



Puesta en marcha y actualización

VSC, VASA Provider, and SRA 9.7

NetApp
March 21, 2024

This PDF was generated from <https://docs.netapp.com/es-es/vsc-vasa-provider-sra-97/deploy/concept-virtual-storage-console-overview.html> on March 21, 2024. Always check docs.netapp.com for the latest.

Tabla de contenidos

- Puesta en marcha y actualización 1
 - Información general del dispositivo virtual para VSC, proveedor VASA y SRA 1
 - Flujo de trabajo de puesta en marcha para nuevos usuarios de VSC, proveedores VASA y dispositivos virtuales SRA 2
 - Requisitos para poner en marcha el dispositivo virtual para VSC, proveedor VASA y SRA 5
 - Ponga en marcha o actualice VSC, proveedor VASA y SRA 10
 - Configure el entorno de Virtual Storage Console para VMware vSphere 21
 - Configure el entorno del sistema de almacenamiento de Virtual Storage Console para VMware vSphere . 35
 - Funciones de control de acceso basado en roles de vCenter Server en VSC para VMware vSphere 39
 - Configure Storage Replication Adapter para la recuperación ante desastres 50
 - Solucione problemas con el dispositivo virtual para VSC, proveedor VASA y SRA 52

Puesta en marcha y actualización

Información general del dispositivo virtual para VSC, proveedor VASA y SRA

El dispositivo virtual para Virtual Storage Console (VSC), el proveedor VASA y el adaptador de replicación de almacenamiento (SRA) proporciona gestión integral del ciclo de vida de las máquinas virtuales en entornos de VMware que usan los sistemas de almacenamiento de NetApp. Simplifica el almacenamiento y la gestión de datos en entornos VMware al permitir que los administradores gestionen directamente el almacenamiento en vCenter Server.

Con vSphere 6.5, VMware presentó un nuevo cliente basado en HTML5 llamado vSphere Client. La versión 9.6 del dispositivo virtual para VSC, proveedor VASA y SRA solo admite vSphere Client. El dispositivo virtual para VSC, VASA Provider y SRA se integra con vSphere Client y permite utilizar servicios de inicio de sesión único (SSO). En un entorno con varias instancias de vCenter Server, cada instancia de vCenter Server que desea gestionar debe tener su propia instancia registrada de VSC.

Cada componente del dispositivo virtual para VSC, proveedor VASA y SRA proporciona funcionalidades para ayudar a gestionar el almacenamiento de forma más eficiente.

Virtual Storage Console (VSC)

VSC le permite realizar las siguientes tareas:

- Añada controladoras de almacenamiento, asigne credenciales y configure permisos para las controladoras de almacenamiento a VSC que tanto el proveedor de SRA como VASA puedan aprovechar
- Aprovechone los almacenes de datos
- Supervise el rendimiento de los almacenes de datos y las máquinas virtuales en el entorno vCenter Server
- Controle el acceso del administrador a los objetos de vCenter Server mediante el control de acceso basado en roles (RBAC) en dos niveles:
 - Objetos de vSphere, como máquinas virtuales y almacenes de datos

Estos objetos se gestionan mediante el control de acceso basado en roles de vCenter Server.

- Y el almacenamiento de ONTAP

Los sistemas de almacenamiento se gestionan mediante RBAC de ONTAP.

- Consulte y actualice la configuración del host de los hosts ESXi conectados al almacenamiento

Las operaciones de aprovisionamiento de VSC se benefician de usar el plugin de NFS para VMware vStorage APIs for Array Integration (VAAI). El plugin de NFS para VAAI es una biblioteca de software que integra las bibliotecas de discos virtuales de VMware que están instaladas en el host ESXi. El paquete VAAI de VMware permite descargar determinadas tareas de los hosts físicos a la cabina de almacenamiento. Puede realizar tareas como thin provisioning y la aceleración de hardware en el nivel de cabina para reducir la carga de trabajo en los hosts ESXi. La función de copia de liberación de sobrecarga y reserva de espacio mejoran el rendimiento de las operaciones de VSC.

El plugin de NetApp NFS para VAAI no se envía con VSC. Sin embargo, puede descargar el paquete de

instalación del plug-in y obtener las instrucciones para instalar el plug-in desde la .

Proveedor de VASA

VASA Provider para ONTAP usa las API VMware vSphere para el reconocimiento del almacenamiento (VASA) para enviar información sobre el almacenamiento que utiliza VMware vSphere al vCenter Server. El dispositivo virtual para VSC, proveedor VASA y SRA, VASA Provider se integra con VSC y VASA Provider le permite realizar las siguientes tareas:

- Aprovechne los almacenes de datos de VMware Virtual Volumes (vVols)
- Cree y utilice perfiles de capacidades de almacenamiento que definan diferentes objetivos de nivel de servicio (SLO) de almacenamiento para su entorno
- Compruebe que cumple las normativas entre los almacenes de datos y los perfiles de funcionalidad de almacenamiento
- Configure las alarmas para que le avise cuando los volúmenes y agregados se aproximen a los límites del umbral
- Supervise el rendimiento de los discos de máquinas virtuales (VMDK) y las máquinas virtuales que se crean en los almacenes de datos vVols

Si utiliza ONTAP 9.6 o una versión anterior, el proveedor de VASA se comunica con el servidor de vCenter mediante las API de VASA y se comunica con ONTAP mediante las API llamadas ZAPI. Para ver la consola de VVol de ONTAP 9.6 y versiones anteriores, debe haber instalado y registrado en vCenter Server. Si utiliza ONTAP 9.7, no es necesario que se registre en el proveedor de VASA para ver la consola de VVol.



Para ONTAP 9.6 y versiones anteriores, VASA Provider requiere una instancia dedicada de servicios API de OnCommand. Una instancia de los servicios de API de OnCommand no se puede compartir con varias instancias de proveedor VASA.

Adaptador de replicación de almacenamiento (SRA)

Cuando se habilita el SRA y se usa junto con VMware Site Recovery Manager (SRM), es posible recuperar los almacenes de datos y las máquinas virtuales de vCenter Server en caso de fallo. El SRA permite configurar sitios protegidos y sitios de recuperación en el entorno para garantizar la recuperación ante desastres en caso de que se produzca un fallo.

Información relacionada

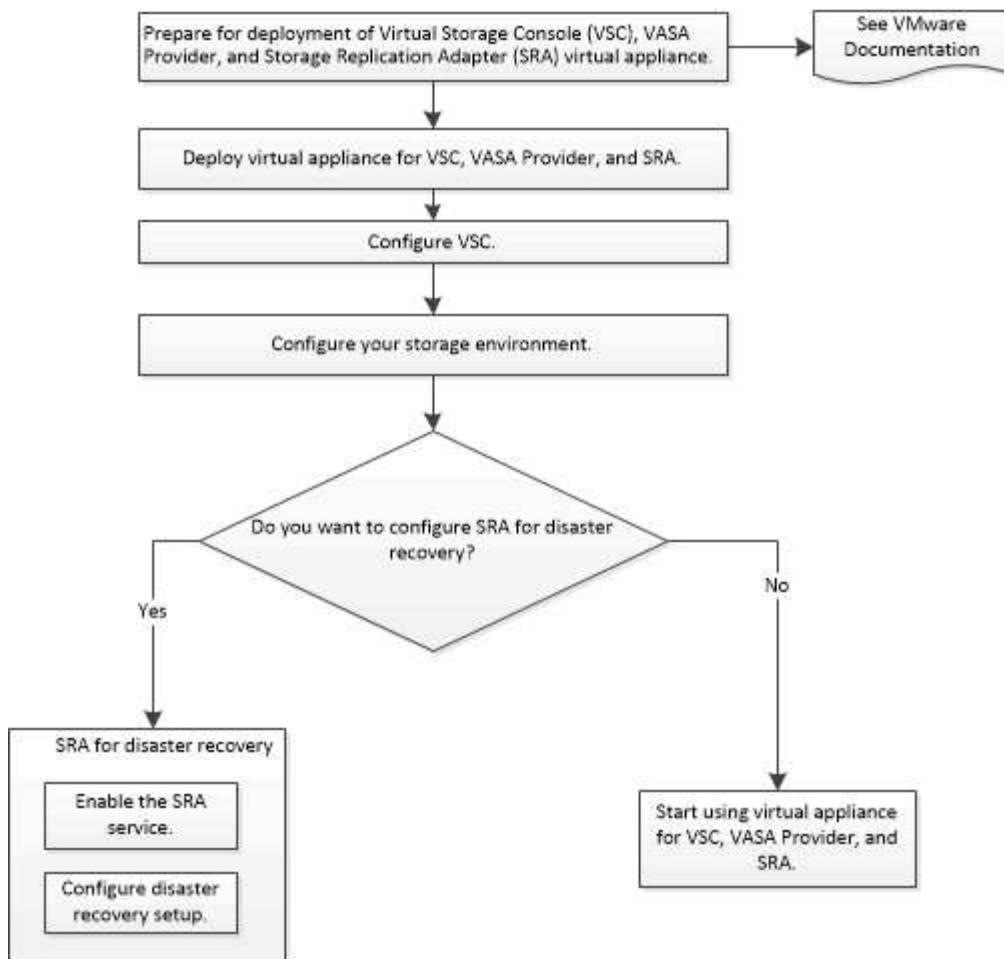
["Documentación de NetApp: Servicios de API de OnCommand"](#)

["Documentación de NetApp: Plugin de NetApp NFS para VMware VAAI"](#)

["Soporte de NetApp"](#)

Flujo de trabajo de puesta en marcha para nuevos usuarios de VSC, proveedores VASA y dispositivos virtuales SRA

Si es nuevo en VMware y nunca utilizó un producto VSC de NetApp, debe configurar el vCenter Server y configurar un host ESXi, antes de poner en marcha y configurar el dispositivo virtual para VSC, proveedor VASA y SRA.



Flujo de trabajo de puesta en marcha para los usuarios existentes de VSC, proveedores VASA y SRA

Las versiones 9.7 del dispositivo virtual para VSC, proveedores VASA y SRA admiten actualización directa a la versión más reciente.

Las versiones anteriores de aplicaciones individuales como VSC, proveedores VASA y SRA usan un proceso de actualización diferente. Si tiene instalado VSC o VASA Provider o SRA en la configuración, debe realizar las siguientes operaciones:

1. Ponga en marcha la versión más reciente del dispositivo virtual para VSC, proveedor VASA y SRA.
2. Migre los datos de configuración existentes.

Los datos de configuración incluyen las credenciales del sistema de almacenamiento, así como las preferencias que se encuentran en `kaminoprefs.xml` y `vscPreferences.xml` archivos.

"Configure los archivos de preferencias de VSC"

En muchos casos, es posible que no sea necesario migrar datos de configuración. Sin embargo, si ha personalizado anteriormente los archivos de preferencias, quizás desee revisarlos y realizar cambios similares en el dispositivo virtual recién implementado. Puede realizar una de las siguientes acciones:

- Uso ["Import Utility para SnapCenter y Virtual Storage Console"](#) Para migrar las credenciales del sistema de almacenamiento de VSC 6.X y SRA 4.X a la nueva implementación.

- Añada los sistemas de almacenamiento al dispositivo virtual recién implementado y especifique las credenciales a medida que las añada.

Si va a actualizar desde VASA Provider 6.X, debe cancelar el registro del proveedor VASA antes de la actualización. Consulte la documentación de su versión actual para obtener más detalles.

Si también va a actualizar desde SRA 4.0 o una versión anterior:

- Si utiliza SRA 4.0P1, primero debe actualizar a SRA9.6 y solo entonces puede realizar una actualización in situ de SRA 9.6 a la última versión.

["Actualice al dispositivo virtual 9.7.1 para VSC, proveedor VASA y SRA"](#)

- Si utiliza SRA 2.1 o 3.0, primero debe tomar nota de los detalles de configuración del sitio existente.

Guía de instalación y configuración del adaptador de replicación de almacenamiento 4.0 para ONTAP contiene las instrucciones detalladas en la sección "Descripción general de la actualización". Estas versiones de SRA también usan el proveedor VASA, de modo que debe anular el registro del proveedor VASA y, a continuación, poner en marcha la versión más reciente del dispositivo virtual para VSC, proveedor VASA y SRA. La versión anterior del servidor (.ova) se puede quitar cuando la actualización se haya completado.

Para cualquier actualización del SRA, el software del SRA (el adaptador del servidor del Site Recovery Manager, instalado por el .msi Archivo) debe eliminarse del servidor de Site Recovery Manager. Puede utilizar el panel de control del sistema de Windows para desinstalar el software y, a continuación, instalar el software del SRA más reciente en el servidor SRA mediante el .msi archivo.

Si tiene la puesta en marcha del proveedor de VASA, después de la actualización desde la configuración existente, debe configurar el tamaño de la memoria para que el dispositivo virtual sea de 12 GB con el `Edit Settings` opción. También debe modificar la reserva de memoria virtual. La máquina virtual debe estar apagada para modificar el tamaño de la memoria.

El dispositivo virtual para VSC, proveedor VASA y SRA no admite una actualización directa de cualquier versión anterior a la versión 9.7 a 9.7P2 o posterior. Primero debe actualizar la configuración existente a la versión 9.7 del dispositivo virtual para VSC, proveedor VASA y SRA antes de actualizar a cualquier versión posterior.

Si va a poner en marcha la versión más reciente del dispositivo virtual, debe ver el tema «requisitos para poner en marcha el dispositivo virtual para VSC, proveedor VASA y SRA». El tema «Actualizar a la versión 9.6 del dispositivo virtual para VSC, proveedores VASA y SRA» tiene información sobre cómo realizar una actualización in situ.

Información relacionada

["Toolchest de NetApp: Utilidad de importación para SnapCenter y Virtual Storage Console"](#)

["Requisitos para poner en marcha el dispositivo virtual para VSC, proveedor VASA y SRA"](#)

["Actualice al dispositivo virtual 9.7.1 para VSC, proveedor VASA y SRA"](#)

Requisitos para poner en marcha el dispositivo virtual para VSC, proveedor VASA y SRA

Debe conocer los requisitos de implementación antes de implementar el dispositivo virtual para Virtual Storage Console (VSC), el proveedor VASA y el adaptador de replicación de almacenamiento (SRA), y debe decidir las tareas que desea realizar. Según sus tareas, puede elegir el modelo de puesta en marcha para poner en marcha el dispositivo virtual para VSC, proveedor VASA y SRA.

Requisitos de puertos para VSC

De forma predeterminada, (VSC) utiliza puertos designados para habilitar la comunicación entre sus componentes, incluidos los sistemas de almacenamiento y VMware vCenter Server. Si tiene firewalls habilitados, debe asegurarse de que los firewalls están configurados para permitir excepciones.

Para firewalls diferentes de Windows, debe otorgar acceso manualmente a puertos específicos que utiliza VSC. Si no concede acceso a estos puertos, aparecerá un mensaje de error como el siguiente.

No se puede comunicar con el servidor

VSC utiliza los siguientes puertos TCP bidireccionales predeterminados:

Número de puerto predeterminado	Descripción
9083	Cuando se encuentra habilitada, tanto el proveedor VASA como el adaptador de replicación de almacenamiento (SRA) utilizan este puerto para comunicarse con vCenter Server. Este puerto también es necesario para obtener los ajustes de TCP/IP.
443	Según la forma en que haya configurado sus credenciales, VMware vCenter Server y los sistemas de almacenamiento escuchan las comunicaciones seguras en este puerto.
8143	VSC escucha comunicaciones seguras en este puerto.
7	VSC envía una solicitud de eco a ONTAP para verificar la accesibilidad, y solo es necesario cuando se añade un sistema de almacenamiento y se puede deshabilitar más adelante.

Debe haber habilitado el protocolo de mensajes de control de Internet (ICMP) antes de implementar el dispositivo virtual para VSC, proveedor VASA y SRA.



Si ICMP está deshabilitado, produce un error en la configuración inicial del dispositivo virtual para VSC, proveedor VASA y SRA, y VSC no puede iniciar los servicios de VSC y proveedor VASA después de la implementación. Es necesario habilitar manualmente los servicios de VSC y proveedor VASA después de la implementación.

Requisitos de espacio y tamaño del dispositivo virtual para VSC, proveedor VASA y SRA

Antes de implementar el dispositivo virtual para Virtual Storage Console (VSC), el proveedor VASA y el adaptador de replicación de almacenamiento (SRA), debe conocer los requisitos de espacio del paquete de implementación y algunos requisitos básicos del sistema host.

- **Requisitos de espacio del paquete de instalación**
 - 2.1 GB para instalaciones con thin provisioning
 - 54.0 GB para instalaciones de Thick-Provisioning
- **Requisitos de dimensionamiento del sistema principal**
 - ESXi 6.5U2 o posterior
 - Memoria recomendada: 12 GB de RAM
 - CPU recomendadas: 2

Es compatible con el sistema de almacenamiento, las licencias y las aplicaciones para el dispositivo virtual para VSC, proveedor VASA y SRA

Debe conocer los requisitos básicos del sistema de almacenamiento, los requisitos de la aplicación y los requisitos de licencia antes de empezar a implementar el dispositivo virtual para Virtual Storage Console (VSC), el proveedor VASA y el adaptador de replicación de almacenamiento (SRA).

