Unified Manager de SANtricity

SANtricity 11.9

NetApp
February 14, 2025

Tabla de contenidos

Gestión de varias cabinas con SANtricity Unified Manager 7

Interfaz principal

Información general de la interfaz de SANtricity Unified Manager

Unified Manager de SANtricity es una interfaz basada en Web que permite gestionar varias cabinas de almacenamiento en una sola vista.

Página principal

Al iniciar sesión en Unified Manager, la página principal se abre en **gestionar - todo**. En esta página, puede desplazarse por una lista de cabinas de almacenamiento detectadas en la red, ver su estado y realizar operaciones en una sola cabina o en un grupo de cabinas.

Barra lateral Navegación

Puede acceder a las funciones y funciones de Unified Manager desde la barra lateral de navegación.

Zona	Descripción
Gestione	Detecte las cabinas de almacenamiento en la red, inicie la instancia de SANtricity System Manager de una cabina, importe la configuración de una cabina a varias, y gestione grupos de cabinas. Marque las casillas de comprobación junto a los nombres de las cabinas para realizar distintas operaciones, como importar configuraciones y crear grupos de cabinas. Los tres puntos al final de cada fila permiten acceder al menú en línea con las operaciones para cada cabina, por ejemplo, las operaciones de cambio de nombre.
Operaciones	Vea el progreso de las operaciones en lote, como la importación de la configuración de una cabina a otra. Algunas operaciones no están disponibles si una cabina de almacenamiento no tiene un estado óptimo.
Gestión de certificados	Administrar certificados para autenticar entre exploradores y clientes.
Access Management	Establezca la autenticación de usuario para la interfaz de Unified Manager.
Soporte técnico	Vea opciones de soporte técnico, recursos y contactos.

La configuración de la interfaz y la ayuda

En la parte superior derecha de la interfaz, puede acceder a la Ayuda y a otra documentación. También puede acceder a las opciones de administración que están disponibles en el menú desplegable junto a su nombre de inicio de sesión.

Inicios de sesión y contraseñas de usuario

El usuario actual que ha iniciado sesión en el sistema se muestra en la esquina superior derecha de la interfaz.

Para obtener más información sobre usuarios y contraseñas, consulte:

- "Configure la protección con contraseña de administrador"
- "Cambie la contraseña de administrador"
- "Cambiar contraseñas de perfiles de usuario local"

Exploradores compatibles

Para acceder a SANtricity Unified Manager pueden usarse varios tipos de exploradores.

Se admiten los siguientes exploradores en las versiones mencionadas.

Navegador	Versión mínima
Google Chrome	89
Mozilla Firefox	80
Safari	14
Microsoft Edge	90

El proxy de servicios web debe estar instalado y disponible para el explorador.

Configure la protección con contraseña de administrador

Debe configurar Unified Manager de SANtricity con una contraseña de administrador para proteger la instancia del acceso no autorizado.

Contraseña de administrador y perfiles de usuario

Cuando se inicia Unified Manager por primera vez, se le solicita que establezca una contraseña de administrador. Cualquier usuario que tenga la contraseña de administrador puede realizar cambios de configuración en las cabinas de almacenamiento.

Además de la contraseña de administrador, la interfaz de Unified Manager incluye perfiles de usuario preconfigurados con uno o varios roles asignados. Para obtener más información, consulte "Cómo funciona Access Management".

Los usuarios y las asignaciones no pueden cambiarse. Solo las contraseñas pueden modificarse. Para cambiar las contraseñas, consulte:

- "Cambie la contraseña de administrador"
- "Cambiar contraseñas de perfiles de usuario local"

Tiempos de espera de sesión

El software solicita la contraseña una sola vez durante una misma sesión de gestión. De forma predeterminada, una sesión finaliza a los 30 minutos de inactividad; después de ese plazo, deberá introducir la contraseña otra vez. Si otro usuario accede al software desde otro cliente de gestión y cambia la contraseña mientras su sesión está en progreso, se le solicitará a usted una contraseña la próxima vez que intente realizar una operación de configuración o de vista.

Por razones de seguridad, puede intentar introducir una contraseña solo cinco veces antes de que el software quede bloqueado. En este estado, el software rechaza cualquier nuevo intento de introducir una contraseña. Se deben esperar 10 minutos para que el software se restablezca a un estado normal y usted pueda volver a introducir una contraseña.

Es posible ajustar los tiempos de espera de la sesión, o bien directamente pueden deshabilitarse los tiempos de espera de sesión. Para obtener más información, consulte "Gestionar los tiempos de espera de sesión".

Cambie la contraseña de administrador

Es posible cambiar la contraseña de administrador que se utiliza para acceder a SANtricity Unified Manager.

Antes de empezar

- Inició sesión como administrador local, lo que incluye permisos de administrador raíz.
- Debe conocer la contraseña de administrador actual.

Acerca de esta tarea

Tenga en cuenta estas directrices al elegir una contraseña:

- Las contraseñas distinguen mayúsculas de minúsculas.
- Los espacios al final de la contraseña no se eliminan si se los utiliza. Procure incluir espacios si se incluyeron en la contraseña.
- Para mayor seguridad, use al menos 15 caracteres alfanuméricos y cambie la contraseña con frecuencia.

Pasos

1. Seleccione MENU:Settings[Access Management].
2. Seleccione la ficha **roles de usuario local**.
3. Seleccione el usuario **admin** de la tabla.

   Se habilita el botón Cambiar contraseña.

4. Seleccione **Cambiar contraseña**.

   Se abre el cuadro de diálogo Cambiar contraseña.

5. Si no se estableció una longitud mínima para las contraseñas de usuario local, marque la casilla de aprobación para solicitarle al usuario que introduzca una contraseña a fin de acceder al sistema.
6. Introduzca la nueva contraseña en los dos campos.
7. Introduzca su contraseña de administrador local para confirmar esta operación y, a continuación, haga clic en **Cambiar**.

Gestionar los tiempos de espera de sesión

Es posible configurar 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 Unified 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. En la barra de menú, seleccione la flecha desplegable junto a su nombre de inicio de sesión.
2. Seleccione **Activar/Desactivar tiempo de espera de sesión**.

   Se abre el cuadro de diálogo Habilitar/deshabilitar tiempo de espera de la sesión.

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

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

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

4. Haga clic en **Guardar**.

Cabinas de almacenamiento

Información general de detección

Para gestionar los recursos de almacenamiento, primero se deben detectar las cabinas de almacenamiento en la red.

¿Cómo se detectan cabinas?

Utilice la página Añadir/detectar para encontrar y añadir las cabinas de almacenamiento que desea gestionar en la red de la organización. Es posible detectar varias cabinas de almacenamiento o una sola. Para hacerlo, debe introducir direcciones IP de red y, a continuación, Unified Manager intentar establecer conexiones individuales con cada dirección IP de ese rango.

Obtenga más información:

- "Consideraciones sobre la detección de cabinas"
- "Detectar varias cabinas de almacenamiento"
- "Detectar una sola cabina"

¿Cómo se gestionan las cabinas?

Después de descubrir las matrices, vaya a la página **gestionar - todo**. En esta página, puede desplazarse por una lista de cabinas de almacenamiento detectadas en la red, ver su estado y realizar operaciones en una sola cabina o en un grupo de cabinas.

Si desea gestionar una sola cabina, puede seleccionarla y abrir System Manager.

Obtenga más información:

- "Consideraciones para acceder a System Manager"
- "Gestione una cabina de almacenamiento individual"
- "Ver el estado de la cabina de almacenamiento"

Conceptos

Consideraciones sobre la detección de cabinas

Para poder mostrar y gestionar los recursos de almacenamiento, SANtricity Unified Manager debe detectar las cabinas de almacenamiento que se desean gestionar en la red de la organización. Es posible detectar varias cabinas de almacenamiento o una sola.

Detección de varias cabinas de almacenamiento

Si decide detectar varias cabinas de almacenamiento, debe introducir un rango de direcciones IP de red. A continuación, Unified Manager intentar establecer conexiones individuales con cada dirección IP de ese rango. Cada cabina de almacenamiento a la que se accedió correctamente se muestra en la página detectar y se puede añadir al dominio de gestión.

Detección de una sola cabina de almacenamiento

Si decide detectar una sola cabina de almacenamiento, debe introducir la dirección IP única para una de las controladoras de la cabina de almacenamiento. A continuación, se añade la cabina de almacenamiento individual.

> Unified Manager detecta y muestra solamente la dirección IP única o la dirección IP dentro del rango asignado a una controladora. Si existen controladoras alternativas o direcciones IP asignadas a estas controladoras que no se incluyen en esta dirección IP única o este rango de direcciones IP, Unified Manager no las detectará ni las mostrará. Sin embargo, una vez añadida la cabina de almacenamiento, se detectarán todas las direcciones IP asociadas y se mostrarán en la vista gestionar.

Credenciales de usuario

Como parte del proceso de detección, debe suministrar la contraseña de administrador para cada cabina de almacenamiento que desee añadir.

Certificados de servicios web

Como parte del proceso de detección, Unified Manager verifica que las cabinas de almacenamiento detectadas utilicen certificados de un origen de confianza. Unified Manager utiliza dos tipos de autenticación basada en certificados para todas las conexiones que establece con el explorador:

- **Certificados de confianza**

  Para las cabinas de almacenamiento detectadas mediante Unified Manager, es posible que deba instalar certificados de confianza adicionales suministrados por la entidad de certificación.

  Utilice el botón **Importar** para importar estos certificados. Si ya se conectó a esta cabina anteriormente, los certificados de una o ambas controladoras caducaron o se revocaron, o no se encuentra un certificado intermedio o de raíz en la cadena de certificados, Debe sustituir el certificado caducado o revocado, o añadir el certificado intermedio o de raíz ausente para gestionar la cabina de almacenamiento.

- **Certificados autofirmados**

  Además, se pueden utilizar certificados autofirmados. Si el administrador intenta detectar las cabinas sin importar los certificados firmados, Unified Manager muestra un cuadro de diálogo de error en el que el administrador puede aceptar el certificado autofirmado. El certificado autofirmado de la cabina de almacenamiento se marcará como de confianza y la cabina de almacenamiento se añadirá a Unified Manager.

  Si no confía en las conexiones a la cabina de almacenamiento, seleccione **Cancelar** y valide la estrategia de certificación de seguridad de la cabina de almacenamiento antes de añadir la cabina de almacenamiento a Unified Manager.

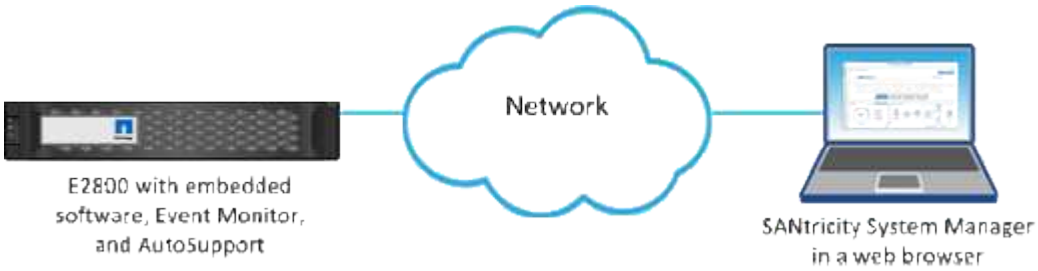
Consideraciones para acceder a System Manager de SANtricity

Es posible seleccionar una o varias cabinas de almacenamiento y usar la opción Iniciar para abrir SANtricity System Manager cuando se desean configurar y gestionar las cabinas de almacenamiento.

System Manager es una aplicación integrada en las controladoras, que está conectada a la red a través de un puerto de gestión Ethernet. Incluye todas las funciones basadas en cabina.

Para acceder a System Manager, debe tener:

- Uno de los modelos de matriz aquí enumerados: "Información general del hardware de E-Series"
- Una conexión fuera de banda con un cliente de administración de red en un explorador web.



Detectar cabinas de almacenamiento

Detectar varias cabinas de almacenamiento

Detecte varias cabinas para descubrir todas las cabinas de almacenamiento de la subred donde reside el servidor de gestión y añadir automáticamente las cabinas detectadas al dominio de gestión.

Antes de empezar

- Inició sesión con un perfil de usuario que cuenta con permisos de administración de seguridad.
- La cabina de almacenamiento debe estar instalada y configurada correctamente.
- Las contraseñas de las cabinas de almacenamiento deben configurarse mediante el icono Access Management de System Manager.
- Para resolver certificados que no son de confianza, debe tener archivos de certificado de confianza de una entidad de certificación (CA) y los archivos de certificado están disponibles en el sistema local.

La detección de cabinas es un procedimiento de varios pasos.

Paso 1: Introduzca la dirección de red

Se debe introducir un rango de direcciones de red para buscar dentro de la subred local. Todas las cabinas a las que se puede acceder correctamente se muestran en la página detectar, y se pueden añadir al dominio de gestión.

Si necesita detener la operación de detección por cualquier motivo, haga clic en **Detener detección**.

Pasos

1. En la página gestionar, seleccione **Agregar/detectar**.

   Se muestra el cuadro de diálogo Añadir/detectar.

2. Seleccione el botón de opción **detectar todas las cabinas de almacenamiento en un rango de red**.
3. Introduzca la dirección de red inicial y la dirección de red final para buscar en la subred local y, a continuación, haga clic en **Iniciar detección**.

   Se inicia el proceso de detección. El proceso puede tardar varios minutos en completarse. La tabla de la página detectar se carga a medida que se van detectando las cabinas de almacenamiento.

   > Si no se detectan cabinas gestionables, compruebe que las cabinas de almacenamiento estén bien conectadas a la red y que las direcciones asignadas se encuentren dentro del rango correspondiente. Haga clic en **nuevos parámetros de descubrimiento** para volver a la página Agregar/detectar.

4. Revise la lista de cabinas de almacenamiento detectadas.
5. Marque la casilla de comprobación junto a la cabina de almacenamiento que desea añadir al dominio de gestión y haga clic en **Siguiente**.

   Unified Manager comprueba las credenciales de cada cabina que se añade al dominio de gestión. Es posible que deba resolver los certificados autofirmados y los certificados no confiables que estén asociados con esa cabina.

6. Haga clic en **Siguiente** para continuar con el siguiente paso del asistente.

Paso 2: Resuelva los certificados autofirmados durante la detección

Como parte del proceso de detección, el sistema comprueba que las cabinas de almacenamiento estén usando certificados de un origen de confianza.

Pasos

1. Debe realizar una de las siguientes acciones:

- Si confía en las conexiones con las cabinas de almacenamiento detectadas, continúe a la siguiente tarjeta del asistente. Los certificados autofirmados se marcarán como certificados de confianza y las cabinas de almacenamiento se añadirán a Unified Manager.
- Si no confía en dichas conexiones, seleccione **Cancelar** y valide la estrategia de certificado de seguridad de cada cabina de almacenamiento antes de añadir cualquiera de ellas a Unified Manager.

2. Haga clic en **Siguiente** para continuar con el siguiente paso del asistente.

Paso 3: Resolver certificados que no son de confianza durante la detección

Los certificados dejan de ser de confianza cuando una cabina de almacenamiento intenta establecer una conexión con Unified Manager, pero no se confirma que la conexión sea segura. Durante el proceso de detección de cabinas, puede resolver certificados que no son de confianza al importar un certificado de una entidad de certificación (CA) (o certificado firmado por CA) que emitió un tercero de confianza.

Es posible que necesite instalar otros certificados de CA de confianza si se da alguna de las siguientes condiciones:

- Añadió recientemente una cabina de almacenamiento.
- Uno o ambos certificados caducaron.
- Uno o ambos certificados fueron revocados.
- Falta un certificado raíz o intermedio en uno o ambos certificados.

Pasos

1. Marque la casilla de comprobación junto a una cabina de almacenamiento para la cual desee resolver certificados que no son de confianza; a continuación, seleccione el botón **Importar**.

   Se abre un cuadro de diálogo para importar los archivos de certificado de confianza.

2. Haga clic en **examinar** para seleccionar los archivos de certificado para las matrices de almacenamiento.

   Se muestran los nombres de los archivos en el cuadro de diálogo.

3. Haga clic en **Importar**.

   Los archivos se cargan y validan.

   Si una cabina de almacenamiento tiene problemas de certificados que no son de confianza y aún no se han resuelto, no se podrá añadir a Unified Manager.

4. Haga clic en **Siguiente** para continuar con el siguiente paso del asistente.

Paso 4: Proporcionar contraseñas

Debe introducir las contraseñas de las cabinas de almacenamiento que desea añadir al dominio de gestión.

Pasos

1. Introduzca la contraseña para cada cabina de almacenamiento que desea añadir a Unified Manager.
2. **Opcional:** asocie las matrices de almacenamiento a un grupo: En la lista desplegable, seleccione el grupo que desee asociar a las matrices de almacenamiento seleccionadas.
3. Haga clic en **Finalizar**.

Después de terminar

Las cabinas de almacenamiento se añaden al dominio de gestión y se asocian con el grupo seleccionado (si se especificó alguno).

Unified Manager puede tardar varios minutos en conectarse a las cabinas de almacenamiento especificadas.

Detectar una sola cabina

Utilice la opción Añadir/detectar una cabina de almacenamiento única para detectar y añadir manualmente una sola cabina de almacenamiento a la red de la organización.

Antes de empezar

- La cabina de almacenamiento debe estar instalada y configurada correctamente.
- Las contraseñas de las cabinas de almacenamiento deben configurarse mediante el icono Access Management de System Manager.

Pasos

1. En la página gestionar, seleccione **Agregar/detectar**.

   Se muestra el cuadro de diálogo Añadir/detectar.

2. Seleccione el botón de opción **detectar una única cabina de almacenamiento**.
3. Introduzca la dirección IP de una de las controladoras de la cabina de almacenamiento y haga clic en **Iniciar la detección**.

   Es posible que Unified Manager demore varios minutos en conectarse a la cabina de almacenamiento especificada.

   Se mostrará el mensaje cabina de almacenamiento no accesible cuando no se pueda establecer la conexión con la dirección IP de la controladora especificada.

4. Si se le solicita, resuelva los certificados autofirmados.

   Como parte del proceso de detección, el sistema verifica que las cabinas de almacenamiento detectadas utilicen certificados de un origen de confianza. Si no puede localizar un certificado digital para una cabina de almacenamiento, el sistema le solicita que añada una excepción de seguridad para resolver el certificado que no está firmado por una entidad de certificación (CA) reconocida.

5. Si se le solicita, resuelva los certificados que no son de confianza.

   Los certificados dejan de ser de confianza cuando una cabina de almacenamiento intenta establecer una conexión con Unified Manager, pero no se confirma que la conexión sea segura. Importe un certificado de entidad de certificación (CA) emitido por un tercero de confianza para resolver los certificados no confiables.

6. Haga clic en **Siguiente**.
7. **Opcional:** asocie la cabina de almacenamiento detectada a un grupo: En la lista desplegable, seleccione el grupo que desea asociar a la cabina de almacenamiento.

   El grupo "todo" está seleccionado de forma predeterminada.

8. Introduzca la contraseña de administrador para la cabina de almacenamiento que desea añadir al dominio de gestión y haga clic en **Aceptar**.

Después de terminar

La cabina de almacenamiento se añade a Unified Manager y, si se especificó, también se añade al grupo seleccionado.

Si se habilitó la recogida automática de datos de soporte, se recogen automáticamente datos de soporte para la cabina de almacenamiento que se añade.

Gestione las cabinas

Ver el estado de la cabina de almacenamiento

SANtricity Unified Manager muestra el estado de cada cabina de almacenamiento que se detectó.

Vaya a la página **Administrar - todo**. En esta página, es posible ver el estado de la conexión entre el proxy de servicios web y la cabina de almacenamiento.

Los indicadores de estado se describen en la siguiente tabla.

Estado	Lo que indica
Óptimo	La cabina de almacenamiento tiene el estado óptimo. No hay problemas de certificados y la contraseña es válida.
Contraseña no válida	Se proporcionó una contraseña no válida para la cabina de almacenamiento.
Certificado no confiable	Una o varias conexiones con la cabina de almacenamiento no son de confianza porque el certificado HTTPS está autofirmado o no se ha importado; o bien, se trata de un certificado firmado por una CA y los certificados de CA raíz e intermedios no se importaron.
Necesita atención	Hay un problema con la cabina de almacenamiento que requiere de su intervención para corregirlo.
Bloqueo	La cabina de almacenamiento está en estado bloqueado.
Desconocido	No se contactó a la cabina de almacenamiento. Esto puede ocurrir cuando el proxy de servicios web se está iniciando y aún no estableció contacto con la cabina de almacenamiento, o bien cuando la cabina se encuentra sin conexión y nunca se la contactó desde que se inició el proxy de servicios web.
Sin conexión	El proxy de servicios web se había contactado previamente con la cabina de almacenamiento, pero ahora perdió toda conexión con ella.

Gestione una cabina de almacenamiento individual

Si desea realizar operaciones de gestión, puede usar la opción Iniciar para abrir la

instancia de SANtricity System Manager basada en el explorador que corresponde a una o más cabinas de almacenamiento.

Pasos

1. En la página gestionar, seleccione una o más cabinas de almacenamiento que desee gestionar.
2. Haga clic en **Iniciar**.

   El sistema abre una nueva ventana y muestra la página de inicio de sesión de System Manager.

3. Introduzca su nombre de usuario y contraseña y, a continuación, haga clic en **Iniciar sesión**.

Cambiar contraseñas de las cabinas de almacenamiento

Puede actualizar las contraseñas que se utilizan para ver y acceder a las cabinas de almacenamiento en SANtricity Unified Manager.

Antes de empezar

- Debe iniciar sesión con un perfil de usuario que cuente con permisos de administración de almacenamiento.
- Debe conocer la contraseña actual de la cabina de almacenamiento que se estableció en System Manager.

