Gestione los roles de control de acceso

ONTAP 9

NetApp
February 12, 2026

This PDF was generated from https://docs.netapp.com/es-es/ontap/authentication/manage-access-control-roles-concept.html on February 12, 2026. Always check docs.netapp.com for the latest.

Tabla de contenidos

Gestione los roles de control de acceso . . . 1
- Obtenga más información sobre la gestión de roles de control de acceso de ONTAP . . . 1
- Modificar el rol asignado a un administrador de ONTAP . . . 1
- Defina roles personalizados para administradores de ONTAP . . . 1
- Roles predefinidos para administradores de clústeres de ONTAP . . . 3
- Roles predefinidos para administradores de SVM de ONTAP . . . 5
- Gestione el acceso del administrador de ONTAP con System Manager . . . 7
  - Asignación de un rol a un administrador . . . 8
  - Cambiar el rol de un administrador . . . 8
- Acceso a la elevación de privilegios JIT en ONTAP . . . 8
- Configurar la elevación de privilegios JIT en ONTAP . . . 9
  - Modificar la configuración global de JIT . . . 10
  - Configurar el acceso de elevación de privilegios JIT para un usuario . . . 11
  - Casos de uso comunes de JIT . . . 12

Gestione los roles de control de acceso

Obtenga más información sobre la gestión de roles de control de acceso de ONTAP

El rol asignado a un administrador determina los comandos a los que el administrador tiene acceso. La función se asigna al crear la cuenta para el administrador. Puede asignar un rol diferente o definir roles personalizados según sea necesario.

Modificar el rol asignado a un administrador de ONTAP

Puede usar el `security login modify` comando para cambiar el rol de una cuenta de administrador de clúster o de SVM. Puede asignar un rol predefinido o personalizado.

Antes de empezar

Para realizar esta tarea, debe ser un administrador de clústeres.

Paso

1. Cambie la función de un administrador de clúster o SVM:

   ```
   security login modify -vserver SVM_name -user-or-group-name user_or_group_name
   -application application -authmethod authentication_method -role role -comment
   comment
   ```

   "Crear o modificar cuentas de inicio de sesión"

   El siguiente comando cambia el rol de la cuenta de administrador de clúster de AD `DOMAIN1\guest1` al `readonly` rol predefinido.

   ```
   cluster1::>security login modify -vserver engCluster -user-or-group-name
   DOMAIN1\guest1 -application ssh -authmethod domain -role readonly
   ```

   El siguiente comando cambia el rol de las cuentas de administrador de SVM en la cuenta de AD group `DOMAIN1\adgroup` al `vol_role` rol personalizado.

   ```
   cluster1::>security login modify -vserver engData -user-or-group-name
   DOMAIN1\adgroup -application ssh -authmethod domain -role vol_role
   ```

   Obtenga más información sobre `security login modify` en el "Referencia de comandos del ONTAP".

Defina roles personalizados para administradores de ONTAP

Puede usar el `security login role create` comando para definir un rol

personalizado. Puede ejecutar el comando tantas veces como sea necesario para obtener la combinación exacta de funcionalidades que desea asociar al rol.

Acerca de esta tarea

- Un rol, ya sea predefinido o personalizado, concede o deniega el acceso a los comandos o directorios de comandos de ONTAP.

  Un directorio de comandos (`volume`, por ejemplo) es un grupo de comandos y subdirectorios de comandos relacionados. Excepto como se describe en este procedimiento, la concesión o denegación del acceso a un directorio de comandos otorga o deniega el acceso a cada comando del directorio y sus subdirectorios.

- El acceso a comandos específicos o al subdirectorio anula el acceso al directorio principal.

  Si se define un rol con un directorio de comandos y se define de nuevo con un nivel de acceso diferente para un comando específico o para un subdirectorio del directorio principal, el nivel de acceso especificado para el comando o subdirectorio anula el nivel del primario.

> No puede asignar a un administrador de SVM un rol que proporciona acceso a un comando o directorio de comandos que solo esté disponible para `admin` el administrador del clúster, por ejemplo, el `security` directorio de comandos.

Antes de empezar

Para realizar esta tarea, debe ser un administrador de clústeres.

Paso

1. Defina un rol personalizado:

   ```
   security login role create -vserver SVM_name -role role -cmddirname
   command_or_directory_name -access access_level -query query
   ```

   Los siguientes comandos otorgan al `vol_role` rol acceso total a los comandos del `volume` directorio de comandos y acceso de solo lectura a los comandos del `volume snapshot` subdirectorio.

