



Gestione la autenticación de administrador y RBAC

ONTAP 9

NetApp
April 24, 2024

Tabla de contenidos

- Gestione la autenticación de administrador y RBAC 1
 - Autenticación de administrador y información general de RBAC con la interfaz de línea de comandos 1
 - Flujo de trabajo de autenticación de administrador y RBAC 1
 - Hojas de cálculo para la autenticación del administrador y la configuración de RBAC..... 3
 - Crear cuentas de inicio de sesión 17
 - Gestione los roles de control de acceso 32
 - Administrar cuentas de administrador 39
 - Gestione la verificación de varios administradores 64

Gestione la autenticación de administrador y RBAC

Autenticación de administrador y información general de RBAC con la interfaz de línea de comandos

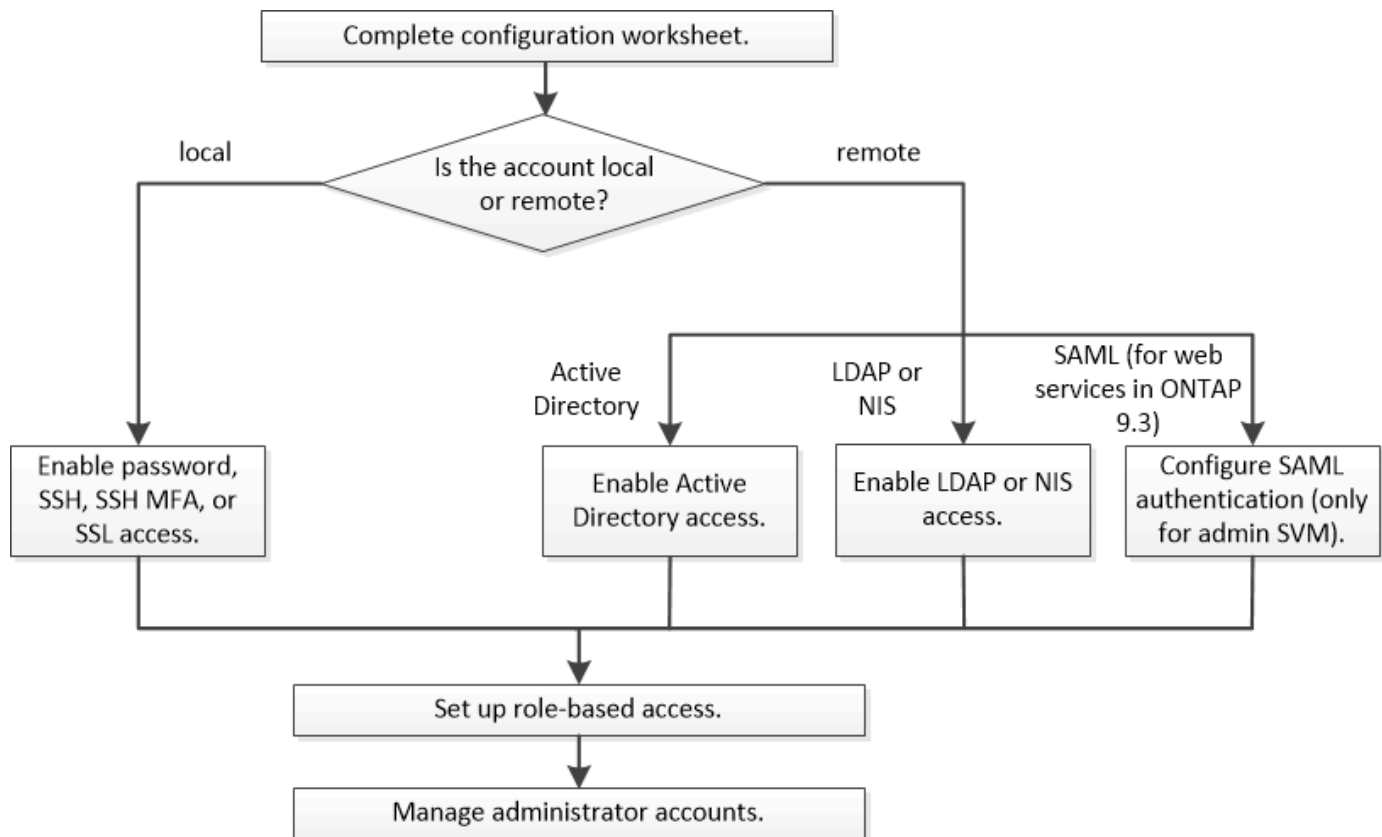
Puede habilitar cuentas de inicio de sesión para los administradores del clúster ONTAP y los administradores de máquinas virtuales de almacenamiento (SVM). También es posible usar el control de acceso basado en roles (RBAC) para definir las funcionalidades de los administradores.

Las cuentas de inicio de sesión y RBAC se habilitan de las siguientes maneras:

- Desea usar la interfaz de línea de comandos (CLI) de ONTAP, no System Manager ni una herramienta de secuencias de comandos automatizada.
- Quiere utilizar las prácticas recomendadas, no explorar todas las opciones disponibles.
- No utiliza SNMP para recopilar información sobre el clúster.

Flujo de trabajo de autenticación de administrador y RBAC

Puede habilitar la autenticación para cuentas de administrador locales o cuentas de administrador remotas. La información de cuentas de una cuenta local reside en el sistema de almacenamiento de y la información de la cuenta de una cuenta remota se encuentra en otro lugar. Cada cuenta puede tener una función predefinida o una función personalizada.



Es posible habilitar cuentas de administrador local para acceder a una SVM o una SVM de administrador con los siguientes tipos de autenticación:

- Contraseña
- Clave pública SSH
- Certificado SSL
- Autenticación multifactor (MFA) de SSH

A partir de ONTAP 9.3, se admite la autenticación con contraseña y clave pública.

Puede habilitar cuentas de administrador remoto para acceder a una SVM de administrador o a una SVM de datos con los siguientes tipos de autenticación:

- Active Directory
- Autenticación SAML (solo para SVM de administrador)

A partir de ONTAP 9.3, la autenticación del lenguaje de marcado de aserción de seguridad (SAML) puede usarse para acceder a la SVM de administración utilizando cualquiera de los siguientes servicios web: Infraestructura de procesador de servicio, API de ONTAP o System Manager.

- A partir de ONTAP 9.4, la MFA de SSH puede utilizarse para usuarios remotos en servidores LDAP o NIS. Se admite la autenticación con nsswitch y clave pública.

Hojas de cálculo para la autenticación del administrador y la configuración de RBAC

Antes de crear cuentas de inicio de sesión y configurar el control de acceso basado en roles (RBAC), debe recopilar información para cada elemento de las hojas de cálculo de configuración.

Crear o modificar cuentas de inicio de sesión

Se deben proporcionar estos valores con el `security login create` Comando cuando habilita las cuentas de inicio de sesión para acceder a una máquina virtual de almacenamiento. Se proporcionan los mismos valores con `security login modify` Comando al modificar la forma en que una cuenta accede a una máquina virtual de almacenamiento.

Campo	Descripción	Su valor
<code>-vserver</code>	El nombre de la máquina virtual de almacenamiento a la que accede la cuenta. El valor predeterminado es el nombre de la máquina virtual de almacenamiento de administrador para el clúster.	
<code>-user-or-group-name</code>	El nombre de usuario o el nombre de grupo de la cuenta. La especificación de un nombre de grupo permite el acceso a cada usuario del grupo. Puede asociar un nombre de usuario o un nombre de grupo con varias aplicaciones.	
<code>-application</code>	La aplicación que se utiliza para acceder a la VM de almacenamiento: <ul style="list-style-type: none">• <code>http</code>• <code>ontapi</code>• <code>snmp</code>• <code>ssh</code>	

-authmethod	<p>El método que se utiliza para autenticar la cuenta:</p> <ul style="list-style-type: none"> • <code>cert</code> Para la autenticación de certificados SSL • <code>domain</code> Para la autenticación de Active Directory • <code>nsswitch</code> Para la autenticación LDAP o NIS • <code>password</code> para autenticación de contraseña de usuario • <code>publickey</code> para la autenticación de claves públicas • <code>community</code> Para cadenas de comunidad SNMP • <code>usm</code> Para el modelo de seguridad de usuario SNMP • <code>saml</code> Para la autenticación del lenguaje de marcado de aserción de seguridad (SAML) 	
-remote-switch-ipaddress	<p>La dirección IP del switch remoto. El conmutador remoto puede ser un conmutador de clúster supervisado por el monitor de estado del conmutador de clúster (CSHM) o un conmutador Fibre Channel (FC) supervisado por el monitor de estado MetroCluster (MCC-HM). Esta opción sólo se aplica cuando la aplicación está <code>snmp</code> y el método de autenticación es <code>usm</code>.</p>	
-role	<p>El rol de control de acceso que se asigna a la cuenta:</p> <ul style="list-style-type: none"> • Para el clúster (la VM de almacenamiento del administrador), el valor predeterminado es <code>admin</code>. • Para una máquina virtual de almacenamiento de datos, el valor predeterminado es <code>vsadmin</code>. 	

<code>-comment</code>	(Opcional) texto descriptivo para la cuenta. El texto debe escribirse entre comillas dobles (").	
<code>-is-ns-switch-group</code>	Si la cuenta es una cuenta de grupo LDAP o una cuenta de grupo NIS (yes o. no).	
<code>-second-authentication-method</code>	<p>Segundo método de autenticación en caso de autenticación multifactor:</p> <ul style="list-style-type: none"> • <code>none</code> si no utiliza la autenticación multifactor, valor predeterminado • <code>publickey</code> para la autenticación de claves públicas cuando el <code>authmethod</code> es la contraseña o <code>nsswitch</code> • <code>password</code> para la autenticación de contraseña de usuario cuando el <code>authmethod</code> es clave pública • <code>nsswitch</code> para la autenticación de contraseña de usuario cuando <code>authmethod</code> es <code>publickey</code> <p>El orden de autenticación es siempre la clave pública seguida de la contraseña.</p>	
<code>-is-ldap-fastbind</code>	A partir de ONTAP 9.11.1, cuando se establece en <code>true</code> , habilita el enlace rápido LDAP para la autenticación <code>nsswitch</code> ; el valor predeterminado es <code>false</code> . Para utilizar el enlace rápido LDAP, el <code>-authentication-method</code> el valor se debe establecer en <code>nsswitch</code> . "Obtenga información acerca de ldap fastbind para la autenticación nsswitch."	

Configurar la información de seguridad de Cisco Duo

Se deben proporcionar estos valores con el `security login duo create` Comando cuando se habilita la autenticación de dos factores Cisco Duo con inicios de sesión SSH para una máquina virtual de almacenamiento.

Campo	Descripción	Su valor
-vserver	El equipo virtual de almacenamiento (denominado Vserver en la CLI de ONTAP) al que se aplica la configuración de autenticación Duo.	
-integration-key	Su clave de integración, obtenida al registrar su aplicación SSH con Duo.	
-secret-key	Su clave secreta, obtenida al registrar su aplicación SSH con Duo.	
-api-host	<p>El nombre de host de la API, obtenido al registrar su aplicación SSH con Duo. Por ejemplo:</p> <pre>api- <HOSTNAME>.duosecurity.com</pre>	
-fail-mode	En los errores de servicio o configuración que impiden la autenticación Duo, se produce un error <code>safe</code> (permitir acceso) o. <code>secure</code> (denegar acceso). El valor predeterminado es <code>safe</code> , Lo que significa que la autenticación DUO se omite si falla debido a errores como el servidor Duo API no es accesible.	
-http-proxy	<p>Utilice el proxy HTTP especificado. Si el proxy HTTP requiere autenticación, incluya las credenciales en la URL del proxy. Por ejemplo:</p> <pre>http- proxy=http://username :password@proxy.example.org:8080</pre>	

<p>-autopush</p>	<p>Uno de los dos <code>true</code> o <code>false</code>. El valor predeterminado es <code>false</code>. Si <code>true</code>, Duo envía automáticamente una solicitud de inicio de sesión push al teléfono del usuario, volviendo a una llamada telefónica si no está disponible push. Tenga en cuenta que esto desactiva efectivamente la autenticación de contraseña. Si <code>false</code>, se le pide al usuario que elija un método de autenticación.</p> <p>Cuando se configura con <code>autopush = true</code>, recomendamos el ajuste <code>max-prompts = 1</code>.</p>	
<p>-max-prompts</p>	<p>Si un usuario no se autentica con un segundo factor, Duo solicita al usuario que se autentique de nuevo. Esta opción establece el número máximo de peticiones de datos que Duo muestra antes de denegar el acceso. Debe ser 1, 2, o 3. El valor predeterminado es 1.</p> <p>Por ejemplo, cuando <code>max-prompts = 1</code>, el usuario debe autenticarse correctamente en la primera petición de datos, mientras que si <code>max-prompts = 2</code>, si el usuario introduce información incorrecta en el prompt inicial, se le pedirá que se autentique de nuevo.</p> <p>Cuando se configura con <code>autopush = true</code>, recomendamos el ajuste <code>max-prompts = 1</code>.</p> <p>Para la mejor experiencia, un usuario con solo autenticación <code>publickey</code> siempre tendrá <code>max-prompts</code> establezca en 1.</p>	

-enabled	Active la autenticación de dos factores Duo. Establezca en <code>true</code> de forma predeterminada. Cuando está activada, la autenticación de dos factores Duo se aplica durante el inicio de sesión SSH de acuerdo con los parámetros configurados. Cuando Duo está desactivado (establecido en <code>false</code>), se ignora la autenticación Duo.	
----------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--

Definir funciones personalizadas

Se deben proporcionar estos valores con el `security login role create` comando al definir un rol personalizado.

Campo	Descripción	Su valor
-vserver	(Opcional) Nombre del equipo virtual de almacenamiento (denominado Vserver en la CLI de ONTAP) asociado al rol.	
-role	El nombre del rol.	
-cmddirname	El comando o el directorio de comandos al que tiene acceso el rol. Debe escribir los nombres de subdirectorio de comandos entre comillas dobles ("). Por ejemplo: "volume snapshot". Debe entrar <code>DEFAULT</code> para especificar todos los directorios de comandos.	

-access	<p>(Opcional) el nivel de acceso del rol. Para directorios de comandos:</p> <ul style="list-style-type: none"> • none (el valor predeterminado para las funciones personalizadas) niega el acceso a los comandos del directorio de comandos • readonly concede acceso a show comandos del directorio de comandos y sus subdirectorios • all concede acceso a todos los comandos del directorio de comandos y sus subdirectorios <p>Para <i>comandos no intrínsecos</i> (comandos que no terminan en create, modify, delete, o. show):</p> <ul style="list-style-type: none"> • none (el valor predeterminado para los roles personalizados) niega el acceso al comando • readonly no es aplicable • all concede acceso al comando <p>Para conceder o denegar el acceso a comandos intrínsecos, debe especificar el directorio de comandos.</p>	
-query	<p>(Opcional) el objeto de consulta que se utiliza para filtrar el nivel de acceso, que se especifica en forma de una opción válida para el comando o para un comando en el directorio de comandos. El objeto de consulta debe escribirse entre comillas dobles ("). Por ejemplo, si el directorio de comandos es volume, el objeto de consulta "-aggr aggr0" habilitará el acceso para el aggr0 solo agregados.</p>	

Asociar una clave pública a una cuenta de usuario

Se deben proporcionar estos valores con el `security login publickey create` Cuando asocia una clave pública SSH a una cuenta de usuario.

Campo	Descripción	Su valor
-vserver	(Opcional) Nombre de la máquina virtual de almacenamiento a la que accede la cuenta.	
-username	El nombre de usuario de la cuenta. El valor predeterminado, <code>admin</code> , que es el nombre predeterminado del administrador del clúster.	
-index	El número de índice de la clave pública. El valor predeterminado es 0 si la clave es la primera clave que se crea para la cuenta; de lo contrario, el valor predeterminado es uno más que el número de índice más alto existente para la cuenta.	
-publickey	La clave pública de OpenSSH. La clave debe escribirse entre comillas dobles (").	
-role	El rol de control de acceso que se asigna a la cuenta.	
-comment	(Opcional) texto descriptivo para la clave pública. El texto debe escribirse entre comillas dobles (").	

-x509-certificate	<p>(Opcional) A partir de ONTAP 9.13.1, le permite gestionar la asociación de certificados X,509 con la clave pública SSH.</p> <p>Cuando asocia un certificado X,509 a la clave pública SSH, ONTAP comprueba el inicio de sesión SSH para ver si este certificado es válido. Si ha caducado o se ha revocado, el inicio de sesión no está permitido y la clave pública SSH asociada está deshabilitada. Los posibles valores son los siguientes:</p> <ul style="list-style-type: none"> • <code>install</code>: Instale el certificado X,509 codificado PEM especificado y asócielo a la clave pública SSH. Incluya el texto completo del certificado que desea instalar. • <code>modify</code>: Actualizar el certificado X,509 con codificación PEM existente con el certificado especificado y asociarlo con la clave pública SSH. Incluya el texto completo para el nuevo certificado. • <code>delete</code>: Eliminar la asociación de certificados X,509 existente con la clave pública SSH. 	
-------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--

Instale un certificado digital de servidor firmado por CA

Se deben proporcionar estos valores con el `security certificate generate-csr` Comando cuando se genera una solicitud de firma de certificación digital (CSR) para utilizarla en la autenticación de una máquina virtual de almacenamiento como un servidor SSL.

Campo	Descripción	Su valor
-common-name	El nombre del certificado, que es un nombre de dominio completo (FQDN) o un nombre común personalizado.	