Acerca de esta tarea

En esta tarea, debe introducir la contraseña actual de una cabina de almacenamiento para poder acceder a esta en Unified Manager. Esto puede ser necesario si se modificó la contraseña de la cabina en System Manager y ahora se debe modificar también Unified Manager.

Pasos

1. En la página gestionar, seleccione una o varias cabinas de almacenamiento.
2. Seleccione menú:tareas no comunes[proporcionar contraseñas de cabina de almacenamiento].
3. Introduzca la contraseña o las contraseñas de cada cabina de almacenamiento y haga clic en **Guardar**.

Quite las cabinas de almacenamiento de SANtricity Unified Manager

Es posible quitar una o varias cabinas de almacenamiento si ya no se van a gestionar desde Unified Manager de SANtricity.

Acerca de esta tarea

No es posible acceder a ninguna de las cabinas de almacenamiento que se quiten. Sin embargo, puede establecerse una conexión con cualquiera de las cabinas de almacenamiento eliminadas si se apunta un explorador directamente a su dirección IP o nombre de host.

Al quitar una cabina de almacenamiento, ni ella ni sus datos se ven afectados de forma alguna. Si una cabina de almacenamiento se quita por error, es posible volver a añadirla.

Pasos

1. Seleccione la página **Administrar**.
2. Seleccione una o varias cabinas de almacenamiento que desee quitar.
3. Seleccione menú:tareas no comunes[Quitar cabina de almacenamiento].

La cabina de almacenamiento se elimina de todas las vistas de SANtricity Unified Manager.

Importación de la configuración

Información general de importación de la configuración

La función Importar configuración permite realizar una operación en lote para importar la configuración de una cabina a varias. Esta función permite ahorrar tiempo cuando se necesitan configurar varias matrices en la red.

¿Qué configuración se puede importar?

Es posible importar métodos de alerta, configuraciones de AutoSupport, configuraciones de servicios de directorio, configuraciones de almacenamiento (como grupos de volúmenes y pools) y configuraciones del sistema (como equilibrio de carga automático).

Obtenga más información:

- "Cómo funciona la importación de configuración"
- "Requisitos para replicar configuraciones de almacenamiento"

¿Cómo se realiza una importación por lotes?

En una cabina de almacenamiento que se usará como origen, abra System Manager y configure los ajustes deseados. A continuación, desde Unified Manager, vaya a la página gestionar e importe la configuración a una o varias cabinas.

Obtenga más información:

- "Importar la configuración de alerta"
- "Importe la configuración de AutoSupport"
- "Importe la configuración de servicios de directorio"
- "Importe los ajustes de configuración de almacenamiento"
- "Importe la configuración del sistema"

Conceptos

Cómo funciona la importación de configuración

Es posible usar SANtricity Unified Manager para importar la configuración de una cabina de almacenamiento a varias cabinas de almacenamiento. La función Importar configuración es una operación en lote que permite ahorrar tiempo cuando se necesitan configurar varias cabinas en la red.

Configuración disponible para la importación

Las siguientes configuraciones pueden importarse en varias cabinas:

- **Alertas** — métodos de alerta para enviar eventos importantes a los administradores, mediante correo

electrónico, un servidor syslog o un servidor SNMP.

- **AutoSupport**: Función que supervisa el estado de una matriz de almacenamiento y envía mensajes automáticos al soporte técnico.
- **Servicios de directorio** — método de autenticación de usuario que se administra a través de un servidor LDAP (protocolo ligero de acceso a directorios) y un servicio de directorio, como Active Directory de Microsoft.
- **Configuración de almacenamiento** — configuraciones relacionadas con lo siguiente:
  - Volúmenes (solo volúmenes gruesos y que no pertenecen al repositorio)
  - Grupos de volúmenes y pools
  - Asignaciones de unidad de repuesto
- **Ajustes del sistema** — configuraciones relacionadas con lo siguiente:
  - Configuración de escaneo de medios para un volumen
  - Configuración de SSD
  - Equilibrio de carga automático (no incluye la generación de informes de conectividad de host)

Flujo de trabajo de configuración

Para importar la configuración, siga este flujo de trabajo:

1. En una cabina de almacenamiento que se usará como origen, configure los ajustes mediante System Manager.
2. En las cabinas de almacenamiento que se usarán como objetivo, realice una copia de seguridad de la configuración mediante System Manager.
3. Desde Unified Manager, vaya a la página **Administrar** e importe la configuración.
4. En la página **Operaciones**, revise los resultados de la operación Importar configuración.

Requisitos para replicar configuraciones de almacenamiento

Antes de importar una configuración de almacenamiento desde una cabina de almacenamiento a otra, revise los requisitos y las directrices.

Bandejas

- Las bandejas donde residen las controladoras deben ser idénticas en las cabinas de origen y objetivo.
- Los ID de bandeja deben ser idénticos en las cabinas de origen y objetivo.
- Las bandejas de expansión deben llenarse en las mismas ranuras con los mismos tipos de unidad (si la unidad se usó en la configuración, la ubicación de las unidades sin usar no importa).

Controladoras

- El tipo de controladora puede ser diferente para las cabinas de origen y objetivo (por ejemplo, se puede importar de E2800 a E5700), pero el tipo de compartimento RBOD debe ser idéntico.
- Las HIC, incluidas las capacidades DE GARANTÍA de DATOS del host, deben ser idénticas para las cabinas de origen y objetivo.
- No se admite la importación de una configuración doble a una simple; sí se admite la configuración simple a doble.

- La configuración de unidades FDE no está incluida en el proceso de importación.

Estado

- Las cabinas objetivo deben tener el estado óptimo.
- La cabina de origen no necesita tener el estado óptimo.

Reducida

- La capacidad de una unidad puede variar entre las cabinas de origen y las objetivo, siempre y cuando la capacidad de volumen en la cabina objetivo sea mayor que en la de origen. (Una cabina objetivo puede tener unidades más nuevas y con mayor capacidad que la operación de replicación quizás no configure por completo en volúmenes).
- Un volumen de pool de discos de 64 TB o mayor en la cabina de origen impide el proceso de importación en las cabinas objetivo.
- Los volúmenes finos no están incluidos en el proceso de importación.

Utilizar importaciones por lotes

Importar la configuración de alerta

Es posible importar la configuración de alerta de una cabina de almacenamiento en otras cabinas de almacenamiento. Esta operación en lote permite ahorrar tiempo cuando se necesitan configurar varias matrices en la red.

Antes de empezar

- Las alertas se configuran en la instancia de System Manager correspondiente a la cabina de almacenamiento que se quiere usar como origen (**Configuración › Alertas**).
- La configuración actual de las cabinas de almacenamiento objetivo cuenta con una copia de seguridad en System Manager (menú:Configuración[sistema > Guardar configuración de la cabina de almacenamiento]).

Acerca de esta tarea

Puede seleccionar las opciones de correo electrónico, SNMP o alertas de syslog para la operación de importación. La configuración importada incluye lo siguiente:

- **Alertas por correo electrónico** — una dirección de servidor de correo y las direcciones de correo electrónico de los destinatarios de las alertas.
- **Alertas Syslog** — una dirección de servidor syslog y un puerto UDP.
- **Alertas SNMP** — un nombre de comunidad y una dirección IP para el servidor SNMP.

Pasos

1. En la página gestionar, haga clic en **Importar configuración**.

   Se abre el asistente Importar configuración.

2. En el cuadro de diálogo Seleccionar configuración, seleccione **Alertas por correo electrónico**, **Alertas SNMP** o **Alertas Syslog** y, a continuación, haga clic en **Siguiente**.

   Se abre un cuadro de diálogo para seleccionar la cabina de almacenamiento.

3. En el cuadro de diálogo Seleccionar origen, seleccione la matriz con la configuración que desea importar y, a continuación, haga clic en **Siguiente**.
4. En el cuadro de diálogo Seleccionar objetivos, elija una o más cabinas para que reciban la nueva configuración.

> Las cabinas de almacenamiento con una versión de firmware inferior a 8.50 no están disponibles y no pueden seleccionarse. Asimismo, una cabina no aparecerá en este cuadro de diálogo si Unified Manager no puede comunicarse con esa cabina (por ejemplo, si está desconectada o si tiene problemas de red o con un certificado o una contraseña).

5. Haga clic en **Finalizar**.

   En la página Operaciones, se muestran los resultados de la operación de importación. Si se produce un error en la operación, puede hacer clic en la fila para ver más información.

Resultados

Las cabinas de almacenamiento objetivo ahora están configuradas para enviar alertas a los administradores mediante correo electrónico, SNMP o syslog.

Importe la configuración de AutoSupport

Es posible importar la configuración de AutoSupport desde una cabina de almacenamiento a otras cabinas de almacenamiento. Esta operación en lote permite ahorrar tiempo cuando se necesitan configurar varias matrices en la red.

Antes de empezar

- AutoSupport se configura en la instancia de System Manager correspondiente a la cabina de almacenamiento que se quiere usar como origen (MENU:Support[Support Center]).
- La configuración actual de las cabinas de almacenamiento objetivo cuenta con una copia de seguridad en System Manager (menú:Configuración[sistema > Guardar configuración de la cabina de almacenamiento]).

Acerca de esta tarea

La configuración importada incluye las funciones por separado (Basic AutoSupport, AutoSupport OnDemand y Remote Diagnostics), la ventana de mantenimiento, el método de entrega, y programa de envío.

Pasos

1. En la página gestionar, haga clic en **Importar configuración**.

   Se abre el asistente Importar configuración.

2. En el cuadro de diálogo Seleccionar configuración, seleccione **AutoSupport** y, a continuación, haga clic en **Siguiente**.

   Se abre un cuadro de diálogo para seleccionar la cabina de almacenamiento.

3. En el cuadro de diálogo Seleccionar origen, seleccione la matriz con la configuración que desea importar y, a continuación, haga clic en **Siguiente**.
4. En el cuadro de diálogo Seleccionar objetivos, elija una o más cabinas para que reciban la nueva configuración.

Las cabinas de almacenamiento con una versión de firmware inferior a 8.50 no están disponibles y no pueden seleccionarse. Asimismo, una cabina no aparecerá en este cuadro de diálogo si Unified Manager no puede comunicarse con esa cabina (por ejemplo, si está desconectada o si tiene problemas de red o con un certificado o una contraseña).

5. Haga clic en **Finalizar**.

   En la página Operaciones, se muestran los resultados de la operación de importación. Si se produce un error en la operación, puede hacer clic en la fila para ver más información.

Resultados

Las cabinas de almacenamiento objetivo ahora están configuradas con los mismos ajustes de AutoSupport que la cabina de origen.

Importe la configuración de servicios de directorio

Es posible importar la configuración de los servicios de directorio desde una cabina de almacenamiento a otras cabinas de almacenamiento. Esta operación en lote permite ahorrar tiempo cuando se necesitan configurar varias matrices en la red.

Antes de empezar

- Los servicios de directorio están configurados en la instancia de System Manager correspondiente a la cabina de almacenamiento que se quiere usar como origen (MENU:Settings[Access Management]).
- La configuración actual de las cabinas de almacenamiento objetivo cuenta con una copia de seguridad en System Manager (menú:Configuración[sistema > Guardar configuración de la cabina de almacenamiento]).

Acerca de esta tarea

La configuración importada 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 con los roles predefinidos de la cabina de almacenamiento.

Pasos

1. En la página gestionar, haga clic en **Importar configuración**.

   Se abre el asistente Importar configuración.

2. En el cuadro de diálogo Seleccionar configuración, seleccione **Servicios de directorio** y, a continuación, haga clic en **Siguiente**.

   Se abre un cuadro de diálogo para seleccionar la cabina de almacenamiento.

3. En el cuadro de diálogo Seleccionar origen, seleccione la matriz con la configuración que desea importar y, a continuación, haga clic en **Siguiente**.
4. En el cuadro de diálogo Seleccionar objetivos, elija una o más cabinas para que reciban la nueva configuración.

Las cabinas de almacenamiento con una versión de firmware inferior a 8.50 no están disponibles y no pueden seleccionarse. Asimismo, una cabina no aparecerá en este cuadro de diálogo si Unified Manager no puede comunicarse con esa cabina (por ejemplo, si está desconectada o si tiene problemas de red o con un certificado o una contraseña).

5. Haga clic en **Finalizar**.

   En la página Operaciones, se muestran los resultados de la operación de importación. Si se produce un error en la operación, puede hacer clic en la fila para ver más información.

Resultados

Las cabinas de almacenamiento objetivo ahora están configuradas con los mismos servicios de directorio que la cabina de origen.

Importe la configuración del sistema

Es posible importar la configuración del sistema desde una cabina de almacenamiento a otras cabinas de almacenamiento. Esta operación en lote permite ahorrar tiempo cuando se necesitan configurar varias matrices en la red.

Antes de empezar

- La configuración del sistema se define en la instancia de System Manager correspondiente a la cabina de almacenamiento que se quiere usar como origen.
- La configuración actual de las cabinas de almacenamiento objetivo cuenta con una copia de seguridad en System Manager (menú:Configuración[sistema > Guardar configuración de la cabina de almacenamiento]).

Acerca de esta tarea

La configuración importada incluye los ajustes de escaneo de medios de un volumen, los ajustes de SSD de las controladoras y el equilibrio de carga automático (no incluye la generación de informes de conectividad de host).

Pasos

1. En la página gestionar, haga clic en **Importar configuración**.

   Se abre el asistente Importar configuración.

2. En el cuadro de diálogo Seleccionar configuración, seleccione **sistema** y, a continuación, haga clic en **Siguiente**.

   Se abre un cuadro de diálogo para seleccionar la cabina de almacenamiento.

3. En el cuadro de diálogo Seleccionar origen, seleccione la matriz con la configuración que desea importar y, a continuación, haga clic en **Siguiente**.
4. En el cuadro de diálogo Seleccionar objetivos, elija una o más cabinas para que reciban la nueva configuración.

   > Las cabinas de almacenamiento con una versión de firmware inferior a 8.50 no están disponibles y no pueden seleccionarse. Asimismo, una cabina no aparecerá en este cuadro de diálogo si Unified Manager no puede comunicarse con esa cabina (por ejemplo, si está desconectada o si tiene problemas de red o con un certificado o una contraseña).

5. Haga clic en **Finalizar**.

   En la página Operaciones, se muestran los resultados de la operación de importación. Si se produce un error en la operación, puede hacer clic en la fila para ver más información.

Resultados

Las cabinas de almacenamiento objetivo ahora están configuradas con los mismos ajustes del sistema que la cabina de origen.

Importe los ajustes de configuración de almacenamiento

Es posible importar la configuración de almacenamiento de una cabina de almacenamiento en otras cabinas de almacenamiento. Esta operación en lote permite ahorrar tiempo cuando se necesitan configurar varias matrices en la red.

Antes de empezar

- El almacenamiento se configura en la instancia de SANtricity System Manager correspondiente a la cabina de almacenamiento que se quiere usar como origen.
- La configuración actual de las cabinas de almacenamiento objetivo cuenta con una copia de seguridad en System Manager (menú:Configuración[sistema > Guardar configuración de la cabina de almacenamiento]).
- Las cabinas de origen y objetivo deben cumplir con los siguientes requisitos:
  - Las bandejas donde residan las controladoras deben ser idénticas.
  - Los ID de bandeja deben ser idénticos.
  - Las bandejas de expansión deben llenarse en las mismas ranuras con los mismos tipos de unidad.
  - El tipo de compartimento RBOD debe ser idéntico.
  - Las HIC, incluidas las capacidades de garantía de datos del host, deben ser idénticas.
  - Las cabinas objetivo deben tener el estado óptimo.
  - La capacidad de volumen de la cabina objetivo es mayor que la capacidad de la cabina de origen.
- Debe considerar las siguientes restricciones:
  - No se admite la importación de una configuración doble a una simple; sí se admite la configuración simple a doble.
  - Un volumen de pool de discos de 64 TB o mayor en la cabina de origen impide el proceso de importación en las cabinas objetivo.
  - Los volúmenes finos no están incluidos en el proceso de importación.

Acerca de esta tarea

La configuración importada incluye volúmenes configurados (solo volúmenes gruesos y que no pertenecen al repositorio), grupos de volúmenes, pools y asignaciones de unidades de repuesto.

Pasos

1. En la página gestionar, haga clic en **Importar configuración**.

   Se abre el asistente Importar configuración.

2. En el cuadro de diálogo Seleccionar configuración, seleccione **Configuración de almacenamiento** y, a continuación, haga clic en **Siguiente**.

   Se abre un cuadro de diálogo para seleccionar la cabina de almacenamiento.

3. En el cuadro de diálogo Seleccionar origen, seleccione la matriz con la configuración que desea importar y, a continuación, haga clic en **Siguiente**.

4. En el cuadro de diálogo Seleccionar objetivos, elija una o más cabinas para que reciban la nueva configuración.

> Las cabinas de almacenamiento con una versión de firmware inferior a 8.50 no están disponibles y no pueden seleccionarse. Asimismo, una cabina no aparecerá en este cuadro de diálogo si Unified Manager no puede comunicarse con esa cabina (por ejemplo, si está desconectada o si tiene problemas de red o con un certificado o una contraseña).

5. Haga clic en **Finalizar**.

   En la página Operaciones, se muestran los resultados de la operación de importación. Si se produce un error en la operación, puede hacer clic en la fila para ver más información.

Resultados

Las cabinas de almacenamiento objetivo ahora están configuradas con los mismos ajustes de almacenamiento que la cabina de origen.

Preguntas frecuentes

¿Qué configuración se importará?

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 SANtricity 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).

Grupos de cabinas

Información general sobre grupos

En la página gestionar grupos, puede crear un conjunto de grupos de cabinas de almacenamiento para simplificar la gestión.

¿Qué son los grupos de cabinas?

Es posible gestionar la infraestructura física y virtualizada si se agrupa un conjunto de cabinas de almacenamiento. Las cabinas de almacenamiento pueden agruparse de modo que sea más sencillo ejecutar las tareas de supervisión o generación de informes.

Existen dos tipos de grupos:

- **Todo el grupo** — el grupo todo es el grupo predeterminado e incluye todas las matrices de almacenamiento detectadas en su organización. Es posible acceder al grupo desde la vista principal.
- **Grupo creado por el usuario** — Un grupo creado por el usuario incluye las matrices de almacenamiento que selecciona manualmente para agregar a ese grupo. Es posible acceder a este tipo de grupo desde la vista principal.

¿Cómo se configuran los grupos?

En la página gestionar grupos, puede crear un grupo y, a continuación, añadir cabinas a dicho grupo.

Obtenga más información:

- "Configure el grupo de cabinas de almacenamiento"

Configure el grupo de cabinas de almacenamiento

Cree grupos de almacenamiento y, a continuación, añada cabinas de almacenamiento a los grupos.

La configuración de grupos es un procedimiento de dos pasos.

Paso 1: Crear grupo

En primer lugar, cree un grupo. El grupo de almacenamiento define las unidades que proporcionan el almacenamiento con el que se compone el volumen.

Pasos

1. En la página gestionar, seleccione **gestionar grupos › Crear grupo de cabinas de almacenamiento**.
2. En el campo **Nombre**, escriba un nombre para el nuevo grupo.
3. Seleccione las cabinas de almacenamiento que desea añadir al nuevo grupo.
4. Haga clic en **Crear**.

Paso 2: Añadir una cabina de almacenamiento a un grupo

Es posible añadir una o varias cabinas de almacenamiento a un grupo creado por un usuario.

Pasos

1. En la vista principal, seleccione **gestionar** y, a continuación, seleccione el grupo al que desea agregar matrices de almacenamiento.
2. Seleccione menú:gestionar grupos[Añadir cabinas de almacenamiento a grupo].
3. Seleccione las cabinas de almacenamiento que desea añadir al grupo.
4. Haga clic en **Agregar.**

Quite las cabinas de almacenamiento del grupo

Es posible quitar una o varias cabinas de almacenamiento gestionadas de un grupo si ya no se van a gestionar desde un grupo de almacenamiento específico.

Acerca de esta tarea

Al quitar cabinas de almacenamiento de un grupo, ni ellas ni sus datos se ven afectados de forma alguna. Si System Manager gestiona su cabina de almacenamiento, es posible gestionarla desde un explorador. Si una cabina de almacenamiento se quita por error de un grupo, es posible volver a añadirla.

Pasos

1. En la página gestionar, seleccione menú:gestionar grupos[Quitar cabinas de almacenamiento del grupo].
2. En el menú desplegable, seleccione el grupo que contiene las cabinas de almacenamiento que desea quitar y luego haga clic en la casilla de comprobación junto a cada cabina de almacenamiento que desea quitar del grupo.
3. Haga clic en **Quitar**.

Elimine grupo de cabinas de almacenamiento

Puede eliminar uno o varios grupos de cabinas de almacenamiento que ya no sean necesarios.

Acerca de esta tarea

Esta operación solo elimina el grupo de cabinas de almacenamiento. Todavía es posible acceder a las cabinas de almacenamiento asociadas con el grupo eliminado a través de la vista gestionar todo o de otro grupo con el que todavía se encuentren asociadas.

Pasos

1. En la página gestionar, seleccione **gestionar grupos › Eliminar grupo de cabinas de almacenamiento**.
2. Seleccione el o los grupos de cabinas de almacenamiento que desee eliminar.
3. Haga clic en **Eliminar**.

Cambiar el nombre de un grupo de cabinas de almacenamiento

Es posible cambiar el nombre de un grupo de cabinas de almacenamiento si el nombre actual ya no es significativo o no corresponde.

Acerca de esta tarea

Tenga en cuenta estas directrices.