El (IMT) contiene la información más reciente sobre las versiones compatibles de ONTAP, vCenter Server, hosts ESXi, aplicaciones de plugins y Site Recovery Manager (SRM).

- ["Herramienta de matriz de interoperabilidad: VSC 9.7.1"](#)
- ["Herramienta de matriz de interoperabilidad: Proveedor DE VASA 9.7.1"](#)
- ["Herramienta de matriz de interoperabilidad: SRA 9.7.1"](#)

Debe habilitar la licencia de FlexClone para realizar operaciones de snapshots de máquina virtual y operaciones de clonado para almacenes de datos de VMware Virtual Volumes (vVols).

El adaptador de replicación de almacenamiento (SRA) requiere las siguientes licencias:

- Licencia de SnapMirror

Debe habilitar la licencia de SnapMirror para realizar operaciones de conmutación al nodo de respaldo para el SRA.

- Licencia de FlexClone

Debe habilitar la licencia de FlexClone para realizar operaciones de conmutación al nodo de respaldo de prueba para el SRA.

Para ver las IOPS de un almacén de datos, debe habilitar el control de I/o de almacenamiento o bien anular la selección de la casilla de comprobación Disable Storage I/o statistics Collection en la configuración de Storage I/o control. Solo puede habilitar el control de I/o de almacenamiento si tiene la licencia Enterprise Plus de VMware.

- ["Artículo de la base de conocimientos de VMware 1022091: Solución de problemas de Storage I/o Control"](#)
- ["Documentación de VMware vSphere: Requisitos de control de I/o de almacenamiento"](#)

Consideraciones y requisitos para implementar el dispositivo virtual para VSC, proveedor VASA y SRA

Antes de poner en marcha el dispositivo virtual para Virtual Storage Console (VSC), el proveedor VASA y el adaptador de replicación de almacenamiento (SRA), es recomendable planificar la implementación y decidir cómo desea configurar VSC, proveedor VASA y SRA en su entorno.

En la siguiente tabla, se presenta información general sobre lo que debe tener en cuenta antes de implementar el dispositivo virtual para VSC, proveedor VASA y SRA.

Consideraciones	Descripción
Puesta en marcha por primera vez del dispositivo virtual para VSC, proveedor VASA y SRA	<p>La puesta en marcha del dispositivo virtual para VSC, proveedor VASA y SRA instala automáticamente las funciones de VSC. "Poner en marcha o actualizar VSC, proveedor VASA y SRA"</p> <p>"Flujo de trabajo de puesta en marcha para nuevos usuarios de VSC, proveedores VASA y dispositivos virtuales SRA"</p>

Consideraciones	Descripción
Actualizar desde una puesta en marcha existente de VSC	<p>El procedimiento de actualización de una puesta en marcha existente de VSC en el dispositivo virtual para VSC, proveedor VASA y SRA depende de la versión de VSC y de si ha puesto en marcha VSC, proveedor VASA y SRA. La sección de flujos de trabajo de implementación y actualización contiene más información. "Flujo de trabajo de puesta en marcha para los usuarios existentes de VSC, proveedores VASA y SRA"</p> <p>Prácticas recomendadas antes de una actualización:</p> <ul style="list-style-type: none"> • Debe registrar información sobre los sistemas de almacenamiento que se están usando y sus credenciales. <p>Después de la actualización, debe verificar que todos los sistemas de almacenamiento se detectaron automáticamente y que tienen las credenciales correctas.</p> <ul style="list-style-type: none"> • Si modificó alguno de los roles estándar de VSC, debe copiar dichos roles para guardar los cambios. <p>VSC sobrescribe los roles estándar con los valores predeterminados actuales cada vez que reinicia el servicio VSC.</p>
Regeneración de un certificado SSL para VSC	<p>El certificado SSL se genera automáticamente cuando se pone en marcha el dispositivo virtual para VSC, proveedor VASA y SRA. Es posible que tenga que regenerar el certificado SSL para crear un certificado específico de sitio. "Regenere un certificado SSL para"</p>
Configuración de los valores del servidor ESXi	<p>Aunque la mayoría de los valores del servidor ESXi se establecen de forma predeterminada, es una buena práctica comprobar los valores. Estos valores se basan en pruebas internas. En función de su entorno, es posible que deba cambiar algunos de los valores para mejorar el rendimiento.</p> <ul style="list-style-type: none"> • "Configure los valores de multivía y de tiempo de espera del servidor ESXi" • "Los valores de host de ESXi se establecen mediante Virtual Storage Console para VMware vSphere"

Consideraciones	Descripción
Valores de tiempo de espera del sistema operativo invitado	Los scripts de tiempo de espera del sistema operativo invitado (SO invitado) configuran los valores de tiempo de espera de I/O SCSI para sistemas operativos invitados de Linux, Solaris y Windows compatibles con el fin de proporcionar una conducta de conmutación por error correcta.

En la siguiente tabla, se presenta información general sobre lo que es necesario configurar el dispositivo virtual para VSC, proveedor VASA y SRA.

Consideraciones	Descripción
Requisitos de control de acceso basado en roles (RBAC)	<p>VSC es compatible con el control de acceso basado en roles de vCenter Server y de ONTAP. La cuenta utilizada para registrar VSC en vCenter Server (mediante <code>https://<appliance_ip>:8143/Register.html</code>) Debe ser un administrador de vCenter Server (asignado al rol de administrador de vCenter Server o de administrador). Si piensa ejecutar VSC como administrador, debe tener todos los permisos y privilegios necesarios para todas las tareas.</p> <p>Si la empresa requiere que limite el acceso a objetos de vSphere, puede crear y asignar roles VSC estándar a los usuarios para que cumplan los requisitos de vCenter Server.</p> <p>Puede crear los roles de ONTAP recomendados mediante el Administrador del sistema de ONTAP mediante el archivo JSON proporcionado con el dispositivo virtual para VSC, proveedor VASA y SRA.</p> <p>Si un usuario intenta realizar una tarea sin los privilegios y permisos correctos, las opciones de la tarea aparecen atenuadas.</p> <ul style="list-style-type: none"> • "Roles estándar que se incluyen en el dispositivo virtual para VSC, proveedor VASA y SRA" • "Roles de ONTAP recomendados cuando se usa VSC para VMware vSphere"
Versión de ONTAP	Los sistemas de almacenamiento deben ejecutar ONTAP 9.1, 9.3, 9.5, 9.6 o 9.7.

Consideraciones	Descripción
Perfiles de funcionalidad de almacenamiento	<p>Para usar perfiles de funcionalidad de almacenamiento o configurar alarmas, es necesario habilitar VASA Provider para ONTAP. Después de habilitar VASA Provider, es posible configurar almacenes de datos de VMware Virtual Volumes (vVols), y se pueden crear y gestionar perfiles de capacidades de almacenamiento y alarmas.</p> <p>Las alarmas se avisan cuando un volumen o un agregado tienen una capacidad casi completa o cuando un almacén de datos ya no cumple con el perfil de la funcionalidad de almacenamiento asociada.</p>

Ponga en marcha o actualice VSC, proveedor VASA y SRA

Debe descargar y poner en marcha el dispositivo virtual para VSC, proveedor VASA y SRA en un entorno de VMware vSphere y, a continuación, configurar las aplicaciones necesarias en función de las tareas que desee realizar mediante VSC, proveedor VASA y SRAVSC, proveedor VASA y SRA.

Información relacionada

[Habilite VASA Provider para configurar almacenes de datos virtuales](#)

Cómo descargar el dispositivo virtual para VSC, proveedor VASA y SRA

Puede descargar la `.ova` Archivo del dispositivo virtual para Virtual Storage Console, VASA Provider y el adaptador de replicación de almacenamiento de `.`

La `.ova` El archivo incluye VSC, proveedor VASA y SRA. Una vez finalizada la implementación, los tres productos se instalan en el entorno. De forma predeterminada, VSC comienza a trabajar en cuanto decida sobre el modelo de puesta en marcha siguiente y decida si desea habilitar el proveedor VASA y el SRA en función de sus requisitos.

Puede descargar el dispositivo virtual para VSC, proveedor VASA y SRA en "[Sitio de soporte de NetApp](#)" mediante la página de descarga del software.

Si desea habilitar el SRA en implementación del dispositivo virtual para VSC, proveedor VASA y SRA, debe haber instalado el plugin de SRA en el servidor del administrador de recuperación del sitio (SRM). Puede descargar el archivo de instalación del complemento SRA en el menú **adaptador de replicación de almacenamiento para ONTAP** de la sección **Descargas de software**.

Ponga en marcha el dispositivo virtual para VSC, proveedor VASA y SRA

Debe poner en marcha el dispositivo virtual para Virtual Storage Console (VSC), el proveedor VASA y el adaptador de replicación de almacenamiento (SRA) en el entorno y especificar los parámetros necesarios para poder usar el dispositivo.

Antes de empezar

- Debe ejecutar una versión compatible de vCenter Server.



El dispositivo virtual para VSC, el proveedor VASA y SRA pueden registrarse en la puesta en marcha de Windows de vCenter Server o en una puesta en marcha de VMware vCenter Server Virtual Appliance (vcsa).

"Herramienta de matriz de interoperabilidad: VSC 9.7"

- Debe haber configurado y configurado el entorno de vCenter Server.
- Debe haber configurado un host ESXi para la máquina virtual.
- Debe haber descargado el .ova archivo.
- Debe tener credenciales de inicio de sesión de administrador para la instancia de vCenter Server.
- Debe haber cerrado sesión en vSphere Client y cerrado todas las sesiones en el explorador para evitar cualquier problema con la caché del explorador durante la puesta en marcha del dispositivo virtual para VSC, proveedor VASA y SRA.

Borre los paquetes de plugins descargados en caché de vSphere

- Debe haber habilitado el protocolo de mensajes de control de Internet (ICMP).

Si ICMP está deshabilitado, produce un error en la configuración inicial del dispositivo virtual para VSC, proveedor VASA y SRA, y VSC no puede iniciar los servicios de VSC y proveedor VASA después de la implementación. Es necesario habilitar manualmente los servicios de VSC y proveedor VASA después de la implementación.

Acerca de esta tarea

Si va a poner en marcha una instalación nueva del dispositivo virtual para VSC, proveedor VASA y SRA, el proveedor VASA está habilitado de forma predeterminada. Sin embargo, en caso de actualización de una versión anterior del dispositivo virtual, se conserva el estado de VASA Provider y es posible que deba habilitar VASA Provider manualmente.

"Habilite VASA Provider para configurar almacenes de datos virtuales"

Pasos

1. Inicie sesión en vSphere Client.
2. Seleccione MENU:Home[Host & Clusters].
3. Haga clic con el botón secundario del ratón en el centro de datos necesario y, a continuación, haga clic en **implementar plantilla OVA**.
4. Seleccione el método correspondiente para proporcionar el archivo de implementación para VSC, VASA Provider y SRA y, a continuación, haga clic en **Siguiente**.

Ubicación	Acción
URL	Proporcione la URL para el .ova Archivo del dispositivo virtual para VSC, proveedor VASA y SRA.

Ubicación	Acción
Carpeta	Seleccione la .ova Archivo del dispositivo virtual para VSC, proveedor VASA y SRA de la ubicación guardada.

5. Introduzca los detalles para personalizar el asistente de implementación.

Consulte "[Consideraciones sobre la personalización de la implantación](#)" para obtener todos los detalles.

6. Revise los datos de configuración y, a continuación, haga clic en **Siguiente** para finalizar la implementación.

Mientras espera a que termine la implementación, puede ver el progreso de la implementación desde la ficha **tareas**.

7. Encienda la máquina virtual del dispositivo virtual y, a continuación, abra una consola de la máquina virtual que ejecute el dispositivo virtual.

8. Compruebe que los servicios de VSC, proveedor VASA y SRA se estén ejecutando una vez completada la implementación.

9. Si el dispositivo virtual para VSC, proveedor VASA y SRA no está registrado en ninguna instancia de vCenter Server, use `https://appliance_ip:8143/Register.html` Para registrar la instancia de VSC.

10. Cierre sesión y vuelva a iniciar sesión en vSphere Client para ver el dispositivo virtual implementado para VSC, proveedor VASA y SRA.

Es posible que el plugin se actualice en vSphere Client durante unos minutos.



Si no se puede ver el plugin incluso después de iniciar sesión, se debe limpiar la caché de vSphere Client. [Borre los paquetes de plugins descargados en caché de vSphere](#)

Después de terminar



Si utiliza ONTAP 9.6 o una versión anterior, para ver el panel de VVol, debe descargar e instalar . Sin embargo, para ONTAP 9.7 no es necesario que se registre en el proveedor de VASA.

[Regístrese en el dispositivo virtual para VSC, proveedor VASA y SRA](#)

Consideraciones sobre la personalización de la implantación

Debe tener en cuenta algunas limitaciones a la hora de personalizar la puesta en marcha de dispositivos virtuales para VSC, proveedores VASA y SRA.

Contraseña de usuario del administrador del dispositivo

No debe usar ningún espacio en la contraseña de administrador.

Credenciales de la consola de mantenimiento del dispositivo

Debe acceder a la consola de mantenimiento utilizando el nombre de usuario «mant». Puede establecer la contraseña para el usuario «mant» durante la implementación. Puede utilizar el menú **Configuración de la aplicación** de la consola de mantenimiento de su dispositivo virtual para VSC, VASA Provider y SRA para cambiar la contraseña.

Credenciales de administrador de vCenter Server

Es posible configurar las credenciales de administrador para vCenter Server mientras se implementa el dispositivo virtual para VSC, proveedor VASA y SRA.

Si cambia la contraseña del administrador de vCenter Server, puede actualizar la contraseña del administrador con la siguiente URL: `https://<IP>:8143/Register.html` Donde la dirección IP es del dispositivo virtual para VSC, proveedor VASA y SRA que se proporciona durante la implementación.

Dirección IP de vCenter Server

- Debe proporcionar la dirección IP (IPv4 o IPv6) de la instancia de vCenter Server en la que desea registrar el dispositivo virtual para VSC, proveedor VASA y SRA.

El tipo de certificados VSC y VASA generados depende de la dirección IP (IPv4 o IPv6) que haya proporcionado durante la implementación. Al implementar el dispositivo virtual para VSC, proveedor VASA y SRA, si no introdujo ningún detalle IP estático y DHCP, la red proporciona direcciones IPv4 e IPv6.

- El dispositivo virtual para VSC, proveedor VASA y la dirección IP de SRA que se usa para registrar en vCenter Server dependen del tipo de dirección IP de vCenter Server (IPv4 o IPv6) que se introdujo en el asistente de implementación.

Tanto los certificados VSC como los certificados VASA se generarán con el mismo tipo de dirección IP que se usó durante el registro de vCenter Server.



IPv6 solo es compatible con vCenter Server 6.7 y versiones posteriores.

Propiedades de la red del dispositivo

Si no utiliza DHCP, especifique un nombre de host DNS válido (no cualificado), así como la dirección IP estática del dispositivo virtual para VSC, proveedor VASA y SRA y los otros parámetros de red. Todos estos parámetros son necesarios para una instalación y funcionamiento correctos.

Habilite VASA Provider para configurar almacenes de datos virtuales

El dispositivo virtual para Virtual Storage Console (VSC), el proveedor VASA y el adaptador de replicación de almacenamiento (SRA) tiene habilitada la funcionalidad del proveedor VASA de forma predeterminada. Puede configurar almacenes de datos VMware Virtual Volumes (vVols) con perfiles de capacidad de almacenamiento necesarios para cada almacén de datos vVols.

Antes de empezar

- Debe haber configurado la instancia de vCenter Server y ESXi.
- Debe haber implementado el dispositivo virtual para VSC, proveedor VASA y SRA.

Acerca de esta tarea

Si la funcionalidad del proveedor de VASA está deshabilitada antes de actualizar a la versión 9.7.1 del dispositivo virtual para Virtual Storage Console (VSC), el proveedor VASA y el adaptador de replicación de almacenamiento (SRA), la funcionalidad del proveedor de VASA sigue deshabilitada después de la actualización. Esta versión le permite habilitar la función de replicación vVols para almacenes de datos vVols.

Pasos

1. Inicie sesión en la interfaz de usuario web de VMware vSphere.
2. En vSphere Client, haga clic en MENU:Menu[Virtual Storage Console].
3. Haga clic en **Configuración**.
4. Haga clic en **Administrar capacidades** en la ficha **Configuración administrativa**.
5. En el cuadro de diálogo **Administrar capacidades**, seleccione la extensión VASA Provider para habilitar.
6. Si desea utilizar la capacidad de replicación para almacenes de datos vVols, utilice el botón de alternar **Activar replicación vVols**.
7. Introduzca la dirección IP del dispositivo virtual para VSC, VASA Provider y SRA y la contraseña de administrador y, a continuación, haga clic en **Apply**.