-size	El número de bits de la clave privada. Cuanto mayor sea el valor, más segura será la clave. El valor predeterminado es 2048. Los valores posibles son 512, 1024, 1536, y. 2048.	
-country	El país de la máquina virtual de almacenamiento, en un código de dos letras. El valor predeterminado es US. Consulte las páginas de manual para obtener una lista de códigos.	
-state	El estado o la provincia de la máquina virtual de almacenamiento.	
-locality	La localidad de la máquina virtual de almacenamiento.	
-organization	La organización de la máquina virtual de almacenamiento.	
-unit	La unidad de la organización de la máquina virtual de almacenamiento.	
-email-addr	La dirección de correo electrónico del administrador de contacto para la máquina virtual de almacenamiento.	
-hash-function	Función de hash criptográfico para firmar el certificado. El valor predeterminado es SHA256. Los valores posibles son SHA1, SHA256, y. MD5.	

Se deben proporcionar estos valores con el `security certificate install` Comando cuando instala un certificado digital firmado por CA para utilizarlo en la autenticación del clúster o de la máquina virtual de almacenamiento como un servidor SSL. En la siguiente tabla solo se muestran las opciones relevantes para la configuración de la cuenta.

Campo	Descripción	Su valor
-vserver	Nombre de la máquina virtual de almacenamiento en la que se va a instalar el certificado.	

<code>-type</code>	<p>El tipo de certificado:</p> <ul style="list-style-type: none"> • <code>server</code> para los certificados de servidor y los certificados intermedios • <code>client-ca</code> Para el certificado de clave pública de la CA raíz del cliente SSL • <code>server-ca</code> Para el certificado de clave pública de la CA raíz del servidor SSL del que ONTAP es un cliente • <code>client</code> Para un certificado digital autofirmado o firmado por CA y una clave privada para ONTAP como cliente SSL 	
--------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--

Configurar el acceso al controlador de dominio de Active Directory

Se deben proporcionar estos valores con el `security login domain-tunnel create` Comando cuando ya configuró un servidor SMB para una máquina virtual de almacenamiento de datos y desea configurar la máquina virtual de almacenamiento como una puerta de enlace o *tunnel* para el acceso de la controladora de dominio de Active Directory al clúster.

Campo	Descripción	Su valor
<code>-vserver</code>	El nombre de la máquina virtual de almacenamiento para la que se configuró el servidor SMB.	

Se deben proporcionar estos valores con el `vserver active-directory create` Comando cuando no configuró un servidor SMB y desea crear una cuenta de equipo virtual de almacenamiento en el dominio de Active Directory.

Campo	Descripción	Su valor
<code>-vserver</code>	Nombre de la máquina virtual de almacenamiento para la que desea crear una cuenta de equipo de Active Directory.	
<code>-account-name</code>	Nombre NetBIOS de la cuenta de equipo.	
<code>-domain</code>	El nombre de dominio completo (FQDN).	

-ou	La unidad organizativa del dominio. El valor predeterminado es CN=Computers. ONTAP agrega este valor al nombre de dominio para producir el nombre distintivo de Active Directory.	
-----	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--

Configurar el acceso a servidores LDAP o NIS

Se deben proporcionar estos valores con el `vserver services name-service ldap client create` Comando cuando crea una configuración de cliente LDAP para la máquina virtual de almacenamiento.

En la tabla siguiente solo se muestran las opciones relevantes para la configuración de la cuenta:

Campo	Descripción	Su valor
-vserver	El nombre de la máquina virtual de almacenamiento para la configuración del cliente.	
-client-config	El nombre de la configuración del cliente.	
-ldap-servers	Lista separada por comas de direcciones IP y nombres de host para los servidores LDAP a los que se conecta el cliente.	
-schema	Esquema que utiliza el cliente para realizar consultas LDAP.	
-use-start-tls	<p>Si el cliente utiliza Start TLS para cifrar la comunicación con el servidor LDAP (<code>true</code> o <code>false</code>).</p> <div>  <p>Start TLS solo es compatible para el acceso a las máquinas virtuales de almacenamiento de datos. No se admite para el acceso a las máquinas virtuales de almacenamiento de administradores.</p> </div>	

Se deben proporcionar estos valores con el `vserver services name-service ldap create` Comando cuando se asocia una configuración de cliente LDAP a la máquina virtual de almacenamiento.

Campo	Descripción	Su valor
<code>-vserver</code>	Nombre de la máquina virtual de almacenamiento a la que se asociará la configuración del cliente.	
<code>-client-config</code>	El nombre de la configuración del cliente.	
<code>-client-enabled</code>	Si la máquina virtual de almacenamiento puede usar la configuración de clientes LDAP (<code>true</code> o <code>false</code>).	

Se deben proporcionar estos valores con el `vserver services name-service nis-domain create` Comando cuando se crea una configuración de dominio NIS en una máquina virtual de almacenamiento.

Campo	Descripción	Su valor
<code>-vserver</code>	Nombre de la máquina virtual de almacenamiento en la que se creará la configuración del dominio.	
<code>-domain</code>	El nombre del dominio.	
<code>-active</code>	Si el dominio está activo (<code>true</code> o <code>false</code>).	
<code>-servers</code>	ONTAP 9.0, 9.1: Lista separada por comas de direcciones IP para los servidores NIS que se utilizan en la configuración de dominio.	
<code>-nis-servers</code>	Lista separada por comas de direcciones IP y nombres de host para los servidores NIS que utiliza la configuración de dominio.	

Se deben proporcionar estos valores con el `vserver services name-service ns-switch create` al especificar el orden de búsqueda para fuentes de servicio de nombres.

Campo	Descripción	Su valor
<code>-vserver</code>	Nombre de la máquina virtual de almacenamiento en la que se va a configurar el orden de consulta del servicio de nombres.	

-database	<p>La base de datos del servicio de nombres:</p> <ul style="list-style-type: none"> • <code>hosts</code> Para los archivos y los servicios de nombres DNS • <code>group</code> Para archivos, LDAP y servicios de nombres NIS • <code>passwd</code> Para archivos, LDAP y servicios de nombres NIS • <code>netgroup</code> Para archivos, LDAP y servicios de nombres NIS • <code>namemap</code> Para archivos y servicios de nombres LDAP 	
-sources	<p>El orden en el que buscar fuentes de servicio de nombres (en una lista separada por comas):</p> <ul style="list-style-type: none"> • <code>files</code> • <code>dns</code> • <code>ldap</code> • <code>nis</code> 	

Configure el acceso SAML

A partir de ONTAP 9.3, se proporcionan estos valores con el `security saml-sp create` Comando para configurar la autenticación SAML.

Campo	Descripción	Su valor
-idp-uri	La dirección FTP o la dirección HTTP del host del proveedor de identidades (IDP) desde el que se pueden descargar los metadatos de IDP.	
-sp-host	El nombre de host o la dirección IP del host del proveedor de servicios SAML (sistema ONTAP). De manera predeterminada, se utiliza la dirección IP de la LIF de administración del clúster.	

<code>-cert-ca y. -cert-serial, o. -cert-common-name</code>	Los detalles del certificado de servidor del host del proveedor de servicios (sistema ONTAP). Puede introducir la entidad emisora de certificados (CA) del proveedor de servicios y el número de serie del certificado o el nombre común del certificado del servidor.	
<code>-verify-metadata-server</code>	Si la identidad del servidor de metadatos de IDP debe validarse (<code>true</code> o <code>false</code>). Lo más recomendable es establecer siempre este valor como <code>true</code> .	

Crear cuentas de inicio de sesión

Información general de las cuentas de inicio de sesión de

Puede habilitar cuentas de administrador de SVM y de clúster local o remoto. Una cuenta local es aquella en la que reside la información de la cuenta, la clave pública o el certificado de seguridad en el sistema de almacenamiento. La información DE la cuenta DE AD se almacena en un controlador de dominio. Las cuentas LDAP y NIS residen en servidores LDAP y NIS.

Administradores de clústeres y SVM

Un administrador de *cluster* accede a la SVM de administrador del clúster. La SVM de administrador y un administrador de clúster con el nombre reservado `admin` se crean automáticamente cuando se configura el clúster.

Un administrador de clúster con los valores predeterminados `admin` el rol puede administrar todo el clúster y sus recursos. El administrador de clúster puede crear administradores de clúster adicionales con diferentes roles según sea necesario.

Un administrador de SVM accede a una SVM de datos. El administrador de clúster crea SVM de datos y administradores de SVM según sea necesario.

A los administradores de SVM se les asigna el `vsadmin` función predeterminada. El administrador de clúster puede asignar diferentes roles a los administradores de SVM según sea necesario.

Convenciones de nomenclatura

Los siguientes nombres genéricos no se pueden utilizar para cuentas de administrador de SVM o de clúster remoto:

- `adm`
- `bandeja`
- `cli`

- demonio
- ftp
- “juegos”
- detener
- lp
- correo
- «hombre»
- «naroot»
- «NetApp»
- «noticias»
- «nadie»
- operador
- «raíz»
- apagado
- sshd
- sincronizar
- sistema
- uucp
- «www»

Roles fusionados

Si habilita varias cuentas remotas para el mismo usuario, se le asigna la unión de todas las funciones especificadas para las cuentas. Es decir, si se asigna una cuenta LDAP o NIS el `vsadmin`. Asimismo, se asigna el rol y la cuenta de grupo AD del mismo usuario `vsadmin-volume`. El rol, el usuario de AD inicia sesión con más incluido `vsadmin` funcionalidades. Se dice que los roles son *fusionado*.

Habilite el acceso de cuenta local

Habilite la información general de acceso de la cuenta local

Una cuenta local es aquella en la que reside la información de la cuenta, la clave pública o el certificado de seguridad en el sistema de almacenamiento. Puede utilizar el `security login create` Comando para habilitar cuentas locales para acceder a un administrador o una SVM de datos.

Active el acceso a la cuenta de contraseña

Puede utilizar el `security login create` Comando para habilitar las cuentas de administrador para acceder a una SVM de administrador o de datos con una contraseña. Se le pedirá la contraseña después de introducir el comando.

Acerca de esta tarea

Si no está seguro de la función de control de acceso que desea asignar a la cuenta de inicio de sesión, puede usar la `security login modify` comando para añadir el rol más adelante.

Antes de empezar

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

Paso

1. Habilite las cuentas de administrador local para acceder a una SVM mediante una contraseña:

```
security login create -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"](#).

El siguiente comando habilita la cuenta de administrador de clúster `admin1` con los predefinidos `backup` Rol para acceder a la SVM de administrador `engCluster` usar una contraseña. Se le pedirá la contraseña después de introducir el comando.

```
cluster1::>security login create -vserver engCluster -user-or-group-name
admin1 -application ssh -authmethod password -role backup
```

Habilite cuentas de clave pública de SSH

Puede utilizar el `security login create` Comando para habilitar cuentas de administrador para acceder a una SVM de administrador o de datos con una clave pública SSH.

Acerca de esta tarea

- Debe asociar la clave pública a la cuenta para que esta pueda acceder a la SVM.

[Asociación de una clave pública con una cuenta de usuario](#)

Puede realizar esta tarea antes o después de habilitar el acceso a la cuenta.

- Si no está seguro de la función de control de acceso que desea asignar a la cuenta de inicio de sesión, puede usar la `security login modify` comando para añadir el rol más adelante.

Si desea habilitar el modo FIPS en su clúster, las cuentas de claves públicas SSH existentes sin los algoritmos de clave admitidos deben volver a configurarse con un tipo de clave admitida. Las cuentas se deben volver a configurar antes de habilitar FIPS o se producirá un error en la autenticación del administrador.

La siguiente tabla indica los algoritmos de tipo de clave de host que se admiten para las conexiones SSH de ONTAP. Estos tipos de claves no se aplican a la configuración de la autenticación pública SSH.

Versión de ONTAP	Tipos de clave compatibles con el modo FIPS	Tipos de clave compatibles con el modo no FIPS
------------------	---------------------------------------------	------------------------------------------------

9.11.1 y posterior	ecdsa-sha2-nistp256	ecdsa-sha2-nistp256 rsa-sha2-512 rsa-sha2-256 ssh-ed25519 ssh-dss ssh-rsa
9.10.1 y anteriores	ecdsa-sha2-nistp256 ssh-ed25519	ecdsa-sha2-nistp256 ssh-ed25519 ssh-dss ssh-rsa



La compatibilidad con el algoritmo de clave de host ssh-ed25519 se elimina a partir de ONTAP 9.11.1.

Para obtener más información, consulte ["Configurar la seguridad de red con FIPS"](#).

Antes de empezar

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

Paso

1. Habilite cuentas de administrador local para acceder a una SVM mediante una clave pública de SSH:

```
security login create -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"](#).

El siguiente comando habilita la cuenta de administrador de SVM `svmadmin1` con los predefinidos `vsadmin-volume` Rol para acceder a la SVM `engData1` Mediante una clave pública SSH:

```
cluster1::>security login create -vserver engData1 -user-or-group-name
svmadmin1 -application ssh -authmethod publickey -role vsadmin-volume
```

Después de terminar

Si no ha asociado una clave pública a la cuenta de administrador, debe hacerlo para que la cuenta pueda acceder a la SVM.

[Asociación de una clave pública con una cuenta de usuario](#)

Habilite las cuentas de autenticación multifactor (MFA)

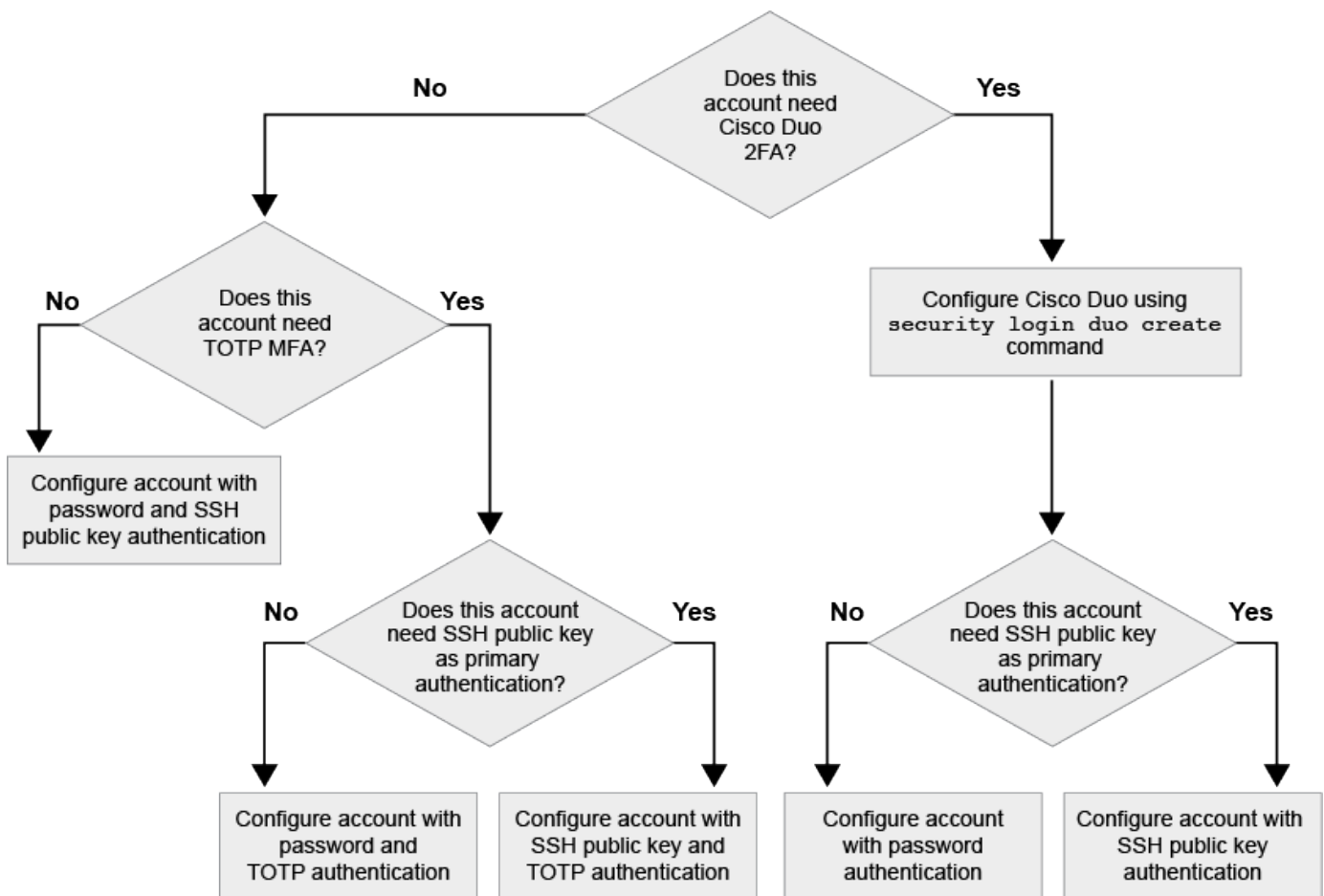
Información general de la autenticación multifactor

La autenticación multifactor (MFA) permite mejorar la seguridad al requerir que los usuarios proporcionen dos métodos de autenticación para iniciar sesión en un administrador o en un equipo virtual de almacenamiento de datos.

Dependiendo de la versión de ONTAP, puede utilizar una combinación de una clave pública SSH, una contraseña de usuario y una contraseña de un solo uso basada en el tiempo (TOTP) para la autenticación multifactor. Al habilitar y configurar Cisco Duo (ONTAP 9.14.1 y posterior), sirve como un método de autenticación adicional, que complementa los métodos existentes para todos los usuarios.

