Autenticación y control de acceso

ONTAP 9

NetApp
February 12, 2026

Tabla de contenidos

Autenticación y control de acceso

Información general sobre el control de acceso y autenticación

La autenticación de clústeres ONTAP y el control de acceso a los servicios web de ONTAP se pueden gestionar.

Mediante System Manager o la CLI, puede controlar y proteger el acceso de cliente y administrador al clúster y al almacenamiento.

Si utiliza el administrador del sistema clásico (disponible solo en ONTAP 9,7 y versiones anteriores), consulte "System Manager Classic (ONTAP de 9.0 a 9.7)"

Autenticación y autorización de clientes

ONTAP autentica un equipo de cliente y un usuario al verificar sus identidades con un origen de confianza. ONTAP autoriza a un usuario a acceder a un archivo o directorio comparando las credenciales del usuario con los permisos configurados en el archivo o directorio.

Autenticación de administrador y RBAC

Los administradores utilizan cuentas de inicio de sesión locales o remotas para autenticarse en el clúster y en las máquinas virtuales de almacenamiento. El control de acceso basado en roles (RBAC) determina los comandos a los que tiene acceso un administrador.

Gestione la autenticación de administrador y RBAC

Obtenga información sobre la autenticación de administrador y el control de acceso basado en roles en ONTAP

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.

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"

  A partir de ONTAP 9.13.1, puede usar una clave pública SSH como método de autenticación principal o secundario para un usuario de 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.

- "LDAP o NIS"

  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.

Autenticación de administrador de ONTAP y flujo de trabajo de 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.

Complete la hoja de datos de configuración

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 la "hojas de trabajo de configuración".

Determine si la cuenta de administrador es local o remota

- **Si es local:** Activar "contraseña", , , "SSH" "MFA DE SSH"o "SSL" acceso.
- **Si es remoto:** Determina el tipo de acceso remoto. En función del tipo de acceso, "Active el acceso a Active Directory", "Active el acceso LDAP o NIS"o "Configurar autenticación SAML (solo para la SVM de administrador)".

Configure el acceso basado en roles

El rol asignado a un administrador determina los comandos a los que el administrador tiene acceso. El rol se asigna al crear la cuenta de administrador y puede ser "modificado" posterior. Puede usar roles predefinidos para "clúster"administradores y"SVM", o "defina roles personalizados" según sea necesario.

Gestionar cuentas de administrador

Dependiendo de cómo haya habilitado el acceso a la cuenta, es posible que necesite asociar una "clave pública con una cuenta local" , administrar "Claves públicas y certificados X,509" , configurar "Cisco Duo 2FA para inicios de sesión SSH" , instalar un "Certificado digital de servidor firmado por CA" , o configurar "Active Directory" , "LDAP o NIS" Acceso. Puede realizar cualquiera de estas tareas antes o después de habilitar el acceso a la cuenta.

5 **Configurar funciones de seguridad adicionales**

- "Gestione la verificación de varias administradores" si desea asegurarse de que ciertas operaciones requieren la aprobación de los administradores designados.
- "Gestionar la autorización dinámica" si desea aplicar dinámicamente comprobaciones de autorización adicionales basadas en el nivel de confianza de un usuario.
- "Configurar la elevación de privilegios justo a tiempo (JIT)" Si desea permitir que los usuarios accedan temporalmente a privilegios elevados para realizar determinadas tareas.

Hojas de trabajo para la autenticación de administrador de ONTAP 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.

Obtenga más información sobre los comandos descritos en este procedimiento en el "Referencia de comandos del ONTAP".

Crear o modificar cuentas de inicio de sesión

Estos valores se deben proporcionar con el `security login create` comando cuando se habilitan cuentas de inicio de sesión para acceder a una máquina virtual de almacenamiento. Obtenga más información sobre `security login create` en el "Referencia de comandos del ONTAP".

Con el `security login modify` comando se proporcionan los mismos valores cuando se modifica la forma en que una cuenta accede a una máquina virtual de almacenamiento. Obtenga más información sobre `security login modify` en el "Referencia de comandos del ONTAP".

Campo	Descripción	Su valor
`-vserver`	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.	
`-user-or-group-name`	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.	

`-application`	La aplicación que se utiliza para acceder a la VM de almacenamiento: • `http` • `ontapi` • `snmp` • `ssh`	
`-authmethod`	El método que se utiliza para autenticar la cuenta: • `cert` Para la autenticación de certificados SSL • `domain` Para la autenticación de Active Directory • `nsswitch` Para autenticación LDAP o NIS • `password` para la autenticación de contraseña de usuario • `publickey` para la autenticación de clave pública • `community` Para las cadenas de comunidad SNMP • `usm` Para el modelo de seguridad de usuario SNMP • `saml` Para la autenticación del lenguaje de marcado de aserción de seguridad (SAML)	
`-remote-switch-ipaddress`	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 solo se aplica cuando la aplicación es `snmp` y el método de autenticación es `usm`.	

`-role`	El rol de control de acceso que se asigna a la cuenta: • Para el clúster (la VM de almacenamiento del administrador), el valor predeterminado es `admin`. • Para una máquina virtual de almacenamiento de datos, el valor predeterminado es `vsadmin`.	
`-comment`	(Opcional) texto descriptivo para la cuenta. El texto debe escribirse entre comillas dobles (").	
`-is-ns-switch-group`	Si la cuenta es una cuenta de grupo LDAP o una cuenta de grupo NIS (`yes`o `no`).	
`-second-authentication -method`	Segundo método de autenticación en caso de autenticación multifactor: • `none` si no se utiliza la autenticación multifactor, el valor predeterminado • `publickey` para la autenticación de clave pública cuando `authmethod` es contraseña o nsswitch • `password` para la autenticación de contraseña de usuario cuando la `authmethod` es clave pública • `nsswitch` para la autenticación de contraseña de usuario cuando authmethod es publickey El orden de autenticación es siempre la clave pública seguida de la contraseña.	

`-is-ldap-fastbind`	A partir de ONTAP 9.11.1, cuando se establece en true, habilita el enlace rápido LDAP para la autenticación nsswitch; el valor predeterminado es false. Para utilizar el enlace rápido de LDAP, el `-authentication-method` valor se debe definir en `nsswitch`. "Utilice el enlace rápido LDAP para la autenticación nsswitch para SVM NFS de ONTAP".	

Configurar la información de seguridad de Cisco Duo

Se proporcionan estos valores con `security login duo create` el comando cuando se habilita la autenticación de dos factores Cisco Duo con inicios de sesión SSH para una máquina virtual de almacenamiento. Obtenga más información sobre `security login duo create` en el "Referencia de comandos del ONTAP".

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`	El nombre de host de la API, obtenido al registrar su aplicación SSH con Duo. Por ejemplo: `api-<HOSTNAME>.duosecurity.com`	

`-fail-mode`	En los errores de servicio o configuración que impiden la autenticación Duo, fallan `safe` (permitir acceso) o `secure` (denegar acceso). El valor por defecto es `safe`, lo que significa que la autenticación Duo se omite si falla debido a errores como el acceso al servidor API Duo.	
`-http-proxy`	Utilice el proxy HTTP especificado. Si el proxy HTTP requiere autenticación, incluya las credenciales en la URL del proxy. Por ejemplo: `http-proxy=http://username:password@proxy.example.org:8080`	

`-autopush`	`true`O `false`. El valor por defecto es `false`. `true`Si , Duo envía automáticamente una solicitud de inicio de sesión push al teléfono del usuario, volviendo a una llamada telefónica si no está disponible la inserción. Tenga en cuenta que esto desactiva efectivamente la autenticación de contraseña. `false`Si , se le solicita al usuario que elija un método de autenticación. Cuando se configura con `autopush = true`, se recomienda establecer `max-prompts = 1`.	

`-max-prompts`	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`. Por ejemplo, cuando `max-prompts = 1`, el usuario necesita autenticarse correctamente en la primera petición de datos, mientras que `max-prompts = 2` si , el usuario introduce información incorrecta en la petición de datos inicial, se le pedirá que vuelva a autenticarse. Cuando se configura con `autopush = true`, se recomienda establecer `max-prompts = 1`. Para la mejor experiencia, un usuario con solo autenticación publickey siempre tendrá `max-prompts` establecido en `1`.	
`-enabled`	Active la autenticación de dos factores Duo. Establecido en `true` 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 `false`), la autenticación Duo se ignora.	
`-pushinfo`	Esta opción proporciona información adicional en la notificación push, como el nombre de la aplicación o el servicio al que se accede. Esto ayuda a los usuarios a verificar que están iniciando sesión en el servicio correcto y proporciona una capa adicional de seguridad.	

Definir funciones personalizadas

Estos valores se proporcionan con el `security login role create` comando al definir un rol personalizado. Obtenga más información sobre `security login role create` en el "Referencia de comandos del ONTAP".

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 introducir `DEFAULT` para especificar todos los directorios de comandos.	

`-access`	(Opcional) el nivel de acceso del rol. Para directorios de comandos: • `none` (el valor predeterminado para los roles personalizados) deniega el acceso a los comandos del directorio de comandos • `readonly` otorga acceso a los `show` comandos en el directorio de comandos y sus subdirectorios • `all` otorga acceso a todos los comandos del directorio de comandos y sus subdirectorios Para comandos *nonintrinsic* (comandos que no terminan en `create`, , , `modify` `delete` o `show`): • `none` (el valor predeterminado para los roles personalizados) deniega el acceso al comando • `readonly` no es aplicable • `all` otorga acceso al comando Para conceder o denegar el acceso a comandos intrínsecos, debe especificar el directorio de comandos.	
`-query`	(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"` habilitaría el acceso `aggr0` sólo para el agregado.	

Asociar una clave pública a una cuenta de usuario

Proporciona estos valores con `security login publickey create` el comando al asociar una clave pública SSH a una cuenta de usuario. Obtenga más información sobre `security login publickey create` en el "Referencia de comandos del ONTAP".

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 por defecto `admin` , que es el nombre por defecto del administrador del cluster.	
`-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`	(Opcional) A partir de ONTAP 9.13.1, le permite gestionar la asociación de certificados X,509 con la clave pública SSH. 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: • `install`: Instale el certificado X,509 codificado PEM especificado y asócielo a la clave pública SSH. Incluya el texto completo del certificado que desea instalar. • `modify`: 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. • `delete`: Eliminar la asociación de certificados X,509 existente con la clave pública SSH.	

Configure los valores globales de autorización dinámica

A partir de ONTAP 9.15,1, proporcione estos valores con el `security dynamic-authorization modify` comando. Obtenga más información sobre `security dynamic-authorization modify` en el "Referencia de comandos del ONTAP".

Campo	Descripción	Su valor
`-vserver`	Nombre de la máquina virtual de almacenamiento para la que se debe modificar la configuración de puntuación de confianza. Si omite este parámetro, se usará la configuración de nivel del clúster.	

`-state`	El modo de autorización dinámica. Los posibles valores son los siguientes: • `disabled`: (Predeterminado) La autorización dinámica está desactivada. • `visibility`: Este modo es útil para probar la autorización dinámica. En este modo, la puntuación de confianza se comprueba con cada actividad restringida, pero no se aplica. Sin embargo, se registra cualquier actividad que hubiera sido denegada o sujeta a problemas de autenticación adicionales. • `enforced`: Destinado para su uso después de haber completado las pruebas con `visibility` MODE. En este modo, la puntuación de confianza se comprueba con cada actividad restringida y las restricciones de actividad se aplican si se cumplen las condiciones de restricción. El intervalo de supresión también se aplica, lo que evita problemas de autenticación adicionales dentro del intervalo especificado.	
`-suppression-interval`	Evita problemas de autenticación adicionales dentro del intervalo especificado. El intervalo está en formato ISO-8601 y acepta valores de 1 minuto a 1 hora inclusive. Si se establece en 0, el intervalo de supresión se desactiva y el usuario siempre se le solicita una comprobación de autenticación si es necesario.	