   ```
   cluster1::>security login role create -role vol_role -cmddirname
   "volume" -access all

   cluster1::>security login role create -role vol_role -cmddirname "volume
   snapshot" -access readonly
   ```

   Los siguientes comandos otorgan al `SVM_storage` rol acceso de solo lectura a los comandos del `storage` directorio de comandos, sin acceso a los comandos del `storage encryption` subdirectorio y acceso completo al `storage aggregate plex offline` comando no intrínseco.

```
cluster1::>security login role create -role SVM_storage -cmddirname
"storage" -access readonly

cluster1::>security login role create -role SVM_storage -cmddirname
"storage encryption" -access none

cluster1::>security login role create -role SVM_storage -cmddirname
"storage aggregate plex offline" -access all
```

Obtenga más información sobre `security login role create` en el "Referencia de comandos del ONTAP".

Información relacionada

- "seguridad rol de inicio de sesión crear"
- "plex de agregado de almacenamiento sin conexión"
- "cifrado del almacenamiento"

Roles predefinidos para administradores de clústeres de ONTAP

Los roles predefinidos para administradores de clúster deben cumplir con la mayoría de las necesidades. Puede crear roles personalizados según sea necesario. De forma predeterminada, se asigna `admin` el rol predefinido a un administrador de clúster.

En la siguiente tabla, se enumeran los roles predefinidos para los administradores de clúster:

Este rol…	Tiene este nivel de acceso…	A los siguientes comandos o directorios de comandos
admin	todo	Todos los directorios de comandos (`DEFAULT`)
admin-no-fsa (disponible a partir de ONTAP 9.12.1)	Lectura/Escritura	• Todos los directorios de comandos (`DEFAULT`) • `security login rest-role` • `security login role`

Solo lectura	• `security login rest-role create` • `security login rest-role delete` • `security login rest-role modify` • `security login rest-role show` • `security login role create` • `security login role create` • `security login role delete` • `security login role modify` • `security login role show` • `volume activity-tracking` • `volume analytics`	Ninguno
`volume file show-disk-usage`	AutoSupport	todo
• `set` • `system node autosupport`	ninguno	Todos los demás directorios de comandos (`DEFAULT`)
backup	todo	`vserver services ndmp`
sólo lectura	`volume`	ninguno
Todos los demás directorios de comandos (`DEFAULT`)	sólo lectura	todo

• `security login password` Sólo para gestionar la contraseña local y la información de claves de la cuenta de usuario propia • `set`	• A partir de ONTAP 9,8, sólo lectura • Antes de ONTAP 9,8, ninguna	`security`
sólo lectura	Todos los demás directorios de comandos (`DEFAULT`)	SnapLock
todo	• `set` • `volume create` • `volume modify` • `volume move` • `volume show`	ninguno
• `volume move governor` • `volume move recommend`	ninguno	Todos los demás directorios de comandos (`DEFAULT`)
ninguno	ninguno	Todos los directorios de comandos (`DEFAULT`)

`autosupport`El rol se asigna a la `autosupport` cuenta predefinida, que usa AutoSupport OnDemand. ONTAP le impide modificar o eliminar la `autosupport` cuenta. ONTAP también le impide asignar `autosupport` el rol a otras cuentas de usuario.

Información relacionada

- "inicio de sesión de seguridad"
- "listo"
- "volumen"
- "ndmp de servicios vserver"

Roles predefinidos para administradores de SVM de ONTAP

Los roles predefinidos para administradores de SVM deben cumplir con la mayoría de las necesidades. Puede crear roles personalizados según sea necesario. De forma predeterminada, se asigna `vsadmin` el rol predefinido a un administrador de SVM.