Disponible empezando por...	Primer método de autenticación	Segundo método de autenticación
ONTAP 9.14.1	Clave pública SSH	TOTP
	Contraseña de usuario	TOTP
	Clave pública SSH	Cisco Duo
	Contraseña de usuario	Cisco Duo
ONTAP 9.13.1	Clave pública SSH	TOTP
	Contraseña de usuario	TOTP
ONTAP 9,3	Clave pública SSH	Contraseña de usuario

Si se configura MFA, el administrador del clúster primero debe habilitar la cuenta de usuario local, entonces el usuario local debe configurar la cuenta.



Habilite la autenticación multifactor

La autenticación multifactor (MFA) permite mejorar la seguridad al requerir que los

usuarios proporcionen dos métodos de autenticación para iniciar sesión en un administrador o una SVM de datos.

Acerca de esta tarea

- Para realizar esta tarea, debe ser un administrador de clústeres.
- Si no está seguro de la función de control de acceso que desea asignar a la cuenta de inicio de sesión, puede usar la `security login modify` comando para añadir el rol más adelante.

"Modificar el rol asignado a un administrador"

- Si utiliza una clave pública para la autenticación, debe asociar la clave pública con la cuenta para que la cuenta pueda acceder a la SVM.

"Asociar una clave pública a una cuenta de usuario"

Puede realizar esta tarea antes o después de habilitar el acceso a la cuenta.

- A partir de ONTAP 9.12.1, puede usar dispositivos de autenticación de hardware Yubikey para la MFA del cliente SSH mediante los estándares de autenticación FIDO2 (Fast Identity Online) o de verificación de identidad personal (PIV).

Habilite MFA con clave pública SSH y contraseña de usuario

A partir de ONTAP 9.3, un administrador de clúster puede configurar cuentas de usuario locales para iniciar sesión con MFA mediante una clave pública SSH y una contraseña de usuario.

1. Habilite MFA en cuenta de usuario local con clave pública SSH y contraseña de usuario:

```
security login create -vserver <svm_name> -user-or-group-name  
<user_name> -application ssh -authentication-method <password|publickey>  
-role admin -second-authentication-method <password|publickey>
```

El siguiente comando requiere la cuenta de administrador de SVM `admin2` con los predefinidos `admin` Rol que desea iniciar sesión en la SVM `engData1` Con una clave pública SSH y una contraseña de usuario:

```
cluster-1::> security login create -vserver engData1 -user-or-group-name  
admin2 -application ssh -authentication-method publickey -role admin  
-second-authentication-method password
```

Please enter a password for user 'admin2':

Please enter it again:

Warning: To use public-key authentication, you must create a public key
for user "admin2".

Habilite MFA con TOTP

A partir de ONTAP 9.13.1, puede mejorar la seguridad al requerir que los usuarios locales inicien sesión en un

administrador o una SVM de datos con una clave pública SSH o una contraseña de usuario y una contraseña de un solo uso basada en un tiempo (TOTP). Después de habilitar la cuenta para MFA con TOTP, el usuario local debe iniciar sesión en ["complete la configuración"](#).

TOTP es un algoritmo informático que utiliza la hora actual para generar una contraseña de un solo uso. Si se utiliza TOTP, siempre es la segunda forma de autenticación después de la clave pública SSH o la contraseña de usuario.

Antes de empezar

Debe ser un administrador de almacenamiento para realizar estas tareas.

Pasos

Puede configurar MFA con una contraseña de usuario o una clave pública SSH como primer método de autenticación y TOTP como segundo método de autenticación.

Habilite MFA con contraseña de usuario y TOTP

1. Habilite una cuenta de usuario para la autenticación multifactor con una contraseña de usuario y TOTP.

Para nuevas cuentas de usuario

```
security login create -vserver <svm_name> -user-or-group-name  
<user_or_group_name> -application ssh -authentication-method  
password -second-authentication-method totp -role <role> -comment  
<comment>
```

Para cuentas de usuario existentes

```
security login modify -vserver <svm_name> -user-or-group-name  
<user_or_group_name> -application ssh -authentication-method  
password -second-authentication-method totp -role <role> -comment  
<comment>
```

2. Compruebe que MFA con TOTP está activado:

```
security login show
```

Habilite MFA con clave pública SSH y TOTP

1. Habilite una cuenta de usuario para la autenticación multifactor con una clave pública SSH y TOTP.

Para nuevas cuentas de usuario

```
security login create -vserver <svm_name> -user-or-group-name  
<user_or_group_name> -application ssh -authentication-method  
publickey -second-authentication-method totp -role <role> -comment  
<comment>
```

Para cuentas de usuario existentes

```
security login modify -vserver <svm_name> -user-or-group-name  
<user_or_group_name> -application ssh -authentication-method  
publickey -second-authentication-method totp -role <role> -comment  
<comment>
```

2. Compruebe que MFA con TOTP está activado:

```
security login show
```

Después de terminar

- Si no ha asociado una clave pública a la cuenta de administrador, debe hacerlo para que la cuenta pueda acceder a la SVM.

["Asociación de una clave pública con una cuenta de usuario"](#)

- El usuario local debe iniciar sesión para completar la configuración MFA con TOTP.

["Configure la cuenta de usuario local para MFA con TOTP"](#)

Información relacionada

Más información acerca de ["Autenticación multifactor en ONTAP 9 \(TR-4647\)"](#).

Configure la cuenta de usuario local para MFA con TOTP

A partir de ONTAP 9.13.1, las cuentas de usuario se pueden configurar con autenticación multifactor (MFA) con una contraseña de un solo uso basada en tiempo (TOTP).

Antes de empezar

- El administrador de almacenamiento debe ["Habilite MFA con TOTP"](#) como segundo método de autenticación para su cuenta de usuario.
- El método de autenticación de la cuenta de usuario principal debe ser una contraseña de usuario o una clave SSH pública.
- Debes configurar tu aplicación TOTP para que funcione con tu smartphone y crear tu clave secreta TOTP.

TOTP es compatible con varias aplicaciones de autenticación como Google Authenticator.

Pasos

1. Inicie sesión en su cuenta de usuario con el método de autenticación actual.

Su método de autenticación actual debe ser una contraseña de usuario o una clave pública SSH.

2. Cree la configuración de TOTP en su cuenta:

```
security login totp create -vserver "<svm_name>" -username  
"<account_username >"
```

3. Compruebe que la configuración de TOTP está activada en su cuenta:

```
security login totp show -vserver "<svm_name>" -username  
"<account_username>"
```

Restablezca la clave secreta TOTP

Para proteger la seguridad de su cuenta, si su clave secreta TOTP se ve comprometida o se pierde, debe deshabilitarla y crear una nueva.

Restablezca TOTP si su clave está comprometida

Si tu clave secreta TOTP está comprometida, pero aún tienes acceso a ella, puedes quitar la clave comprometida y crear una nueva.

1. Inicie sesión en su cuenta de usuario con su contraseña de usuario o clave pública SSH y su clave secreta TOTP comprometida.
2. Elimine la clave secreta TOTP comprometida:

```
security login totp delete -vserver <svm_name> -username  
<account_username>
```

3. Cree una nueva clave secreta de TOTP:

```
security login totp create -vserver <svm_name> -username  
<account_username>
```

4. Compruebe que la configuración de TOTP está activada en su cuenta:

```
security login totp show -vserver <svm_name> -username  
<account_username>
```

Restablezca TOTP si se pierde la clave

Si se pierde la clave secreta de TOTP, comuníquese con el administrador de almacenamiento de ["tener la clave desactivada"](#). Una vez desactivada la clave, puede utilizar el primer método de autenticación para iniciar sesión y configurar un nuevo TOTP.

Antes de empezar

La clave secreta de TOTP debe ser deshabilitada por un administrador de almacenamiento. Si no tiene una cuenta de administrador de almacenamiento, póngase en contacto con su administrador de almacenamiento para deshabilitar la clave.

Pasos

1. Una vez que un administrador de almacenamiento haya desactivado el secreto TOTP, utilice el método de autenticación principal para iniciar sesión en su cuenta local.
2. Cree una nueva clave secreta de TOTP:

```
security login totp create -vserver <svm_name> -username  
<account_username >
```

3. Compruebe que la configuración de TOTP está activada en su cuenta:

```
security login totp show -vserver <svm_name> -username  
<account_username>
```

Desactive la clave secreta TOTP para la cuenta local

Si se pierde la clave secreta de una sola vez basada en el tiempo (TOTP) de un usuario local, el administrador de almacenamiento debe desactivar la clave perdida antes de que el usuario pueda crear una nueva clave secreta TOTP.

Acerca de esta tarea

Esta tarea solo se puede realizar desde una cuenta de administrador de clúster.

Paso

1. Desactive la clave secreta TOTP:

```
security login totp delete -vserver "<svm_name>" -username  
"<account_username>"
```

Habilite cuentas de certificado SSL

Puede utilizar el `security login create` Comando para habilitar las cuentas de administrador para acceder a una SVM de administrador o de datos con un certificado SSL.

Acerca de esta tarea

- Para que la cuenta pueda acceder a la SVM, debe instalar un certificado digital de servidor firmado por CA.

[Generar e instalar un certificado de servidor firmado por CA](#)

Puede realizar esta tarea antes o después de habilitar el acceso a la cuenta.

- Si no está seguro del rol de control de acceso que desea asignar a la cuenta de inicio de sesión, puede añadir el rol más adelante con la `security login modify` comando.

[Modificar el rol asignado a un administrador](#)



Para las cuentas de administrador de clúster, se admite la autenticación de certificados con el `http`, `ontapi`, y `rest` más grandes. Para las cuentas de administrador de SVM, la autenticación de certificados solo se admite con el `ontapi` y `rest` más grandes.

Paso

1. Habilite las cuentas de administrador local para acceder a una SVM mediante un certificado SSL:

```
security login create -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 ["Páginas manuales de ONTAP por versión"](#).

El siguiente comando habilita la cuenta de administrador de SVM `svmadmin2` con el valor predeterminado `vsadmin` Rol para acceder a la `SVMengData2` Mediante un certificado digital SSL.

```
cluster1::>security login create -vserver engData2 -user-or-group-name
svmadmin2 -application ontapi -authmethod cert
```

Después de terminar

Si no instaló un certificado digital de servidor firmado por CA, debe hacerlo para que la cuenta pueda acceder a la SVM.

[Generar e instalar un certificado de servidor firmado por CA](#)

Habilite el acceso de cuenta de Active Directory

Puede utilizar el `security login create` Comando para habilitar cuentas de usuarios o grupos de Active Directory (AD) para acceder a un administrador o a la SVM de datos. Cualquier usuario del grupo de AD puede acceder a la SVM con el rol asignado al grupo.

Acerca de esta tarea

- Para poder acceder a la SVM, es necesario configurar el acceso de la controladora de dominio de AD al clúster o a la SVM.

[Configuración del acceso al controlador de dominio de Active Directory](#)

Puede realizar esta tarea antes o después de habilitar el acceso a la cuenta.

- A partir de ONTAP 9.13.1, puede usar una clave pública SSH como método de autenticación principal o secundario con una contraseña de usuario de AD.

Si elige usar una clave pública SSH como autenticación principal, no se realiza ninguna autenticación de AD.

- A partir de ONTAP 9.11.1, se puede utilizar ["Enlace rápido LDAP para la autenticación nsswitch"](#) Si es compatible con el servidor LDAP de AD.
- Si no está seguro de la función de control de acceso que desea asignar a la cuenta de inicio de sesión, puede usar la `security login modify` comando para añadir el rol más adelante.

[Modificar el rol asignado a un administrador](#)



El acceso a la cuenta DE grupo DE AD solo se admite con SSH, `ontapi`, y. rest más grandes. Los grupos de AD no se admiten con la autenticación de clave pública SSH, que se utiliza comúnmente para la autenticación multifactor.

Antes de empezar

- La hora del clúster debe sincronizarse con un plazo de cinco minutos desde la hora del controlador de dominio de AD.
- Para realizar esta tarea, debe ser un administrador de clústeres.

Paso

1. Habilite las cuentas de administrador de usuario o de grupo de AD para acceder a una SVM:

Para usuarios de AD:

Versión de ONTAP	Autenticación principal	Autenticación secundaria	Comando
9.13.1 y posterior	Clave pública	Ninguno	<pre>security login create -vserver <svm_name> -user-or-group-name <user_name> -application ssh -authentication-method publickey -role <role></pre>
9.13.1 y posterior	Dominio	Clave pública	<p>Para un nuevo usuario</p> <pre>security login create -vserver <svm_name> -user-or-group-name <user_name> -application ssh -authentication-method domain -second -authentication-method publickey -role <role></pre> <p>Para un usuario existente</p> <pre>security login modify -vserver <svm_name> -user-or-group-name <user_name> -application ssh -authentication-method domain -second -authentication-method publickey -role <role></pre>

Versión de ONTAP	Autenticación principal	Autenticación secundaria	Comando
9,0 y posterior	Dominio	Ninguno	<pre>security login create -vserver <svm_name> -user-or-group-name <user_name> -application <application> -authentication-method domain -role <role> -comment <comment> [-is-ldap- fastbind true]</pre>

Para grupos AD:

Versión de ONTAP	Autenticación principal	Autenticación secundaria	Comando
9,0 y posterior	Dominio	Ninguno	<pre>security login create -vserver <svm_name> -user-or-group-name <user_name> -application <application> -authentication-method domain -role <role> -comment <comment> [-is-ldap- fastbind true]</pre>

Para obtener una sintaxis completa del comando, consulte ["Hojas de trabajo para la autenticación de administrador y la configuración de RBAC"](#)

Después de terminar

Si no configuró el acceso de la controladora de dominio de AD al clúster o a la SVM, debe hacerlo antes de que la cuenta pueda acceder a la SVM.

[Configuración del acceso al controlador de dominio de Active Directory](#)

Habilite el acceso a cuenta de LDAP o NIS

Puede utilizar el `security login create` Comando para habilitar cuentas de usuario LDAP o NIS para acceder a un administrador o una SVM de datos. Si no ha configurado el acceso del servidor LDAP o NIS a la SVM, debe hacerlo antes de que la cuenta pueda acceder a la SVM.

Acerca de esta tarea

- Las cuentas de grupo no son compatibles.
- Para que la cuenta pueda acceder a la SVM, debe configurar el acceso del servidor LDAP o NIS con la SVM.

[Configurar el acceso a servidores LDAP o NIS](#)

Puede realizar esta tarea antes o después de habilitar el acceso a la cuenta.

- Si no está seguro de la función de control de acceso que desea asignar a la cuenta de inicio de sesión, puede usar la `security login modify` comando para añadir el rol más adelante.

Modificar el rol asignado a un administrador

- A partir de ONTAP 9.4, la autenticación multifactor (MFA) es compatible para usuarios remotos a través de servidores LDAP o NIS.
- A partir de ONTAP 9.11.1, se puede utilizar ["Enlace rápido LDAP para la autenticación nsswitch"](#) Si es compatible con el servidor LDAP.
- Debido a un problema LDAP conocido, no debe utilizar el ' : ' (Dos puntos) carácter en cualquier campo de la información de la cuenta de usuario LDAP (por ejemplo, `gecos`, `userPassword`, y así sucesivamente). De lo contrario, la operación de búsqueda fallará para ese usuario.

Antes de empezar

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

Pasos

1. Habilite las cuentas de usuario o grupo de LDAP o NIS para acceder a una SVM:

```
security login create -vserver SVM_name -user-or-group-name user_name  
-application application -authmethod nsswitch -role role -comment comment -is  
-ns-switch-group yes|no [-is-ldap-fastbind true]
```

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

"Crear o modificar cuentas de inicio de sesión"

El siguiente comando habilita la cuenta de administrador de clúster LDAP o NIS `guest2` con los predefinidos `backup` Rol para acceder a la SVM de `administradorengCluster`.

```
cluster1::>security login create -vserver engCluster -user-or-group-name  
guest2 -application ssh -authmethod nsswitch -role backup
```

2. Habilitar el inicio de sesión MFA para usuarios de LDAP o NIS:

```
security login modify -user-or-group-name rem_usr1 -application ssh  
-authentication-method nsswitch -role admin -is-ns-switch-group no -second  
-authentication-method publickey
```

El método de autenticación se puede especificar como `publickey` y el segundo método de autenticación como `nsswitch`.

En el siguiente ejemplo, se muestra la autenticación MFA que está habilitada:

```
cluster-1::*> security login modify -user-or-group-name rem_usr2  
-application ssh -authentication-method nsswitch -vserver  
cluster-1 -second-authentication-method publickey"
```

Después de terminar

Si no ha configurado el acceso del servidor LDAP o NIS a la SVM, debe hacerlo antes de que la cuenta pueda acceder a la SVM.

[Configurar el acceso a servidores LDAP o NIS](#)

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` el 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**.

Administrar cuentas de administrador

Información general sobre las cuentas de administrador

En función de cómo haya habilitado el acceso a una cuenta, puede que deba asociar una clave pública a una cuenta local, instalar un certificado digital de servidor firmado por CA o configurar AD, LDAP o NIS. Es posible realizar todas estas tareas antes o después de habilitar el acceso a la cuenta.

Asociar una clave pública a una cuenta de administrador

Para la autenticación de clave pública SSH, debe asociar la clave pública a una cuenta de administrador para que la cuenta pueda acceder a la SVM. Puede utilizar el `security login publickey create` comando para asociar una clave a una cuenta de administrador.

Acerca de esta tarea

Si autentica una cuenta a través de SSH tanto con una contraseña como con una clave pública SSH, la cuenta se autentica primero con la clave pública.

Antes de empezar

- Debe haber generado la clave SSH.
- Debe ser un administrador de clúster o de SVM para ejecutar esta tarea.

Pasos

1. Asociar una clave pública a una cuenta de administrador:

```
security login publickey create -vserver SVM_name -username user_name -index  
index -publickey certificate -comment comment
```

Para obtener una sintaxis completa del comando, consulte la referencia de la hoja de datos de ["Asociación"](#)

de una clave pública con una cuenta de usuario".

2. Verifique el cambio visualizando la clave pública:

```
security login publickey show -vserver SVM_name -username user_name -index index
```

Ejemplo

El siguiente comando asocia una clave pública con la cuenta de administrador de SVM `svmin1`. Para la SVM `engData1`. A la clave pública se le asigna el número de índice 5.