`-lower-challenge-boundary`	El límite inferior del porcentaje de desafío de autenticación multifactor (MFA). El rango válido es de 0 a 99. El valor 100 no es válido, ya que esto hace que se rechacen todas las solicitudes. El valor predeterminado es 0.	
`-upper-challenge-boundary`	Límite superior del porcentaje de comprobación de MFA. El rango válido es de 0 a 100. Debe ser igual o mayor que el valor del límite inferior. Un valor de 100 significa que cada solicitud será denegada o sujeta a un desafío de autenticación adicional; no hay solicitudes que se permitan sin un desafío. El valor predeterminado es 90.	

Instale un certificado digital de servidor firmado por CA

Proporciona estos valores con el `security certificate generate-csr` comando cuando se genera una solicitud de firma de certificación digital (CSR) para su uso en la autenticación de una máquina virtual de almacenamiento como un servidor SSL. Obtenga más información sobre `security certificate generate-csr` en el "Referencia de comandos del ONTAP".

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`. Para obtener una lista de códigos, consulte la "Referencia de comandos del ONTAP".	

`-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`.	

Proporciona estos valores con `security certificate install` el comando al instalar un certificado digital firmado por CA para usarlo 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. Obtenga más información sobre `security certificate install` en el "Referencia de comandos del ONTAP".

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

`-type`	El tipo de certificado: • `server` para certificados de servidor y certificados intermedios • `client-ca` Para el certificado de clave pública de la CA raíz del cliente SSL • `server-ca` Para el certificado de clave pública de la CA raíz del servidor SSL del que ONTAP es cliente • `client` 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

Estos valores se proporcionan con el `security login domain-tunnel create` comando cuando ya se configuró un servidor SMB para una máquina virtual de almacenamiento de datos y se desea configurar la máquina virtual de almacenamiento como una puerta de enlace o *túnel* para el acceso de la controladora de dominio de Active Directory al clúster. Obtenga más información sobre `security login domain-tunnel create` en el "Referencia de comandos del ONTAP".

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

Proporciona estos valores con `vserver active-directory create` el comando cuando no se configuró un servidor SMB y desea crear una cuenta de equipo virtual de almacenamiento en el dominio de Active Directory. Obtenga más información sobre `vserver active-directory create` en el "Referencia de comandos del ONTAP".

Campo	Descripción	Su valor
`-vserver`	Nombre de la máquina virtual de almacenamiento para la que desea crear una cuenta de equipo de Active Directory.	
`-account-name`	Nombre NetBIOS de la cuenta de equipo.	
`-domain`	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

Debe proporcionar estos valores con `vserver services name-service ldap client create` el comando al crear una configuración de cliente LDAP para la máquina virtual de almacenamiento. Obtenga más información sobre `vserver services name-service ldap client create` en el "Referencia de comandos del ONTAP".

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`	Si el cliente utiliza Start TLS para cifrar la comunicación con el servidor LDAP (`true`o `false`). 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.	

Proporciona estos valores con `vserver services name-service ldap create` el comando al asociar

una configuración de cliente LDAP a la máquina virtual de almacenamiento. Obtenga más información sobre `vserver services name-service ldap create` en el "Referencia de comandos del ONTAP".

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

Estos valores se proporcionan con `vserver services name-service nis-domain create` el comando al crear una configuración de dominio NIS en una máquina virtual de almacenamiento. Obtenga más información sobre `vserver services name-service nis-domain create` en el "Referencia de comandos del ONTAP".

Campo	Descripción	Su valor
`-vserver`	Nombre de la máquina virtual de almacenamiento en la que se creará la configuración del dominio.	
`-domain`	El nombre del dominio.	
`-nis-servers`	Lista separada por comas de direcciones IP y nombres de host para los servidores NIS que utiliza la configuración de dominio.	

Estos valores se proporcionan con el `vserver services name-service ns-switch create` comando cuando se especifica el orden de búsqueda para los orígenes del servicio de nombres. Obtenga más información sobre `vserver services name-service ns-switch create` en el "Referencia de comandos del ONTAP".

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

`-database`	La base de datos del servicio de nombres: • `hosts` Para archivos y servicios de nombres DNS • `group` Para archivos, LDAP y servicios de nombres NIS • `passwd` Para archivos, LDAP y servicios de nombres NIS • `netgroup` Para archivos, LDAP y servicios de nombres NIS • `namemap` Para los archivos y los servicios de nombres LDAP	
`-sources`	El orden en el que buscar fuentes de servicio de nombres (en una lista separada por comas): • `files` • `dns` • `ldap` • `nis`	

Configure el acceso SAML

A partir de ONTAP 9.3, es posible proporcionar estos valores con el `security saml-sp create` comando para configurar la autenticación SAML. Obtenga más información sobre `security saml-sp create` en el "Referencia de comandos del ONTAP".

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.	

`-cert-ca` y `-cert-serial`, o. `-cert-common-name`	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.	
`-verify-metadata-server`	Si la identidad del servidor de metadatos de IdP debe ser validada `true` o `false`). Lo mejor es establecer siempre este valor en `true`.	

Crear cuentas de inicio de sesión

Obtenga más información sobre la creación de cuentas de inicio de sesión de ONTAP

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 clústeres con `admin` el rol predeterminado 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.

```
`vsadmin`De forma predeterminada, a los administradores de SVM se les
asigna el rol. 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 `vsadmin` el rol a una cuenta de LDAP o NIS y se asigna `vsadmin-volume` el rol a la cuenta de grupo de AD para el mismo usuario, el usuario de AD inicia sesión con las `vsadmin` capacidades más inclusivas. Se dice que los roles son *fusionado*.

Habilite el acceso de cuenta local

Obtenga más información sobre cómo habilitar el acceso a la cuenta local de ONTAP

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 usar el `security login create` comando para habilitar las cuentas locales para que accedan a un administrador o a una SVM de datos.

Información relacionada

- "seguridad de inicio de sesión creado"

Active el acceso de contraseña de la cuenta de ONTAP

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

Acerca de esta tarea

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

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

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`*

   El siguiente comando habilita la cuenta de administrador de clúster `admin1` con `backup` el rol predefinido para acceder a la SVM de administrador`engCluster` con 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
   ```

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

Habilite el acceso de clave pública SSH para la cuenta de ONTAP

Puede utilizar el `security login create` comando para habilitar las cuentas de administrador para que accedan a una SVM de datos o administrador 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 del rol de control de acceso que desea asignar a la cuenta de inicio de sesión, puede utilizar `security login modify` el comando para añadir el rol más adelante.

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

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`*

   El siguiente comando habilita la cuenta de administrador de SVM `svmadmin1` con `vsadmin-volume` el rol predefinido para acceder a la SVM`engData1` mediante una clave pública de SSH:

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

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

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)

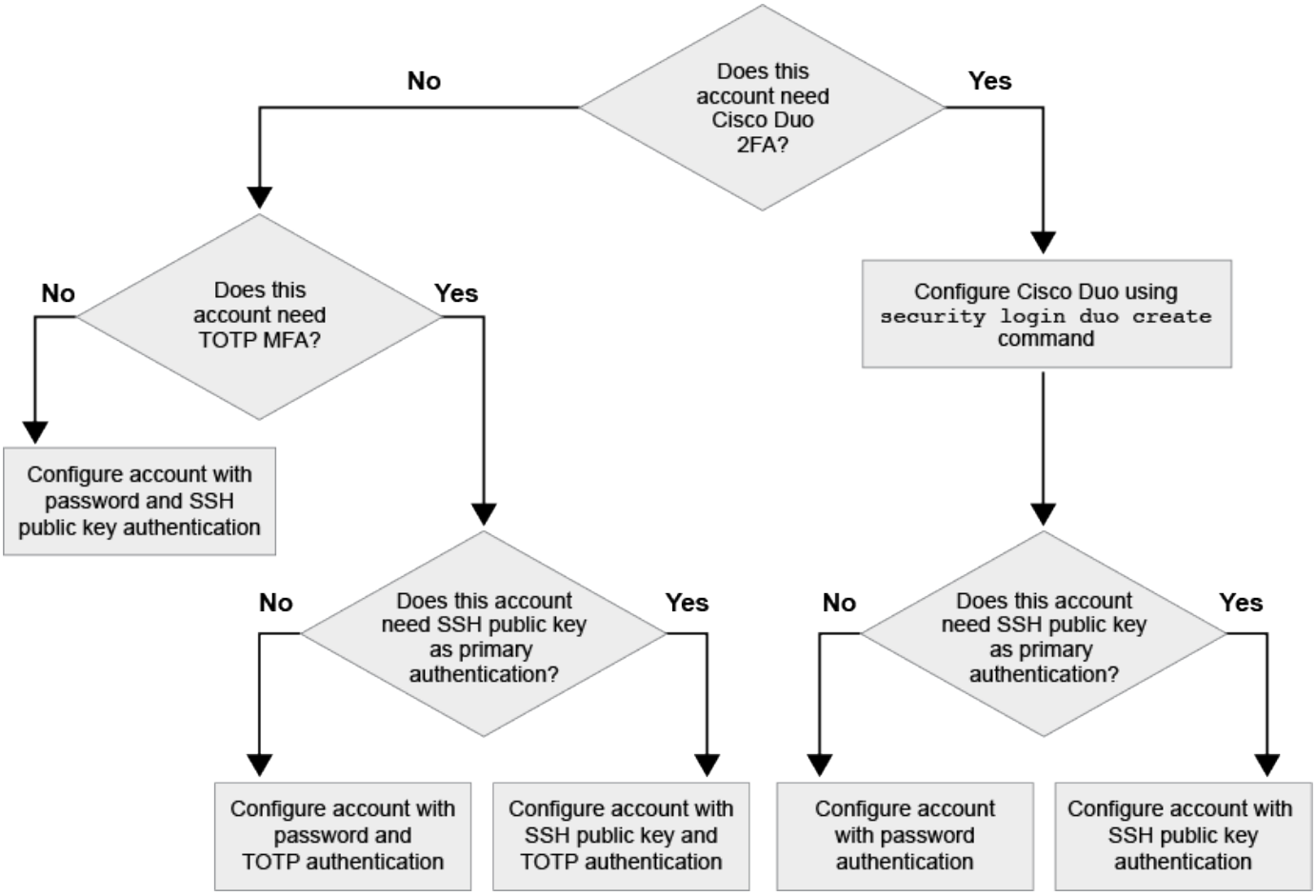
Obtenga más información sobre la autenticación multifactor de ONTAP

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 de ONTAP con SSH y TOTP

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 del rol de control de acceso que desea asignar a la cuenta de inicio de sesión, puede utilizar `security login modify` el comando para añadir el rol más adelante.

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

  "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 que la cuenta de administrador de SVM `admin2` con `admin` el rol predefinido inicie 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".
```

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

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). Una vez que la cuenta se habilita 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>
   ```

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

2. Compruebe que MFA con TOTP está activado:

```
security login show
```

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

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

- "Autenticación multifactor en ONTAP 9 (TR-4647)"
- "Referencia de comandos del ONTAP"

Configure cuentas de usuario locales de ONTAP 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.

  Microsoft Authenticator, Google Authenticator, Authy y cualquier otro autenticador compatible con TOTP son compatibles.

