Preguntas frecuentes

E-Series Systems

NetApp
June 14, 2024

Tabla de contenidos

Preguntas frecuentes

¿Qué configuración se importa?

La función Importar configuración es una operación en lote que carga las configuraciones desde una cabina de almacenamiento a varias cabinas de almacenamiento.

La configuración que se importe durante esta operación dependerá de cómo esté configurada la cabina de almacenamiento de origen en System Manager. Las siguientes configuraciones pueden importarse a varias cabinas:

- **Alertas por correo electrónico** — la configuración incluye una dirección de servidor de correo y las direcciones de correo electrónico de los destinatarios de las alertas.
- **Alertas Syslog** — las configuraciones incluyen una dirección de servidor syslog y un puerto UDP.
- **Alertas SNMP** — las configuraciones incluyen un nombre de comunidad y una dirección IP para el servidor SNMP.
- **AutoSupport** — los ajustes incluyen las características independientes (Basic AutoSupport, AutoSupport OnDemand y Remote Diagnostics), la ventana de mantenimiento, el método de entrega, y programa de envío.
- **Servicios de directorio** — la configuración incluye el nombre de dominio y la URL de un servidor LDAP (protocolo ligero de acceso a directorios), junto con las asignaciones de los grupos de usuarios del servidor LDAP a los roles predefinidos de la cabina de almacenamiento.
- **Configuración de almacenamiento** — las configuraciones incluyen volúmenes (sólo volúmenes gruesos y que no pertenecen al repositorio), grupos de volúmenes, pools y asignaciones de unidades de repuesto activo.
- **Ajustes del sistema** — las configuraciones incluyen la configuración de escaneo de medios para un volumen, caché SSD para controladores y equilibrio de carga automático (no incluye la generación de informes de conectividad de host).

¿Por qué no se muestran todas las cabinas de almacenamiento?

Durante la operación Importar configuración, es posible que algunas cabinas de almacenamiento no estén disponibles en el cuadro de diálogo de selección de objetivos.

Que las cabinas de almacenamiento no aparezcan puede deberse a los siguientes motivos:

- La versión de firmware es inferior a 8.50.
- La cabina de almacenamiento se encuentra sin conexión.
- El sistema no puede comunicarse con esa cabina (por ejemplo, la cabina tiene problemas de red o con un certificado o una contraseña).

¿Por qué estos volúmenes no están asociados a una carga de trabajo?

Los volúmenes no se asocian a una carga de trabajo si se los creó mediante la interfaz

de línea de comandos (CLI) o si se migraron (importaron/exportaron) desde una cabina de almacenamiento diferente.

¿Cómo afecta la creación de volúmenes la carga de trabajo seleccionada?

Durante la creación del volumen, se le solicita información sobre el uso de una carga de trabajo. El sistema utiliza esta información para crear una configuración de volumen óptima para el usuario, que se puede editar en caso de ser necesario. De manera opcional, es posible omitir este paso en la secuencia de creación de volúmenes.

Una carga de trabajo es un objeto de almacenamiento que admite una aplicación. Se pueden definir una o más cargas de trabajo o instancias por aplicación. En algunas aplicaciones, el sistema configura la carga de trabajo para contener volúmenes con características subyacentes similares. Estas características de volumen se optimizan según el tipo de aplicación que es compatible con la carga de trabajo. Por ejemplo, si crea una carga de trabajo que es compatible con la aplicación Microsoft SQL Server y, a continuación, crea volúmenes para esa carga de trabajo, las características de volumen subyacentes se optimizan para ser compatibles con Microsoft SQL Server.

- **Específico de la aplicación** — cuando se crean volúmenes con una carga de trabajo específica de la aplicación, el sistema puede recomendar una configuración de volumen optimizada para minimizar la contención entre las E/S de la carga de trabajo de la aplicación y otro tráfico de la instancia de la aplicación. Las características del volumen, como tipo de I/o, tamaño de segmentos, propiedad de la controladora, y caché de lectura y escritura, se recomiendan y se optimizan automáticamente para las cargas de trabajo que se crean para los siguientes tipos de aplicaciones.
  - Microsoft SQL Server
  - Servidor de Microsoft Exchange
  - Aplicaciones de videovigilancia
  - VMware ESXi (para volúmenes que se usarán con Virtual Machine File System)

    Se puede revisar la configuración de volumen recomendada y editar, añadir o eliminar volúmenes y características recomendados por el sistema mediante el cuadro de diálogo Añadir/editar volúmenes.
- **Otros (o aplicaciones sin compatibilidad con la creación de volúmenes específicos)** — Otras cargas de trabajo utilizan una configuración de volumen que debe especificar manualmente cuando desea crear una carga de trabajo no asociada con una aplicación específica, o si no hay optimización integrada para la aplicación que piensa utilizar en la cabina de almacenamiento. Debe especificar manualmente la configuración del volumen en el cuadro de diálogo Añadir/editar volúmenes.

¿Por qué no se muestran todos los volúmenes, los hosts o los clústeres de hosts?

Los volúmenes Snapshot que incluyen un volumen base con la función DA habilitada no son aptos para asignarse a un host que no es compatible con la función Data Assurance (DA). Debe deshabilitar DA en el volumen base para poder asignar un volumen Snapshot a un host que no es compatible con DA.

Tenga en cuenta las siguientes directrices para el host al cual planea asignar el volumen Snapshot:

- Un host no es compatible con DA si está conectado a la cabina de almacenamiento a través de una interfaz de I/o que no es compatible con DA.
- Un clúster de hosts no es compatible con DA si tiene al menos un miembro de host que no es compatible con DA.