Después de terminar

Si utiliza ONTAP 9.6 o clústeres anteriores, debe registrarse en VASA Provider para obtener detalles de los almacenes de datos vVols y los equipos virtuales que se utilizan en los informes DE almacenes de datos SAN vVols VM y SAN vVols. Sin embargo, si utiliza ONTAP 9.7 o una versión posterior, no es necesario que se registre con el proveedor de VASA.

Regístrese en el dispositivo virtual para VSC, proveedor VASA y SRA

Si utiliza ONTAP 9.6 o una versión anterior, la consola de VVol puede mostrar los detalles de los almacenes de datos de VMware Virtual Volumes (vVols) y las máquinas virtuales solo si se ha registrado para VASA Provider para obtener datos para los informes de máquina virtual y almacén de datos vVols.

Antes de empezar

Debe haber descargado 2.1 o posterior de .



La consola de VVol muestra las métricas de rendimiento solo cuando los almacenes de datos DE SAN vVols y las máquinas virtuales se configuran mediante ONTAP 9.3 o posterior.

Pasos

1. En la página Virtual Storage Console (VSC) **Inicio**, haga clic en **Configuración**.
2. Haga clic en **Administrar extensión** en la ficha **Configuración administrativa**.
3. Utilice el control deslizante **Registrar servicios de API de OnCommand** para activar .
4. Introduzca la dirección IP, el puerto de servicio y las credenciales de .

También puede utilizar el cuadro de diálogo **Administrar extensiones de proveedor VASA** para las siguientes modificaciones:

- Para actualizar el registro cuando se produce algún cambio en las credenciales.
- Para cancelar el registro cuando ya no se requiere la consola de VVol.

Debe desactivar la casilla de verificación **Registrar servicios de API de OnCommand** para eliminar el registro de VASA Provider.

5. Haga clic en **aplicar**.

La consola de VVol muestra las métricas para los almacenes de datos DE SAN VVol ONTAP 9.6 o anteriores solo una vez que se completa el registro del.

Información relacionada

["Soporte de NetApp"](#)

Instale el complemento NFS VAAI

Es posible instalar el plugin de NFS para API de VMware vStorage para la integración de cabinas (VAAI) mediante la interfaz gráfica de usuario del dispositivo virtual para Virtual Storage Console (VSC), el proveedor VASA y el adaptador de replicación de almacenamiento (SRA).

Antes de empezar

- Debe haber descargado el paquete de instalación del plugin de NFS para VAAI (.vib) de .

["Soporte de NetApp"](#)

- Debe haber instalado el host ESXi 6.5 o posterior y ONTAP 9.1 o posterior.
- Debe haber encendido el host ESXi y montado un almacén de datos NFS.
- Debe haber configurado los valores de `DataMover.HardwareAcceleratedMove`, `DataMover.HardwareAcceleratedInit`, y `VMFS3.HardwareAcceleratedLocking` ajustes del host a «1».

Estos valores se establecen automáticamente en el host ESXi cuando se actualiza el cuadro de diálogo

Configuración recomendada.

- Debe haber habilitado la opción vstorage en el mediante el `vserver nfs modify -vserver vserver_name -vstorage enabled` comando.

Pasos

1. Cambie el nombre de .vib archivo que ha descargado de a `NetAppNasPlugin.vib` Para que coincida con el nombre predefinido que utiliza VSC.
2. Haga clic en **Configuración** en la página de inicio de VSC.
3. Haga clic en la ficha **NFS VAAI Tools**.
4. Haga clic en **Cambiar** en la sección **Versión existente**.
5. Examine y seleccione el nombre cambiado .vib File y, a continuación, haga clic en **Upload** para cargar el archivo en el dispositivo virtual.
6. En la sección **Install on ESXi hosts**, seleccione el host ESXi en el que desea instalar el complemento NFS VAAI y, a continuación, haga clic en **Install**.

Debe seguir las instrucciones que aparecen en pantalla para completar la instalación. Puede supervisar el progreso de la instalación en la sección Tasks de vSphere Web Client.

7. Reinicie el host ESXi después de que finalice la instalación.

Cuando reinicia el host ESXi, VSC detecta automáticamente el plugin NFS VAAI. No es necesario realizar pasos adicionales para habilitar el plugin.

Habilite Storage Replication Adapter

El dispositivo virtual para Virtual Storage Console (VSC), el proveedor VASA y el adaptador de replicación de almacenamiento (SRA) proporciona la opción de permitir que la funcionalidad SRA se use con VSC para configurar la recuperación ante desastres.

Antes de empezar

- Debe haber configurado la instancia de vCenter Server y ESXi.
- Debe haber implementado el dispositivo virtual para VSC, proveedor VASA y SRA.
- Debe haber descargado el `.msi` Archivo del plugin de SRA o del `.tar.gz` File para SRM Appliance solo si desea configurar la solución de recuperación ante desastres de Site Recovery Manager (SRM).

["Site Recovery Manager instalación y configuración Site Recovery Manager 8.2"](#) tiene más información.

Acerca de esta tarea

La flexibilidad para habilitar las funcionalidades VASA Provider y SRA le permite ejecutar solo los flujos de trabajo necesarios para la empresa.

Pasos

1. Inicie sesión en la interfaz de usuario web de VMware vSphere.
2. En vSphere Client, haga clic en MENU:Menu[Virtual Storage Console].
3. Haga clic en **Configuración**.
4. Haga clic en **Administrar capacidades** en la ficha **Configuración administrativa**.
5. En el cuadro de diálogo **Administrar capacidades**, seleccione la extensión SRA que desee activar.
6. Introduzca la dirección IP del dispositivo virtual para VSC, VASA Provider y SRA y la contraseña de administrador y, a continuación, haga clic en **Apply**.
7. Puede usar uno de los siguientes métodos para implementar el SRA:

Opción	Descripción
Para SRM de Windows	<ol style="list-style-type: none">a. Haga doble clic en el descargado <code>.msi</code> Instalador del plugin SRA.b. Siga las instrucciones que aparecen en pantalla.c. Introduzca la dirección IP y la contraseña del dispositivo virtual implementado.

Opción	Descripción
Para dispositivo SRM	<ol style="list-style-type: none"> Acceda a la página del dispositivo SRM y, a continuación, vaya a la página Adaptadores de replicación de almacenamiento del dispositivo SRM. Haga clic en Nuevo adaptador. Cargue el instalador .tar.gz del plugin de SRA en SRM. Vuelva a analizar los adaptadores para verificar que los detalles se actualizan en la página SRM adaptadores de replicación de almacenamiento.

Debe cerrar la sesión en vSphere Client y, a continuación, volver a iniciar sesión para verificar que la extensión seleccionada esté disponible para la configuración.

Información relacionada

[Configure Storage Replication Adapter para la recuperación ante desastres](#)

Configure SRA en el dispositivo SRM

Después de implementar el dispositivo de SRM, debe configurar SRA en el dispositivo de SRM. La configuración correcta del SRA permite que el dispositivo SRM se comunice con el SRA para la gestión de la recuperación ante desastres. Debe almacenar el dispositivo virtual para VSC, proveedores VASA y credenciales de SRA (dirección IP y contraseña de administrador) en el dispositivo SRM para habilitar la comunicación entre el dispositivo SRM y el SRA.

Antes de empezar

Debe cargar el `tar.gz` Archivo a dispositivo SRM.

Acerca de esta tarea

La configuración del SRA en el dispositivo de SRM almacena las credenciales del SRA en el dispositivo de SRM.

Pasos

1. Inicie sesión utilizando la cuenta de administrador en el dispositivo SRM utilizando putty.
2. Cambie al usuario raíz mediante el comando: `su root`
3. En la ubicación del registro, introduzca el comando para obtener el identificador de Docker utilizado por el SRA `docker ps -l`
4. Para iniciar sesión en el identificador del contenedor, introduzca el comando `docker exec -it -u srm <container id> sh`
5. Configure el SRM con el dispositivo virtual para VSC, proveedor VASA y la dirección IP y la contraseña de SRA mediante el comando: `perl command.pl -I <va-IP> administrator <va-password>`

Se muestra un mensaje indicando que las credenciales de almacenamiento están almacenadas correctamente. El SRA puede comunicarse con el servidor SRA mediante la dirección IP, el puerto y las credenciales proporcionados.

Actualice las credenciales del adaptador de replicación de almacenamiento (SRA)

Para que el SRM se comuniquen con el SRA, debe actualizar las credenciales del SRA en el servidor SRM si ha modificado las credenciales.

Antes de empezar

Debe haber ejecutado los pasos mencionados en el tema "Configuración de SRA en dispositivo SRM".

[Configure SRA en el dispositivo SRM](#)

Pasos

1. Elimine el contenido de `/srm/sra/confuso` del directorio:
 - a. `cd /srm/sra/conf`
 - b. `rm -rf *`
2. Ejecute el comando `perl` para configurar SRA con las nuevas credenciales:
 - a. `cd /srm/sra/`
 - b. `perl command.pl -i Administrador de <va-IP> <va-password>`

Migración de SRM de Windows a SRM Appliance

Si utiliza Site Recovery Manager (SRM) basado en Windows para la recuperación ante desastres y desea utilizar SRM para la misma configuración, debe migrar su configuración de recuperación ante desastres de Windows a SRM basado en dispositivos.

Los pasos involucrados en la migración de la recuperación ante desastres son:

1. Actualizar el dispositivo virtual existente para VSC, proveedor VASA y SRA con la versión 9.7.1.

["Actualice al dispositivo virtual 9.7.1 para VSC, proveedor VASA y SRA"](#)

2. Migración de adaptador de replicación de almacenamiento basado en Windows a SRA basado en dispositivo.
3. Migración de datos de SRM de Windows a SRM Appliance.

["Haga clic aquí"](#) para conocer los pasos detallados.

Actualice al dispositivo virtual 9.7.1 para VSC, proveedor VASA y SRA

Puede realizar una actualización directa a la versión 9.7.1 del dispositivo virtual para VSC, proveedor VASA y SRA desde la configuración actual de la versión 9.7 siguiendo las instrucciones que se indican aquí.

Antes de empezar

- Debe haber descargado el `.iso` Archivo para el lanzamiento de la versión 9.7.1 del dispositivo virtual para VSC, proveedor VASA y SRA.
- Debe haber reservado al menos 12 GB de RAM para que el dispositivo virtual funcione correctamente después de la actualización, para que VSC, proveedor VASA y SRA.
- Debe limpiar la caché del explorador de vSphere Client.

Borre los paquetes de plugins descargados en caché de vSphere

Acerca de esta tarea

El estado del proveedor de VASA de la implementación existente se conserva después de la actualización. Después de la actualización, es necesario habilitar o deshabilitar manualmente VASA Provider según sus requisitos. Sin embargo, es mejor habilitar VASA Provider incluso si los volúmenes virtuales de VMware (vVols) no están en uso, ya que permite los perfiles de funcionalidades de almacenamiento para el aprovisionamiento de almacenes de datos tradicionales y las alarmas de almacenamiento.



El dispositivo virtual para VSC, proveedor VASA y SRA no admite una actualización directa de cualquier versión anterior a la versión 9.7 a 9.7P2 o posterior. Primero debe actualizar la configuración existente a la versión 9.7 del dispositivo virtual para VSC, proveedor VASA y SRA antes de actualizar a cualquier versión posterior. Cuando actualice a la versión 9.7.1 del dispositivo virtual para VSC, proveedor VASA y SRA y desee usar la replicación de vVols, tendrá que configurar una instancia más de vCenter Server con el dispositivo virtual con el administrador de recuperación de sitio (SRM) instalado.

Pasos

1. Monte el descargado `.iso` archivo al dispositivo virtual:
 - a. Haga clic en MENU:Editar configuración[Unidad de DVD/CD-ROM].
 - b. Seleccione **Datastore ISO** file en la lista desplegable.
 - c. Desplácese hasta la opción descargada y selecciónela `.iso` File y, a continuación, seleccione la casilla de verificación **conectar al encender**.

2. Acceda a la ficha **Resumen** del dispositivo virtual implementado.

3. Haga clic en  para iniciar la consola de mantenimiento.

4. En el indicador «Menú principal», introduzca la opción 2 Para **Configuración del sistema** y, a continuación, introduzca la opción 8 Para **actualización**.

Cuando se complete la actualización, el dispositivo virtual se reiniciará. El dispositivo virtual para VSC, el proveedor VASA y SRA están registrados en vCenter Server con la misma dirección IP que antes de la actualización.

5. Si desea que el dispositivo virtual para VSC, proveedor VASA y SRA se registre en el vCenter Server con la dirección IPv6, debe realizar lo siguiente:
 - a. Cancele el registro del dispositivo virtual para VSC, proveedor VASA y SRA.
 - b. Registre la dirección IPv6 del dispositivo virtual para VSC, VASA Provider y SRA en vCenter Server mediante la página **Register**.
 - c. Vuelva a generar los certificados de VSC y proveedores VASA después del registro.



IPv6 solo es compatible con vCenter Server 6.7 y versiones posteriores.

6. Cierre sesión y vuelva a iniciar sesión en vSphere Client para ver el dispositivo virtual implementado para VSC, proveedor VASA y SRA.
 - a. Cierre la sesión en vSphere Web Client o vSphere Client existente y cierre la ventana.
 - b. Inicie sesión en vSphere Client.

Es posible que el plugin se actualice en vSphere Client durante unos minutos.

Información relacionada

[Habilite VASA Provider para configurar almacenes de datos virtuales](#)

Actualice el adaptador de replicación de almacenamiento

Después de actualizar el dispositivo virtual para VSC, proveedor VASA y SRA, o de implementar la versión más reciente del dispositivo virtual, debe actualizar el adaptador de replicación de almacenamiento (SRA).

Pasos

1. Debe actualizar al adaptador más reciente mediante uno de los siguientes procedimientos basados en su adaptador:

Para...	Realice lo siguiente...
Windows	<ol style="list-style-type: none">a. Inicie sesión en SRM Windows Server.b. Desinstale el instalador de SRA <i>.msi</i> existente del servidor SRM.c. Cambie la ruta del sistema a. C:\Program Files\VMware\VMware vCenter Site Recovery Manager\external\perl\c\bind. Haga doble clic en el instalador <i>.msi</i> que ha descargado desde el sitio de soporte de NetApp y siga las instrucciones en pantalla.e. Introduzca la dirección IP y la contraseña del dispositivo virtual puesto en marcha para VSC, proveedor VASA y SRA.

Para...	Realice lo siguiente...
Adaptador basado en dispositivo	<p>a. Inicie sesión en la página Gestión del dispositivo SRM.</p> <p>b. Haga clic en adaptador de replicación de almacenamiento y haga clic en Eliminar para eliminar el SRA existente.</p> <p>c. Haga clic en menú:Nuevo adaptador[examinar].</p> <p>d. Haga clic aquí para seleccionar el último archivo de tarball de SRA que descargó del sitio de soporte de NetApp y, a continuación, haga clic en instalar.</p> <p>e. Configure SRA en el dispositivo SRM.</p> <p>Configure SRA en el dispositivo SRM</p>

Configure el entorno de Virtual Storage Console para VMware vSphere

(VSC) admite numerosos entornos. Algunas de las funciones de estos entornos pueden requerir una configuración adicional.

Es posible que tenga que realizar algunas de las siguientes tareas para configurar los hosts ESXi, los sistemas operativos invitados y VSC:

- Compruebe la configuración del host ESXi, incluida la configuración UNMAP
- Adición de valores de tiempo de espera para sistemas operativos invitados
- Regeneración del certificado SSL de VSC
- Creación de perfiles de capacidad de almacenamiento y alarmas de umbral
- Modificar el archivo de preferencias para permitir el montaje de almacenes de datos en subredes diferentes

Configure los valores de multivía y de tiempo de espera del servidor ESXi

Virtual Storage Console para VMware vSphere comprueba y establece la configuración de accesos múltiples del host ESXi y del tiempo de espera de HBA que funcionan mejor con los sistemas de almacenamiento.