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>"
```

Información relacionada

- "inicio de sesión de seguridad totp create"
- "Inicio de sesión de seguridad totp show"

Restablezca la clave secreta TOTP para una cuenta de usuario de ONTAP

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, póngase en contacto con el administrador de almacenamiento para "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>
```

Información relacionada

- "inicio de sesión de seguridad totp create"
- "inicio de sesión de seguridad totp eliminar"
- "Inicio de sesión de seguridad totp show"

Deshabilite la clave secreta TOTP para una cuenta de usuario de ONTAP

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 modify -vserver <svm_name> -username
<account_username> -enabled false
```

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

Active el acceso a la cuenta de ONTAP del certificado SSL

Puede usar el `security login create` comando para habilitar las cuentas de administrador de para acceder a una SVM de datos o administrador 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 `security login modify` el comando.

  Modificar el rol asignado a un administrador

> Para las cuentas de administrador de clúster, se admite la autenticación de certificados con `http` `ontapi` `rest` las aplicaciones , y. En el caso de las cuentas de administrador de SVM, la autenticación de certificados solo es compatible con `ontapi` `rest` las aplicaciones y.

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`

   El siguiente comando habilita la cuenta de administrador de SVM `svmadmin2` con `vsadmin` el rol predeterminado para acceder a la SVM`engData2` con un certificado digital de SSL.

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

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

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

Obtenga más información sobre los comandos descritos en este procedimiento en el "Referencia de comandos del ONTAP".

Habilite el acceso a la cuenta de Active Directory ONTAP

Puede usar el `security login create` comando para habilitar cuentas de usuario o de grupo de Active Directory (AD) para acceder a un administrador o a una 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 "Utilice el enlace rápido LDAP para la autenticación nsswitch para SVM NFS de ONTAP" si es compatible con el servidor LDAP de AD.
- Si no está seguro del rol de control de acceso que desea asignar a la cuenta de inicio de sesión, puede utilizar `security login modify` el comando para añadir el rol más adelante.

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

  Modificar el rol asignado a un administrador

> El acceso a la cuenta de grupo de ANUNCIOS sólo se admite con `SSH` `ontapi` `rest` las aplicaciones , y. 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	`security login create -vserver <svm_name> -user-or-group-name <user_name> -application ssh -authentication-method publickey -role <role>`

Versión de ONTAP	Autenticación principal	Autenticación secundaria	Comando

9.13.1 y posterior	Dominio	Clave pública	**Para un nuevo usuario**
			`security login create -vserver <svm_name> -user-or-group-name <user_name> -application ssh -authentication-method domain -second -authentication-method publickey -role <role>`
			Para un usuario existente
			`security login modify -vserver <svm_name> -user-or-group-name <user_name> -application ssh -authentication-method domain -second -authentication-method publickey -role <role>`

9,0 y posterior	Dominio	Ninguno	`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]`

Para grupos AD:

Versión de ONTAP	Autenticación principal	Autenticación secundaria	Comando
9,0 y posterior	Dominio	Ninguno	`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]`

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

Información relacionada

- "seguridad de inicio de sesión creado"

Active el acceso a la cuenta de ONTAP LDAP o NIS

Puede usar el `security login create` comando para habilitar las cuentas de usuario LDAP o NIS para acceder a una SVM de datos o administrador. 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 del rol de control de acceso que desea asignar a la cuenta de inicio de sesión, puede utilizar `security login modify` el comando para añadir el rol más adelante.

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

  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 "Utilice el enlace rápido LDAP para la autenticación nsswitch para SVM NFS de ONTAP" si es compatible con el servidor LDAP.
- Debido a un problema conocido de LDAP, no debe utilizar el `':'` carácter (dos puntos) en ningún campo de información de cuenta de usuario de LDAP (por ejemplo, `gecos` `userPassword` ,, etc.). 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]
   ```

   "Crear o modificar cuentas de inicio de sesión"

El siguiente comando habilita la cuenta de administrador del clúster LDAP o NIS `guest2` con `backup` el rol predefinido para acceder a la SVM de administrador`engCluster` .

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

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

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 `publickey` como y 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

Información relacionada

- "inicio de sesión de seguridad"

Gestione los roles de control de acceso

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

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

Modificar el rol asignado a un administrador de ONTAP

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

Antes de empezar

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

Paso

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

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

   "Crear o modificar cuentas de inicio de sesión"

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

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

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

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

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

Defina roles personalizados para administradores de ONTAP

Puede usar el `security login role create` comando para definir un rol personalizado. Puede ejecutar el comando tantas veces como sea necesario para obtener la combinación exacta de funcionalidades que desea asociar al rol.

Acerca de esta tarea

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

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

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

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

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

Antes de empezar

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

Paso

1. Defina un rol personalizado:

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

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

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

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

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

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

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

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

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

Información relacionada

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

Roles predefinidos para administradores de clústeres de ONTAP

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

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

Este rol…	Tiene este nivel de acceso…	A los siguientes comandos o directorios de comandos
admin	todo	Todos los directorios de comandos (`DEFAULT`)
admin-no-fsa (disponible a partir de ONTAP 9.12.1)	Lectura/Escritura	• Todos los directorios de comandos (`DEFAULT`) • `security login rest-role` • `security login role`
Solo lectura	• `security login rest-role create` • `security login rest-role delete` • `security login rest-role modify` • `security login rest-role show` • `security login role create` • `security login role create` • `security login role delete` • `security login role modify` • `security login role show` • `volume activity-tracking` • `volume analytics`	Ninguno
`volume file show-disk-usage`	AutoSupport	todo
• `set` • `system node autosupport`	ninguno	Todos los demás directorios de comandos (`DEFAULT`)
backup	todo	`vserver services ndmp`

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

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

Información relacionada

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

Roles predefinidos para administradores de SVM de ONTAP

Los roles predefinidos para administradores de SVM deben cumplir con la mayoría de las necesidades. Puede crear roles personalizados según sea necesario. De forma

predeterminada, se asigna `vsadmin` el rol predefinido a un administrador de SVM.

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

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

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

Gestione el acceso del administrador de ONTAP con System Manager

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

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

- Asociar una clave pública a una cuenta local.
- Instale un certificado digital de servidor firmado por CA.
- Configure el acceso AD, LDAP o NIS.

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

Asignación de un rol a un administrador

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

Pasos

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

Cambiar el rol de un administrador

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

Pasos

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

Acceso a la elevación de privilegios JIT en ONTAP

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

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

Acerca de esta tarea

- La elevación de privilegios JIT solo está disponible para usuarios que acceden a ONTAP mediante SSH. Esta elevación de privilegios solo está disponible en la sesión SSH actual, pero se pueden elevar en tantas sesiones SSH simultáneas como sea necesario.
- La elevación de privilegios JIT solo es compatible con usuarios que usan contraseña, nsswitch o autenticación de dominio para iniciar sesión. La autenticación multifactor (MFA) no es compatible con la elevación de privilegios JIT.
- La sesión JIT de un usuario finalizará si la sesión configurada o el período de validez de JIT expira, o si un administrador del clúster revoca el acceso JIT para el usuario.

Antes de empezar

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

Pasos

1. Eleve temporalmente sus privilegios al rol configurado:

   ```
   security jit-privilege elevate
   ```

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

2. Ver el tiempo restante en su sesión JIT:

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

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

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

   ```
   security jit-privilege reset
   ```

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

Configurar la elevación de privilegios JIT en ONTAP

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

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

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

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

consulte Casos de uso comunes de JIT .

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

Acerca de esta tarea

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

Antes de empezar

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

Modificar la configuración global de JIT

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

Acerca de esta tarea

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

Pasos

1. Compruebe la configuración JIT actual:

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

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

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

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

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

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

Configurar el acceso de elevación de privilegios JIT para un usuario

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

Pasos

1. Comprobar el acceso JIT actual de un usuario:

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

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

2. Asignar nuevo acceso JIT para un usuario:

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

- Si `-vserver` no se especifica, el acceso JIT se asigna a nivel de clúster.
- `-role` es el rol RBAC al que se elevará el usuario. Si no se especifica, `-role` El valor predeterminado es `admin` .
- `-session-validity-period` Es el tiempo durante el cual el usuario puede acceder al rol elevado antes de tener que iniciar una nueva sesión JIT. Si no se especifica, el valor global o SVM `default-session-validity-period` se utiliza
- `-jit-validity-period` es la duración máxima durante la cual un usuario puede iniciar sesiones JIT después de la fecha de inicio configurada. Si no se especifica, `session-validity-period` Se utiliza. Este parámetro no puede exceder el valor global o SVM. `max-jit-validity-period` .
- `-start-time` Es la fecha y hora a partir de las cuales el usuario puede iniciar sesiones JIT. Si no se especifica, se utiliza la fecha y hora actuales.

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

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

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

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

Casos de uso comunes de JIT

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

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

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

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

Información relacionada

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

Administrar cuentas de administrador

Obtenga más información sobre la gestión de cuentas de administrador de ONTAP

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.

Asocie una clave pública con una cuenta de administrador de ONTAP

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 usar 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`*

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

2. Verifique el cambio visualizando la clave pública:

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

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

Ejemplo

El siguiente comando asocia una clave pública con la cuenta de administrador de SVM `svmadmin1` para la SVM `engData1`. A la clave pública se le asigna el número de índice 5.

```
cluster1::> security login publickey create -vserver engData1 -username
svmadmin1 -index 5 -publickey
"<key text>"
```

Gestione claves públicas SSH y certificados X,509 para administradores de ONTAP

Para una mayor seguridad de autenticación SSH con cuentas de administrador, puede usar el `security login publickey` conjunto de comandos para administrar la clave pública SSH y su asociación con los 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) con `security certificate install` comandos. Obtenga más información sobre `security certificate install` en el "Referencia de comandos del ONTAP".
  - Debe habilitar OCSP para SSH. Consulte "Verifique que los certificados digitales sean válidos mediante OCSP" para 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`

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

2. Verifique el cambio visualizando la clave pública:

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

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

Ejemplo

El siguiente comando asocia una clave pública y un certificado X,509 a la cuenta de administrador de SVM `svmadmin2` para la SVM `engData2`. A la clave pública se le asigna el número de índice 6.

```
cluster1::> security login publickey create -vserver engData2 -username
svmadmin2 -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`

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

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 `svmadmin2` para la SVM `engData2` en el número de índice 6.

```
cluster1::> security login publickey modify -vserver engData2 -username
svmadmin2 -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`*

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

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 `svmadmin3` para la SVM `engData3` en el número de índice 7.

```
cluster1::> security login publickey delete -vserver engData3 -username
svmadmin3 -index 7
```

Información relacionada

- "clave pública de inicio de sesión de seguridad"

Configurar Cisco Duo 2FA para inicios de sesión SSH de ONTAP

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 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 (conocido como Vserver en la CLI de ONTAP) mediante `security login duo create` el

comando. Cuando hace esto, Cisco Duo se habilita para inicios de sesión SSH para este clúster o máquina virtual de almacenamiento. Obtenga más información sobre `security login duo create` en el "Referencia de comandos del ONTAP".

