



Gestione los roles de control de acceso

ONTAP 9

NetApp
April 24, 2024

Tabla de contenidos

- Gestione los roles de control de acceso 1
 - Información general sobre los roles de gestión de control de acceso 1
 - Modifique la función asignada a un administrador 1
 - Definir funciones personalizadas 1
 - Roles predefinidos para administradores de clúster 3
 - Roles predefinidos para administradores de SVM 5
 - Control del acceso de administradores 7

Gestione los roles de control de acceso

Información general sobre los roles de gestión de control de acceso

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.

Modifique la función asignada a un administrador

Puede utilizar el `security login modify` Comando para cambiar la función de una cuenta de administrador de clúster o 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
```

Para obtener una sintaxis completa del comando, consulte ["hoja de trabajo"](#).

"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 a los predefinidos `readonly` función.

```
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 grupo AD DOMAIN1\adgroup al personalizado `vol_role` función.

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

Definir funciones personalizadas

Puede utilizar 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 un administrador de SVM un rol que otorga acceso a un comando o un directorio de comandos que solo esté disponible para el `admin` administrador de 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
```

Para obtener una sintaxis completa del comando, consulte ["hoja de trabajo"](#).

Los siguientes comandos conceden el `vol_role` rol de acceso completo a los comandos de la `volume` directorio de comandos y el acceso de sólo lectura a los comandos de la `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 conceden el `SVM_storage` el acceso de solo lectura de roles a los comandos de la `storage` directorio de comandos, sin acceso a los comandos de la `storage encryption` y acceso completo al subdirectorio `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
```

Roles predefinidos para administradores de clúster

Los roles predefinidos para administradores de clúster deben cumplir con la mayoría de las necesidades. Puede crear roles personalizados según sea necesario. De manera predeterminada, un administrador de clúster asigna las opciones predefinidas `admin` función.

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	<ul style="list-style-type: none"> • Todos los directorios de comandos (DEFAULT) • <code>security login rest-role</code> • <code>security login role</code>

Solo lectura	<ul style="list-style-type: none"> • 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
<ul style="list-style-type: none"> • 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

<ul style="list-style-type: none"> • security login password <p>Sólo para gestionar la contraseña local y la información de claves de la cuenta de usuario propia</p> <ul style="list-style-type: none"> • set 	ninguno	security
sólo lectura	Todos los demás directorios de comandos (DEFAULT)	ninguno



La autosupport el rol se asigna a los predefinidos autosupport Cuenta, que utiliza AutoSupport OnDemand. ONTAP le impide modificar o eliminar el autosupport cuenta. ONTAP también le impide asignar el autosupport función para otras cuentas de usuario.

Roles predefinidos para administradores de SVM

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

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

Nombre del rol	Funcionalidades
vsadmin	<ul style="list-style-type: none"> • 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, copias Snapshot y archivos • 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	<ul style="list-style-type: none"> • Administrar la información de clave y la contraseña local de la cuenta de usuario propia • Gestión de volúmenes, incluidos los movimientos de volúmenes • Gestión de cuotas, qtrees, copias Snapshot y archivos • 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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 las relaciones de SnapMirror y las copias de Snapshot • Visualización de información de volúmenes y de red

vsadmin-snaplock	<ul style="list-style-type: none"> • 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, copias Snapshot y archivos • 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	<ul style="list-style-type: none"> • 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

Control del acceso de administradores

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 de usuario cuyo rol desea cambiar y 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**.

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.