro se admiten automáticamente para iSCSI?

La implementación de iSCSI es compatible con el método de detección Servicio de nombres de almacenamiento de Internet (iSNS) o con el uso del comando Send Targets.

El método iSNS permite la detección iSNS entre los iniciadores (hosts iSCSI) y los objetivos (controladoras). La controladora objetivo se registra para proporcionar al servidor iSNS la información sobre el puerto y el nombre completo de iSCSI (IQN) de la controladora.

Si no se configura iSNS, el host iSCSI puede enviar el comando Send Targets durante una sesión de detección iSCSI. En respuesta, la controladora devuelve la información del puerto (por ejemplo, el IQN objetivo, la dirección IP del puerto, el puerto de escucha y el grupo de puertos de destino). Este método de detección no es necesario si utiliza iSNS, dado que el iniciador del host puede recuperar las IP objetivo del servidor iSNS.

¿Cómo se interpretan las estadísticas de Iser over InfiniBand?

El cuadro de diálogo **Ver estadísticas de Iser over InfiniBand** muestra las estadísticas de destino local (protocolo) y las estadísticas de la interfaz Iser over InfiniBand (IB). 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 over InfiniBand 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.

¿Qué más debo hacer para configurar o diagnosticar Iser over InfiniBand?

En la tabla a continuación, se enumeran las funciones de System Manager que se pueden utilizar para configurar y gestionar sesiones Iser over InfiniBand.

> La configuración de Iser over InfiniBand solo está disponible si la controladora de la cabina de almacenamiento incluye un puerto de gestión de hosts Iser over InfiniBand.

Configure y diagnostique Iser over InfiniBand

Acción	Ubicación
Configure los puertos Iser over InfiniBand	1. Seleccione **hardware**. 2. Seleccione **Mostrar parte posterior de la bandeja**. 3. Seleccione una controladora. 4. Seleccione **Configurar puertos Iser over InfiniBand**. o. 1. Seleccione MENU:Settings[System]. 2. Desplácese hasta **Configuración de Iser over InfiniBand** y seleccione **Configurar puertos Iser over InfiniBand**.
Ver estadísticas de Iser over InfiniBand	1. Seleccione MENU:Settings[System]. 2. Desplácese hasta **Configuración de Iser over InfiniBand** y seleccione **Ver estadísticas de Iser over InfiniBand**.

Sistema: Configuración de NVMe

Conceptos

Información general de NVMe

Algunas controladoras incluyen un puerto para complementar NVMe (Non-Volatile Memory Express) sobre una estructura InfiniBand o sobre una estructura roce (RDMA over Converged Ethernet). NVMe permite una comunicación de alto rendimiento entre los hosts y la cabina de almacenamiento.

¿Qué es NVMe?

NVM significa "memoria no volátil", y es una memoria persistente utilizada en muchos tipos de dispositivos de almacenamiento. *NVMe* (NVM Express) es una interfaz o un protocolo estandarizados diseñados específicamente para la comunicación de varias colas de alto rendimiento con dispositivos NVM.

¿Qué es NVMe over Fabrics?

NVMe over Fabrics (NVMe-of) es una especificación de tecnología que permite la transferencia de datos y comandos basados en mensajes de NVMe entre un equipo host y un almacenamiento a través de una red. Con la versión de SANtricity OS 11.40 y posteriores, es posible acceder a una cabina de almacenamiento NVMe (que se denomina *SUBSYSTEM*) a través de un host con una estructura InfiniBand o RDMA. Los comandos NVMe se habilitan y se encapsulan en capas de abstracción de transporte en el lado del host y del subsistema. Esto extiende la interfaz NVMe integral de alto rendimiento desde el host hasta el almacenamiento, además de estandarizar y simplificar el conjunto de comandos.

El almacenamiento NVMe-of se presenta a un host como dispositivo de almacenamiento basado en bloques local. El volumen (que se denomina *Namespace*) puede montarse en un sistema de archivos, como sucede con cualquier otro dispositivo de almacenamiento en bloques. Es posible usar la API de REST, la SMcli o SANtricity System Manager para aprovisionar el almacenamiento según sea necesario.

¿Qué es un nombre completo de NVMe (NQN)?

El nombre completo de NVMe (NQN) se utiliza para identificar el destino de almacenamiento remoto. El nombre completo de NVMe para la cabina de almacenamiento siempre es una asignación del subsistema que no puede modificarse. Hay un solo nombre completo de NVMe para toda la cabina. El nombre completo de NVMe se limita a 223 caracteres de longitud. Es posible compararlo con un nombre completo de iSCSI.

¿Qué es un espacio de nombres y un identificador de espacio de nombres?

Un espacio de nombres es el equivalente a una unidad lógica en SCSI, que está relacionada con un volumen en la cabina. El identificador de espacio de nombres (NSID) es equivalente a un número de unidad lógica (LUN) en SCSI. Es posible crear el NSID en el momento de la creación del espacio de nombres, y configurarlo con un valor entre 1 y 255.

¿Qué es una controladora NVMe?

Como un SCSI I_T nexus, que representa la ruta desde el iniciador del host hasta el objetivo del sistema de almacenamiento, una controladora NVMe creada durante el proceso de conexión del host ofrece una ruta de acceso entre un host y los espacios de nombres en la cabina de almacenamiento. Un NQN para el host más un identificador de puerto de host identifican de manera única una controladora NVMe. Si bien una controladora NVMe solo puede asociarse con un solo host, puede acceder a varios espacios de nombres.

Es posible configurar los hosts que pueden acceder a determinados espacios de nombres y configurar el identificador de espacio de nombres para el host con SANtricity System Manager. A continuación, cuando se crea la controladora NVMe, esta puede acceder a la lista de identificadores de espacio de nombres creada y utilizada para configurar las conexiones permitidas.

Terminología de NVMe

Conozca la forma en que los términos de NVMe se aplican a su cabina de almacenamiento.

Duración	Descripción
Estructura	InfiniBand (IB) es una norma de comunicación para la transmisión de datos entre servidores de alto rendimiento y sistemas de almacenamiento.
Espacio de nombres	Un espacio de nombres es almacenamiento NVM que se formateó para el acceso en bloque. Es análogo a una unidad lógica en SCSI, que se relaciona con un volumen en la cabina de almacenamiento.
Identificador de espacio de nombres	El ID del espacio de nombres es el identificador único de la controladora NVMe para el espacio de nombres y se puede configurar con un valor entre 1 y 255. Es análogo a un número de unidad lógica (LUN) en SCSI.
NQN	El nombre completo de NVMe (NQN) se utiliza para identificar el destino de almacenamiento remoto (la cabina de almacenamiento).
NVM	La memoria no volátil (NVM) es la memoria persistente utilizada en muchos tipos de dispositivos de almacenamiento.

Duración	Descripción
NVMe	La memoria no volátil rápida (NVMe) es una interfaz designada para dispositivos de almacenamiento basados en flash, por ejemplo, unidades SSD. NVMe reduce la sobrecarga de I/o e incluye mejoras de rendimiento, en comparación con las interfaces de dispositivos lógicos anteriores.
NVMe-of	La memoria no volátil rápida sobre estructuras (NVMe-of) es una especificación que permite el funcionamiento de comandos y la transferencia de datos de NVMe en una red entre un host y el almacenamiento.
Controladora NVMe	Se crea una controladora NVMe durante el proceso de conexión del host. Esta ofrece una ruta de acceso entre un host y los espacios de nombres en la cabina de almacenamiento.
Cola NVMe	Una cola que se utiliza para pasar comandos y mensajes a través de la interfaz de NVMe.
Subsistema NVMe	La cabina de almacenamiento con una conexión NVMe.
RDMA	El acceso remoto a memoria directa (RDMA) permite un movimiento de datos más directo hacia y desde un servidor gracias a la implementación de un protocolo de transporte en el hardware de la tarjeta de interfaz de red (NIC).
Roce	RDMA over Converged Ethernet (roce) es un protocolo de red que permite el acceso remoto a memoria directa (RDMA) sobre una red Ethernet.
SSD	Los discos de estado sólido (SSD) son dispositivos de almacenamiento de datos que usan memoria de estado sólido (flash) para almacenar datos en forma persistente. Los SSD emulan las unidades de discos duros convencionales y están disponibles con las mismas interfaces que usan las unidades de disco duro.