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>
```

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 una máquina virtual de almacenamiento (conocida como Vserver en la CLI de ONTAP), puede utilizar `security login duo modify` el comando. Obtenga más información sobre `security login duo modify` en el "Referencia de comandos del ONTAP".

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 \
-max-prompts 1|2|3 \
-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 autentiquen mediante Duo al iniciar sesión. Para eliminar la configuración de Cisco Duo para una máquina virtual de almacenamiento (conocida como Vserver en la CLI de ONTAP), puede utilizar `security login duo delete` el comando. Obtenga más información sobre `security login duo delete` en el "Referencia de comandos del ONTAP".

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 la 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 una máquina virtual de almacenamiento (denominada Vserver en la CLI de ONTAP) mediante `security login duo show` el comando. Obtenga más información sobre `security login duo show` en el "Referencia de comandos del ONTAP".

Pasos

1. Inicie sesión en su cuenta de ONTAP con SSH.
2. Muestre la configuración de Cisco Duo para esta máquina virtual de almacenamiento. De manera opcional, se puede usar el `vserver` parámetro para especificar una máquina virtual de almacenamiento, sustituyendo el nombre de máquina virtual de almacenamiento por `<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 el `security login duo group create` comando. Al crear un grupo, opcionalmente puede excluir usuarios específicos de ese grupo del proceso de autenticación Duo. Obtenga más información sobre `security login duo group create` en el "Referencia de comandos del ONTAP".

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 el `-vserver` parámetro, el grupo se crea en el nivel de clúster:

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

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

Ver grupos Duo

Puede ver las entradas de grupo existentes de Cisco Duo mediante el `security login duo group show` comando. Obtenga más información sobre `security login duo group show` en el "Referencia de comandos del ONTAP".

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 el `-vserver` parámetro, el grupo se muestra a nivel de clúster:

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

El nombre del grupo Duo debe coincidir con un directorio activo, LDAP o grupo local. Los usuarios que especifique con el `-excluded-users` parámetro opcional no se mostrarán.

Eliminar un grupo Duo

Puede eliminar una entrada de grupo Duo con el `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. Obtenga más información sobre `security login duo group delete` en el "Referencia de comandos del ONTAP".

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` el 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 Cisco Duo para usuarios SSH, sustituyendo el nombre Vserver por `<STORAGE_VM_NAME>`:

```
security login duo modify -vserver <STORAGE_VM_NAME> -is-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 duo group modify -group-name <GROUP_NAME> -excluded-users
<USER1, USER2>
```

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

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

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 la "Documentación de Cisco Duo".

Genere e instale un certificado de servidor firmado por CA en ONTAP

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 `security certificate generate-csr` el comando para generar una solicitud de firma de certificación (CSR) y el `security certificate install` comando para instalar el certificado que recibe de la entidad de certificación. Obtenga más información sobre `security certificate generate-csr` y `security certificate install` en el "Referencia de comandos del ONTAP".

Genere una solicitud de firma de certificación

Es posible usar 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 una CSR con una clave privada de 2048 bits generada por la `SHA256` función hash para que la utilice el `Software` grupo en `IT` el departamento de una empresa cuyo nombre común personalizado es `server1.companyname.com`, ubicada en Sunnyvale, California, EE.UU. La dirección de correo electrónico del administrador del 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-----
<certificate_value>
-----END CERTIFICATE REQUEST-----


Private Key :
-----BEGIN RSA PRIVATE KEY-----
<key_value>
-----END RSA PRIVATE KEY-----

NOTE: 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 usar 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. Obtenga más información sobre `security certificate install` en el "Referencia de comandos del ONTAP".

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
```

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-----
<certificate_value>
-----END CERTIFICATE-----


Please enter Private Key: Press <Enter> when done
-----BEGIN RSA PRIVATE KEY-----
<key_value>
-----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-----
<certificate_value>
-----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-----
<certificate_value>
-----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.
```

Información relacionada

- "Generación de certificado de seguridad CSR"

Gestione certificados de ONTAP 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**, puedes 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	• [install-trusted-cert] • Elimine una entidad de certificación de confianza • Renueve una entidad de certificación de confianza
Certificados cliente/servidor	• [install-cs-cert] • [gen-cs-cert] • [delete-cs-cert] • [renew-cs-cert]

Autoridades de certificados locales	• 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 + Add .
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 y, a continuación, seleccione **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 y luego **Renovar**.

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 + Add .
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 y, a continuación, 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 y, a continuación, 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. Selecciona ⋮ junto al nombre y 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 y 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 y, a continuación, haga clic en **Renovar**.

Configure el acceso de la controladora de dominio de Active Directory en ONTAP

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 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 `security login domain-tunnel create` el comando para configurar la SVM como puerta de enlace, o *tunnel*, para el acceso de AD al clúster.

Antes de ONTAP 9.16.1, debe usar un túnel de autenticación para gestionar cuentas de administrador de clústeres con AD.

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.

Pasos

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>
```

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

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

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

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

Cree una cuenta de equipo SVM en el dominio

Si no configuró un servidor SMB para una SVM de datos, puede usar `vserver active-directory create` el 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` comando, se le pedirá que proporcione las credenciales de una cuenta de usuario de AD con suficiente Privileges para agregar equipos a la unidad organizativa especificada en el dominio. La contraseña de la cuenta no puede estar vacía.

A partir de ONTAP 9.16.1, puede usar este procedimiento para gestionar cuentas de administrador de clúster con AD.

Antes de empezar

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

Pasos

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>
```

A partir de ONTAP 9.16.1, `-vserver` el parámetro acepta la SVM admin. Obtenga más información sobre `vserver active-directory create` en el "Referencia de comandos del ONTAP".

El siguiente comando crea una cuenta de equipo denominada `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 el acceso al servidor LDAP o NIS en ONTAP

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.

Configurar el acceso al servidor LDAP

Debe configurar el acceso del servidor LDAP a una SVM antes de que las cuentas LDAP puedan acceder a la SVM. Puede usar el `vserver services name-service ldap client create` comando para crear una configuración de cliente LDAP en la SVM. Luego puede usar el `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 a "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.

Obtenga más información sobre `vserver services name-service ldap client create` en el "Referencia de comandos del ONTAP".

El siguiente comando crea una configuración de cliente LDAP llamada `corp` en la 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
```

> El `-ldap-servers` El campo reemplaza el `-servers` campo. Puedes utilizar el `-ldap -servers` campo para especificar 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>`

   Obtenga más información sobre `vserver services name-service ldap create` en el "Referencia de comandos del ONTAP".

   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
   ```

   > El `vserver services name-service ldap create` El comando realiza una validación de configuración automática e informa 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".                                                   |
```

Puedes utilizar el `name service check` Comando para validar el estado de los servidores de nombres.

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 usar el `vserver services name-service nis-domain create` comando para crear una configuración de dominio NIS en una SVM.

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> -nis-servers <NIS_server_IPs>
   ```

   Obtenga más información sobre `vserver services name-service nis-domain create` en el "Referencia de comandos del ONTAP".

   > El `-nis-servers` El campo reemplaza el `-servers` campo. Puedes utilizar el `-nis-servers` campo para especificar un nombre de host o una dirección IP para el servidor NIS.

   El siguiente comando crea una configuración de dominio NIS en la SVM `engData`. El dominio NIS `nisdomain` 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 -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 `vserver services name-service ns-switch modify` el comando para especificar el orden de búsqueda de los orígenes del 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>`

   Obtenga más información sobre `vserver services name-service ns-switch modify` en el "Referencia de comandos del ONTAP".

   El siguiente comando especifica el orden de consulta de los orígenes de servicio de nombres LDAP y NIS para la `passwd` base de datos en SVM `engData`.

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

Cambiar una contraseña de administrador de ONTAP

Debe cambiar la contraseña inicial inmediatamente después de iniciar sesión en el sistema por primera vez. Si es administrador de SVM, puede usar `security login password` el comando para cambiar su propia contraseña. Si es un administrador de clúster, puede usar `security login password` el comando 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 usar el `security login role config modify` comando para modificar las reglas de contraseñas de las cuentas asociadas a un rol determinado.

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:
```

Información relacionada

- "Modificar la configuración del rol de inicio de sesión de seguridad"
- "contraseña de inicio de sesión de seguridad"

Bloquear y desbloquear una cuenta de administrador de ONTAP

Puede utilizar el `security login lock` comando para bloquear una cuenta de administrador y el `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 de `admin1` la SVM`vs1.example.com`:

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

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

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
   ```

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

Información relacionada

- "inicio de sesión de seguridad"

Gestionar intentos fallidos de inicio de sesión en ONTAP

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 de inicio de sesión fallidos en el `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 usar el `security login role config modify` comando para ejecutar estas tareas. Obtenga más información sobre `security login role config modify` en el "Referencia de comandos del ONTAP".

A largo plazo, puede realizar estos pasos adicionales:

- Utilice `security ssh modify` el comando para limitar el número de intentos de inicio de sesión fallidos para todas las SVM recién creadas. Obtenga más información sobre `security ssh modify` en el "Referencia de comandos del ONTAP".
- Migre las cuentas de algoritmo MD5 existentes al algoritmo SHA-512 más seguro al requerir que los usuarios cambien sus contraseñas.

Aplique SHA-2 en las contraseñas de la cuenta de administrador de ONTAP

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 (`security-login-create` y `security-login-modify-password`) de capacidad de gestión de NetApp.

Pasos

1. Migrar las cuentas de administrador MD5 a la función hash de contraseña SHA-512:
   a. Caduque 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. Bloquear cuentas 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 Núm. De días especificado por `-lock-after`, los usuarios no pueden acceder a sus cuentas MD5.

   b. Desbloquee las cuentas cuando los usuarios estén listos 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.

Información relacionada

- "inicio de sesión de seguridad caducará la contraseña"
- "desbloqueo de inicio de sesión de seguridad"

Diagnostique y corrija problemas de acceso a archivos ONTAP con System Manager

A partir de ONTAP 9.8, puede rastrear y ver 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 Resultados para ver los permisos de acceso a archivos.

Gestione la verificación de varias administradores

Obtenga más información sobre la verificación multiadministrador de ONTAP

A partir de ONTAP 9.11.1, puede utilizar la verificación multiadministrador (MAV) para garantizar que determinadas operaciones, como la eliminación de volúmenes o snapshots, solo se puedan ejecutar después de las aprobaciones de los 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 multiadministrador está habilitada, completar todas las operaciones protegidas requiere los siguientes pasos:

1. Cuando un usuario inicia la operación, a. "se genera la solicitud."
2. Antes de que se pueda ejecutar la operación, al menos una "El administrador de MAV debe aprobar."
3. Tras la aprobación, se solicita al usuario y finaliza la operación.

> ⓘ Si necesita deshabilitar la funcionalidad de verificación de múltiples administradores sin la aprobación del administrador de MAV, comuníquese con el soporte de NetApp y mencione lo siguiente"Base de conocimientos de NetApp : Cómo deshabilitar la verificación de múltiples administradores si el administrador de MAV no está disponible" .

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 juntos, se recomienda que utilice consultas para operaciones de MAV específicas. Por ejemplo, puede aplicar `volume delete` reglas MAV solo a volúmenes en los que no esté implicada la automatización, y puede designar esos volúmenes con un esquema de nomenclatura particular.

> ⓘ La verificación multi-admin no está disponible con Cloud Volumes ONTAP.

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` funcionamiento `*`

  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 las operaciones definidas por el sistema, los siguientes comandos están protegidos de forma predeterminada cuando la verificación de múltiples administradores está habilitada, pero puede modificar las reglas para eliminar la protección de estos comandos:

- "contraseña de inicio de sesión de seguridad"
- "desbloqueo de inicio de sesión de seguridad"
- "listo"

Cada versión de ONTAP proporciona más comandos que puede elegir de protección con reglas de verificación multiadministrador. Elija la versión de ONTAP para obtener una lista completa de comandos disponibles para proteger.

9.17.1

- `cluster date modify` [3]
- `cluster log-forwarding create` [3]
- `cluster log-forwarding delete` [3]
- `cluster log-forwarding modify` [3]
- `cluster peer delete`
- `cluster time-service ntp server create` [3]
- `cluster time-service ntp server delete` [3]
- `cluster time-service ntp key create` [3]
- `cluster time-service ntp key delete` [3]
- `cluster time-service ntp key modify` [3]
- `cluster time-service ntp server modify` [3]
- `event config modify`
- `event config set-mail-server-password` [3]
- `lun delete` [3]
- `security anti-ransomware volume attack clear-suspect` [1]
- `security anti-ransomware volume disable` [1]
- `security anti-ransomware volume event-log modify` [2]
- `security anti-ransomware volume pause` [1]
- `security anti-ransomware vserver event-log modify` [2]
- `security audit modify` [3]
- `security ipsec config modify` [3]
- `security ipsec policy create` [3]
- `security ipsec policy delete` [3]
- `security ipsec policy modify` [3]
- `security login create`
- `security login delete`
- `security login modify`
- `security login publickey create`
- `security login publickey delete`
- `security login publickey modify`
- `security key-manager onboard update-passphrase` [3]
- `security saml-sp create` [3]

- security saml-sp delete [3]
- security saml-sp modify [3]
- security webauthn credentials delete [4]
- snaplock legal-hold end [3]
- storage aggregate delete [3]
- storage aggregate offline [4]
- storage encryption disk destroy [3]
- storage encryption disk modify [3]
- storage encryption disk revert-to-original-state [3]
- storage encryption disk sanitize [3]
- system bridge run-cli [3]
- system controller flash-cache secure-erase run [3]
- system controller service-event delete [3]
- system health alert delete [3]
- system health alert modify [3]
- system health policy definition modify [3]
- system node autosupport modify [3]
- system node autosupport trigger modify [3]
- system node coredump delete [3]
- system node coredump delete-all [3]
- system node hardware nvram-encryption modify [3]
- system node run
- system node systemshell
- system script delete [3]
- system service-processor ssh add-allowed-addresses [3]
- system service-processor ssh remove-allowed-addresses [3]
- system smtape restore [3]
- system switch ethernet log disable-collection [3]
- system switch ethernet log modify [3]
- timezone [3]
- volume create [3]
- volume delete
- volume encryption conversion start [4]
- volume encryption rekey start [4]

- volume file privileged-delete [3]
- volume flexcache delete
- volume modify [3]
- volume rename [5]
- volume recovery-queue modify [2]
- volume recovery-queue purge [2]
- volume recovery-queue purge-all [2]
- volume snaplock modify [1]
- volume snapshot autodelete modify
- volume snapshot create [3]
- volume snapshot delete
- volume snapshot modify [3]
- volume snapshot policy add-schedule
- volume snapshot policy create
- volume snapshot policy delete
- volume snapshot policy modify
- volume snapshot policy modify-schedule
- volume snapshot policy remove-schedule
- volume snapshot rename [3]
- volume snapshot restore
- vserver audit create [3]
- vserver audit delete [3]
- vserver audit disable [3]
- vserver audit modify [3]
- vserver audit rotate-log [3]
- vserver create [2]
- vserver consistency-group create [4]
- vserver consistency-group delete [4]
- vserver consistency-group modify [4]
- vserver consistency-group snapshot create [4]
- vserver consistency-group snapshot delete [4]
- vserver delete [3]
- vserver modify [2]
- vserver object-store-server audit create [3]

- vserver object-store-server audit delete [3]
- vserver object-store-server audit disable [3]
- vserver object-store-server audit modify [3]
- vserver object-store-server audit rotate-log [3]
- vserver object-store-server bucket cors-rule create [4]
- vserver object-store-server bucket cors-rule delete [4]
- vserver options [3]
- vserver peer delete
- vserver security file-directory apply [3]
- vserver security file-directory remove-slag [3]
- vserver stop [4]
- vserver vscan disable [3]
- vserver vscan on-access-policy create [3]
- vserver vscan on-access-policy delete [3]
- vserver vscan on-access-policy disable [3]
- vserver vscan on-access-policy modify [3]
- vserver vscan scanner-pool create [3]
- vserver vscan scanner-pool delete [3]
- vserver vscan scanner-pool modify [3]

9.16.1

- cluster date modify [3]
- cluster log-forwarding create [3]
- cluster log-forwarding delete [3]
- cluster log-forwarding modify [3]
- cluster peer delete
- cluster time-service ntp server create [3]
- cluster time-service ntp server delete [3]
- cluster time-service ntp key create [3]
- cluster time-service ntp key delete [3]
- cluster time-service ntp key modify [3]
- cluster time-service ntp server modify [3]
- event config modify
- event config set-mail-server-password [3]

- lun delete [3]
- security anti-ransomware volume attack clear-suspect [1]
- security anti-ransomware volume disable [1]
- security anti-ransomware volume event-log modify [2]
- security anti-ransomware volume pause [1]
- security anti-ransomware vserver event-log modify [2]
- security audit modify [3]
- security ipsec config modify [3]
- security ipsec policy create [3]
- security ipsec policy delete [3]
- security ipsec policy modify [3]
- security login create
- security login delete
- security login modify
- security login publickey create
- security login publickey delete
- security login publickey modify
- security key-manager onboard update-passphrase [3]
- security saml-sp create [3]
- security saml-sp delete [3]
- security saml-sp modify [3]
- security webauthn credentials delete [4]
- snaplock legal-hold end [3]
- storage aggregate delete [3]
- storage aggregate offline [4]
- storage encryption disk destroy [3]
- storage encryption disk modify [3]
- storage encryption disk revert-to-original-state [3]
- storage encryption disk sanitize [3]
- system bridge run-cli [3]
- system controller flash-cache secure-erase run [3]
- system controller service-event delete [3]
- system health alert delete [3]
- system health alert modify [3]

- system health policy definition modify [3]
- system node autosupport modify [3]
- system node autosupport trigger modify [3]
- system node coredump delete [3]
- system node coredump delete-all [3]
- system node hardware nvram-encryption modify [3]
- system node run
- system node systemshell
- system script delete [3]
- system service-processor ssh add-allowed-addresses [3]
- system service-processor ssh remove-allowed-addresses [3]
- system smtape restore [3]
- system switch ethernet log disable-collection [3]
- system switch ethernet log modify [3]
- timezone [3]
- volume create [3]
- volume delete
- volume encryption conversion start [4]
- volume encryption rekey start [4]
- volume file privileged-delete [3]
- volume flexcache delete
- volume modify [3]
- volume recovery-queue modify [2]
- volume recovery-queue purge [2]
- volume recovery-queue purge-all [2]
- volume snaplock modify [1]
- volume snapshot autodelete modify
- volume snapshot create [3]
- volume snapshot delete
- volume snapshot modify [3]
- volume snapshot policy add-schedule
- volume snapshot policy create
- volume snapshot policy delete
- volume snapshot policy modify

- volume snapshot policy modify-schedule
- volume snapshot policy remove-schedule
- volume snapshot rename [3]
- volume snapshot restore
- vserver audit create [3]
- vserver audit delete [3]
- vserver audit disable [3]
- vserver audit modify [3]
- vserver audit rotate-log [3]
- vserver create [2]
- vserver consistency-group create [4]
- vserver consistency-group delete [4]
- vserver consistency-group modify [4]
- vserver consistency-group snapshot create [4]
- vserver consistency-group snapshot delete [4]
- vserver delete [3]
- vserver modify [2]
- vserver object-store-server audit create [3]
- vserver object-store-server audit delete [3]
- vserver object-store-server audit disable [3]
- vserver object-store-server audit modify [3]
- vserver object-store-server audit rotate-log [3]
- vserver object-store-server bucket cors-rule create [4]
- vserver object-store-server bucket cors-rule delete [4]
- vserver options [3]
- vserver peer delete
- vserver security file-directory apply [3]
- vserver security file-directory remove-slag [3]
- vserver stop [4]
- vserver vscan disable [3]
- vserver vscan on-access-policy create [3]
- vserver vscan on-access-policy delete [3]
- vserver vscan on-access-policy disable [3]
- vserver vscan on-access-policy modify [3]

- vserver vscan scanner-pool create [3]
- vserver vscan scanner-pool delete [3]
- vserver vscan scanner-pool modify [3]

9.15.1

- cluster date modify [3]
- cluster log-forwarding create [3]
- cluster log-forwarding delete [3]
- cluster log-forwarding modify [3]
- cluster peer delete
- cluster time-service ntp server create [3]
- cluster time-service ntp server delete [3]
- cluster time-service ntp key create [3]
- cluster time-service ntp key delete [3]
- cluster time-service ntp key modify [3]
- cluster time-service ntp server modify [3]
- event config modify
- event config set-mail-server-password [3]
- lun delete [3]
- security anti-ransomware volume attack clear-suspect [1]
- security anti-ransomware volume disable [1]
- security anti-ransomware volume event-log modify [2]
- security anti-ransomware volume pause [1]
- security anti-ransomware vserver event-log modify [2]
- security audit modify [3]
- security ipsec config modify [3]
- security ipsec policy create [3]
- security ipsec policy delete [3]
- security ipsec policy modify [3]
- security login create
- security login delete
- security login modify
- security login publickey create
- security login publickey delete

- security login publickey modify
- security key-manager onboard update-passphrase [3]
- security saml-sp create [3]
- security saml-sp delete [3]
- security saml-sp modify [3]
- snaplock legal-hold end [3]
- storage aggregate delete [3]
- storage encryption disk destroy [3]
- storage encryption disk modify [3]
- storage encryption disk revert-to-original-state [3]
- storage encryption disk sanitize [3]
- system bridge run-cli [3]
- system controller flash-cache secure-erase run [3]
- system controller service-event delete [3]
- system health alert delete [3]
- system health alert modify [3]
- system health policy definition modify [3]
- system node autosupport modify [3]
- system node autosupport trigger modify [3]
- system node coredump delete [3]
- system node coredump delete-all [3]
- system node hardware nvram-encryption modify [3]
- system node run
- system node systemshell
- system script delete [3]
- system service-processor ssh add-allowed-addresses [3]
- system service-processor ssh remove-allowed-addresses [3]
- system smtape restore [3]
- system switch ethernet log disable-collection [3]
- system switch ethernet log modify [3]
- timezone [3]
- volume create [3]
- volume delete
- volume file privileged-delete [3]

- volume flexcache delete
- volume modify [3]
- volume recovery-queue modify [2]
- volume recovery-queue purge [2]
- volume recovery-queue purge-all [2]
- volume snaplock modify [1]
- volume snapshot autodelete modify
- volume snapshot create [3]
- volume snapshot delete
- volume snapshot modify [3]
- volume snapshot policy add-schedule
- volume snapshot policy create
- volume snapshot policy delete
- volume snapshot policy modify
- volume snapshot policy modify-schedule
- volume snapshot policy remove-schedule
- volume snapshot rename [3]
- volume snapshot restore
- vserver audit create [3]
- vserver audit delete [3]
- vserver audit disable [3]
- vserver audit modify [3]
- vserver audit rotate-log [3]
- vserver create [2]
- vserver delete [3]
- vserver modify [2]
- vserver object-store-server audit create [3]
- vserver object-store-server audit delete [3]
- vserver object-store-server audit disable [3]
- vserver object-store-server audit modify [3]
- vserver object-store-server audit rotate-log [3]
- vserver options [3]
- vserver peer delete
- vserver security file-directory apply [3]

- vserver security file-directory remove-slag [3]
- vserver vscan disable [3]
- vserver vscan on-access-policy create [3]
- vserver vscan on-access-policy delete [3]
- vserver vscan on-access-policy disable [3]
- vserver vscan on-access-policy modify [3]
- vserver vscan scanner-pool create [3]
- vserver vscan scanner-pool delete [3]
- vserver vscan scanner-pool modify [3]

9.14.1

- cluster peer delete
- event config modify
- security anti-ransomware volume attack clear-suspect [1]
- security anti-ransomware volume disable [1]
- security anti-ransomware volume event-log modify [2]
- security anti-ransomware volume pause [1]
- security anti-ransomware vserver event-log modify [2]
- security login create
- security login delete
- security login modify
- security login publickey create
- security login publickey delete
- security login publickey modify
- system node run
- system node systemshell
- volume delete
- volume flexcache delete
- volume recovery-queue modify [2]
- volume recovery-queue purge [2]
- volume recovery-queue purge-all [2]
- volume snaplock modify [1]
- volume snapshot autodelete modify
- volume snapshot delete

- volume snapshot policy add-schedule
- volume snapshot policy create
- volume snapshot policy delete *
- volume snapshot policy modify
- volume snapshot policy modify-schedule
- volume snapshot policy remove-schedule
- volume snapshot restore
- vserver create [2]
- vserver modify [2]
- vserver peer delete

9.13.1

- cluster peer delete
- event config modify
- security anti-ransomware volume attack clear-suspect [1]
- security anti-ransomware volume disable [1]
- security anti-ransomware volume pause [1]
- security login create
- security login delete
- security login modify
- security login publickey create
- security login publickey delete
- security login publickey modify
- system node run
- system node systemshell
- volume delete
- volume flexcache delete
- volume snaplock modify [1]
- volume snapshot autodelete modify
- volume snapshot delete
- volume snapshot policy add-schedule
- volume snapshot policy create
- volume snapshot policy delete *
- volume snapshot policy modify

- volume snapshot policy modify-schedule
- volume snapshot policy remove-schedule
- volume snapshot restore
- vserver peer delete

9.12.1 PB/9.11.1

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

1. Nuevo comando protegido por reglas para 9.13.1
2. Nuevo comando protegido por reglas para 9.14.1
3. Nuevo comando protegido por reglas para 9.15.1
4. Nuevo comando protegido por reglas para 9.16.1
5. Nuevo comando protegido por reglas para 9.17.1

*Este comando solo está disponible con CLI y no está disponible para System Manager en algunas versiones.

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 iniciar operaciones protegidas; los administradores normales deben iniciar operaciones protegidas y el administrador de MAV solo puede aprobar.
- 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.

Un solicitante no puede aprobar sus propias solicitudes incluso si están en el grupo de aprobación (aunque puede recibir notificaciones por correo electrónico para sus propias solicitudes). 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.

Las reglas MAV se evalúan antes de ejecutar la operación protegida. Esto significa que las reglas se aplican según el estado actual del sistema. Por ejemplo, si se crea una regla MAV para `volume modify` con una consulta de `-size 5GB` , usando `volume modify` Para cambiar el tamaño de un volumen de 5 GB a 2 GB se requerirá la aprobación de MAV, pero para cambiar el tamaño de un volumen de 2 GB a 5 GB no.

Información relacionada

- "clúster"
- "lun"
- "seguridad"
- "extremo de sujeción legal con cierre a presión"
- "agregado de almacenamiento"
- "cifrado del almacenamiento"
- "sistema"

Gestionar grupos de aprobación de administrador de ONTAP para MAV

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 posibles administradores 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 particular los `Mail From` `Mail Server` parámetros y, o bien puede borrar estos parámetros para desactivar la notificación. Sin alertas de correo electrónico, los administradores de MAV deben comprobar manualmente la cola de aprobación.

A partir de ONTAP 9.15.1, puede configurar los usuarios de Active Directory (AD) como administradores de MAV. El usuario de AD debe ser"configurado como administrador de ONTAP" .

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 **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 → junto a **Aprobación multiadministrador** en la sección **Seguridad**. (Verá ⚙ el 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 definido valores para los `Mail From` `Mail Server` parámetros y. 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
   ```