Acerca de esta tarea

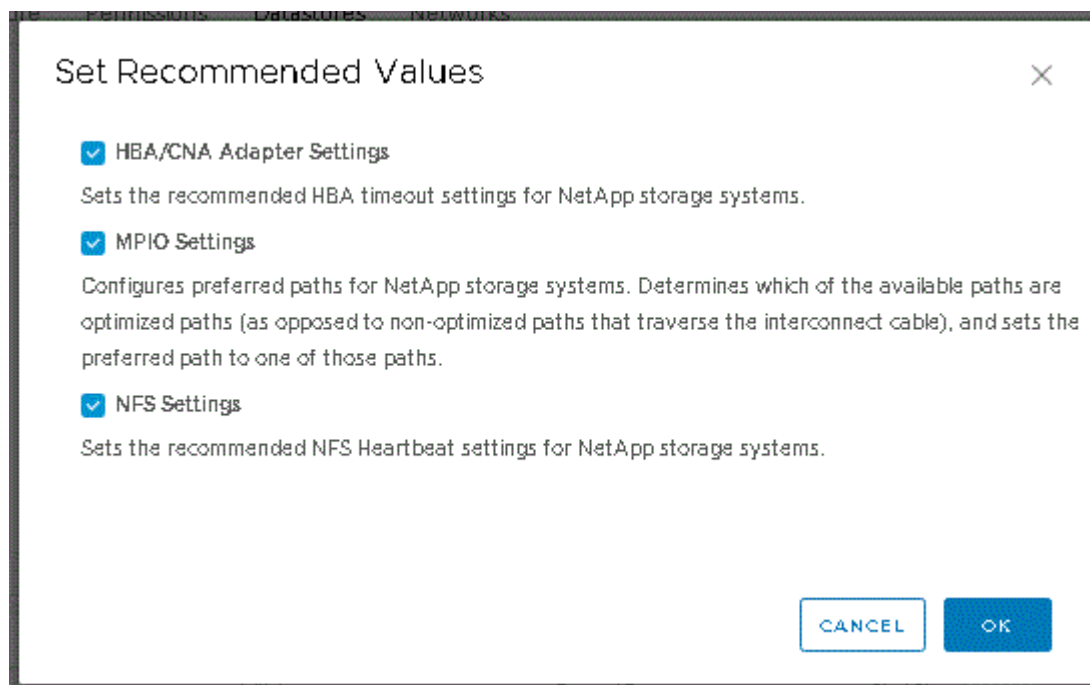
Este proceso puede llevar mucho tiempo, según la configuración y la carga del sistema. El progreso de la tarea se muestra en el panel **tareas recientes**. Cuando se completan las tareas, el icono de alerta de estado del host se sustituye por el icono normal o el icono de reinicio pendiente.

Pasos

1. En la página VMware vSphere Web Client **Home**, haga clic en MENU:vCenter[hosts].

2. Haga clic con el botón derecho en un host y seleccione MENU:Actions[NetApp VSC > Set recommended Values].
3. En el cuadro de diálogo **Configuración recomendada de NetApp**, seleccione los valores que mejor se adapten a su sistema.

Los valores estándar recomendados se establecen de forma predeterminada.



4. Haga clic en **Aceptar**.

Los valores de host de ESXi se establecen mediante Virtual Storage Console para VMware vSphere

Es posible configurar tiempos de espera y otros valores en los hosts ESXi mediante Virtual Storage Console para VMware vSphere con el fin de garantizar el mejor rendimiento y una conmutación por error correcta. Los valores que establece Virtual Storage Console (VSC) se basan en pruebas internas.

Puede configurar los siguientes valores en un host ESXi:

Configuración avanzada de ESXi

- **VMFS3.HardwareAcceleratedLocking**

Debe establecer este valor en 1.

- **VMFS3.EnableBlockDelete**

Debe configurar este valor en 0.

Configuración de NFS

- **Net.TcpipHeapSize**

Si utiliza vSphere 6.0 o una versión posterior, debe configurar este valor en 32.

- **Net.TcpipHeapMax**

Si utiliza vSphere 6.0 o una versión posterior, debe configurar este valor en 1536.

- **NFS.MaxVolumes**

Si utiliza vSphere 6.0 o una versión posterior, debe configurar este valor en 256.

- **NFS41.MaxVolumes**

Si utiliza vSphere 6.0 o una versión posterior, debe configurar este valor en 256.

- **NFS.MaxQueueDepth**

Si utiliza vSphere 6.0 o una versión posterior del host ESXi, debe configurar este valor en 128 o superior para evitar los cuellos de botella en la cola.

Para las versiones de vSphere anteriores a la 6.0, debe configurar este valor en 64.

- **NFS.HeartbeatMaxFailures**

Debe establecer este valor en 10 para todas las configuraciones de NFS.

- **NFS.HeartbeatFrequency**

Debe establecer este valor en 12 para todas las configuraciones de NFS.

- **NFS.HeartbeatTimeout**

Debe establecer este valor en 5 para todas las configuraciones de NFS.

Configuración de FC/FCoE

- **Política de selección de ruta**

Debe establecer este valor en "RR" (operación por turnos) cuando se utilicen rutas FC con ALUA.

Debería establecer este valor en «FIJO» para todas las demás configuraciones.

Establecer este valor en «RR» ayuda a proporcionar equilibrio de carga en todas las rutas activas/optimizadas. El valor "FIXED" se utiliza para configuraciones antiguas y no ALUA y ayuda a evitar las operaciones de E/S proxy

- **Disk.QFullSampleSize**

Debe establecer este valor en 32 para todas las configuraciones. Si configura este valor, se evitan los errores de I/O.

- **Disk.QFullThreshold**

Debe establecer este valor en 8 para todas las configuraciones. Si configura este valor, se evitan los errores de I/O.

- **Tiempos de espera de HBA FC Emulex**

Se utiliza el valor predeterminado.

- **Tiempo de espera de HBA FC QLogic**

Se utiliza el valor predeterminado.

Configuración de iSCSI

- **Política de selección de ruta**

Debería establecer este valor en «'RR'» para todas las rutas de iSCSI.

Establecer este valor en «'RR'» ayuda a proporcionar equilibrio de carga en todas las rutas activas/optimizadas.

- **Disk.QFullSampleSize**

Debe establecer este valor en 32 para todas las configuraciones. Si configura este valor, se evitan los errores de I/O.

- **Disk.QFullThreshold**

Debe establecer este valor en 8 para todas las configuraciones. Si configura este valor, se evitan los errores de I/O.

Configurar los scripts del sistema operativo invitado

Las imágenes ISO de los scripts del sistema operativo invitado (SO) se montan en Virtual Storage Console para el servidor VMware vSphere. Para utilizar los scripts del sistema operativo invitado para configurar los tiempos de espera de almacenamiento de las máquinas virtuales, se deben montar los scripts desde vSphere Client.

Tipo de sistema operativo	configuración de tiempo de espera de 60 segundos	configuración de tiempo de espera de 190 segundos
Linux	<code>https://<appliance_ip>:8143/vsc/public/writable/linux_gos_timeout-install.iso</code>	<code>https://<appliance_ip>:8143/vsc/public/writable/linux_gos_timeout_190-install.iso</code>
Windows	<code>https://<appliance_ip>:8143/vsc/public/writable/windows_gos_timeout.iso</code>	<code>https://<appliance_ip>:8143/vsc/public/writable/windows_gos_timeout_190.iso</code>
Solaris	<code>https://<appliance_ip>:8143/vsc/public/writable/solaris_gos_timeout-install.iso</code>	<code>https://<appliance_ip>:8143/vsc/public/writable/solaris_gos_timeout_190-install.iso</code>

Debe instalar el script a partir de la copia de la instancia de VSC que está registrada en vCenter Server que gestiona la máquina virtual. Si el entorno incluye varias instancias de vCenter Server, debe seleccionar el

servidor que contiene la máquina virtual para la cual desea configurar los valores de tiempo de espera de almacenamiento.

Debe iniciar sesión en la máquina virtual y ejecutar el script para configurar los valores de tiempo de espera de almacenamiento.

Configurar valores de tiempo de espera para sistemas operativos invitados de Windows

Las secuencias de comandos de tiempo de espera del sistema operativo invitado configuran los ajustes de tiempo de espera de I/O SCSI para sistemas operativos invitados Windows. Puede especificar un tiempo de espera de 60 segundos o un tiempo de espera de 190 segundos. Debe reiniciar el sistema operativo invitado de Windows para que la configuración surta efecto.

Antes de empezar

Debe haber montado la imagen ISO que contiene la secuencia de comandos de Windows.

Pasos

1. Acceda a la consola de la máquina virtual de Windows e inicie sesión en una cuenta con privilegios de administrador.
2. Si la secuencia de comandos no se inicia automáticamente, abra la unidad de CD y, a continuación, ejecute la `windows_gos_timeout.reg` guión.

Aparecerá el cuadro de diálogo Editor del Registro.

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

Se muestra el siguiente mensaje: The keys and values contained in
D:\windows_gos_timeout.reg have been successfully added to the registry.

4. Reinicie el sistema operativo invitado Windows.
5. Desmonte la imagen ISO.

Defina los valores de tiempo de espera para los sistemas operativos invitados Solaris

Los scripts de tiempo de espera del sistema operativo invitado definen los ajustes de tiempo de espera de I/O SCSI para Solaris 10. Puede especificar un tiempo de espera de 60 segundos o un tiempo de espera de 190 segundos.

Antes de empezar

Debe haber montado la imagen ISO que contenga la secuencia de comandos de Solaris.

Pasos

1. Acceda a la consola de la máquina virtual Solaris e inicie sesión en una cuenta con privilegios de root.
2. Ejecute el `solaris_gos_timeout-install.sh` guión.

Para Solaris 10, se muestra un mensaje similar al siguiente:

```
Setting I/O Timeout for /dev/s-a - SUCCESS!
```

3. Desmonte la imagen ISO.

Configurar valores de tiempo de espera para sistemas operativos invitados Linux

Las secuencias de comandos de tiempo de espera del sistema operativo invitado definen la configuración de tiempo de espera de E/S SCSI para las versiones 4, 5, 6 y 7 de Red Hat Enterprise Linux y las versiones 9, 10 y 11 de SUSE Linux Enterprise Server. Puede especificar un tiempo de espera de 60 segundos o un tiempo de espera de 190 segundos. Debe ejecutar el script cada vez que actualice a una nueva versión de Linux.

Antes de empezar

Debe haber montado la imagen ISO que contiene el script de Linux.

Pasos

1. Acceda a la consola de la máquina virtual Linux e inicie sesión en una cuenta con privilegios de usuario raíz.
2. Ejecute el `linux_gos_timeout-install.sh` guión.

Para Red Hat Enterprise Linux 4 o SUSE Linux Enterprise Server 9, se muestra un mensaje similar al siguiente:

```
Restarting udev... this may take a few seconds.
```

```
Setting I/O Timeout (60s) for /dev/sda - SUCCESS!
```

Para Red Hat Enterprise Linux 5, Red Hat Enterprise Linux 6 y Red Hat Enterprise Linux 7 se muestra un mensaje similar al siguiente:

```
patching file /etc/udev/rules.d/50-udev.rules
```

```
Hunk #1 succeeded at 333 (offset 13 lines).
```

```
Restarting udev... this may take a few seconds.
```

```
Starting udev: [ OK ]
```

```
Setting I/O Timeout (60s) for /dev/sda - SUCCESS!
```

Para SUSE Linux Enterprise Server 10 o SUSE Linux Enterprise Server 11, aparece un mensaje similar al siguiente:

```
patching file /etc/udev/rules.d/50-udev-default.rules
```

```
Hunk #1 succeeded at 114 (offset 1 line).
```

```
Restarting udev ...this may take a few seconds.
```

```
Updating all available device nodes in /dev: done
```

3. Desmonte la imagen ISO.

Regenere un certificado SSL para Virtual Storage Console

El certificado SSL se genera al instalar (VSC). El nombre distintivo (DN) que se genera para el certificado SSL puede no ser un nombre común (CN) que reconocen los equipos cliente. Al cambiar las contraseñas del almacén de claves y de la clave privada, puede volver a generar el certificado y crear un certificado específico del sitio.

Acerca de esta tarea

Puede habilitar el diagnóstico remoto mediante la consola de mantenimiento y generar un certificado específico de cada sitio.

["Respuesta 1075654 de la base de conocimientos de NetApp: Virtual Storage Console 7.x: Implementación de certificados firmados por CA"](#)

Pasos

1. Inicie sesión en la consola de mantenimiento.
2. Introduzca 1 para acceder a `Application Configuration` de windows
3. En la `Application Configuration` menú, acceder 3 Para detener el servicio VSC.
4. Introduzca 7 Para regenerar el certificado SSL.

Requisitos para registrar VSC en varios entornos de vCenter Server

Si utiliza Virtual Storage Console para VMware vSphere en un entorno donde un único cliente HTML5 de VMware vSphere. Está gestionando varias instancias de vCenter Server, debe registrar una instancia de VSC en cada instancia de vCenter Server, de modo que haya un emparejamiento 1:1 entre VSC y vCenter Server. Esta acción le permite gestionar todos los servidores que ejecutan vCenter 6.0 o una versión posterior en el modo vinculado y en el modo no vinculado desde un único cliente HTML5 de vSphere.



Si desea utilizar VSC con una instancia de vCenter Server, debe haber configurado o registrado una instancia de VSC para cada instancia de vCenter Server que desee gestionar. Cada instancia de VSC registrada debe tener la misma versión.

El modo vinculado se instala automáticamente durante la puesta en marcha de vCenter Server. El modo vinculado utiliza el modo de aplicación de Microsoft Active Directory (ADAM) para almacenar y sincronizar datos en varios sistemas de vCenter Server.

El uso del cliente HTML5 de vSphere para realizar tareas VSC en varias instancias de vCenter Server requiere lo siguiente:

- Cada instancia de vCenter Server del inventario de VMware que desee gestionar debe tener un único servidor VSC registrado con él en un emparejamiento único 1:1.

Por ejemplo, puede tener un servidor VSC A registrado en vCenter Server A, el servidor VSC B registrado en vCenter Server B, el servidor VSC C registrado en vCenter Server C, etc.

No puede tener un servidor VSC a registrado tanto en vCenter Server a como en vCenter Server B.

Si un inventario de VMware incluye una instancia de vCenter Server que no tiene ningún servidor VSC registrado, pero hay una o más instancias de vCenter Server registradas en VSC, a continuación, puede ver las instancias de VSC y realizar operaciones VSC para las instancias de vCenter Server que tienen registrado VSC.

- Debe tener el privilegio View específico de VSC para cada instancia de vCenter Server que se registre en el inicio de sesión único (SSO).

También debe tener los permisos de RBAC correctos.

Cuando va a realizar una tarea que requiere especificar una instancia de vCenter Server, el cuadro desplegable **vCenter Server** muestra los servidores vCenter disponibles en orden alfanumérico. El servidor vCenter Server predeterminado siempre es el primer servidor de la lista desplegable.

Si se conoce la ubicación del almacenamiento (por ejemplo, cuando se utiliza el asistente **Provisioning** y el almacén de datos se encuentra en un host gestionado por un vCenter Server específico), la lista de vCenter Server se muestra como una opción de solo lectura. Esto sucede solo cuando se utiliza la opción de clic con el botón derecho para seleccionar un elemento en vSphere Web Client.

VSC le avisa cuando se intenta seleccionar un objeto que no gestiona.

Puede filtrar los sistemas de almacenamiento según una instancia específica de vCenter Server en la página de resumen de VSC. Se muestra una página de resumen para cada instancia de VSC que está registrada en una instancia de vCenter Server. Puede gestionar los sistemas de almacenamiento asociados con una instancia de VSC específica y una instancia de vCenter Server, pero debe mantener la información de registro de cada sistema de almacenamiento separada si ejecuta varias instancias de VSC.

Configure los archivos de preferencias de VSC

Los archivos de preferencias contienen una configuración que controla las operaciones de Virtual Storage Console para VMware vSphere. En la mayoría de los casos, no es necesario modificar la configuración de estos archivos. Es útil saber qué archivos de preferencias (VSC) utiliza.

VSC tiene varios archivos de preferencias. Estos archivos incluyen claves de entrada y valores que determinan el modo en que VSC realiza diversas operaciones. A continuación se muestran algunos de los archivos de preferencias que utiliza VSC:

```
/opt/netapp/vscserver/etc/kamino/kaminoprefs.xml
```

```
/opt/netapp/vscserver/etc/vsc/vscPreferences.xml
```

Puede que tenga que modificar los archivos de preferencias en determinadas situaciones. Por ejemplo, si utiliza iSCSI o NFS y la subred es diferente para los hosts ESXi y el sistema de almacenamiento, deberá modificar los archivos de preferencias. Si no modifica la configuración en el archivo de preferencias, el aprovisionamiento del almacén de datos genera errores porque VSC no puede montar el almacén de datos.

Establezca IPv4 o IPv6

Hay una nueva opción agregada al archivo de preferencias `kaminoprefs.xml` que puede configurar para habilitar la compatibilidad con IPv4 o IPv6 en todos los sistemas de almacenamiento añadidos a VSC.

- La `default.override.option.provision.mount.datastore.address.family` el parámetro se ha agregado a la `kaminoprefs.xml` Archivo de preferencias para establecer un protocolo LIF de datos preferido para el aprovisionamiento del almacén de datos.

Esta preferencia es aplicable para todos los sistemas de almacenamiento añadidos a VSC.

- Los valores de la nueva opción son IPv4, IPv6, y NONE.
- De forma predeterminada, el valor se establece en NONE.

Valor	Descripción
NINGUNO	<ul style="list-style-type: none">• El aprovisionamiento ocurre mediante el mismo tipo de LIF de datos IPv6 o IPv4 que el tipo de clúster o LIF de gestión utilizado para añadir el almacenamiento.• Si el mismo tipo de dirección IPv6 o IPv4 de LIF de datos no está presente en , el aprovisionamiento se realiza a través del otro tipo de LIF de datos, si está disponible.
IPv4	<ul style="list-style-type: none">• El aprovisionamiento se realiza utilizando la LIF de datos IPv4 en el seleccionado .• Si el no tiene una LIF de datos IPv4, el aprovisionamiento se realiza a través de la LIF de datos IPv6, si está disponible en .
IPv6	<ul style="list-style-type: none">• El aprovisionamiento se realiza utilizando la LIF de datos IPv6 en el seleccionado .• Si el no tiene una LIF de datos IPv6, el aprovisionamiento se realiza a través de la LIF de datos IPv4, si está disponible en .