No se puede deshabilitar LA DA en un volumen asociado con Snapshot (grupos de coherencia, grupos Snapshot, imágenes Snapshot y volúmenes Snapshot), copias de volumen, y espejos. Toda la capacidad reservada y los objetos Snapshot asociados deben eliminarse para poder deshabilitar DA en el volumen base.

¿Por qué no se puede eliminar la carga de trabajo seleccionada?

Esta carga de trabajo consta de un grupo de volúmenes que se creó mediante la interfaz de línea de comandos (CLI) o se migró (se importó/exportó) de una cabina de almacenamiento diferente. Como resultado, los volúmenes de esta carga de trabajo no están asociados a una carga de trabajo específica de la aplicación, por lo que no es posible eliminar la carga de trabajo.

¿Cómo ayudan las cargas de trabajo específicas de la aplicación a gestionar la cabina de almacenamiento?

Las características de volumen de la carga de trabajo específica de la aplicación determinan la manera en que la carga de trabajo interactúa con los componentes de la cabina de almacenamiento, y ayudan a determinar el rendimiento de su entorno en una determinada configuración.

Una aplicación es un software, como SQL Server o Exchange. Se definen una o más cargas de trabajo que sean compatibles con cada aplicación. En algunas aplicaciones, el sistema recomienda automáticamente una configuración de volumen que optimice el almacenamiento. Las características como el tipo de I/o, el tamaño de segmento, la propiedad de controladora y la caché de lectura y escritura se incluyen en la configuración de volumen.

¿Qué debo hacer para reconocer la capacidad expandida?

Si se aumenta la capacidad de un volumen, es posible que el host no reconozca de inmediato el aumento de la capacidad del volumen.

La mayoría de los sistemas operativos reconocen la capacidad expandida del volumen y se expanden automáticamente después de que se inicia la expansión de volumen. Sin embargo, es posible que algunos no lo hagan. Si el sistema operativo no reconoce automáticamente la capacidad de volumen expandida, es posible que se deba volver a analizar el disco o reiniciar.

Después de haber expandido la capacidad del volumen, se debe aumentar manualmente el tamaño del sistema de archivos para que coincida. La forma de hacerlo depende del sistema de archivos utilizado.

Consulte la documentación del sistema operativo host para obtener más detalles.

¿Cuándo quieres usar la selección asignar el host más adelante?

Si desea acelerar el proceso para crear volúmenes, puede omitir el paso de asignación de host para que los volúmenes recién creados se inicialicen sin conexión.

Los volúmenes recién creados deben inicializarse. El sistema puede inicializarlos utilizando uno de los dos modos: Un proceso de inicialización en segundo plano de formato disponible inmediato (IAF) o un proceso fuera de línea.

Cuando se asigna un volumen a un host, se fuerza la inicialización de todos los volúmenes en ese grupo a realizar la transición a la inicialización en segundo plano. Este proceso de inicialización en segundo plano permite realizar operaciones de I/o del host simultáneas, que a veces pueden requerir mucho tiempo.

Cuando ninguno de los volúmenes de un grupo de volúmenes se asigna, se realiza una inicialización sin conexión. El proceso fuera de línea es mucho más rápido que el proceso en segundo plano.

¿Qué debo saber acerca de los requisitos de tamaño de bloque del host?

Para los sistemas EF300 y EF600, es posible configurar un volumen para que admita un tamaño de bloque de 512 bytes o 4 KiB (también llamado "tamaño de sector"). Debe configurar el valor correcto durante la creación del volumen. Si es posible, el sistema sugiere el valor predeterminado adecuado.

Antes de configurar el tamaño de bloque de volumen, lea las siguientes limitaciones y directrices.

- Algunos sistemas operativos y máquinas virtuales (principalmente VMware, por el momento) requieren un tamaño de bloque de 512 bytes y no admiten 4 KiB, por lo tanto, asegúrese de conocer los requisitos del host antes de crear un volumen. Por lo general, puede alcanzar el mejor rendimiento configurando un volumen para que presente un tamaño de bloque de 4 KiB; sin embargo, asegúrese de que su host permita bloques de 4 KiB (o “4Kn”).
- El tipo de unidades que se selecciona para el pool o el grupo de volúmenes también determina qué tamaños de bloque de volumen se admiten, como se indica a continuación:
  - Si se crea un grupo de volúmenes con unidades que escriben en bloques de 512 bytes, solo se pueden crear volúmenes con bloques de 512 bytes.
  - Si crea un grupo de volúmenes con unidades que escriben en bloques de 4 KiB, puede crear volúmenes con bloques de 512 bytes o 4 KiB.
- Si la cabina tiene una tarjeta de interfaz del host iSCSI, todos los volúmenes se limitan a bloques de 512 bytes (independientemente del tamaño de bloque del grupo de volúmenes). Esto se debe a una implementación específica del hardware.
- No se puede cambiar el tamaño de un bloque una vez configurado. Si necesita cambiar el tamaño de bloque, debe eliminar el volumen y volver a crearlo.

¿Por qué debería crear un clúster de hosts?

Debe crear un clúster de hosts si desea que dos o más hosts compartan el acceso al mismo conjunto de volúmenes. Por lo general, los hosts individuales tienen instalado

software de clustering a fin de coordinar el acceso a los volúmenes.

¿Cómo saber cuál es el tipo de sistema operativo de host correcto?

El campo Tipo de sistema operativo de host contiene el sistema operativo del host. Puede seleccionar el tipo de host recomendado en la lista desplegable.

Los tipos de hosts que aparecen en la lista desplegable dependen del modelo de cabina de almacenamiento y la versión del firmware. Las versiones más recientes muestran primero las opciones más comunes, que son las más probables ser apropiadas. La aparición en esta lista no implica que la opción esté totalmente admitida.