   Obtenga más información sobre `event config show` y `event config modify` en el "Referencia de comandos del ONTAP".

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

Si desea…	Introduzca este comando
Mostrar los administradores actuales	`security login show`
Modifique las credenciales de los administradores actuales	`security login modify <parameters>`
Crear nuevas cuentas de administrador	`security login create -user-or-group -name admin_name -application ssh -authentication-method password`

Obtenga más información acerca de `security login show`, `security login modify` y `security login create` en el "Referencia de comandos del ONTAP".

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 el admin SVM es compatible en esta versión.
- `-name` - El nombre del grupo MAV, hasta 64 caracteres.
- `-approvers`- La lista de uno o más aprobadores. Para los usuarios de AD, utilice el formato `domain\user` . Por ejemplo, `mydomain\pavan` .
- `-email` - Una o más direcciones de correo electrónico que son notificadas cuando una solicitud es creada, aprobada, vetada o ejecutada.

  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	`security multi-admin-verify approval-group modify [parameters]`
Agregar o quitar miembros	`security multi-admin-verify approval-group replace [-vserver svm_name] -name group_name [-approvers-to-add approver1[,approver2…]][-approvers-to-remove approver1[,approver2…]]`
Eliminar un grupo	`security multi-admin-verify approval-group delete [-vserver svm_name] -name group_name`

Información relacionada

- "verificación de seguridad multiadministrador"

Habilitar o deshabilitar la verificación multiadministrador en ONTAP

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 de múltiples administradores sin la aprobación del administrador de MAV, comuníquese con el soporte de NetApp y mencione lo siguiente"Base de conocimientos de NetApp : Cómo deshabilitar la verificación de múltiples administradores 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 sustituir cualquiera de estos parámetros para especificarlos "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 **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 ⚙ junto a **Aprobación multiadministrador** en la sección **Seguridad**.
   c. Haga + Add clic 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 visualizar 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 ⚙ junto a **Aprobación multiadministrador** 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, "Grupo de administradores MAV"se debe haber creado al menos una.

Si desea…	Introduzca este comando

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

Modificar una configuración de MAV (requiere aprobación de MAV)	`security multi-admin-verify approval-group modify [-approval-groups group1 [,group2…]] [-required-approvers nn ] [ -execution-expiry [nnh][nnm][nns]] [ -approval-expiry [nnh][nnm][nns]]`

Verifique la funcionalidad de MAV	`security multi-admin-verify show`
	
	Ejemplo:
	
	`cluster-1::> security multi-admin-verify show`
	`Is Required Execution`
	`Approval Approval`
	`Enabled Approvers Expiry Expiry`
	`Groups`
	`------- --------- ---------`
	`-------- ----------`
	`true 2 1h 1h`
	`mav-grp1`

Desactivar la función MAV (requiere la aprobación MAV)	`security multi-admin-verify modify -enabled false`

Información relacionada

- "verificación de seguridad multiadministrador"

Gestione reglas de verificación multiadministradoras para las operaciones protegidas en ONTAP

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.

Puede crear reglas para proteger "estos comandos". Puede proteger cada comando comenzando por la versión de ONTAP, en la que se encuentra disponible la funcionalidad de protección para el comando primero.

Las reglas para los comandos MAV por defecto del sistema `security multi-admin-verify` "comandos", , no se pueden modificar.

Además de las operaciones definidas por el sistema, los siguientes comandos están protegidos de forma predeterminada cuando la verificación de múltiples administradores está habilitada, pero puede modificar las reglas para eliminar la protección de estos comandos:

- "contraseña de inicio de sesión de seguridad"
- "desbloqueo de inicio de sesión de seguridad"
- "listo"

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. `-query`La opción también puede usarse para limitar elementos de configuración, como los nombres de la SVM, de los volúmenes y de snapshots.

Por ejemplo, en el `volume snapshot delete` comando, `-query` se puede definir en `-snapshot !hourly*,!daily*,!weekly*`, lo que significa que las instantáneas de volumen con el prefijo de atributos por hora, por día o por semana se excluyen de las protecciones MAV.

```
smci-vsim20::> 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 el `security multi-admin-verify request create "protected_operation"` comando correspondiente se genera automáticamente cuando se introduce una operación protegida. Puede modificar este valor predeterminado para requerir que `request create` el comando se introduzca 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 agregar 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 multiadministrador** en la sección **Seguridad**.
3. Seleccione esta opción + Add para agregar al menos una regla; también puede modificar o suprimir las 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

ⓘ Todos `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	`security multi-admin-verify rule create -operation "protected_operation" [-query operation_subset] [parameters]`

Si desea…	Introduzca este comando

Modifique las credenciales de los administradores actuales	`security login modify <parameters>`
	
	Ejemplo: La siguiente regla requiere aprobación para eliminar el volumen raíz.
	
	`security multi-admin-verify rule create -operation "volume delete" -query "-vserver vs0"`

Modificar una regla	`security multi-admin-verify rule modify -operation "protected_operation" [parameters]`
Eliminar una regla	`security multi-admin-verify rule delete -operation "protected_operation"`
Muestra las reglas	`security multi-admin-verify rule show`

Información relacionada

- "regla de verificación de seguridad multiadministrador"
- "modificación del inicio de sesión de seguridad"

Solicitar la ejecución de operaciones protegidas por MAV en ONTAP

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 vol1 -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 vol1
             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 vol1 -vserver vs0

Info: Volume "vol1" 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 vol1_*" 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 "vol1" 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 vol1
             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 vol1 -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".
```

Información relacionada

- "verificación de seguridad multiadministrador"

Gestionar solicitudes de operación protegidas por MAV en ONTAP

Cuando a los administradores de un grupo de aprobación MAV (administradores MAV) se les notifica sobre una solicitud de ejecución de operación pendiente, deben responder con un mensaje de aprobación o veto dentro de un tiempo fijo (vencimiento de la aprobación). Si no se recibe un número suficiente de aprobaciones, el solicitante deberá 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.

> `multi-admin-verify`Las solicitudes en un estado terminal pueden sobrescribirse o eliminarse automáticamente. Utilice el"registro de auditoría" para revisar solicitudes anteriores.

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, cualquier usuario con los permisos adecuados puede realizar la operación.

System Manager

Los administradores de MAV reciben mensajes de correo electrónico con detalles de la solicitud de aprobación, el período de vencimiento de la solicitud y un enlace para aprobar o rechazar la solicitud. Pueden acceder a un cuadro de diálogo de aprobación haciendo clic en el enlace del correo electrónico o navegando a **Eventos y trabajos > Solicitudes** en el Administrador del sistema.

La ventana **Solicitudes** está disponible cuando la verificación de múltiples administradores está habilitada y muestra las solicitudes pendientes según el ID de inicio de sesión del usuario y el rol 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.

CLI

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

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

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 el `-fields` parámetro) o sobre 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 relacionada

- "verificación de seguridad multiadministrador"

Gestionar la autorización dinámica

Obtenga información sobre la autorización dinámica de ONTAP

A partir de ONTAP 9.15.1, los administradores pueden configurar y habilitar la autorización dinámica para aumentar la seguridad del acceso remoto a ONTAP al tiempo que se mitigan los daños potenciales que podría causar un agente malintencionado. Con ONTAP 9.15.1, la autorización dinámica proporciona un marco inicial para asignar una puntuación de seguridad a los usuarios y, si su actividad parece sospechosa, desafiarlos con comprobaciones de autorización adicionales o denegar una operación por completo.

Los administradores pueden crear reglas, asignar puntuaciones de confianza y restringir comandos para determinar cuándo se permite o se deniega cierta actividad para un usuario. Los administradores pueden activar la autorización dinámica en todo el clúster o para máquinas virtuales de almacenamiento individuales.

Cómo funciona la autorización dinámica

La autorización dinámica utiliza un sistema de puntuación de confianza para asignar a los usuarios un nivel de confianza diferente en función de las políticas de autorización. Según el nivel de confianza del usuario, se puede permitir o denegar una actividad que realice, o se puede solicitar al usuario que realice una autenticación adicional.

Consulte "Personalizar la autorización dinámica"para obtener más información sobre cómo configurar ponderaciones de puntuación de criterios y otros atributos de autorización dinámica.

Dispositivos de confianza

Cuando se utiliza la autorización dinámica, la definición de un dispositivo de confianza es un dispositivo utilizado por un usuario para iniciar sesión en ONTAP mediante la autenticación de clave pública como uno de los métodos de autenticación. El dispositivo es de confianza porque solo ese usuario posee la clave privada correspondiente.