Procedimientos

Configure los puertos NVMe over InfiniBand

Si la controladora incluye una conexión NVMe over InfiniBand, los ajustes del puerto NVMe se pueden configurar desde la página hardware o la página sistema.

Antes de empezar

- La controladora debe incluir un puerto de host NVMe over InfiniBand; de lo contrario, los ajustes de NVMe over InfiniBand no estarán disponibles en System Manager.
- Se debe conocer la dirección IP de la conexión de host.

Acerca de esta tarea

Es posible acceder a la configuración de NVMe over InfiniBand desde la página **hardware** o desde el menú:Configuración[sistema]. En esta tarea se describe cómo configurar los puertos desde la página **hardware**.

La configuración y las funciones de NVMe over InfiniBand aparecen solamente si la controladora de la cabina de almacenamiento contiene un puerto NVMe over InfiniBand.

Pasos

1. Seleccione **hardware**.
2. Si el gráfico muestra las unidades, haga clic en **Mostrar parte posterior de la bandeja**.

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

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

   Aparece el menú contextual de la controladora.

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

   Se abre el cuadro de diálogo **Configurar puertos NVMe 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. Una vez terminada la configuración, haga clic en **Sí** para reiniciar el puerto NVMe over InfiniBand.

Configure los puertos NVMe over roce

Si la controladora incluye una conexión para NVMe over roce (RDMA over Converged Ethernet), es posible configurar las opciones del puerto NVMe desde la página hardware o la página sistema.

Antes de empezar

- La controladora debe incluir un puerto de host NVMe over roce; de lo contrario, los ajustes de NVMe over roce no estarán disponibles en System Manager.
- Se debe conocer la dirección IP de la conexión de host.

Acerca de esta tarea

Es posible acceder a la configuración de NVMe over roce desde la página **hardware** o desde el menú:Configuración[sistema]. En esta tarea, se describe cómo configurar los puertos desde la página hardware.

La configuración y las funciones de NVMe over roce aparecen solamente si la controladora de la cabina de almacenamiento contiene un puerto NVMe over roce.

Pasos

1. Seleccione **hardware**.
2. Si el gráfico muestra las unidades, haga clic en **Mostrar parte posterior de la bandeja**.

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

3. Haga clic en la controladora que tenga el puerto NVMe over roce que desea configurar.

   Aparece el menú contextual de la controladora.

4. Seleccione **Configurar puertos NVMe over roce**.

   Se abre el cuadro de diálogo Configurar puertos NVMe over roce.

5. En la lista desplegable, seleccione el puerto HIC que desea configurar.
6. 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 de puerto ethernet configurada	Seleccione la velocidad que coincida que la capacidad de velocidad del SFP en el puerto.
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.
Tamaño de MTU (disponible cuando se hace 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.

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

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.

8. Haga clic en **Finalizar**.

Ver estadísticas de NVMe over Fabrics

Es posible ver datos acerca de las conexiones NVMe over Fabrics a la cabina de almacenamiento.

Acerca de esta tarea

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

- **Estadísticas del subsistema NVMe** — se muestran estadísticas para la controladora NVMe, que incluyen tiempos de espera y fallos de conexión.
- **Estadísticas de la interfaz RDMA** — proporciona estadísticas para la interfaz RDMA, incluyendo información de paquetes recibidos y transmitidos.

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.

Es posible acceder a estadísticas de NVMe over Fabrics desde las páginas sistema (MENU:Settings[System]) o Soporte. Estas instrucciones describen cómo acceder a las estadísticas desde la página Soporte.

Pasos

1. Seleccione menú:ficha Soporte[Centro de soporte > Diagnóstico].
2. Seleccione **Ver estadísticas de NVMe over Fabrics**.
3. 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. Se usa la misma línea de base para todas las estadísticas de NVMe.

Preguntas frecuentes

¿Cómo se interpretan las estadísticas de NVMe over InfiniBand?

El cuadro de diálogo **Ver estadísticas de NVMe over Fabrics** muestra estadísticas para el subsistema NVMe y la interfaz de NVMe over InfiniBand. Todas las estadísticas son de solo lectura y no pueden configurarse.

- **Estadísticas del subsistema NVMe** — muestra estadísticas para la controladora NVMe y su cola. La controladora NVMe ofrece una ruta de acceso entre un host y los espacios de nombres en la cabina de almacenamiento. Es posible revisar las estadísticas del subsistema NVMe para consultar elementos, como errores de conexión, reinicios y apagados. Para obtener más información sobre estas estadísticas, haga clic en **Ver leyenda de encabezados de tabla**.
- **Estadísticas de la interfaz RDMA** — proporciona estadísticas para todos los puertos NVMe over Fabrics de la interfaz RDMA, que incluye estadísticas de rendimiento e información de errores de enlace asociados con cada puerto del switch. Para obtener más información sobre las estadísticas, haga clic en **Ver leyenda de encabezados de tabla**.

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.

¿Cómo se interpretan las estadísticas de NVMe over Fabrics?

El cuadro de diálogo **Ver estadísticas de NVMe over Fabrics** muestra estadísticas para el subsistema NVMe y la interfaz de NVMe over roce. Todas las estadísticas son de solo lectura y no pueden configurarse.

- **Estadísticas del subsistema NVMe** — muestra estadísticas para la controladora NVMe y su cola. La controladora NVMe ofrece una ruta de acceso entre un host y los espacios de nombres en la cabina de almacenamiento. Es posible revisar las estadísticas del subsistema NVMe para consultar elementos, como errores de conexión, reinicios y apagados. Para obtener más información sobre estas estadísticas, haga clic en **Ver leyenda de encabezados de tabla**.
- **Estadísticas de la interfaz RDMA** — proporciona estadísticas para todos los puertos NVMe over Fabrics de la interfaz RDMA, que incluye estadísticas de rendimiento e información de errores de enlace asociados con cada puerto del switch. Para obtener más información sobre las estadísticas, haga clic en **Ver leyenda de encabezados de tabla**.

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.

¿Qué más debo hacer para configurar o diagnosticar NVMe over InfiniBand?

En la tabla a continuación, se enumeran las funciones de System Manager que se pueden utilizar para configurar y gestionar sesiones NVMe over InfiniBand.

> La configuración de NVMe over InfiniBand solo está disponible si la controladora de la cabina de almacenamiento incluye un puerto NVMe over InfiniBand.

Configure y diagnostique NVMe over InfiniBand

Acción	Ubicación
Configure los puertos NVMe over InfiniBand	1. Seleccione **hardware**. 2. Seleccione **Mostrar parte posterior de la bandeja**. 3. Seleccione una controladora. 4. Seleccione **Configurar puertos NVMe over InfiniBand**. o. 1. Seleccione MENU:Settings[System]. 2. Desplácese hasta **Configuración de NVMe over InfiniBand** y seleccione **Configurar puertos NVMe over InfiniBand**.
Ver estadísticas de NVMe over InfiniBand	1. Seleccione MENU:Settings[System]. 2. Desplácese hasta **Configuración de NVMe over InfiniBand** y seleccione **Ver estadísticas de NVMe over Fabrics**.

¿Qué más debo hacer para configurar o diagnosticar NVMe over roce?

Es posible configurar y gestionar NVMe over roce desde las páginas hardware y Configuración.

> La configuración de NVMe over roce solo está disponible si la controladora de la cabina de almacenamiento incluye un puerto NVMe over roce.

Configurar y diagnosticar NVMe over roce

Acción	Ubicación
Configure los puertos NVMe over roce	1. Seleccione **hardware**. 2. Seleccione **Mostrar parte posterior de la bandeja**. 3. Seleccione una controladora. 4. Seleccione **Configurar puertos NVMe over roce**. o. 1. Seleccione MENU:Settings[System]. 2. Desplácese hasta **Configuración de NVMe over roce** y seleccione **Configurar puertos NVMe over roce**.
Ver estadísticas de NVMe over Fabrics	1. Seleccione MENU:Settings[System]. 2. Desplácese hasta **Configuración de NVMe over roce** y seleccione **Ver estadísticas de NVMe over Fabrics**.