- Un nombre puede consistir de letras, números y los caracteres especiales de subrayado (_), guión (-) y almohadilla (#). Si elige otros caracteres, aparece un mensaje de error. Se le solicitará que elija otro nombre.
- El nombre puede tener 30 caracteres como máximo. Los espacios iniciales o finales del nombre se eliminan.
- Use un nombre único, significativo, que sea fácil de entender y de recordar.
- Evite nombres arbitrarios o nombres que rápidamente pueden perder sentido en el futuro.

Pasos

1. En la ventana principal, seleccione **gestionar** y seleccione el grupo de cabinas de almacenamiento al que desea cambiarle el nombre.
2. Seleccione **gestionar grupos › Cambiar nombre de grupo de cabinas de almacenamiento**.
3. En el campo **Nombre del grupo**, escriba un nuevo nombre para el grupo.
4. Haga clic en **Cambiar nombre.**

Actualizaciones

Información general del centro de actualización

En el Centro de actualización, puede gestionar las actualizaciones de NVSRAM y de software de sistema operativo SANtricity para varias cabinas de almacenamiento.

¿Cómo funcionan las actualizaciones?

Descargue el software de sistema operativo más reciente y después actualice una o varias cabinas.

Actualizar el flujo de trabajo

Los siguientes pasos constituyen un flujo de trabajo de alto nivel para ejecutar actualizaciones de software.

1. Descargue el archivo de software del sistema operativo SANtricity más reciente en el sitio de soporte (hay un enlace disponible en Unified Manager, en la página Soporte). Guarde el archivo en el sistema host de gestión (el host desde donde se accede a Unified Manager en un explorador) y descomprima el archivo.
2. En Unified Manager, puede cargar el archivo de software del sistema operativo SANtricity y el archivo NVSRAM en el repositorio (un área del servidor proxy de servicios web donde se almacenan los archivos). Puede añadir archivos desde MENU:Centro de actualización[Actualizar software de sistema operativo SANtricity o desde Centro de actualización > gestionar el repositorio de software].
3. Una vez que se hayan cargado los archivos en el repositorio, seleccione el archivo que usará en la actualización. En la página Actualizar software de sistema operativo SANtricity (menú:Centro de actualización[Actualizar software de sistema operativo SANtricity]), puede seleccionar el archivo de software de sistema operativo SANtricity y el archivo de NVSRAM. Después de seleccionar un archivo de

software, se muestra en la página una lista con las cabinas de almacenamiento compatibles. A continuación, seleccione las cabinas de almacenamiento que desea actualizar con el nuevo software. (No puede seleccionar cabinas incompatibles).

4. Luego, puede iniciar una transferencia y activación inmediatas del software, o puede optar por preconfigurar los archivos para su activación más adelante. Durante el proceso de actualización, Unified Manager realiza las siguientes tareas:
   a. Realiza una comprobación del estado de las cabinas de almacenamiento para determinar si existe alguna condición que pudiera impedir que se complete la actualización. Si ocurre un error en la comprobación del estado de alguna cabina, puede omitir esa cabina en particular y continuar la actualización de las otras cabinas. Otra opción es detener el proceso por completo y solucionar los problemas de las cabinas que presentaron errores.
   b. Transfiere los archivos de actualización a cada controladora.
   c. Reinicia las controladoras y activa el nuevo software del sistema operativo SANtricity de a una controladora por vez. Durante la activación, el archivo del sistema operativo SANtricity existente se reemplaza por el nuevo archivo.

      También es posible especificar que el software se active en otro momento.

Actualización inmediata o almacenamiento temporal

Puede activar la actualización de inmediato o almacenarla temporalmente para otro momento. Puede optar por activarlos más tarde por los siguientes motivos:

- **Hora del día** — la activación del software puede llevar mucho tiempo, por lo que es posible que desee esperar hasta que las cargas de E/S sean más livianas. Según la carga de I/o y el tamaño de caché, la actualización de una controladora generalmente puede demorar entre 15 y 25 minutos en completarse. Las controladoras se reinician y conmutan al nodo de respaldo durante la activación, de manera que el rendimiento podría ser inferior al habitual hasta que finalice la actualización.
- **Tipo de paquete**: Es posible que desee probar el nuevo software y firmware en una matriz de almacenamiento antes de actualizar los archivos en otras matrices de almacenamiento.

Para activar el software almacenado temporalmente, vaya al menú:Soporte[Centro de actualización] y haga clic en **Activar** en el área etiquetada como actualización de software del controlador de sistema operativo SANtricity.

Comprobación del estado

Una comprobación del estado se ejecuta como parte del proceso de actualización, pero es posible ejecutarla por separado, antes de comenzar (vaya a menú:Centro de actualización[Comprobación del estado previa a la actualización]).

La comprobación del estado evalúa todos los componentes de la cabina de almacenamiento para garantizar que se pueda proceder con la actualización. Las siguientes condiciones podrían evitar la actualización:

- Unidades asignadas con errores
- Piezas de repuesto en uso
- Grupos de volúmenes incompletos
- Operaciones exclusivas en ejecución
- Volúmenes faltantes

- Estado no óptimo de la controladora
- Cantidad excesiva de eventos en el registro de eventos
- Fallo de validación de la base de datos de configuración
- Unidades con versiones de DACstore anteriores

¿Qué debo saber antes de actualizar?

Antes de actualizar varias cabinas de almacenamiento, revise las consideraciones fundamentales como parte de la planificación.

Versiones actuales

Puede ver las versiones actuales del software de sistema operativo SANtricity desde la página gestionar de Unified Manager en cada cabina de almacenamiento detectada. La versión se muestra en la columna Software de sistema operativo SANtricity. Si hace clic en la versión de sistema operativo SANtricity en cada fila, puede encontrar información de NVSRAM y del firmware de la controladora en un cuadro de diálogo emergente.

Otros componentes que requieren actualización

Como parte del proceso de actualización, es posible que también necesite actualizar el controlador de conmutación al nodo de respaldo/multivía del host o el controlador de HBA de modo que el host pueda interactuar con las controladoras correctamente.

Para obtener información sobre compatibilidad, consulte "Matriz de interoperabilidad de NetApp". Asimismo, consulte los procedimientos en las guías exprés del sistema operativo. Las guías exprés están disponibles en "Documentación de E-Series y SANtricity".

Controladoras dobles

Si una cabina de almacenamiento contiene dos controladoras y existe un controlador multivía instalado, la cabina de almacenamiento puede seguir procesando las operaciones de I/o mientras se realiza la actualización. Durante la actualización, ocurre el siguiente proceso:

1. La controladora A conmuta todos sus LUN a la controladora B.
2. La actualización se produce en la controladora A.
3. La controladora A recupera sus LUN y todos los LUN de la controladora B.
4. La actualización se produce en la controladora B.

Una vez que finaliza la actualización, es posible que sea necesario redistribuir los volúmenes manualmente entre las controladoras para garantizar que los volúmenes regresen a la controladora correspondiente.

Actualice software y firmware

Realice la comprobación del estado previa a la actualización

Una comprobación del estado se ejecuta como parte del proceso de actualización, pero también es posible ejecutarla por separado, antes de comenzar. La comprobación del estado evalúa los componentes de la cabina de almacenamiento para garantizar que se pueda proceder con la actualización.

Pasos

1. En la vista principal, seleccione **gestionar** y, a continuación, elija Menú:Centro de actualización[Comprobación del estado previa a la actualización].

   Se abre el cuadro de diálogo Comprobación del estado previa a la actualización, donde se enumeran todos los sistemas de almacenamiento detectados.

2. Si es necesario, puede filtrar u ordenar los sistemas de almacenamiento de la lista, de modo que pueda ver todos los sistemas que están actualmente en estado óptimo.
3. Marque las casillas de comprobación de los sistemas de almacenamiento que quiere incluir en la comprobación del estado.
4. Haga clic en **Inicio**.

   Mientras se lleva a cabo la comprobación del estado, se muestra el progreso en el cuadro de diálogo.

5. Una vez finalizada la comprobación del estado, puede hacer clic en los tres puntos (…) a la derecha de cada fila para ver más información y realizar otras tareas.

> Si ocurre un error en la comprobación del estado de alguna cabina, puede omitir esa cabina en particular y continuar la actualización de las otras cabinas. Otra opción es detener el proceso por completo y solucionar los problemas de las cabinas que presentaron errores.

Actualice el sistema operativo SANtricity

Puede actualizar una o varias cabinas de almacenamiento con el software más reciente y NVSRAM para asegurarse de contar con las funciones y correcciones de errores más recientes. NVSRAM de controladora es un archivo de la controladora que especifica las configuraciones predeterminadas para las controladoras.

Antes de empezar

- Los archivos del sistema operativo SANtricity más reciente están disponibles en el sistema host donde se ejecutan Unified Manager y el proxy de servicios web SANtricity.
- Sabe si desea activar la actualización del software ahora o más adelante.

  Puede optar por activarlos más tarde por los siguientes motivos:

  - **Hora del día** — la activación del software puede llevar mucho tiempo, por lo que es posible que desee esperar hasta que las cargas de E/S sean más livianas. Las controladoras conmutan al nodo de respaldo durante la activación, de manera que el rendimiento podría ser inferior al habitual hasta que finalice la actualización.
  - **Tipo de paquete**: Es posible que desee probar el nuevo software de sistema operativo en una matriz de almacenamiento antes de actualizar los archivos en otras matrices de almacenamiento.

> Los sistemas deben ejecutar SANtricity OS 11.70.5 para actualizar a la versión 11,80.x o posterior.

Acerca de esta tarea

Riesgo de pérdida de datos o riesgo de daños a la cabina de almacenamiento: No introduzca cambios en la cabina de almacenamiento mientras se realiza la actualización. Mantenga encendida la cabina de almacenamiento.

Pasos

1. Si la cabina de almacenamiento contiene una sola controladora o un controlador multivía no está en uso, detenga la actividad de I/o de la cabina de almacenamiento para evitar errores en la aplicación. Si la cabina de almacenamiento tiene dos controladoras y existe un controlador multivía instalado, no necesita detener la actividad de I/O.
2. En la vista principal, seleccione **gestionar** y, a continuación, seleccione una o varias cabinas de almacenamiento que desee actualizar.
3. Seleccione MENU:Centro de actualización[Actualizar software de sistema operativo SANtricity].

   Se muestra la página Actualizar software de sistema operativo SANtricity.

4. Descargue el paquete de software de sistema operativo de SANtricity del sitio de soporte de NetApp en el equipo local.

   a. Haga clic en **Agregar nuevo archivo al repositorio de software**.
   b. Haga clic en el enlace para buscar las últimas **Descargas de SANtricity OS**.
   c. Haga clic en el enlace **Descargar la versión más reciente**.
   d. Siga las restantes instrucciones para descargar el archivo de sistema operativo de SANtricity y el archivo de NVSRAM en el equipo local.

   Se requiere firmware con firma digital en la versión 8.42 y posteriores. Si intenta descargar firmware sin firmar, se muestra un error y se anula la descarga.

5. Seleccione el archivo de software de sistema operativo y el archivo de NVSRAM que desea usar para actualizar las controladoras:

   a. En el menú desplegable **Seleccione un archivo de software del sistema operativo SANtricity**, seleccione el archivo del sistema operativo que descargó en el equipo local.

      Si hay varios archivos disponibles, se ordenarán del más reciente al más antiguo.

   En el repositorio de software, figuran todos los archivos de software relacionados con el proxy de servicios web. Si no ve el archivo que desea utilizar, haga clic en el vínculo **Agregar nuevo archivo al repositorio de software**, para buscar la ubicación donde reside el archivo de sistema operativo que desea agregar.

   a. En el menú desplegable **Seleccione un archivo NVSRAM**, seleccione el archivo de la controladora que desea utilizar.

      Si hay varios archivos, se ordenarán del más reciente al más antiguo.

6. En la tabla cabina de almacenamiento compatible, revise las cabinas de almacenamiento que son compatibles con el archivo de software del sistema operativo seleccionado. A continuación, seleccione las cabinas que desea actualizar.
   - Las cabinas de almacenamiento seleccionadas en la vista gestionar que son compatibles con el archivo de firmware elegido están seleccionadas de forma predeterminada en la tabla cabina de almacenamiento compatible.

- Las matrices de almacenamiento que no se pueden actualizar con el archivo de firmware seleccionado no se pueden seleccionar en la tabla matriz de almacenamiento compatible, como indica el estado **incompatible**.

7. **Opcional:** para transferir el archivo de software a las matrices de almacenamiento sin activarlo, active la casilla de verificación **transferir el software del sistema operativo a las matrices de almacenamiento, marcarlo como preconfigurado y activarlo posteriormente**.
8. Haga clic en **Inicio**.
9. Según elija activar ahora o más adelante, realice una de las siguientes acciones:
   - Escriba **TRANSFER** para confirmar que desea transferir las versiones propuestas de software del sistema operativo en las matrices que seleccionó para actualizar y, a continuación, haga clic en **transferir**.

     Para activar el software transferido, seleccione MENU:Centro de actualización[Activar software de sistema operativo almacenado temporalmente].

   - Escriba **UPGRADE** para confirmar que desea transferir y activar las versiones propuestas de software del sistema operativo en las matrices que seleccionó para actualizar y, a continuación, haga clic en **Actualizar**.

     El sistema transfiere el archivo de software a cada cabina de almacenamiento que seleccionó para actualizar y, luego, activa el archivo mediante un reinicio.

     Durante la operación de actualización, ocurren las siguientes acciones:

   - Como parte del proceso de actualización, se ejecuta una comprobación del estado previa a la actualización. La comprobación del estado antes de la actualización evalúa todos los componentes de la cabina de almacenamiento para garantizar que se pueda proceder con la actualización.
   - Si ocurre un error en la comprobación del estado de una cabina de almacenamiento, la actualización se detiene. Puede hacer clic en los tres puntos (…). Y seleccione **Guardar registro** para revisar los errores. También puede optar por anular el error de comprobación del estado y hacer clic en **continuar** para continuar con la actualización.
   - Puede cancelar la operación de actualización después de la comprobación del estado previa a la actualización.
10. **Opcional:** una vez completada la actualización, puede ver una lista de lo que se actualizó en una cabina de almacenamiento específica haciendo clic en los tres puntos (…) Y, a continuación, seleccione **Guardar registro**.

    El archivo se guarda en la carpeta de descargas del explorador con el nombre `upgrade_log-<date>.json`.

Active el software de sistema operativo almacenado temporalmente

Puede optar por activar el archivo de actualización inmediatamente o esperar hasta un momento más conveniente. Este procedimiento entiende que se optó por activar el archivo de software más adelante.

Acerca de esta tarea

Puede transferir los archivos del firmware sin activarlos. Puede optar por activarlos más tarde por los siguientes motivos:

- **Hora del día** — la activación del software puede llevar mucho tiempo, por lo que es posible que desee esperar hasta que las cargas de E/S sean más livianas. Las controladoras se reinician y conmutan al nodo de respaldo durante la activación, de manera que el rendimiento podría ser inferior al habitual hasta que finalice la actualización.
- **Tipo de paquete**: Es posible que desee probar el nuevo software y firmware en una matriz de almacenamiento antes de actualizar los archivos en otras matrices de almacenamiento.

No se puede detener el proceso de activación una vez iniciado.

Pasos

1. En la vista principal, seleccione **gestionar**. Si es necesario, haga clic en la columna Estado para ordenar, en la parte superior de la página, todas las cabinas de almacenamiento con el estado "actualización del sistema operativo (esperando la activación)".
2. Seleccione una o varias cabinas de almacenamiento para las cuales desee activar el software y, a continuación, seleccione MENU:Centro de actualización[Activar software de sistema operativo almacenado temporalmente].

   Durante la operación de actualización, ocurren las siguientes acciones:

   - Como parte del proceso de activación, se ejecuta una comprobación del estado previa a la actualización. La comprobación del estado antes de la actualización evalúa todos los componentes de la cabina de almacenamiento para garantizar que se pueda proceder con la activación.
   - Si ocurre un error en la comprobación del estado de una cabina de almacenamiento, la activación se detiene. Puede hacer clic en los tres puntos (…). Y seleccione **Guardar registro** para revisar los errores. También puede optar por anular el error en la comprobación del estado y hacer clic en **continuar** para continuar con la activación.
   - Puede cancelar la operación de activación después de la comprobación del estado previa a la actualización. Cuando la comprobación del estado previa a la actualización se realiza correctamente, se produce la activación. El tiempo que requiere la activación depende de la configuración de la cabina de almacenamiento y los componentes que se van a activar.
3. **Opcional:** una vez completada la activación, puede ver una lista de lo que se activó para una matriz de almacenamiento específica haciendo clic en los tres puntos (…) Y, a continuación, seleccione **Guardar registro**.

   El archivo se guarda en la carpeta de descargas del explorador con el nombre `activate_log-<date>.json`.

Gestionar el repositorio de software

En el repositorio de software, figuran todos los archivos de software relacionados con el proxy de servicios web.

Si no puede ver el archivo que desea utilizar, puede utilizar la opción gestionar repositorio de software para importar uno o más archivos de sistema operativo SANtricity al sistema host donde se ejecutan el proxy de servicios web y Unified Manager. También puede optar por eliminar uno o varios de los archivos de sistema operativo SANtricity que están disponibles en el repositorio de software.

Antes de empezar

Si añade archivos de sistema operativo SANtricity, asegúrese de que estén disponibles en el sistema local.

Pasos

1. En la vista principal, seleccione **gestionar** y, a continuación, elija MENU:Centro de actualización[gestionar el repositorio de software].

   Se muestra el cuadro de diálogo gestionar el repositorio de software.

2. Realice una de las siguientes acciones:

Opción	Haga esto
Importar	a. Haga clic en **Importar.** b. Haga clic en **examinar** y, a continuación, desplácese hasta la ubicación en la que residen los archivos del sistema operativo que desea agregar. Los archivos de sistema operativo tienen un nombre similar a `N2800-830000-000.dlp`. c. Seleccione uno o más archivos de sistema operativo que desee agregar y, a continuación, haga clic en **Importar**.
Eliminar	a. Seleccione uno o varios archivos de sistema operativo que desee quitar del repositorio de software. b. Haga clic en **Eliminar**.

Resultados

Si seleccionó Importar, los archivos se cargan y se validan. Si seleccionó Eliminar, los archivos se quitan del repositorio de software.

Borre el software de sistema operativo almacenado temporalmente

Puede quitar el software de sistema operativo almacenado temporalmente para garantizar que no se active una versión pendiente de manera accidental más adelante. La eliminación del software de sistema operativo almacenado temporalmente no afecta la versión actual que está en ejecución en las cabinas de almacenamiento.

Pasos

1. En la vista principal, seleccione **gestionar** y, a continuación, elija menú:Centro de actualización[Borrar software de sistema operativo almacenado temporalmente].

   Se abre el cuadro de diálogo Borrar software de sistema operativo almacenado temporalmente, donde se enumeran todos los sistemas de almacenamiento detectados con software o NVSRAM pendiente.

2. Si es necesario, puede filtrar u ordenar los sistemas de almacenamiento de la lista, de modo que pueda ver todos los sistemas que tienen software almacenado temporalmente.
3. Marque las casillas de comprobación de los sistemas de almacenamiento con software pendiente que desea borrar.
4. Haga clic en **Borrar**.

   El estado de la operación se muestra en el cuadro de diálogo.

Mirroring

Información general de mirroring

Utilice las funciones de mirroring para replicar datos entre una cabina de almacenamiento local y una cabina de almacenamiento remota, ya sea de forma asíncrona o síncrona.

El mirroring síncrono no está disponible en los sistemas de almacenamiento EF600 o EF300.

¿Qué es el mirroring?

Las aplicaciones de SANtricity incluyen dos tipos de mirroring: Asíncrono y síncrono. El mirroring asíncrono copia los volúmenes de datos bajo demanda o por programación, lo que minimiza o evita el tiempo de inactividad que se puede producir por pérdidas o daños en los datos. El mirroring síncrono replica los volúmenes de datos en tiempo real para garantizar la disponibilidad continua.

Obtenga más información:

- "Cómo funciona el mirroring"
- "Terminología de mirroring"

¿Cómo se configura el mirroring?

El mirroring síncrono o asíncrono se debe configurar en Unified Manager y, posteriormente, se debe utilizar System Manager para gestionar las sincronizaciones.

Obtenga más información:

- "Flujo de trabajo de configuración de mirroring"
- "Requisitos para usar el mirroring"
- "Cree una pareja reflejada asíncrona"
- "Cree una pareja reflejada síncrona"

Conceptos

Cómo funciona el mirroring

SANtricity Unified Manager incluye opciones de configuración para las funciones de mirroring de SANtricity, con las cuales los administradores pueden replicar datos entre dos cabinas de almacenamiento para la protección de los datos.

El mirroring síncrono no está disponible en los sistemas de almacenamiento EF600 o EF300.

Tipos de mirroring

Las aplicaciones de SANtricity incluyen dos tipos de mirroring: Asíncrono y síncrono.

El mirroring asíncrono copia los volúmenes de datos bajo demanda o por programación, lo que minimiza o

evita el tiempo de inactividad que se puede producir por pérdidas o daños en los datos. El mirroring asíncrono captura el estado de un volumen primario en un momento específico y copia solo los datos que han cambiado desde la última captura de imagen. El sitio primario se puede actualizar de inmediato y el sitio secundario se puede actualizar según lo permita el ancho de banda. La información se guarda en la caché y se envía más tarde, a medida que los recursos de red se vuelven disponibles. Este tipo de mirroring es ideal para los procesos periódicos como el backup y el archivado.

