



Conceptos

ONTAP tools for VMware vSphere 9.12

NetApp
December 19, 2023

Tabla de contenidos

- Conceptos 1
 - Descripción general de las herramientas de ONTAP 1
 - Configuraciones del proveedor VASA para vVols 2
 - Configure la configuración de la recuperación ante desastres 4
 - Control de acceso basado en roles 4
 - Configurar la alta disponibilidad para las herramientas de ONTAP 14
 - Configuraciones de MetroCluster compatibles con las herramientas de ONTAP 15

Conceptos

Descripción general de las herramientas de ONTAP

Las herramientas de ONTAP para VMware vSphere permiten gestionar su ciclo de vida de extremo a extremo para máquinas virtuales en entornos VMware que usan los sistemas de almacenamiento de NetApp. Permite a los administradores gestionar el almacenamiento desde el servidor de vCenter directamente y, por tanto, simplifica la gestión de datos y el almacenamiento para entornos VMware.

Las herramientas de ONTAP se integran con vSphere Client y permiten utilizar servicios de inicio de sesión único (SSO). En un entorno con varias instancias de vCenter Server, cada instancia de vCenter Server que desee gestionar debe tener su propia instancia registrada de las herramientas de ONTAP.

Cada componente de las herramientas de ONTAP ofrece funcionalidades para ayudarle a gestionar su almacenamiento de forma más eficiente.

La herramienta del complemento remoto de VMware vSphere Client está diseñada para integrar la funcionalidad del plugin en vSphere Client sin tener que ejecutarse dentro de vCenter Server. Esto ofrece aislamiento de complementos y permite la escalabilidad horizontal de complementos que funcionan en entornos vSphere grandes.

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 de VSC, que tanto el proveedor de SRA como VASA puedan aprovechar
- Aprovechne 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 de NetApp

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. Pero puede descargar el paquete de instalación del plugin y obtener las instrucciones de instalación del plugin en el sitio de soporte de NetApp.

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. Las herramientas de ONTAP cuentan con VASA Provider integrado con VSC. EL proveedor DE VASA 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

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 utilizar la replicación basada en cabina (ABR) para sitios protegidos y sitios de recuperación para la recuperación ante desastres en caso de un fallo.

Información relacionada

["Soporte de NetApp"](#)

Configuraciones del proveedor VASA para vVols

Es posible usar VASA Provider para ONTAP para crear y gestionar VMware Virtual Volumes (vVols). Puede aprovisionar, editar, montar y eliminar un almacén de datos vVols. También puede agregar almacenamiento al almacén de datos vVols o quitar almacenamiento del almacén de datos vVols. para proporcionar mayor flexibilidad. Puede aprovisionar y gestionar cada máquina virtual y el VMDK relacionado.

Un almacén de datos vVols consta de uno o varios volúmenes FlexVol dentro de un contenedor de almacenamiento (también llamado almacenamiento de respaldo). Un equipo virtual puede propagarse por un almacén de datos vVols o varios almacenes de datos vVols.

Si bien puede crear un almacén de datos vVols que tenga varios volúmenes FlexVol, todos los volúmenes FlexVol dentro del contenedor de almacenamiento deben usar el mismo protocolo (NFS, iSCSI, FCP o NVMe/FC) y las mismas máquinas virtuales de almacenamiento (SVM).

No necesita tener conocimientos detallados del almacenamiento subyacente. Por ejemplo, no es necesario identificar un volumen FlexVol específico para que contenga el almacenamiento. Después de añadir volúmenes FlexVol al almacén de datos vVols, el contenedor de almacenamiento gestiona los requisitos de almacenamiento y evita que se produzcan situaciones durante el aprovisionamiento de la máquina virtual

donde VMware se aprovisionó a un volumen de respaldo sin capacidad.



Se recomienda incluir varios volúmenes FlexVol en un almacén de datos vVols para obtener rendimiento y flexibilidad. Dado que los volúmenes FlexVol tienen restricciones en el número de LUN que limitan el número de equipos virtuales, incluidos varios volúmenes FlexVol, le permiten almacenar más equipos virtuales en su almacén de datos vVols.