Habilite el montaje del almacén de datos en diferentes subredes

Si utiliza iSCSI o NFS y la subred es diferente entre los hosts ESXi y el sistema de almacenamiento, debe modificar los archivos de preferencias de Virtual Storage Console para VMware vSphere. Si no modifica el archivo de preferencias, el aprovisionamiento del almacén de datos genera errores porque (VSC) no puede montar el almacén de datos.

Acerca de esta tarea

Cuando el aprovisionamiento del almacén de datos falla, VSC registra los siguientes mensajes de error:

```
Unable to continue. No ip addresses found when cross-referencing kernel ip addresses and addresses on the controller.
```

```
Unable to find a matching network to NFS mount volume to these hosts."
```

Pasos

1. Inicie sesión en la instancia de vCenter Server.
2. Inicie la consola de mantenimiento con la máquina virtual unificada del dispositivo.

["Acceda a las opciones de la consola de mantenimiento del dispositivo virtual para VSC, proveedor VASA y SRA"](#)
3. Introduzca 4 Para acceder a la opción **Soporte y Diagnóstico**.
4. Introduzca 2 Para acceder a la opción **acceder al shell de diagnóstico**.
5. Introduzca `vi /opt/netapp/vscserver/etc/kamino/kaminoprefs.xml` para actualizar la `kaminoprefs.xml` archivo.
6. Actualice el `kaminoprefs.xml` archivo.

Si usa...	Realice lo siguiente...
ISCSI	Cambie el valor de la clave de entrada <code>default.allow.iscsi.mount.networks</code> Desde TODO hasta el valor de las redes de host ESXi.
NFS	Cambie el valor de la clave de entrada <code>default.allow.nfs.mount.networks</code> Desde TODO hasta el valor de las redes de host ESXi.

El archivo de preferencias incluye valores de ejemplo para estas claves de entrada.



El valor «'TODOS'» no significa todas las redes. «TODO» permite utilizar todas las redes coincidentes entre el host y el sistema de almacenamiento para montar almacenes de datos. Cuando se especifican redes host, puede habilitar el montaje solo en las subredes especificadas.

7. Guarde y cierre el `kaminoprefs.xml` archivo.

Acceda a las opciones de la consola de mantenimiento del dispositivo virtual para VSC, proveedor VASA y SRA

Puede gestionar las configuraciones de aplicaciones, sistema y redes mediante la consola de mantenimiento del dispositivo virtual para Virtual Storage Console (VSC), proveedor VASA y Storage Replication Adapter (SRA). Puede cambiar la contraseña de administrador y la contraseña de mantenimiento. También puede generar paquetes de soporte, establecer diferentes niveles de registro, ver y gestionar configuraciones de TLS e iniciar diagnósticos remotos.


Antes de empezar

Debe haber instalado herramientas de VMware después de implementar el dispositivo virtual para VSC, proveedor VASA y SRA.

Acerca de esta tarea

- Debe utilizar «mant» como nombre de usuario y la contraseña que configuró durante la implementación para iniciar sesión en la consola de mantenimiento del dispositivo virtual para VSC, VASA Provider y SRA.
- Debe establecer una contraseña para el usuario «diag» mientras habilita el diagnóstico remoto.

Pasos

1. Acceda a la ficha **Resumen** del dispositivo virtual implementado.
2. Haga clic en  para iniciar la consola de mantenimiento.

Puede acceder a las siguientes opciones de la consola de mantenimiento:

◦ Configuración de la aplicación

Están disponibles las siguientes opciones:

- Mostrar resumen de estado del servidor
- Inicie el servicio Virtual Storage Console
- Detenga el servicio Virtual Storage Console
- Inicie el proveedor VASA y el servicio SRA
- Detenga el proveedor VASA y el servicio SRA
- Cambie la contraseña de usuario del administrador
- Volver a generar certificados
- Restablecimiento completo del almacén de claves y los certificados
- Restablecimiento manual de la base de datos
- Cambie el nivel DE REGISTRO del servicio Virtual Storage Console
- Cambiar el nivel DE REGISTRO del proveedor VASA y el servicio SRA
- Mostrar la configuración de TLS
- Habilite el protocolo TLS
- Deshabilite el protocolo TLS

◦ Configuración del sistema

Están disponibles las siguientes opciones:

- Reiniciar la máquina virtual
- Apagar la máquina virtual
- Cambiar la contraseña de usuario "mant"
- Cambiar zona horaria
- Cambie el servidor NTP

Es posible proporcionar una dirección IPv6 para el servidor NTP.

- Habilitar/deshabilitar acceso SSH
- Aumentar el tamaño de los discos de cárcel (/prisión)
- Renovar
- Instalación de VMware Tools

◦ **Configuración de red**

Están disponibles las siguientes opciones:

- Mostrar la configuración de la dirección IP
- Cambiar la configuración de la dirección IP

Puede usar esta opción para cambiar a IPv6 la dirección IP posterior a la implementación.

- Mostrar la configuración de búsqueda de nombres de dominio
- Cambiar la configuración de búsqueda de nombres de dominio
- Mostrar rutas estáticas
- Cambiar rutas estáticas

Puede usar esta opción para añadir una ruta IPv6.

- Confirmar cambios
- Hacer ping a un host

Puede usar esta opción para hacer ping a un host IPv6.

- Restaurar la configuración predeterminada

◦ **Soporte y diagnóstico**

Están disponibles las siguientes opciones:

- Genere el bundle de soporte
- Acceder al shell de diagnóstico
- Active el acceso de diagnóstico remoto

Información relacionada

[Archivos de registro de VSC y VASA Provider](#)

Cambie la contraseña del administrador

Es posible cambiar la contraseña de administrador del dispositivo virtual para VSC, proveedor VASA y SRA después de la implementación mediante la consola de mantenimiento.

Pasos

1. Desde vCenter Server, abra una consola al dispositivo virtual para VSC, proveedor VASA y SRA.
2. Inicie sesión como el usuario de mantenimiento.
3. Introduzca 1 En la consola de mantenimiento para seleccionar **Configuración de la aplicación**.
4. Introduzca 6 Para seleccionar **Cambiar la contraseña de usuario de administrador**.
5. Introduzca una contraseña con un mínimo de ocho caracteres y un máximo de 63.
6. Introduzca y en el cuadro de diálogo de confirmación.

Configure la alta disponibilidad del dispositivo virtual para VSC, proveedores VASA y SRA

El dispositivo virtual para Virtual Storage Console (VSC), el proveedor VASA y el adaptador de replicación de almacenamiento (SRA) admite una configuración de alta disponibilidad para ayudar a proporcionar funcionalidad sin interrupciones de VSC, proveedor VASA y SRA en caso de fallo.

El dispositivo virtual para VSC, VASA Provider y SRA confía en la función VMware vSphere (ha) y la función vSphere de tolerancia a fallos (FT) para proporcionar . (HA) permite una rápida recuperación tras interrupciones provocadas por:

- Error del host
- Fallo de red
- Fallo de máquina virtual (fallo de SO invitado)
- Fallo de la aplicación (VSC, proveedor VASA y SRA)

No se requiere ninguna configuración adicional en el dispositivo virtual para proporcionar . Solo las instancias de vCenter Server y los hosts ESXi deben configurarse con la función de alta disponibilidad de VMware vSphere o la función vSphere FT en función de sus requisitos. Tanto la alta disponibilidad COMO FT requieren hosts en clúster junto con almacenamiento compartido. FT tiene requisitos y limitaciones adicionales.

Además de la solución de alta disponibilidad de VMware vSphere y la solución VSPHERE FT, el dispositivo virtual también ayuda a mantener en funcionamiento los servicios VSC, proveedores VASA y SRA en todo momento. El proceso de vigilancia del dispositivo virtual supervisa periódicamente los tres servicios y los reinicia automáticamente cuando se detecta cualquier tipo de fallo. Esto ayuda a evitar que se produzcan fallos en las aplicaciones.



La alta disponibilidad de vCenter no es compatible con el dispositivo virtual para VSC, el proveedor VASA y SRA.

VMware vSphere ha

Es posible configurar el entorno de vSphere donde el dispositivo virtual para Virtual Storage Console (VSC), el proveedor VASA y el adaptador de replicación de almacenamiento (SRA) se ponga en marcha para (ha). La función de alta disponibilidad de VMware ofrece protección tras fallos frente a fallos del hardware y fallos del sistema operativo en entornos virtuales.

La función de alta disponibilidad de VMware supervisa las máquinas virtuales para detectar fallos del sistema operativo y fallos del hardware. Cuando se detecta un fallo, la función de alta disponibilidad de VMware reinicia las máquinas virtuales en los demás servidores físicos del pool de recursos. No es necesaria la intervención manual cuando se detecta un fallo del servidor.

El procedimiento para configurar VMware ha depende de la versión de su vCenter Server. Por ejemplo, puede utilizar el siguiente enlace de referencia y seleccionar la versión necesaria de vCenter Server para ver los pasos necesarios para configurar la alta disponibilidad de VMware.

["Documentación de VMware vSphere: Crear y usar clústeres de alta disponibilidad de vSphere"](#)

Tolerancia a fallos de VMware vSphere

La función DE tolerancia a fallos (FT) de VMware vSphere proporciona (ha) a un nivel superior y le permite proteger las máquinas virtuales sin que se pierdan datos o conexiones. Debe habilitar o deshabilitar vSphere FT para el dispositivo virtual para VSC, proveedor VASA y SRA en vCenter Server.

Compruebe que la licencia de vSphere sea compatible CON FT con el número de vCPU necesarias para el dispositivo virtual en su entorno (al menos 2 vCPU y 4 vCPU para entornos a gran escala).

VSphere FT permite que las máquinas virtuales funcionen continuamente incluso durante fallos de servidores. Cuando se habilita vSphere FT en una máquina virtual, se crea automáticamente una copia de la máquina virtual primaria en otro host (la máquina virtual secundaria) seleccionado por Distributed Resource Scheduler (DRS). Si DRS no está habilitado, el host de destino se selecciona de entre los hosts disponibles. VSphere FT opera la máquina virtual principal y la máquina virtual secundaria en modo de bloqueo, con cada mirroring del estado de ejecución de la máquina virtual principal a la máquina virtual secundaria.

Cuando se produce un error de hardware que provoca un fallo en la máquina virtual primaria, la máquina virtual secundaria recupera inmediatamente dónde se detuvo la máquina virtual principal. La máquina virtual secundaria continúa ejecutándose sin pérdida de conexiones de red, transacciones o datos.

El sistema debe cumplir los requisitos de CPU, los requisitos de límite de máquinas virtuales y los requisitos de licencias para configurar vSphere FT para la instancia de vCenter Server.

El procedimiento para configurar la alta disponibilidad depende de la versión del servidor de vCenter Server. Por ejemplo, puede utilizar el siguiente enlace de referencia y seleccionar la versión necesaria de vCenter Server para ver los pasos necesarios para configurar la alta disponibilidad.

["Documentación de VMware vSphere: Requisitos, límites y licencias de Fault Tolerance"](#)

Configuraciones de MetroCluster compatibles con el dispositivo virtual para VSC, proveedor VASA y SRA

El dispositivo virtual para Virtual Storage Console (VSC), el proveedor VASA y el adaptador de replicación de almacenamiento (SRA) admiten entornos que usan configuraciones de IP y FC de MetroCluster para ONTAP. La mayor parte de este soporte es automático. Sin embargo, es posible que note algunas diferencias cuando utiliza un entorno de MetroCluster con VSC y VASA Provider.

Configuraciones de MetroCluster y VSC

Debe asegurarse de que VSC detecte las controladoras del sistema de almacenamiento en el sitio primario y en el sitio secundario. Generalmente, VSC detecta automáticamente las controladoras de almacenamiento. Si utiliza una LIF de gestión de clústeres, es una buena práctica verificar que VSC ha detectado los clústeres en ambos sitios. De lo contrario, puede añadir manualmente las controladoras de almacenamiento a VSC. También puede modificar el nombre de usuario y las parejas de contraseñas que utiliza VSC para conectarse a las controladoras de almacenamiento.

Cuando se produce una conmutación, el sitio secundario toma el control. Estos contienen el sufijo "-mc" adjunto a sus nombres. Si se produce una operación de switchover mientras se realizan operaciones como el aprovisionamiento de un almacén de datos, el nombre del almacén de datos donde reside se cambia para incluir el sufijo "-mc". Este sufijo se descarta cuando se produce la conmutación de regreso, y el en el sitio principal se reanuda el control.



Si ha añadido directamente la configuración de MetroCluster a VSC, tras la conmutación, no se verá reflejado el cambio en el nombre de SVM (la adición del sufijo "-mc"). El resto de las operaciones de conmutación se siguen ejecutando con normalidad.

Cuando se produce una conmutación de sitios o una conmutación de estado, VSC puede tardar unos minutos en detectar y detectar los clústeres automáticamente. Si esto sucede mientras realiza una operación VSC, como el aprovisionamiento de un almacén de datos, es posible que experimente una demora.

Configuraciones de MetroCluster y proveedor VASA

VASA Provider admite automáticamente entornos que utilizan configuraciones MetroCluster. El cambio es transparente en los entornos de proveedores de VASA. No es posible añadir directamente al proveedor de VASA.



VASA Provider no incorpora el sufijo "-mc" a los nombres de en el sitio secundario después de una conmutación por sitios.

Configuraciones de MetroCluster y SRA

El SRA no es compatible con las configuraciones de MetroCluster.

Configure el entorno del sistema de almacenamiento de Virtual Storage Console para VMware vSphere

Virtual Storage Console para VMware vSphere ofrece un único mecanismo para detectar sistemas de almacenamiento y configurar las credenciales de almacenamiento. Las

credenciales proporcionan los permisos de ONTAP necesarios para que los usuarios de Virtual Storage Console (VSC) puedan realizar tareas mediante los sistemas de almacenamiento.

Para poder mostrar y gestionar los recursos de almacenamiento, VSC debe detectar los sistemas de almacenamiento. Como parte del proceso de detección, debe suministrar las credenciales de ONTAP para los sistemas de almacenamiento. Estos son los privilegios (o roles) asociados con el nombre de usuario y la pareja de contraseñas que se asignan a cada sistema de almacenamiento. Estas parejas de nombres de usuario y contraseñas utilizan el control de acceso basado en roles (RBAC) de ONTAP y deben configurarse desde ONTAP. No puede cambiar estas credenciales desde VSC. Puede definir roles de RBAC de ONTAP mediante .



Si inicia sesión como administrador, tiene automáticamente todos los privilegios de ese sistema de almacenamiento.

Cuando se añade un sistema de almacenamiento a VSC, debe suministrar una dirección IP para el sistema de almacenamiento, así como el nombre de usuario y la pareja de contraseñas que estén asociados con ese sistema. Se pueden configurar credenciales predeterminadas que VSC utilizará durante el proceso de detección del sistema de almacenamiento, o bien se pueden introducir credenciales manualmente cuando se detecte el sistema de almacenamiento. Los detalles del sistema de almacenamiento que se añaden a VSC se insertan automáticamente en las extensiones que habilitan en la puesta en marcha. No es necesario añadir manualmente el almacenamiento al proveedor VASA y al adaptador de replicación de almacenamiento (SRA). Tanto VSC como SRA admiten la adición de credenciales a nivel de clúster y a nivel de clúster. El proveedor DE VASA de solo admite credenciales en el nivel del clúster para añadir sistemas de almacenamiento.

Si el entorno incluye varias instancias de vCenter Server, cuando se añade un sistema de almacenamiento a VSC desde la página Storage Systems, el cuadro de diálogo Add Storage System muestra un cuadro de diálogo vCenter Server donde puede especificar la instancia de vCenter Server que se debe añadir el sistema de almacenamiento. Si añade un sistema de almacenamiento haciendo clic con el botón derecho en el nombre de un centro de datos, no tiene la opción de especificar una instancia de vCenter Server debido a que el servidor ya está asociado a ese centro de datos.

La detección se realiza de una de las siguientes maneras. En cada caso, debe proporcionar credenciales para todos los sistemas de almacenamiento recién detectados.

- Cuando se inicia el servicio VSC, VSC inicia su proceso de detección automático en segundo plano.
- Puede hacer clic en el botón **REDISCOVER All** de la página Storage Systems, o en un host o centro de datos para seleccionarlo en el menú **acciones** (menú:acciones[NetApp VSC > Actualizar datos de almacenamiento y host]). También puede hacer clic en **DESCUBRIR** en la ficha Introducción de la sección Descripción general.

Todas las funciones de VSC requieren permisos específicos para realizar tareas. Es posible limitar qué pueden hacer los usuarios según las credenciales asociadas con el rol ONTAP. Todos los usuarios que tienen el mismo nombre de usuario del sistema de almacenamiento y la pareja de contraseñas comparten el mismo conjunto de credenciales del sistema de almacenamiento y pueden ejecutar las mismas operaciones.

