Acceder al clúster mediante la CLI (solo administradores de clúster)

ONTAP 9

NetApp
April 24, 2024

This PDF was generated from https://docs.netapp.com/es-es/ontap/system-admin/access-serial-port-task.html on April 24, 2024. Always check docs.netapp.com for the latest.

Tabla de contenidos

Acceder al clúster mediante la CLI (solo administradores de clúster) . . . 1
Acceda al clúster mediante el puerto serie . . . 1
Acceda al clúster mediante SSH . . . 1
Seguridad de inicio de sesión SSH . . . 4
Active el acceso Telnet o RSH al clúster . . . 6
Acceda al clúster mediante Telnet . . . 6
Acceda al clúster mediante RSH . . . 8

Acceder al clúster mediante la CLI (solo administradores de clúster)

Acceda al clúster mediante el puerto serie

Puede acceder al clúster directamente desde una consola conectada al puerto de serie de un nodo.

Pasos

1. En la consola, pulse Intro.

   El sistema responde con la solicitud de inicio de sesión.

2. En la solicitud de inicio de sesión, realice una de las siguientes acciones:

Para acceder al clúster con…	Introduzca el siguiente nombre de cuenta…
La cuenta de clúster predeterminada	**`admin`**
Una cuenta de usuario administrativo alternativa	*`username`*

   El sistema responde con el aviso de contraseña.

3. Introduzca la contraseña de la cuenta de usuario administrador o administrativa y, a continuación, pulse Intro.

Acceda al clúster mediante SSH

Puede emitir solicitudes de SSH al clúster para realizar tareas administrativas. De forma predeterminada, SSH está habilitado.

Lo que necesitará

- Debe tener una cuenta de usuario configurada para usar `ssh` como método de acceso.

  La `-application` parámetro de `security login` los comandos especifican el método de acceso para una cuenta de usuario. La `security login` "páginas de manual" contienen información adicional.

- Si utiliza una cuenta de usuario de dominio de Active Directory (AD) para acceder al clúster, debe haberse configurado un túnel de autenticación del clúster a través de una máquina virtual de almacenamiento habilitada para CIFS, y la cuenta de usuario de dominio de AD también se debe haber añadido al clúster con `ssh` como método de acceso y. `domain` como método de autenticación.
- Si utiliza conexiones IPv6, IPv6 ya debe estar configurado y habilitado en el clúster, y las políticas de firewall ya deben estar configuradas con direcciones IPv6.

  La `network options ipv6 show` Command muestra si IPv6 está habilitado. La `system services firewall policy show` comando muestra las directivas de firewall.

Acerca de esta tarea

- Debe utilizar un cliente OpenSSH 5.7 o posterior.
- Solo se admite el protocolo SSH v2; no se admite SSH v1.
- ONTAP admite un máximo de 64 sesiones de SSH simultáneas por nodo.

  Si el LIF de gestión del clúster reside en el nodo, comparte este límite con la LIF de gestión del nodo.

  Si la tasa de conexiones entrantes es superior a 10 por segundo, el servicio se deshabilitará temporalmente durante 60 segundos.

- ONTAP solo admite los algoritmos de cifrado AES y 3DES (también conocidos como *cifrados*) para SSH.

  AES es compatible con una longitud de clave de 128, 192 y 256 bits. 3DES tiene una longitud de clave de 56 bits como EN EL DES original, pero se repite tres veces.

- Cuando el modo FIPS está activado, los clientes SSH deben negociar con los algoritmos de clave pública del algoritmo de firma digital de curva elíptica (ECDSA) para que la conexión sea exitosa.
- Si desea acceder a la CLI de ONTAP desde un host de Windows, puede utilizar una herramienta de otro proveedor, como PuTTY.
- Si utiliza un nombre de usuario de Windows AD para iniciar sesión en ONTAP, debe usar las mismas letras mayúsculas o minúsculas que se usaron cuando se crearon el nombre de usuario y el nombre de dominio de AD en ONTAP.

  Los nombres de usuario Y de dominio DE AD no distinguen mayúsculas de minúsculas. Sin embargo, los nombres de usuario de ONTAP distinguen mayúsculas de minúsculas. La discrepancia entre el nombre de usuario creado en ONTAP y el nombre de usuario creado en AD provoca un error de inicio de sesión.

Opciones de autenticación SSH

- A partir de ONTAP 9,3, puede hacerlo "Habilite la autenticación multifactor SSH" para cuentas de administrador local.

  Cuando la autenticación multifactor en SSH está habilitada, los usuarios se autentican mediante una clave pública y una contraseña.