```
cluster1::> security login publickey create -vserver engData1 -username svmin1 -index 5 -publickey "<key text>"
```

Gestione claves públicas SSH y certificados X,509 para una cuenta de administrador

Para una mayor seguridad de autenticación SSH con cuentas de administrador, puede utilizar el `security login publickey` Conjunto de comandos para administrar la clave pública SSH y su asociación con certificados X,509.

Asocie una clave pública y un certificado X,509 a una cuenta de administrador

A partir de ONTAP 9.13.1, puede asociar un certificado X,509 a la clave pública asociada a la cuenta de administrador. Esto le proporciona la seguridad añadida de las comprobaciones de caducidad o revocación de certificados al iniciar sesión SSH para esa cuenta.

Acerca de esta tarea

Si autentica una cuenta a través de 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 rechazará si ese certificado caduca o se revoca y la clave pública se deshabilitará automáticamente.

Antes de empezar

- Debe ser un administrador de clúster o de SVM para ejecutar esta tarea.
- Debe haber generado la clave SSH.
- Si solo necesita que el certificado X,509 sea verificado para su vencimiento, puede usar un certificado autofirmado.
- Si necesita que el certificado X,509 sea comprobado para su vencimiento y revocación:
 - Debe haber recibido el certificado de una CA.
 - Debe instalar la cadena de certificados (certificados de CA intermedios y raíz) mediante `security certificate install` comandos.
 - Debe habilitar OCSP para SSH. Consulte ["Verifique que los certificados digitales sean válidos mediante OCSP"](#) si desea obtener instrucciones.

Pasos

1. Asocie una clave pública y un certificado X,509 a una cuenta de administrador:

```
security login publickey create -vserver SVM_name -username user_name -index
index -publickey certificate -x509-certificate install
```

Para obtener una sintaxis completa del comando, consulte la referencia de la hoja de datos de ["Asociación de una clave pública con una cuenta de usuario"](#).

2. Verifique el cambio visualizando la clave pública:

```
security login publickey show -vserver SVM_name -username user_name -index
index
```

Ejemplo

El siguiente comando asocia una clave pública y un certificado X,509 con la cuenta de administrador de SVM svmin2 Para la SVM engData2. A la clave pública se le asigna el número de índice 6.

```
cluster1::> security login publickey create -vserver engData2 -username
svmin2 -index 6 -publickey
"<key text>" -x509-certificate install
Please enter Certificate: Press <Enter> when done
<certificate text>
```

Elimine la asociación de certificados de la clave pública SSH para una cuenta de administrador

Puede eliminar la asociación de certificados actual de la clave pública SSH de la cuenta, mientras conserva la clave pública.

Antes de empezar

Debe ser un administrador de clúster o de SVM para ejecutar esta tarea.

Pasos

1. Elimine la asociación de certificados X,509 de una cuenta de administrador y conserve la clave pública SSH existente:

```
security login publickey modify -vserver SVM_name -username user_name -index
index -x509-certificate delete
```

2. Verifique el cambio visualizando la clave pública:

```
security login publickey show -vserver SVM_name -username user_name -index
index
```

Ejemplo

El siguiente comando quita la asociación de certificados X,509 de la cuenta de administrador de SVM svmin2 Para la SVM engData2 en el índice número 6.

```
cluster1::> security login publickey modify -vserver engData2 -username
svmin2 -index 6 -x509-certificate delete
```

Elimine la asociación de clave pública y certificado de una cuenta de administrador

Puede eliminar la configuración de clave pública y certificado actual de una cuenta.

Antes de empezar

Debe ser un administrador de clúster o de SVM para ejecutar esta tarea.

Pasos

1. Elimine la clave pública y una asociación de certificados X,509 de una cuenta de administrador:

```
security login publickey delete -vserver SVM_name -username user_name -index  
index
```

2. Verifique el cambio visualizando la clave pública:

```
security login publickey show -vserver SVM_name -username user_name -index  
index
```

Ejemplo

El siguiente comando quita una clave pública y un certificado X,509 de la cuenta de administrador de SVM svmin3 Para la SVM engData3 en el índice número 7.

```
cluster1::> security login publickey delete -vserver engData3 -username  
svmin3 -index 7
```

Configurar Cisco Duo 2FA para inicios de sesión SSH

A partir de ONTAP 9.14.1, puede configurar ONTAP para que use Cisco Duo para la autenticación de dos factores (2FA) durante los inicios de sesión SSH. Se configura Duo a nivel de clúster y se aplica a todas las cuentas de usuario de forma predeterminada. También puede configurar Duo a nivel del equipo virtual de almacenamiento (anteriormente denominado Vserver), en cuyo caso sólo se aplica a los usuarios para dicho equipo virtual de almacenamiento. Si habilita y configura DUO, sirve como un método de autenticación adicional, que complementa los métodos existentes para todos los usuarios.

Si habilita la autenticación Duo para los inicios de sesión SSH, los usuarios tendrán que inscribir un dispositivo la próxima vez que inicien sesión con SSH. Para obtener información sobre la inscripción, consulte el Cisco Duo ["documentación de inscripción"](#).

Puede utilizar la interfaz de línea de comandos de ONTAP para realizar las siguientes tareas con Cisco Duo:

- [Configurar Cisco Duo](#)
- [Cambie la configuración de Cisco Duo](#)
- [Elimine la configuración de Cisco Duo](#)
- [Vea la configuración de Cisco Duo](#)
- [Eliminar un grupo Duo](#)

- [Ver grupos Duo](#)
- [Omitir autenticación Duo para usuarios](#)

Configurar Cisco Duo

Puede crear una configuración de Cisco Duo para todo el clúster o para un equipo virtual de almacenamiento específico (denominado Vserver en la CLI de ONTAP) mediante el `security login duo create` comando. Cuando hace esto, Cisco Duo se habilita para inicios de sesión SSH para este clúster o máquina virtual de almacenamiento.

Pasos

1. Inicie sesión en el panel de administración de Cisco Duo.
2. Vaya a **Aplicaciones > Aplicación UNIX**.
3. Registre la clave de integración, la clave secreta y el nombre de host de la API.
4. Inicie sesión en su cuenta de ONTAP con SSH.
5. Habilite la autenticación de Cisco Duo para esta VM de almacenamiento, sustituyendo la información de su entorno por los valores entre paréntesis:

```
security login duo create \  
-vserver <STORAGE_VM_NAME> \  
-integration-key <INTEGRATION_KEY> \  
-secret-key <SECRET_KEY> \  
-apihost <API_HOSTNAME>
```

Para obtener más información sobre los parámetros necesarios y opcionales para este comando, consulte ["Hojas de cálculo para la autenticación del administrador y la configuración de RBAC"](#).

Cambie la configuración de Cisco Duo

Puede cambiar la forma en que Cisco Duo autentica a los usuarios (por ejemplo, cuántas peticiones de datos de autenticación se dan o qué proxy HTTP se utiliza). Si necesita cambiar la configuración de Cisco Duo para un equipo virtual de almacenamiento (conocido como Vserver en la CLI de ONTAP), puede utilizar el `security login duo modify` comando.

Pasos

1. Inicie sesión en el panel de administración de Cisco Duo.
2. Vaya a **Aplicaciones > Aplicación UNIX**.
3. Registre la clave de integración, la clave secreta y el nombre de host de la API.
4. Inicie sesión en su cuenta de ONTAP con SSH.
5. Cambie la configuración de Cisco Duo para esta máquina virtual de almacenamiento, sustituyendo la información actualizada de su entorno por los valores entre paréntesis:

```
security login duo modify \  
-vserver <STORAGE_VM_NAME> \  
-integration-key <INTEGRATION_KEY> \  
-secret-key <SECRET_KEY> \  
-apihost <API_HOSTNAME> \  
-pushinfo true|false \  
-http-proxy <HTTP_PROXY_URL> \  
-autopush true|false \  
-prompts 1|2|3 \  
-max-unenrolled-logins <NUM_LOGINS> \  
-is-enabled true|false \  
-fail-mode safe|secure
```

Elimine la configuración de Cisco Duo

Puede eliminar la configuración de Cisco Duo, que eliminará la necesidad de que los usuarios de SSH se autenticuen mediante Duo al iniciar sesión. Para eliminar la configuración de Cisco Duo para un equipo virtual de almacenamiento (denominado Vserver en la CLI de ONTAP), puede utilizar el `security login duo delete` comando.

Pasos

1. Inicie sesión en su cuenta de ONTAP con SSH.
2. Elimine la configuración de Cisco Duo para esta máquina virtual de almacenamiento y sustituya el nombre de máquina virtual de almacenamiento para `<STORAGE_VM_NAME>`:

```
security login duo delete -vserver <STORAGE_VM_NAME>
```

De este modo se elimina de forma permanente la configuración de Cisco Duo para este equipo virtual de almacenamiento.

Vea la configuración de Cisco Duo

Puede ver la configuración existente de Cisco Duo para un equipo virtual de almacenamiento (denominado Vserver en la CLI de ONTAP) mediante el `security login duo show` comando.

Pasos

1. Inicie sesión en su cuenta de ONTAP con SSH.
2. Muestre la configuración de Cisco Duo para esta máquina virtual de almacenamiento. Opcionalmente, puede utilizar la `vserver` Parámetro para especificar una máquina virtual de almacenamiento, en lugar del nombre de la máquina virtual de almacenamiento para `<STORAGE_VM_NAME>`:

```
security login duo show -vserver <STORAGE_VM_NAME>
```

Debería ver una salida similar a la siguiente:

```
Vserver: testcluster
Enabled: true

Status: ok
INTEGRATION-KEY: DI89811J9JWMJCCO7IOH
SKEY SHA Fingerprint:
b79ffa4b1c50b1c747fbacdb34g671d4814
API Host: api-host.duosecurity.com
Autopush: true
Push info: true
Failmode: safe
Http-proxy: 192.168.0.1:3128
Prompts: 1
Comments: -
```

Cree un grupo Duo

Puede indicar a Cisco Duo que incluya solo los usuarios de un determinado Active Directory, LDAP o grupo de usuarios local en el proceso de autenticación Duo. Si crea un grupo Duo, sólo se solicita la autenticación Duo a los usuarios de ese grupo. Puede crear un grupo Duo mediante `security login duo group create` comando. Al crear un grupo, opcionalmente puede excluir usuarios específicos de ese grupo del proceso de autenticación Duo.

Pasos

1. Inicie sesión en su cuenta de ONTAP con SSH.
2. Cree el grupo DUO, sustituyendo la información del entorno por los valores entre paréntesis. Si omite `-vserver` parámetro, el grupo se crea en el nivel de clúster:

```
security login duo group create -vserver <STORAGE_VM_NAME> -group-name
<GROUP_NAME> -exclude-users <USER1, USER2>
```

El nombre del grupo Duo debe coincidir con un directorio activo, LDAP o grupo local. Usuarios que especifique con el opcional `-exclude-users` El parámetro no se incluirá en el proceso de autenticación Duo.

Ver grupos Duo

Puede ver las entradas de grupo Cisco Duo existentes mediante el `security login duo group show` comando.

Pasos

1. Inicie sesión en su cuenta de ONTAP con SSH.
2. Muestra las entradas del grupo Duo, sustituyendo la información del entorno por los valores entre paréntesis. Si omite `-vserver` parámetro, el grupo se muestra en el nivel de clúster:

```
security login duo group show -vserver <STORAGE_VM_NAME> -group-name  
<GROUP_NAME> -exclude-users <USER1, USER2>
```

El nombre del grupo Duo debe coincidir con un directorio activo, LDAP o grupo local. Usuarios que especifique con el opcional `-exclude-users` no se mostrará el parámetro.

Eliminar un grupo Duo

Puede eliminar una entrada de grupo Duo mediante `security login duo group delete` comando. Si elimina un grupo, los usuarios de ese grupo ya no se incluirán en el proceso de autenticación Duo.

Pasos

1. Inicie sesión en su cuenta de ONTAP con SSH.
2. Elimine la entrada de grupo Duo, sustituyendo la información de su entorno por los valores entre paréntesis. Si omite `-vserver` parámetro, el grupo se elimina en el nivel de clúster:

```
security login duo group delete -vserver <STORAGE_VM_NAME> -group-name  
<GROUP_NAME>
```

El nombre del grupo Duo debe coincidir con un directorio activo, LDAP o grupo local.

Omitir autenticación Duo para usuarios

Puede excluir a todos los usuarios o usuarios específicos del proceso de autenticación Duo SSH.

Excluir todos los usuarios de DUO

Puede deshabilitar la autenticación SSH de Cisco Duo para todos los usuarios.

Pasos

1. Inicie sesión en su cuenta de ONTAP con SSH.
2. Desactive la autenticación de Cisco Duo para usuarios SSH, sustituyendo el nombre de Vserver por `<STORAGE_VM_NAME>`:

```
security login duo -vserver <STORAGE_VM_NAME> -is-duo-enabled=false
```

Excluir usuarios del grupo DUO

Puede excluir ciertos usuarios que forman parte de un grupo Duo del proceso de autenticación Duo SSH.

Pasos

1. Inicie sesión en su cuenta de ONTAP con SSH.
2. Desactive la autenticación de Cisco Duo para usuarios específicos de un grupo. Sustituya el nombre de grupo y la lista de usuarios para excluir los valores entre paréntesis:


```
security login group modify -group-name <GROUP_NAME> -exclude-users  
<USER1, USER2>
```

El nombre del grupo Duo debe coincidir con un directorio activo, LDAP o grupo local. Usuarios que especifique con `-exclude-users` El parámetro no se incluirá en el proceso de autenticación Duo.

Excluir usuarios locales de DUO

Puede excluir a usuarios locales específicos del uso de la autenticación Duo mediante el panel de administración de Cisco Duo. Para obtener instrucciones, consulte ["Documentación de Cisco Duo"](#).

Genere e instale una información general de certificados de servidor firmados por CA

En los sistemas de producción, se recomienda instalar un certificado digital firmado por CA para usarlo en la autenticación del clúster o SVM como servidor SSL. Puede utilizar el `security certificate generate-csr` Para generar una solicitud de firma de certificación (CSR) y la `security certificate install` comando para instalar el certificado que recibe de la autoridad de certificación.

Genere una solicitud de firma de certificación

Puede utilizar el `security certificate generate-csr` Comando para generar una solicitud de firma de certificación (CSR). Después de procesar la solicitud, la entidad de certificación (CA) envía el certificado digital firmado.

Antes de empezar

Debe ser un administrador de clúster o de SVM para ejecutar esta tarea.

Pasos

1. Genere una CSR:

```
security certificate generate-csr -common-name FQDN_or_common_name -size  
512|1024|1536|2048 -country country -state state -locality locality  
-organization organization -unit unit -email-addr email_of_contact -hash  
-function SHA1|SHA256|MD5
```

El siguiente comando crea un CSR con una clave privada de 2048 bits generada por la función de hash «SHA256» para su uso por el grupo «Software» en el departamento «IT» de una empresa cuyo nombre común personalizado es «`server1.companyname.com``», ubicada en Sunnyvale, California, EE.UU. La dirección de correo electrónico del administrador de contacto de SVM es «`web@example.com`». El sistema muestra la CSR y la clave privada en la salida.

Ejemplo de creación de una CSR

```
cluster1::>security certificate generate-csr -common-name  
server1.companyname.com -size 2048 -country US -state California  
-locality Sunnyvale -organization IT -unit Software -email-addr  
web@example.com -hash-function SHA256
```

Certificate Signing Request :

-----BEGIN CERTIFICATE REQUEST-----

```
MIIBGjCBxQIBADBgMRQwEgYDVQQDEwtleGFtcGxlLmNvbTELMakGA1UEBhMCVVMx  
CTAHBgNVBAgTADRJMAcGA1UEBxMAMQkwBwYDVQQKEwAxCTAHBgNVBAStADEPMA0G  
CSqGSIB3DQEJARYAMFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAPXFanNoJApTlnzS  
xOcxixqImRRGZCR7tVmTYyqPSuTvfVtWdJbmXuj6U3alwoUsb13wfEvQnHVFNCi  
2ninsJ8CAwEAAaAAMA0GCSqGSIB3DQEBChUAA0EA6EagLfso5+4g+ejiRKKTUPQO  
UqOUEoKuvxhOvPC2w7b//fNSFsFHvXloqEOhYECn/NX9h8mbphCoM5YZ4OfnKw==  
-----END CERTIFICATE REQUEST-----
```

Private Key :

-----BEGIN RSA PRIVATE KEY-----