Para obtener más información sobre la compatibilidad con hosts, consulte "Herramienta de matriz de interoperabilidad de NetApp".

En la lista pueden aparecer algunos de los siguientes tipos de hosts:

Tipo de sistema operativo de host	Sistema operativo (SO) y controlador multivía
Linux DM-MP (Kernel 3.10 o posterior)	Es compatible con sistemas operativos Linux que utilizan una solución de conmutación por error multivía de Device Mapper con un kernel 3.10 o posterior.
VMware ESXi	Es compatible con los sistemas operativos VMware ESXi que ejecutan la arquitectura nativa del complemento multivía (NMP) mediante el módulo VMware incorporado Storage Array Type Policy SATP_ALUA.
Windows (en clúster o sin clúster)	Admite configuraciones en clúster o no en clúster de Windows que no ejecuten el controlador multivía de ATTO.
Clúster ATTO (todos los sistemas operativos)	Admite todas las configuraciones de clúster con el controlador ATTO Technology, Inc. Y multipathing.
Linux (Veritas DMP)	Admite sistemas operativos Linux mediante una solución multivía Veritas DMP.
Linux (ATTO)	Admite sistemas operativos Linux que usan un controlador ATTO Technology, Inc. Y multiruta.
So Mac	Admite versiones de Mac OS que usan un controlador ATTO Technology, Inc. Y multipathing.
Windows (ATTO)	Admite sistemas operativos Windows que usan un controlador ATTO Technology, Inc. Y multiruta.
FlexArray (ALUA)	Admite un sistema FlexArray de NetApp mediante ALUA para accesos múltiples.
SVC DE IBM	Es compatible con la configuración de la controladora de volúmenes SAN de IBM.

Tipo de sistema operativo de host	Sistema operativo (SO) y controlador multivía
Predeterminado de fábrica	Reservada para el inicio inicial de la cabina de almacenamiento. Si el tipo de sistema operativo del host está configurado como valor predeterminado de fábrica, cambie este valor para que coincida con el sistema operativo del host y el controlador multivía que se ejecuta en el host conectado.
Linux DM-MP (Kernal 3.9 o anterior)	Es compatible con sistemas operativos Linux que utilizan una solución de conmutación por error multivía de Device Mapper con un kernel 3.9 o anterior.
Ventana en clúster (obsoleto)	Si el tipo de sistema operativo del host está establecido en este valor, utilice la opción Windows (almacenado en clúster o no en clúster).

¿Cómo se emparejan los puertos de host con un host?

Si se crea manualmente un host, en primer lugar debe usarse la utilidad de adaptador de bus de host (HBA) adecuada disponible en el host para determinar los identificadores de puerto de host asociados con cada HBA instalada en el host.

Cuando cuente con esta información, seleccione los identificadores de puerto de host con los cuales se inició sesión en la cabina de almacenamiento de la lista proporcionada en el cuadro de diálogo Crear host.

Asegúrese de seleccionar los identificadores de puerto de host adecuados para el host que va a crear. Si asocia los identificadores de puerto de host incorrectos, es posible que se provoque un acceso no intencional de otro host a estos datos.

¿Qué es el clúster predeterminado?

El clúster predeterminado es una entidad definida por el sistema que permite que cualquier identificador de puerto de host no asociado que haya iniciado sesión en la cabina de almacenamiento acceda a los volúmenes asignados al clúster predeterminado.

Un identificador de puerto de host no asociado es un puerto de host que no está asociado de forma lógica con un host en particular, pero que se instala físicamente en un host y se inicia sesión en la cabina de almacenamiento.

Si desea que los hosts tengan acceso específico a ciertos volúmenes en la cabina de almacenamiento, no se debe utilizar el clúster predeterminado. En cambio, se deben asociar los identificadores del puerto de host con sus hosts correspondientes. Esta tarea se puede realizar manualmente durante la operación Crear host. A continuación, se deben asignar los volúmenes a un host individual o a un clúster de hosts.

Solo se debe usar el clúster predeterminado en situaciones especiales en las que el entorno de almacenamiento externo sea propicio para permitir que todos los hosts y todos los identificadores de puerto de host con sesión iniciada conectados a la cabina de almacenamiento tengan acceso a todos los volúmenes (modo de acceso total) sin dar a conocer específicamente los hosts a la cabina de almacenamiento o a la

interfaz de usuario.

Inicialmente, se pueden asignar los volúmenes solo al clúster predeterminado a través de la interfaz de línea de comandos (CLI). Sin embargo, luego de asignar al menos un volumen al clúster predeterminado, esta entidad (denominada clúster predeterminado) se muestra en la interfaz de usuario donde podrá gestionar esta entidad.

¿Qué es una comprobación de redundancia?

Una comprobación de redundancia determina si los datos de un volumen en un pool o grupo de volúmenes son consistentes. Los datos de redundancia se utilizan para reconstruir información rápidamente en una unidad de reemplazo si falla una de las unidades de un pool o grupo de volúmenes.

Es posible realizar esta comprobación solo en un pool o grupo de volúmenes a la vez. Una comprobación de redundancia de un volumen realiza las acciones siguientes:

- Escanea los bloques de datos en un volumen RAID 3, un volumen RAID 5 o un volumen RAID 6 y, a continuación, comprueba la información de redundancia de cada bloque. (RAID 3 solo puede asignarse a grupos de volúmenes con interfaz de línea de comandos.)
- Compara los bloques de datos en unidades reflejadas RAID 1.
- Devuelve errores de redundancia si el firmware de la controladora determina que los datos no son consistentes.

Si se ejecuta de inmediato una comprobación de redundancia en el mismo pool o grupo de volúmenes, se puede generar un error. Para evitar este problema, espere de uno a dos minutos antes de ejecutar otra comprobación de redundancia en el mismo pool o grupo de volúmenes.