- A partir de ONTAP 9,4, puede hacerlo "Habilite la autenticación multifactor SSH" Para usuarios remotos LDAP y NIS.
- A partir de ONTAP 9.13.1, opcionalmente puede añadir validación de certificados al proceso de autenticación SSH para mejorar la seguridad de inicio de sesión. Para hacer esto, "Asocie un certificado X,509 a la clave pública" que utiliza una cuenta. Si inicia sesión mediante SSH con una clave pública SSH y un certificado X,509, ONTAP comprueba la validez del certificado X,509 antes de autenticarse con la clave pública SSH. El inicio de sesión SSH se rechaza si ese certificado caduca o se revoca y la clave pública SSH se deshabilita automáticamente.
- A partir de ONTAP 9.14.1, puede agregar opcionalmente la autenticación de dos factores Cisco Duo al proceso de autenticación SSH para mejorar la seguridad de inicio de sesión. Tras iniciar sesión por primera vez después de habilitar la autenticación de Cisco Duo, los usuarios deberán inscribir un dispositivo para que sirva como autenticador para las sesiones SSH. Consulte "Configurar Cisco Duo 2FA para inicios de sesión SSH" Para obtener más información sobre la configuración de la autenticación SSH de Cisco Duo para ONTAP.

Pasos

1. Desde un host de administración, introduzca el `ssh` comando en uno de los siguientes formatos:

- **ssh *username@hostname_or_IP* [*command*]**
- **ssh -l *username hostname_or_IP* [*command*]**

Si utiliza una cuenta de usuario de dominio de AD, debe especificar *username* en el formato de *domainname\\AD_accountname* (con barras diagonales dobles después del nombre de dominio) o "*domainname\AD_accountname*" (entre comillas dobles y con una sola barra diagonal inversa después del nombre de dominio).

hostname_or_IP Es el nombre de host o la dirección IP de la LIF de gestión de clústeres o una LIF de gestión de nodos. Se recomienda utilizar la LIF de gestión del clúster. Es posible usar una dirección IPv4 o IPv6.

command No es necesario para las sesiones interactivas con SSH.

Ejemplos de solicitudes SSH

Los siguientes ejemplos muestran cómo la cuenta de usuario denominada «'joe» puede emitir una solicitud SSH para acceder a un clúster cuya LIF de gestión de clústeres sea 10.72.137.28:

```
$ ssh joe@10.72.137.28
Password:
cluster1::> cluster show
Node                  Health  Eligibility
--------------------- ------- ------------
node1                 true    true
node2                 true    true
2 entries were displayed.
```

```
$ ssh -l joe 10.72.137.28 cluster show
Password:
Node                  Health  Eligibility
--------------------- ------- ------------
node1                 true    true
node2                 true    true
2 entries were displayed.
```

Los siguientes ejemplos muestran cómo la cuenta de usuario denominada «'john» del dominio denominado «DOMAIN1» puede emitir una solicitud SSH para acceder a un clúster cuya LIF de gestión de clústeres sea 10.72.137.28:

```
$ ssh DOMAIN1\\john@10.72.137.28
Password:
cluster1::> cluster show
Node                  Health  Eligibility
--------------------- ------- ------------
node1                 true    true
node2                 true    true
2 entries were displayed.
```

```
$ ssh -l "DOMAIN1\john" 10.72.137.28 cluster show
Password:
Node                  Health  Eligibility
--------------------- ------- ------------
node1                 true    true
node2                 true    true
2 entries were displayed.
```

En el siguiente ejemplo, se muestra cómo la cuenta de usuario llamada «'joe» puede emitir una solicitud MFA de SSH para acceder a un clúster cuyo LIF de gestión de clústeres sea 10.72.137.32:

```
$ ssh joe@10.72.137.32
Authenticated with partial success.
Password:
cluster1::> cluster show
Node                  Health  Eligibility
--------------------- ------- ------------
node1                 true    true
node2                 true    true
2 entries were displayed.
```

Información relacionada

"Autenticación de administrador y RBAC"

Seguridad de inicio de sesión SSH

A partir de ONTAP 9.5, puede ver información acerca de inicios de sesión anteriores, intentos fallidos de inicio de sesión y cambios en sus privilegios desde el último inicio de sesión correcto.

La información relacionada con la seguridad se muestra cuando inicia sesión correctamente como usuario administrador de SSH. Se le ha alertado de las siguientes condiciones:

- La última vez que se inició sesión en su nombre de cuenta.

- Número de intentos de inicio de sesión fallidos desde el último inicio de sesión correcto.
- Si el rol ha cambiado desde el último inicio de sesión (por ejemplo, si el rol de la cuenta del administrador ha cambiado de "admin" a "backup").
- Si las funcionalidades de adición, modificación o eliminación del rol se modificaron desde el último inicio de sesión.