Como parte del proceso de instalación, debe especificar un perfil de capacidad de almacenamiento para el almacén de datos vVols que va a crear. Es posible seleccionar uno o varios perfiles de funcionalidad de almacenamiento del proveedor VASA para un almacén de datos vVols. También puede especificar un perfil de funcionalidad de almacenamiento predeterminado para todos los almacenes de datos vVols que se creen automáticamente en ese contenedor de almacenamiento.

VASA Provider crea diferentes tipos de vVols durante el aprovisionamiento de máquinas virtuales o la creación de VMDK, según sea necesario.

- **Config**

VMware vSphere utiliza este almacén de datos vVols para almacenar información de configuración.

En implementaciones SAN (en bloques), el almacenamiento es un LUN de 4 GB.

En una implementación de NFS, se trata de un directorio que contiene archivos de configuración de equipos virtuales, como el archivo vmx y punteros a otros almacenes de datos vVols.

- **Datos**

Este vVols contiene información del sistema operativo y archivos de usuario.

En implementaciones SAN, este es un LUN que tiene el tamaño del disco virtual.

En una implementación NFS, este es un archivo que tiene el tamaño del disco virtual.

Para cada vVols de datos NFS aprovisionado en clústeres ONTAP 9.8 y posteriores, todos los archivos VMDK están registrados para supervisar métricas de rendimiento como IOPS, rendimiento y latencia.

- **Swap**

Este vVols se crea cuando la máquina virtual está encendida y se elimina cuando la máquina virtual está apagada.

En implementaciones DE SAN, este es un LUN del tamaño de la memoria virtual.

En una implementación de NFS, se trata de un archivo que tiene el tamaño de la memoria virtual.

- **Memoria**

Este vVols se crea si se selecciona la opción Memory snapshots (instantáneas de memoria) al crear la instantánea de VM.

En implementaciones DE SAN, este es un LUN del tamaño de la memoria virtual.

En una implementación de NFS, se trata de un archivo que tiene el tamaño de la memoria virtual.

Configure la configuración de la recuperación ante desastres

Es posible crear y gestionar la configuración de recuperación de desastres en vCenter Server junto con Site Recovery Manager (SRM) de VMware.

El proveedor DE VASA ahora viene integrado con las funcionalidades del adaptador de replicación de almacenamiento (SRA). Si ha configurado almacenes de datos vVols en el centro de datos, para la recuperación de almacenes de datos vVols, no es necesario instalar SRA por separado para la recuperación ante desastres. En Site Recovery Manager (SRM), debe emparejar los sitios protegidos y de recuperación. Después de que se haya producido el emparejamiento de sitios, la próxima parte de la configuración de SRM implica configurar un par de cabinas que permite que SRM se comunique con el sistema de almacenamiento para detectar dispositivos y replicación de dispositivos. Para poder configurar el par de matrices, primero debe crear un par de sitios en SRM.

Esta versión de herramientas de ONTAP le ofrece la opción de utilizar una configuración de SnapMirror síncrona para la recuperación ante desastres.



El administrador de recuperación de sitio de VMware (SRM) no usa el SRA para gestionar la recuperación ante desastres de los almacenes de datos vVols. En su lugar, VASA Provider se utiliza para el control de replicación y conmutación al nodo de respaldo de almacenes de datos vVols en clústeres de ONTAP 9.7 y posteriores.

Consulte "[Habilite Storage Replication Adapter](#)" sección del procedimiento.

activación de la función quick_resync

Puede activar el indicador QUICK_RESINNC para realizar la operación de reprotcción y restauración en SRA. Esto solo se aplica a los almacenes de datos respaldados por volúmenes con relación asíncrona con SnapMirror. la marca quick_resync permite que el tiempo de resincronización sea más rápido del volumen de destino, ya que la resincronización no incurre en sobrecarga de eficiencia del almacenamiento antes de la transferencia de nuevos datos. Quick_resync no está habilitado de forma predeterminada. Se recomienda activar el indicador quick_resync:

- Cuando el origen de la resincronización no tiene habilitada la eficiencia del volumen.
- Cuando se reduce el tiempo de resincronización, es más importante que conservar toda la eficiencia del almacenamiento posible en la red.