En la siguiente tabla, se enumeran los roles predefinidos para los administradores de SVM:

Nombre del rol	Funcionalidades

vsadmin	• Administrar la información de clave y la contraseña local de la cuenta de usuario propia • Gestión de volúmenes, excepto movimientos de volúmenes • Gestión de cuotas, qtrees, snapshots y ficheros • Gestionar las LUN • Realizar operaciones de SnapLock, excepto la eliminación con privilegios • Configuración de protocolos: NFS, SMB, iSCSI, FC, FCoE y NVMe/FC y NVMe/TCP • Servicios de configuración: DNS, LDAP y NIS • Supervisar trabajos de • Supervisar las conexiones de red y la interfaz de red • Supervisar el estado del SVM
vsadmin-volumen	• Administrar la información de clave y la contraseña local de la cuenta de usuario propia • Gestión de volúmenes, excepto movimientos de volúmenes • Gestión de cuotas, qtrees, snapshots y ficheros • Gestionar las LUN • Configuración de protocolos: NFS, SMB, iSCSI, FC, FCoE y NVMe/FC y NVMe/TCP • Servicios de configuración: DNS, LDAP y NIS • Supervisar la interfaz de red • Supervisar el estado del SVM
protocolo vsadmin	• Administrar la información de clave y la contraseña local de la cuenta de usuario propia • Configuración de protocolos: NFS, SMB, iSCSI, FC, FCoE y NVMe/FC y NVMe/TCP • Servicios de configuración: DNS, LDAP y NIS • Gestionar las LUN • Supervisar la interfaz de red • Supervisar el estado del SVM

vsadmin-backup	• Administrar la información de clave y la contraseña local de la cuenta de usuario propia • Gestión de operaciones de NDMP • Hacer que un volumen restaurado sea de lectura/escritura • Gestionar relaciones de SnapMirror y snapshots • Visualización de información de volúmenes y de red
vsadmin-snaplock	• Administrar la información de clave y la contraseña local de la cuenta de usuario propia • Gestión de volúmenes, excepto movimientos de volúmenes • Gestión de cuotas, qtrees, snapshots y ficheros • Realizar operaciones de SnapLock, incluida la eliminación con privilegios • Configurar protocolos: NFS y SMB • Servicios de configuración: DNS, LDAP y NIS • Supervisar trabajos de • Supervisar las conexiones de red y la interfaz de red
vsadmin-readonly	• Administrar la información de clave y la contraseña local de la cuenta de usuario propia • Supervisar el estado del SVM • Supervisar la interfaz de red • Ver volúmenes y LUN • Servicios y protocolos de visualización

Gestione el acceso del administrador de ONTAP con System Manager

El rol asignado a un administrador determina qué funciones puede realizar el administrador con System Manager. Los roles predefinidos para los administradores de clúster y los administradores de máquinas virtuales de almacenamiento son provistos por System Manager. Puede asignar la función al crear la cuenta del administrador o asignar una función diferente más adelante.

En función de cómo haya habilitado el acceso a cuentas, es posible que deba realizar cualquiera de las siguientes acciones:

- Asociar una clave pública a una cuenta local.

- Instale un certificado digital de servidor firmado por CA.
- Configure el acceso AD, LDAP o NIS.

Puede ejecutar estas tareas antes o después de habilitar el acceso a la cuenta.

Asignación de un rol a un administrador

Asigne un rol a un administrador, como se indica a continuación:

Pasos

1. Seleccione **Cluster > Settings**.
2. Seleccione → junto a **Usuarios y Roles**.
3. Seleccione + Add en **Usuarios**.
4. Especifique un nombre de usuario y seleccione un rol en el menú desplegable **rol**.
5. Especifique un método de inicio de sesión y una contraseña para el usuario.

Cambiar el rol de un administrador

Cambie el rol de un administrador, como se indica a continuación:

Pasos

1. Haga clic en **clúster > Configuración**.
2. Seleccione el nombre del usuario cuyo rol desea cambiar y, a continuación, haga clic en el ⋮ que aparece junto al nombre de usuario.
3. Haga clic en **Editar**.
4. Seleccione un rol en el menú desplegable para **rol**.

Acceso a la elevación de privilegios JIT en ONTAP

A partir de ONTAP 9.17.1, los administradores de clúster pueden "configurar la elevación de privilegios justo a tiempo (JIT)" Permite a los usuarios de ONTAP elevar temporalmente sus privilegios para realizar ciertas tareas. Al configurar JIT para un usuario, este puede elevar temporalmente sus privilegios a un rol con los permisos necesarios para realizar una tarea. Tras finalizar la sesión, el usuario recupera su nivel de acceso original.