Establezca las credenciales predeterminadas para los sistemas de almacenamiento

Puede usar Virtual Storage Console para VMware vSphere a fin de configurar credenciales predeterminadas para un sistema de almacenamiento en el vCenter Server.

Antes de empezar

Debe haber seleccionado la instancia de vCenter Server que desea utilizar para crear credenciales predeterminadas.

Acerca de esta tarea

Si se configuran credenciales predeterminadas para sistemas de almacenamiento, (VSC) utiliza estas credenciales para iniciar sesión en un sistema de almacenamiento que VSC acaba de detectar. Si las credenciales predeterminadas no funcionan, debe iniciar sesión manualmente en el sistema de almacenamiento. Adición de soporte para VSC y SRA de credenciales del sistema de almacenamiento en el nivel del clúster o del clúster. Sin embargo, el proveedor de VASA solo funcionará con las credenciales en el nivel del clúster.

Pasos

1. En la página VSC **Home**, haga clic en MENU:Settings[Administrative Settings > Configure Default Credentials for Storage System].
2. En el cuadro de diálogo **credenciales predeterminadas del sistema de almacenamiento**, introduzca el nombre de usuario y la contraseña del sistema de almacenamiento.

Las credenciales de la controladora de almacenamiento se asignan en ONTAP según el nombre de usuario y la pareja de contraseñas. Las credenciales de la controladora de almacenamiento pueden ser la cuenta de administrador o una cuenta personalizada que utilice el control de acceso basado en roles (RBAC).

No puede usar VSC para cambiar los roles asociados con el nombre de usuario y el par de contraseñas de la controladora de almacenamiento. Para modificar o crear un nuevo rol de usuario de ONTAP para usarlo con el dispositivo virtual para VSC, proveedor VASA y SRA, puede usar System Manager.

Consulte la sección «Configuración de funciones y privilegios de usuario» en la *Virtual Storage Console, VASA Provider y Storage Replication Adapter for VMware® vSphere Deployment and Setup Guide for 9.7 Release*.

3. Haga clic en **Aceptar** para guardar las credenciales predeterminadas.

Después de terminar

Si ha actualizado las credenciales del sistema de almacenamiento porque un sistema de almacenamiento ha informado del estado "fallo de autenticación", haga clic en la opción **REDISCOVER ALL** disponible en la página Storage Systems. Al hacerlo, VSC intenta conectarse al sistema de almacenamiento usando las nuevas credenciales.

Añada sistemas de almacenamiento a VSC

Puede añadir manualmente el sistema de almacenamiento a Virtual Storage Console (VSC).

Acerca de esta tarea

Cada vez que inicie (VSC) o seleccione la opción **REDISCOVER All**, VSC detecta automáticamente los sistemas de almacenamiento disponibles.

Pasos

1. Añada un sistema de almacenamiento a VSC usando la página de inicio de VSC:
 - Haga clic en MENU:Storage Systems[Add].
 - Haga clic en MENU:Overview[Getting Started] y, a continuación, haga clic en el botón **ADD** en **Add Storage System**.

2. En el cuadro de diálogo **Add Storage System**, introduzca la dirección IP de administración y las credenciales de ese sistema de almacenamiento.

También puede añadir sistemas de almacenamiento con la dirección IPv6 del clúster o . También puede cambiar los valores predeterminados para TLS y el número de puerto en este cuadro de diálogo.

Cuando añada almacenamiento desde la página VSC **Storage System**, también debe especificar la instancia de vCenter Server donde se ubicará el almacenamiento. El cuadro de diálogo **Add Storage System** proporciona una lista desplegable de las instancias disponibles de vCenter Server. VSC no muestra esta opción si añade almacenamiento a un centro de datos que ya está asociado a una instancia de vCenter Server.

3. Haga clic en **Aceptar** después de haber añadido toda la información necesaria.

Detectar sistemas de almacenamiento y hosts

Cuando se ejecuta por primera vez (VSC) en una instancia de vSphere Client, VSC detecta los hosts ESXi, sus LUN y exportaciones NFS y los sistemas de almacenamiento de NetApp que poseen esos LUN y exportaciones.

Antes de empezar

- Todos los hosts ESXi deben estar encendidos y conectados.
- Todos los que se van a detectar deben estar en ejecución y cada nodo del clúster debe tener al menos una LIF de datos configurada para el protocolo de almacenamiento que se está utilizando (NFS, iSCSI o FC).

Acerca de esta tarea

Puede detectar nuevos sistemas de almacenamiento o actualizar información sobre los sistemas de almacenamiento existentes para obtener la información más reciente sobre la configuración y la capacidad en cualquier momento. También puede modificar las credenciales que utiliza VSC para iniciar sesión en los sistemas de almacenamiento.

Al detectar los sistemas de almacenamiento de, VSC recopila información de los hosts ESXi gestionados por la instancia de vCenter Server.

Pasos

1. En la página Home* de vSphere Client, seleccione **hosts and Clusters**.
2. Haga clic con el botón derecho en el centro de datos deseado y seleccione MENU:NetApp VSC[Update Host and Storage Data].

VSC muestra un cuadro de diálogo de confirmación para informar de que esta operación puede llevar mucho tiempo.

3. Haga clic en **Aceptar**.
4. Seleccione los controladores de almacenamiento detectados que tengan el estado "'fallo de autenticación"' y, a continuación, haga clic en menú:ACCIONES[Modificar].
5. Rellene la información necesaria en el cuadro de diálogo **Modificar sistema de almacenamiento**.
6. Repita los pasos 4 y 5 en todas las controladoras de almacenamiento con el estado «"fallo de autenticación"».

Después de terminar

Una vez completado el proceso de detección, realice lo siguiente:

- Utilice VSC para configurar los ajustes del host ESXi para los hosts que muestran el icono Alerta en la columna **Configuración del adaptador**, la columna **Configuración MPIO** o la columna **Configuración NFS**.
- Proporcione las credenciales del sistema de almacenamiento.

Actualice la pantalla del sistema de almacenamiento

Puede utilizar la función de actualización que ofrece Virtual Storage Console para VMware vSphere para actualizar la información sobre los sistemas de almacenamiento y forzar Virtual Storage Console (VSC) a detectar sistemas de almacenamiento.

Acerca de esta tarea

La opción «relativamente fresco» es útil si ha cambiado las credenciales predeterminadas de los sistemas de almacenamiento después de recibir un error de autenticación. Siempre debe realizar una operación de actualización si ha cambiado las credenciales del sistema de almacenamiento después de que el sistema de almacenamiento haya informado de un ""Estado de fallo de autenticación"". Durante la operación de actualización, VSC intenta conectarse al sistema de almacenamiento usando las nuevas credenciales.

Según la configuración del sistema, esta tarea puede tardar mucho tiempo en completarse.

Pasos

1. En la página VMware vSphere Client **Home**, haga clic en **Storage Systems**.
2. Inicie la actualización:

Si la ubicación es...	Haga clic en...
Consola de almacenamiento virtual	El icono REDISCOVER ALL .
Centro de datos	Haga clic con el botón derecho en el centro de datos y, a continuación, haga clic en MENU:NetApp VSC[Update Host and Storage Data].

3. En el cuadro de diálogo **Actualizar datos de host y almacenamiento**, haga clic en **Aceptar**.

La detección puede tardar unos minutos, en función de la cantidad de hosts y sistemas de almacenamiento del centro de datos. Esta operación de detección funciona en segundo plano.

4. Haga clic en **Aceptar** en el cuadro de diálogo **éxito**.

Funciones de control de acceso basado en roles de vCenter Server en VSC para VMware vSphere

vCenter Server proporciona un control de acceso basado en roles (RBAC) que permite controlar el acceso a los objetos de vSphere. En Virtual Storage Console para VMware vSphere, el control de acceso basado en roles de vCenter Server funciona con ONTAP para determinar qué tareas de VSC puede ejecutar un usuario específico en objetos de un sistema de almacenamiento específico.

Para completar correctamente una tarea, debe tener los permisos de control de acceso basado en roles de vCenter Server correspondientes. Durante una tarea, VSC comprueba los permisos de vCenter Server de un usuario antes de comprobar los privilegios de ONTAP del usuario.

Es posible establecer los permisos de vCenter Server para el objeto raíz (también denominado carpeta raíz). Posteriormente, es posible refinar la seguridad aplicando restricciones a entidades secundarias que no necesitan los mismos permisos.

Componentes de permisos de vCenter Server

El servidor de vCenter reconoce permisos, no privilegios. Cada permiso de vCenter Server consta de tres componentes.

El servidor vCenter tiene los siguientes componentes:

- Uno o más privilegios (el rol)

Los privilegios definen las tareas que un usuario puede realizar.

- Un objeto de vSphere

El objeto es el destino de las tareas.

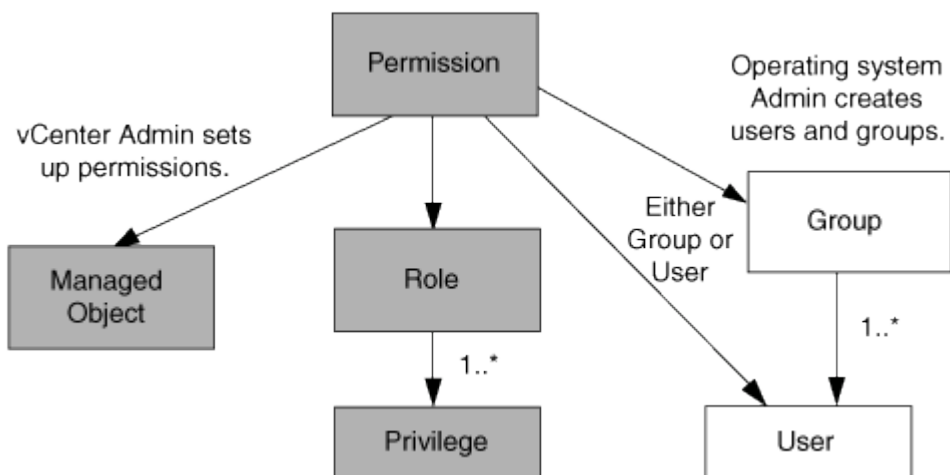
- Un usuario o grupo

El usuario o grupo define quién puede realizar la tarea.

Como se muestra en el siguiente diagrama, debe tener los tres elementos para tener un permiso.



En este diagrama, los cuadros grises indican los componentes que existen en vCenter Server y los recuadros blancos indican componentes que existen en el sistema operativo donde se ejecuta vCenter Server.



Privilegios

Existen dos tipos de privilegios asociados con Virtual Storage Console para VMware vSphere:

- Privilegios nativos de vCenter Server

Estos privilegios vienen con vCenter Server.

- Privilegios específicos de VSC

Estos privilegios se definen para tareas de VSC específicas. Son exclusivos de VSC.

Las tareas de VSC requieren privilegios específicos de VSC y privilegios nativos de vCenter Server. Estos privilegios constituyen el "rol" del usuario. Un permiso puede tener varios privilegios. Estos privilegios corresponden a un usuario que ha iniciado sesión en vCenter Server.



Para simplificar el uso del control de acceso basado en roles de vCenter Server, VSC ofrece varias funciones estándar que contienen todos los privilegios nativos y específicos de VSC necesarios para ejecutar tareas de VSC.

Si cambia los privilegios dentro de un permiso, el usuario asociado a ese permiso debe cerrar sesión y, a continuación, iniciar sesión para activar el permiso actualizado.

Privilegio	Funciones	Tareas
Menú:consola de almacenamiento virtual de NetApp[View]	<ul style="list-style-type: none">• Administrador de VSC• Aprovisionamiento de VSC• Solo lectura de VSC	Todas las tareas específicas de VSC y VASA Provider requieren el privilegio View.
Menu:NetApp Virtual Storage Console[Administración basada en políticas > Gestión] o privilege.nvpfVSC.VASAGroup.com.netapp.nvpf.label > Management	Administrador de VSC	Tareas de VSC y VASA Provider relacionadas con los perfiles de funcionalidad de almacenamiento y la configuración de umbral.

Objetos de vSphere

Los permisos se asocian con objetos de vSphere, como vCenter Server, hosts ESXi, máquinas virtuales, almacenes de datos, centros de datos, y carpetas. Puede asignar permisos a cualquier objeto de vSphere. Según el permiso que se asigna a un objeto de vSphere, vCenter Server determina quién puede ejecutar qué tareas en ese objeto. Para tareas específicas de VSC, los permisos se asignan y validan solo en el nivel de carpeta raíz (vCenter Server), no en ninguna otra entidad. Excepto para la operación del complemento VAAI, donde se validan los permisos en ESXi en cuestión.

Usuarios y grupos

Es posible usar Active Directory (o la máquina local de vCenter Server) para configurar usuarios y grupos de usuarios. A continuación, es posible usar permisos de vCenter Server para otorgar acceso a estos usuarios o grupos con el fin de permitirles ejecutar tareas VSC específicas.



Estos permisos de vCenter Server se aplican a los usuarios de VSC vCenter, no a los administradores de VSC. De forma predeterminada, los administradores de VSC tienen acceso completo al producto y no requieren permisos asignados.

Los usuarios y grupos no tienen roles asignados. Estos obtienen acceso a un rol mediante el permiso de vCenter Server.

Puntos clave sobre la asignación y modificación de permisos para vCenter Server

Hay varios puntos clave que se deben tener en cuenta cuando se trabaja con permisos de vCenter Server. Si una tarea de Virtual Storage Console para VMware vSphere se realiza correctamente puede depender de la ubicación en la que se asignó un permiso o de las acciones que realizó un usuario después de modificar un permiso.

Asignación de permisos

Solo debe configurar permisos de vCenter Server si desea limitar el acceso a los objetos y tareas de vSphere. De lo contrario, puede iniciar sesión como administrador. Este inicio de sesión permite acceder automáticamente a todos los objetos de vSphere.

Donde se asigna un permiso determina las tareas de VSC que puede ejecutar un usuario.

A veces, para garantizar la finalización de una tarea, debe asignar el permiso a un nivel superior, como el objeto raíz. Es así cuando una tarea requiere un privilegio que no se aplica a un objeto de vSphere específico (por ejemplo, un seguimiento de la tarea) o cuando un privilegio requerido se aplica a un objeto que no es vSphere (por ejemplo, un sistema de almacenamiento).

En estos casos, puede configurar un permiso para que sea heredado por las entidades secundarias. También puede asignar otros permisos a las entidades secundarias. El permiso asignado a una entidad hijo siempre anula el permiso heredado de la entidad padre. Esto significa que puede tener permisos para una entidad secundaria como una manera de restringir el ámbito de un permiso que se asignó a un objeto raíz y que la entidad secundaria hereda.



A menos que las políticas de seguridad de la empresa requieran permisos más restrictivos, es recomendable asignar permisos al objeto raíz (también denominado carpeta raíz).

Permisos y objetos que no son de vSphere

El permiso que crea se aplica a un objeto que no sea de vSphere. Por ejemplo, un sistema de almacenamiento no es un objeto de vSphere. Si se aplica un privilegio a un sistema de almacenamiento, debe asignar el permiso que contiene ese privilegio al objeto raíz de VSC porque no hay ningún objeto de vSphere al cual pueda asignarlo.

Por ejemplo, todos los permisos que incluyan un privilegio, como el privilegio VSC "Add/Modify/Skip Storage systems", se deben asignar en el nivel de objetos raíz.

Modificar permisos

Puede modificar un permiso en cualquier momento.

Si cambia los privilegios dentro de un permiso, el usuario asociado con ese permiso debe cerrar la sesión y, a continuación, volver a iniciar la sesión para habilitar el permiso actualizado.

Roles estándar que se incluyen en el dispositivo virtual para VSC, proveedor VASA y SRA

Para simplificar el uso de los privilegios de vCenter Server y el control de acceso basado en roles (RBAC), (VSC) ofrece roles estándar de VSC que permiten ejecutar tareas clave de VSC. También hay un rol de solo lectura que le permite ver la información de VSC,

pero no ejecutar tareas.

Los roles estándar de VSC tienen privilegios específicos requeridos de VSC y los privilegios nativos de vCenter Server necesarios para que los usuarios ejecuten tareas de VSC. Además, los roles están configurados para contar con todos los privilegios necesarios en todas las versiones compatibles de vCenter Server.

El administrador puede asignar estos roles a los usuarios, según sea necesario.



Cuando actualiza VSC a la versión más reciente, los roles estándar se actualizan automáticamente para que funcionen con la nueva versión de VSC.

Para ver los roles estándar de VSC, haga clic en **roles** en la página **Inicio** de vSphere Client.