Siga estos pasos para activar el indicador QUICK_REINNC:

Pasos

1. Inicie sesión en el panel de control en <https://<IP address>:9083> y haga clic en Interfaz CLI basada en web.
2. Ejecute el comando `vp updateconfig -key=snapmirror.quick.resync.enabled -value=true`.
3. Ejecute el comando `vp reloadconfig`.

Control de acceso basado en roles

Información general sobre el control de acceso basado en roles en las herramientas de ONTAP

VCenter Server proporciona un control de acceso basado en roles (RBAC) que permite controlar el acceso a los objetos de vSphere. En las herramientas de ONTAP® para VMware vSphere, el control de acceso basado en roles de vCenter Server funciona con el control de acceso basado en roles de ONTAP para determinar qué tareas de herramientas de ONTAP puede realizar 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, las herramientas de ONTAP comprueban 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.

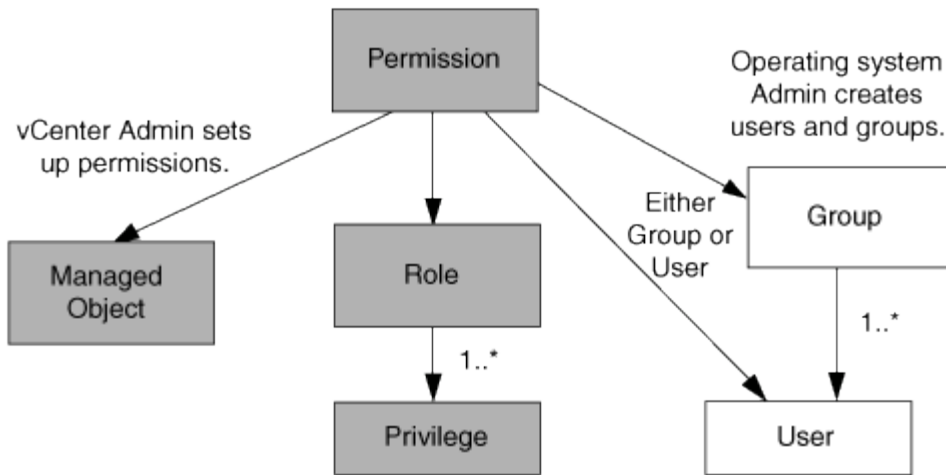
- Un usuario o grupo

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 las herramientas de ONTAP para VMware vSphere:

- Privilegios nativos de vCenter Server

Estos privilegios vienen con vCenter Server.

- Privilegios específicos de herramientas de ONTAP

Estos privilegios se definen para tareas específicas de herramientas de ONTAP. Son exclusivas de las herramientas de ONTAP.

Las tareas de las herramientas de ONTAP requieren privilegios específicos de las herramientas de ONTAP 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, las herramientas de ONTAP proporcionan varios roles estándar que contienen todos los privilegios nativos y específicos de las herramientas de ONTAP necesarios para ejecutar tareas de herramientas de ONTAP.

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	Roles	Tareas
Herramientas de NetApp ONTAP Consola > Ver	<ul style="list-style-type: none"> • Administrador de VSC • Aprovisionamiento de VSC • Solo lectura de VSC 	Todas las herramientas de ONTAP y las tareas específicas del proveedor VASA requieren el privilegio de visualización.
Virtual Storage Console de NetApp > Gestión basada en políticas > Gestión o privilege.nvpfVSC.VASAGroup.com.netapp.nvpf.label > Gestión	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 las tareas específicas de herramientas de ONTAP, los permisos se asignan y validan solo en el nivel de carpeta raíz (vCenter Server) y 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. Luego, puede utilizar los permisos de vCenter Server para otorgar acceso a estos usuarios o grupos para permitirles ejecutar tareas específicas de herramientas de ONTAP.



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

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 las herramientas de ONTAP para VMware vSphere se complete correctamente, puede depender de la ubicación en la que se haya asignado un permiso o de las acciones que haya realizado 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 las herramientas de ONTAP que un usuario puede realizar.