Los administradores de clústeres pueden configurar el tiempo durante el cual un usuario puede acceder a la elevación JIT. Por ejemplo, pueden configurar el acceso de los usuarios a la elevación JIT con un límite de 30 minutos por sesión (el *período de validez de la sesión*) durante un período de 30 días (el *período de validez de la sesión*). Durante este período, el usuario puede elevar sus privilegios tantas veces como necesite, pero cada sesión está limitada a 30 minutos.

Acerca de esta tarea

- La elevación de privilegios JIT solo está disponible para usuarios que acceden a ONTAP mediante SSH. Esta elevación de privilegios solo está disponible en la sesión SSH actual, pero se pueden elevar en tantas sesiones SSH simultáneas como sea necesario.
- La elevación de privilegios JIT solo es compatible con usuarios que usan contraseña, nsswitch o

autenticación de dominio para iniciar sesión. La autenticación multifactor (MFA) no es compatible con la elevación de privilegios JIT.

- La sesión JIT de un usuario finalizará si la sesión configurada o el período de validez de JIT expira, o si un administrador del clúster revoca el acceso JIT para el usuario.

Antes de empezar

- Para acceder a la elevación de privilegios JIT, un administrador del clúster debe configurar el acceso JIT para su cuenta. El administrador del clúster determina el rol al que puede elevar sus privilegios y el tiempo durante el cual puede acceder a ellos.

Pasos

1. Eleve temporalmente sus privilegios al rol configurado:

   ```
   security jit-privilege elevate
   ```

   Tras introducir este comando, se le solicitará su contraseña de inicio de sesión. Si su cuenta tiene configurado el acceso JIT, se le concederá acceso con privilegios elevados durante la sesión configurada. Una vez finalizada, volverá a su nivel de acceso original. Puede aumentar sus privilegios tantas veces como necesite dentro del periodo de validez del acceso JIT configurado.

2. Ver el tiempo restante en su sesión JIT:

   ```
   security jit-privilege show-remaining-time
   ```

   Si actualmente está en una sesión JIT, este comando muestra el tiempo restante.

3. Si es necesario, finalice su sesión JIT antes de tiempo:

   ```
   security jit-privilege reset
   ```

   Si actualmente está en una sesión JIT, este comando finaliza la sesión JIT y restaura su nivel de acceso original.

Configurar la elevación de privilegios JIT en ONTAP

A partir de ONTAP 9.17.1, los administradores de clústeres pueden configurar la elevación de privilegios Just-In-Time (JIT) para permitir que los usuarios de ONTAP eleven temporalmente sus privilegios para realizar ciertas tareas. Cuando se configura JIT para un usuario, este puede… "elevar sus privilegios" A un rol con los permisos necesarios para realizar una tarea. Una vez finalizada la sesión, el usuario recupera su nivel de acceso original.

Los administradores de clústeres pueden configurar el tiempo durante el cual un usuario puede acceder a la elevación JIT. Por ejemplo, se puede configurar el acceso de los usuarios a la elevación JIT con un límite de 30 minutos por sesión (el *período de validez de la sesión*) durante un período de 30 días (el *período de validez de la sesión*). Durante este período, el usuario puede elevar sus privilegios tantas veces como necesite, pero

cada sesión está limitada a 30 minutos.

La elevación de privilegios JIT se basa en el principio de privilegios mínimos, lo que permite a los usuarios realizar tareas que requieren privilegios elevados sin que se les otorguen permanentemente. Esto ayuda a reducir el riesgo de acceso no autorizado o cambios accidentales en el sistema. Los siguientes ejemplos describen algunos casos de uso comunes para la elevación de privilegios JIT:

- Permitir acceso temporal a la `security login create` y `security login delete` Comandos para habilitar la incorporación y salida de usuarios.
- Permitir acceso temporal a `system node image update` y `system node upgrade-revert` Durante una ventana de actualización. Una vez completada la actualización, se revoca el acceso al comando.
- Permitir acceso temporal a `cluster add-node` , `cluster remove-node` , y `cluster modify` Para habilitar la expansión o reconfiguración del clúster. Una vez completados los cambios en el clúster, se revoca el acceso a los comandos.
- Permitir acceso temporal a `volume snapshot restore` Para habilitar las operaciones de restauración y la gestión de destinos de copia de seguridad. Una vez completada la restauración o configuración, se revoca el acceso a los comandos.
- Permitir acceso temporal a `security audit log show` para permitir la revisión y exportación del registro de auditoría durante una verificación de cumplimiento.

consulte Casos de uso comunes de JIT .