Ejemplo de autorización dinámica

Tome el ejemplo de tres usuarios diferentes que intentan eliminar un volumen. Cuando intentan realizar la operación, se examina la clasificación de riesgo de cada usuario:

- El primer usuario inicia sesión desde un dispositivo de confianza con muy pocos fallos de autenticación anteriores, lo que hace que su calificación de riesgo sea baja; la operación se permite sin autenticación adicional.
- El segundo usuario inicia sesión desde un dispositivo de confianza con un porcentaje moderado de fallos de autenticación anteriores, lo que hace que la clasificación de riesgo sea moderada; se le solicita autenticación adicional antes de permitir la operación.
- El tercer usuario inicia sesión desde un dispositivo que no es de confianza con un alto porcentaje de fallos de autenticación anteriores, lo que hace que la clasificación de riesgo sea alta; la operación no está permitida.

El futuro

- "Activar o desactivar la autorización dinámica"
- "Personalizar la autorización dinámica"

Active o desactive la autorización dinámica en ONTAP

A partir de ONTAP 9.15,1, los administradores pueden configurar y activar la autorización dinámica tanto en `visibility` modo para probar la configuración como en `enforced` modo para activar la configuración para usuarios CLI que se conectan a través de SSH. Si ya no necesita autorización dinámica, puede desactivarla. Cuando desactiva la autorización dinámica, los ajustes de configuración permanecen disponibles y puede utilizarlos más adelante si decide volver a habilitarla.

Obtenga más información sobre `security dynamic-authorization modify` en el "Referencia de

comandos del ONTAP".

Active la autorización dinámica para realizar pruebas

Puede activar la autorización dinámica en el modo de visibilidad, lo que le permite probar la función y garantizar que los usuarios no se bloquearán accidentalmente. En este modo, la puntuación de confianza se comprueba con cada actividad restringida, pero no se aplica. Sin embargo, se registra cualquier actividad que hubiera sido denegada o sujeta a problemas de autenticación adicionales. Como práctica recomendada, debe probar la configuración deseada en este modo antes de aplicarla.

Puede seguir este paso para activar la autorización dinámica por primera vez, incluso si aún no ha configurado ninguna otra configuración de autorización dinámica. Consulte "Personalizar la autorización dinámica"los pasos para configurar otros valores de autorización dinámica para personalizarlos en su entorno.

Pasos

1. Active la autorización dinámica en modo de visibilidad configurando los ajustes globales y cambiando el estado de la característica a `visibility`. Si no se usa `-vserver` el parámetro, el comando se ejecuta a nivel del clúster. Actualice los valores entre paréntesis <> para que coincidan con el entorno. Los parámetros en negrita son necesarios:

```
security dynamic-authorization modify \
<strong>-state visibility</strong> \
-lower-challenge-boundary <percent> \
-upper-challenge-boundary <percent> \
-suppression-interval <interval> \
-vserver <storage_VM_name>
```

2. Compruebe el resultado mediante el `show` comando para mostrar la configuración global:

```
security dynamic-authorization show
```

Active la autorización dinámica en modo forzado

Puede activar la autorización dinámica en modo forzado. Normalmente, se utiliza este modo después de haber completado las pruebas con el modo de visibilidad. En este modo, la puntuación de confianza se comprueba con cada actividad restringida y las restricciones de actividad se aplican si se cumplen las condiciones de restricción. El intervalo de supresión también se aplica, lo que evita problemas de autenticación adicionales dentro del intervalo especificado.

Este paso supone que ha configurado y activado previamente la autorización dinámica en `visibility` modo, lo cual es muy recomendable.

Pasos

1. Active la autorización dinámica en `enforced` modo cambiando su estado a `enforced`. Si no se usa `-vserver` el parámetro, el comando se ejecuta a nivel del clúster. Actualice los valores entre paréntesis <> para que coincidan con el entorno. Los parámetros en negrita son necesarios:

```
security dynamic-authorization modify \
<strong>-state enforced</strong> \
-vserver <storage_VM_name>
```

2. Compruebe el resultado mediante el `show` comando para mostrar la configuración global:

```
security dynamic-authorization show
```

Desactive la autorización dinámica

Puede desactivar la autorización dinámica si ya no necesita la seguridad de autenticación añadida.

Pasos

1. Desactive la autorización dinámica cambiando su estado a `disabled`. Si no se usa `-vserver` el parámetro, el comando se ejecuta a nivel del clúster. Actualice los valores entre paréntesis <> para que coincidan con el entorno. Los parámetros en negrita son necesarios:

```
security dynamic-authorization modify \
<strong>-state disabled</strong> \
-vserver <storage_VM_name>
```

2. Compruebe el resultado mediante el `show` comando para mostrar la configuración global:

```
security dynamic-authorization show
```

   Obtenga más información sobre `security dynamic-authorization show` en el "Referencia de comandos del ONTAP".

El futuro

(Opcional) Dependiendo del entorno, consulte "Personalizar la autorización dinámica"para configurar otros ajustes de autorización dinámica.

Personalizar la autorización dinámica en ONTAP

Como administrador, puede personalizar diferentes aspectos de su configuración de autorización dinámica para aumentar la seguridad de las conexiones SSH de administrador remoto al clúster de ONTAP.

Puede personalizar los siguientes ajustes de autorización dinámica en función de sus necesidades de seguridad:

- Configure los valores globales de autorización dinámica
- Configure los componentes de puntuación de confianza de autorización dinámica

- Configurar un proveedor de puntuación de confianza personalizado
- Configurar comandos restringidos
- Configurar grupos de autorización dinámicos

Configure los valores globales de autorización dinámica

Puede configurar valores globales para la autorización dinámica, incluida la máquina virtual de almacenamiento que se protegerá, el intervalo de supresión para los desafíos de autenticación y los ajustes de la puntuación de confianza.

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

Pasos

1. Configure los valores globales para la autorización dinámica. Si no se usa `-vserver` el parámetro, el comando se ejecuta a nivel del clúster. Actualice los valores entre paréntesis <> para que coincidan con el entorno:

```
security dynamic-authorization modify \
-lower-challenge-boundary <percent> \
-upper-challenge-boundary <percent> \
-suppression-interval <interval> \
-vserver <storage_VM_name>
```

2. Vea la configuración resultante:

```
security dynamic-authorization show
```

Configurar comandos restringidos

Al activar la autorización dinámica, la función incluye un conjunto predeterminado de comandos restringidos. Puede modificar esta lista para adaptarla a sus necesidades. Consulte la "Documentación de verificación multi-admin (MAV)" para obtener información sobre la lista predeterminada de comandos restringidos.

Agregue un comando restringido

Puede agregar un comando a la lista de comandos restringidos con autorización dinámica.

Obtenga más información sobre `security dynamic-authorization rule create` en el "Referencia de comandos del ONTAP".

Pasos

1. Agregue el comando. Actualice los valores entre paréntesis <> para que coincidan con el entorno. Si no se usa `-vserver` el parámetro, el comando se ejecuta a nivel del clúster. Los parámetros en negrita son necesarios:

```
security dynamic-authorization rule create \
-query <query> \
<strong>-operation <text></strong> \
-index <integer> \
-vserver <storage_VM_name>
```

2. Vea la lista resultante de comandos restringidos:

```
security dynamic-authorization rule show
```

Eliminar un comando restringido

Puede eliminar un comando de la lista de comandos restringidos con autorización dinámica.

Obtenga más información sobre `security dynamic-authorization rule delete` en el "Referencia de comandos del ONTAP".

Pasos

1. Quite el comando. Actualice los valores entre paréntesis <> para que coincidan con el entorno. Si no se usa `-vserver` el parámetro, el comando se ejecuta a nivel del clúster. Los parámetros en negrita son necesarios:

```
security dynamic-authorization rule delete \
<strong>-operation <text></strong> \
-vserver <storage_VM_name>
```

2. Vea la lista resultante de comandos restringidos:

```
security dynamic-authorization rule show
```

Configurar grupos de autorización dinámicos

De forma predeterminada, la autorización dinámica se aplica a todos los usuarios y grupos tan pronto como la habilite. Sin embargo, puede crear grupos mediante el `security dynamic-authorization group create` comando, de modo que la autorización dinámica solo se aplique a esos usuarios específicos.

Agregue un grupo de autorización dinámica

Puede agregar un grupo de autorización dinámica.

Obtenga más información sobre `security dynamic-authorization group create` en el "Referencia de comandos del ONTAP".

Pasos

1. Cree el grupo. Actualice los valores entre paréntesis <> para que coincidan con el entorno. Si no se usa `-vserver` el parámetro, el comando se ejecuta a nivel del clúster. Los parámetros en negrita son necesarios:

```
security dynamic-authorization group create \
<strong>-name <group-name></strong> \
-vserver <storage_VM_name> \
-excluded-usernames <user1,user2,user3...>
```

2. Vea los grupos de autorización dinámica resultantes:

```
security dynamic-authorization group show
```

Eliminar un grupo de autorización dinámica

Puede eliminar un grupo de autorización dinámica.

Obtenga más información sobre `security dynamic-authorization group delete` en el "Referencia de comandos del ONTAP".

Pasos

1. Elimine el grupo. Actualice los valores entre paréntesis <> para que coincidan con el entorno. Si no se usa `-vserver` el parámetro, el comando se ejecuta a nivel del clúster. Los parámetros en negrita son necesarios:

```
security dynamic-authorization group delete \
<strong>-name <group-name></strong> \
-vserver <storage_VM_name>
```

2. Vea los grupos de autorización dinámica resultantes:

```
security dynamic-authorization group show
```

Configure los componentes de puntuación de confianza de autorización dinámica

Puede configurar el peso máximo de puntuación para cambiar la prioridad de los criterios de puntuación o para eliminar determinados criterios de la puntuación de riesgo.

> Como práctica recomendada, debe dejar los valores predeterminados de ponderación de puntuación en su lugar y ajustarlos solo si es necesario.

Obtenga más información sobre `security dynamic-authorization trust-score-component modify` en el "Referencia de comandos del ONTAP".

Los siguientes son los componentes que puede modificar, junto con su puntuación predeterminada y sus

ponderaciones porcentuales:

Criterios	Nombre del componente	Peso bruto por defecto de la puntuación	Peso porcentual predeterminado
Dispositivo de confianza	`trusted-device`	20	50
Historial de autenticación de inicio de sesión de usuario	`authentication-history`	20	50

Pasos

1. Modificar componentes de puntuación de confianza. Actualice los valores entre paréntesis <> para que coincidan con el entorno. Si no se usa `-vserver` el parámetro, el comando se ejecuta a nivel del clúster. Los parámetros en negrita son necesarios:

```
security dynamic-authorization trust-score-component modify \
<strong>-component <component-name></strong> \
<strong>-weight <integer></strong> \
-vserver <storage_VM_name>
```

2. Vea la configuración del componente de puntuación de confianza resultante:

```
security dynamic-authorization trust-score-component show
```

Restablezca la puntuación de confianza de un usuario

Si se deniega el acceso a un usuario debido a políticas del sistema y es capaz de probar su identidad, el administrador puede restablecer la puntuación de confianza del usuario.

Obtenga más información sobre `security dynamic-authorization user-trust-score reset` en el "Referencia de comandos del ONTAP".

Pasos

1. Agregue el comando. Consulte Configure los componentes de puntuación de confianza de autorización dinámicapara obtener una lista de componentes de puntuación de confianza que puede restablecer. Actualice los valores entre paréntesis <> para que coincidan con el entorno. Si no se usa `-vserver` el parámetro, el comando se ejecuta a nivel del clúster. Los parámetros en negrita son necesarios:

```
security dynamic-authorization user-trust-score reset \
<strong>-username <username></strong> \
<strong>-component <component-name></strong> \
-vserver <storage_VM_name>
```

Muestra tu puntuación de confianza

Un usuario puede mostrar su propia puntuación de confianza para una sesión de conexión.