> Si alguna de las informaciones mostradas es sospechosa, debe ponerse en contacto inmediatamente con su departamento de seguridad.

Para obtener esta información al iniciar sesión, se deben cumplir los siguientes requisitos previos:

- Su cuenta de usuario SSH debe estar aprovisionada en ONTAP.
- Se debe crear el inicio de sesión de seguridad SSH.
- Su intento de inicio de sesión debe ser correcto.

Restricciones y otras consideraciones sobre la seguridad de inicio de sesión SSH

Las siguientes restricciones y consideraciones se aplican a la información de seguridad de inicio de sesión SSH:

- La información solo está disponible para inicios de sesión basados en SSH.
- En el caso de las cuentas admin basadas en grupos, como las cuentas LDAP/NIS y AD, los usuarios pueden ver la información de inicio de sesión SSH si el grupo al que pertenecen se aprovisiona como una cuenta de administrador en ONTAP.

  Sin embargo, estos usuarios no pueden mostrar alertas sobre los cambios en el rol de la cuenta de usuario. Además, los usuarios que pertenecen a un grupo AD aprovisionado como cuenta de administrador en ONTAP no pueden ver el número de intentos de inicio de sesión fallidos que se produjeron desde la última vez que se iniciaron sesión.

- La información que se mantiene para un usuario se elimina cuando la cuenta de usuario se elimina de ONTAP.
- La información no se muestra para las conexiones con aplicaciones distintas de SSH.

Ejemplos de información de seguridad de inicio de sesión SSH

Los siguientes ejemplos muestran el tipo de información que se muestra después de iniciar sesión.

- Este mensaje se muestra después de cada inicio de sesión correcto:

```
Last Login : 7/19/2018 06:11:32
```

- Estos mensajes se muestran si no se han podido iniciar sesión desde la última sesión correcta:

```
Last Login : 4/12/2018 08:21:26
Unsuccessful login attempts since last login - 5
```

- Estos mensajes se muestran si no se ha podido iniciar sesión y los privilegios se han modificado desde el último inicio de sesión correcto:

```
Last Login : 8/22/2018 20:08:21
Unsuccessful login attempts since last login - 3
Your privileges have changed since last login
```

Active el acceso Telnet o RSH al clúster

Como práctica recomendada de seguridad, Telnet y RSH están desactivados en la directiva de firewall de administración predefinida (`mgmt`). Para permitir que el clúster acepte solicitudes Telnet o RSH, debe crear una nueva política de firewall de administración que tenga habilitada Telnet o RSH y, a continuación, asociar la nueva directiva con la LIF de administración de clústeres.

Acerca de esta tarea

ONTAP evita el cambio de políticas de firewall predefinidas, pero puede crear una nueva política clonando los predefinidos `mgmt` Política de firewall de administración y, a continuación, habilitar Telnet o RSH bajo la nueva directiva. Sin embargo, Telnet y RSH no son protocolos seguros, por lo que se debe considerar el uso de SSH para acceder al clúster. SSH proporciona un shell remoto seguro y una sesión de red interactiva.

Siga estos pasos para activar el acceso Telnet o RSH a los clústeres:

Pasos

1. Entre en el modo de privilegio avanzado:
   `set advanced`
2. Activar un protocolo de seguridad (RSH o Telnet):
   `security protocol modify -application` ***`security_protocol`*** **`-enabled true`**
3. Cree una nueva política de firewall de administración basada en `mgmt` política de firewall de gestión:
   `system services firewall policy clone -policy mgmt -destination-policy` ***`policy-name`***
4. Active Telnet o RSH en la nueva política de firewall de administración:
   `system services firewall policy create -policy` ***`policy-name`*** **`-service`** ***`security_protocol`*** **`-action allow -ip-list`** ***`ip_address/netmask`***
   Para permitir todas las direcciones IP, debe especificar `-ip-list 0.0.0.0/0`
5. Asocie la nueva política con la LIF de gestión del clúster:
   `network interface modify -vserver` ***`cluster_management_LIF`*** **`-lif cluster_mgmt -firewall-policy`** ***`policy-name`***

Acceda al clúster mediante Telnet

Puede enviar solicitudes Telnet al clúster para realizar tareas administrativas. Telnet está desactivado de forma predeterminada.

Lo que necesitará

Para poder utilizar Telnet para acceder al clúster se deben cumplir las siguientes condiciones:

- Debe tener una cuenta de usuario local de clúster configurada para utilizar Telnet como método de acceso.

  La `-application` parámetro de `security login` los comandos especifican el método de acceso para una cuenta de usuario. Para obtener más información, consulte `security login` páginas de manual.

- Telnet debe estar activado en la política de firewall de gestión que utilizan las LIF de administración del clúster o nodo para que las solicitudes Telnet puedan pasar por el firewall.