```
MIIBOwIBAAJBAPXFanNoJApTlnzSxOcxixqImRRGZCR7tVmTYyqPSuTvfVtWdJb  
mXuj6U3alwoUsb13wfEvQnHVFNCi2ninsJ8CAwEAAQJAWt2AO+bW3FKezEuIrQlu  
KoMyRYK455wtMk8BrOyJfhYsB20B28eifjJvRWdTOBEav99M7cEzgPv+p5kaZTTM  
gQIhAPsp+j1hrUXSRj979LIJJY0sNez397i7ViFXWQScx/ehAiEA+oDbOooWlVvu  
xj4aitxVBu6ByVckYU8LbsfeRNsZwD8CIQCbZ1/ENvmlJ/P7N9Exj2NCtEYxd0Q5  
cwBZ5NfZeMBpwQIhAPk0KWQSLadGfsKO077itF+h9FGFNHbtuNTrVq4vPW3nAiAA  
peMBQgEv28y2r8D4dkYzxcXmjzJluUSZSZ9c/wS6fA==  
-----END RSA PRIVATE KEY-----
```

Note: Please keep a copy of your certificate request and private key for future reference.

2. Copie la solicitud de certificado de la salida CSR y envíela en formato electrónico (por ejemplo, correo electrónico) a una CA de terceros de confianza para su firma.

Después de procesar la solicitud, la CA envía el certificado digital firmado. Debe conservar una copia de la clave privada y el certificado digital firmado por la CA.

Instale un certificado de servidor firmado por CA

Puede utilizar el `security certificate install` Comando para instalar un certificado de servidor firmado por CA en una SVM. ONTAP solicita los certificados raíz y intermedios de la entidad de certificación (CA) que forman la cadena de certificados del certificado de servidor.

Antes de empezar

Debe ser un administrador de clúster o de SVM para ejecutar esta tarea.

Paso

1. Instale un certificado de servidor firmado por CA:

```
security certificate install -vserver SVM_name -type certificate_type
```

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



ONTAP solicita los certificados intermedios y de raíz de CA que forman la cadena de certificados del certificado de servidor. La cadena comienza con el certificado de la CA que emitió el certificado de servidor y puede llegar hasta el certificado raíz de la CA. Cualquier certificado intermedio que falte provocará el error en la instalación del certificado de servidor.

El siguiente comando instala el certificado de servidor firmado por CA y los certificados intermedios en SVM 'engData2'.

Ejemplo de instalación de certificados intermedios de certificado de servidor firmados por CA

```
cluster1::>security certificate install -vserver engData2 -type
server
Please enter Certificate: Press <Enter> when done
-----BEGIN CERTIFICATE-----
MIIB8TCCA ZugAwIBAwIBADANBgkqhkiG9w0BAQQFADBfMRMwEQYDVQQDEwpuZXRh
cHAuY29tMQswCQYDVQQGEwJVUzEJMAcGA1UECBMAMQkwBwYDVQQHEwAxCTAHBgNV
BAoTADAEJMAcGA1UECXMAMQ8wDQYJKoZIhvcNAQkBFgAwHhcNMTAwNDI2MTk0OTI4
WhcNMTAwNTI2MTk0OTI4WjBfMRMwEQYDVQQDEwpuZXRhcHAuY29tMQswCQYDVQQG
EwJVUzEJMAcGA1UECBMAMQkwBwYDVQQHEwAxCTAHBgNVBAoTADAEJMAcGA1UECXM
AMQ8wDQYJKoZIhvcNAQkBFgAwXDANBgkqhkiG9w0BAQEFAANLADBIAkEAyXrK2sry
-----END CERTIFICATE-----
```

```
Please enter Private Key: Press <Enter> when done
-----BEGIN RSA PRIVATE KEY-----
MIIBPAIBAAJBAMl6ytrK8nQj82UsWeHOeT8gk0BPX+Y5MLyCsUdXA7hXhumHNpvF
C6lX2G32Sx8VEalth94tx+vOEzq+UaqHlt0CAwEAAQJBAMZjDWlgmlm3qIr/n8VT
PFnnZnbVcXVM70tbUsgPKw+QCCh9dF1jmuQKeDr+wUMWkn1DeGrfhILpzfJGHRlJ
z7UCIQDr8d3gOG7lUyX+BbFmo/N0uAKjS2cvUU+Y8a8pDxGLLwIhANqa99SuS18U
DiPvdaKTj6+EcGuXfCXz+G0rfgTZK8uzAiEArlmnrfYC8KwE9k7A0ylRzBLdUwK9
AvuJDn+/z+H1Bd0CIQDD93P/xpaJETNz53Au49VE5Jba/Jugckrbosd/lSd7nQIg
aEMAZt6qHHT4mndi8Bo8sDGedG2SKx6Qbn2IpuNZ7rc=
-----END RSA PRIVATE KEY-----
```

Do you want to continue entering root and/or intermediate
certificates {y|n}: y

```
Please enter Intermediate Certificate: Press <Enter> when done
-----BEGIN CERTIFICATE-----
MIIE+zCCBGSGAwIBAgICAQ0wDQYJKoZIhvcNAQEFBQAwgbsxJDAiBgNVBAcTG1Zh
bGlDZXJ0IFZhbG1kYXRpb24gTmV0d29yazEXMBUGA1UEChMOVmFsaUNlcnQsIElu
Yy4xNTAzBgNVBAsTTFZhbG1DZXJ0IENsYXNzIDIGUG9saWN5IFZhbG1kYXRpb24g
QXV0aG9yaXR5MSEwHwYDVQQDExhodHRwOi8vd3d3LnZhbG1jZXJ0LmNvbS8xIDAe
BgkqhkiG9w0BCQEWEluZm9AdmFsaWNlcnQuY29tMB4XDTA0MDYyOTE3MDYyMFoX
DTI0MDYyOTE3MDYyMFowYzELMAkGA1UEBhMCVVMxITAfBgNVBAoTGFROZSBHbyBE
YWRkeSBHcm91cCwgSW5jLjExMC8GA1UECXMOR28gRGFkZkhkgQ2xhc3MgMiBDZXJ0
-----END CERTIFICATE-----
```

Do you want to continue entering root and/or intermediate
certificates {y|n}: y

```
Please enter Intermediate Certificate: Press <Enter> when done
-----BEGIN CERTIFICATE-----
```

```
MIIC5zCCAlACAQEwDQYJKoZIhvcNAQEFBQAwbgsxJDAiBgNVBACGTG1ZhbG1DZXJ0
IFZhbG1kYXRpb24gTmV0d29yazEXMBUGA1UEChMOVmFsaUNlcnQsIEluYy4xNTAz
BgNVBAsTTFZhbG1DZXJ0IENsYXNzIDIGUG9saWN5IFZhbG1kYXRpb24gQXV0aG9y
aXR5MSEwHwYDVQQDEzhodHRwOi8vd3d3LnZhbG1jZXJ0LmNvbS8xIDAeBgkqhkiG
9w0BCQEWEluZm9AdmFsaWNlcnQuY29tMB4XDTE5MDYyNjAwMTk1NFoXDTE5MDYy
NjAwMTk1NFowgbsxJDAiBgNVBACGTG1ZhbG1DZXJ0IFZhbG1kYXRpb24gTmV0d29y
azEXMBUGA1UEChMOVmFsaUNlcnQsIEluYy4xNTAzBgNVBAsTTFZhbG1DZXJ0IENs
YXNzIDIGUG9saWN5IFZhbG1kYXRpb24gQXV0aG9yaXR5MSEwHwYDVQQDEzhodHRw
-----END CERTIFICATE-----
```

Do you want to continue entering root and/or intermediate
certificates {y|n}: n

You should keep a copy of the private key and the CA-signed digital
certificate for future reference.

Gestione los certificados con System Manager

A partir de ONTAP 9.10.1, se puede utilizar System Manager para gestionar autoridades de certificados de confianza, certificados de cliente/servidor y autoridades de certificados locales (integradas).

Con System Manager, puede gestionar los certificados recibidos de otras aplicaciones para que pueda autenticar las comunicaciones de dichas aplicaciones. También puede administrar sus propios certificados que identifican su sistema a otras aplicaciones.

Ver información del certificado

Con System Manager, es posible ver las autoridades de certificados de confianza, los certificados de cliente/servidor y las autoridades de certificados locales almacenadas en el clúster.

Pasos

1. En System Manager, seleccione **Cluster > Settings**.
2. Desplácese hasta el área **Seguridad**.
En la sección **certificados**, se muestran los siguientes detalles:
 - El número de autoridades de certificados de confianza almacenadas.
 - El número de certificados de cliente/servidor almacenados.
 - El número de autoridades de certificados locales almacenadas.
3. Seleccione cualquier número para ver los detalles de una categoría de certificados o seleccione → Para abrir la página **Certificados**, que contiene información sobre todas las categorías.
La lista muestra la información del clúster completo. Si desea mostrar información solo de una máquina virtual de almacenamiento específica, realice los pasos siguientes:
 - a. Selecciona **Almacenamiento > Storage VMs**.
 - b. Seleccione la máquina virtual de almacenamiento.

- c. Cambie a la pestaña **Settings**.
- d. Seleccione un número que se muestra en la sección **Certificado**.

Qué hacer a continuación

- Desde la página **certificados**, puede [Genere una solicitud de firma de certificación](#).
- La información del certificado se divide en tres fichas, una para cada categoría. Es posible realizar las siguientes tareas desde cada pestaña:

En esta pestaña...	Puede ejecutar estos procedimientos...
Autoridades de certificados de confianza	<ul style="list-style-type: none"> • [install-trusted-cert] • Elimine una entidad de certificación de confianza • Renueve una entidad de certificación de confianza
Certificados cliente/servidor	<ul style="list-style-type: none"> • [install-cs-cert] • [gen-cs-cert] • [delete-cs-cert] • [renew-cs-cert]
Autoridades de certificados locales	<ul style="list-style-type: none"> • Cree una nueva entidad de certificación local • Firme un certificado mediante una entidad de certificación local • Elimine una entidad de certificación local • Renueve una autoridad de certificación local

Genere una solicitud de firma de certificación

Puede generar una solicitud de firma de certificación (CSR) con System Manager desde cualquier pestaña de la página **certificados**. Se genera una clave privada y una CSR correspondiente, que se pueden firmar mediante una autoridad de certificación para generar un certificado público.


Pasos

1. Abra la página **certificados**. Consulte [Ver información del certificado](#).
2. Seleccione **+Generar CSR**.
3. Complete la información del nombre del asunto:
 - a. Introduzca un **nombre común**.
 - b. Seleccione un **país**.
 - c. Introduzca una **organización**.
 - d. Introduzca una **unidad organizativa**.
4. Si desea anular los valores predeterminados, seleccione **más opciones** y proporcione información adicional.

Instale (añada) una entidad de certificación de confianza

Puede instalar autoridades de certificado de confianza adicionales en System Manager.

Pasos

1. Abra la pestaña **autoridades de certificados de confianza**. Consulte [Ver información del certificado](#).
2. Seleccione .
3. En el panel **Agregar autoridad de certificado de confianza**, realice lo siguiente:
 - Introduzca un **nombre**.
 - Para **Scope**, seleccione un equipo virtual de almacenamiento.
 - Introduzca un **nombre común**.
 - Seleccione un **tipo**.
 - Introduzca o importe **detalles del certificado**.


Elimine una entidad de certificación de confianza

Con System Manager, es posible eliminar una entidad de certificación de confianza.



No puede eliminar las autoridades de certificación de confianza preinstaladas con ONTAP.


Pasos

1. Abra la pestaña **autoridades de certificados de confianza**. Consulte [Ver información del certificado](#).
2. Seleccione el nombre de la entidad de certificación de confianza.
3. Seleccione  Junto al nombre, luego selecciona **Eliminar**.

Renueve una entidad de certificación de confianza

Con System Manager, puede renovar una entidad de certificación de confianza que ha caducado o está a punto de expirar.

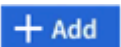
Pasos

1. Abra la pestaña **autoridades de certificados de confianza**. Consulte [Ver información del certificado](#).
2. Seleccione el nombre de la entidad de certificación de confianza.
3. Seleccione  Junto al nombre del certificado, luego **Renew**.

Instale (agregue) un certificado de cliente/servidor

Con System Manager, puede instalar certificados de cliente/servidor adicionales.

Pasos

1. Abra la ficha **certificados cliente/servidor**. Consulte [Ver información del certificado](#).
2. Seleccione .
3. En el panel **Agregar certificado de cliente/servidor**, realice lo siguiente:
 - Introduzca un **nombre de certificado**.
 - Para **Scope**, seleccione un equipo virtual de almacenamiento.
 - Introduzca un **nombre común**.
 - Seleccione un **tipo**.

- Introduzca o importe **detalles del certificado**.
Puede escribir o copiar y pegar los detalles del certificado desde un archivo de texto o puede importar el texto desde un archivo de certificado haciendo clic en **Importar**.
- Introduzca la **clave privada**.
Puede escribir o copiar y pegar en la clave privada desde un archivo de texto o puede importar el texto desde un archivo de claves privadas haciendo clic en **Importar**.

Genere (agregue) un certificado de cliente/servidor autofirmado

Con System Manager, puede generar otros certificados de cliente/servidor autofirmados.


Pasos

1. Abra la ficha **certificados cliente/servidor**. Consulte [Ver información del certificado](#).
2. Seleccione **+Generar certificado autofirmado**.
3. En el panel **generar certificado autofirmado**, realice lo siguiente:
 - Introduzca un **nombre de certificado**.
 - Para **Scope**, seleccione un equipo virtual de almacenamiento.
 - Introduzca un **nombre común**.
 - Seleccione un **tipo**.
 - Seleccione una función **hash**.
 - Seleccione un **tamaño de clave**.
 - Seleccione una **VM de almacenamiento**.

Eliminar un certificado de cliente/servidor

Con System Manager, puede eliminar certificados de cliente/servidor.


Pasos

1. Abra la ficha **certificados cliente/servidor**. Consulte [Ver información del certificado](#).
2. Seleccione el nombre del certificado de cliente/servidor.
3. Seleccione  Junto al nombre, haga clic en **Eliminar**.

Renueve un certificado de cliente/servidor

Con System Manager, puede renovar un certificado de cliente/servidor que ha caducado o está a punto de expirar.


Pasos

1. Abra la ficha **certificados cliente/servidor**. Consulte [Ver información del certificado](#).
2. Seleccione el nombre del certificado de cliente/servidor.
3. Seleccione  Junto al nombre, haga clic en **renovar**.

Cree una nueva entidad de certificación local

Con System Manager, es posible crear una nueva entidad de certificación local.

Pasos

1. Abra la ficha **autoridades de certificado local**. Consulte [Ver información del certificado](#).
2. Seleccione  **Add**.
3. En el panel **Agregar autoridad de certificación local**, realice lo siguiente:
 - Introduzca un **nombre**.
 - Para **Scope**, seleccione un equipo virtual de almacenamiento.
 - Introduzca un **nombre común**.
4. Si desea anular los valores predeterminados, seleccione **más opciones** y proporcione información adicional.

Firme un certificado mediante una entidad de certificación local

En System Manager, es posible usar una entidad de certificación local para firmar un certificado.


Pasos

1. Abra la ficha **autoridades de certificado local**. Consulte [Ver información del certificado](#).
2. Seleccione el nombre de la autoridad de certificación local.
3. Seleccione  Junto al nombre luego **Firma un certificado**.
4. Complete el formulario **firmar una solicitud de firma de certificado**.
 - Puede pegar el contenido de firma de certificados o importar un archivo de solicitud de firma de certificados haciendo clic en **Importar**.
 - Especifique el número de días para los que será válido el certificado.

Elimine una entidad de certificación local

Con System Manager, es posible eliminar una entidad de certificación local.


Pasos

1. Abra la ficha **Autoridad de certificado local**. Consulte [Ver información del certificado](#).
2. Seleccione el nombre de la autoridad de certificación local.
3. Seleccione  Junto al nombre luego **Eliminar**.

Renueve una autoridad de certificación local

Con System Manager, puede renovar una autoridad de certificado local que ha caducado o está a punto de expirar.

Pasos

1. Abra la ficha **Autoridad de certificado local**. Consulte [Ver información del certificado](#).
2. Seleccione el nombre de la autoridad de certificación local.
3. Seleccione  Junto al nombre, haga clic en **renovar**.

Configurar la información general de acceso al controlador de dominio de Active Directory

Para poder acceder a la SVM, es necesario configurar el acceso de la controladora de

dominio de AD al clúster o a la SVM. Si ya ha configurado un servidor SMB para una SVM de datos, puede configurar la SVM como puerta de enlace, o *tunnel*, para el acceso de AD al clúster. Si no configuró un servidor SMB, puede crear una cuenta de equipo para la SVM en el dominio de AD.

ONTAP admite los siguientes servicios de autenticación de controladores de dominio:

- Kerberos
- LDAP
- Netlogon
- Autoridad de seguridad local (LSA)


ONTAP admite los siguientes algoritmos de clave de sesión para conexiones seguras de Netlogon:

Algoritmo de clave de sesión	Disponible empezando por...
HMAC-SHA256, basado en el estándar de cifrado avanzado (AES) Si el clúster ejecuta ONTAP 9.9.1 o una versión anterior y el controlador de dominio aplica AES para los servicios seguros de Netlogon, la conexión falla. En este caso, debe reconfigurar el controlador de dominio para aceptar conexiones de clave fuerte con ONTAP.	ONTAP 9.10.1
DES y HMAC-MD5 (cuando se establece la clave fuerte)	Todas las versiones de ONTAP 9

Si desea utilizar claves de sesión AES durante la creación de canal seguro Netlogon, debe verificar que AES esté habilitado en su SVM.

- A partir de ONTAP 9.14.1, AES se habilita de forma predeterminada cuando crea una SVM y no necesita modificar la configuración de seguridad de su SVM para utilizar las claves de sesión AES durante la establecimiento de canal seguro Netlogon.
- En ONTAP 9.10.1 a 9.13.1, AES se deshabilita de forma predeterminada al crear una SVM. Debe habilitar AES mediante el siguiente comando:

```
cifs security modify -vserver vs1 -aes-enabled-for-netlogon-channel true
```



Cuando se actualice a ONTAP 9.14.1 o una versión posterior, la configuración de AES para las SVM existentes creadas con versiones de ONTAP anteriores no cambiará automáticamente. Aún debe actualizar el valor de esta configuración para habilitar AES en esas SVM.

Configure un túnel de autenticación

Si ya ha configurado un servidor SMB para una SVM de datos, puede usar el `security login domain-tunnel create` Comando para configurar la SVM como puerta de enlace, o *tunnel*, para obtener acceso AD al clúster.

Antes de empezar

- Debe haber configurado un servidor SMB para una SVM de datos.
- Debe haber habilitado una cuenta de usuario de dominio de AD para acceder a la SVM de administrador para el clúster.
- Para realizar esta tarea, debe ser un administrador de clústeres.

A partir de ONTAP 9.10.1, si tiene una puerta de enlace SVM (túnel de dominio) para acceso AD, puede usar Kerberos para autenticación de administrador si ha deshabilitado NTLM en el dominio de AD. En versiones anteriores, Kerberos no era compatible con la autenticación de administrador para puertas de enlace de SVM. Esta funcionalidad está disponible de forma predeterminada; no se requiere configuración.



La autenticación Kerberos siempre se intenta primero. En caso de error, se intenta la autenticación NTLM.

Paso

1. Configure una SVM de datos habilitada para SMB como túnel de autenticación para el acceso de la controladora de dominio AD al clúster:

```
security login domain-tunnel create -vserver svm_name
```

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



La SVM debe estar en ejecución para que el usuario se autentique.

El siguiente comando configura la SVM de datos habilitada para SMB como túnel de autenticación.