Funciones complementarias

Conceptos

Cómo trabajar con las funciones complementarias

Las funciones complementarias son las que no se incluyen en la configuración estándar de System Manager y requieren una clave para su habilitación. Una función complementaria puede ser una sola función excepcional o un paquete de funciones agrupadas.

Los siguientes pasos proporcionan información general sobre cómo habilitar una función excepcional o un paquete de funciones:

1. Obtenga la siguiente información:
   - El número de serie del chasis y el identificador de habilitación de la función, el cual identifica la cabina de almacenamiento para la función que se instalará. Estos elementos están disponibles en System Manager.
   - El código de activación de la función, que está disponible en el sitio de soporte al adquirir la función.
2. Obtenga la clave de función. Para ello, póngase en contacto con el proveedor de almacenamiento o acceda al sitio de activación de funciones prémium. Proporcione el número de serie del chasis, el identificador de habilitación de la función y el código de activación de la función.
3. En System Manager, habilite la función excepcional o el paquete de funciones con el archivo de claves de función.

Terminología de la función complementaria

Conozca la forma en que los términos de las funciones complementarias se aplican a su cabina de almacenamiento.

Duración	Descripción
Identificador de habilitación de la función	Un identificador de habilitación de la función es una cadena única que identifica una cabina de almacenamiento específica. Este identificador garantiza que cuando se obtiene la función excepcional, esta se asocie únicamente con una cabina de almacenamiento en particular. Esta cadena aparece en la sección funciones adicionales de la página sistema.
Archivo de claves de función	Un archivo de claves de función es un archivo que se recibe para desbloquear y habilitar una función excepcional o un paquete de funciones.

Duración	Descripción
Paquete de funciones	Un paquete de funciones es un paquete que cambia los atributos de la cabina de almacenamiento (por ejemplo, cambiar el protocolo Fibre Channel a iSCSI). Los paquetes de funciones requieren una clave especial para habilitarlos.
Función excepcional	Una función prémium es una opción adicional que requiere una clave para habilitarla. No se incluye en la configuración estándar de System Manager.

Procedimientos

Obtener un archivo de claves de función

Para habilitar una función excepcional o un paquete de funciones en una cabina de almacenamiento, primero es necesario obtener un archivo de claves de función. Una clave se asociada con una sola cabina de almacenamiento.

Acerca de esta tarea

En esta tarea, se describe cómo obtener la información requerida para la función y, a continuación, enviar una solicitud para un archivo de claves de función. Entre la información requerida se encuentra la siguiente:

- Número de serie del chasis
- Identificador de habilitación de la función
- Código de activación de la función

Pasos

1. En System Manager, busque y registre el número de serie del chasis. Para ver este número de serie, debe pasar el ratón por el icono Centro de soporte.
2. En System Manager, busque Identificador de habilitación de funciones. Vaya a MENU:Settings[System] y, a continuación, desplácese hacia abajo hasta **Add-ons**. Busque **Identificador de habilitación de funciones**. Registre el número de la opción Identificador de habilitación de funciones.
3. Busque y registre el contenido de la opción Feature Activation Code. Para paquetes de funciones, este código de activación se proporciona en las instrucciones correspondientes para realizar la conversión.

   Es posible acceder a las instrucciones de NetApp en "Centro de documentación para sistemas E-Series y EF-Series de NetApp".

   Para funciones excepcionales, es posible acceder al código de activación en el sitio de soporte de la siguiente manera:

   a. Inicie sesión en "Soporte de NetApp".
   b. Vaya al menú:Productos[gestionar productos > licencias de software].
   c. Introduzca el número de serie del chasis de la cabina de almacenamiento y, a continuación, haga clic en **Ir**.
   d. Busque los códigos de activación de la función en la columna **clave de licencia**.

e. Registre el contenido de la opción Feature Activation Code de la función deseada.

4. Para solicitar un archivo de claves de función, envíe un correo electrónico o un documento de texto al proveedor de almacenamiento con la siguiente información: Número de serie del chasis, el contenido de la opción Feature Activation Code y el contenido de la opción Identificador de habilitación de funciones.

   También puede ir a. "Activación de licencias de NetApp: Activación de funciones prémium de matriz de almacenamiento" e introduzca la información requerida para obtener la función o el paquete de funciones. (Las instrucciones en este sitio son para funciones excepcionales, no paquetes de funciones.)

Después de terminar

Una vez que tenga el archivo de claves de la función, podrá habilitar la función excepcional o el paquete de funciones.

Habilite una función excepcional

Una función prémium es una opción adicional que requiere una clave para habilitarla.

Antes de empezar

- Obtuvo una clave de función. Si es necesario, comuníquese con soporte técnico para obtener una clave.
- Cargó el archivo de claves en el cliente de gestión (el sistema con un explorador para acceder a System Manager).

Acerca de esta tarea

En esta tarea, se describe cómo usar System Manager para habilitar una función excepcional.

> Si desea deshabilitar una función excepcional, debe utilizar el comando Deshabilitar función de cabina de almacenamiento `(disable storageArray (featurePack | feature=featureAttributeList)` En la interfaz de línea de comandos (CLI).

Pasos

1. Seleccione MENU:Settings[System].
2. En **Complementos**, seleccione **Activar característica Premium**.

   Se abre el cuadro de diálogo Habilitar una función prémium.

3. Haga clic en **examinar** y, a continuación, seleccione el archivo de claves.

   El nombre del archivo aparece en el cuadro de diálogo.

4. Haga clic en **Activar**.

Habilite el paquete de funciones

Un paquete de funciones es un paquete que cambia los atributos de la cabina de almacenamiento (por ejemplo, cambiar el protocolo Fibre Channel a iSCSI). Para habilitar paquetes de funciones, se requiere una clave especial.

Antes de empezar

- Siguió las instrucciones adecuadas para realizar la conversión y preparar el sistema para los nuevos atributos de la cabina de almacenamiento.

Es posible acceder a las instrucciones de conversión en "Centro de documentación para sistemas E-Series y EF-Series de NetApp".

- La cabina de almacenamiento está sin conexión, por lo que ningún host ni aplicación accede a la cabina.
- Existen backups de todos los datos.
- Obtuvo un archivo de paquete de funciones.

  El paquete de funciones está cargado en el cliente de gestión (el sistema con un explorador para acceder a System Manager).

Debe programar una ventana de mantenimiento de tiempo de inactividad y detener todas las operaciones de I/o entre el host y las controladoras. Además, tenga en cuenta que no podrá acceder a los datos en la cabina de almacenamiento hasta después de completar correctamente la conversión.

Acerca de esta tarea

En esta tarea, se describe cómo usar System Manager para habilitar un paquete de funciones. Al finalizar, debe reiniciar la cabina de almacenamiento.

Pasos

1. Seleccione MENU:Settings[System].
2. En **Complementos**, seleccione **Cambiar paquete de funciones**.
3. Haga clic en **examinar** y, a continuación, seleccione el archivo de claves.

   El nombre del archivo aparece en el cuadro de diálogo.

4. Escriba **CHANGE** en el campo.
5. Haga clic en **Cambiar**.

   Comienza la migración del paquete de funciones y se reinician las controladoras. Se eliminan los datos no escritos en la caché, lo que garantiza que no exista actividad de I/O. Las dos controladoras se reinician automáticamente para que el nuevo paquete de funciones entre en vigencia. La cabina de almacenamiento vuelve a responder cuando se completa el reinicio.

Gestión de claves de seguridad

Conceptos

Cómo opera la función Drive Security

Drive Security es una función de la cabina de almacenamiento que ofrece una capa adicional de seguridad con unidades de cifrado de disco completo (FDE) o unidades de estándar de procesamiento de información federal (FIPS). Cuando estas unidades se usan con la función Drive Security, se requiere una clave de seguridad para acceder a los datos. Cuando se retiran físicamente, las unidades de la cabina no pueden operar hasta que se instalan en otra cabina, instancia en la cual tendrán el estado Security Locked hasta que se proporcione la clave de seguridad correcta.

Cómo implementar Drive Security

Para implementar Drive Security, siga estos pasos.