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 un privilegio se aplica a un sistema de almacenamiento, debe asignar el permiso que incluye ese privilegio al objeto raíz de herramientas de ONTAP porque no existe ningún objeto de vSphere al que pueda asignarlo.

Por ejemplo, cualquier permiso que incluya un privilegio como el privilegio ONTAP tools «Agregar/modificar/omitir sistemas de almacenamiento» se debe asignar en el nivel de objeto 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.

Funciones estándar incluidas en las herramientas de ONTAP

Para simplificar el uso de los privilegios de vCenter Server y el control de acceso basado en roles (RBAC), las herramientas de ONTAP ofrecen funciones de herramientas estándar de ONTAP que permiten realizar tareas clave de herramientas de ONTAP. También hay un rol de solo lectura que permite ver la información, pero no ejecutar tareas.

Los roles de herramientas estándar de ONTAP tienen privilegios específicos para las herramientas de ONTAP y los privilegios nativos de vCenter Server requeridos para que los usuarios ejecuten tareas de herramientas de ONTAP. 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.



Al actualizar las herramientas de ONTAP a la versión más reciente, las funciones estándar se actualizan automáticamente para que funcionen con la nueva versión de la herramienta.

Puede ver las funciones estándar de las herramientas de ONTAP haciendo clic en **Roles** en la página inicial del cliente de vSphere.

Los roles que las herramientas de ONTAP proporcionan le permiten realizar las siguientes tareas:

Rol	Descripción
Administrador de VSC	Ofrece todos los privilegios nativos de vCenter Server y los privilegios específicos de las herramientas de ONTAP que se requieren para ejecutar todas las tareas de las herramientas de ONTAP.

Solo lectura de VSC	Ofrece acceso de solo lectura a herramientas de ONTAP. Estos usuarios no pueden realizar ninguna acción de las herramientas de ONTAP que esté controlada por acceso.
Aprovisionamiento de VSC	<p>Ofrece todos los privilegios nativos de vCenter Server y los privilegios específicos de la herramienta ONTAP que se requieren para aprovisionar el almacenamiento. Es posible realizar las siguientes tareas:</p> <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 los roles estándar de las herramientas de ONTAP

Cuando trabaja con herramientas estándar de ONTAP para roles de VMware vSphere, hay ciertas directrices que deben seguir.

No debe modificar directamente los roles estándar. Si lo hace, las herramientas de ONTAP sobrescribirán los cambios cada vez que actualice. Installer actualiza las definiciones de rol estándar cada vez que actualiza las herramientas de ONTAP. Al hacer esto, se garantiza que los roles sean actualizados para la versión de las herramientas de ONTAP, 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 herramientas de ONTAP y, a continuación, editar el rol copiado. Al crear una nueva función, puede mantener esta función incluso cuando reinicie o actualice el servicio Windows de las herramientas de ONTAP.

Algunas de las formas en que puede utilizar las funciones estándar de ONTAP Tools incluyen las siguientes:

- Utilice los roles de herramientas estándar de ONTAP para todas las tareas de herramientas de ONTAP.

En este escenario, los roles estándar proporcionan todos los privilegios que un usuario necesita para realizar las tareas de las herramientas de ONTAP.

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

Si los roles de ONTAP Tools estándar proporcionan demasiada granularidad para su entorno, puede expandir los roles creando grupos de nivel superior que contengan varios roles.

Si un usuario debe ejecutar otras tareas de herramientas que no son de ONTAP y que requieren privilegios nativos adicionales de vCenter Server, puede crear un rol que proporcione dichos privilegios y añadirlo al grupo también.

- Cree funciones más detalladas.

Si su empresa requiere que implemente funciones que son más restrictivas que las funciones de herramientas estándar de ONTAP, puede utilizar las funciones de herramientas de ONTAP para crear nuevas funciones.

En este caso, debe clonar los roles de herramientas ONTAP necesarios y, a continuación, editar el rol clonado para que solo tenga los privilegios que necesite el usuario.