```
cluster1::>security login domain-tunnel create -vserver engData
```

Cree una cuenta de equipo SVM en el dominio

Si no ha configurado un servidor SMB para una SVM de datos, puede usar el `vserver active-directory create` Comando para crear una cuenta de equipo para la SVM en el dominio.

Acerca de esta tarea

Después de introducir el `vserver active-directory create` Se le pedirá que proporcione las credenciales de una cuenta de usuario de AD con privilegios suficientes para agregar equipos a la unidad organizativa especificada en el dominio. La contraseña de la cuenta no puede estar vacía.

Antes de empezar

Debe ser un administrador de clúster o de SVM para ejecutar esta tarea.

Paso

1. Cree una cuenta de equipo para una SVM en el dominio de AD:

```
vserver active-directory create -vserver SVM_name -account-name  
NetBIOS_account_name -domain domain -ou organizational_unit
```

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

El siguiente comando crea una cuenta de computadora llamada 'ADSERVER1' en el dominio 'example.com' para SVM 'engData'. Se le pedirá que introduzca las credenciales de cuenta de usuario de AD después de introducir el comando.

```
cluster1::>vserver active-directory create -vserver engData -account  
-name ADSERVER1 -domain example.com
```

In order to create an Active Directory machine account, you must supply the name and password of a Windows account with sufficient privileges to add computers to the "CN=Computers" container within the "example.com" domain.

Enter the user name: Administrator

Enter the password:

Configure la información general sobre el acceso a servidores LDAP o NIS

Debe configurar el acceso del servidor LDAP o NIS a una SVM para que las cuentas LDAP o NIS puedan acceder a la SVM. La función de conmutador le permite utilizar LDAP o NIS como fuentes alternativas de servicio de nombres.

Configure el acceso al servidor LDAP

Para que las cuentas LDAP puedan acceder a la SVM, debe configurar el acceso del servidor LDAP a una SVM. Puede utilizar el `vserver services name-service ldap client create` Comando para crear una configuración de cliente LDAP en la SVM. A continuación, puede utilizar la `vserver services name-service ldap create` Comando para asociar la configuración del cliente LDAP con la SVM.

Acerca de esta tarea

La mayoría de los servidores LDAP pueden utilizar los esquemas predeterminados proporcionados por ONTAP:

- MS-AD-BIS (el esquema preferido para la mayoría de los servidores AD de Windows 2012 y posteriores)
- AD-IDMU (Windows 2008, Windows 2016 y servidores AD posteriores)
- AD-SFU (servidores Windows 2003 y anteriores de AD)
- RFC-2307 (SERVIDORES UNIX LDAP)

Es mejor utilizar los esquemas predeterminados a menos que haya un requisito para hacer lo contrario. Si es así, puede crear su propio esquema copiando un esquema predeterminado y modificando la copia. Para obtener más información, consulte:

- ["Configuración de NFS"](#)
- ["Informe técnico de NetApp 4835: Cómo configurar LDAP en ONTAP"](#)

Antes de empezar

- Debe haber instalado un ["Certificado digital de servidor firmado por CA"](#) En la SVM.

- Debe ser un administrador de clúster o de SVM para ejecutar esta tarea.

Pasos

1. Cree una configuración de cliente LDAP en una SVM:

```
vserver services name-service ldap client create -vserver SVM_name -client
-config client_configuration -servers LDAP_server_IPs -schema schema -use
-start-tls true|false
```



Start TLS es compatible únicamente para acceder a las SVM de datos. No admite el acceso a las SVM de administración.

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

El siguiente comando crea una configuración de cliente LDAP llamada «corp» en SVM «engData». El cliente hace enlaces anónimos a los servidores LDAP con las direcciones IP 172.160.0.100 y 172.16.0.101. El cliente utiliza el esquema RFC-2307 para realizar consultas LDAP. La comunicación entre el cliente y el servidor se cifra mediante Start TLS.

```
cluster1::> vserver services name-service ldap client create
-vserver engData -client-config corp -servers 172.16.0.100,172.16.0.101
-schema RFC-2307 -use-start-tls true
```



A partir de ONTAP 9.2, el campo `-ldap-servers` reemplaza el campo `-servers`. Este nuevo campo puede tomar un nombre de host o una dirección IP para el servidor LDAP.

2. Asocie la configuración del cliente LDAP con la SVM: `vserver services name-service ldap create -vserver SVM_name -client-config client_configuration -client-enabled true|false`

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

El siguiente comando asocia la configuración del cliente LDAP corp Con la SVM engData, Y habilita el cliente LDAP en la SVM.

```
cluster1::>vserver services name-service ldap create -vserver engData
-client-config corp -client-enabled true
```



A partir de ONTAP 9.2, el `vserver services name-service ldap create` El comando realiza una validación automática de la configuración e informa de un mensaje de error si ONTAP no puede comunicarse con el servidor de nombres.

3. Validar el estado de los servidores de nombres mediante el comando `vserver Services NAME-service ldap check`.

El siguiente comando valida los servidores LDAP en la SVM vs0.

```
cluster1::> vserver services name-service ldap check -vserver vs0

| Vserver: vs0 |
| Client Configuration Name: c1 |
| LDAP Status: up |
| LDAP Status Details: Successfully connected to LDAP server |
| "10.11.12.13". |
```

El comando `name service check` está disponible a partir de ONTAP 9.2.

Configurar el acceso al servidor NIS

Debe configurar el acceso del servidor NIS a una SVM antes de que las cuentas NIS puedan acceder a la SVM. Puede utilizar el `vserver services name-service nis-domain create` Comando para crear una configuración de dominio NIS en una SVM.

Acerca de esta tarea

Puede crear varios dominios NIS. Sólo se puede establecer un dominio NIS en `active` a la vez.

Antes de empezar

- Todos los servidores configurados deben estar disponibles y accesibles antes de configurar el dominio NIS en la SVM.
- Debe ser un administrador de clúster o de SVM para ejecutar esta tarea.

Paso

1. Cree una configuración de dominio NIS en una SVM:

```
vserver services name-service nis-domain create -vserver SVM_name -domain
client_configuration -active true|false -nis-servers NIS_server_IPs
```

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



A partir de ONTAP 9.2, el campo `-nis-servers` reemplaza el campo `-servers`. Este nuevo campo puede tomar un nombre de host o una dirección IP para el servidor NIS.

El siguiente comando crea una configuración de dominio NIS en 'engData' de SVM. El dominio NIS `nisdomain` Está activo durante la creación y se comunica con un servidor NIS con la dirección IP `192.0.2.180`.

```
cluster1::>vserver services name-service nis-domain create
-vserver engData -domain nisdomain -active true -nis-servers 192.0.2.180
```

Crear un conmutador de servicio de nombres

La función de conmutador de servicio de nombres le permite utilizar LDAP o NIS como fuentes alternativas de servicio de nombres. Puede utilizar el `vserver services name-service ns-switch modify` para especificar el orden de búsqueda de fuentes de servicio de nombres.

Antes de empezar

- Debe haber configurado el acceso a los servidores LDAP y NIS.
- Debe ser un administrador de clúster o un administrador de SVM para ejecutar esta tarea.

Paso

1. Especifique el orden de búsqueda para los orígenes de servicios de nombres:

```
vserver services name-service ns-switch modify -vserver SVM_name -database name_service_switch_database -sources name_service_source_order
```

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

El siguiente comando especifica el orden de búsqueda de los orígenes de servicios de nombres LDAP y NIS para la base de datos «passwd» en SVM «engData».

```
cluster1::>vserver services name-service ns-switch  
modify -vserver engData -database passwd -source files ldap,nis
```

Cambiar una contraseña de administrador

Debe cambiar la contraseña inicial inmediatamente después de iniciar sesión en el sistema por primera vez. Si es un administrador de SVM, puede usar el `security login password` para cambiar su propia contraseña. Si es un administrador de clúster, puede utilizar el `security login password` para cambiar la contraseña de cualquier administrador.

Acerca de esta tarea

La nueva contraseña debe respetar las siguientes reglas:

- No puede contener el nombre de usuario
- Debe tener al menos 8 caracteres
- Debe contener al menos una letra y un número
- No puede ser igual que las últimas seis contraseñas



Puede utilizar el `security login role config modify` comando para modificar las reglas de contraseña de las cuentas de asociadas con un rol determinado. Para obtener más información, consulte ["referencia de comandos"](#).

Antes de empezar

- Debe ser un administrador de clústeres o SVM para cambiar su propia contraseña.
- Para cambiar la contraseña de otro administrador, debe ser un administrador de clústeres.

Paso

1. Cambiar una contraseña de administrador: `security login password -vserver svm_name -username user_name`

El siguiente comando cambia la contraseña del administrador `admin1` Para la SVM `vs1.example.com`. Se le pedirá que introduzca la contraseña actual, a continuación, introduzca y vuelva a introducir la nueva contraseña.

```
vs1.example.com::>security login password -vserver engData -username
admin1
Please enter your current password:
Please enter a new password:
Please enter it again:
```

Bloquear y desbloquear una cuenta de administrador

Puede utilizar el `security login lock` para bloquear una cuenta de administrador y la `security login unlock` comando para desbloquear la cuenta.

Antes de empezar

Para poder realizar estas tareas, debe ser un administrador de clústeres.

Pasos

1. Bloquear una cuenta de administrador:

```
security login lock -vserver SVM_name -username user_name
```

El siguiente comando bloquea la cuenta de administrador `admin1` Para la SVM `vs1.example.com`:

```
cluster1::>security login lock -vserver engData -username admin1
```

2. Desbloquear una cuenta de administrador:

```
security login unlock -vserver SVM_name -username user_name
```

El siguiente comando desbloquea la cuenta de administrador `admin1` Para la SVM `vs1.example.com`:

```
cluster1::>security login unlock -vserver engData -username admin1
```

Gestionar intentos fallidos de inicio de sesión

Los intentos repetidos de inicio de sesión fallidos a veces indican que un intruso está intentando acceder al sistema de almacenamiento. Puede tomar una serie de pasos para asegurarse de que no se produzca una intrusión.

Cómo sabrá que los intentos de inicio de sesión han fallado

El sistema de gestión de eventos (EMS) notifica los intentos de inicio de sesión con errores cada hora. Puede encontrar un registro de intentos fallidos de inicio de sesión en `audit.log` archivo.

Qué hacer si fallan los intentos repetidos de inicio de sesión

A corto plazo, puede tomar una serie de pasos para evitar una intrusión:

- Requerir que las contraseñas estén compuestas por un número mínimo de caracteres en mayúscula, caracteres en minúscula, caracteres especiales y/o dígitos
- Imponer un retraso tras un intento de inicio de sesión fallido
- Limite el número de intentos fallidos permitidos y bloquee los usuarios después del número especificado de intentos fallidos
- Caducar y bloquee cuentas que estén inactivas durante un número determinado de días

Puede utilizar el `security login role config modify` comando para ejecutar estas tareas.

A largo plazo, puede realizar estos pasos adicionales:

- Utilice la `security ssh modify` Comando para limitar el número de intentos de inicio de sesión con errores de todas las SVM recién creadas.
- Migre las cuentas de algoritmo MD5 existentes al algoritmo SHA-512 más seguro al requerir que los usuarios cambien sus contraseñas.

Aplicar SHA-2 en contraseñas de cuenta de administrador

Las cuentas de administrador creadas antes de ONTAP 9.0 siguen utilizando contraseñas MD5 después de la actualización, hasta que las contraseñas se modifican manualmente. MD5 es menos seguro que SHA-2. Por lo tanto, después de la actualización, debería pedir a los usuarios de cuentas MD5 que cambien sus contraseñas para utilizar la función hash SHA-512 predeterminada.

Acerca de esta tarea

La funcionalidad hash de contraseña le permite hacer lo siguiente:

- Muestra las cuentas de usuario que coinciden con la función hash especificada.
- Caducar cuentas que utilizan una función hash especificada (por ejemplo, MD5), obligando a los usuarios a cambiar sus contraseñas en su siguiente inicio de sesión.
- Bloquear cuentas cuyas contraseñas utilizan la función hash especificada.
- Al volver a una versión anterior a ONTAP 9, restablezca la contraseña propia del administrador del clúster para que sea compatible con la función hash (MD5) admitida por la versión anterior.

ONTAP solo acepta contraseñas SHA-2 predefinidas mediante el SDK de capacidad de gestión de NetApp (`security-login-create` y `security-login-modify-password`).

Pasos

1. Migrar las cuentas de administrador MD5 a la función hash de contraseña SHA-512:

- a. Caducar todas las cuentas de administrador de MD5: `security login expire-password -vserver * -username * -hash-function md5`

Al hacerlo, se obliga a los usuarios de cuentas MD5 a cambiar sus contraseñas al siguiente inicio de sesión.

- b. Pida a los usuarios de cuentas MD5 que inicien sesión a través de una consola o una sesión SSH.

El sistema detecta que las cuentas han caducado y solicita a los usuarios que cambien sus contraseñas. SHA-512 se utiliza de forma predeterminada para las contraseñas modificadas.

2. Para las cuentas MD5 cuyos usuarios no inician sesión para cambiar sus contraseñas en un período de tiempo, fuerce la migración de la cuenta:

- a. Cuentas de bloqueo que todavía utilizan la función hash MD5 (nivel de privilegio avanzado):

```
security login expire-password -vserver * -username * -hash-function md5  
-lock-after integer
```

Después del número de días especificado por `-lock-after`, Los usuarios no pueden acceder a sus cuentas MD5.

- b. Desbloquee las cuentas cuando los usuarios estén preparados para cambiar sus contraseñas:

```
security login unlock -vserver svm_name -username user_name
```


- c. Hacer que los usuarios inicien sesión en sus cuentas mediante una sesión SSH o de consola y cambien sus contraseñas cuando el sistema les solicite que lo hagan.

Diagnosticar y corregir problemas de acceso a archivos

Pasos

1. En System Manager, seleccione **almacenamiento > Storage VMs**.
2. Seleccione la máquina virtual de almacenamiento a la que desee realizar un seguimiento.
3. Haga clic en **Más**.
4. Haga clic en **acceso a archivos de rastreo**.
5. Proporcione el nombre de usuario y la dirección IP del cliente y, a continuación, haga clic en **Iniciar rastreo**.

Los resultados del seguimiento se muestran en una tabla. La columna **razones** proporciona la razón por la que no se pudo acceder a un archivo.

6. Haga clic en  en la columna izquierda de la tabla de resultados para ver los permisos de acceso a archivos.

Gestione la verificación de varias administradores

Información general de verificación de varios administradores

A partir de ONTAP 9.11.1, puede utilizar la verificación multiprotocolo (MAV) para garantizar que determinadas operaciones, como la eliminación de volúmenes o copias snapshot, solo se puedan ejecutar tras las aprobaciones de administradores designados. De este modo, se evita que administradores comprometidos, malintencionados o inexpertos realicen cambios no deseados o eliminen datos.

La configuración de la verificación multi-admin consta de:

- "Crear uno o varios grupos de aprobación de administrador."

- ["Habilitar la funcionalidad de verificación multi-administrador."](#)
- ["Adición o modificación de reglas."](#)

Tras la configuración inicial, estos elementos sólo los pueden modificar los administradores de un grupo de aprobación MAV (administradores MAV).

Cuando la verificación multi-administrador está habilitada, la finalización de cada operación protegida requiere tres pasos:

- Cuando un usuario inicia la operación, un ["se genera la solicitud."](#)
- Antes de que pueda ejecutarse, al menos uno ["El administrador de MAV debe aprobar."](#)
- Tras la aprobación, el usuario completa la operación.

La verificación de varios administradores no está pensada para utilizarse con volúmenes o flujos de trabajo que implican una fuerte automatización, ya que cada tarea automatizada requeriría la aprobación antes de poder completar la operación. Si desea utilizar la automatización y MAV conjuntamente, se recomienda utilizar consultas para operaciones MAV específicas. Por ejemplo, puede aplicar `volume delete` MAV sólo rige para volúmenes en los que la automatización no está involucrada, y puede designar dichos volúmenes con un esquema de nomenclatura en particular.



Si necesita deshabilitar la funcionalidad de verificación multi-admin sin la aprobación del administrador de MAV, póngase en contacto con el soporte de NetApp y mencione el siguiente artículo de la base de conocimientos: ["Cómo deshabilitar la verificación de administrador múltiple si el administrador de MAV no está disponible"](#).

Cómo funciona la verificación multi-administrador

La verificación multi-admin consta de:

- Grupo de uno o más administradores con facultades de aprobación y veto.
- Conjunto de operaciones o comandos protegidos en una *rules table*.
- Un *motor de reglas* para identificar y controlar la ejecución de operaciones protegidas.

Las reglas de MAV se evalúan después de las reglas de control de acceso basado en funciones (RBAC). Por lo tanto, los administradores que ejecutan o aprueban operaciones protegidas ya deben disponer de privilegios mínimos de RBAC para esas operaciones. ["Más información acerca de RBAC."](#)

Reglas definidas por el sistema

Cuando se activa la verificación de varios administradores, las reglas definidas por el sistema (también conocidas como reglas *Guard-Rail*) establecen un conjunto de operaciones MAV para contener el riesgo de eludir el propio proceso MAV. Estas operaciones no se pueden quitar de la tabla de reglas. Una vez activado MAV, las operaciones designadas por un asterisco (*) requieren la aprobación de uno o más administradores antes de la ejecución, excepto los comandos **show**.

- `security multi-admin-verify modify` operación*

Controla la configuración de la funcionalidad de verificación multi-administrador.

- `security multi-admin-verify approval-group` operaciones*

Controlar la pertenencia al conjunto de administradores con credenciales de verificación de varios

administradores.

- `security multi-admin-verify rule operaciones*`

Controle el conjunto de comandos que requieren verificación multiadministrador.

- `security multi-admin-verify request operaciones`

Controle el proceso de aprobación.

Comandos protegidos por reglas

Además de los comandos definidos por el sistema, los siguientes comandos están protegidos de forma predeterminada cuando se habilita la verificación multi-administrador, pero se pueden modificar las reglas para quitar la protección de estos comandos.

- `security login password`
- `security login unlock`
- `set`

Los siguientes comandos pueden protegerse en ONTAP 9.11.1 y versiones posteriores.

<code>cluster peer delete</code>	<code>volume snapshot autodelete modify</code>
<code>event config modify</code>	<code>volume snapshot delete</code>
<code>security login create</code>	<code>volume snapshot policy add-schedule</code>
<code>security login delete</code>	<code>volume snapshot policy create</code>
<code>security login modify</code>	<code>volume snapshot policy delete</code>
<code>system node run</code>	<code>volume snapshot policy modify</code>
<code>system node systemshell</code>	<code>volume snapshot policy modify-schedule</code>
<code>volume delete</code>	<code>volume snapshot policy remove-schedule</code>
<code>volume flexcache delete</code>	<code>volume snapshot restore</code>
	<code>vserver peer delete</code>

Los siguientes comandos se pueden proteger a partir de ONTAP 9.13.1:

- `volume snaplock modify`
- `security anti-ransomware volume attack clear-suspect`
- `security anti-ransomware volume disable`
- `security anti-ransomware volume pause`

Los siguientes comandos se pueden proteger a partir de ONTAP 9.14.1:

- `volume recovery-queue modify`
- `volume recovery-queue purge`
- `volume recovery-queue purge-all`
- `vserver modify`

Cómo funciona la aprobación multi-admin

Cada vez que se introduce una operación protegida en un cluster protegido MAV, se envía una solicitud de ejecución de operación al grupo de administradores de MAV designado.

Puede configurar:

- Los nombres, la información de contacto y el número de administradores del grupo MAV.

Un administrador de MAV debe tener una función RBAC con privilegios de administrador de clúster.

- El número de grupos de administradores de MAV.
 - Se asigna un grupo MAV para cada regla de operación protegida.
 - Para varios grupos MAV, puede configurar qué grupo MAV aprueba una regla determinada.
- El número de aprobaciones MAV necesarias para ejecutar una operación protegida.
- Período *de caducidad de aprobación* dentro del cual un administrador MAV debe responder a una solicitud de aprobación.
- Un período *expiration* de ejecución dentro del cual el administrador solicitante debe completar la operación.

Una vez configurados estos parámetros, se requiere la aprobación MAV para modificarlos.

Los administradores de MAV no pueden aprobar sus propias solicitudes para ejecutar operaciones protegidas. Por lo tanto:

- MAV no debe habilitarse en clústeres con un solo administrador.
- Si sólo hay una persona en el grupo MAV, ese administrador de MAV no puede introducir operaciones protegidas; los administradores regulares deben introducirlas y el administrador de MAV sólo puede aprobarlas.
- Si desea que los administradores de MAV puedan ejecutar operaciones protegidas, el número de administradores de MAV debe ser uno mayor que el número de aprobaciones necesarias. Por ejemplo, si se necesitan dos aprobaciones para una operación protegida y desea que los administradores de MAV las ejecuten, debe haber tres personas en el grupo de administradores de MAV.

Los administradores de MAV pueden recibir solicitudes de aprobación en alertas de correo electrónico (mediante EMS) o pueden consultar la cola de solicitudes. Cuando reciben una solicitud, pueden realizar una de estas tres acciones:

- Aprobar
- Rechazar (veto)
- Ignorar (sin acción)

Las notificaciones de correo electrónico se envían a todos los aprobadores asociados a una regla MAV cuando:

- Se crea una solicitud.
- Se ha aprobado o vetado una solicitud.
- Se ejecuta una solicitud aprobada.

Si el solicitante se encuentra en el mismo grupo de aprobación para la operación, recibirá un correo electrónico cuando se apruebe su solicitud.

Nota: Un solicitante no puede aprobar sus propias solicitudes, incluso si están en el grupo de aprobación. Pero pueden recibir las notificaciones por correo electrónico. Los solicitantes que no se encuentren en grupos de aprobación (es decir, que no sean administradores de MAV) no recibirán notificaciones por correo electrónico.

Cómo funciona la ejecución de operaciones protegidas

Si se aprueba la ejecución para una operación protegida, el usuario solicitante continúa con la operación cuando se le solicita. Si la operación es vetada, el usuario solicitante debe eliminar la solicitud antes de continuar.

Las reglas de MAV se evalúan después de los permisos de RBAC. Como resultado, un usuario sin suficientes permisos de RBAC para la ejecución de la operación no puede iniciar el proceso de solicitud de MAV.

Administrar grupos de aprobación de administradores

Antes de habilitar la verificación multi-admin (MAV), debe crear un grupo de aprobación de administrador que contenga a uno o más administradores a los que se les conceda la autorización de aprobación o de veto. Una vez que haya habilitado la verificación de varios administradores, cualquier modificación de la pertenencia al grupo de aprobación requiere la aprobación de uno de los administradores cualificados existentes.

Acerca de esta tarea

Puede agregar administradores existentes a un grupo MAV o crear nuevos administradores.

La funcionalidad MAV cumple la configuración de control de acceso basado en funciones (RBAC) existente. Los administradores potenciales de MAV deben tener privilegios suficientes para ejecutar operaciones protegidas antes de agregarlas a los grupos de administradores de MAV. ["Más información acerca de RBAC."](#)



Puede configurar MAV para avisar a los administradores de MAV de que las solicitudes de aprobación están pendientes. Para ello, debe configurar las notificaciones por correo electrónico, en concreto, el Mail From y.. Mail Server parámetros—o puede borrar estos parámetros para deshabilitar la notificación. Sin alertas de correo electrónico, los administradores de MAV deben comprobar manualmente la cola de aprobación.

Procedimiento de System Manager

Si desea crear un grupo de aprobación MAV por primera vez, consulte el procedimiento de System Manager a. ["habilite la verificación multi-admin."](#)



Para modificar un grupo de aprobación existente o crear un grupo de aprobación adicional:

1. Identifique a los administradores para que reciban una verificación de varios administradores.

- a. Haga clic en **clúster > Configuración**.
- b. Haga clic en  Junto a **usuarios y roles**.
- c. Haga clic en  **Add** En **usuarios**.
- d. Modifique la planilla según sea necesario.

Para obtener más información, consulte ["Control del acceso de administradores."](#)

2. Crear o modificar el grupo de aprobación MAV:

- a. Haga clic en **clúster > Configuración**.
- b. Haga clic en  Junto a **aprobación Multi-Admin** en la sección **Seguridad**.
(Verá la  Icono si MAV aún no está configurado.)
 - Nombre: Introduzca un nombre de grupo.
 - Autorizadores: Seleccione autorizadores de una lista de usuarios.
 - Dirección de correo electrónico: Introduzca las direcciones de correo electrónico.
 - Grupo predeterminado: Seleccione un grupo.

Se requiere aprobación MAV para editar una configuración existente una vez que MAV está activado.

Procedimiento de la CLI

1. Compruebe que se han establecido valores para Mail From y Mail Server parámetros. Introduzca:

```
event config show
```

La pantalla debe ser similar a la siguiente:

```
cluster01::> event config show
                        Mail From:  admin@localhost
                        Mail Server: localhost
                        Proxy URL:   -
                        Proxy User:  -
                        Publish/Subscribe Messaging Enabled: true
```

Para configurar estos parámetros, introduzca:

```
event config modify -mail-from email_address -mail-server server_name
```

2. Identifique a los administradores para que reciban una verificación de varios administradores

Si desea...	Introduzca este comando
Mostrar los administradores actuales	<code>security login show</code>
Modifique las credenciales de los administradores actuales	<code>security login modify <parameters></code>

Si desea...	Introduzca este comando
Crear nuevas cuentas de administrador	<code>security login create -user-or-group -name <i>admin_name</i> -application ssh -authentication-method password</code>

3. Cree el grupo de aprobación MAV:

```
security multi-admin-verify approval-group create [ -vserver svm_name] -name group_name -approvers approver1[,approver2...] [[-email address1], address1...]
```

- `-vserver` - Solo se admite la SVM de administrador en esta versión.
- `-name` - El nombre del grupo MAV, hasta 64 caracteres.
- `-approvers` - La lista de uno o más aprobadores.
- `-email` - Una o varias direcciones de correo electrónico que se notifican cuando se crea, aprueba, vetó o ejecuta una solicitud.

Ejemplo: el siguiente comando crea un grupo MAV con dos miembros y direcciones de correo electrónico asociadas.

```
cluster-1::> security multi-admin-verify approval-group create -name mav-grp1 -approvers pavan,julia -email pavan@myfirm.com,julia@myfirm.com
```

4. Verificar la creación y pertenencia a grupos:

```
security multi-admin-verify approval-group show
```

Ejemplo:

```
cluster-1::> security multi-admin-verify approval-group show
Vserver  Name           Approvers      Email
-----  -
svm-1    mav-grp1       pavan,julia    email
pavan@myfirm.com,julia@myfirm.com
```

Utilice estos comandos para modificar la configuración inicial del grupo MAV.

Nota: todos requieren la aprobación del administrador de MAV antes de la ejecución.

Si desea...	Introduzca este comando
Modifique las características del grupo o modifique la información de miembro existente	<code>security multi-admin-verify approval-group modify [<i>parameters</i>]</code>

Si desea...	Introduzca este comando
Agregar o quitar miembros	<code>security multi-admin-verify approval-group replace [-vserver svm_name] -name group_name [-approvers-to-add approver1[, approver2...]] [-approvers-to-remove approver1[, approver2...]]</code>
Eliminar un grupo	<code>security multi-admin-verify approval-group delete [-vserver svm_name] -name group_name</code>

Habilitar y deshabilitar la verificación de varios administradores

La verificación de varios administradores (MAV) se debe habilitar explícitamente. Una vez activada la verificación de varios administradores, se requiere la aprobación de un grupo de aprobación MAV (administradores MAV) para eliminarlo.

Acerca de esta tarea

Una vez que MAV está activado, la modificación o desactivación de MAV requiere la aprobación del administrador de MAV.



Si necesita deshabilitar la funcionalidad de verificación multi-admin sin la aprobación del administrador de MAV, póngase en contacto con el soporte de NetApp y mencione el siguiente artículo de la base de conocimientos: ["Cómo deshabilitar la verificación de administrador múltiple si el administrador de MAV no está disponible"](#).

Al activar MAV, puede especificar los siguientes parámetros globalmente.

Grupos de aprobación

Lista de grupos de aprobación globales. Se necesita al menos un grupo para activar la funcionalidad MAV.



Si utiliza MAV con protección autónoma contra ransomware (ARP), defina un grupo de aprobación nuevo o existente que sea responsable de aprobar la pausa de ARP, deshabilitar y borrar solicitudes sospechosas.

Autorizadores requeridos

Número de autorizadores necesarios para ejecutar una operación protegida. El número predeterminado y el número mínimo son 1.



El Núm. Necesario de aprobadores debe ser menor que el Núm. Total de aprobadores únicos en los grupos de aprobación por defecto.

Caducidad de la aprobación (horas, minutos, segundos)

El período dentro del cual un administrador MAV debe responder a una solicitud de aprobación. El valor predeterminado es una hora (1h), el valor mínimo soportado es un segundo (1s) y el valor máximo soportado es 14 días (14d).



Caducidad de la ejecución (horas, minutos, segundos)

El período dentro del cual el administrador solicitante debe completar la operación. El valor predeterminado es una hora (1h), el valor mínimo soportado es un segundo (1s) y el valor máximo soportado es 14 días (14d).

También puede anular cualquiera de estos parámetros para un parámetro específico "[reglas de funcionamiento](#)."



Procedimiento de System Manager

1. Identifique a los administradores para que reciban una verificación de varios administradores.

- a. Haga clic en **clúster > Configuración**.
- b. Haga clic en  Junto a **usuarios y roles**.
- c. Haga clic en  **Add** En **usuarios**.
- d. Modifique la planilla según sea necesario.

Para obtener más información, consulte "[Control del acceso de administradores](#)."

2. Active la verificación de varios administradores creando al menos un grupo de aprobación y agregando al menos una regla.


- a. Haga clic en **clúster > Configuración**.
- b. Haga clic en  Junto a **aprobación Multi-Admin** en la sección **Seguridad**.
- c. Haga clic en  **Add** para agregar al menos un grupo de aprobación.
 - Nombre: Introduzca un nombre de grupo.
 - Autorizadores: Seleccione autorizadores de una lista de usuarios.
 - Dirección de correo electrónico: Introduzca las direcciones de correo electrónico.
 - Grupo predeterminado: Seleccione un grupo.
- d. Agregue al menos una regla.
 - Operación: Seleccione un comando admitido de la lista.
 - Query: Introduzca los valores y las opciones de comandos que desee.
 - Parámetros opcionales; déjelo en blanco para aplicar la configuración global o asigne un valor diferente para reglas específicas para anular la configuración global.
 - Número requerido de aprobadores
 - Grupos de aprobación
- e. Haga clic en **Configuración avanzada** para ver o modificar los valores predeterminados.
 - Número requerido de autorizadores (valor predeterminado: 1)
 - Caducidad de la solicitud de ejecución (valor predeterminado: 1 hora)
 - Caducidad de la solicitud de aprobación (valor predeterminado: 1 hora)
 - Servidor de correo*
 - Desde la dirección de correo electrónico*

*Estos actualizan la configuración de correo electrónico administrada en "Notification Management". Se le pedirá que los configure si aún no se han configurado.


f. Haga clic en **Activar** para completar la configuración inicial de MAV.

Después de la configuración inicial, el estado actual de MAV se muestra en el mosaico **Multi-Admin Approval**.

- Estado (habilitado o no)
- Operaciones activas para las que se necesitan aprobaciones
- Número de solicitudes abiertas en estado pendiente

Puede mostrar una configuración existente haciendo clic en . Se requiere aprobación MAV para editar una configuración existente.

Para deshabilitar la verificación multi-admin:

1. Haga clic en **clúster > Configuración**.
2. Haga clic en  Junto a **aprobación Multi-Admin** en la sección **Seguridad**.
3. Haga clic en el botón de alternar habilitado.

Se requiere la aprobación MAV para completar esta operación.

Procedimiento de la CLI

Antes de activar la funcionalidad MAV en la CLI, al menos una "**Grupo de administradores MAV**" debe haber sido creado.

Si desea...	Introduzca este comando
Active la funcionalidad de MAV	<pre>security multi-admin-verify modify -approval-groups group1[,group2...] [- required-approvers nn] -enabled true [-execution-expiry [nnh][nmm][nns]] [-approval-expiry [nnh][nmm][nns]]</pre> <p>Ejemplo : el siguiente comando habilita MAV con 1 grupo de aprobación, 2 aprobadores requeridos y períodos de caducidad predeterminados.</p> <div><pre>cluster-1::> security multi-admin- verify modify -approval-groups mav-grp1 -required-approvers 2 -enabled true</pre></div> <p>Complete la configuración inicial agregando al menos una "regla de operación."</p>

Si desea...	Introduzca este comando
Modificar una configuración de MAV (requiere aprobación de MAV)	<pre>security multi-admin-verify approval-group modify [-approval-groups group1 [,group2...]] [-required-approvers nn] [-execution-expiry [nnh][nm][nns]] [-approval-expiry [nnh][nm][nns]]</pre>
Verifique la funcionalidad de MAV	<pre>security multi-admin-verify show</pre> <p>Ejemplo:</p> <pre>cluster-1::> security multi-admin-verify show Is Required Execution Approval Approval Enabled Approvers Expiry Expiry Groups ----- true 2 1h 1h mav-grp1</pre>
Desactivar la función MAV (requiere la aprobación MAV)	<pre>security multi-admin-verify modify -enabled false</pre>

Gestione reglas de operaciones protegidas

Se crean reglas de verificación de varios administradores (MAV) para designar operaciones que requieren aprobación. Siempre que se inicia una operación, las operaciones protegidas se interceptan y se genera una solicitud de aprobación.

Las reglas se pueden crear antes de habilitar MAV por cualquier administrador con las capacidades RBAC adecuadas, pero una vez que MAV está activado, cualquier modificación del conjunto de reglas requiere la aprobación de MAV.

Sólo se puede crear una regla MAV por operación; por ejemplo, no se pueden crear varias `volume-snapshot-delete` reglas. Cualquier restricción de regla deseada debe estar contenida dentro de una regla.

Comandos protegidos por reglas

Puede crear reglas para proteger los siguientes comandos que comienzan con ONTAP 9.11.1.

cluster peer delete	volume snapshot autodelete modify
event config modify	volume snapshot delete
security login create	volume snapshot policy add-schedule
security login delete	volume snapshot policy create
security login modify	volume snapshot policy delete
system node run	volume snapshot policy modify
system node systemshell	volume snapshot policy modify-schedule
volume delete	volume snapshot policy remove-schedule
volume flexcache delete	volume snapshot restore
	vserver peer delete

Puede crear reglas para proteger los siguientes comandos que comienzan con ONTAP 9.13.1:

- volume snaplock modify
- security anti-ransomware volume attack clear-suspect
- security anti-ransomware volume disable
- security anti-ransomware volume pause

Puede crear reglas para proteger los siguientes comandos que comienzan con ONTAP 9.14.1:

- volume recovery-queue modify
- volume recovery-queue purge
- volume recovery-queue purge-all
- vserver modify

Las reglas para los comandos MAV system-default, el security multi-admin-verify "comandos", no se puede modificar.

Además de los comandos definidos por el sistema, los siguientes comandos están protegidos de forma predeterminada cuando se habilita la verificación multi-administrador, pero se pueden modificar las reglas para quitar la protección de estos comandos.

- security login password
- security login unlock
- set

Restricciones de regla

Al crear una regla, puede especificar opcionalmente la `-query` opción para limitar la solicitud a un subconjunto de la funcionalidad del comando. La `-query` La opción también se puede usar para limitar elementos de configuración, como los nombres de la SVM, del volumen y de las snapshots.

Por ejemplo, en la `volume snapshot delete` comando, `-query` se puede establecer en `-snapshot !hourly*,!daily*,!weekly*`, Lo que significa que las instantáneas de volumen con el prefijo de atributos por hora, diario o semanal se excluyen de las protecciones MAV.