¿Qué es la capacidad de conservación?

La capacidad de conservación es la cantidad de capacidad (cantidad de unidades) que se reserva en un pool para admitir fallos de unidad potenciales.

Cuando se crea un pool, el sistema reserva automáticamente una cantidad predeterminada de capacidad de conservación según el número de unidades del pool.

Los pools utilizan la capacidad de conservación durante la reconstrucción, mientras que los grupos de volúmenes utilizan unidades de pieza de repuesto con el mismo fin. El método de capacidad de conservación es una mejora con respecto a las unidades de pieza de repuesto, dado que permite realizar la reconstrucción con mayor rapidez. La capacidad de conservación se distribuye en varias unidades del pool, en lugar de en una unidad como en el caso de la unidad de repuesto, por lo que la velocidad o disponibilidad de una unidad no representan una limitación.

¿Cuál es el nivel de RAID óptimo para cada aplicación?

Para maximizar el rendimiento de un grupo de volúmenes, se debe seleccionar el nivel de RAID adecuado.

Es posible determinar el nivel de RAID apropiado si se conocen los porcentajes de escritura y lectura de las aplicaciones que acceden al grupo de volúmenes. Utilice la página rendimiento para obtener estos

porcentajes.

Niveles de RAID y rendimiento de la aplicación

RAID se basa en una serie de configuraciones, denominadas niveles, para determinar cómo los datos de redundancia y usuario se escriben en las unidades y se recuperan de ellas. Cada nivel de RAID proporciona diferentes funciones de rendimiento. Las aplicaciones con un porcentaje alto de lectura tendrán un buen rendimiento con volúmenes RAID 5 o RAID 6 debido al rendimiento de lectura destacado de las configuraciones RAID 5 y RAID 6.

Las aplicaciones con un porcentaje bajo de lectura (de escritura intensiva) no rinden tan bien con volúmenes RAID 5 o RAID 6. El rendimiento degradado resulta de la forma en que una controladora escribe los datos y los datos de redundancia en las unidades de un grupo de volúmenes RAID 5 o RAID 6.

Seleccione un nivel de RAID según la información siguiente.

RAID 0

Descripción:

- No redundante, modo de segmentación.
- RAID 0 segmenta los datos en todas las unidades del grupo de volúmenes.

Funciones de protección de datos:

- RAID 0 no se recomienda para necesidades de alta disponibilidad. RAID 0 es más adecuado para datos no cruciales.
- Si una unidad única falla en el grupo de volúmenes, todos los volúmenes asociados fallarán y se perderán todos los datos.

Requisitos del número de la unidad:

- Se requiere un mínimo de una unidad para el nivel de RAID 0.
- Los grupos de volúmenes de RAID 0 pueden tener más de 30 unidades.
- Es posible crear un grupo de volúmenes que incluya todas las unidades en la cabina de almacenamiento.

RAID 1 o RAID 10

Descripción:

- Modo de segmentación/reflejo.

Cómo funciona:

- RAID 1 utiliza las operaciones de mirroring de discos para escribir datos en dos discos duplicados en simultáneo.
- RAID 10 utiliza la segmentación de unidades para segmentar los datos de un conjunto de parejas de unidades reflejadas.

Funciones de protección de datos:

- RAID 1 y RAID 10 ofrecen alto rendimiento y la mejor disponibilidad de datos.

- RAID 1 y RAID 10 utilizan las operaciones de mirroring de unidades para realizar una copia exacta de una unidad en otra.
- Si una de las unidades de una pareja de unidades falla, la cabina de almacenamiento puede cambiar instantáneamente a la otra sin perder datos o servicios.
- Un fallo de unidad única provoca el estado degradado de los volúmenes asociados. La unidad reflejo permite acceder a los datos.
- Un fallo de la pareja de unidades en un grupo de volúmenes provoca el fallo de todos los volúmenes asociados, y podría ocurrir una pérdida de datos.

Requisitos del número de la unidad:

- Se requiere un mínimo de dos unidades para RAID 1: Una unidad para los datos de usuario y una unidad para los datos reflejados.
- Si se seleccionan cuatro o más unidades, RAID 10 se configura automáticamente en el grupo de volúmenes: Dos unidades para los datos de usuario y dos unidades para los datos reflejados.
- El grupo de volúmenes debe tener un número par de unidades. Si no se cuenta con un número par de unidades y quedan algunas sin asignar, vaya a **Pools y grupos de volúmenes** para añadir unidades adicionales al grupo de volúmenes y vuelva a intentar la operación.
- Los grupos de volúmenes de RAID 1 y RAID 10 pueden tener más de 30 unidades. Se puede crear un grupo de volúmenes que incluya todas las unidades de la cabina de almacenamiento.

RAID 5

Descripción:

- Modo de I/o elevado.

Cómo funciona:

- Los datos de usuario y la información redundante (paridad) se segmentan en las unidades.
- Se utiliza la capacidad equivalente de una unidad para la información redundante.

Funciones de protección de datos

- Si una unidad única falla en un grupo de volúmenes RAID 5, todos los volúmenes asociados se degradan. La información redundante permite que aún pueda accederse a los datos.
- Si dos o más unidades fallan en un grupo de volúmenes RAID 5, todos los volúmenes asociados fallarán y se perderán todos los datos.

Requisitos del número de la unidad:

- Se debe contar con un mínimo de tres unidades en el grupo de volúmenes.
- Por lo general, el grupo de volúmenes tiene un límite máximo de 30 unidades.

RAID 6

Descripción:

- Modo de I/o elevado.