Los roles que ofrece VSC permiten realizar las siguientes tareas:

Función	Descripción
Administrador de VSC	Ofrece todos los privilegios nativos de vCenter Server y los privilegios específicos de VSC requeridos para ejecutar todas las tareas de VSC.
Solo lectura de VSC	Proporciona acceso de solo lectura a VSC. Estos usuarios no pueden realizar ninguna acción VSC que esté controlada por el acceso.
Aprovisionamiento de VSC	Ofrece todos los privilegios nativos de vCenter Server y los privilegios específicos de VSC necesarios para aprovisionar almacenamiento. Es posible realizar las siguientes tareas: <ul style="list-style-type: none">• Crear nuevos almacenes de datos• Destrucción de almacenes de datos• Ver información sobre los perfiles de funcionalidad del almacenamiento

Directrices para usar roles estándar de VSC

Cuando trabaja con roles estándar de Virtual Storage Console para VMware vSphere, hay ciertas directrices que debe seguir.

No debe modificar directamente los roles estándar. Si lo hace, VSC sobrescribirá los cambios cada vez que actualice VSC. El instalador actualiza las definiciones de rol estándar cada vez que actualiza VSC. Si hace esto, se garantiza que los roles sean actuales para la versión de VSC, así como para todas las versiones compatibles de vCenter Server.

Sin embargo, puede usar los roles estándar para crear roles que se ajusten a su entorno. Para ello, debe copiar el rol estándar de VSC y editar el rol copiado. Al crear un rol nuevo, puede mantener esta función incluso al reiniciar o actualizar el servicio VSC Windows.

Algunas de las formas de utilizar las funciones estándar de VSC incluyen las siguientes:

- Utilice los roles estándar de VSC para todas las tareas de VSC.

En esta situación, los roles estándar ofrecen todos los privilegios que un usuario necesita para realizar las tareas de VSC.

- Combinar roles para expandir las tareas que un usuario puede realizar.

Si los roles estándar de VSC proporcionan demasiada granularidad en el entorno, puede ampliar los roles creando grupos de nivel superior que contengan varias funciones.

Si un usuario tiene que ejecutar otras tareas que no son de VSC y requieren privilegios nativos de vCenter Server adicionales, puede crear una función que incluya esos privilegios y también añadirla al grupo.

- Cree funciones más detalladas.

Si su empresa necesita implementar funciones más restrictivas que las funciones estándar de VSC, puede usar los roles de VSC para crear nuevas funciones.

En este caso, debe clonar los roles de VSC necesarios y editar el rol clonado para que solo tenga los privilegios que requiere el usuario.

Privilegios necesarios para las tareas de VSC

Las diferentes tareas de Virtual Storage Console para VMware vSphere requieren diferentes combinaciones de privilegios específicas de (VSC) y los privilegios nativos de vCenter Server.

Puede encontrar información sobre los privilegios necesarios para las tareas de VSC en el artículo 1032542 de la base de conocimientos de NetApp.

["Cómo configurar RBAC para Virtual Storage Console"](#)

Privilegios a nivel de producto que requiere VSC para VMware vSphere

Para acceder a la interfaz gráfica de usuario de Virtual Storage Console para VMware vSphere, es necesario contar con el privilegio View específico de VSC para el producto asignado en el nivel de objeto de vSphere correspondiente. Si se inicia sesión sin este privilegio, VSC muestra un mensaje de error al hacer clic en el icono de NetApp y no le permite acceder a VSC.

En la siguiente tabla, se describe el privilegio View en el nivel de producto de VSC:

Privilegio	Descripción	Nivel de asignación
Ver	Puede acceder a la interfaz gráfica de usuario de VSC. Este privilegio no le permite realizar tareas en VSC. Para realizar cualquier tarea de VSC, debe tener los privilegios correctos específicos de VSC y nativos de vCenter Server para esas tareas.	<p>El nivel de asignación determina qué porciones de la interfaz de usuario se muestran.</p> <p>Al asignar el privilegio View en el objeto raíz (carpeta), es posible ingresar a VSC haciendo clic en el icono de NetApp.</p> <p>Es posible asignar el privilegio View a otro nivel de objeto de vSphere. No obstante, de esta forma se limitan los menús de VSC que se pueden ver y usar.</p> <p>El objeto raíz es el lugar recomendado para asignar cualquier permiso que contiene el privilegio View.</p>

Control de acceso basado en roles de ONTAP para el dispositivo virtual para VSC, proveedor VASA y SRA

El control de acceso basado en roles de ONTAP permite controlar el acceso a sistemas de almacenamiento específicos y controlar las acciones que un usuario puede ejecutar en esos sistemas de almacenamiento. En Virtual Storage Console para VMware vSphere, el control de acceso basado en roles de ONTAP funciona con el control de acceso basado en roles de vCenter Server para determinar qué tareas de VSC (Virtual Storage Console) puede ejecutar un usuario específico en los objetos de un sistema de almacenamiento específico.

VSC usa las credenciales (nombre de usuario y contraseña) configuradas en VSC para autenticar cada sistema de almacenamiento y determinar qué operaciones de almacenamiento se pueden ejecutar en ese sistema de almacenamiento. VSC usa un conjunto de credenciales para cada sistema de almacenamiento. Estas credenciales determinan qué tareas de VSC se pueden ejecutar en ese sistema de almacenamiento, es decir, las credenciales se aplican a VSC, no a un usuario individual de VSC.

El control de acceso basado en roles de ONTAP se aplica únicamente al acceso a sistemas de almacenamiento y a la ejecución de tareas de VSC relacionadas con el almacenamiento, como el aprovisionamiento de máquinas virtuales. Si no se cuenta con los privilegios de control de acceso basado en roles de ONTAP correspondientes a un sistema de almacenamiento específico, no es posible ejecutar ninguna tarea en un objeto de vSphere que se encuentre alojado en ese sistema de almacenamiento. Es posible utilizar el control de acceso basado en roles de ONTAP junto con los privilegios específicos de VSC para controlar qué tareas de VSC puede ejecutar un usuario:

- Supervisar y configurar objetos de almacenamiento o de vCenter Server que residen en un sistema de almacenamiento
- Aprovisionamiento de objetos de vSphere que residen en un sistema de almacenamiento

El uso de RBAC de ONTAP con los privilegios específicos de VSC ofrece una capa de seguridad orientada al

almacenamiento que puede gestionar el administrador de almacenamiento. Como resultado, dispone de un control de acceso más detallado del que admite RBAC de ONTAP o RBAC de vCenter Server por sí solo. Por ejemplo, con RBAC de vCenter Server, puede permitir que vCenterUserB aprovisiona un almacén de datos con el almacenamiento, mientras impide que vCenterUserA aprovisiona almacenes de datos. Si las credenciales del sistema de almacenamiento para un sistema de almacenamiento específico no admiten la creación de almacenamiento, ni vCenterUserB ni vCenterUserA pueden aprovisionar un almacén de datos en ese sistema de almacenamiento.

Cuando se inicia una tarea VSC, VSC primero comprueba si tiene el permiso correcto de vCenter Server para esa tarea. Si el permiso de vCenter Server no es suficiente para permitir ejecutar la tarea, VSC no tiene que comprobar los privilegios de ONTAP de ese sistema de almacenamiento debido a que no ha superado la comprobación de seguridad inicial de vCenter Server. Como resultado, no podrá acceder al sistema de almacenamiento.

Si el permiso de vCenter Server es suficiente, VSC comprueba los privilegios de RBAC de ONTAP (su rol de ONTAP) asociados con las credenciales del sistema de almacenamiento (el nombre de usuario y la contraseña) Determinar si tiene privilegios suficientes para realizar las operaciones de almacenamiento que requiere esa tarea de VSC en ese sistema de almacenamiento. Si cuenta con los privilegios de ONTAP correctos, puede acceder al sistema de almacenamiento y ejecutar la tarea de VSC. Los roles de ONTAP determinan las tareas de VSC que se pueden ejecutar en el sistema de almacenamiento.

Cada sistema de almacenamiento está asociado con un conjunto de privilegios de ONTAP.

Usar el control de acceso basado en roles de ONTAP y de vCenter Server ofrece los siguientes beneficios:

- Seguridad

El administrador puede controlar qué usuarios pueden realizar qué tareas a nivel de objeto de vCenter Server específico y a nivel de sistema de almacenamiento.

- Información de auditoría

En muchos casos, VSC ofrece un seguimiento de auditoría del sistema de almacenamiento que permite asociar los eventos con el usuario de vCenter Server que aplicó el cambio en el almacenamiento.

- Facilidad de uso

Es posible conservar todas las credenciales de la controladora en un mismo lugar.

Roles de ONTAP recomendados cuando se usa VSC para VMware vSphere

Puede configurar varios roles de ONTAP recomendados para trabajar con la consola de almacenamiento virtual para VMware vSphere y el control de acceso basado en roles (RBAC). Estos roles contienen los privilegios de ONTAP necesarios para ejecutar las operaciones de almacenamiento necesarias que ejecutan las tareas de (VSC).

Para crear roles de usuario nuevos, debe iniciar sesión como administrador en sistemas de almacenamiento que ejecutan ONTAP. Es posible crear roles de ONTAP mediante uno de los siguientes:

- 9.7 o posterior

["Configure los roles y privilegios de usuario"](#)

- Herramienta de creación de usuarios de RBAC para ONTAP (si se usa ONTAP 9.6 o una versión anterior)

Cada rol de ONTAP tiene asociado un nombre de usuario y una pareja de contraseñas que constituyen las credenciales del rol. Si no inicia sesión con estas credenciales, no podrá acceder a las operaciones de almacenamiento que están asociadas con el rol.

Como medida de seguridad, los roles de ONTAP específicos de VSC se ordenan jerárquicamente. Esto significa que la primera función es la más restrictiva y que sólo tiene los privilegios asociados con el conjunto más básico de operaciones de almacenamiento VSC. El siguiente rol incluye sus propios privilegios y todos los privilegios asociados con el rol anterior. Cada puesto adicional resulta menos restrictivo en relación con las operaciones de almacenamiento admitidas.

A continuación, se enumeran algunos de los roles de control de acceso basado en roles de ONTAP recomendados cuando se usa VSC. Después de crear estos roles, es posible asignar los roles a los usuarios que deben realizar tareas relacionadas con el almacenamiento, como el aprovisionamiento de máquinas virtuales.

1. Detección

Este rol le permite añadir sistemas de almacenamiento.

2. Cree almacenamiento

Este rol le permite crear almacenamiento. Este rol también incluye todos los privilegios asociados con el rol de detección.

3. Modificar almacenamiento

Este rol permite modificar almacenamiento. Este rol también incluye todos los privilegios asociados con el rol de detección y creación de almacenamiento.

4. Destruya el almacenamiento

Este rol le permite destruir almacenamiento. Este rol también incluye todos los privilegios asociados con el rol Discovery, el rol Create Storage y el rol Modify Storage.

Si utiliza VASA Provider para ONTAP, también debe configurar un rol de gestión basada en políticas (PBM). Este rol le permite gestionar el almacenamiento mediante políticas de almacenamiento. Esta función requiere que usted también establezca el papel de «recuperación».

Cómo configurar el control de acceso basado en roles de ONTAP para VSC para VMware vSphere

Debe configurar el control de acceso basado en roles de ONTAP en el sistema de almacenamiento si desea utilizar el control de acceso basado en roles con Virtual Storage Console para VMware vSphere (VSC). Es posible crear una o varias cuentas de usuario personalizadas con privilegios de acceso limitados mediante la función RBAC de ONTAP.

VSC y SRA pueden acceder a los sistemas de almacenamiento a nivel de clúster o de. Si va a añadir sistemas de almacenamiento en el nivel del clúster, debe proporcionar las credenciales del usuario administrador para proporcionar todas las funcionalidades necesarias. Si va a añadir sistemas de almacenamiento agregando detalles directamente, debe ser consciente de que el usuario "vsadmin" no tiene

todos los roles y capacidades requeridos para realizar ciertas tareas.

EL proveedor DE VASA puede acceder a los sistemas de almacenamiento únicamente en el nivel del clúster. Si se requiere un proveedor de VASA para una controladora de almacenamiento en particular, debe añadir el sistema de almacenamiento a VSC en el nivel del clúster aunque utilice VSC o SRA.

Para crear un usuario nuevo y conectar un clúster o un a VSC, proveedor VASA y SRA, debe realizar lo siguiente:

- Cree un administrador de clúster o un rol de administrador



Es posible usar uno de los siguientes para crear estos roles:

- ONTAP System Manager 9.7 o posterior

"Configure los roles y privilegios de usuario"

- Herramienta de creación de usuarios de RBAC para ONTAP (si se usa ONTAP 9.6 o una versión anterior)

"Herramienta RBAC User Creator para VSC, proveedor VASA y Storage Replication Adapter 7.0 para VMware vSphere"

- Cree usuarios con el rol asignado y el conjunto de aplicaciones adecuado mediante ONTAP

Es necesario contar con estas credenciales del sistema de almacenamiento para configurar los sistemas de almacenamiento para VSC. Puede configurar sistemas de almacenamiento para VSC introduciendo las credenciales en VSC. Cada vez que inicie sesión en un sistema de almacenamiento con estas credenciales, tendrá permisos sobre las funciones VSC que haya configurado en ONTAP al crear las credenciales.

- Añada el sistema de almacenamiento a VSC y proporcione las credenciales del usuario que acaba de crear

Roles de VSC

VSC clasifica los privilegios de ONTAP en el siguiente conjunto de funciones de VSC:

- Detección

Permite la detección de todas las controladoras de almacenamiento conectadas

- Cree almacenamiento

Permite la creación de volúmenes y número de unidad lógica (LUN).

- Modificar almacenamiento

Permite redimensionar y deduplicar los sistemas de almacenamiento

- Destruya el almacenamiento

Permite la destrucción de volúmenes y LUN

Roles del proveedor DE VASA

Solo puede crear gestión basada en políticas en el nivel de clúster. Este rol permite la gestión basada en políticas del almacenamiento mediante perfiles de capacidades de almacenamiento.

Roles SRA

El SRA clasifica los privilegios del ONTAP en un rol DE SAN o NAS a nivel de clúster o de. Esto permite a los usuarios ejecutar operaciones de SRM.



Debe consultar los artículos de la base de conocimientos si desea configurar manualmente roles y privilegios mediante comandos ONTAP.

- ["Configuración de RBAC de ONTAP para VSC, VASA y SRA 7.0"](#)
- ["Implementación de todos los comandos para VSC y SRA en nivel de SVM"](#)

VSC realiza una validación de privilegios inicial de los roles de control de acceso basado en roles de ONTAP cuando se añade el clúster a VSC. Si ha añadido una IP de almacenamiento directo, VSC no realizará la validación inicial. VSC comprueba y aplica los privilegios más adelante en el flujo de trabajo de las tareas.

Configure los roles y privilegios de usuario

Es posible configurar roles de usuario nuevos para gestionar los sistemas de almacenamiento mediante el archivo JSON que se proporciona con el dispositivo virtual para VSC, proveedor VASA y SRA y System Manager de ONTAP.

Antes de empezar

- Debe haber descargado el archivo de privilegios de ONTAP del dispositivo virtual para VSC, proveedor VASA y SRA con
`https://{virtual_appliance_IP}:9083/vsc/config/VSC_ONTAP_User_Privileges.zip`.
- Debe haber configurado ONTAP 9.7 System Manager.
- Inició sesión con privilegios de administrador del sistema de almacenamiento.

pasos

1. Descomprima el archivo descargado
`https://{virtual_appliance_IP}:9083/vsc/config/VSC_ONTAP_User_Privileges.zip`
archivo.
2. Acceda a ONTAP System Manager.
3. Haga clic en **CLUSTER > Configuración > usuarios y roles**.
4. Haga clic en **Agregar usuario**.
5. En el cuadro de diálogo **Agregar usuario**, seleccione **Productos de virtualización**.
6. Haga clic en **examinar** para seleccionar y cargar el archivo JSON de privilegios de ONTAP.

El campo DE PRODUCTO se completa automáticamente.

7. Seleccione la capacidad necesaria en el menú desplegable **CAPACIDAD DEL PRODUCTO**.

El campo **ROL** se rellena automáticamente en función de la capacidad del producto seleccionada.

8. Introduzca el nombre de usuario y la contraseña necesarios.
9. Seleccione los privilegios (Discovery, Create Storage, Modify Storage, Destroy Storage) necesarios para el usuario y, a continuación, haga clic en **Add**.

Resultados

Se añaden el nuevo rol y el usuario, y se pueden ver los privilegios detallados en el rol que se configuró.

Configure Storage Replication Adapter para la recuperación ante desastres

Si desea configurar vCenter Server para la recuperación ante desastres, debe habilitar el adaptador de replicación de almacenamiento (SRA) después de implementar el dispositivo virtual para Virtual Storage Console (VSC), el proveedor VASA y el adaptador de replicación de almacenamiento (SRA). La puesta en marcha del dispositivo virtual instala VSC de manera predeterminada. Debe habilitar el SRA para vCenter Server después de la implementación del dispositivo virtual.

Información relacionada

[Habilite Storage Replication Adapter](#)

Configurar Storage Replication Adapter para entorno SAN

Debe configurar los sistemas de almacenamiento antes de ejecutar Storage Replication Adapter (SRA) para el administrador de recuperación del sitio (SRM).