```
smci-vsrm20::> security multi-admin-verify rule show
```

		Required	Approval
Vserver	Operation	Approvers	Groups
vs01	volume snapshot delete	-	-
Query: -snapshot !hourly*,!daily*,!weekly*			



MAV no protegería ningún elemento de configuración excluido y cualquier administrador podría suprimirlos o cambiarles el nombre.

De forma predeterminada, las reglas especifican que corresponde `security multi-admin-verify request create "protected_operation"` el comando se genera automáticamente cuando se introduce una operación protegida. Puede modificar este valor predeterminado para requerir que el `request create` el comando se introduce por separado.

De forma predeterminada, las reglas heredan la siguiente configuración global de MAV, aunque se pueden especificar excepciones específicas de reglas:

- Número de aprobadores requerido
- Grupos de aprobación
- Período de caducidad de la aprobación
- Periodo de caducidad de ejecución

Procedimiento de System Manager

Si desea añadir una regla de operación protegida por primera vez, consulte el procedimiento de System Manager a. "[habilite la verificación multi-admin.](#)"

Para modificar el conjunto de reglas existente:

1. Seleccione **Cluster > Settings**.
2. Seleccione Junto a **aprobación Multi-Admin** en la sección **Seguridad**.
3. Seleccione **Add** para agregar al menos una regla, también puede modificar o eliminar reglas existentes.
 - Operación: Seleccione un comando admitido de la lista.
 - Query: Introduzca los valores y las opciones de comandos que desee.
 - Parámetros opcionales: Dejar en blanco para aplicar la configuración global o asignar un valor diferente para reglas específicas para anular la configuración global.

- Número requerido de aprobadores
- Grupos de aprobación

Procedimiento de la CLI



Todo `security multi-admin-verify rule` Los comandos requieren la aprobación del administrador de MAV antes de la ejecución excepto `security multi-admin-verify rule show`.

Si desea...	Introduzca este comando
Cree una regla	<code>security multi-admin-verify rule create -operation "protected_operation" [-query operation_subset] [parameters]</code>
Modifique las credenciales de los administradores actuales	<code>security login modify <parameters></code> Ejemplo: La siguiente regla requiere aprobación para eliminar el volumen raíz. <code>security multi-admin-verify rule create -operation "volume delete" -query "-vserver vs0"</code>
Modificar una regla	<code>security multi-admin-verify rule modify -operation "protected_operation" [parameters]</code>
Eliminar una regla	<code>security multi-admin-verify rule delete -operation "protected_operation"</code>
Muestra las reglas	<code>security multi-admin-verify rule show</code>

Para obtener detalles de sintaxis de comandos, consulte `security multi-admin-verify rule` páginas de manual.

Solicite la ejecución de operaciones protegidas

Cuando inicia una operación o comando protegido en un clúster habilitado para la verificación de varios administradores (MAV), ONTAP intercepta automáticamente la operación y solicita generar una solicitud, que debe ser aprobada por uno o más administradores de un grupo de aprobación de MAV (administradores de MAV). También puede crear una solicitud MAV sin el diálogo.

Si se aprueba, deberá responder a la consulta para completar la operación dentro del período de caducidad de la solicitud. Si se ha vetado o si se han superado los períodos de solicitud o caducidad, debe eliminar la solicitud y volver a enviarla.

La funcionalidad MAV cumple la configuración de RBAC existente. Es decir, la función de administrador debe tener privilegios suficientes para ejecutar una operación protegida sin tener en cuenta la configuración de MAV. "[Más información acerca de RBAC](#)".

Si es administrador de MAV, sus solicitudes de ejecución de operaciones protegidas también deben ser aprobadas por un administrador de MAV.

Procedimiento de System Manager

Cuando un usuario hace clic en un elemento de menú para iniciar una operación y la operación está protegida, se genera una solicitud de aprobación y el usuario recibe una notificación similar a la siguiente:

```
Approval request to delete the volume was sent.
Track the request ID 356 from Events & Jobs > Multi-Admin Requests.
```

La ventana **solicitudes de administrador múltiple** está disponible cuando MAV está activado, mostrando solicitudes pendientes basadas en el ID de inicio de sesión del usuario y la función MAV (aprobador o no). Para cada solicitud pendiente, se muestran los siguientes campos:

- Funcionamiento
- Índice (número)
- Estado (pendiente, aprobado, rechazado, ejecutado o caducado)

Si un aprobador rechaza una solicitud, no es posible realizar ninguna otra acción.

- Consulta (cualquier parámetro o valor para la operación solicitada)
- Usuario solicitante
- La solicitud caduca el
- (Número de) aprobadores pendientes
- (Número de) posibles aprobadores

Una vez aprobada la solicitud, el usuario solicitante puede volver a intentar la operación dentro del período de caducidad.

Si el usuario vuelve a intentar la operación sin aprobación, se muestra una notificación similar a la siguiente:

```
Request to perform delete operation is pending approval.
Retry the operation after request is approved.
```

Procedimiento de la CLI

1. Introduzca la operación protegida directamente o mediante el comando MAV Request.

Ejemplos: Para eliminar un volumen, introduzca uno de los siguientes comandos:

```
° volume delete
```



```
cluster-1::*> volume delete -volume voll -vserver vs0
```

```
Warning: This operation requires multi-admin verification. To create  
a
```

```
    verification request use "security multi-admin-verify  
request  
    create".
```

```
    Would you like to create a request for this operation?  
    {y|n}: y
```

```
Error: command failed: The security multi-admin-verify request (index  
3) is  
    auto-generated and requires approval.
```

```
° security multi-admin-verify request create "volume delete"
```

```
Error: command failed: The security multi-admin-verify request (index  
3)  
    requires approval.
```

2. Compruebe el estado de la solicitud y responda al aviso de MAV.

a. Si se aprueba la solicitud, responda al mensaje de la CLI para completar la operación.

Ejemplo:

```
cluster-1::> security multi-admin-verify request show 3
```

```
    Request Index: 3
      Operation: volume delete
        Query: -vserver vs0 -volume voll
        State: approved
Required Approvers: 1
Pending Approvers: 0
  Approval Expiry: 2/25/2022 14:32:03
  Execution Expiry: 2/25/2022 14:35:36
    Approvals: admin2
    User Vetoed: -
      Vserver: cluster-1
User Requested: admin
  Time Created: 2/25/2022 13:32:03
  Time Approved: 2/25/2022 13:35:36
    Comment: -
  Users Permitted: -
```

```
cluster-1::*> volume delete -volume voll -vserver vs0
```

Info: Volume "voll" in Vserver "vs0" will be marked as deleted and placed in the volume recovery queue. The space used by the volume will be recovered only after the retention period of 12 hours has completed. To recover the space immediately, get the volume name using (privilege:advanced) "volume recovery-queue show voll_*" and then "volume recovery-queue purge -vserver vs0 -volume <volume_name>" command. To recover the volume use the (privilege:advanced) "volume recovery-queue recover -vserver vs0 -volume <volume_name>" command.

Warning: Are you sure you want to delete volume "voll" in Vserver "vs0" ?
{y|n}: y

- b. Si se vetó la solicitud o el período de caducidad ha pasado, elimine la solicitud y vuelva a enviarla o póngase en contacto con el administrador de MAV.

Ejemplo:

```
cluster-1::> security multi-admin-verify request show 3
```

```
Request Index: 3
  Operation: volume delete
    Query: -vserver vs0 -volume voll1
    State: vetoed
Required Approvers: 1
Pending Approvers: 1
  Approval Expiry: 2/25/2022 14:38:47
  Execution Expiry: -
    Approvals: -
    User Vetoed: admin2
    Vserver: cluster-1
User Requested: admin
  Time Created: 2/25/2022 13:38:47
  Time Approved: -
    Comment: -
Users Permitted: -
```

```
cluster-1::*> volume delete -volume voll1 -vserver vs0
```

```
Error: command failed: The security multi-admin-verify request (index 3)
hasbeen vetoed. You must delete it and create a new verification
request.
To delete, run "security multi-admin-verify request delete 3".
```

Gestione solicitudes de operaciones protegidas

Cuando se notifica a los administradores de un grupo de aprobación MAV (administradores MAV) de una solicitud de ejecución de operación pendiente, deben responder con un mensaje de aprobación o de veto dentro de un período de tiempo fijo (caducidad de la aprobación). Si no se recibe un número suficiente de aprobaciones, el solicitante debe eliminar la solicitud y realizar otra.

Acerca de esta tarea

Las solicitudes de aprobación se identifican con números de índice, que se incluyen en los mensajes de correo electrónico y se muestran en la cola de solicitudes.

Se puede mostrar la siguiente información de la cola de solicitudes:

Funcionamiento

La operación protegida para la que se crea la solicitud.

Consulta

El objeto (u objetos) sobre el que el usuario desea aplicar la operación.

Estado

El estado actual de la solicitud; pendiente, aprobado, rechazado, caducado, ejecutado. Si un aprobador rechaza una solicitud, no es posible realizar ninguna otra acción.

Autorizadores requeridos

El número de administradores de MAV que se necesitan para aprobar la solicitud. Un usuario puede establecer el parámetro aprobadores requeridos para la regla de operación. Si un usuario no establece los aprobadores requeridos en la regla, se aplican los autorizadores requeridos de la configuración global.

Aprobadores pendientes

El número de administradores de MAV que todavía deben aprobar la solicitud para que se marque como aprobada.

Caducidad de la aprobación

El período dentro del cual un administrador MAV debe responder a una solicitud de aprobación. Cualquier usuario autorizado puede definir la fecha de caducidad de la aprobación de una regla de operación. Si no se ha establecido la fecha de caducidad de la regla, se aplicará la fecha de caducidad de la aprobación del valor global.

Caducidad de la ejecución

El período en el que el administrador solicitante debe completar la operación. Cualquier usuario autorizado puede establecer la caducidad de la ejecución de una regla de operación. Si no se ha definido la caducidad de la ejecución para la regla, se aplicará la caducidad de la ejecución desde el valor global.

Usuarios aprobados

Los administradores de MAV que han aprobado la solicitud.

El usuario ha vetado

Los administradores de MAV que han vetado la solicitud.

VM de almacenamiento (Vserver)

La SVM con la que se asocia la solicitud. Solo esta versión admite la SVM de administrador.

Usuario solicitado

Nombre de usuario del usuario que creó la solicitud.

Hora de creación

Hora a la que se crea la solicitud.

Tiempo aprobado

Hora a la que el estado de la solicitud cambió a aprobado.

Comentar

Cualquier comentario asociado a la solicitud.

Se permiten usuarios

Lista de usuarios autorizados para realizar la operación protegida para la que se aprueba la solicitud. Si `users-permitted` está vacío y, a continuación, cualquier usuario con los permisos adecuados puede realizar la operación.

Todas las solicitudes vencidas o ejecutadas se eliminan cuando se alcanza un límite de 1000 solicitudes o cuando el tiempo de vencimiento es superior a 8 horas para las solicitudes caducadas. Las solicitudes de

vetoed se eliminan una vez marcadas como caducadas.

Procedimiento de System Manager

Los administradores de MAV reciben mensajes de correo electrónico con detalles sobre la solicitud de aprobación, el período de caducidad de la solicitud y un vínculo para aprobar o rechazar la solicitud. Pueden acceder a un diálogo de aprobación haciendo clic en el enlace del correo electrónico o navegue hasta **Eventos y trabajos>solicitudes** en System Manager.

La ventana **Requests** está disponible cuando está habilitada la verificación de varios administradores, mostrando solicitudes pendientes basadas en el ID de inicio de sesión del usuario y la función MAV (aprobador o no).

- Funcionamiento
- Índice (número)
- Estado (pendiente, aprobado, rechazado, ejecutado o caducado)

Si un aprobador rechaza una solicitud, no es posible realizar ninguna otra acción.

- Consulta (cualquier parámetro o valor para la operación solicitada)
- Usuario solicitante
- La solicitud caduca el
- (Número de) aprobadores pendientes
- (Número de) posibles aprobadores

Los administradores de MAV tienen controles adicionales en esta ventana; pueden aprobar, rechazar o eliminar operaciones individuales o grupos de operaciones seleccionados. Sin embargo, si el administrador MAV es el usuario solicitante, no puede aprobar, rechazar o eliminar sus propias solicitudes.

Procedimiento de la CLI

1. Cuando se le notifique por correo electrónico acerca de las solicitudes pendientes, anote el número de índice y el período de caducidad de la aprobación de la solicitud. El número de índice también se puede mostrar utilizando las opciones **show** o **show-anPending** que se mencionan a continuación.
2. Aprobar o vetar la solicitud.

Si desea...	Introduzca este comando
Aprobar una solicitud	<code>security multi-admin-verify request approve nn</code>
Vetar una solicitud	<code>security multi-admin-verify request veto nn</code>
Mostrar todas las solicitudes, solicitudes pendientes o una sola solicitud	<code>`security multi-admin-verify request { show</code>

Si desea...	Introduzca este comando
show-pending } [nn] { -fields field1[,field2...]	[-instance] }` Puede mostrar todas las solicitudes de la cola o sólo las solicitudes pendientes. Si introduce el número de índice, solo se mostrará la información correspondiente. Puede mostrar información sobre campos específicos (mediante la -fields parámetro) o todos los campos (mediante el -instance parámetro).
Eliminar una solicitud	security multi-admin-verify request delete nn

Ejemplo:

La siguiente secuencia aprueba una solicitud después de que el administrador de MAV haya recibido el correo electrónico de solicitud con el número de índice 3, que ya tiene una aprobación.

```
cluster1::> security multi-admin-verify request show-pending
Pending
Index Operation      Query State  Approvers Requestor
-----
3 volume delete -    pending 1      julia

cluster-1::> security multi-admin-verify request approve 3

cluster-1::> security multi-admin-verify request show 3

Request Index: 3
Operation: volume delete
Query: -
State: approved
Required Approvers: 2
Pending Approvers: 0
Approval Expiry: 2/25/2022 14:32:03
Execution Expiry: 2/25/2022 14:35:36
Approvals: mav-admin2
User Vetoed: -
Vserver: cluster-1
User Requested: julia
Time Created: 2/25/2022 13:32:03
Time Approved: 2/25/2022 13:35:36
Comment: -
Users Permitted: -
```

Ejemplo:

En la siguiente secuencia se vetará una solicitud después de que el administrador MAV haya recibido el correo electrónico de solicitud con el número de índice 3, que ya tiene una aprobación.

```
cluster1::> security multi-admin-verify request show-pending
                                     Pending
Index Operation      Query State  Approvers Requestor
-----
3 volume delete -    pending 1      pavan

cluster-1::> security multi-admin-verify request veto 3

cluster-1::> security multi-admin-verify request show 3

Request Index: 3
Operation: volume delete
Query: -
State: vetoed
Required Approvers: 2
Pending Approvers: 0
Approval Expiry: 2/25/2022 14:32:03
Execution Expiry: 2/25/2022 14:35:36
Approvals: mav-admin1
User Vetoed: mav-admin2
Vserver: cluster-1
User Requested: pavan
Time Created: 2/25/2022 13:32:03
Time Approved: 2/25/2022 13:35:36
Comment: -
Users Permitted: -
```

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.