Privilegios requeridos para las tareas de herramientas de ONTAP

Las diferentes herramientas de ONTAP para las tareas de VMware vSphere requieren diferentes combinaciones de privilegios específicos de las herramientas de ONTAP y los privilegios nativos de vCenter Server.

En el artículo de la base de conocimientos de NetApp 1032542, encontrará información sobre los privilegios requeridos para las tareas de las herramientas ONTAP.

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

Privilegios a nivel de producto que requieren las herramientas de ONTAP para VMware vSphere

Para tener acceso a las herramientas ONTAP para la interfaz gráfica de usuario de VMware vSphere, es necesario contar con el privilegio View específico para las herramientas ONTAP para el producto asignado en el nivel de objeto de vSphere correspondiente. Si inicia sesión sin este privilegio, las herramientas de ONTAP muestran un mensaje de error al hacer clic en el icono de NetApp y le impiden acceder a las herramientas de ONTAP.

En el privilegio **Ver**, puede acceder a la GUI de herramientas de ONTAP. Este privilegio no le permite realizar tareas dentro de las herramientas de ONTAP. Para ejecutar tareas de herramientas ONTAP, es necesario contar con los privilegios nativos y específicos de ONTAP para esas tareas.

El nivel de asignación determina qué porciones de la interfaz de usuario se muestran. Al asignar el privilegio View en el objeto raíz (carpeta), es posible acceder a las herramientas de ONTAP haciendo clic en el icono NetApp.

Es posible asignar el privilegio View a otro nivel de objeto de vSphere. No obstante, de esta forma se limitan los menús de herramientas de ONTAP que se pueden ver y usar.

El objeto raíz es el lugar recomendado para asignar cualquier permiso que contiene el privilegio View.

Permisos para los sistemas de almacenamiento ONTAP y objetos de vSphere

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 las herramientas de ONTAP® 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 herramientas de ONTAP puede realizar un usuario específico en los objetos de un sistema de almacenamiento específico.

Las herramientas de ONTAP utilizan las credenciales (nombre de usuario y contraseña) que se configuran en herramientas de ONTAP para autenticar cada sistema de almacenamiento y determinar qué operaciones de almacenamiento se pueden ejecutar en ese sistema de almacenamiento. Las herramientas de ONTAP usan un conjunto de credenciales por cada sistema de almacenamiento. Estas credenciales determinan qué tareas de las herramientas de ONTAP se pueden ejecutar en ese sistema de almacenamiento, es decir, las credenciales se aplican a las herramientas de ONTAP, no a un usuario individual de las herramientas de ONTAP.

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 herramientas de ONTAP 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. Puede utilizar el control de acceso basado en roles de ONTAP junto con los privilegios específicos de ONTAP tools para controlar las tareas que un usuario puede realizar de las herramientas de ONTAP:

- 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 control de acceso basado en roles de ONTAP con los privilegios específicos de ONTAP aporta 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 aprovisione un almacén de datos con almacenamiento de NetApp mientras impide que vCenterUserA aprovisione 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.

Al iniciar una tarea de ONTAP tools, las herramientas de ONTAP primero verifican si cuenta con el permiso correcto de vCenter Server para esa tarea. Si el permiso de vCenter Server no es suficiente para permitir que realice la tarea, las herramientas de ONTAP no tienen que comprobar los privilegios de ONTAP para ese sistema de almacenamiento, ya que no se superó 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, las herramientas de ONTAP luego comprueba los privilegios de RBAC de ONTAP (el rol de ONTAP) asociados con las credenciales del sistema de almacenamiento (el nombre de usuario y la contraseña). Para determinar si cuenta con privilegios suficientes para realizar las operaciones de almacenamiento que requiere esa tarea de herramientas ONTAP en ese sistema de almacenamiento. Si tiene los privilegios de ONTAP correctos, puede acceder al sistema de almacenamiento y ejecutar la tarea de herramientas de ONTAP. Los roles ONTAP determinan las tareas de herramientas de ONTAP que se pueden realizar 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, las herramientas de ONTAP ofrecen 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 al usar herramientas de ONTAP para VMware vSphere

Puede configurar varias funciones ONTAP recomendadas para trabajar con las herramientas de ONTAP® para VMware vSphere y el control de acceso basado en funciones (RBAC). Estos roles contienen los privilegios de la ONTAP que se requieren para ejecutar las operaciones de almacenamiento requeridas que ejecutan las tareas de las herramientas de ONTAP.