Cómo funciona:

- Los datos de usuario y la información redundante (doble paridad) se segmentan en las unidades.
- Se utiliza la capacidad equivalente de dos unidades para la información redundante.

Funciones de protección de datos:

- Si una o dos unidades fallan en un grupo de volúmenes RAID 6, todos los volúmenes asociados se degradarán, pero la información redundante permitirá que aún pueda accederse a los datos.
- Si tres o más unidades fallan en un grupo de volúmenes RAID 6, todos los volúmenes asociados fallarán y se perderán todos los datos.

Requisitos del número de la unidad:

- Se debe contar con un mínimo de cinco unidades en el grupo de volúmenes.
- Por lo general, el grupo de volúmenes tiene un límite máximo de 30 unidades.

No es posible cambiar el nivel de RAID de un pool. La interfaz de usuario configura automáticamente los pools como RAID 6.

Niveles de RAID y protección de datos

RAID 1, RAID 5 y RAID 6 escriben los datos de redundancia en los medios de la unidad para la tolerancia a fallos. Los datos de redundancia pueden ser una copia de los datos (reflejados) o un código de corrección de error derivado de los datos. Es posible utilizar los datos de redundancia para reconstruir información rápidamente en una unidad de reemplazo si se produce un error en una unidad.

Se configura un nivel de RAID único en un grupo de volúmenes único. Todos los datos de redundancia de ese grupo de volúmenes se almacenan en el grupo de volúmenes. La capacidad del grupo de volúmenes es la capacidad agregada de las unidades miembro menos la capacidad reservada para los datos de redundancia. La cantidad de capacidad necesaria para la redundancia depende del nivel de RAID utilizado.

¿Por qué no se muestran algunas unidades?

En el cuadro de diálogo Añadir capacidad, no todas las unidades se encuentran disponibles para añadir capacidad a un pool o grupo de volúmenes existente.

Las unidades no serán elegibles por cualquiera de los motivos siguientes:

- Una unidad debe estar sin asignar y no debe tener la función de seguridad habilitada. Las unidades que son parte de otro pool, de otro grupo de volúmenes o que están configuradas como pieza de repuesto no son elegibles. Si una unidad está sin asignar, pero tiene la función de seguridad habilitada, se debe eliminar manualmente esa unidad para que sea elegible.
- Una unidad que se encuentra en un estado distinto a Optimal no es elegible.
- Si una unidad tiene muy poca capacidad, no es elegible.
- El tipo de medios de la unidad debe coincidir dentro de un pool o grupo de volúmenes. No puede mezclar lo siguiente:
  - Unidades de disco duro (HDD) con discos de estado sólido (SSD)
  - NVMe con unidades SAS
  - Unidades con tamaños de bloques de volúmenes de 512 bytes y 4 KiB

- Si todas las unidades de un pool o un grupo de volúmenes son compatibles con la función de seguridad, las unidades no compatibles con la función de seguridad no se enumeran.
- Si un pool o grupo de volúmenes contiene todas unidades compatibles con el estándar de procesamiento de información federal (FIPS), las unidades no compatibles con FIPS no se enumeran.
- Si un pool o grupo de volúmenes contiene todas unidades compatibles con la función Garantía de datos (DA) y al menos un volumen del pool o grupo de volúmenes tiene habilitada la función DA, una unidad que no sea compatible con DA no es elegible, por lo que no puede añadirse a ese pool o grupo de volúmenes. Sin embargo, si ningún volumen tiene la función DA habilitada en el pool o grupo de volúmenes, una unidad que no sea compatible con LA función DA puede añadirse a ese pool o grupo de volúmenes. Si decide combinar estas unidades, tenga en cuenta que no podrá crear ningún volumen con la función DA habilitada.

Es posible aumentar la capacidad de la cabina de almacenamiento con la adición de unidades nuevas o la eliminación de pools o grupos de volúmenes.

¿Por qué no es posible aumentar la capacidad de conservación?

Si se crearon volúmenes en toda la capacidad utilizable disponible, es posible que no se pueda aumentar la capacidad de conservación.

La capacidad de conservación es la cantidad de capacidad (número de unidades) reservada en un pool para dar soporte a fallos de unidad potenciales. Cuando se crea un pool, el sistema reserva automáticamente una cantidad predeterminada de capacidad de conservación según el número de unidades del pool. Si creó volúmenes en toda la capacidad utilizable disponible, no puede aumentar la capacidad de conservación sin agregar capacidad al pool, ya sea sumando unidades o eliminando volúmenes.

Es posible cambiar la capacidad de conservación de los pools y los grupos de volúmenes. Seleccione el pool que desea editar. Haga clic en **Ver/editar configuración** y, a continuación, seleccione la ficha **Configuración**.

La capacidad de conservación se especifica como el número de unidades, a pesar de que la capacidad de conservación real se distribuya en las unidades del pool.

¿Qué es la garantía de datos?

La garantía de datos (DA) implementa el estándar de información de protección (PI) T10, con el cual se comprueban y corrigen los errores que se pueden producir durante la transferencia de datos a través de la ruta de I/o con el fin de aumentar la integridad de los datos.

El uso típico de la función Garantía de datos es revisar la porción de la ruta de I/o entre las controladoras y las unidades. Las funcionalidades DE DA se presentan a nivel del pool y grupo de volúmenes.

Si esta función está habilitada, la cabina de almacenamiento añade códigos de comprobación de errores (también conocidos como comprobaciones de redundancia cíclicas o CRC) a cada bloque de datos del volumen. Una vez movido un bloque de datos, la cabina de almacenamiento utiliza estos códigos de CRC para determinar si se produjeron errores durante la transmisión. Los datos posiblemente dañados no se escriben en el disco ni se vuelven a transferir al host. Si desea utilizar la función DA, seleccione un pool o grupo de volúmenes compatible con DA al crear un volumen nuevo (busque **Sí** junto a **DA** en la tabla de

candidatos de pools y grupos de volúmenes).