Los administradores de clúster pueden configurar el acceso JIT para los usuarios de ONTAP y configurar los períodos de validez JIT predeterminados a nivel global en el clúster o para SVM específicos.

Acerca de esta tarea

- La elevación de privilegios JIT solo está disponible para usuarios que acceden a ONTAP mediante SSH. Estos privilegios solo están disponibles dentro de la sesión SSH actual del usuario, pero pueden elevarse en tantas sesiones SSH simultáneas como sea necesario.
- La elevación de privilegios JIT solo es compatible con usuarios que usan contraseña, nsswitch o autenticación de dominio para iniciar sesión. La autenticación multifactor (MFA) no es compatible con la elevación de privilegios JIT.

Antes de empezar

- Debe ser un administrador del clúster ONTAP en el `admin` nivel de privilegio para realizar las siguientes tareas.

Modificar la configuración global de JIT

Puede modificar la configuración JIT predeterminada globalmente en todo el clúster de ONTAP o para una SVM específica. Esta configuración determina el periodo de validez de la sesión predeterminado y el periodo máximo de validez JIT para los usuarios configurados para el acceso JIT.

Acerca de esta tarea

- El valor predeterminado `default-session-validity-period` El valor es de una hora. Esta configuración determina durante cuánto tiempo un usuario puede acceder a privilegios elevados en una sesión JIT antes de tener que volver a elevarlos.
- El valor predeterminado `max-jit-validity-period` El valor es de 90 días. Esta configuración determina el periodo máximo durante el cual un usuario puede acceder a la elevación JIT después de la fecha de inicio configurada. Puede configurar el periodo de validez de JIT para usuarios individuales, pero no puede superar el periodo máximo de validez de JIT.

Pasos

1. Compruebe la configuración JIT actual:

```
security jit-privilege show -vserver <svm_name>
```

`-vserver` Es opcional. Si no se especifica una SVM, el comando muestra la configuración JIT global.

2. Modificar la configuración JIT globalmente o para un SVM:

```
security jit-privilege modify -vserver <svm_name> -default-session
-validity-period <period> -max-jit-validity-period <period>
```

Si no se especifica una SVM, el comando modifica la configuración global de JIT. El siguiente ejemplo establecerá la duración predeterminada de la sesión JIT en 45 minutos y la duración máxima en 30 días para SVM. `svm1` :
`security jit-privilege modify -vserver svm1 -default-session-validity-period 45m -max-jit-validity-period 30d`

En este ejemplo, los usuarios podrán acceder a la elevación JIT durante 45 minutos a la vez y podrán iniciar sesiones JIT durante un máximo de 30 días después de su fecha de inicio configurada.

Configurar el acceso de elevación de privilegios JIT para un usuario

Puede asignar acceso de elevación de privilegios JIT a los usuarios de ONTAP .

Pasos

1. Comprobar el acceso JIT actual de un usuario:

```
security jit-privilege user show -username <username>
```

`-username` Es opcional. Si no se especifica un nombre de usuario, el comando muestra el acceso JIT para todos los usuarios.

2. Asignar nuevo acceso JIT para un usuario:

```
security jit-privilege create -username <username> -vserver <svm_name>
-role <rbac_role> -session-validity-period <period> -jit-validity-period
<period> -start-time <date>
```

- Si `-vserver` no se especifica, el acceso JIT se asigna a nivel de clúster.
- `-role` es el rol RBAC al que se elevará el usuario. Si no se especifica, `-role` El valor predeterminado es `admin` .
- `-session-validity-period` Es el tiempo durante el cual el usuario puede acceder al rol elevado antes de tener que iniciar una nueva sesión JIT. Si no se especifica, el valor global o SVM `default-`

`session-validity-period` se utiliza

- `-jit-validity-period` es la duración máxima durante la cual un usuario puede iniciar sesiones JIT después de la fecha de inicio configurada. Si no se especifica, `session-validity-period` Se utiliza. Este parámetro no puede exceder el valor global o SVM. `max-jit-validity-period` .
- `-start-time` Es la fecha y hora a partir de las cuales el usuario puede iniciar sesiones JIT. Si no se especifica, se utiliza la fecha y hora actuales.