1. Equipe la cabina de almacenamiento con unidades compatibles con la función de seguridad, ya sea con unidades FDE o FIPS. (Para los volúmenes que requieren compatibilidad con FIPS, debe utilizar únicamente unidades FIPS. Si se mezclan unidades FIPS y FDE en un grupo de volúmenes o un pool, todas las unidades se tratarán como unidades FDE. Además, una unidad FDE no puede añadirse a ni usarse como pieza de repuesto en un grupo de volúmenes o un pool completamente FIPS.)
2. Cree una clave de seguridad, que es una cadena de caracteres compartida por la controladora y las unidades para acceso de lectura/escritura. Es posible crear una clave interna desde la memoria persistente de la controladora o una clave externa desde un servidor de gestión de claves. Para la gestión de claves externas, debe establecerse una autenticación con el servidor de gestión de claves.
3. Habilite Drive Security para pools y grupos de volúmenes:
   - Cree un pool o grupo de volúmenes (busque **Sí** en la columna **compatible con la función de seguridad** de la tabla candidatos).
   - Seleccione un pool o grupo de volúmenes cuando cree un volumen nuevo (busque **Sí** junto a **compatible con la función de seguridad** en la tabla de candidatos de pools y grupos de volúmenes).

Cómo funciona Drive Security en el nivel de unidad

Una unidad compatible con la función de seguridad, FDE o FIPS, cifra los datos durante la escritura y descifra los datos durante la lectura. Estas operaciones de cifrado y descifrado no afectan al rendimiento ni al flujo de trabajo del usuario. Cada unidad tiene su propia clave de cifrado, que jamás puede transferirse de la unidad.

La función Drive Security ofrece una capa adicional de protección en unidades compatibles con la función de seguridad. Cuando se seleccionan grupos de volúmenes o pools en estas unidades para Drive Security, las unidades buscan una clave de seguridad antes de permitir el acceso a los datos. Es posible habilitar Drive Security para pools y grupos de volúmenes en cualquier momento sin afectar a los datos existentes en la unidad. Sin embargo, no es posible deshabilitar Drive Security sin borrar todos los datos en la unidad.

Cómo funciona Drive Security en el nivel de cabina de almacenamiento

Con la función Drive Security, se crea una clave de seguridad que se comparte entre las unidades con la función de seguridad habilitada y las controladoras en una cabina de almacenamiento. Siempre que se encienden y se apagan las unidades, las unidades con la función de seguridad habilitada cambian al estado Security Locked hasta que la controladora aplica la clave de seguridad.

Si se quita una unidad con la función de seguridad habilitada de la cabina de almacenamiento y se vuelve a instalar en otra, la unidad tendrá el estado Security Locked. La unidad reubicada busca la clave de seguridad para que pueda volver a accederse a los datos. Para desbloquear los datos, debe aplicar la clave de seguridad desde la cabina de almacenamiento de origen. Después de un proceso de desbloqueo correcto, la unidad reubicada utilizará la clave de seguridad ubicada en la cabina de almacenamiento objetivo, y el archivo de claves de seguridad importado ya no será necesario.

Para la gestión de claves internas, la clave de seguridad se almacena en una ubicación inaccesible de la controladora. No está en formato legible, y el usuario no puede acceder a ella.

Cómo funciona Drive Security en el nivel de volumen

Al crear un pool o un grupo de volúmenes desde unidades compatibles con la función de seguridad, también es posible habilitar Drive Security para estos pools o grupos de volúmenes. La opción Drive Security permite que las unidades y los pools y los grupos de volúmenes asociados tengan la función de seguridad-*enabled*.

Tenga en cuenta las siguientes directrices antes de crear pools y grupos de volúmenes con la función de seguridad habilitada:

- Los grupos de volúmenes y los pools deben estar compuestos en su totalidad por unidades compatibles con la función de seguridad. (Para los volúmenes que requieren compatibilidad con FIPS, debe utilizar únicamente unidades FIPS. Si se mezclan unidades FIPS y FDE en un grupo de volúmenes o un pool, todas las unidades se tratarán como unidades FDE. Además, una unidad FDE no puede añadirse a ni usarse como pieza de repuesto en un grupo de volúmenes o un pool completamente FIPS.)
- Los grupos de volúmenes y los pools deben tener el estado Optimal.

Cómo funciona la gestión de claves de seguridad

Cuando se implementa la función Drive Security, las unidades con la función de seguridad habilitada (FIPS o FDE) requieren una clave de seguridad para acceder a los datos. Una clave de seguridad es una cadena de caracteres que se comparte entre estos tipos de unidades y las controladoras en una cabina de almacenamiento.

Siempre que se encienden y se apagan las unidades, las unidades con la función de seguridad habilitada cambian al estado Security Locked hasta que la controladora aplica la clave de seguridad. Si se elimina una unidad habilitada para seguridad de la cabina de almacenamiento, se bloquean los datos de esa unidad. Cuando se vuelve a instalar la unidad en otra cabina de almacenamiento, se busca la clave de seguridad para que pueda volver a accederse a los datos. Para desbloquear los datos, debe aplicar la clave de seguridad original.

Puede crear y gestionar claves de seguridad mediante uno de los siguientes métodos:

- Gestión de claves internas en la memoria persistente de la controladora.
- Gestión de claves externas en un servidor de gestión de claves externo.

Gestión de claves internas

Las claves internas se conservan en la memoria persistente de la controladora. Para implementar la gestión de claves internas, siga estos pasos:

1. Instale unidades compatibles con la función de seguridad en la cabina de almacenamiento. Estas unidades pueden ser de cifrado de disco completo (FDE) o de estándar de procesamiento de información federal (FIPS).
2. Asegúrese de que la función Drive Security esté habilitada. Si fuera necesario, comuníquese con el proveedor de almacenamiento para pedir indicaciones sobre cómo habilitar la función Drive Security.
3. Cree una clave de seguridad interna, que implica definir un identificador y una frase de contraseña. El identificador es una frase que está asociada con la clave de seguridad, y se almacena en la controladora y en todas las unidades asociadas con la clave. La frase de contraseña se utiliza para cifrar la clave de seguridad con fines de backup. Para crear una clave interna, vaya a menú:Configuración[sistema > Gestión de claves de seguridad > Crear clave interna].

La clave de seguridad se almacena en una ubicación inaccesible de la controladora. Es posible crear grupos de volúmenes o pools con la función de seguridad habilitada, o bien habilitar la seguridad en grupos de volúmenes o pools existentes.

Gestión de claves externas

Las claves externas se mantienen en un servidor de gestión de claves individual mediante un protocolo de

interoperabilidad de gestión de claves (KMIP). Para implementar la gestión de claves externas, siga estos pasos:

1. Instale unidades compatibles con la función de seguridad en la cabina de almacenamiento. Estas unidades pueden ser de cifrado de disco completo (FDE) o de estándar de procesamiento de información federal (FIPS).
2. Asegúrese de que la función Drive Security esté habilitada. Si fuera necesario, comuníquese con el proveedor de almacenamiento para pedir indicaciones sobre cómo habilitar la función Drive Security.
3. Complete y descargue una solicitud de firma de certificación (CSR) de cliente para la autenticación entre la cabina de almacenamiento y el servidor de gestión de claves. Vaya a menú:Configuración[certificados > Gestión de claves > completar CSR].
4. Cree y descargue un certificado de cliente desde el servidor de gestión de claves con el archivo CSR descargado.
5. Asegúrese de que el certificado de cliente y una copia del certificado para el servidor de gestión de claves estén disponibles en el host local.
6. Cree una clave externa, que implica definir la dirección IP del servidor de gestión de claves y el número de puerto utilizado para comunicaciones KMIP. Durante este proceso, también debe cargar los archivos de certificado. Para crear una clave externa, vaya a menú:Configuración[sistema > Gestión de claves de seguridad > Crear clave externa].

El sistema se conecta al servidor de gestión de claves con las credenciales introducidas. Es posible crear grupos de volúmenes o pools con la función de seguridad habilitada, o bien habilitar la seguridad en grupos de volúmenes o pools existentes.

Terminología de Drive Security

Conozca la forma en que los términos de Drive Security se aplican a su cabina de almacenamiento.