El mirroring síncrono replica los volúmenes de datos en tiempo real para garantizar la disponibilidad continua. El propósito es lograr un objetivo de punto de recuperación (RPO) de cero datos perdidos mediante la copia de datos importantes disponibles en caso de que se produzca un desastre en una de las dos cabinas de almacenamiento. La copia es idéntica a los datos de producción en cada momento, ya que cada vez que se realiza una escritura en el volumen primario, se realiza una escritura en el volumen secundario. El host no recibe la confirmación de que la escritura se realizó correctamente hasta que el volumen secundario se actualiza con los cambios realizados en el volumen primario. Este tipo de mirroring es ideal para fines de continuidad del negocio como la recuperación ante desastres.

Diferencias entre los tipos de mirroring

En la siguiente tabla, se describen las principales diferencias entre los dos tipos de mirroring.

Atributo	Asíncrona	Síncrona
Método de replicación	Momento específico: El mirroring se ejecuta bajo demanda o automáticamente de acuerdo con una programación definida por el usuario.	Continuo: El mirroring se ejecuta automáticamente de forma continua; se copian datos en cada escritura del host.
Distancia	Admite largas distancias entre las cabinas. Generalmente, solo las funcionalidades de la red y la tecnología de extensión de canal limitan la distancia.	Limitado a distancias menores entre las cabinas. Generalmente, la distancia debe ser inferior o igual a 10 km (6.2 millas) con respecto a la cabina de almacenamiento local para satisfacer los requisitos de latencia y rendimiento de la aplicación.
Método de comunicación	Una red Fibre Channel o IP estándar.	Solo red Fibre Channel.
Tipos de volúmenes	Estándares o finos.	Solo estándares.

Flujo de trabajo de configuración de mirroring

El mirroring síncrono o asíncrono se debe configurar en SANtricity Unified Manager y, posteriormente, se debe utilizar SANtricity System Manager para gestionar las sincronizaciones.

Flujo de trabajo de mirroring asíncrono

El mirroring asíncrono conlleva el siguiente flujo de trabajo:

1. Realice la configuración inicial en Unified Manager:
   a. Seleccione la cabina de almacenamiento local como el origen de la transferencia de datos.
   b. Cree un grupo de coherencia de reflejos o seleccione uno existente que funcione como contenedor para el volumen primario de la cabina local y el volumen secundario de la cabina remota. Los volúmenes primario y secundario se conocen como la "pareja reflejada". Si es la primera vez que crea el grupo de coherencia de reflejos, debe especificar si desea ejecutar sincronizaciones manuales o programadas.
   c. Seleccione un volumen primario de la cabina de almacenamiento local y determine su capacidad reservada. La capacidad reservada es la capacidad física asignada que se utilizará para la operación de copia.
   d. Seleccione una cabina de almacenamiento remota como el destino de la transferencia y un volumen secundario y, a continuación, determine su capacidad reservada.
   e. Inicie la transferencia de datos inicial desde el volumen primario hacia el volumen secundario. Según el tamaño de los volúmenes, esta transferencia inicial puede tardar varias horas.
2. Compruebe el progreso de la sincronización inicial:
   a. En Unified Manager, inicie la instancia de System Manager para la cabina local.
   b. En System Manager, consulte el estado de la operación de mirroring. Cuando se complete el mirroring, el estado de la pareja reflejada será "óptimo".
3. De manera opcional, puede reprogramar o realizar manualmente transferencias de datos subsiguientes en System Manager. Solo se transferirán los bloques nuevos y cambiados del volumen primario al volumen secundario.

Como la replicación asíncrona es periódica, el sistema puede consolidar los bloques cambiados y ahorrar ancho de banda de red. El impacto sobre el rendimiento de escritura y la latencia de escritura es mínimo.

Flujo de trabajo de mirroring síncrono

El mirroring síncrono conlleva el siguiente flujo de trabajo:

1. Realice la configuración inicial en Unified Manager:
   a. Seleccione una cabina de almacenamiento local como el origen de la transferencia de datos.
   b. Seleccione un volumen primario de la cabina de almacenamiento local.
   c. Seleccione una cabina de almacenamiento remota como el destino de la transferencia de datos y, a continuación, seleccione un volumen secundario.
   d. Seleccione las prioridades de sincronización y resincronización.
   e. Inicie la transferencia de datos inicial desde el volumen primario hacia el volumen secundario. Según el tamaño de los volúmenes, esta transferencia inicial puede tardar varias horas.
2. Compruebe el progreso de la sincronización inicial:
   a. En Unified Manager, inicie la instancia de System Manager para la cabina local.
   b. En System Manager, consulte el estado de la operación de mirroring. Cuando se complete el mirroring, el estado de la pareja reflejada será "óptimo". Las dos cabinas intentarán mantener la sincronización a través de las operaciones normales. Solo se transferirán los bloques nuevos y cambiados del volumen primario al volumen secundario.
3. De manera opcional, puede cambiar la configuración de sincronización en System Manager.

Como la replicación síncrona es continua, el enlace de replicación entre los dos sitios debe proporcionar funcionalidades de ancho de banda suficientes.

Terminología de mirroring

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

Duración	Descripción
Cabina de almacenamiento local	La cabina de almacenamiento local es aquella sobre la que se actúa en el momento.
Grupo de coherencia de reflejos	Un grupo de coherencia de reflejos es un contenedor para una o más parejas reflejadas. Para las operaciones de mirroring asíncrono, se debe crear un grupo de coherencia de reflejos. Todas las parejas reflejadas de un grupo se resincronizan de forma simultánea para mantener un punto de recuperación consistente. El mirroring síncrono no utiliza grupo de coherencia de reflejos.
Pareja reflejada	Una pareja reflejada comprende dos volúmenes: Un volumen primario y uno secundario. En el mirroring asíncrono, una pareja reflejada siempre pertenece a un grupo de coherencia de reflejos. Primero, se realizan las operaciones de escritura en el volumen primario y, luego, se replican en el secundario. Cada pareja reflejada de un grupo de coherencia de reflejos comparte la misma configuración de sincronización.
Volumen primario	El volumen primario de una pareja reflejada es el volumen de origen que se reflejará.
Cabina de almacenamiento remota	La cabina de almacenamiento remota se designa normalmente como el sitio secundario, que normalmente contiene una réplica de los datos en una configuración de mirroring.
Capacidad reservada	La capacidad reservada es la capacidad física asignada que se usa para cualquier operación de servicio de copia y objeto de almacenamiento. El host no puede leerla directamente. Se requieren estos volúmenes para que la controladora pueda guardar de forma persistente la información necesaria para mantener el mirroring en un estado operativo. Los volúmenes contienen información como registros delta y datos de copia en escritura.
Volumen secundario	El volumen secundario de una pareja reflejada está normalmente ubicado en un sitio secundario y contiene una réplica de los datos.

Duración	Descripción
Sincronización	La sincronización se produce en la sincronización inicial entre la cabina de almacenamiento local y la cabina de almacenamiento remota. La sincronización también se produce cuando los volúmenes primario y secundario dejan de estar sincronizados después de una interrupción de comunicación. Cuando el enlace de comunicación se restablece, todos los datos sin replicar se sincronizan con la cabina de almacenamiento del volumen secundario.

Requisitos para usar el mirroring

Si planea configurar el mirroring, tenga en cuenta los siguientes requisitos.

Unified Manager

- El proxy de servicios web se encuentra en ejecución.
- Unified Manager se ejecuta en el host local a través de una conexión HTTPS.
- SANtricity Unified Manager debe mostrar los certificados SSL válidos para la cabina de almacenamiento. Es posible aceptar un certificado autofirmado o instalar una certificación de seguridad propia con Unified Manager. Para hacerlo, debe navegar hasta MENU:Certificate[Gestión de certificados].

Cabinas de almacenamiento

El mirroring síncrono no está disponible en las cabinas de almacenamiento EF600 o EF300.

- Debe tener dos cabinas de almacenamiento.
- Cada cabina de almacenamiento debe tener dos controladoras.
- Las dos cabinas de almacenamiento se encuentran detectadas en Unified Manager.
- Cada controladora en la cabina primaria y la cabina secundaria debe tener un puerto Ethernet de gestión configurado y debe estar conectada a la red.
- Las cabinas de almacenamiento deben tener la versión de firmware 7.84 como mínimo. (Cada una puede ejecutar versiones de sistema operativo diferentes).
- Debe conocer la contraseña de las cabinas de almacenamiento remota y local.
- Debe tener suficiente capacidad libre en la cabina de almacenamiento remota para crear un volumen secundario mayor o igual que el volumen primario que desea reflejar.
- El mirroring asíncrono se admite en controladoras con puertos de host Fibre Channel (FC) o iSCSI, mientras que el mirroring síncrono solo se admite en controladoras con puertos de host FC.

Requisitos de conectividad

El mirroring (asíncrono o síncrono) a través de una interfaz de FC requiere lo siguiente:

- Cada controladora de la cabina de almacenamiento dedica su puerto de host FC numerado más alto a las operaciones de mirroring.
- Si la controladora tiene tanto puertos base FC como puertos FC de tarjeta de interfaz del host (HIC), en la HIC se encuentra el puerto numerado más alto. Se cerrará la sesión de cualquier host que haya iniciado sesión en el puerto dedicado y no se aceptará ninguna solicitud de inicio de sesión de host. Solo se aceptan las solicitudes I/o en este puerto de las controladoras que participan en las operaciones de

mirroring.

- Los puertos de mirroring dedicados deben pertenecer al entorno estructural de FC que sea compatible con el servicio de directorio y las interfaces del servicio de nombres. En particular, FC-AL y punto a punto no son opciones de conectividad compatibles entre las controladoras que participan en las relaciones de mirroring.

El mirroring (solo asíncrono) a través de una interfaz iSCSI requiere lo siguiente:

- A diferencia de FC, iSCSI no requiere un puerto dedicado. Cuando se utiliza el mirroring asíncrono en entornos iSCSI, no es necesario dedicar ninguno de los puertos iSCSI front-end de la cabina de almacenamiento para usarlos con mirroring asíncrono; esos puertos se comparten tanto para las conexiones de tráfico de reflejos asíncronos como de I/o de host a cabina.
- La controladora conserva una lista de los sistemas de almacenamiento remoto con los cuales el iniciador de iSCSI intenta establecer una sesión. El primer puerto que logra establecer una conexión iSCSI se utiliza para todas las comunicaciones subsiguientes con esa cabina de almacenamiento remota. Si no se produce la comunicación, se intenta una nueva sesión con todos los puertos disponibles.
- Los puertos iSCSI se configuran en el nivel de la cabina, puerto por puerto. La comunicación entre controladoras para la mensajería de configuración y la transferencia de datos utiliza la configuración global, lo que incluye:
  - VLAN: Tanto los sistemas locales como los remotos deben tener el mismo valor de VLAN para comunicarse
  - Puertos de escucha iSCSI
  - Tramas gigantes
  - Prioridad para Ethernet

> La comunicación entre las controladoras iSCSI debe utilizar un puerto con conexión a un host y no el puerto Ethernet de gestión.

Candidatos de volumen reflejado

- El nivel de RAID, los parámetros de almacenamiento en caché y el tamaño de los segmentos pueden ser diferentes en los volúmenes primario y secundario de una pareja reflejada.

> Para las controladoras EF600 y EF300, los volúmenes primario y secundario de una pareja reflejada asíncrona deben coincidir con el mismo protocolo, nivel de soporte, tamaño de segmento, tipo de seguridad y nivel de RAID. Las parejas reflejadas asíncronas no elegibles no aparecerán en la lista de volúmenes disponibles.

- El volumen secundario deber tener al menos el tamaño del volumen primario.
- Un volumen puede participar solo en una relación de reflejo.
- Para una pareja reflejada síncrona, los volúmenes primario y secundario deben ser volúmenes estándar. No pueden ser volúmenes finos o Snapshot.
- Para el mirroring síncrono, existen límites sobre la cantidad de volúmenes que se admiten en una cabina de almacenamiento determinada. Asegúrese de que la cantidad de volúmenes configurados en la cabina de almacenamiento sea menor que el límite admitido. Cuando se activa el mirroring síncrono, los dos volúmenes de capacidad reservada creados se cuentan para el límite de volúmenes.
- Para el mirroring asíncrono, el volumen primario y el volumen secundario deben tener las mismas capacidades Drive Security.

- Si el volumen primario es compatible con FIPS, el volumen secundario debe ser compatible con FIPS.
- Si el volumen primario es compatible con FDE, el volumen secundario debe ser compatible con FDE.
- Si el volumen primario no utiliza Drive Security, el volumen secundario no debe usar Drive Security.

Capacidad reservada

Mirroring asíncrono:

- Se requiere un volumen de capacidad reservada en el volumen primario y en el volumen secundario de una pareja reflejada para registrar la información de escritura que se utiliza en la recuperación de los restablecimientos de la controladora y otras interrupciones temporales.
- Debido a que tanto el volumen primario como el volumen secundario de una pareja reflejada requieren capacidad reservada adicional, debe asegurarse de contar con capacidad libre disponible en ambas cabinas de almacenamiento de la relación de reflejo.

Mirroring síncrono:

- Se requiere capacidad reservada en el volumen primario y en el volumen secundario para registrar la información de escritura que se utiliza en la recuperación de los restablecimientos de la controladora y otras interrupciones temporales.
- Los volúmenes de capacidad reservada se crean automáticamente cuando se activa el mirroring síncrono. Debido a que tanto el volumen primario como el volumen secundario de una pareja reflejada requieren capacidad reservada, debe asegurarse de contar con capacidad libre suficiente en ambas cabinas de almacenamiento que participan en la relación de reflejo síncrono.

Función Drive Security

- Si utiliza unidades compatibles con la función de seguridad, tanto el volumen primario como el secundario deben tener una configuración de seguridad compatible. Esta restricción no se aplica; por lo tanto, debe verificarlo por su cuenta.
- Si utiliza unidades compatibles con la función de seguridad, tanto el volumen primario como el secundario deberían usar el mismo tipo de unidad. Esta restricción no se aplica; por lo tanto, debe verificarlo por su cuenta.
- Si utiliza Data Assurance (DA), el volumen primario y el secundario deben tener la misma configuración DE DA.

Configurar el mirroring

Cree una pareja reflejada asíncrona

Para configurar el mirroring asíncrono, debe crear una pareja reflejada que incluya un volumen primario en la cabina local y un volumen secundario en la cabina remota.

Antes de empezar

Antes de crear una pareja reflejada, debe cumplir con los requisitos para Unified Manager:

- El proxy de servicios web se encuentra en ejecución.
- Unified Manager se ejecuta en el host local a través de una conexión HTTPS.
- SANtricity Unified Manager debe mostrar los certificados SSL válidos para la cabina de almacenamiento. Es posible aceptar un certificado autofirmado o instalar una certificación de seguridad propia con Unified

Manager. Para hacerlo, debe navegar hasta MENU:Certificate[Gestión de certificados].

También debe cumplir con los siguientes requisitos para las cabinas de almacenamiento y los volúmenes:

- Cada cabina de almacenamiento debe tener dos controladoras.
- Las dos cabinas de almacenamiento se encuentran detectadas en Unified Manager.
- Cada controladora en la cabina primaria y la cabina secundaria debe tener un puerto Ethernet de gestión configurado y debe estar conectada a la red.
- Las cabinas de almacenamiento deben tener la versión de firmware 7.84 como mínimo. (Cada una puede ejecutar versiones de sistema operativo diferentes).
- Debe conocer la contraseña de las cabinas de almacenamiento remota y local.
- Debe tener suficiente capacidad libre en la cabina de almacenamiento remota para crear un volumen secundario mayor o igual que el volumen primario que desea reflejar.
- Las cabinas de almacenamiento local y remota se encuentran conectadas a través de una estructura Fibre Channel o una interfaz iSCSI.
- Creó el volumen primario y el volumen secundario que desea usar en la relación de reflejo asíncrono.
- El volumen secundario deber tener al menos el tamaño del volumen primario.

Acerca de esta tarea

El proceso para crear una pareja reflejada asíncrona es un procedimiento de varios pasos.

Paso 1: Cree o seleccione un grupo de coherencia de reflejos

En este paso, debe crear un grupo de coherencia de reflejos nuevo o seleccionar uno existente. Un grupo de coherencia de reflejos es un contenedor para los volúmenes primario y secundario (la pareja reflejada), y especifica el método de resincronización deseado (manual o automático) para todas las parejas del grupo.

Pasos

1. En la página **gestionar**, seleccione la matriz de almacenamiento local que desea utilizar para el origen.
2. Seleccione **acciones › Crear pareja reflejada asíncrona**.

   Se abrirá el asistente Crear pareja reflejada asíncrona.

3. Seleccione un grupo de coherencia de reflejos existente o cree uno nuevo.

   Para seleccionar un grupo existente, asegúrese de que **un grupo de consistencia de mirroring** existente está seleccionado y, a continuación, seleccione el grupo de la tabla. Un grupo de coherencia puede incluir varias parejas reflejadas.

   Para crear un grupo nuevo, realice lo siguiente:

   a. Seleccione **Un nuevo grupo de coherencia de reflejos** y, a continuación, haga clic en **Siguiente**.
   b. Introduzca un nombre único que describa mejor los datos de los volúmenes que se reflejarán entre las dos cabinas de almacenamiento. Un nombre sólo puede contener letras, números y los caracteres especiales de subrayado (_), guión (-) y el signo de hash (#). Un nombre no puede superar los 30 caracteres y no puede contener espacios.
   c. Seleccione la cabina de almacenamiento remota en la que desea establecer una relación de reflejo con la cabina de almacenamiento local.

Si la cabina de almacenamiento remota está protegida con contraseña, el sistema solicita la contraseña.

d. Elija si desea sincronizar las parejas reflejadas de forma manual o automática:

- **Manual** — Seleccione esta opción para iniciar manualmente la sincronización de todas las parejas reflejadas dentro de este grupo. Tenga en cuenta que, cuando desee realizar una resincronización más tarde, deberá iniciar System Manager para la cabina de almacenamiento primaria y, a continuación, deberá ir al menú:almacenamiento[Mirroring asíncrono], seleccionar el grupo en la pestaña **grupos de coherencia de reflejos** y seleccionar MENU:más[Resincronizar manualmente].
- **Automático** — Seleccione el intervalo deseado en **minutos**, **horas** o **días**, desde el comienzo de la actualización anterior hasta el comienzo de la siguiente. Por ejemplo, si se establece el intervalo de sincronización en 30 minutos y el proceso de sincronización comienza a las 4:00 p. m., el siguiente proceso comenzará a las 4:30 p. m.

e. Seleccione las opciones de alerta deseadas:

- Para las sincronizaciones manuales, especifique el umbral (que se define según el porcentaje de capacidad restante) cuando desea recibir alertas.
- Para las sincronizaciones automáticas, puede establecer tres métodos de alerta: cuando la sincronización no se completa en un lapso específico, cuando los datos del punto de recuperación en la cabina remota son más antiguos que un límite de tiempo específico y cuando la capacidad reservada está cerca de un umbral específico (definido por el porcentaje de capacidad restante).

4. Seleccione **Siguiente** y vaya a. Paso 2: Seleccione el volumen primario.

Si definió un grupo de coherencia de reflejos nuevo, Unified Manager crea el grupo de coherencia de reflejos en la cabina de almacenamiento local primero y, a continuación, crea el grupo de coherencia de reflejos en la cabina de almacenamiento remota. Para ver y gestionar el grupo de coherencia de reflejos, inicie la instancia de System Manager de cada cabina.

Si Unified Manager crea correctamente el grupo de coherencia de reflejos en la cabina de almacenamiento local, pero no logra crearlo en la cabina de almacenamiento remota, elimina automáticamente el grupo de coherencia de reflejos de la cabina de almacenamiento local. Si se produce un error mientras Unified Manager intenta eliminar el grupo de coherencia de reflejos, es necesario eliminarlo en forma manual.

Paso 2: Seleccione el volumen primario

En este paso, se selecciona el volumen primario que se usará en la relación de reflejo y se asigna la capacidad reservada. Si selecciona un volumen primario en la cabina de almacenamiento local, el sistema muestra una lista de todos los volúmenes elegibles para esa pareja reflejada. Si algún volumen no es apto para el uso, no se muestra en esa lista.

Todos los volúmenes que añada al grupo de coherencia de reflejos de la cabina de almacenamiento local tendrán el rol primario en la relación de reflejo.

Pasos

1. En la lista de volúmenes elegibles, seleccione el volumen que desea usar como el volumen primario y haga clic en **Siguiente** para asignar la capacidad reservada.
2. En la lista de candidatos elegibles, seleccione la capacidad reservada para el volumen primario.

   Tenga en cuenta las siguientes directrices:

- La configuración predeterminada para la capacidad reservada es del 20 % del volumen base y, por lo general, esta capacidad es suficiente. Si cambia el porcentaje, haga clic en **Actualizar candidatos**.
- La capacidad necesaria varía, según la frecuencia y el tamaño de las escrituras de I/o en el volumen primario y el tiempo que se requiere conservar la capacidad.
- En general, elija una capacidad mayor para la capacidad reservada si se presentan una o ambas de estas condiciones:
  - Se pretende conservar la pareja reflejada por un periodo prolongado.
  - Un gran porcentaje de bloques de datos cambiará en el volumen primario debido a una gran actividad de I/O. Utilice datos históricos de rendimiento u otra utilidad del sistema operativo para determinar la actividad de I/o típica del volumen primario.

3. Seleccione **Siguiente** y vaya a. Paso 3: Seleccione el volumen secundario.

Paso 3: Seleccione el volumen secundario

En este paso, se selecciona el volumen secundario que se usará en la relación de reflejo y se asigna la capacidad reservada. Si selecciona un volumen secundario en la cabina de almacenamiento remota, el sistema muestra una lista de todos los volúmenes aptos para esa pareja reflejada. Si algún volumen no es apto para el uso, no se muestra en esa lista.

Todos los volúmenes que añada al grupo de coherencia de reflejos de la cabina de almacenamiento remota tendrán el rol secundario en la relación de reflejo.