Para crear roles de usuario nuevos, debe iniciar sesión como administrador en sistemas de almacenamiento que ejecutan ONTAP. Se pueden crear roles de ONTAP con ONTAP System Manager 9.8P1 o posterior. Consulte "[Configure los roles y privilegios de usuario](#)" si quiere más información.

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 ONTAP específicos de las herramientas de ONTAP se ordenan jerárquicamente. Esto significa que el primer rol es el más restrictivo y solo tiene los privilegios asociados al conjunto más básico de operaciones de almacenamiento de herramientas de ONTAP. 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 muestran algunos de los roles de control de acceso basado en roles recomendados de ONTAP cuando se utilizan las herramientas de ONTAP. 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 las herramientas de ONTAP para VMware vSphere

Debe configurar el control de acceso basado en roles (RBAC) de ONTAP en el sistema de almacenamiento para poder utilizar el control de acceso basado en roles con las

herramientas ONTAP para VMware vSphere. Es posible crear una o varias cuentas de usuario personalizadas con privilegios de acceso limitados mediante la función RBAC de ONTAP.

Las herramientas de ONTAP y el SRA pueden acceder a los sistemas de almacenamiento a nivel del clúster o al nivel de SVM de la máquina virtual de almacenamiento (SVM). 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 añadiendo detalles de SVM directamente, debe tener en cuenta 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 necesita VASA Provider para una controladora de almacenamiento determinada, el sistema de almacenamiento se debe añadir a las herramientas de ONTAP en el nivel de clúster, incluso si utiliza herramientas de ONTAP o SRA.

Para crear un nuevo usuario y conectar un clúster o una SVM a las herramientas de ONTAP, debe realizar lo siguiente:

- Cree un rol de administrador de clúster o de administrador de SVM mediante ONTAP System Manager 9.8P1 o posterior. Consulte ["Configure los roles y privilegios de usuario"](#) si quiere más información.
- Cree usuarios con el rol asignado y el conjunto de aplicaciones adecuado mediante ONTAP

Estas credenciales del sistema de almacenamiento son necesarias para configurar los sistemas de almacenamiento para las herramientas de ONTAP. Puede configurar sistemas de almacenamiento para las herramientas ONTAP introduciendo las credenciales en las herramientas de ONTAP. Cada vez que se inicie sesión en un sistema de almacenamiento con estas credenciales, se tendrán permisos para las funciones de herramientas de ONTAP que se configuraron en ONTAP al crear las credenciales.

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

Funciones de herramientas de ONTAP

Las herramientas de ONTAP clasifican los privilegios de ONTAP en el siguiente conjunto de funciones de herramientas de ONTAP:

- 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 del clúster o de SVM. Esto permite a los usuarios ejecutar operaciones de SRM.

Las herramientas de ONTAP realizan una validación inicial de privilegios de roles de control de acceso basado en roles de ONTAP al añadir el clúster a las herramientas de ONTAP. Si añadió una dirección IP de almacenamiento SVM directa, las herramientas de ONTAP no realizan la validación inicial. Las herramientas de ONTAP comprueban y aplican los privilegios más adelante en el flujo de trabajo de la tarea.

Configurar la alta disponibilidad para las herramientas de ONTAP

Las herramientas de ONTAP son compatibles con una configuración de alta disponibilidad (ha) para ayudar a proporcionar la funcionalidad sin interrupciones de las herramientas de ONTAP durante el fallo.

Las herramientas de ONTAP se basan en la función de alta disponibilidad (ha) de VMware vSphere y en la función de tolerancia a fallos (FT) de vSphere para proporcionar una alta disponibilidad. La solución de alta disponibilidad permite recuperarse rápidamente de las interrupciones provocadas por:

- Error del host
- Fallo de red
- Fallo de máquina virtual (fallo de SO invitado)
- Fallo de la aplicación (herramientas ONTAP)

No se necesita ninguna configuración adicional para que las herramientas de ONTAP proporcionen una alta disponibilidad. 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, las herramientas de ONTAP también contribuyen a que los servicios de herramientas de ONTAP se ejecuten en todo momento. El proceso de vigilancia de las herramientas ONTAP 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.