Duración	Descripción
Función Drive Security	Drive Security es una función de la cabina de almacenamiento que ofrece una capa adicional de seguridad con unidades de cifrado de disco completo (FDE) o unidades de estándar de procesamiento de información federal (FIPS). Cuando estas unidades se usan con la función Drive Security, se requiere una clave de seguridad para acceder a los datos. Cuando se retiran físicamente, las unidades de la cabina no pueden operar hasta que se instalan en otra cabina, instancia en la cual tendrán el estado Security Locked hasta que se proporcione la clave de seguridad correcta.
Unidades FDE	Las unidades de cifrado de disco completo (FDE) realizan el cifrado en la unidad de disco en el nivel de hardware. La unidad de disco duro contiene un chip ASIC que cifra los datos durante las escrituras y, a continuación, descifra los datos durante las lecturas.

Duración	Descripción
Unidades FIPS	Las unidades con FIPS utilizan estándares de procesamiento de información federal (FIPS) 140-2 nivel 2. Son esencialmente unidades FDE que cumplen con las normas gubernamentales de los Estados Unidos para garantizar algoritmos y métodos de cifrado sólidos. Las unidades FIPS tienen normas de seguridad más rigurosas que las unidades FDE.
Cliente de gestión	Un sistema local (equipo, tablet, etc.) que incluye un explorador para acceder a System Manager.
Frase de contraseña	La frase de contraseña se utiliza para cifrar la clave de seguridad con fines de backup. La misma frase de contraseña utilizada para cifrar la clave de seguridad debe incluirse cuando se importa la clave de seguridad como resultado de una migración de unidad o un cambio de cabezal. La frase de contraseña puede tener entre 8 y 32 caracteres. La frase de contraseña de Drive Security es independiente de la contraseña de administrador de la cabina de almacenamiento.
Unidades compatibles con la función de seguridad	Las unidades compatibles con la función de seguridad pueden ser unidades de cifrado de disco completo (FDE) o de estándar de procesamiento de información federal (FIPS) que cifran datos durante la escritura y descifran datos durante la lectura. Estas unidades se consideran Secure-*capable* porque se pueden usar para obtener más seguridad mediante la función Drive Security. Si está habilitada la función Drive Security para los grupos de volúmenes y pools que se utilizan con estas unidades, las unidades pasan a tener habilitada la función de seguridad-*enabled*.
Unidades con la función de seguridad habilitada	Las unidades con la función de seguridad habilitada se usan con Drive Security. Cuando se habilita la función Drive Security y se aplica Drive Security a un pool o un grupo de volúmenes en unidades_ compatibles con la función de seguridad, las unidades pasan a ser seguras *habilitadas*. El acceso de lectura y escritura solo está disponible a través de una controladora que está configurada con la clave de seguridad correcta. Esta seguridad adicional evita el acceso no autorizado a los datos en una unidad que se quita físicamente de la cabina de almacenamiento.

Duración	Descripción
Clave de seguridad	Una clave de seguridad es una cadena de caracteres que se comparte entre las unidades habilitadas para seguridad y las controladoras en una cabina de almacenamiento. Siempre que se encienden y se apagan las unidades, las unidades con la función de seguridad habilitada cambian al estado Security Locked hasta que la controladora aplica la clave de seguridad. Si se elimina una unidad habilitada para seguridad de la cabina de almacenamiento, se bloquean los datos de esa unidad. Cuando se vuelve a instalar la unidad en otra cabina de almacenamiento, se busca la clave de seguridad para que pueda volver a accederse a los datos. Para desbloquear los datos, debe aplicar la clave de seguridad original. Puede crear y gestionar claves de seguridad mediante uno de los siguientes métodos: • Gestión de claves internas: Crea y mantiene claves de seguridad en la memoria persistente de la controladora. • Gestión de claves externas: Crea y mantiene claves de seguridad en un servidor de gestión de claves externo.
Identificador de clave de seguridad	El identificador de clave de seguridad es una cadena asociada con la clave de seguridad durante su creación. El identificador se almacena en la controladora y en todas las unidades asociadas con la clave de seguridad.

Procedimientos

Cree una clave de seguridad interna

Para usar la función Drive Security, se puede crear una clave de seguridad interna que compartan las controladoras y las unidades compatibles con la función de seguridad de la cabina de almacenamiento. Las claves internas se conservan en la memoria persistente de la controladora.

Antes de empezar

- Se deben instalar unidades compatibles con la función de seguridad en la cabina de almacenamiento. Estas unidades pueden ser de cifrado de disco completo (FDE) o de estándar de procesamiento de información federal (FIPS).
- Se debe habilitar la función Drive Security. De lo contrario, se abre el cuadro de diálogo **no se puede crear la clave de seguridad** durante esta tarea. Si fuera necesario, comuníquese con el proveedor de almacenamiento para pedir indicaciones sobre cómo habilitar la función Drive Security.

Si se instalan unidades FDE y FIPS en la cabina de almacenamiento, ambas compartirán la misma clave de seguridad.

Acerca de esta tarea

En esta tarea, se deben definir un identificador y una frase de contraseña para asociarlos con la clave de seguridad interna.

La frase de contraseña de Drive Security es independiente de la contraseña de administrador de la cabina de almacenamiento.

Pasos

1. Seleccione MENU:Settings[System].
2. En **Gestión de claves de seguridad**, seleccione **Crear clave interna**.

   Si aún no ha generado una clave de seguridad, se abre el cuadro de diálogo **Crear clave de seguridad**.

3. Introduzca información en los siguientes campos:

   - Definir un identificador de claves de seguridad: Puede aceptar el valor predeterminado (el nombre de la cabina de almacenamiento y la Marca de tiempo que genera el firmware de la controladora) o introducir el valor deseado. Puede introducir hasta 189 caracteres alfanuméricos sin espacios, puntuación ni símbolos.

     Se generarán otros caracteres automáticamente, incorporados a ambos extremos de la cadena que introdujo. Los caracteres generados garantizan que el identificador sea único.

   - Definir una frase de contraseña/Volver a introducir la frase de contraseña — Introduzca y confirme una frase de contraseña. El valor puede tener entre 8 y 32 caracteres, y debe incluir uno de los siguientes caracteres:
     - Una letra mayúscula (o varias). Se debe tener en cuenta que la frase de contraseña distingue mayúsculas de minúsculas.
     - Un número (o varios).
     - Un carácter no alfanumérico, como !, *, @ (o varios).

   Asegúrese de registrar lo introducido para usarlo en el futuro. Si se necesita transferir una unidad con la función de seguridad habilitada de la cabina de almacenamiento, se deben conocer el identificador y la frase de contraseña para desbloquear los datos de la unidad.

4. Haga clic en **Crear**.

   La clave de seguridad se almacena en una ubicación inaccesible de la controladora. Además de la clave real, se descarga un archivo de claves cifrado del explorador.

   La ruta del archivo descargado podría depender de la ubicación predeterminada de las descargas del explorador.

5. Anote el identificador de claves, la frase de la contraseña y la ubicación del archivo de claves descargado y, a continuación, haga clic en **Cerrar**.

Resultado

Ahora se pueden crear grupos de volúmenes o pools con la función de seguridad habilitada o puede habilitar la seguridad en los grupos de volúmenes y pools existentes.

> Cada vez que se apagan y se vuelven a encender las unidades, todas las unidades con la función de seguridad habilitada cambian al estado Security Locked. En este estado, no se puede acceder a los datos hasta que la controladora aplica la clave de seguridad correcta durante la inicialización de la unidad. Si alguien quita físicamente la unidad bloqueada y la instala en otro sistema, el estado Security Locked evita el acceso no autorizado de los datos.

Después de terminar

Debe validar la clave de seguridad para asegurarse de que no se haya dañado el archivo de claves.

Cree una clave de seguridad externa

Para usar la función Drive Security con un servidor de gestión de claves, se debe crear una clave externa que se compartirá con el servidor de gestión de claves y las unidades compatibles con la función de seguridad de la cabina de almacenamiento.

Antes de empezar

- Se deben instalar unidades compatibles con la función de seguridad en la cabina. Estas unidades pueden ser de cifrado de disco completo (FDE) o de estándar de procesamiento de información federal (FIPS).