Pasos

1. En la lista de volúmenes elegibles, seleccione el volumen que desea usar como el volumen secundario en la pareja reflejada y haga clic en **Siguiente** para asignar la capacidad reservada.
2. En la lista de candidatos elegibles, seleccione la capacidad reservada para el volumen secundario.

   Tenga en cuenta las siguientes directrices:

   - La configuración predeterminada para la capacidad reservada es del 20 % del volumen base y, por lo general, esta capacidad es suficiente. Si cambia el porcentaje, haga clic en **Actualizar candidatos**.
   - La capacidad necesaria varía, según la frecuencia y el tamaño de las escrituras de I/o en el volumen primario y el tiempo que se requiere conservar la capacidad.
   - En general, elija una capacidad mayor para la capacidad reservada si se presentan una o ambas de estas condiciones:
     - Se pretende conservar la pareja reflejada por un periodo prolongado.
     - Un gran porcentaje de bloques de datos cambiará en el volumen primario debido a una gran actividad de I/O. Utilice datos históricos de rendimiento u otra utilidad del sistema operativo para determinar la actividad de I/o típica del volumen primario.

3. Seleccione **Finalizar** para completar la secuencia de duplicación asíncrona.

Resultados

Unified Manager realiza las siguientes acciones:

- Comienza la sincronización inicial entre la cabina de almacenamiento local y la remota.
- Crea la capacidad reservada para la pareja reflejada en la cabina de almacenamiento local y la remota.

Si el volumen que se está reflejando es fino, solo los bloques de aprovisionamiento (capacidad asignada en lugar de capacidad notificada) se transfieren al volumen secundario durante la sincronización inicial. Esto reduce la cantidad de datos que se deben transferir para completar la sincronización inicial.

Cree una pareja reflejada síncrona

Para configurar el mirroring síncrono, debe crear una pareja reflejada que incluya un volumen primario en la cabina local y un volumen secundario en la cabina remota.

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

Antes de empezar

Antes de crear una pareja reflejada, debe cumplir con los requisitos para Unified Manager:

- El proxy de servicios web se encuentra en ejecución.
- Unified Manager se ejecuta en el host local a través de una conexión HTTPS.
- SANtricity Unified Manager debe mostrar los certificados SSL válidos para la cabina de almacenamiento. Es posible aceptar un certificado autofirmado o instalar una certificación de seguridad propia con Unified Manager. Para hacerlo, debe navegar hasta MENU:Certificate[Gestión de certificados].

También debe cumplir con los siguientes requisitos para las cabinas de almacenamiento y los volúmenes:

- Las dos cabinas de almacenamiento que planea usar para el mirroring se detectaron en Unified Manager.
- Cada cabina de almacenamiento debe tener dos controladoras.
- Cada controladora en la cabina primaria y la cabina secundaria debe tener un puerto Ethernet de gestión configurado y debe estar conectada a la red.
- Las cabinas de almacenamiento deben tener la versión de firmware 7.84 como mínimo. (Cada una puede ejecutar versiones de sistema operativo diferentes).
- Debe conocer la contraseña de las cabinas de almacenamiento remota y local.
- Las cabinas de almacenamiento local y remota se encuentran conectadas a través de una estructura Fibre Channel.
- Creó el volumen primario y el volumen secundario que desea usar en la relación de reflejo síncrono.
- El volumen primario deber ser un volumen estándar. No puede ser un volumen fino ni un volumen Snapshot.
- El volumen secundario deber ser un volumen estándar. No puede ser un volumen fino ni un volumen Snapshot.
- El volumen secundario deber tener al menos el mismo tamaño que el volumen primario.

Acerca de esta tarea

El proceso para crear parejas reflejadas síncronas es un procedimiento de varios pasos.

Paso 1: Seleccione el volumen primario

En este paso, se selecciona el volumen primario que se usará en la relación de reflejo síncrono. Si selecciona un volumen primario en la cabina de almacenamiento local, el sistema muestra una lista de todos los volúmenes elegibles para esa pareja reflejada. Si algún volumen no es apto para el uso, no se muestra en esa lista. El volumen que seleccione tendrá el rol primario en la relación de reflejo.

Pasos

1. En la página **gestionar**, seleccione la matriz de almacenamiento local que desea utilizar para el origen.
2. Seleccione **acciones › Crear pareja reflejada síncrona**.

   Se abrirá el asistente Crear pareja reflejada síncrona.

3. En la lista de volúmenes elegibles, seleccione el volumen que desea usar como el volumen primario en el reflejo.
4. Seleccione **Siguiente** y vaya a. Paso 2: Seleccione el volumen secundario.

Paso 2: Seleccione el volumen secundario

En este paso, seleccione el volumen secundario que desea usar en la relación de reflejo. Si selecciona un volumen secundario en la cabina de almacenamiento remota, el sistema muestra una lista de todos los volúmenes aptos para esa pareja reflejada. Si algún volumen no es apto para el uso, no se muestra en esa lista. El volumen que seleccione tendrá el rol secundario en la relación de reflejo.

Pasos

1. Seleccione la cabina de almacenamiento remota en la que desea establecer una relación de reflejo con la cabina de almacenamiento local.

   Si la cabina de almacenamiento remota está protegida con contraseña, el sistema solicita la contraseña.

   - Las cabinas de almacenamiento se enumeran en una lista por nombre. Si no asignó ningún nombre a una cabina de almacenamiento, esta se muestra en la lista como "unnamed".
   - Si la cabina de almacenamiento que desea utilizar no aparece en la lista, asegúrese de que se haya detectado en Unified Manager.

2. En la lista de volúmenes elegibles, seleccione el volumen que desea usar como el volumen secundario en el reflejo.

   Si se eligió un volumen secundario con una capacidad mayor a la del volumen primario, la capacidad utilizable se restringe al tamaño del volumen primario.

3. Haga clic en **Siguiente** y vaya a. Paso 3: Seleccione la configuración de sincronización.

Paso 3: Seleccione la configuración de sincronización

En este paso, se seleccionan las opciones de configuración que determinan la forma en que se deben sincronizar los datos después de una interrupción de comunicación. Es posible establecer la prioridad que tendrá en cuenta el propietario de la controladora del volumen primario para resincronizar los datos con el volumen secundario después de una interrupción de comunicación. Además, es necesario seleccionar la política de resincronización: Manual o automática.

Pasos

1. Use la barra de desplazamiento para configurar la prioridad de sincronización.

   La prioridad de sincronización determina cuántos recursos del sistema se usan para completar la sincronización inicial y la operación de resincronización después de una interrupción de la comunicación en comparación con las solicitudes de I/o del servicio.

La prioridad que se configure en este cuadro de diálogo se aplicará tanto al volumen primario, como al secundario. Para modificar la tasa del volumen primario en otro momento, deberá ir a System Manager y seleccionar MENU:almacenamiento[Mirroring síncrono > más > Editar configuración].

Las tasas de prioridad de sincronización son las siguientes cinco:

- El más bajo
- Bajo
- Mediano
- Alto
- Máxima

Si la prioridad de sincronización se configuró con la tasa mínima, se prioriza la actividad de I/o y la operación de resincronización lleva más tiempo. Si la prioridad de sincronización se configuró con la tasa máxima, la operación de resincronización tiene prioridad, pero podría afectar a la actividad de I/o de la cabina de almacenamiento.

2. Elija si desea volver a sincronizar las parejas reflejadas de la cabina de almacenamiento remota en forma manual o automática.
   - **Manual** (la opción recomendada) — Seleccione esta opción para requerir que la sincronización se reanude manualmente después de restaurar la comunicación a una pareja reflejada. Esta opción proporciona la mejor oportunidad para recuperar datos.
   - **Automático** — Seleccione esta opción para iniciar la resincronización automáticamente después de restaurar la comunicación a un par reflejado.

     Para reanudar la sincronización manualmente, vaya a System Manager y seleccione MENU:Storage[Synchronous Mirroring], resalte la pareja reflejada en la tabla y seleccione **Reanudar** en **más**.
3. Haga clic en **Finalizar** para completar la secuencia de duplicación sincrónica.

Resultados

Una vez que se activa el mirroring, el sistema ejecuta las siguientes acciones:

- Comienza la sincronización inicial entre la cabina de almacenamiento local y la remota.
- Configura la prioridad de sincronización y la política de resincronización.
- Reserva el puerto que tiene el número más alto de la HIC de la controladora para reflejar la transmisión de datos.

  Las solicitudes de I/o que se reciben en este puerto son aceptadas únicamente de la controladora remota preferida, propietaria del volumen secundario en la pareja reflejada. (Se permiten las reservas en el volumen primario.)

- Crea dos volúmenes de capacidad reservada, uno para cada controladora, que se utilizan para registrar información de escritura para recuperarse de reinicios de controladoras y otras interrupciones temporales.

  La capacidad de cada volumen es 128 MIB. Sin embargo, si los volúmenes se colocan en un pool, se reservarán 4 GIB para cada volumen.

Después de terminar

Vaya a System Manager y seleccione MENU:Inicio[Ver operaciones en curso] para ver el progreso de la

operación de mirroring síncrono. Es posible que esta operación demore y que afecte el rendimiento del sistema.

Preguntas frecuentes

¿Qué debo saber antes de crear un grupo de coherencia de reflejos?

Siga estas directrices para poder crear un grupo de coherencia de reflejos.

Cumpla con los siguientes requisitos para Unified Manager:

- El proxy de servicios web se encuentra en ejecución.
- Unified Manager se ejecuta en el host local a través de una conexión HTTPS.
- SANtricity Unified Manager debe mostrar los certificados SSL válidos para la cabina de almacenamiento. Es posible aceptar un certificado autofirmado o instalar una certificación de seguridad propia con Unified Manager. Para hacerlo, debe navegar hasta MENU:Certificate[Gestión de certificados].

También debe cumplir con los siguientes requisitos para las cabinas de almacenamiento:

- Las dos cabinas de almacenamiento se encuentran detectadas en Unified Manager.
- Cada cabina de almacenamiento debe tener dos controladoras.
- Cada controladora en la cabina primaria y la cabina secundaria debe tener un puerto Ethernet de gestión configurado y debe estar conectada a la red.
- Las cabinas de almacenamiento deben tener la versión de firmware 7.84 como mínimo. (Cada una puede ejecutar versiones de sistema operativo diferentes).
- Debe conocer la contraseña de las cabinas de almacenamiento remota y local.
- Las cabinas de almacenamiento local y remota se encuentran conectadas a través de una estructura Fibre Channel o una interfaz iSCSI.

El mirroring síncrono no está disponible en los sistemas de almacenamiento EF600 o EF300.

¿Qué debo saber antes de crear una pareja reflejada?

Antes de crear una pareja reflejada, siga estas directrices.

- Debe tener dos cabinas de almacenamiento.
- Cada cabina de almacenamiento debe tener dos controladoras.
- Las dos cabinas de almacenamiento se encuentran detectadas en Unified Manager.
- Cada controladora en la cabina primaria y la cabina secundaria debe tener un puerto Ethernet de gestión configurado y debe estar conectada a la red.
- Las cabinas de almacenamiento deben tener la versión de firmware 7.84 como mínimo. (Cada una puede ejecutar versiones de sistema operativo diferentes).
- Debe conocer la contraseña de las cabinas de almacenamiento remota y local.
- Debe tener suficiente capacidad libre en la cabina de almacenamiento remota para crear un volumen secundario mayor o igual que el volumen primario que desea reflejar.
- El mirroring asíncrono se admite en controladoras con puertos de host Fibre Channel (FC) o iSCSI, mientras que el mirroring síncrono solo se admite en controladoras con puertos de host FC.

El mirroring síncrono no está disponible en los sistemas de almacenamiento EF600 o EF300.

¿Por qué debería cambiar este porcentaje?

En general, la capacidad reservada constituye el 20 % del volumen base para operaciones de mirroring asíncrono. Por lo general, esta capacidad es suficiente.

La capacidad necesaria varía, según la frecuencia y el tamaño de las escrituras de I/o en el volumen base y el periodo durante el cual se pretenda utilizar la operación de servicios de copia del objeto de almacenamiento. Por lo general, se debe seleccionar un porcentaje alto de capacidad reservada si existe una de estas condiciones, o ambas:

- Si la vida útil de la operación de servicios de copia de un objeto de almacenamiento en particular será muy prolongada.
- Si un gran porcentaje de bloques de datos cambiará en el volumen base debido a una gran actividad de I/O. Utilice los datos históricos de rendimiento u otras utilidades del sistema operativo como ayuda para determinar la actividad de I/o típica en el volumen base.

¿Por qué se muestra más de un candidato de capacidad reservada?

Si existe más de un volumen en un pool o grupo de volúmenes que cumple con el porcentaje de capacidad seleccionado para el objeto de almacenamiento, se mostrarán varios candidatos.

Para actualizar la lista de candidatos recomendados, es posible modificar el porcentaje de espacio de la unidad física que desea reservar en el volumen base para las operaciones de servicios de copia. Se mostrarán los mejores candidatos en función de su selección.

¿Por qué no se muestran todos los volúmenes?

Cuando se selecciona un volumen primario para una pareja reflejada, se muestra una lista con todos los volúmenes elegibles.

Si algún volumen no es apto para el uso, no se muestra en esa lista. Es posible que los volúmenes no sean admisibles por uno de los siguientes motivos:

- El volumen no está en estado óptimo.
- El volumen ya participa en una relación de mirroring.
- Para el mirroring síncrono, los volúmenes primario y secundario de una pareja reflejada deben ser volúmenes estándar. No pueden ser volúmenes finos o Snapshot.
- Para el mirroring asíncrono, los volúmenes finos deben tener la expansión automática habilitada.

Para las controladoras EF600 y EF300, los volúmenes primario y secundario de una pareja reflejada asíncrona deben coincidir con el mismo protocolo, nivel de soporte, tamaño de segmento, tipo de seguridad y nivel de RAID. Las parejas reflejadas asíncronas no elegibles no aparecerán en la lista de volúmenes disponibles.

¿Por qué no se muestran todos los volúmenes en la cabina de almacenamiento remota?

Cuando se selecciona un volumen secundario en la cabina de almacenamiento remota, se muestra una lista de todos los volúmenes elegibles para esa pareja reflejada.

Todos los volúmenes que no son elegibles no aparecen en esa lista. Es posible que haya volúmenes no elegibles por alguno de los siguientes motivos:

- El volumen no es estándar, por ejemplo, un volumen Snapshot.
- El volumen no está en estado óptimo.
- El volumen ya participa en una relación de mirroring.
- Para el mirroring asíncrono, los atributos de volumen fino entre el volumen primario y el volumen secundario no coinciden.
- Si utiliza Data Assurance (DA), el volumen primario y el secundario deben tener la misma configuración DE DA.
  - Si el volumen primario tiene la función DA habilitada, el volumen secundario también debe tenerla.
  - Si el volumen primario no tiene la función DA habilitada, el volumen secundario tampoco debe tenerla.
- Para el mirroring asíncrono, el volumen primario y el volumen secundario deben tener las mismas capacidades Drive Security.
  - Si el volumen primario es compatible con FIPS, el volumen secundario debe ser compatible con FIPS.
  - Si el volumen primario es compatible con FDE, el volumen secundario debe ser compatible con FDE.
  - Si el volumen primario no utiliza Drive Security, el volumen secundario no debe usar Drive Security.

¿Qué impacto tiene la prioridad de sincronización en las tasas de sincronización?

La prioridad de sincronización define la cantidad de tiempo de procesamiento que se asigna a las actividades de sincronización en relación con el rendimiento del sistema.

El propietario de la controladora del volumen primario realiza esta operación en segundo plano. Al mismo tiempo, el propietario de la controladora procesa las escrituras de I/o en el volumen primario y las escrituras remotas asociadas en el volumen secundario. Dado que la resincronización desvía los recursos de procesamiento de la controladora de la actividad de I/o, es posible que tenga un impacto en el rendimiento de la aplicación host.

Tenga en cuentas estas directrices para determinar cuánto puede demorar una prioridad de sincronización y cómo las prioridades de sincronización pueden afectar al rendimiento del sistema.

Las siguientes tasas de prioridad se encuentran disponibles:

- El más bajo
- Bajo
- Mediano
- Alto
- Máxima

La tasa de prioridad más baja es compatible con el rendimiento del sistema, pero la resincronización demora más tiempo. La tasa de prioridad más alta es compatible con la resincronización, pero el rendimiento del sistema puede verse afectado.

Estas directrices aproximan aproximadamente las diferencias entre las prioridades.

Tasa de prioridad para la sincronización completa	Tiempo transcurrido en comparación con la tasa de sincronización más alta
El más bajo	Tiempo aproximadamente 8 veces superior a la tasa de prioridad más alta
Bajo	Tiempo aproximadamente 6 veces superior a la tasa de prioridad más alta
Mediano	Tiempo aproximadamente 3,5 veces superior a la tasa de prioridad más alta
Alto	Tiempo aproximadamente 2 veces superior a la tasa de prioridad más alta

El tamaño del volumen y las cargas de la tasa de I/o del host afectan a las comparaciones de tiempo de sincronización.

¿Por qué se recomienda usar la política de sincronización manual?

Se recomienda la resincronización manual debido a que esta permite gestionar el proceso de resincronización de un modo que garantiza la mejor oportunidad para recuperar los datos.

Si utiliza una política de resincronización automática y surgen problemas de comunicación ocasionales durante la resincronización, podrían dañarse temporalmente los datos del volumen secundario. Una vez finalizada la resincronización, los datos se corrigen.

Certificados

Información general sobre certificados

La gestión de certificados permite crear solicitudes de firma de certificados (CSR), importar certificados y gestionar certificados existentes.

¿Qué son los certificados?

Certificates son archivos digitales que identifican entidades en línea, como sitios web y servidores, para comunicaciones seguras en Internet. Existen dos tipos de certificados: Un *certificado firmado* es validado por una entidad de certificación (CA) y un *certificado autofirmado* es validado por el propietario de la entidad en lugar de por un tercero.

Obtenga más información:

- "Cómo funcionan los certificados"
- "Terminología de certificados"

¿Cómo se configuran los certificados?

En Certificate Management, es posible configurar certificados para la estación de gestión donde se aloja Unified Manager e importar también certificados para las controladoras en las cabinas.

Obtenga más información:

- "Utilice certificados firmados por CA para el sistema de gestión"
- "Importar certificados para cabinas"

Conceptos

Cómo funcionan los certificados

Los certificados son archivos digitales que identifican entidades en línea, como sitios web y servidores, para poder establecer comunicaciones seguras en Internet.

Certificados firmados

Los certificados garantizan que solo se transmitan comunicaciones web en formato cifrado, de forma privada y sin alternaciones, entre el servidor especificado y el cliente. Con Unified Manager, es posible gestionar los certificados para el explorador en un sistema de gestión host y las controladoras en las cabinas de almacenamiento detectadas.

Un certificado puede estar firmado por una autoridad de confianza o puede ser autofirmado. La firma simplemente implica que alguien validó la identidad del propietario y determinó que sus dispositivos son de confianza. Las cabinas de almacenamiento se entregan con un certificado autofirmado generado automáticamente en cada controladora. Puede continuar usando el certificado autofirmado o puede obtener certificados firmados por CA para establecer conexiones más seguras entre las controladoras y los sistemas host.

> Si bien los certificados firmados por CA aumentan la protección de seguridad (por ejemplo, evitan los ataques de tipo "man in the middle"), también aplican tarifas que pueden ser costosas si la red es extensa. En cambio, los certificados autofirmados son menos seguros, pero son gratuitos. Por lo tanto, los certificados autofirmados se utilizan con mayor frecuencia para entornos de prueba internos, no en entornos de producción.

Un certificado firmado es validado por una entidad de certificación (CA), que es una organización de terceros de confianza. Los certificados firmados incluyen detalles sobre el propietario de la entidad (generalmente, un servidor o sitio web), la fecha de emisión y de vencimiento del certificado, los dominios válidos de la entidad, y una firma digital compuesta por letras y números.

Al abrir un explorador y escribir una dirección web, el sistema ejecuta un proceso de comprobación de certificados en segundo plano para determinar si el usuario se está conectando a un sitio web que incluye un certificado válido firmado por una CA. Generalmente, un sitio que está protegido con un certificado firmado incluye un icono de candado y una designación https en la dirección. Si el usuario intenta conectarse a un sitio web que no contiene un certificado firmado por CA, el explorador mostrará una advertencia para indicar que el sitio no es seguro.

La CA toma las medidas necesarias para verificar las identidades durante el proceso de solicitud. La entidad puede enviar un correo electrónico a la empresa registrada, verificar la dirección empresarial, y realizar una verificación de HTTP o DNS. Una vez completado el proceso de solicitud, la CA envía los archivos digitales para cargar en el sistema de gestión host. Normalmente, estos archivos contienen una cadena de confianza

como la siguiente:

- **Raíz** — en la parte superior de la jerarquía está el certificado raíz, que contiene una clave privada utilizada para firmar otros certificados. El certificado raíz identifica una organización de CA determinada. Si utiliza la misma CA para todos los dispositivos de red, solo necesita un certificado raíz.
- **Intermediate** — ramificándose desde la raíz son los certificados intermedios. La CA emite uno o varios certificados intermedios para actuar como intermediarios entre un certificado raíz y los certificados de servidor protegidos.
- **Servidor** — en la parte inferior de la cadena se encuentra el certificado de servidor, que identifica su entidad específica, como un sitio web u otro dispositivo. Cada controladora de una cabina de almacenamiento requiere un certificado de servidor aparte.

Certificados autofirmados

Cada controladora de la cabina de almacenamiento incluye un certificado autofirmado preinstalado. Un certificado autofirmado es similar a un certificado firmado por CA, excepto que es validado por el propietario de la entidad y no por un tercero. Al igual que un certificado firmado por CA, un certificado autofirmado contiene su propia clave privada, y también garantiza que los datos se cifren y se envíen a través de una conexión HTTPS entre un servidor y un cliente.