Antes de empezar

Debe haber instalado los siguientes programas en el sitio protegido y en el sitio de recuperación:

- SRM

La documentación sobre la instalación de SRM se encuentra en el sitio de VMware.

["Documentación de VMware Site Recovery Manager"](#)

- SRA.

El adaptador está instalado en SRM.

Pasos

1. Compruebe que los hosts ESXi principales están conectados a los LUN del sistema de almacenamiento principal en el sitio protegido.
2. Compruebe que LAS LUN se encuentran en iGroups que tienen el **ostype** opción establecida en *vmware* en el sistema de almacenamiento principal.
3. Comprobar que los hosts ESXi del sitio de recuperación tienen la conectividad FC o iSCSI adecuada con .

Puede hacerlo ya sea comprobando que los hosts ESXi tengan LUN locales conectados en o mediante el `fcv show initiators` o el `iscsi show initiators` comando en el .

Configurar el adaptador de replicación de almacenamiento para el entorno NAS

Debe configurar los sistemas de almacenamiento antes de ejecutar Storage Replication Adapter (SRA) para VMware vCenter Site Recovery Manager (SRM).

Antes de empezar

Debe haber instalado los siguientes programas en el sitio protegido y en el sitio de recuperación:

- SRM

Puede encontrar documentación sobre la instalación de SRM en el sitio de VMware.

["Documentación de VMware Site Recovery Manager"](#)

- SRA.

El adaptador se instala en el SRM y en el servidor SRA.

Pasos

1. Compruebe que los almacenes de datos del sitio protegido contienen máquinas virtuales registradas en vCenter Server.
2. Compruebe que los hosts ESXi del sitio protegido han montado los volúmenes NFS exporta desde .
3. Compruebe que las direcciones válidas, como la dirección IP, el nombre de host o el FQDN en el que están presentes las exportaciones NFS, se especifican en el campo **direcciones NFS** cuando se utiliza el asistente **Array Manager** para agregar matrices a SRM.
4. Utilice la `ping` Comando en cada host ESXi del sitio de recuperación para comprobar que el host tiene un puerto de VMkernel que puede acceder a las direcciones IP que se utilizan para utilizar las exportaciones NFS del .

["Soporte de NetApp"](#)

La configuración del adaptador de replicación de almacenamiento para entornos de gran escala

Debe configurar los intervalos de tiempo de espera de almacenamiento de acuerdo con la configuración recomendada para que el adaptador de replicación de almacenamiento (SRA) funcione de forma óptima en entornos con un alto nivel de escalado.

Configuración del proveedor de almacenamiento

- Debe aumentar el valor de `StorageProvider.resignatureTimeout` ajuste de 900 segundos a 12000 segundos.
- Debe habilitar el `StorageProvider.autoResignatureMode` opción.

Consulte la documentación de VMware para obtener más información sobre cómo modificar la configuración del proveedor de almacenamiento.

["Documentación de VMware vSphere: Cambie la configuración del proveedor de almacenamiento"](#)

Configuración de almacenamiento

Debe configurar el valor de `storage.commandTimeout` intervalo de tiempo de espera para entornos con gran escala a 12,000 segundos.



El intervalo de tiempo de espera especificado es el valor máximo. No es necesario esperar hasta que se llegue al tiempo de espera máximo. La mayoría de comandos terminan dentro del intervalo máximo de tiempo de espera establecido.

["Respuesta 1001111 de la base de conocimientos de NetApp: Adaptador de replicación de almacenamiento de NetApp 4.0/7.X para la guía de ajuste de tamaño de ONTAP"](#)

La documentación de VMware sobre la modificación de la configuración del proveedor DE SAN tiene más información.

["Documentación de VMware Site Recovery Manager: Cambiar la configuración de almacenamiento"](#)

Solucione problemas con el dispositivo virtual para VSC, proveedor VASA y SRA

Si encuentra un comportamiento inesperado durante la instalación o la configuración del dispositivo virtual para Virtual Storage Console (VSC), el proveedor VASA y el adaptador de replicación del almacenamiento (SRA), puede seguir los procedimientos específicos para solucionar problemas a fin de identificar y resolver la causa de tales problemas.

Borre los paquetes de plugins descargados en caché de vSphere

Si los plugins no se actualizan automáticamente después de implementar o actualizar el dispositivo virtual para VSC, proveedor VASA y SRA, debe borrar los paquetes de plugins de descarga almacenados en caché en el explorador y en vCenter Server para resolver problemas de plugins de vCenter Server.

Pasos

1. Cierre la sesión en el cliente web de vSphere o en vSphere Client existente.
2. Quite la caché del explorador.
3. Quite los paquetes de plugins almacenados en caché de vSphere Client.

Si está usando...	Realice lo siguiente...
Servidor Windows vCenter	<p>Quite las siguientes carpetas com.netapp.vasa.vvol.webclient-x.x.x.xxxx, com.netapp.nvpf.webclient-x.x.x.xxxx y com.netapp.vsch5-x.x.x.xxxx que se encuentran en:</p> <ul style="list-style-type: none"> • Ruta de vSphere Web Client: C:\ProgramData\VMware\vCenterServer\cfg\vsphere-client\vc-packages\vsphere-client-Serenity • Ruta de vSphere Client (HTML5): C:\ProgramData\VMware\vCenterServer\cfg\vsphere-ui\vc-packages\vsphere-client-Serenity
VCSA	<ol style="list-style-type: none"> SSH en el dispositivo VCSA. Cambie los directorios al directorio de extensiones de la interfaz de usuario del cliente web de vCenter mediante <code>cd /etc/vmware/vsphere-client/vc-packages/vsphere-client-serenity</code> Elimine los paquetes de plugins almacenados en caché mediante los comandos: <ul style="list-style-type: none"> ° <code>rm -rf com.netapp.vasa.vvol.webclient-x.x.x.xxxx</code> ° <code>rm -rf com.netapp.nvpf.webclient-x.x.x.xxxx</code> ° <code>rm -rf com.netapp.vsch5-x.x.x.xxxx</code> Cambie los directorios al directorio de extensiones de la interfaz de usuario del cliente de vCenter (HTML5) mediante <code>cd /etc/vmware/vsphere-ui/vc-packages/vsphere-client-serenity</code> Elimine los paquetes de plugins almacenados en caché mediante los comandos: <ul style="list-style-type: none"> ° <code>rm -rf com.netapp.vasa.vvol.webclient-x.x.x.xxxx</code> ° <code>rm -rf com.netapp.nvpf.webclient-x.x.x.xxxx</code> ° <code>rm -rf com.netapp.vsch5-x.x.x.xxxx</code>

4. Inicie sesión en vSphere y reinicie vSphere Web Client y los servicios de vSphere Client mediante los siguientes comandos:

- ° `service-control --stop vsphere-client vsphere-ui`
- ° `service-control --start vsphere-client vsphere-ui`

La desinstalación no quita los roles estándar de VSC

Cuando desinstala Virtual Storage Console para VMware vSphere (VSC), los roles estándar de VSC permanecen intactos. Este es el comportamiento esperado y no afecta al rendimiento de VSC o a la capacidad de actualizar a una nueva versión de VSC. Puede eliminar manualmente estos roles, si es necesario.

Aunque la operación de desinstalación no quita los roles de VSC, la operación de desinstalación elimina los nombres localizados de los privilegios específicos de VSC y les añade el siguiente prefijo: "XXX Missing Privilege". Por ejemplo, si abre el cuadro de diálogo vSphere **Edit role** después de instalar VSC, verá los privilegios específicos de VSC como.

Este comportamiento ocurre porque vCenter Server no proporciona una opción para quitar privilegios.

Cuando se vuelve a instalar VSC o se actualiza a una versión más reciente de VSC, se restauran todos los roles estándar de VSC y los privilegios específicos de VSC.

Archivos de registro de Virtual Storage Console y VASA Provider

Puede comprobar los archivos de registro en `/opt/netapp/vscserver/log` directorio y la `/opt/netapp/vpserver/log` directorio cuando se encuentran errores.

Los siguientes tres archivos de registro pueden ser útiles para identificar problemas:

- `cxfl.log`, Que contiene información acerca del tráfico API hacia y desde VASA Provider
- `kaminoPrefs.xml`, Que contiene información acerca de la configuración de VSC
- `vvolvlp.log`, Que contiene toda la información de registro acerca de VASA Provider

El menú de mantenimiento del dispositivo virtual para Virtual Storage Console (VSC), el proveedor VASA y el adaptador de replicación de almacenamiento (SRA) permite establecer diferentes niveles de registro para cumplir sus requisitos. Se encuentran disponibles los siguientes niveles de registro:

- Información
- Depurar
- Error
- Traza

Al establecer los niveles de registro, se actualizan los siguientes archivos:

- Servidor VSC: `kamino.log` y `vvolvlp.log`
- Servidor de proveedor de VASA: `vvolvlp.log`, `error.log`, y `netapp.log`

Además, la página de la interfaz de línea de comandos (CLI) web del proveedor VASA contiene las llamadas

API que se realizaron, los errores que se devolvió y varios contadores relacionados con el rendimiento. Puede encontrar la página web CLI en `https://<IP_address_or_hostname>:9083/stats`.

Los servicios de VSC y VASA Provider se reinician en entornos de gran escala

Problema

Es posible que el dispositivo virtual para VSC, el proveedor VASA y el SRA no funcionen de forma óptima en un entorno altamente escalado y puede que note problemas como los servicios de VSC y VASA Provider que se reinician frecuentemente.

Acción correctiva

Modifique los requisitos de memoria RAM y de la pila del dispositivo virtual para VSC, VASA Provider y SRA.

https://kb.netapp.com/Advice_and_Troubleshooting/Data_Storage_Software/Virtual_Storage_Console_for_VMware_vSphere/tune_memory_settings_of_VM_VSC%2C_VASA_Provider%2C_and_SRA_for_scale_and_performance

Configure el proveedor de VASA para que funcione con SSH

Puede configurar VASA Provider para que use SSH a fin de garantizar el acceso seguro mediante la configuración del dispositivo virtual para Virtual Storage Console (VSC), el proveedor VASA y el adaptador de replicación de almacenamiento (SRA).

Acerca de esta tarea

Al configurar SSH, debe iniciar sesión como el usuario de mantenimiento. Esto se debe a que se deshabilitó el acceso raíz al proveedor VASA. Si utiliza otras credenciales de inicio de sesión, no puede usar SSH para acceder al proveedor de VASA.

Pasos

1. Desde vCenter Server, abra una consola al dispositivo virtual para VSC, proveedor VASA y SRA.
2. Inicie sesión como el usuario de mantenimiento.
3. Introduzca 3 Para seleccionar **Configuración del sistema**.
4. Introduzca 6 Para seleccionar **Activar acceso SSH**.
5. Introduzca `y` en el cuadro de diálogo de confirmación.

Configure el dispositivo virtual para VSC, proveedor VASA y SRA de modo que use SSH para el acceso diag remoto

Puede configurar el dispositivo virtual para Virtual Storage Console (VSC), el proveedor VASA y el adaptador de replicación de almacenamiento (SRA) para habilitar el acceso SSH para el usuario de diagnóstico.

Antes de empezar

La extensión del proveedor de VASA debe estar habilitada para la instancia de vCenter Server.

Acerca de esta tarea

El uso de SSH para acceder al usuario diag tiene las siguientes limitaciones:

- Solo se le permite un inicio de sesión por activación de SSH.
- El acceso SSH al usuario de diagnóstico se deshabilita cuando se produce alguna de las siguientes situaciones:
 - La hora caduca.

La sesión de inicio de sesión solo será válida hasta la medianoche del día siguiente.

- Inicie sesión como usuario diag de nuevo con SSH.

Pasos

1. Desde vCenter Server, abra una consola al proveedor VASA.
2. Inicie sesión como usuario de maint.
3. Introduzca 4 Para seleccionar **Soporte y Diagnóstico**.
4. Introduzca 3 Para seleccionar **Activar el acceso a diagnósticos remotos**.
5. Introduzca y En el cuadro de diálogo **confirmación** para activar el acceso a diagnóstico remoto.
6. Introduzca una contraseña para el acceso de diagnóstico remoto.

Se produce un error en la instalación de SRA con un script

Problema

La instalación del adaptador de replicación de almacenamiento (SRA) en Windows 2008 R2 genera un error de credenciales no válido.

Causa

El error puede ocurrir debido a que se habilitan diferentes versiones de la seguridad de la capa de transporte (TLS) en el dispositivo virtual para VSC, proveedor VASA y SRA y Windows 2008 R2.

Acción correctiva

Si intenta instalar SRA en Windows 2008 R2, debe habilitar TLSv1.0 para el dispositivo virtual para VSC, proveedor VASA y SRA con los siguientes pasos en la consola de mantenimiento:

1. Inicie sesión en la consola de mantenimiento utilizando las credenciales de usuario «mant».
2. En el menú principal, seleccione **1** para el menú **Configuración de la aplicación**.
3. Introduzca **13** en el menú **Configuración de la aplicación** para seleccionar **Activar el protocolo TLS** en el menú **Configuración de la aplicación**.
4. Seleccione **TLSv1** en la lista de protocolos TLS.

Los servicios de VSC y VASA Provider se reinician y TLSv1.0 está habilitado.

También puede habilitar TLSv1.2 en Windows 2008 R2.

El SRA no funciona de forma óptima en un entorno muy escalado

Problema

El SRA no funciona de forma óptima en un entorno muy escalado (si se ejecutan límites máximos especificados por VMware como 250 PGS, 250 RPS, 5000 VM) y es posible que note problemas como un error de tiempo de espera o un tiempo de espera de ONTAP.

Acción correctiva

Debe modificar los intervalos de tiempo de espera.

"La configuración del adaptador de replicación de almacenamiento para entornos de gran escala"



También se puede modificar la configuración de la memoria para el escalado y el rendimiento de su dispositivo virtual para VSC, proveedor VASA y SRA en configuraciones a gran escala.

https://kb.netapp.com/Advice_and_Troubleshooting/Data_Storage_Software/Virtual_Storage_Console_for_VMware_vSphere/tune_memory_settings_of_VM_VSC%2C_VASA_Provider%2C_and_SRA_for_scale_and_performance

No se puede instalar el plugin SRA

Problema

Durante la instalación del complemento Storage Replication Adapter (SRA), el sistema se detiene en la pantalla de dirección IP del servidor y contraseña con el siguiente mensaje de error: "las credenciales introducidas no son válidas. Introduzca un nombre de host y una contraseña válidos."

Causa

El error puede producirse por uno de los siguientes motivos:

- Introdujo credenciales de administrador incorrectas.
- La configuración del proxy WinHTTP es incorrecta.

Acción correctiva

- Compruebe sus credenciales de administrador.
- El artículo de la base de conocimientos tiene más información acerca de cómo resolver problemas con la configuración de proxy WinHTTP.

"Respuesta 1005074 de la base de conocimientos de NetApp: La instalación del complemento de cliente de SRA 4.0P1 (netapp_sra_4.0P1_ontap_64bit.msi) no responde en la pantalla de IP de servidor y contraseña"

El adaptador de replicación de almacenamiento de NetApp para ONTAP no aparece en el dispositivo Site Recovery Manager

Problema

El adaptador de replicación de almacenamiento (SRA) no aparece en la interfaz del dispositivo del administrador de recuperación del sitio (SRM) después de cargar y configurar el SRA.

Causa

No se muestra ningún error cuando se utilizan credenciales de SRA incorrectas (nombre de usuario o contraseña) para configurar el SRA mediante el siguiente comando.

```
perl command.pl -I <sra-server-ip> <vp_username> <vp_passwd>
```

Acción correctiva

Actualice los detalles de configuración del SRA con el siguiente comando: `perl command.pl -U <sra-server-ip> <vp_username> <vp_passwd>`

Error al poner en marcha nuevos dispositivos virtuales para VSC, proveedores VASA y SRA

Problema

Aparece el registro de errores "'Herramientas de vmware OVF vCenter no se encuentra la configuración de vCenter'" durante la puesta en marcha nueva del dispositivo virtual para VSC, proveedor VASA y SRA cuando se utiliza una dirección de vCenter Server IPv4 no válida.

Causa

El dispositivo virtual para VSC, proveedor VASA y SRA admite direcciones IPv4 e IPv6. Si el usuario proporciona una dirección IPv4 para vCenter Server que no está disponible en la red y no se proporciona ninguna dirección IPv6, estos mensajes de registro se muestran en la consola de mantenimiento.

Acción correctiva

Debe realizar lo siguiente para eliminar el error:

1. Inicie sesión en la consola de mantenimiento.
2. Acceder al shell de diagnóstico.
3. Cambiar el usuario de «diag» a «root» utilizando `sudo sucomando`.
4. Edite el archivo de interfaz con vi Editor `vi /etc/network/interface`.
5. Retire la entrada de «'inet6'».
6. Guarde el archivo y reinicie el dispositivo virtual para VSC, proveedor VASA y SRA.

Tras reiniciar el dispositivo virtual, no se producen mensajes de error.

Información de copyright

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

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

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

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

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

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

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

Información de la marca comercial

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