  > Si se instalan unidades FDE y FIPS en la cabina de almacenamiento, ambas compartirán la misma clave de seguridad.

- Se debe habilitar la función Drive Security. De lo contrario, se abre el cuadro de diálogo **no se puede crear la clave de seguridad** durante esta tarea. Si fuera necesario, comuníquese con el proveedor de almacenamiento para pedir indicaciones sobre cómo habilitar la función Drive Security.
- Los certificados de cliente y de servidor están disponibles en el host local, por este motivo, el servidor de la cabina de almacenamiento y de gestión de claves pueden autenticarse entre sí. El certificado de cliente valida las controladoras, mientras que el certificado de servidor valida el servidor de gestión de claves.

Acerca de esta tarea

En esta tarea, se deben definir la dirección IP del servidor de gestión de claves y el número de puerto que utiliza y, luego, cargar los certificados para la gestión de claves externas.

Pasos

1. Seleccione MENU:Settings[System].
2. En **Gestión de claves de seguridad**, seleccione **Crear clave externa**.

   > Si está configurada actualmente la gestión de claves internas, se muestra un cuadro de diálogo para solicitar la confirmación de que se desea cambiar a la gestión de claves externas.

   Se abre el cuadro de diálogo **Crear clave de seguridad externa**.

3. En **conectar con el servidor de claves**, introduzca información en los siguientes campos:
   - Dirección del servidor de gestión de claves: Introduzca el nombre de dominio completo o la dirección IP (IPv4 o IPv6) del servidor que se usaron para la gestión de claves.

- Número de puerto de gestión de claves: Introduzca el número de puerto que se usó para la comunicación del protocolo de interoperabilidad de gestión de claves (KMIP). El número de puerto más común que se usa para la comunicación del servidor de gestión de claves es 5696.
- Seleccione certificado de cliente — haga clic en el primer botón examinar para seleccionar el archivo de certificado de las controladoras de la cabina de almacenamiento.
- Seleccionar certificación del servidor de gestión de claves — haga clic en el segundo botón examinar para seleccionar el archivo de certificado del servidor de gestión de claves.

4. Haga clic en **Siguiente**.
5. En **Crear/hacer copia de seguridad de la clave**, introduzca información en el siguiente campo:
   - Definir una frase de contraseña/Volver a introducir la frase de contraseña — Introduzca y confirme una frase de contraseña. El valor puede tener entre 8 y 32 caracteres, y debe incluir uno de los siguientes caracteres:
     - Una letra mayúscula (o varias). Se debe tener en cuenta que la frase de contraseña distingue mayúsculas de minúsculas.
     - Un número (o varios).
     - Un carácter no alfanumérico, como !, *, @ (o varios).

   > Asegúrese de registrar lo introducido para usarlo en el futuro. Si se necesita transferir una unidad con la función de seguridad habilitada de la cabina de almacenamiento, se debe conocer la frase de contraseña para desbloquear los datos de la unidad.

6. Haga clic en **Finalizar**.

   El sistema se conecta al servidor de gestión de claves con las credenciales introducidas. Luego, se almacena una copia de la clave de seguridad en el sistema local.

   > La ruta del archivo descargado podría depender de la ubicación predeterminada de las descargas del explorador.

7. Anote la frase de contraseña y la ubicación del archivo de claves descargado y, a continuación, haga clic en **Cerrar**.

   En la página, se muestra el siguiente mensaje con enlaces adicionales para la gestión de claves externas.

   ```
   Current key management method: External
   ```

8. Pruebe la conexión entre la cabina de almacenamiento y el servidor de gestión de claves. Para ello, seleccione **probar comunicación**.

   Los resultados de la prueba se muestran en el cuadro de diálogo.

Resultados

Cuando se habilita la gestión de claves externas, se pueden crear grupos de volúmenes o pools con la función de seguridad habilitada, o bien se puede habilitar la función de seguridad en los grupos de volúmenes y pools existentes.

Cada vez que se apagan y se vuelven a encender las unidades, todas las unidades con la función de seguridad habilitada cambian al estado Security Locked. En este estado, no se puede acceder a los datos hasta que la controladora aplica la clave de seguridad correcta durante la inicialización de la unidad. Si alguien quita físicamente la unidad bloqueada y la instala en otro sistema, el estado Security Locked evita el acceso no autorizado de los datos.

Después de terminar

- Debe validar la clave de seguridad para asegurarse de que no se haya dañado el archivo de claves.

Cambiar clave de seguridad

Es posible reemplazar una clave de seguridad por una nueva en cualquier momento. Puede resultar necesario cambiar una clave de seguridad en aquellos casos en los que potencialmente se haya comprometido la seguridad en la empresa y en los que se desee garantizar que personal no autorizado no pueda acceder a los datos de las unidades.

Antes de empezar

Ya existe una clave de seguridad.

Acerca de esta tarea

En esta tarea, se describe cómo cambiar una clave de seguridad y reemplazarla por una nueva. Una vez completado este proceso, la clave anterior ya no es más válida.

Pasos

1. Seleccione MENU:Settings[System].
2. En **Gestión de claves de seguridad**, seleccione **Cambiar clave**.

   Se abre el cuadro de diálogo **Cambiar clave de seguridad**.

3. Introduzca información en los siguientes campos.

   - Definir un identificador de claves de seguridad (solo para claves de seguridad internas) Acepte el valor predeterminado (Marca de tiempo y nombre de la cabina de almacenamiento, que genera el firmware de la controladora) o introduzca un valor personalizado. Puede introducir hasta 189 caracteres alfanuméricos sin espacios, puntuación ni símbolos.

     Se generan automáticamente caracteres adicionales y se agregan a ambos extremos de la cadena que introduce. Los caracteres generados ayudan a garantizar que el identificador sea único.

   - Definir una frase de contraseña/Volver a introducir la frase de contraseña — en cada uno de estos campos, introduzca la frase de contraseña. El valor puede tener entre 8 y 32 caracteres, y debe incluir uno de los siguientes caracteres:
     - Una letra mayúscula (o varias). Se debe tener en cuenta que la frase de contraseña distingue mayúsculas de minúsculas.
     - Un número (o varios).
     - Un carácter no alfanumérico, como !, *, @ (o varios).

Asegúrese de registrar las entradas para uso futuro.- Si necesita quitar de la cabina de almacenamiento una unidad con la función de seguridad habilitada, debe conocer el identificador y la frase de contraseña para desbloquear los datos de la unidad.

4. Haga clic en **Cambiar**.

   La clave de seguridad nueva sobrescribe la clave anterior, que ya no es válida.

   La ruta del archivo descargado podría depender de la ubicación predeterminada de las descargas del explorador.

5. Anote el identificador de claves, la frase de la contraseña y la ubicación del archivo de claves descargado y, a continuación, haga clic en **Cerrar**.

Después de terminar

Debe validar la clave de seguridad para asegurarse de que no se haya dañado el archivo de claves.

Alternar de gestión de claves internas a externas

Se puede modificar el método de gestión de Drive Security de un servidor de claves externo a un método interno utilizado por la cabina de almacenamiento. La clave de seguridad definida previamente para la gestión de claves externas luego se utiliza para la gestión de claves internas.

Antes de empezar

Se creó una clave externa.

Acerca de esta tarea

En esta tarea, se deshabilita la gestión de claves externas y se descarga una nueva copia de backup en el host local. La clave existente se sigue usando para Drive Security, pero se gestionará internamente en la cabina de almacenamiento.

Pasos

1. Seleccione MENU:Settings[System].
2. En **Gestión de claves de seguridad**, seleccione **Desactivar administración de claves externa**.

   Se abre el cuadro de diálogo **Deshabilitar administración de claves externa**.

3. En **definir una frase de contraseña/Volver a introducir la frase de contraseña**, introduzca y confirme una frase de contraseña para el backup de la clave. El valor puede tener entre 8 y 32 caracteres, y debe incluir uno de los siguientes caracteres:

   - Una letra mayúscula (o varias). Se debe tener en cuenta que la frase de contraseña distingue mayúsculas de minúsculas.
   - Un número (o varios).
   - Un carácter no alfanumérico, como !, *, @ (o varios).