Los certificados autofirmados no son «'de confianza'» por parte de los navegadores. Cada vez que intente conectarse a un sitio web que solo contiene un certificado autofirmado, el explorador mostrará un mensaje de advertencia. Deberá hacer clic en un enlace del mensaje de advertencia para continuar al sitio web; al hacer eso, estará aceptando básicamente el certificado autofirmado.

Certificados para Unified Manager

La interfaz de Unified Manager se instala con el proxy de servicios web en un sistema host. Al abrir un explorador y intentar una conexión con Unified Manager, el explorador intenta verificar si el host es un origen de confianza mediante la comprobación de un certificado digital. Si el explorador no encuentra un certificado firmado por CA para el servidor, abrirá un mensaje de advertencia. Desde allí, podrá continuar al sitio web para aceptar el certificado autofirmado en esa sesión. También puede obtener certificados digitales firmados de una CA para que ya no vea el mensaje de advertencia.

Certificados para controladoras

Durante una sesión de Unified Manager, es posible que vea mensajes de seguridad adicionales al intentar acceder a una controladora que no tiene un certificado firmado por CA. En este caso, puede confiar de forma permanente en el certificado autofirmado o puede importar los certificados firmados por CA de las controladoras para que el proxy de servicios web pueda autenticar las solicitudes de cliente entrantes procedentes de estas controladoras.

Terminología de certificados

Los siguientes términos se utilizan en la gestión de certificados.

Duración	Descripción
APROX	Una entidad de certificación (CA) es una entidad de confianza que emite documentos electrónicos, denominados certificados digitales, para la seguridad de Internet. Estos certificados identifican a los propietarios de sitios web y, de esta manera, permiten conexiones seguras entre clientes y servidores.

Duración	Descripción
CSR	Una solicitud de firma de certificación (CSR) es un mensaje que envía un solicitante a una entidad de certificación (CA). La CSR valida la información que requiere la CA para emitir un certificado.
Certificado	Un certificado identifica al propietario de un sitio con el fin de brindar seguridad, para evitar que atacantes se hagan pasar por los propietarios del sitio. El certificado tiene información acerca del propietario del sitio y la identidad de la entidad de confianza que certifica (firma) esta información.
Cadena de certificados	La cadena de certificados es una jerarquía de archivos que suma una capa de seguridad a los certificados. Normalmente, la cadena incluye un certificado raíz en la parte superior de la jerarquía, uno o varios certificados intermedios y los certificados de servidor que identifican a las entidades.
Certificado intermedio	Uno o varios certificados intermedios se extienden como una rama del certificado raíz en la cadena de certificados. La CA emite uno o varios certificados intermedios para actuar como intermediarios entre un certificado raíz y los certificados de servidor protegidos.
Almacén de claves	Un almacén de claves es un repositorio en el sistema de gestión host que contiene claves privadas, junto con sus correspondientes claves públicas y certificados. Estas claves y certificados identifican a las entidades propias como, por ejemplo, las controladoras.
Certificado raíz	El certificado raíz se encuentra en la parte superior de la jerarquía de la cadena de certificados y contiene una clave privada que se utiliza para firmar otros certificados. El certificado raíz identifica una organización de CA determinada. Si utiliza la misma CA para todos los dispositivos de red, solo necesita un certificado raíz.
Certificado firmado	Un certificado que ha validado una entidad de certificación (CA). Este archivo de datos contiene una clave privada, y garantiza que los datos se envíen en formato cifrado entre un servidor y un cliente a través de una conexión HTTPS. Además, un certificado firmado incluye detalles sobre el propietario de la entidad (normalmente, un servidor o sitio web) y una firma digital compuesta por letras y números. Un certificado firmado usa una cadena de certificados y, por consiguiente, se utiliza con mayor frecuencia en los entornos de producción. También se conoce como "certificado firmado por CA" o "certificado de gestión".
Certificado autofirmado	Un certificado autofirmado es validado por el propietario de la entidad. Este archivo de datos contiene una clave privada, y garantiza que los datos se envíen en formato cifrado entre un servidor y un cliente a través de una conexión HTTPS. También incluye una firma digital compuesta por letras y números. Un certificado autofirmado no usa la misma cadena de confianza que un certificado firmado por CA y, por consiguiente, se utiliza con mayor frecuencia en los entornos de prueba. También se conoce como certificado "preinstalado".

Duración	Descripción
Certificado de servidor	El certificado de servidor se encuentra en la parte inferior de la cadena de certificados. Este certificado identifica la entidad específica del usuario, por ejemplo, un sitio web u otro dispositivo. Cada controladora de un sistema de almacenamiento requiere un certificado de servidor aparte.
Almacén de confianza	Un almacén de confianza es un repositorio que contiene certificados de terceros de confianza, por ejemplo, entidades de certificación.

Utilice certificados firmados por CA para el sistema de gestión

Es posible obtener e importar certificados firmados por CA para establecer un acceso seguro al sistema de gestión donde se aloja SANtricity Unified Manager.

Antes de empezar

Debe iniciar sesión con un perfil de usuario que cuente con permisos de administración de seguridad. De lo contrario, no se mostrarán las funciones de certificación.

Acerca de esta tarea

El uso de certificados firmados por CA implica un procedimiento de tres pasos.

Paso 1: Complete un archivo CSR

Primero, se debe generar un archivo de solicitud de firma de certificación (CSR), que identifica a la organización y al sistema host donde están instalados el proxy de servicios web y Unified Manager.

> También puede generar un archivo CSR con una herramienta como OpenSSL y saltar a. Paso 2: Enviar archivo CSR.

Pasos

1. Seleccione **Gestión de certificados**.
2. En la ficha Administración, seleccione **completar CSR**.
3. Introduzca la siguiente información y, a continuación, haga clic en **Siguiente**:
   - **Organización** — el nombre completo y legal de su empresa u organización. Incluya sufijos, como Inc. O Corp
   - **Unidad organizativa (opcional)** — la división de su organización que maneja el certificado.
   - **Ciudad/localidad** — la ciudad donde se encuentra su sistema anfitrión o negocio.
   - **Estado/Región (opcional)** — el estado o región donde está ubicado el sistema o negocio anfitrión.
   - **Código ISO de país**: Código ISO (Organización Internacional de Normalización) de dos dígitos de su país, por ejemplo, US.
4. Introduzca la siguiente información sobre el sistema host donde está instalado el proxy de servicios web:
   - **Nombre común** — la dirección IP o el nombre DNS del sistema host donde está instalado Web Services Proxy. Compruebe que la dirección sea correcta; esta debe coincidir exactamente con lo que se escribe para acceder a Unified Manager en el explorador. No incluya http:// ni https://. El nombre DNS no puede comenzar con un comodín.

- **Direcciones IP alternativas** — Si el nombre común es una dirección IP, opcionalmente puede escribir cualquier dirección IP adicional o alias para el sistema host. Si va a introducir varios datos, use un formato delimitado por comas.
- **Nombres DNS alternativos** — Si el nombre común es un nombre DNS, introduzca cualquier nombre DNS adicional para el sistema host. Si va a introducir varios datos, use un formato delimitado por comas. Si no hay nombres DNS alternativos, pero especificó un nombre DNS en el primer campo, copie ese nombre aquí. El nombre DNS no puede comenzar con un comodín.

5. Asegúrese de que la información del host sea correcta. Si no lo es, los certificados que se devuelven de la CA fallarán cuando intente importarlos.
6. Haga clic en **Finalizar**.
7. Vaya a. Paso 2: Enviar archivo CSR.

Paso 2: Enviar archivo CSR

Después de crear un archivo de solicitud de firma de certificación (CSR), se lo envía a una entidad de certificación (CA) para recibir certificados de gestión firmados para el sistema donde se aloja Unified Manager y el proxy de servicios web.

Los sistemas E-Series requieren un formato PEM (codificación ASCII Base64) para certificados firmados, que incluye los siguientes tipos de archivo: .Pem, .crt, .cer o .key.

Pasos

1. Busque el archivo CSR descargado.

   La ubicación de la carpeta de la descarga depende del explorador.

2. Envíe el archivo CSR a una CA (por ejemplo, VeriSign o DigiCert) y solicite certificados firmados en formato PEM.

   Después de enviar un archivo CSR a la CA, NO vuelva a generar otro archivo CSR. cada vez que genere una CSR, el sistema creará un par de claves pública y privada. La clave pública se incluye en la CSR, mientras que la clave privada se conserva en el almacén de claves del sistema. Cuando recibe los certificados firmados e importarlos, el sistema se asegura de que las claves pública y privada sean la pareja original. Si las claves no coinciden, los certificados firmados no funcionarán y debe solicitar certificados nuevos de la CA.

3. Cuando la CA devuelva los certificados firmados, vaya a. Paso 3: Importar certificados de gestión.

Paso 3: Importar certificados de gestión

Después de recibir certificados firmados de la CA, importe los certificados al sistema host donde se instalaron la interfaz de proxy de servicios web y Unified Manager.

Antes de empezar

- Recibió certificados firmados de la CA. Estos archivos incluyen el certificado raíz, uno o varios certificados intermedios y el certificado de servidor.
- Si la CA proporcionó un archivo de certificado encadenado (por ejemplo, un archivo .p7b), debe desempaquetar el archivo encadenado en archivos individuales: El certificado raíz, el o los certificados intermedios y el certificado de servidor. Puede utilizar Windows `certmgr` Utilidad para desempaquetar los archivos (haga clic con el botón derecho y seleccione MENU:todas las tareas[Exportar]). Se recomienda la

codificación base-64. Una vez completadas las exportaciones, se mostrará un archivo CER para cada archivo de certificado de la cadena.

- Copió los archivos de certificado en el sistema host donde se ejecuta el proxy de servicios web.

Pasos

1. Seleccione **Gestión de certificados**.
2. En la ficha Administración, seleccione **Importar**.

   Se abre un cuadro de diálogo para importar los archivos de certificado.

3. Haga clic en **examinar** para seleccionar primero los archivos de certificado raíz e intermedio y, a continuación, seleccionar el certificado de servidor. Si generó la CSR desde una herramienta externa, también debe importar el archivo de claves privadas que se creó junto con la CSR.

   Se muestran los nombres de los archivos en el cuadro de diálogo.

4. Haga clic en **Importar**.

Resultados

Los archivos se cargan y validan. La información del certificado aparece en la página Gestión de certificados.

Restablezca los certificados de gestión

Es posible revertir el certificado de gestión a su estado autofirmado original de fábrica.

Antes de empezar

Debe iniciar sesión con un perfil de usuario que cuente con permisos de administración de seguridad. De lo contrario, no se mostrarán las funciones de certificación.

Acerca de esta tarea

Esta tarea elimina el certificado de gestión actual del sistema host donde están instalados el proxy de servicios web y Unified Manager. Una vez restablecido el certificado, el sistema host se revierte al uso del certificado autofirmado.

Pasos

1. Selecciona **Ajustes > Certificados**.
2. Seleccione la pestaña **Array Management** y, a continuación, seleccione **Reset**.

   Se abre el cuadro de diálogo Confirmar restablecimiento de certificado de gestión.

3. Tipo `reset` En el campo y, a continuación, haga clic en **Restablecer**.

   Una vez que se actualiza el explorador, es posible que el explorador bloquee el acceso al sitio de destino e informe de que el sitio utiliza HTTP estricto Transport Security. Esta condición surge cuando se cambia a certificados autofirmados. Para borrar la condición que bloquea el acceso al destino, debe borrar los datos de navegación del explorador.

Resultados

El sistema se revierte al uso del certificado autofirmado del servidor. Como resultado, el sistema solicita a los usuarios que acepten manualmente el certificado autofirmado para sus sesiones.

Usar certificados de cabina

Importar certificados para cabinas

Si es necesario, puede importar certificados para las cabinas de almacenamiento de modo que estas se puedan autenticar con el sistema donde se aloja SANtricity Unified Manager. Los certificados pueden estar firmados por una entidad de certificación (CA) o ser autofirmados.

Antes de empezar

- Debe iniciar sesión con un perfil de usuario que cuente con permisos de administración de seguridad. De lo contrario, no se mostrarán las funciones de certificación.
- Si desea importar certificados de confianza, es necesario importar los certificados para las controladoras de las cabinas de almacenamiento mediante System Manager.

Pasos

1. Seleccione **Gestión de certificados**.
2. Seleccione la ficha **Trusted**.

   Esta página muestra todos los certificados notificados para las cabinas de almacenamiento.

3. Seleccione menú:Importar[certificados] para importar un certificado de CA o menú:Importar[certificados de la cabina de almacenamiento autofirmados] para importar un certificado autofirmado.

   Para limitar la vista, puede utilizar el campo de filtrado **Mostrar certificados…** o puede ordenar las filas de certificados haciendo clic en uno de los encabezados de columna.

4. En el cuadro de diálogo, seleccione el certificado y, a continuación, haga clic en **Importar**.

   El certificado se carga y se valida.

Elimine certificados de confianza

Puede eliminar uno o varios certificados que ya no sean necesarios, por ejemplo, un certificado caducado.

Antes de empezar

Importe el certificado nuevo antes de eliminar el antiguo.

> Tenga en cuenta que la eliminación de un certificado intermedio o de raíz puede afectar a varias cabinas de almacenamiento, ya que es posible que estas cabinas compartan los mismos archivos de certificado.

Pasos

1. Seleccione **Gestión de certificados**.
2. Seleccione la ficha **Trusted**.
3. Seleccione uno o varios certificados de la tabla y, a continuación, haga clic en **Eliminar**.

> La función **Eliminar** no está disponible para los certificados preinstalados.

Se abrirá el cuadro de diálogo Confirmar eliminación de certificado de confianza.

4. Confirme la eliminación y haga clic en **Eliminar**.

   El certificado se eliminará de la tabla.

Resuelva los certificados que no son de confianza

Los certificados dejan de ser de confianza cuando una cabina de almacenamiento intenta establecer una conexión con SANtricity Unified Manager, pero no se confirma que la conexión sea segura.

En la página Certificado, puede resolver certificados que no son de confianza al importar un certificado autofirmado de la cabina de almacenamiento o al importar un certificado de una entidad de certificación (CA) que emitió un tercero de confianza.

Antes de empezar

- Inició sesión con un perfil de usuario que cuenta con permisos de administración de seguridad.
- Si tiene pensado importar un certificado firmado por una CA:
  - Generó una solicitud de firma de certificación (archivo .CSR) para cada controladora en la cabina de almacenamiento y la envió a la CA.
  - La CA devolvió archivos de certificado de confianza.
  - Los archivos de certificado están disponibles en el sistema local.

Acerca de esta tarea

Es posible que necesite instalar otros certificados de CA de confianza si se da alguna de las siguientes condiciones:

- Añadió recientemente una cabina de almacenamiento.
- Uno o ambos certificados caducaron.
- Uno o ambos certificados fueron revocados.
- Falta un certificado raíz o intermedio en uno o ambos certificados.

Pasos

1. Seleccione **Gestión de certificados**.
2. Seleccione la ficha **Trusted**.

   Esta página muestra todos los certificados notificados para las cabinas de almacenamiento.

3. Seleccione menú:Importar[certificados] para importar un certificado de CA o menú:Importar[certificados de la cabina de almacenamiento autofirmados] para importar un certificado autofirmado.

   Para limitar la vista, puede utilizar el campo de filtrado **Mostrar certificados…** o puede ordenar las filas de certificados haciendo clic en uno de los encabezados de columna.

4. En el cuadro de diálogo, seleccione el certificado y, a continuación, haga clic en **Importar**.

   El certificado se carga y se valida.

Gestionar certificados

Ver certificados

Es posible ver información resumida de un certificado, incluida la organización que utiliza el certificado, la entidad que lo emite, el periodo de validez y las huellas digitales (identificadores únicos).

Antes de empezar

Debe iniciar sesión con un perfil de usuario que cuente con permisos de administración de seguridad. De lo contrario, no se mostrarán las funciones de certificación.

Pasos

1. Seleccione **Gestión de certificados**.
2. Seleccione una de las siguientes pestañas:
   - **Administración** — muestra el certificado para el sistema que aloja el proxy de servicios web. Un certificado de gestión puede estar autofirmado o estar aprobado por una CA. Permite un acceso seguro a Unified Manager.
   - **Trusted**: Muestra los certificados a los que Unified Manager puede acceder para matrices de almacenamiento y otros servidores remotos, como un servidor LDAP. Los certificados pueden emitirse mediante una CA o estar autofirmados.
3. Para ver más información sobre un certificado, seleccione la fila correspondiente, seleccione las tres puntos al final de la fila y haga clic en **Ver** o **Exportar**.

Exportar certificados

Es posible exportar un certificado para ver todos sus detalles.

Antes de empezar

Para abrir el archivo exportado, debe contar con una aplicación para visualización de certificados.

Pasos

1. Seleccione **Gestión de certificados**.
2. Seleccione una de las siguientes pestañas:
   - **Administración** — muestra el certificado para el sistema que aloja el proxy de servicios web. Un certificado de gestión puede estar autofirmado o estar aprobado por una CA. Permite un acceso seguro a Unified Manager.
   - **Trusted**: Muestra los certificados a los que Unified Manager puede acceder para matrices de almacenamiento y otros servidores remotos, como un servidor LDAP. Los certificados pueden emitirse mediante una CA o estar autofirmados.
3. Seleccione un certificado de la página y, a continuación, haga clic en los tres puntos al final de la fila.
4. Haga clic en **Exportar** y guarde el archivo de certificado.
5. Abra el archivo en la aplicación para visualización de certificados.

Gestión del acceso

Información general de Access Management

Access Management es un método para configurar la autenticación de usuario en SANtricity Unified Manager.

¿Qué métodos de autenticación están disponibles?

Están disponibles los siguientes métodos de autenticación:

- **Roles de usuario local** — la autenticación se administra mediante funciones RBAC (control de acceso basado en roles). Los roles de usuario local incluyen perfiles de usuario predefinidos con permisos de acceso específicos.
- **Servicios de directorio** — la autenticación se administra a través de un servidor LDAP (protocolo ligero de acceso a directorios) y un servicio de directorio, como Active Directory de Microsoft.
- **SAML** — la autenticación se gestiona a través de un proveedor de identidades (IDP) que utiliza SAML 2.0.

Obtenga más información:

- "Cómo funciona Access Management"
- "Terminología de Access Management"
- "Permisos para roles asignados"
- "SAML"

¿Cómo se configura Access Management?

El software SANtricity está preconfigurado para usar roles de usuario local. Si desea utilizar LDAP, puede configurarlo en la página Access Management.

Obtenga más información:

- "Access Management con roles de usuario local"
- "Access Management con servicios de directorio"
- "Configure SAML"

Conceptos

Cómo funciona Access Management

Utilice Access Management para establecer la autenticación de usuario en SANtricity Unified Manager.

Flujo de trabajo de configuración

La configuración de Access Management funciona de la siguiente manera:

1. Un administrador inicia sesión en Unified Manager con un perfil de usuario que incluye permisos de administrador de seguridad.

La primera vez que se inicia sesión, el nombre de usuario `admin` se muestra automáticamente y no se puede cambiar. La `admin` el usuario tiene acceso completo a todas las funciones del sistema. La contraseña se debe establecer en el primer inicio de sesión.

2. El administrador se desplaza hasta Access Management en la interfaz de usuario, donde se incluyen roles de usuario local preconfigurados. Estos roles son una implementación de las funcionalidades de control de acceso basado en roles (RBAC).
3. El administrador configura uno o varios de los siguientes métodos de autenticación:
   - **Roles de usuario local** — la autenticación se administra mediante capacidades RBAC. Los roles de usuario local incluyen usuarios predefinidos con permisos de acceso específicos. Los administradores pueden usar estos roles de usuario local como el único método de autenticación o usarlos en combinación con un servicio de directorio. No hace falta configurar nada más allá de las contraseñas de los usuarios.
   - **Servicios de directorio** — la autenticación se administra a través de un servidor LDAP (protocolo ligero de acceso a directorios) y un servicio de directorio, como Active Directory de Microsoft. Un administrador se conecta con el servidor LDAP y, a continuación, asigna los usuarios LDAP a los roles de usuario local.
   - **SAML** — la autenticación se gestiona a través de un proveedor de identidades (IDP) utilizando el lenguaje de marcado de aserción de seguridad (SAML) 2.0. Un administrador establece comunicación entre el sistema IDP y la cabina de almacenamiento, y luego asigna los usuarios IDP a los roles de usuario local integrados en la cabina de almacenamiento.
4. El administrador proporciona credenciales de inicio de sesión en Unified Manager a los usuarios.
5. Los usuarios inician sesión en el sistema con sus credenciales. Durante el inicio de sesión, el sistema realiza las siguientes tareas en segundo plano:
   - Autentica el nombre de usuario y la contraseña en relación con la cuenta de usuario.
   - Determina los permisos del usuario según los roles asignados.
   - Ofrece acceso al usuario a las funciones en la interfaz de usuario.
   - Muestra el nombre de usuario en el banner superior.

Funciones disponibles en Unified Manager

El acceso a las funciones depende de los roles asignados a un usuario, entre los cuales se encuentran los siguientes:

- **Storage admin** — acceso completo de lectura/escritura a los objetos de almacenamiento de las matrices, pero sin acceso a la configuración de seguridad.
- **Security admin** — acceso a la configuración de seguridad en Access Management y Certificate Management.
- **Support admin** — acceso a todos los recursos de hardware en matrices de almacenamiento, datos de fallos y eventos MEL. No brinda acceso a los objetos de almacenamiento ni a la configuración de seguridad.
- **Monitor** — acceso de sólo lectura a todos los objetos de almacenamiento, pero sin acceso a la configuración de seguridad.