  De forma predeterminada, Telnet está desactivado. La `system services firewall policy show` con el `-service telnet` Parámetro muestra si Telnet se ha activado en una directiva de firewall. Para obtener más información, consulte `system services firewall policy` páginas de manual.

- Si utiliza conexiones IPv6, IPv6 ya debe estar configurado y habilitado en el clúster, y las políticas de firewall ya deben estar configuradas con direcciones IPv6.

  La `network options ipv6 show` Command muestra si IPv6 está habilitado. La `system services firewall policy show` comando muestra las directivas de firewall.

Acerca de esta tarea

- Telnet no es un protocolo seguro.

  Debe considerar utilizar SSH para acceder al clúster. SSH proporciona un shell remoto seguro y una sesión de red interactiva.

- ONTAP admite un máximo de 50 sesiones Telnet simultáneas por nodo.

  Si el LIF de gestión del clúster reside en el nodo, comparte este límite con la LIF de gestión del nodo.

  Si la tasa de conexiones próximas es superior a 10 por segundo, el servicio se deshabilitará temporalmente durante 60 segundos.

- Si desea acceder a la CLI de ONTAP desde un host de Windows, puede utilizar una herramienta de otro proveedor, como PuTTY.

Pasos

1. Desde un host de administración, introduzca el siguiente comando:

   `telnet` *`hostname_or_IP`*

   `hostname_or_IP` Es el nombre de host o la dirección IP de la LIF de gestión de clústeres o una LIF de gestión de nodos. Se recomienda utilizar la LIF de gestión del clúster. Es posible usar una dirección IPv4 o IPv6.

Ejemplo de una solicitud Telnet

El siguiente ejemplo muestra cómo el usuario llamado "'joe'", que se ha configurado con acceso Telnet, puede emitir una solicitud Telnet para acceder a un clúster cuya LIF de administración de clúster es 10.72.137.28:

```
admin_host$ telnet 10.72.137.28
Data ONTAP
login: joe
Password:
cluster1::>
```

Acceda al clúster mediante RSH

Puede emitir solicitudes RSH al clúster para realizar tareas administrativas. RSH no es un protocolo seguro y está deshabilitado de forma predeterminada.

Lo que necesitará

Para poder utilizar RSH, se deben cumplir las siguientes condiciones:

- Es necesario tener una cuenta de usuario local de clúster que se haya configurado para utilizar RSH como método de acceso.

  La `-application` parámetro de `security login` los comandos especifican el método de acceso para una cuenta de usuario. Para obtener más información, consulte `security login` páginas de manual.

- RSH ya debe estar habilitado en la directiva de firewall de gestión que utilizan las LIF de administración de clúster o nodo para que las solicitudes RSH puedan atravesar el firewall.

  De forma predeterminada, RSH está desactivado. La `system services firewall policy show` con el `-service rsh` Parámetro muestra si RSH se ha habilitado en una directiva de firewall. Para obtener más información, consulte `system services firewall policy` páginas de manual.

- Si utiliza conexiones IPv6, IPv6 ya debe estar configurado y habilitado en el clúster, y las políticas de firewall ya deben estar configuradas con direcciones IPv6.

  La `network options ipv6 show` Command muestra si IPv6 está habilitado. La `system services firewall policy show` comando muestra las directivas de firewall.

Acerca de esta tarea

- RSH no es un protocolo seguro.

  Debe considerar utilizar SSH para acceder al clúster. SSH proporciona un shell remoto seguro y una sesión de red interactiva.

- ONTAP admite un máximo de 50 sesiones de RSH simultáneas por nodo.

  Si el LIF de gestión del clúster reside en el nodo, comparte este límite con la LIF de gestión del nodo.

  Si la tasa de conexiones próximas es superior a 10 por segundo, el servicio se deshabilitará temporalmente durante 60 segundos.

Pasos

1. Desde un host de administración, introduzca el siguiente comando:

rsh *hostname_or_IP* -l *username:passwordcommand*

hostname_or_IP Es el nombre de host o la dirección IP de la LIF de gestión de clústeres o una LIF de gestión de nodos. Se recomienda utilizar la LIF de gestión del clúster. Es posible usar una dirección IPv4 o IPv6.

command Es el comando que desea ejecutar a través de RSH.

Ejemplo de una solicitud RSH

El siguiente ejemplo muestra cómo el usuario llamado "'joe'", que se ha configurado con acceso RSH, puede emitir una solicitud RSH para ejecutar el `cluster show` comando:

```
admin_host$ rsh 10.72.137.28 -l joe:password cluster show

Node                  Health  Eligibility
--------------------- ------- ------------
node1                 true    true
node2                 true    true
2 entries were displayed.

admin_host$
```

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.