   Asegúrese de registrar las entradas para uso futuro. Si se necesita transferir una unidad con la función de seguridad habilitada de la cabina de almacenamiento, se deben conocer el identificador y la frase de contraseña para desbloquear los datos de la unidad.

4. Haga clic en **Desactivar**.

   La clave de backup se descarga en el host local.

5. Anote el identificador de claves, la frase de la contraseña y la ubicación del archivo de claves descargado y, a continuación, haga clic en **Cerrar**.

Resultados

Drive Security ahora se gestiona internamente mediante la cabina de almacenamiento.

Después de terminar

- Debe validar la clave de seguridad para asegurarse de que no se haya dañado el archivo de claves.

Editar configuración del servidor de gestión de claves

Si configuró la gestión de claves externas, es posible ver y editar los ajustes del servidor de gestión de claves en cualquier momento.

Antes de empezar

Debe configurarse la gestión de claves externas.

Pasos

1. Seleccione MENU:Settings[System].
2. En **Gestión de claves de seguridad**, seleccione **Ver/editar configuración del servidor de administración de claves**.
3. Edite la información en los siguientes campos:
   - Dirección del servidor de gestión de claves: Introduzca el nombre de dominio completo o la dirección IP (IPv4 o IPv6) del servidor que se usaron para la gestión de claves.
   - KMIP Port number — introduzca el número de puerto utilizado para las comunicaciones mediante el protocolo de interoperabilidad de gestión de claves (KMIP).
4. Haga clic en **Guardar**.

Realice un backup de la clave de seguridad

Después de crear o de cambiar una clave de seguridad, es posible crear una copia de backup del archivo de claves en caso de que el original se dañe.

Antes de empezar

- Ya existe una clave de seguridad.

Acerca de esta tarea

En esta tarea, se describe cómo realizar un backup de la clave de seguridad creada previamente. Durante este procedimiento, es posible crear una nueva frase de contraseña para el backup. No es necesario que esta frase de contraseña coincida con la utilizada cuando se creó o se modificó por última vez la clave original. La frase de contraseña se aplica solo al backup que se va a crear.

Pasos

1. Seleccione MENU:Settings[System].
2. En **Gestión de claves de seguridad**, seleccione **clave de copia de seguridad**.

Se abre el cuadro de diálogo **clave de seguridad de copia de seguridad**.

3. En los campos **define a pass phrase/Re-enter pass phrase**, introduzca y confirme una frase de contraseña para este backup.

   El valor puede tener entre 8 y 32 caracteres, y debe incluir uno de los siguientes caracteres:

   - Una letra mayúscula (o varias)
   - Un número (o varios).
   - Un carácter no alfanumérico, como !, *, @ (o varios).

   Asegúrese de registrar lo introducido para usarlo en el futuro. Necesita la frase de contraseña para acceder al backup de esta clave de seguridad.

4. Haga clic en **copia de seguridad**.

   Se descarga una copia de seguridad de la clave de seguridad en el host local y, a continuación, se abre el cuadro de diálogo **Confirmar/registrar copia de seguridad de la clave**.

   La ruta del archivo de claves de seguridad descargado puede depender de la ubicación de descarga predeterminada del explorador.

5. Registre la frase de contraseña en un lugar seguro y, a continuación, haga clic en **Cerrar**.

Después de terminar

Debe validar la clave de seguridad de backup.

Valide la clave de seguridad

Es posible validar la clave de seguridad para asegurarse de que no se haya dañado y verificar que tenga una frase de contraseña correcta.

Antes de empezar

Se creó una clave de seguridad.

Acerca de esta tarea

Esta tarea describe cómo validar la clave de seguridad que se creó anteriormente. Este es un paso importante para asegurarse de que el archivo de claves no esté dañado y que la frase de contraseña sea correcta. Esto permite acceder a datos de la unidad más adelante si se mueve una unidad con la función de seguridad habilitada de una cabina de almacenamiento a otra.

Pasos

1. Seleccione MENU:Settings[System].
2. En **Gestión de claves de seguridad**, seleccione **Validar clave**.

   Se abre el cuadro de diálogo **Validar clave de seguridad**.

3. Haga clic en **examinar** y, a continuación, seleccione el archivo de claves (por ejemplo, `drivesecurity.slk`).
4. Introduzca la frase de contraseña asociada con la clave que seleccionó.

Al seleccionar un archivo de claves válido y una frase de contraseña, el botón **Validar** se vuelve disponible.

5. Haga clic en **Validar**.

   Los resultados de la validación se muestran en el cuadro de diálogo.

6. Si los resultados muestran que la clave de seguridad se validó correctamente, haga clic en **Cerrar**. Si aparece un mensaje de error, siga las instrucciones sugeridas que se muestran en el cuadro de diálogo.

Desbloquee las unidades mediante una clave de seguridad

Si mueve unidades con la función de seguridad habilitada de una cabina de almacenamiento a otra, debe importar la clave de seguridad adecuada a la nueva cabina de almacenamiento. Al importar la clave, se desbloquean los datos de las unidades.

Antes de empezar

- La cabina de almacenamiento de destino (donde se moverán las unidades) ya debe tener una clave de seguridad configurada. Las unidades migradas se volverán a asignar una clave a la cabina de almacenamiento objetivo.
- Debe conocer la clave de seguridad asociada con las unidades que desea desbloquear.
- El archivo de claves de seguridad está disponible en el cliente de gestión (el sistema con un explorador que se utilizó para acceder a System Manager). Si mueve las unidades a una cabina de almacenamiento gestionada por otro sistema, debe mover el archivo de claves de seguridad a ese cliente de gestión.

Acerca de esta tarea

En esta tarea, se describe cómo desbloquear los datos de las unidades con la función de seguridad habilitada que se hayan eliminado de una cabina de almacenamiento y se hayan vuelto a instalar en otra. Una vez que la cabina detecta las unidades, aparece la condición "Needs Attention" junto con el estado "Security Key Needed" para estas unidades reubicadas. Para desbloquear los datos de la unidad, importe la clave de seguridad en la cabina de almacenamiento. Durante este proceso, se selecciona el archivo de claves de seguridad y se introduce la frase de contraseña para la clave.

> La frase de contraseña no es la misma que la contraseña de administrador de la cabina de almacenamiento.

Si se instalan otras unidades con la función de seguridad habilitada en la nueva cabina de almacenamiento, estas podrían usar una clave de seguridad distinta de la que se está importando. Durante el proceso de importación, la clave de seguridad antigua se usa únicamente para desbloquear los datos de las unidades que se instalan. Cuando el proceso de desbloqueo se realiza correctamente, se vuelve a asignar una clave de seguridad de cabina de almacenamiento de destino a las unidades recién instaladas.

Pasos

1. Seleccione MENU:Settings[System].
2. En **Gestión de claves de seguridad**, seleccione **Desbloquear unidades seguras**.

   Se abre el cuadro de diálogo **Desbloquear unidades seguras**. Todas las unidades que requieren una clave de seguridad se muestran en la tabla.

3. De manera opcional, pase el ratón sobre un número de unidad para ver la ubicación de la unidad (número de bandeja y número de bahía).

4. Haga clic en **examinar** y, a continuación, seleccione el archivo de claves de seguridad correspondiente a la unidad que desea desbloquear.

   El archivo de claves seleccionado aparece en el cuadro de diálogo.

5. Introduzca la frase de contraseña asociada con este archivo de claves.

   Los caracteres introducidos están enmascarados.

6. Haga clic en **Desbloquear**.

   Si la operación de desbloqueo se realiza correctamente, en el cuadro de diálogo se muestra un mensaje que indica que se desbloquearon las unidades seguras asociadas.

Resultados

Cuando todas las unidades se bloquean y después se desbloquean, se reinicia cada controladora de la cabina de almacenamiento. Sin embargo, si ya existen algunas unidades desbloqueadas en la cabina de almacenamiento de destino, las controladoras no se reinician.

Preguntas frecuentes

¿Qué debo saber antes de crear una clave de seguridad?

Las controladoras y unidades con seguridad habilitada comparten una clave de seguridad dentro de una cabina de almacenamiento. Si se quita una unidad con la función de seguridad habilitada de la cabina de almacenamiento, la clave de seguridad protege los datos de un acceso no autorizado.

