



# **Configure el entorno de Virtual Storage Console para VMware vSphere**

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/reference-esx-host-values-set-by-vsc-for-vmware-vsphere.html> on March 21, 2024. Always check docs.netapp.com for the latest.

# Tabla de contenidos

- Configure el entorno de Virtual Storage Console para VMware vSphere ..... 1
  - Configure los valores de multivía y de tiempo de espera del servidor ESXi ..... 1
  - Regenere un certificado SSL para Virtual Storage Console ..... 7
  - Requisitos para registrar VSC en varios entornos de vCenter Server..... 7
  - Configure los archivos de preferencias de VSC ..... 8
  - Habilite el montaje del almacén de datos en diferentes subredes..... 10
  - Acceda a las opciones de la consola de mantenimiento del dispositivo virtual para VSC, proveedor VASA y SRA ..... 11
  - Cambie la contraseña del administrador ..... 13
  - Configure la alta disponibilidad del dispositivo virtual para VSC, proveedores VASA y SRA ..... 13
  - Configuraciones de MetroCluster compatibles con el dispositivo virtual para VSC, proveedor VASA y SRA ..... 15

# 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.

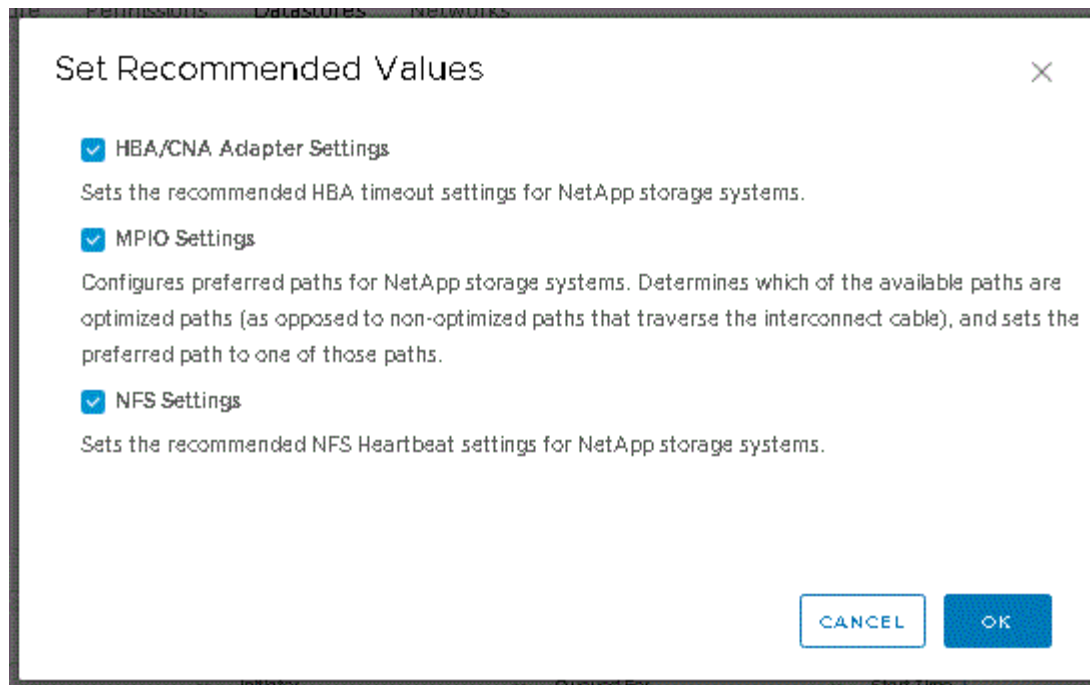
### Acerca de esta tarea

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.HardwaracceleratedLocking**

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://&lt;appliance_ip&gt;:8143/vsc/public/writable/linux_gos_timeout-install.iso</code>	<code>https://&lt;appliance_ip&gt;:8143/vsc/public/writable/linux_gos_timeout_190-install.iso</code>
Windows	<code>https://&lt;appliance_ip&gt;:8143/vsc/public/writable/windows_gos_timeout.iso</code>	<code>https://&lt;appliance_ip&gt;:8143/vsc/public/writable/windows_gos_timeout_190.iso</code>
Solaris	<code>https://&lt;appliance_ip&gt;:8143/vsc/public/writable/solaris_gos_timeout-install.iso</code>	<code>https://&lt;appliance_ip&gt;: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"><li>• 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.</li><li>• 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.</li></ul>
IPv4	<ul style="list-style-type: none"><li>• El aprovisionamiento se realiza utilizando la LIF de datos IPv4 en el seleccionado .</li><li>• 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 .</li></ul>
IPv6	<ul style="list-style-type: none"><li>• El aprovisionamiento se realiza utilizando la LIF de datos IPv6 en el seleccionado .</li><li>• 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 .</li></ul>

# 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**

## 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 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.

## 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.