Las herramientas de ONTAP no admiten la alta disponibilidad del vCenter.

VMware vSphere ha

Puede configurar su entorno de vSphere donde las herramientas de ONTAP para VMware vSphere esté puesto en marcha para una alta disponibilidad (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 alta disponibilidad (ha) a un nivel superior y le permite proteger las máquinas virtuales sin perder datos o conexiones. Debe habilitar o deshabilitar las herramientas de vSphere FT para ONTAP desde vCenter Server.

Asegúrese de que la licencia de vSphere sea compatible CON FT con el número de vCPU necesarias para herramientas ONTAP 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 las herramientas de ONTAP

Las herramientas de ONTAP para VMware vSphere son compatibles con entornos que usan configuraciones de MetroCluster IP y FC para ONTAP. La mayor parte de este soporte es automático. Sin embargo, es posible que observe algunas diferencias cuando se utiliza un entorno de MetroCluster con herramientas de ONTAP y proveedor VASA.



El SRA no es compatible con las configuraciones de MetroCluster.

Configuraciones de MetroCluster y herramientas ONTAP

Debe asegurarse de que las herramientas ONTAP detecten las controladoras del sistema de almacenamiento en el sitio principal y el sitio secundario. Por lo general, las herramientas ONTAP detectan automáticamente las controladoras de almacenamiento. Si usa una LIF de gestión de clúster, una buena práctica es verificar que las herramientas de ONTAP han detectado los clústeres en ambos sitios. De lo contrario, puede añadir manualmente las controladoras de almacenamiento a las herramientas de ONTAP. También es posible modificar los pares de nombre de usuario y contraseña que utilizan las herramientas de ONTAP para conectarse a las controladoras de almacenamiento.

Cuando se produce una conmutación, los SVM del sitio secundario toman el control. Estos SVMs tienen adjunto el sufijo "-mc" a sus nombres. Si se produce una operación de conmutación de sitios mientras realiza operaciones como el aprovisionamiento de un almacén de datos, el nombre de la SVM en la que reside el almacén de datos se modifica para incluir el sufijo "-mc". Este sufijo se descarta cuando se produzca la conmutación de estado y las SVM del sitio principal reanudan el control.



Si ha añadido SVM directas con configuración de MetroCluster a las herramientas de ONTAP, después de la conmutación por error, no se reflejará el cambio en el nombre de la 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, las herramientas de ONTAP pueden demorar varios minutos en detectar automáticamente los clústeres y detectarlos. Si esto sucede mientras realiza una operación de herramientas de ONTAP, como el aprovisionamiento de un almacén de datos, puede experimentar un retraso.

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 puede añadir SVM directas a VASA Provider.



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

Configuraciones de MetroCluster y SRA

El adaptador de replicación de almacenamiento (SRA) es compatible con entornos que usan configuraciones de MetroCluster (MCC) con protocolo NFS, iSCSI y FCP.

Como requisito previo para la configuración del SRA de MCC, todos los nombres de las máquinas virtuales de almacenamiento (SVM) deben ser únicos en los clústeres de MCC. Si los nombres no son únicos, provocará conflictos y fallarán los flujos de trabajo del SRA.

Acciones necesarias:

1. Después de realizar una conmutación de sitios o una conmutación de estado de MCC, asegúrese de que el comando `snapmirror list-destinations` en el clúster de origen muestre la salida correcta con el nuevo nombre de SVM (`<vserver_name>-mc`). El comando puede tardar hasta 30 minutos en ejecutarse.
2. Realice la operación `DetecDevices` desde la interfaz de usuario del SRM antes de continuar con otros flujos de trabajo del SRA. Esta operación garantiza que el SRM reconozca los cambios en los nombres de las SVM después de una conmutación de sitios o una conmutación de estado.

Información de copyright

Copyright © 2023 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 INTERRUPTIÓN 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.