Puede crear y gestionar claves de seguridad mediante uno de los siguientes métodos:

- Gestión de claves internas en la memoria persistente de la controladora.
- Gestión de claves externas en un servidor de gestión de claves externo.

Antes de crear una clave de seguridad interna, debe hacer lo siguiente:

1. Instale unidades compatibles con la función de seguridad en la cabina de almacenamiento. Estas unidades pueden ser de cifrado de disco completo (FDE) o de estándar de procesamiento de información federal (FIPS).
2. Asegúrese de que la función Drive Security esté habilitada. Si fuera necesario, comuníquese con el proveedor de almacenamiento para pedir indicaciones sobre cómo habilitar la función Drive Security.

Luego, podrá crear una clave de seguridad interna, lo que implica definir un identificador y una frase de contraseña. El identificador es una frase que está asociada con la clave de seguridad, y se almacena en la controladora y en todas las unidades asociadas con la clave. La frase de contraseña se utiliza para cifrar la clave de seguridad con fines de backup. Una vez que haya terminado, la clave de seguridad se almacena en una ubicación no accesible de la controladora. Es posible crear grupos de volúmenes o pools con la función de seguridad habilitada, o bien habilitar la seguridad en grupos de volúmenes o pools existentes.

Antes de crear una clave de seguridad externa, debe hacer lo siguiente:

1. Instale unidades compatibles con la función de seguridad en la cabina de almacenamiento. Estas unidades pueden ser de cifrado de disco completo (FDE) o de estándar de procesamiento de información

federal (FIPS).

2. Asegúrese de que la función Drive Security esté habilitada. Si fuera necesario, comuníquese con el proveedor de almacenamiento para pedir indicaciones sobre cómo habilitar la función Drive Security.
3. Complete y descargue una solicitud de firma de certificación (CSR) de cliente para la autenticación entre la cabina de almacenamiento y el servidor de gestión de claves. Vaya a menú:Configuración[certificados > Gestión de claves > completar CSR].
4. Cree y descargue un certificado de cliente desde el servidor de gestión de claves con el archivo CSR descargado.
5. Asegúrese de que el certificado de cliente y una copia del certificado para el servidor de gestión de claves estén disponibles en el host local.

Luego, podrá crear una clave externa, lo que implica definir la dirección IP del servidor de gestión de claves y el número de puerto para las comunicaciones KMIP. Durante este proceso, también debe cargar los archivos de certificado. Una vez que haya terminado, el sistema se conecta al servidor de gestión de claves con las credenciales introducidas. Es posible crear grupos de volúmenes o pools con la función de seguridad habilitada, o bien habilitar la seguridad en grupos de volúmenes o pools existentes.

¿Por qué debo definir una frase de contraseña?

La frase de contraseña se utiliza para cifrar y descifrar el archivo de claves de seguridad almacenado en el cliente de gestión local. Sin la frase de contraseña, la clave de seguridad no se puede descifrar y utilizar para desbloquear datos de una unidad con la función de seguridad habilitada, si se la reinstala en otra cabina de almacenamiento.

¿Por qué es importante registrar la información de claves de seguridad?

Si pierde la información de la clave de seguridad y no cuenta con un backup, podría perder los datos al reubicar las unidades con la función de seguridad habilitada o actualizar una controladora. La clave de seguridad es necesaria para desbloquear los datos en las unidades.

Asegúrese de registrar el identificador de la clave de seguridad, la frase de contraseña asociada y la ubicación en el host local en donde se guardó el archivo de claves de seguridad.

¿Qué debo saber antes de realizar un backup de una clave de seguridad?

Si la clave de seguridad original se daña y no existe un backup, se perderá el acceso a los datos de las unidades al migrarlas de una cabina de almacenamiento a otra.

Antes de realizar el backup de una clave de seguridad, tenga en cuenta las siguientes directrices:

- Asegúrese de conocer el identificador de claves de seguridad y la frase de contraseña del archivo de claves original.

> Solo las claves internas usan identificadores. Cuando se crea el identificador, se crean caracteres adicionales que se anexan automáticamente a ambos extremos de la cadena del identificador. Los caracteres generados garantizan que el identificador sea único.

- Es posible crear una frase de contraseña nueva para el backup. No es necesario que esta frase de contraseña coincida con la utilizada cuando se creó o se modificó por última vez la clave original. La frase

de contraseña solo se aplica al backup que se crea.

> La frase de contraseña para Drive Security no debería confundirse con la contraseña del administrador de la cabina de almacenamiento. La frase de contraseña para Drive Security protege los backups de una clave de seguridad. La contraseña del administrador protege toda la cabina de almacenamiento de un acceso no autorizado.

- El archivo de claves de seguridad de backup se descarga en el cliente de gestión. La ruta del archivo descargado podría depender de la ubicación predeterminada de las descargas del explorador. Asegúrese de registrar dónde se almacena la información de la clave de seguridad.

¿Qué debo saber antes de desbloquear unidades seguras?

Para desbloquear los datos de una unidad compatible con la función de seguridad habilitada que se migra a una cabina de almacenamiento nueva, se debe importar la clave de seguridad.

Antes de desbloquear unidades con la función de seguridad habilitada, recuerde las siguientes directrices:

- La cabina de almacenamiento de destino (donde se moverán las unidades) ya debe tener una clave de seguridad. Las unidades migradas se volverán a asignar una clave a la cabina de almacenamiento objetivo.
- Para las unidades que se van a migrar, se deben conocer el identificador de la clave de seguridad y la frase de contraseña que corresponden al archivo de claves de seguridad.
- El archivo de claves de seguridad está disponible en el cliente de gestión (el sistema con un explorador que se utilizó para acceder a System Manager).

¿Qué es la accesibilidad de lectura/escritura?

La ventana **Configuración de la unidad** incluye información acerca de los atributos **Seguridad de la unidad**. "Read/Write Accessible" es uno de los atributos que se muestran si se bloquearon los datos de una unidad.

Para ver los atributos **Drive Security**, vaya a la página hardware. Seleccione una unidad, haga clic en **Ver configuración** y, a continuación, haga clic en **Mostrar más valores**. En la parte inferior de la página, el valor del atributo Accesibilidad de lectura/escritura será **Sí** cuando la unidad esté desbloqueada. El valor del atributo Accesibilidad de lectura/escritura es **no, clave de seguridad no válida** cuando la unidad está bloqueada. Si desea desbloquear una unidad segura, importe una clave de seguridad (vaya a menú:Configuración[sistema > Desbloquear unidades seguras]).

¿Qué debo saber acerca de la validación de la clave de seguridad?

Después de crear una clave de seguridad, se debe validar el archivo de claves para garantizar que no esté dañado.

Si la validación falla, haga lo siguiente:

- Si el identificador de claves de seguridad no coincide con el identificador de la controladora, busque el archivo de claves de seguridad correcto y vuelva a intentar hacer la validación.
- Si la controladora no puede descifrar la clave de seguridad para la validación, es posible que haya introducido incorrectamente la frase de contraseña. Haga doble clic en la frase de contraseña, vuelva a

introducirla si fuera necesario y vuelva a intentar hacer la validación. Si vuelve a aparecer el mensaje de error, seleccione un backup del archivo de claves (si estuviera disponible) y vuelva a intentar hacer la validación.

- Si aún no puede validar la clave de seguridad, es posible que el archivo original esté dañado. Cree un backup nuevo de la clave y valide esa copia.

¿Cuál es la diferencia entre la gestión de claves de seguridad interna y de claves de seguridad externa?

Cuando implementa la función **Drive Security**, puede utilizar una clave de seguridad interna o una clave de seguridad externa para bloquear los datos cuando se quita una unidad con la función de seguridad habilitada de la cabina de almacenamiento.

Una clave de seguridad es una cadena de caracteres, que se comparte entre las unidades y controladoras con la función de seguridad habilitada en una cabina de almacenamiento. Las claves internas se conservan en la memoria persistente de la controladora. Las claves externas se mantienen en un servidor de gestión de claves individual mediante un protocolo de interoperabilidad de gestión de claves (KMIP).

Información de copyright

Información de la marca comercial