Una función no disponible se muestra atenuada o directamente no se muestra en la interfaz de usuario.

Terminología de Access Management

Conozca la forma en que los términos de Access Management se aplican a SANtricity Unified Manager.

Duración	Descripción
Active Directory	Active Directory (AD) es un servicio de directorio de Microsoft en el que se utiliza LDAP para redes de dominio de Windows.
Vinculación	Las operaciones de vinculación se usan para autenticar clientes en el servidor de directorio. Por lo general, la vinculación requiere credenciales de cuenta y contraseña, pero algunos servidores aceptan operaciones de vinculación anónimas.
APROX	Una entidad de certificación (CA) es una entidad de confianza que emite documentos electrónicos, denominados certificados digitales, para la seguridad de Internet. Estos certificados identifican a los propietarios de sitios web y, de esta manera, permiten conexiones seguras entre clientes y servidores.
Certificado	Un certificado identifica al propietario de un sitio con el fin de brindar seguridad, para evitar que atacantes se hagan pasar por los propietarios del sitio. El certificado tiene información acerca del propietario del sitio y la identidad de la entidad de confianza que certifica (firma) esta información.
LDAP	El protocolo ligero de acceso a directorios (LDAP) es un protocolo de aplicación para acceder a servicios distribuidos de información de directorio y mantenerlos. Este protocolo permite que varias aplicaciones y servicios se conecten con el servidor LDAP para validar usuarios.
RBAC	El control de acceso basado en funciones (RBAC) es un método para regular el acceso a los recursos informáticos o de red en función de las funciones de los usuarios individuales. Unified Manager incluye roles predefinidos.
SAML	El lenguaje de marcado de aserción de seguridad (SAML) es un estándar basado en XML para fines de autenticación y autorización entre dos entidades. SAML permite utilizar la autenticación multifactor, en la cual los usuarios deben introducir dos o más elementos para validar su identidad (por ejemplo, una contraseña y una huella digital). La función de SAML integrada de la cabina de almacenamiento es compatible con SAML2,0 para autenticación, autorización y confirmación de identidades.
SSO	El inicio de sesión único (SSO) es un servicio de autenticación que permite el uso de un conjunto de credenciales de inicio de sesión para acceder a varias aplicaciones.

Duración	Descripción
Proxy de servicios web	El proxy de servicios web, que proporciona acceso mediante mecanismos HTTPS estándar, permite a los administradores configurar servicios de gestión para las cabinas de almacenamiento. El proxy se puede instalar en hosts Windows o Linux. La interfaz de Unified Manager se encuentra disponible con el proxy de servicios web.

Permisos para roles asignados

Las funcionalidades de control de acceso basado en roles (RBAC) incluyen usuarios predefinidos con uno o varios roles asignados. Cada rol incluye permisos para acceder a tareas en SANtricity Unified Manager.

Los roles permiten que los usuarios accedan a tareas de la siguiente manera:

- **Storage admin** — acceso completo de lectura/escritura a los objetos de almacenamiento de las matrices, pero sin acceso a la configuración de seguridad.
- **Security admin** — acceso a la configuración de seguridad en Access Management y Certificate Management.
- **Support admin** — acceso a todos los recursos de hardware en matrices de almacenamiento, datos de fallos y eventos MEL. No brinda acceso a los objetos de almacenamiento ni a la configuración de seguridad.
- **Monitor** — acceso de sólo lectura a todos los objetos de almacenamiento, pero sin acceso a la configuración de seguridad.

Si un usuario no tiene permisos para una función determinada, esa función no se encuentra disponible para selección o no se muestra en la interfaz de usuario.

Access Management con roles de usuario local

Los administradores pueden utilizar las funcionalidades de control de acceso basado en roles (RBAC) que se aplican en Unified Manager de SANtricity. Estas capacidades se denominan "roles de usuario local".

Flujo de trabajo de configuración

Los roles de usuario local están preconfigurados en el sistema. Para usar roles de usuario local con fines de autenticación, los administradores pueden hacer lo siguiente:

1. Un administrador inicia sesión en Unified Manager con un perfil de usuario que incluye permisos de administrador de seguridad.

   > La `admin` el usuario tiene acceso completo a todas las funciones del sistema.

2. Un administrador revisa los perfiles de usuario, que están predefinidos y no pueden modificarse.
3. De manera opcional, el administrador asigna nuevas contraseñas para cada perfil de usuario.
4. Los usuarios inician sesión en el sistema con las credenciales asignadas.

Gestión

Al utilizar solamente los roles de usuario local para la autenticación, los administradores pueden realizar las siguientes tareas de gestión:

- Cambiar contraseñas.
- Configurar la longitud mínima de las contraseñas.
- Permitir que los usuarios inicien sesión sin contraseñas.

Access Management con servicios de directorio

Los administradores puede usar un servidor de protocolo ligero de acceso a directorios (LDAP) y un servicio de directorio, como Active Directory de Microsoft.

Flujo de trabajo de configuración

Si se utilizan un servidor LDAP y un servicio de directorio en la red, la configuración opera de la siguiente manera:

1. Un administrador inicia sesión en Unified Manager con un perfil de usuario que incluye permisos de administrador de seguridad.

   La `admin` el usuario tiene acceso completo a todas las funciones del sistema.

2. El administrador introduce los ajustes de configuración del servidor LDAP. Entre ellas se encuentran el nombre de dominio, la URL y la información de la cuenta vinculada.
3. Si el servidor LDAP utiliza un protocolo seguro (LDAPS), el administrador carga una cadena de certificados de una entidad de certificación (CA) para la autenticación entre el servidor LDAP y el sistema host donde se instaló el proxy de servicios web.
4. Después de establecer la conexión del servidor, el administrador asigna los grupos de usuarios a los roles de usuario local. Estos roles están predefinidos y no pueden modificarse.
5. El administrador prueba la conexión entre el servidor LDAP y el proxy de servicios web.
6. Los usuarios inician sesión en el sistema con las credenciales de LDAP/servicios de directorio asignadas.

Gestión

Al utilizar los servicios de directorio para la autenticación, los administradores pueden realizar las siguientes tareas de gestión:

- Añadir servidor de directorio.
- Editar la configuración del servidor de directorio.
- Asignar usuarios LDAP a roles de usuario local.
- Quitar un servidor de directorio.
- Cambiar contraseñas.
- Configurar la longitud mínima de las contraseñas.
- Permitir que los usuarios inicien sesión sin contraseñas.

Access Management con SAML

Para Access Management, los administradores pueden usar las funcionalidades de lenguaje de marcado de aserción de seguridad (SAML) 2.0 que están integradas en la cabina.

Flujo de trabajo de configuración

La configuración de SAML funciona de la siguiente manera:

1. Un administrador inicia sesión en Unified Manager con un perfil de usuario que incluye permisos de administración de seguridad.

   La `admin` El usuario tiene acceso completo a todas las funciones en System Manager.

2. El administrador se dirige a la ficha **SAML** de Access Management.
3. Un administrador configura las comunicaciones con el proveedor de identidades (IDP). Un IDP es un sistema externo que se usa para solicitar credenciales a un usuario y determinar si el usuario se autentica correctamente. Para configurar las comunicaciones con la cabina de almacenamiento, el administrador descarga el archivo de metadatos de IdP desde el sistema IdP y luego usa Unified Manager para cargarlo a la cabina de almacenamiento.
4. Un administrador establece una relación de confianza entre el proveedor de servicios y el IDP. Un proveedor de servicios controla la autorización de usuarios; en este caso, la controladora en la cabina de almacenamiento actúa como proveedor de servicios. Para configurar las comunicaciones, el administrador usa Unified Manager para exportar el archivo de metadatos del proveedor de servicios de la controladora. Desde el sistema IdP, el administrador importa el archivo de metadatos al IdP.

   Los administradores también deben asegurarse de que el IDP admite la capacidad para obtener un ID de nombre en el momento de la autenticación.

5. El administrador asigna los roles de la cabina de almacenamiento a los atributos de usuario definidos en el IDP. Para hacerlo, el administrador usa Unified Manager y crea las asignaciones.
6. El administrador prueba el inicio de sesión de SSO en la URL del IDP. Esta prueba garantiza que la cabina de almacenamiento y el IDP puedan comunicarse.

   Una vez que se habilita SAML, _no se puede deshabilitar desde la interfaz de usuario, tampoco se puede editar desde la configuración de IDP. Si necesita deshabilitar o editar la configuración de SAML, comuníquese con el soporte técnico para obtener ayuda.

7. En Unified Manager, el administrador del sistema habilita SAML para la cabina de almacenamiento.
8. Los usuarios inician sesión en el sistema con sus credenciales de SSO.

Gestión

Cuando se usa SAML con fines de autenticación, los administradores pueden realizar las siguientes tareas de administración:

- Modifique o cree nuevas asignaciones de roles
- Exporte los archivos del proveedor de servicios

Restricciones de acceso

Cuando se habilita SAML, los usuarios no pueden detectar ni gestionar el almacenamiento de esa cabina desde la interfaz de Storage Manager heredada.

Además, los siguientes clientes no pueden obtener acceso a los recursos y los servicios de la cabina de almacenamiento:

- Enterprise Management Window (EMW)
- Interfaz de línea de comandos (CLI)
- Clientes de kits de desarrollo de software (SDK)
- Clientes en banda
- Clientes HTTP de la API de REST de autenticación básica
- Inicio de sesión mediante extremo estándar de la API de REST

Use los roles de usuario local

Ver los roles de usuario local

Desde la pestaña roles de usuario local, es posible ver las asignaciones de los usuarios a los roles predeterminados. Estas asignaciones forman parte de los RBAC aplicados en el proxy de servicios web de Unified Manager de SANtricity.

Antes de empezar

Debe iniciar sesión con un perfil de usuario que cuente con permisos de administración de seguridad. De lo contrario, no se mostrarán las funciones de Access Management.

Acerca de esta tarea

Los usuarios y las asignaciones no pueden cambiarse. Solo las contraseñas pueden modificarse.

Pasos

1. Seleccione **Access Management**.
2. Seleccione la ficha **roles de usuario local**.

   Los usuarios se muestran en la tabla:

   - **Admin** — Super administrador que tiene acceso a todas las funciones del sistema. Este usuario incluye todos los roles.
   - **Almacenamiento** — el administrador responsable de todo el aprovisionamiento de almacenamiento. Este usuario incluye los siguientes roles: Administrador de almacenamiento, administrador de soporte y Supervisión.
   - **Security**: El usuario responsable de la configuración de seguridad, incluidos Access Management y Certificate Management. Este usuario incluye los siguientes roles: Administrador de seguridad y Supervisión.
   - **Soporte**: El usuario responsable de recursos de hardware, datos de fallos y actualizaciones de firmware. Este usuario incluye los siguientes roles: Administrador de soporte y Supervisión.
   - **Monitor** — un usuario con acceso de sólo lectura al sistema. Este usuario incluye únicamente el rol Supervisión.

- **rw** (lectura/escritura): Este usuario incluye los siguientes roles: Administrador de almacenamiento, administrador de soporte y monitor.
- **Ro** (sólo lectura) — este usuario incluye sólo la función Monitor.

Cambiar contraseñas de perfiles de usuario local

Es posible cambiar las contraseñas de usuario de cada usuario desde Access Management.

Antes de empezar

- Inició sesión como administrador local, lo que incluye permisos de administrador raíz.
- Debe conocer la contraseña de administrador local.

Acerca de esta tarea

Tenga en cuenta estas directrices al elegir una contraseña:

- Todas las contraseñas de usuarios locales nuevas deben alcanzar o superar la configuración de longitud mínima actual de la contraseña (en Ver/editar configuración).
- Las contraseñas distinguen mayúsculas de minúsculas.
- Los espacios al final de la contraseña no se eliminan si se los utiliza. Procure incluir espacios si se incluyeron en la contraseña.
- Para mayor seguridad, use al menos 15 caracteres alfanuméricos y cambie la contraseña con frecuencia.

Pasos

1. Seleccione **Access Management**.
2. Seleccione la ficha **roles de usuario local**.
3. Seleccione un usuario de la tabla.

   Se habilita el botón Cambiar contraseña.

4. Seleccione **Cambiar contraseña**.

   Se abre el cuadro de diálogo Cambiar contraseña.

5. Si no existe una longitud mínima de contraseña establecida para las contraseñas de usuario local, puede seleccionar la casilla de comprobación para requerir que el usuario introduzca una contraseña para acceder al sistema.
6. Introduzca la contraseña nueva para el usuario seleccionado en los dos campos.
7. Introduzca su contraseña de administrador local para confirmar esta operación y, a continuación, haga clic en **Cambiar**.

Resultados

Si el usuario está conectado, el cambio de contraseña provocará el cierre de la sesión activa del usuario.

Cambie la configuración de contraseña de usuario local

Es posible configurar la longitud mínima requerida para todas las contraseñas de usuario local nuevas o actualizadas. También es posible permitir a los usuarios locales que accedan al sistema sin introducir una contraseña.

Antes de empezar

Inició sesión como administrador local, lo que incluye permisos de administrador raíz.

Acerca de esta tarea

Recuerde estas directrices cuando configure la longitud mínima para las contraseñas de usuario local:

- Los cambios en la configuración no afectan a las contraseñas existentes de usuarios locales.
- La configuración de la longitud mínima requerida para las contraseñas de usuario local debe tener entre 0 y 30 caracteres.
- Todas las contraseñas de usuario local nuevas deben alcanzar o superar la configuración de longitud mínima actual.
- No configure una longitud mínima para la contraseña si desea que los usuarios locales accedan al sistema sin introducir una contraseña.

Pasos

1. Seleccione **Access Management**.
2. Seleccione la ficha **roles de usuario local**.
3. Seleccione **Ver/editar configuración**.

   Se abre el cuadro de diálogo Configuración de contraseña de usuario local.

4. Debe realizar una de las siguientes acciones:
   - Para permitir a los usuarios locales que accedan al sistema *without* password, desactive la casilla de verificación "requerir que todas las contraseñas de usuario local tengan al menos…".
   - Si desea configurar una longitud mínima de contraseña para todas las contraseñas de usuario local, active la casilla de comprobación "requerir que todas las contraseñas de usuario local tengan al menos…" y luego use el cuadro de desplazamiento para configurar la longitud mínima requerida para todas las contraseñas de usuario local

     Todas las contraseñas de usuario local nuevas deben alcanzar o superar la configuración actual.

5. Haga clic en **Guardar**.

Uso de los servicios de directorio

Añadir servidor de directorio

Para configurar la autenticación de Access Management, se debe establecer la comunicación entre un servidor LDAP y el host donde se ejecuta el proxy de servicios web para Unified Manager de SANtricity. A continuación, se deben asignar los grupos de usuarios LDAP a los roles de usuario local.

Antes de empezar

- Debe iniciar sesión con un perfil de usuario que cuente con permisos de administración de seguridad. De lo contrario, no se mostrarán las funciones de Access Management.
- Debe haber grupos de usuarios definidos en el servicio de directorio.
- Deben estar disponibles las credenciales del servidor LDAP, incluidos el nombre de dominio y la URL del servidor y, de manera opcional, el nombre de usuario y la contraseña de la cuenta de enlace.

- En el caso de los servidores LDAPS que utilizan un protocolo seguro, se debe instalar la cadena de certificados del servidor LDAP en la máquina local.

Acerca de esta tarea

La adición de un servidor de directorio es un proceso que consta de dos pasos. Primero, se debe introducir la URL y el nombre de dominio. Si el servidor utiliza un protocolo seguro, se debe cargar también un certificado de CA para autenticación si no se encuentra firmado por una entidad de firma estándar. Si se poseen credenciales de una cuenta de enlace, es posible introducir también el nombre de cuenta de usuario y la contraseña. Luego, se deben asignar los grupos de usuarios del servidor LDAP a los roles de usuario local.

Pasos

1. Seleccione **Access Management**.
2. En la ficha **Servicios de directorio**, seleccione **Agregar servidor de directorio**.

   Se abre el cuadro de diálogo Añadir servidor de directorio.

3. En la ficha **Configuración del servidor**, introduzca las credenciales del servidor LDAP.

Detalles del campo

Ajuste	Descripción
Ajustes de configuración	Dominios
Introduzca el nombre de dominio del servidor LDAP. Si desea introducir varios dominios, escríbalos en una lista separada por comas. El nombre de dominio se utiliza en el inicio de sesión (*username@domain*) para especificar con qué servidor de directorio debe realizarse la autenticación.	URL del servidor
Introduzca la URL para acceder al servidor LDAP con el formato de `ldap[s]://**host:***port*`.	Cargar certificado (opcional)

Ajuste	Descripción
Este campo aparece solo si se especifica un protocolo LDAPS en el campo URL del servidor arriba. Haga clic en **examinar** y seleccione un certificado de CA para cargar. Este es el certificado o la cadena de certificados de confianza utilizado para autenticar el servidor LDAP.	Enlazar cuenta (opcional)
Introduzca una cuenta de usuario de solo lectura para realizar consultas de búsqueda en el servidor LDAP y para buscar dentro de los grupos. Introduzca el nombre de cuenta con formato tipo LDAP. Por ejemplo, si el usuario de enlace se denomina "bindacct", es posible introducir un valor como el siguiente `CN=bindacct,CN=Users,DC=cpoc,DC=local`.	Enlazar contraseña (opcional)

Ajuste	Descripción
Este campo se muestra cuando se introduce una cuenta de enlace. Introduzca la contraseña de la cuenta de enlace.	Probar conexión del servidor antes de añadir
Seleccione esta casilla de comprobación si desea asegurarse de que el sistema pueda comunicarse con la configuración de servidor LDAP que introdujo. La prueba se produce después de hacer clic en **Agregar** en la parte inferior del cuadro de diálogo. Si esta casilla de comprobación está seleccionada y la prueba falla, no se añadirá la configuración. Debe resolver el error o anular la selección de la casilla de comprobación para omitir la comprobación y añadir la configuración.	**Configuración de privilegios**
DN base de búsqueda	Introduzca el contexto de LDAP para buscar usuarios, generalmente con el formato de `CN=Users, DC=cpoc, DC=local`.
Atributo de nombre de usuario	Introduzca el atributo vinculado al ID de usuario para los fines de autenticación. Por ejemplo: `sAMAccountName`.

Ajuste	Descripción
Atributos de grupo	Introduzca una lista de atributos de grupo en el usuario, que se utilizará para la asignación de grupos a roles. Por ejemplo: `memberOf, managedObjects`.

4. Haga clic en la ficha **asignación de roles**.
5. Asigne grupos LDAP a los roles predefinidos. Un grupo puede tener varios roles asignados.

Detalles del campo

Ajuste	Descripción
Asignaciones	DN de grupo
Especifique el nombre distintivo (DN) del grupo correspondiente al grupo de usuarios LDAP que se asignará. Se admiten expresiones regulares. Estos caracteres especiales de expresión regular deben escaparse con una barra diagonal inversa (\) si no forman parte de un patrón de expresión regular: \.[]{}()<>*+-=?<$	
Funciones	Haga clic en el campo y seleccione uno de los roles de usuario local que se asignará al DN del grupo. Debe seleccionar individualmente cada rol que desee incluir en este grupo. Se requiere el rol de supervisión junto con los demás roles para iniciar sesión en SANtricity Unified Manager. Los roles asignados incluyen los siguientes permisos: • **Storage admin** — acceso completo de lectura/escritura a los objetos de almacenamiento de las matrices, pero sin acceso a la configuración de seguridad. • **Security admin** — acceso a la configuración de seguridad en Access Management y Certificate Management. • **Support admin** — acceso a todos los recursos de hardware en matrices de almacenamiento, datos de fallos y eventos MEL. No brinda acceso a los objetos de almacenamiento ni a la configuración de seguridad. • **Monitor** — acceso de sólo lectura a todos los objetos de almacenamiento, pero sin acceso a la configuración de seguridad.

El rol de supervisión se requiere para todos los usuarios, incluido el administrador.

6. Si lo desea, haga clic en **Agregar otra asignación** para introducir más asignaciones de grupo a rol.
7. Cuando termine de asignar, haga clic en **Agregar**.

   El sistema realiza una validación y se asegura de que la cabina de almacenamiento y el servidor LDAP pueden comunicarse. Si aparece un mensaje de error, compruebe las credenciales que introdujo en el cuadro de diálogo y vuelva a introducir la información, de ser necesario.

Editar ajustes y asignaciones de roles del servidor de directorios

Si anteriormente configuró un servidor de directorio en Access Management, es posible cambiar sus ajustes en cualquier momento. Entre estos ajustes se encuentran la información de conexión del servidor y las asignaciones de grupos a roles.

Antes de empezar

- Debe iniciar sesión con un perfil de usuario que cuente con permisos de administración de seguridad. De lo contrario, no se mostrarán las funciones de Access Management.
- Debe definirse un servidor de directorio.

Pasos

1. Seleccione **Access Management**.
2. Seleccione la ficha **Servicios de directorio**.
3. Si se define más de un servidor, seleccione el servidor que desea editar en la tabla.
4. Seleccione **Ver/editar configuración**.

   Se abre el cuadro de diálogo Configuración del servidor de directorio.