Asegúrese de asignar estos volúmenes con la función DA habilitada a un host que utilice una interfaz de I/o compatible con DA. Las interfaces de I/o compatibles con DA son Fibre Channel, SAS, iSCSI over TCP/IP, NVMe/FC, NVMe/IB, NVME/roce e Iser over InfiniBand (extensiones iSCSI para RDMA/IB). SRP over InfiniBand no es compatible con DA.

¿Qué es la seguridad FDE/FIPS?

La seguridad FDE/FIPS hace referencia a unidades compatibles con la función de seguridad que cifran datos durante las escrituras y los descifran durante las lecturas mediante una clave de cifrado única.

Estas unidades compatibles con la función de seguridad evitan el acceso no autorizado a los datos en una unidad que se quita físicamente de la cabina de almacenamiento. 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). Las unidades FIPS se sometieron a pruebas de certificación.

> Para los volúmenes que requieren compatibilidad FIPS, se deben utilizar solo 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, no se puede agregar una unidad FDE ni utilizarse como reserva en un pool o grupo de volúmenes FIPS.

¿Qué significa ser compatible con la función de seguridad (Drive Security)?

Drive Security es una función que evita el acceso no autorizado a datos almacenados en unidades con la función de seguridad habilitada cuando la unidad se quita de la cabina de almacenamiento.

Estas unidades pueden ser unidades de cifrado de disco completo (FDE) o de estándar de procesamiento de información federal (FIPS).

¿Cómo se visualizan y se interpretan todas las estadísticas de caché SSD?

Es posible visualizar estadísticas nominales y detalladas para la caché SSD.

Las estadísticas nominales son un subconjunto de las estadísticas detalladas. Las estadísticas detalladas se pueden visualizar solo cuando se exportan todas las estadísticas de SSD a un archivo .csv. Al revisar e interpretar las estadísticas, tenga en cuenta que algunas interpretaciones provienen del análisis de una combinación de estadísticas.

Estadísticas nominales

Para ver las estadísticas de la caché SSD, vaya a la página **Administrar**. Seleccione MENU:Provisioning[Configure Pools & Volume Groups]. Seleccione la caché SSD sobre la cual desea ver estadísticas y, a continuación, seleccione MENU:más[Ver estadísticas]. Las estadísticas nominales se muestran en el cuadro de diálogo Ver estadísticas de la caché SSD.

Esta función no está disponible en los sistemas de almacenamiento EF600 o EF300.

En la lista, se incluyen estadísticas nominales, que son un subconjunto de las estadísticas detalladas.

Estadística detallada

Las estadísticas detalladas consisten en las estadísticas normales más las estadísticas adicionales. Estas estadísticas adicionales se guardan junto con las estadísticas nominales; pero, a diferencia de las estadísticas nominales, no se muestran en el cuadro de diálogo Ver estadísticas de la caché SSD. Es posible ver las estadísticas detalladas solo después de exportar las estadísticas a un archivo .csv.

Las estadísticas detalladas se enumeran después de las estadísticas nominales.

¿Qué son la protección contra pérdida de bandeja y la protección contra pérdida de cajón?

La protección contra pérdida de bandeja y de cajón son atributos de los pools y los grupos de volúmenes para mantener el acceso a los datos en caso de fallo de una bandeja o un cajón individuales.

Protección contra pérdida de bandeja

Una bandeja es el compartimento que contiene las unidades o las unidades y la controladora. La protección contra pérdida de bandeja garantiza la accesibilidad a los datos en los volúmenes de un pool o un grupo de volúmenes en caso de pérdida total de comunicación con una bandeja de unidades única. Un ejemplo de pérdida total de comunicación podría ser la pérdida de energía en la bandeja de unidades o el fallo de ambos módulos de I/o (IOM).

La protección contra pérdida de bandeja no está garantizada si una unidad ya falló en el pool o en el grupo de volúmenes. En este caso, la pérdida de acceso a la bandeja de unidades y, en consecuencia, a otra unidad en el pool o el grupo de volúmenes provoca la pérdida de datos.

El criterio de protección contra pérdida de bandeja depende del método de protección, tal como se describe en la tabla siguiente.

Nivel	Criterios para la protección contra pérdida de bandeja	Cantidad mínima requerida de bandejas
Piscina	El pool debe incluir unidades de al menos cinco bandejas y debe haber la misma cantidad de unidades en cada bandeja. La protección contra pérdida de bandeja no es aplicable a las bandejas de gran capacidad; si el sistema incluye bandejas de gran capacidad, consulte la protección contra pérdida de cajón.	5
RAID 6	El grupo de volúmenes consta de dos unidades como máximo en un solo cajón.	3

Nivel	Criterios para la protección contra pérdida de bandeja	Cantidad mínima requerida de bandejas
RAID 3 o RAID 5	Cada unidad del grupo de volúmenes se encuentra en una bandeja aparte.	3
RAID 1	Cada unidad de una pareja RAID 1 se debe ubicar en una bandeja aparte.	2
RAID 0	No puede contar con protección contra pérdida de bandeja.	No aplicable

Protección contra pérdida de cajón

Un cajón es uno de los compartimentos de una bandeja que se extrae para acceder a las unidades. Solo las bandejas de gran capacidad poseen cajones. La protección contra pérdida de cajón garantiza la accesibilidad a los datos en los volúmenes de un pool o un grupo de volúmenes en caso de pérdida total de comunicación con un cajón único. Un ejemplo de pérdida total de comunicación podría ser la pérdida de energía en el cajón o el fallo de un componente interno dentro del cajón.