  El siguiente ejemplo permitirá `ontap_user` para acceder a la `admin` rol durante 1 hora antes de tener que iniciar una nueva sesión JIT. `ontap_user` Podrán iniciar sesiones JIT por un período de 60 días a partir de la 1:00 p. m. del 1 de julio de 2025:
  `security jit-privilege user create -username ontap_user -role admin -session -validity-period 1h -jit-validity-period 60d -start-time "7/1/25 13:00:00"`

3. Si es necesario, revoque el acceso JIT de un usuario:

```
security jit-privilege user delete -username <username> -vserver
<svm_name>
```

Este comando revocará el acceso JIT de un usuario, incluso si su acceso no ha expirado. Si `-vserver` Si no se especifica, el acceso JIT se revoca a nivel de clúster. Si el usuario está en una sesión JIT activa, esta se cerrará.

Casos de uso comunes de JIT

La siguiente tabla contiene casos de uso comunes para la elevación de privilegios JIT. Para cada caso, se debe configurar un rol RBAC para proporcionar acceso a los comandos relevantes. Cada comando enlaza con la referencia de comandos de ONTAP , con más información sobre el comando y sus parámetros.

Caso de uso	Comandos	Detalles
Gestión de usuarios y roles	• `security login create` • `security login delete`	Elevar temporalmente para agregar o eliminar usuarios o cambiar roles durante la incorporación o salida.
Gestión de certificados	• `security certificate create` • `security certificate install`	Otorgar acceso a corto plazo para la instalación o renovación del certificado.
Control de acceso SSH/CLI	• `security login create -application ssh`	Otorgar acceso SSH temporalmente para resolución de problemas o soporte del proveedor.
Gestión de licencias	• `system license add` • `system license delete`	Otorgar derechos para agregar o eliminar licencias durante la activación o desactivación de funciones.

Caso de uso	Comandos	Detalles
Actualizaciones y parches del sistema	• `system node image update` • `system node upgrade-revert`	Elevar durante la ventana de actualización y luego revocar.
Configuración de seguridad de red	• `security login role create` • `security login role modify`	Permitir cambios temporales en los roles de seguridad relacionados con la red.
Gestión de clústeres	• `cluster add-node` • `cluster remove-node` • `cluster modify`	Elevate para expansión o reconfiguración del clúster.
Gestión de SVM	• `vserver create` • `vserver delete` • `vserver modify`	Otorgar temporalmente derechos de administrador a un SVM para aprovisionamiento o desmantelamiento.
Gestión del volumen	• `volume create` • `volume delete` • `volume modify`	Elevate para aprovisionamiento, cambio de tamaño o eliminación de volumen.
Gestión de instantáneas	• `volume snapshot create` • `volume snapshot delete` • `volume snapshot restore`	Elevar para eliminar o restaurar instantáneas durante la recuperación.
Configuración de red	• `network interface create` • `network port vlan create`	Otorgar derechos para realizar cambios en la red durante las ventanas de mantenimiento.
Gestión de discos/agregados	• `storage disk assign` • `storage aggregate create` • `storage aggregate add-disks`	Elevate para agregar o quitar discos o administrar agregados.

Caso de uso	Comandos	Detalles
Protección de datos	• `snapmirror create` • `snapmirror modify` • `snapmirror restore`	Elevar temporalmente para configurar o restaurar relaciones de SnapMirror .
Ajuste del rendimiento	• `qos policy-group create` • `qos policy-group modify`	Elevate para solucionar problemas de rendimiento o realizar ajustes.
Acceso al registro de auditoría	• `security audit log show`	Elevar temporalmente para revisión o exportación del registro de auditoría durante las verificaciones de cumplimiento.
Gestión de eventos y alertas	• `event notification create` • `event notification modify`	Elevate para configurar o probar notificaciones de eventos o trampas SNMP.
Acceso a datos impulsado por el cumplimiento	• `volume show` • `security audit log show`	Otorgar acceso temporal de solo lectura a los auditores para revisar datos o registros confidenciales.
Reseñas de acceso privilegiado	• `security login show` • `security login role show`	Elevar temporalmente para revisar e informar sobre el acceso privilegiado. Otorgar acceso elevado de solo lectura por tiempo limitado.

Información relacionada

- "clúster"
- "notificación de eventos"
- "red"
- "grupo de políticas de calidad de servicio"
- "seguridad"
- "snapmirror"
- "almacenamiento"
- "sistema"
- "volumen"
- "vserver"

Información de copyright

Copyright © 2026 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.