5. En la ficha **Configuración del servidor**, cambie la configuración deseada.

Detalles del campo

Ajuste	Descripción
Ajustes de configuración	Dominios
Los nombres de dominio de los servidores LDAP. Si desea introducir varios dominios, escríbalos en una lista separada por comas. El nombre de dominio se utiliza en el inicio de sesión (*username@domain*) para especificar con qué servidor de directorio debe realizarse la autenticación.	URL del servidor
La URL para acceder al servidor LDAP con el formato de `ldap[s]://host:port`.	Enlazar cuenta (opcional)
La cuenta de usuario de solo lectura para realizar consultas en el servidor LDAP y buscar dentro de grupo.	Enlazar contraseña (opcional)
La contraseña de la cuenta vinculada. (Este campo se muestra cuando se introduce una cuenta vinculada.)	Probar conexión del servidor antes de guardar

Ajuste	Descripción
Comprueba que el sistema pueda comunicarse con la configuración del servidor LDAP. La prueba se produce después de hacer clic en **Guardar**. Si se selecciona esta casilla de comprobación y la prueba falla, no se modifica la configuración. Debe resolver el error o desmarcar la casilla de comprobación para omitir la prueba y volver a editar la configuración.	**Configuración de privilegios**
DN base de búsqueda	El contexto de LDAP para buscar usuarios, normalmente en la forma de `CN=Users, DC=cpoc, DC=local`.
Atributo de nombre de usuario	El atributo que está vinculado al ID de usuario para la autenticación. Por ejemplo: `sAMAccountName`.
Atributos de grupo	Lista de atributos de grupo en el usuario, que se utiliza para la asignación de grupos a roles. Por ejemplo: `memberOf, managedObjects`.

6. En la ficha **asignación de roles**, cambie la asignación deseada.

Detalles del campo

Ajuste	Descripción
Asignaciones	DN de grupo
El nombre de dominio para asignar el grupo de usuarios LDAP. Se admiten expresiones regulares. Estos caracteres especiales de expresión regular deben escaparse con una barra invertida (\) si no forman parte de un patrón de expresión regular: \.[]{}()<>*+-=	Funciones

El rol de supervisión se requiere para todos los usuarios, incluido el administrador.

7. Si lo desea, haga clic en **Agregar otra asignación** para introducir más asignaciones de grupo a rol.
8. Haga clic en **Guardar**.

Resultados

Una vez finalizada esta tarea, se finalizarán todas las sesiones de usuario activas. Solo se mantiene la sesión de usuario actual.

Quitar un servidor de directorio

Para interrumpir la conexión entre un servidor de directorio y el proxy de servicios web, es posible quitar la información del servidor de la página Access Management. Se recomienda ejecutar esta tarea si se configuró un servidor nuevo y se desea eliminar el anterior.

Antes de empezar

Debe iniciar sesión con un perfil de usuario que cuente con permisos de administración de seguridad. De lo contrario, no se mostrarán las funciones de Access Management.

Acerca de esta tarea

Una vez finalizada esta tarea, se finalizarán todas las sesiones de usuario activas. Solo se mantiene la sesión de usuario actual.

Pasos

1. Seleccione **Access Management**.
2. Seleccione la ficha **Servicios de directorio**.

3. Seleccione el servidor de directorio que desea eliminar de la lista.
4. Haga clic en **Quitar**.

   Se abrirá el cuadro de diálogo Quitar servidor de directorio.

5. Tipo `remove` En el campo y, a continuación, haga clic en **Quitar**.

   Se eliminará la configuración del servidor de directorio, la configuración de privilegios y las asignaciones de roles. Los usuarios ya no podrán iniciar sesión con las credenciales de este servidor.

Use SAML

Configure SAML

Para configurar la autenticación de Access Management, puede usar las funcionalidades de lenguaje de marcado de aserción de seguridad (SAML) que están integradas en la cabina de almacenamiento. Esta configuración establece una conexión entre un proveedor de identidades y el proveedor de almacenamiento.

Antes de empezar

- Debe iniciar sesión con un perfil de usuario que cuente con permisos de administración de seguridad. De lo contrario, no se mostrarán las funciones de Access Management.
- Debe conocer la dirección IP o el nombre de dominio de la controladora de la cabina de almacenamiento.
- Un administrador de IDP configuró un sistema IDP.
- Un administrador de IDP comprobó que el IDP admite la capacidad para obtener un ID de nombre en el momento de la autenticación.
- Un administrador comprobó que el reloj del servidor de IdP y de la controladora está sincronizado (ya sea mediante un servidor NTP o mediante el ajuste de la configuración del reloj de la controladora).
- Se descargó un archivo de metadatos de IdP del sistema de IdP y ese archivo está disponible en el sistema local que se usa para acceder a Unified Manager.

Acerca de esta tarea

Un proveedor de identidades (IDP) es un sistema externo que se usa para solicitar credenciales a un usuario y para determinar si el usuario se autentica correctamente. El IDP se puede configurar para ofrecer autenticación multifactor y para usar cualquier base de datos de usuario, como Active Directory. El equipo de seguridad es responsable de mantener el IDP. Un proveedor de servicios (SP) es un sistema que controla la autenticación y el acceso de usuario. Cuando se configura Access Management con SAML, la cabina de almacenamiento actúa como proveedor de servicios, ya que solicita la autenticación del proveedor de identidades. Para establecer una conexión entre el IDP y la cabina de almacenamiento, se deben compartir archivos de metadatos entre estas dos entidades. A continuación, se deben asignar las entidades de usuario de IDP con los roles de la cabina de almacenamiento. Y, finalmente, se debe probar la conexión y los inicios de sesión SSO antes de habilitar SAML.

SAML y Directory Services. Si SAML se habilita cuando Directory Services está configurado como método de autenticación, SAML sustituye a Directory Services en Unified Manager. Si se deshabilita SAML posteriormente, la configuración de Directory Services se establece en los valores anteriores.

Edición y desactivación. una vez que SAML está habilitado, *no puede* desactivarlo a través de la interfaz de usuario, ni puede editar la configuración de IDP. Si necesita deshabilitar o editar la configuración de SAML, comuníquese con el soporte técnico para obtener ayuda.

La configuración de la autenticación SAML es un procedimiento de varios pasos.

Paso 1: Cargue el archivo de metadatos de IDP

Para brindar información de conexión de IdP a la cabina de almacenamiento, se deben importar los metadatos de IdP en Unified Manager. El sistema IDP necesita los metadatos para redirigir las solicitudes de autenticación a la URL correcta y validar las respuestas recibidas.

Pasos

1. Seleccione MENU:Settings[Access Management].
2. Seleccione la pestaña **SAML**.

   La página muestra información general de los pasos de configuración.

3. Haga clic en el enlace **Import Identity Provider (IDP) file**.

   Se abre el cuadro de diálogo Importar archivo del proveedor de identidades.

4. Haga clic en **examinar** para seleccionar y cargar el archivo de metadatos IDP que copió en el sistema local.

   Una vez seleccionado el archivo, se muestra el ID de entidad IDP.

5. Haga clic en **Importar**.

Paso 2: Exporte los archivos del proveedor de servicios

Para establecer una relación de confianza entre IDP y la cabina de almacenamiento, se deben importar los metadatos del proveedor de servicios en IDP. IDP necesita estos metadatos para establecer una relación de confianza con la controladora y procesar las solicitudes de autorización. El archivo incluye información, como el nombre de dominio de la controladora o la dirección IP, por lo que IDP se puede comunicar con los proveedores de servicios.

Pasos

1. Haga clic en el enlace **Exportar archivos del proveedor de servicios**.

   Se abre el cuadro de diálogo Exportar archivos del proveedor de servicios.

2. Introduzca la dirección IP del controlador o el nombre DNS en el campo **controladora A** y, a continuación, haga clic en **Exportar** para guardar el archivo de metadatos en el sistema local.

   Después de hacer clic en **Exportar**, los metadatos del proveedor de servicios se descargan en el sistema local. Anote en qué lugar se almacena el archivo.

3. Desde el sistema local, busque el archivo de metadatos del proveedor de servicios con formato XML que exportó.
4. Desde el servidor IdP, importe el archivo de metadatos del proveedor de servicios para establecer la relación de confianza. Es posible importar el archivo directamente o bien introducir manualmente la información de la controladora desde el archivo.

Paso 3: Asignar roles

Para proporcionar autorización y acceso a Unified Manager a los usuarios, se deben asignar los atributos de usuario IdP y las membresías de grupo a los roles predefinidos de la cabina de almacenamiento.

Antes de empezar

- Un administrador IDP configuró los atributos del usuario y la pertenencia al grupo en el sistema IDP.
- Se importó el archivo de metadatos de IdP a Unified Manager.
- Para la relación de confianza, se importó un archivo de metadatos del proveedor de servicios para la controladora en el sistema IdP.

Pasos

1. Haga clic en el enlace para **mapping Unified Manager** roles.

   Se abre el cuadro de diálogo asignación de roles.

2. Asigne los grupos y atributos de usuario IDP a los roles predefinidos. Un grupo puede tener varios roles asignados.

   Detalles del campo

Ajuste	Descripción
Asignaciones	Atributo de usuario
Especifique un atributo (por ejemplo, "miembro de") para el grupo SAML que será asignado.	Valor de atributo
Especifique el valor de atributo para el grupo que será asignado. Se admiten expresiones regulares. Estos caracteres especiales de expresión regular deben escaparse con una barra invertida (\) si no forman parte de un patrón de expresión regular: \.[]{}()<>*+-=	Funciones

   El rol de supervisión se requiere para todos los usuarios, incluido el administrador. Unified Manager no funcionará correctamente para los usuarios que no tengan el rol de supervisión.

3. Si lo desea, haga clic en **Agregar otra asignación** para introducir más asignaciones de grupo a rol.

Es posible modificar las asignaciones de roles después de haber habilitado SAML.

4. Cuando termine de asignar, haga clic en **Guardar**.

Paso 4: Probar el inicio de sesión SSO

Para garantizar la comunicación entre el sistema IDP y la cabina de almacenamiento, de manera opcional, se puede probar un inicio de sesión SSO. Esa prueba también se puede llevar a cabo durante el paso final para habilitar SAML.

Antes de empezar

- Se importó el archivo de metadatos de IdP a Unified Manager.
- Para la relación de confianza, se importó un archivo de metadatos del proveedor de servicios para la controladora en el sistema IdP.

Pasos

1. Seleccione el enlace **probar inicio de sesión SSO**.

   Se abre un cuadro de diálogo para introducir las credenciales de SSO.

2. Introduzca las credenciales de inicio de sesión para un usuario, tanto con permisos de administración de seguridad como de supervisión.

   Se abre un cuadro de diálogo mientras el sistema prueba el inicio de sesión.

3. Busque el mensaje Test Successful. Si el análisis se realiza correctamente, vaya al siguiente paso para habilitar SAML.

   Si el análisis no se realiza correctamente, se muestra un mensaje de error con más información. Asegúrese de que:

   - El usuario pertenezca a un grupo con permisos de administración de seguridad y supervisión.
   - Los metadatos cargados para el servidor IDP sean correctos.
   - La dirección de la controladora en los archivos de metadatos de SP sea correcta.

Paso 5: Habilite SAML

El paso final es completar la configuración de SAML para la autenticación de usuarios. Durante este proceso, el sistema también le indica que pruebe un inicio de sesión SSO. El proceso de prueba de inicio de sesión con SSO se describe en el paso anterior.

Antes de empezar

- Se importó el archivo de metadatos de IdP a Unified Manager.
- Para la relación de confianza, se importó un archivo de metadatos del proveedor de servicios para la controladora en el sistema IdP.
- Se debe configurar al menos una asignación de rol de administración de seguridad y una de rol de supervisión.

Edición y desactivación. una vez que SAML está habilitado, *no puede* desactivarlo a través de la interfaz de usuario, ni puede editar la configuración de IDP. Si necesita deshabilitar o editar la configuración de SAML, comuníquese con el soporte técnico para obtener ayuda.

Pasos

1. En la ficha **SAML**, seleccione el enlace **Habilitar SAML**.

   Se abre el cuadro de diálogo Confirmar acción de habilitar SAML.

2. Tipo `enable`Y, a continuación, haga clic en **Activar**.
3. Introduzca las credenciales de usuario para llevar a cabo una prueba de inicio de sesión SSO.

Resultados

Una vez que el sistema habilita SAML, se cierran todas las sesiones activas y se inicia la autenticación de usuarios a través de SAML.

Cambiar las asignaciones de roles SAML

Si anteriormente configuró SAML para Access Management, puede cambiar las asignaciones de roles entre los grupos IDP y los roles predefinidos de la cabina de almacenamiento.

Antes de empezar

- Debe iniciar sesión con un perfil de usuario que cuente con permisos de administración de seguridad. De lo contrario, no se mostrarán las funciones de Access Management.
- Un administrador IDP configuró los atributos del usuario y la pertenencia al grupo en el sistema IDP.
- SAML debe estar configurado y habilitado.

Pasos

1. Seleccione MENU:Settings[Access Management].
2. Seleccione la pestaña **SAML**.
3. Seleccione **asignación de roles**.

   Se abre el cuadro de diálogo asignación de roles.

4. Asigne los grupos y atributos de usuario IDP a los roles predefinidos. Un grupo puede tener varios roles asignados.

   Tenga cuidado de no quitar los permisos mientras SAML está habilitado; de lo contrario, perderá el acceso a Unified Manager.

Detalles del campo

Ajuste	Descripción
Asignaciones	Atributo de usuario
Especifique un atributo (por ejemplo, "miembro de") para el grupo SAML que será asignado.	Valor de atributo
Especifique el valor de atributo para el grupo que será asignado.	Funciones

El rol de supervisión se requiere para todos los usuarios, incluido el administrador. Unified Manager no funcionará correctamente para los usuarios que no tengan el rol de supervisión.

5. Opcionalmente, haga clic en **Agregar otra asignación** para introducir más asignaciones de grupo a rol.
6. Haga clic en **Guardar**.

Resultados

Una vez finalizada esta tarea, se finalizarán todas las sesiones de usuario activas. Solo se mantiene la sesión de usuario actual.

Exporte los archivos de proveedor de servicios SAML

Si es necesario, se pueden exportar metadatos de proveedor de servicios para la cabina de almacenamiento y volver a importar el archivo en el sistema del proveedor de identidades (IdP).

Antes de empezar

- Debe iniciar sesión con un perfil de usuario que cuente con permisos de administración de seguridad. De lo contrario, no se mostrarán las funciones de Access Management.
- SAML debe estar configurado y habilitado.

Acerca de esta tarea

En esta tarea, se exportan metadatos de la controladora. IDP necesita estos metadatos para establecer una relación de confianza con la controladora y procesar solicitudes de autenticación. El archivo incluye información, como el nombre de dominio o la dirección IP de la controladora, que IDP puede usar para enviar solicitudes.

Pasos

1. Seleccione MENU:Settings[Access Management].
2. Seleccione la pestaña **SAML**.

3. Seleccione **Exportar**.

   Se abre el cuadro de diálogo Exportar archivos del proveedor de servicios.

4. Haga clic en **Exportar** para guardar el archivo de metadatos en su sistema local.

   El campo de nombre de dominio es de sólo lectura.

   Anote en qué lugar se almacena el archivo.

5. Desde el sistema local, busque el archivo de metadatos del proveedor de servicios con formato XML que exportó.
6. Desde el servidor IdP, importe el archivo de metadatos del proveedor de servicios. Es posible importar el archivo directamente o introducir manualmente la información de la controladora.
7. Haga clic en **Cerrar**.

Preguntas frecuentes

¿Por qué no puedo iniciar sesión?

Si recibe un error al intentar iniciar sesión, revise estas causas posibles.

Los errores de inicio de sesión pueden ocurrir por uno de estos motivos:

- Introdujo un nombre de usuario o contraseña incorrectos.
- No tiene privilegios suficientes.
- Intentó iniciar sesión reiteradamente sin éxito y se activó el modo de bloqueo. Aguarde 10 minutos y vuelva a intentarlo.
- La autenticación SAML está habilitada. Actualice el explorador para iniciar sesión.

¿Qué debo saber antes de añadir un servidor de directorio?

Antes de añadir un servidor de directorio en Access Management, debe cumplir ciertos requisitos.

- Debe haber grupos de usuarios definidos en el servicio de directorio.
- Deben estar disponibles las credenciales del servidor LDAP, incluidos el nombre de dominio y la URL del servidor y, de manera opcional, el nombre de usuario y la contraseña de la cuenta de enlace.
- En el caso de los servidores LDAPS que utilizan un protocolo seguro, se debe instalar la cadena de certificados del servidor LDAP en la máquina local.

¿Qué debo saber acerca de la asignación de roles de la cabina de almacenamiento?

Antes de asignar grupos a roles, revise las directrices.

Las funcionalidades de RBAC incluyen los siguientes roles:

- **Storage admin** — acceso completo de lectura/escritura a los objetos de almacenamiento de las matrices, pero sin acceso a la configuración de seguridad.

- **Security admin** — acceso a la configuración de seguridad en Access Management y Certificate Management.
- **Support admin** — acceso a todos los recursos de hardware en matrices de almacenamiento, datos de fallos y eventos MEL. No brinda acceso a los objetos de almacenamiento ni a la configuración de seguridad.
- **Monitor** — acceso de sólo lectura a todos los objetos de almacenamiento, pero sin acceso a la configuración de seguridad.

El rol de supervisión se requiere para todos los usuarios, incluido el administrador.

Si usa un servidor de protocolo ligero de acceso a directorios (LDAP) y servicios de directorio, asegúrese de que:

- Un administrador haya definido grupos de usuarios en el servicio de directorio.
- Conoce los nombres de dominio de los grupos de usuarios LDAP.

SAML

Si usa las funcionalidades de lenguaje de marcado de aserción de seguridad (SAML) incorporadas en la cabina de almacenamiento, asegúrese de que:

- Un administrador de proveedor de identidades (IDP) haya configurado atributos de usuario y pertenencia a grupos en el sistema del IDP.
- Conoce los nombres de pertenencia a grupos.
- Conoce el valor de atributo para el grupo que será asignado. Se admiten expresiones regulares. Estos caracteres especiales de expresión regular deben escaparse con una barra invertida (\) si no forman parte de un patrón de expresión regular:

```
\.[]{}()<>*+-=!?^$|
```

- El rol de supervisión se requiere para todos los usuarios, incluido el administrador. Unified Manager no funcionará correctamente para los usuarios que no tengan el rol de supervisión.

¿Qué debo saber antes de configurar y habilitar SAML?

Antes de configurar y habilitar las funcionalidades de lenguaje de marcado de aserción de seguridad (SAML) para la autenticación, asegúrese de cumplir con los siguientes requisitos y comprender las restricciones de SAML.

Requisitos

Antes de comenzar, compruebe lo siguiente:

- Se configuró un proveedor de identidades (IDP) en la red. Un IDP es un sistema externo que se usa para solicitar credenciales a un usuario y determinar si el usuario se autentica correctamente. El equipo de seguridad es responsable de mantener el IDP.
- Un administrador IDP configuró los atributos y los grupos del usuario en el sistema IDP.
- Un administrador de IDP comprobó que el IDP admite la capacidad para obtener un ID de nombre en el momento de la autenticación.

- Un administrador comprobó que el reloj del servidor de IdP y de la controladora está sincronizado (ya sea mediante un servidor NTP o mediante el ajuste de la configuración del reloj de la controladora).
- Se descargó un archivo de metadatos de IdP del sistema de IdP y ese archivo está disponible en el sistema local que se usa para acceder a Unified Manager.
- Conoce la dirección IP o el nombre de dominio de la controladora de la cabina de almacenamiento.

Restricciones

Además de los requisitos mencionados más arriba, asegúrese de comprender las siguientes restricciones:

- Una vez que se habilita SAML, _no se puede deshabilitar desde la interfaz de usuario, tampoco se puede editar desde la configuración de IDP. Si necesita deshabilitar o editar la configuración de SAML, comuníquese con el soporte técnico para obtener ayuda. Se recomienda que pruebe los inicios de sesión SSO para poder habilitar SAML en el paso final de la configuración. (El sistema también hace una prueba de inicio de sesión SSO antes de habilitar SAML.)
- Si deshabilita SAML en el futuro, el sistema restaura automáticamente la configuración anterior (local User roles o Directory Services).
- Si Directory Services está actualmente configurado para la autenticación de usuario, SAML anula esa configuración.
- Cuando se configura SAML, los siguientes clientes no pueden acceder a los recursos de la cabina de almacenamiento:
  - Enterprise Management Window (EMW)
  - Interfaz de línea de comandos (CLI)
  - Clientes de kits de desarrollo de software (SDK)
  - Clientes en banda
  - Clientes HTTP de la API de REST de autenticación básica
  - Inicio de sesión mediante extremo estándar de la API de REST

¿De qué se tratan los usuarios locales?

Los usuarios locales están predefinidos en el sistema e incluyen permisos específicos.

Entre ellos, se incluyen:

- **Admin** — Super administrador que tiene acceso a todas las funciones del sistema. Este usuario incluye todos los roles. La contraseña se debe establecer en el primer inicio de sesión.
- **Almacenamiento** — el administrador responsable de todo el aprovisionamiento de almacenamiento. Este usuario incluye los siguientes roles: Administrador de almacenamiento, administrador de soporte y Supervisión. Esta cuenta está deshabilitada hasta que se defina una contraseña.
- **Security**: El usuario responsable de la configuración de seguridad, incluidos Access Management y Certificate Management. Este usuario incluye los siguientes roles: Administrador de seguridad y Supervisión. Esta cuenta está deshabilitada hasta que se defina una contraseña.
- **Soporte**: El usuario responsable de recursos de hardware, datos de fallos y actualizaciones de firmware. Este usuario incluye los siguientes roles: Administrador de soporte y Supervisión. Esta cuenta está deshabilitada hasta que se defina una contraseña.
- **Monitor** — un usuario con acceso de sólo lectura al sistema. Este usuario incluye únicamente el rol Supervisión. Esta cuenta está deshabilitada hasta que se defina una contraseña.

- **rw** (lectura/escritura): Este usuario incluye los siguientes roles: Administrador de almacenamiento, administrador de soporte y monitor. Esta cuenta está deshabilitada hasta que se defina una contraseña.
- **Ro** (sólo lectura) — este usuario incluye sólo la función Monitor. Esta cuenta está deshabilitada hasta que se defina una contraseña.