La protección contra pérdida de cajón no está garantizada si una unidad ya falló en el pool o en el grupo de volúmenes. En este caso, la pérdida de acceso al cajón (y, en consecuencia, a otra unidad en el pool o el grupo de volúmenes) provoca la pérdida de datos.

El criterio de protección contra pérdida de cajón depende del método de protección, tal como se describe en la tabla siguiente:

Nivel	Criterios para la protección contra pérdida de cajón	Cantidad mínima requerida de cajones
Piscina	Los candidatos de pool deben incluir unidades de todos los cajones y debe haber la misma cantidad de unidades por cajón. El pool debe incluir unidades de al menos cinco cajones y debe haber la misma cantidad de unidades por cajón. Una bandeja de 60 unidades puede contar con protección contra pérdida de cajón cuando el pool consta de 15, 20, 25, 30, 35, 40, 45, 50, 55 o 60 unidades. Los incrementos en múltiplos de 5 se pueden agregar al pool después de la creación inicial.	5
RAID 6	El grupo de volúmenes consta de dos unidades como máximo en un solo cajón.	3
RAID 3 o 5	Cada unidad del grupo de volúmenes se encuentra en un cajón aparte	3

Nivel	Criterios para la protección contra pérdida de cajón	Cantidad mínima requerida de cajones
RAID 1	Cada unidad de una pareja reflejada se debe ubicar en un cajón aparte.	2
RAID 0	No puede contar con protección contra pérdida de cajón.	No aplicable

¿Cómo se mantiene la protección contra pérdida de bandeja y cajón?

Para mantener la protección contra pérdida de bandeja y cajón para un pool o un grupo de volúmenes, use los criterios especificados en la siguiente tabla.

Nivel	Criterios para la protección contra pérdida de bandeja/cajón	Cantidad mínima de bandejas/cajones requeridos
Piscina	Para las bandejas, el pool no debe contener más de dos unidades en una sola bandeja. Para los cajones, el pool debe incluir la misma cantidad de unidades en cada uno de ellos.	6 para bandejas 5 para cajones
RAID 6	El grupo de volúmenes no contiene más de dos unidades por bandeja o cajón.	3
RAID 3 o RAID 5	Cada unidad del grupo de volúmenes está ubicada en una bandeja o un cajón por separado.	3
RAID 1	Cada unidad de una pareja reflejada debe ubicarse en una bandeja o un cajón por separado.	2
RAID 0	No se puede lograr la protección contra pérdida de bandeja/cajón.	No aplicable

La protección contra pérdida de bandeja/cajón no se mantiene si una unidad ya tuvo fallos en el pool o el grupo de volúmenes. En este caso, la pérdida de acceso a la bandeja o el cajón de unidades y, en consecuencia, a otra unidad en el pool o el grupo de volúmenes provoca la pérdida de datos.

¿Qué es la capacidad de optimización para pools?

Las unidades SSD tendrán una mayor vida útil y mejor rendimiento de escritura máximo cuando una parte de su capacidad no está asignada.

Para las unidades asociadas con un pool, la capacidad sin asignar consta de la capacidad de conservación de un pool, la capacidad libre (capacidad que no usan los volúmenes) y una parte de la capacidad utilizable como

capacidad de optimización adicional. La capacidad de optimización adicional garantiza un nivel mínimo de capacidad de optimización mediante la reducción de la capacidad utilizable, y, como tal, no está disponible para la creación de volúmenes.

Cuando se crea un pool, se genera una capacidad de optimización recomendada que ofrece un equilibrio del rendimiento, la vida útil de la unidad y la capacidad disponible. El control deslizante capacidad de optimización adicional ubicado en el cuadro de diálogo Configuración del pool permite ajustar la capacidad de optimización del pool. El ajuste del control deslizante proporciona un mejor rendimiento y una mayor vida útil de la unidad cuando se descuenta la capacidad disponible, o bien capacidad disponible adicional, costa del rendimiento y la vida útil de la unidad.

> El control deslizante de capacidad de optimización adicional solo está disponible para los sistemas de almacenamiento EF600 y EF300.

¿Qué es la capacidad de optimización de los grupos de volúmenes?

Las unidades SSD tendrán una mayor vida útil y mejor rendimiento de escritura máximo cuando una parte de su capacidad no está asignada.

Para las unidades asociadas con un grupo de volúmenes, la capacidad sin asignar consta de la capacidad libre de un grupo de volúmenes (capacidad que no utilizan los volúmenes) y una parte del conjunto de capacidad utilizable como capacidad de optimización. La capacidad de optimización adicional garantiza un nivel mínimo de capacidad de optimización mediante la reducción de la capacidad utilizable, y, como tal, no está disponible para la creación de volúmenes.

Cuando se crea un grupo de volúmenes, se genera una capacidad de optimización recomendada que ofrece un equilibrio entre rendimiento, vida útil de la unidad y capacidad disponible. El control deslizante capacidad de optimización adicional en el cuadro de diálogo Configuración del grupo de volúmenes permite ajustar la capacidad de optimización de un grupo de volúmenes. El ajuste del control deslizante proporciona un mejor rendimiento y una mayor vida útil de la unidad cuando se descuenta la capacidad disponible, o bien capacidad disponible adicional, costa del rendimiento y la vida útil de la unidad.

> El control deslizante de capacidad de optimización adicional solo está disponible para los sistemas de almacenamiento EF600 y EF300.

¿Qué permite el aprovisionamiento de recursos?

El aprovisionamiento de recursos es una función disponible en las cabinas de almacenamiento EF300 y EF600, lo que permite poner en uso los volúmenes de inmediato sin proceso de inicialización en segundo plano.

Un volumen aprovisionado por recursos es un volumen grueso de un grupo de volúmenes SSD o pool, donde se asigna capacidad de la unidad (asignada al volumen) cuando se crea el volumen, pero los bloques de unidades no se asignan (anula la asignación). En comparación, en un volumen grueso tradicional, todos los bloques de unidades se asignan o se asignan durante una operación de inicialización de volúmenes en segundo plano para inicializar los campos de información de protección de Data Assurance y para hacer que la paridad de datos y RAID sea coherente en cada franja de RAID. Con un volumen aprovisionado, no existe una inicialización en segundo plano vinculada al tiempo. En su lugar, cada franja RAID se inicializa con la primera escritura en un bloque de volumen en la franja.

Los volúmenes aprovisionados mediante recursos solo se admiten en los grupos de volúmenes SSD y pools, donde todas las unidades del grupo o pool admiten la funcionalidad de recuperación de error de bloque lógico no escrito o desasignado (DULBE). Cuando se crea un volumen aprovisionado por recursos, todos los bloques de unidades asignados al volumen se desasignan (desasignan). Asimismo, los hosts pueden desasignar bloques lógicos del volumen mediante el comando Gestión de conjuntos de datos de NVMe. Si se desasignan bloques, es posible mejorar la vida útil de las unidades de estado sólido y aumentar el rendimiento de escritura máximo. La mejora varía en función del modelo y la capacidad de cada unidad.

¿Qué debo saber acerca de la función de volúmenes aprovisionados mediante recursos?

El aprovisionamiento de recursos es una función disponible en las cabinas de almacenamiento EF300 y EF600, lo que permite poner en uso los volúmenes de inmediato sin proceso de inicialización en segundo plano.

> La función de aprovisionamiento de recursos no está disponible en este momento. En algunas vistas, los componentes pueden notificarse como compatibles con el aprovisionamiento de recursos, pero se ha deshabilitado la capacidad para crear volúmenes aprovisionados mediante recursos hasta que se pueda volver a habilitar en una actualización futura.

Volúmenes aprovisionados mediante recursos

Un volumen aprovisionado por recursos es un volumen grueso de un grupo de volúmenes SSD o pool, donde se asigna capacidad de la unidad (asignada al volumen) cuando se crea el volumen, pero los bloques de unidades no se asignan (anula la asignación). En comparación, en un volumen grueso tradicional, todos los bloques de unidades se asignan o se asignan durante una operación de inicialización de volúmenes en segundo plano para inicializar los campos de información de protección de Data Assurance y para hacer que la paridad de datos y RAID sea coherente en cada franja de RAID. Con un volumen aprovisionado, no existe una inicialización en segundo plano vinculada al tiempo. En su lugar, cada franja RAID se inicializa con la primera escritura en un bloque de volumen en la franja.

Los volúmenes aprovisionados mediante recursos solo se admiten en los grupos de volúmenes SSD y pools, donde todas las unidades del grupo o pool admiten la funcionalidad de recuperación de error de bloque lógico no escrito o desasignado (DULBE). Cuando se crea un volumen aprovisionado por recursos, todos los bloques de unidades asignados al volumen se desasignan (desasignan). Asimismo, los hosts pueden desasignar bloques lógicos del volumen mediante el comando Gestión de conjuntos de datos de NVMe. Si se desasignan bloques, es posible mejorar la vida útil de las unidades de estado sólido y aumentar el rendimiento de escritura máximo. La mejora varía en función del modelo y la capacidad de cada unidad.

Habilitar y deshabilitar la función

El aprovisionamiento de recursos está habilitado de forma predeterminada en sistemas donde las unidades admiten DULBE. Puede deshabilitar esa configuración predeterminada en Pools y grupos de volúmenes. La deshabilitación del aprovisionamiento de recursos es una acción permanente para los volúmenes existentes y no se puede revertir (es decir, no se puede volver a habilitar el aprovisionamiento de recursos para estos grupos de volúmenes y pools).

Sin embargo, si desea volver a habilitar el aprovisionamiento de recursos para los volúmenes nuevos que cree, puede hacerlo en **Settings › System**. Tenga en cuenta que cuando se vuelve a habilitar el aprovisionamiento de recursos, solo se ven afectados los grupos de volúmenes y pools recién creados. Todos los grupos de volúmenes y pools existentes se mantendrán sin cambios. Si lo desea, también puede deshabilitar el aprovisionamiento de recursos de nuevo desde MENU:Settings[System].

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

Cuando se implementa la función Drive Security, es posible 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).

¿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.

Gestión de claves internas

Las claves internas se mantienen y se “ocultan” en una ubicación sin acceso en la memoria persistente del controlador. 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.

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). 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. Obtener un archivo de certificado de cliente firmado. Un certificado de cliente valida las controladoras de la cabina de almacenamiento para que el servidor de gestión de claves pueda confiar en sus solicitudes KMIP.
   a. En primer lugar, complete y descargue una solicitud de firma de certificación (CSR) de cliente. Vaya a menú:Configuración[certificados > Gestión de claves > completar CSR].
   b. A continuación, se solicita un certificado de cliente firmado de una CA de confianza para el servidor de gestión de claves. (También se puede crear y descargar un certificado de cliente desde el servidor de gestión de claves con el archivo CSR descargado).
   c. Una vez que tenga un archivo de certificado de cliente, copie ese archivo en el host en el que accede a System Manager.
4. Recupere un archivo de certificado del servidor de gestión de claves y copie ese archivo en el host donde accede a System Manager. Un certificado de servidor de gestión de claves valida el servidor de gestión de claves para que la cabina de almacenamiento pueda confiar en su dirección IP. Es posible usar un certificado raíz, intermedio o de servidor para el servidor de gestión de claves.

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.