Pasos

1. Mostrar su puntuación de confianza:

   ```
   security login whoami
   ```

   Debería ver una salida similar a la siguiente:

   ```
   User: admin
   Role: admin
   Trust Score: 50
   ```

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

Configurar un proveedor de puntuación de confianza personalizado

Si ya recibe métodos de puntuación de un proveedor de puntuación de confianza externo, puede agregar el proveedor personalizado a la configuración de autorización dinámica.

Antes de empezar

- El proveedor de puntuación de confianza personalizado debe devolver una respuesta JSON. Deben cumplirse los siguientes requisitos de sintaxis:
  - El campo que devuelve la puntuación de confianza debe ser un campo escalar y no un elemento de una matriz.
  - El campo que devuelve la puntuación de confianza puede ser un campo anidado, `trust_score.value` como .
  - Debe haber un campo dentro de la respuesta JSON que devuelva una puntuación de confianza numérica. Si esto no está disponible de forma nativa, puede escribir un script de contenedor para devolver este valor.
- El valor proporcionado puede ser una puntuación de confianza o una puntuación de riesgo. La diferencia es que la puntuación de confianza está en orden ascendente con una puntuación más alta que indica un nivel de confianza más alto, mientras que la puntuación de riesgo está en orden descendente. Por ejemplo, una puntuación de confianza de 90 para un rango de puntuación de 0 a 100 indica que la puntuación es muy confiable y probable que resulte en un “permiso” sin desafío adicional, mientras que una puntuación de riesgo de 90 para un rango de puntuación de 0 a 100 indica un alto riesgo y es probable que resulte en una “denegación” sin un desafío adicional.
- Se debe poder acceder al proveedor de puntuación de confianza personalizado a través de la API DE REST DE ONTAP.
- El proveedor de puntuación de confianza personalizada debe configurarse mediante uno de los parámetros admitidos. No se admiten los proveedores de puntuación de confianza personalizados que requieren una configuración que no esté en la lista de parámetros soportados.

  Obtenga más información sobre `security dynamic-authorization trust-score-component create` en el "Referencia de comandos del ONTAP".

Pasos

1. Agregar un proveedor de puntuación de confianza personalizado. Actualice los valores entre paréntesis <> para que coincidan con el entorno. Si no se usa `-vserver` el parámetro, el comando se ejecuta a nivel del clúster. Los parámetros en negrita son necesarios:

```
security dynamic-authorization trust-score-component create \
-component <text> \
<strong>-provider-uri <text></strong> \
-score-field <text> \
-min-score <integer> \
<strong>-max-score <integer></strong> \
<strong>-weight <integer></strong> \
-secret-access-key "<key_text>" \
-provider-http-headers <list<header,header,header>> \
-vserver <storage_VM_name>
```

2. Vea la configuración del proveedor de puntuación de confianza resultante:

```
security dynamic-authorization trust-score-component show
```

Configurar etiquetas personalizadas de proveedor de puntuación de confianza

Puede comunicarse con proveedores de puntuación de confianza externos mediante etiquetas. Esto le permite enviar información en la URL al proveedor de puntuación de confianza sin exponer información confidencial.

Obtenga más información sobre `security dynamic-authorization trust-score-component create` en el "Referencia de comandos del ONTAP".

Pasos

1. Activar etiquetas de proveedor de puntuación de confianza. Actualice los valores entre paréntesis <> para que coincidan con el entorno. Si no se usa `-vserver` el parámetro, el comando se ejecuta a nivel del clúster. Los parámetros en negrita son necesarios:

```
security dynamic-authorization trust-score-component create \
<strong>-component <component_name></strong> \
-weight <initial_score_weight> \
-max-score <max_score_for_provider> \
<strong>-provider-uri <provider_URI></strong> \
-score-field <REST_API_score_field> \
<strong>-secret-access-key "<key_text>"</strong>
```

   Por ejemplo:

```
security dynamic-authorization trust-score-component create -component
comp1 -weight 20 -max-score 100 -provider-uri https://<url>/trust-
scores/users/<user>/<ip>/component1.html?api-key=<access-key> -score
-field score -access-key "MIIBBjCBrAIBArqyTHFvYdWiOpLkLKHGjUYUNSwfzX"
```

Autenticación y autorización mediante OAuth 2,0

Descripción general de la implementación de ONTAP OAuth 2,0

A partir de ONTAP 9,14, tiene la opción de controlar el acceso a sus clústeres de ONTAP mediante el marco de autorización abierta (OAuth 2,0). Es posible configurar esta función mediante cualquiera de las interfaces administrativas de ONTAP, incluida la interfaz de línea de comandos de ONTAP, System Manager y la API de REST. Sin embargo, las decisiones de autorización y control de acceso de OAuth 2,0 solo se pueden aplicar cuando un cliente accede a ONTAP mediante la API REST.

La compatibilidad con OAuth 2,0 se introdujo por primera vez con ONTAP 9.14.0, por lo que su disponibilidad depende de la versión de ONTAP que esté utilizando. Consulte la "Notas de la versión de ONTAP" para obtener más información.

Funciones y beneficios

A continuación se describen las principales características y ventajas del uso de OAuth 2,0 con ONTAP.

Compatibilidad con el estándar OAuth 2,0

OAuth 2,0 es el marco de autorización estándar de la industria. Se utiliza para restringir y controlar el acceso a recursos protegidos mediante tokens de acceso firmados. Hay varios beneficios al usar OAuth 2,0:

- Muchas opciones para la configuración de autorización
- Nunca reveles las credenciales del cliente, incluidas las contraseñas
- Los tokens se pueden definir para que caduquen según la configuración
- Ideal para su uso con API DE REST

Probado con servidores de autorización populares

La implementación de ONTAP OAuth 2,0 se ha probado con varios servidores o servicios populares basados en la versión de ONTAP de la siguiente manera:

- ONTAP 9.16,1 (compatibilidad con UUID de grupo para asignación de nombres y roles externos):
  - ID de Microsoft Entra
- ONTAP 9.14,1 (soporte para las funciones estándar de OAuth 2,0)
  - Auth0
  - Servicio de federación de Active Directory (ADFS)
  - Keycloak

Consulte "Servidores de autorización y tokens de acceso" para obtener más información sobre las funciones y

capacidades disponibles con cada versión de ONTAP.

Compatibilidad con varios servidores de autorización simultáneos

Puede definir hasta ocho servidores de autorización para un solo clúster de ONTAP. Esto le da la flexibilidad para satisfacer las necesidades de su diverso entorno de seguridad.

Integración con los roles REST

Las decisiones de autorización de ONTAP se basan en última instancia en los roles REST asignados a usuarios o grupos. Estos roles se incluyen en el token de acceso como ámbitos independientes o se basan en definiciones de ONTAP locales junto con grupos de Active Directory o LDAP.

Opción para utilizar tokens de acceso restringido por remitente

Puede configurar ONTAP y los servidores de autorización para utilizar la seguridad de la capa de transporte mutuo (MTLS), lo que refuerza la autenticación del cliente. Garantiza que los tokens de acceso OAuth 2,0 solo son utilizados por los clientes a los que fueron emitidos originalmente. Esta característica admite y se alinea con varias recomendaciones de seguridad populares, incluidas las establecidas por FAPI y MITER.

Implementación y configuración

En un nivel alto, hay varios aspectos de una implementación y configuración de OAuth 2,0 que debe tener en cuenta al comenzar.

OAuth 2,0 entidades dentro de ONTAP

El marco de autorización OAuth 2,0 define varias entidades que se pueden asignar a elementos reales o virtuales dentro de su centro de datos o red. Las entidades OAuth 2,0 y su adaptación a ONTAP se presentan en la tabla siguiente.

Entidad OAuth 2,0	Descripción
Recurso	Los extremos de la API de REST que proporcionan acceso a los recursos de la ONTAP mediante comandos internos de la ONTAP.
Propietario del recurso	El usuario de clúster de ONTAP que creó el recurso protegido o lo posee de forma predeterminada.
Servidor de recursos	El host de los recursos protegidos que es el clúster de ONTAP.
Cliente	Una aplicación que solicita acceso a un extremo de API DE REST en nombre o con permiso del propietario del recurso.
Servidor de autorización	Por lo general, un servidor dedicado responsable de emitir tokens de acceso y aplicar políticas administrativas.

Configuración principal de ONTAP

Debe configurar el clúster de ONTAP para habilitar y utilizar OAuth 2,0. Esto incluye establecer una conexión con el servidor de autorización y definir la configuración de autorización ONTAP necesaria. Esta configuración se puede realizar mediante cualquiera de las interfaces administrativas, incluidas las siguientes:

- Interfaz de línea de comandos de ONTAP
- System Manager
- API REST de ONTAP

Medio ambiente y servicios de apoyo

Además de las definiciones de ONTAP, también debe configurar los servidores de autorización. Si usa la

asignación de grupo a rol, también es necesario configurar los grupos de Active Directory o el equivalente de LDAP.

Clientes ONTAP compatibles

A partir de ONTAP 9,14, un cliente API DE REST puede acceder a ONTAP con OAuth 2,0. Antes de emitir una llamada a la API de REST, debe obtener un token de acceso del servidor de autorización. A continuación, el cliente pasa este token al cluster de ONTAP como *bearer token* mediante el encabezado de solicitud de autorización HTTP. Dependiendo del nivel de seguridad necesario, también puede crear e instalar un certificado en el cliente para utilizar tokens restringidos por remitente basados en MTLS.

Terminología seleccionada

A medida que comience a explorar una implementación de OAuth 2,0 con ONTAP, es útil familiarizarse con algunos de los términos. Consulte "Recursos adicionales"los enlaces para obtener más información sobre OAuth 2,0.

Token de acceso

Token emitido por un servidor de autorización y utilizado por una aplicación cliente OAuth 2,0 para realizar solicitudes de acceso a los recursos protegidos.

Token web JSON

Estándar utilizado para formatear los tokens de acceso. JSON se utiliza para representar las reclamaciones OAuth 2,0 en un formato compacto con las reclamaciones dispuestas en tres secciones principales.

Token de acceso restringido por el remitente

Función opcional basada en el protocolo de seguridad de la capa de transporte mutuo (MTLS). Mediante el uso de una reclamación de confirmación adicional en el token, esto garantiza que el token de acceso solo sea utilizado por el cliente para el que se emitió originalmente.

Juego de claves web JSON

Un JWKS es una colección de claves públicas utilizadas por ONTAP para verificar los tokens JWT presentados por los clientes. Los conjuntos de claves suelen estar disponibles en el servidor de autorización a través de un URI dedicado.

Ámbito

Los ámbitos proporcionan una forma de limitar o controlar el acceso de una aplicación a recursos protegidos como la API REST DE ONTAP. Se representan como cadenas en el token de acceso.

Rol DE REST de ONTAP

Los roles de REST se introdujeron con ONTAP 9,6 y son una parte principal del marco de control de acceso basado en roles de ONTAP. Estos roles son diferentes a los roles tradicionales anteriores que todavía son compatibles con ONTAP. La implementación de OAuth 2,0 en ONTAP solo admite roles REST.

Cabecera de autorización HTTP

Un encabezado incluido en la solicitud HTTP para identificar el cliente y los permisos asociados como parte de realizar una llamada a la API REST. Hay varios tipos o implementaciones disponibles dependiendo de cómo se realice la autenticación y la autorización. Al presentar un token de acceso OAuth 2,0 a ONTAP, el token se identifica como un token *bearer*.

Autenticación básica HTTP

Una técnica de autenticación HTTP temprana aún soportada por ONTAP. Las credenciales de texto sin formato (nombre de usuario y contraseña) se concatenan con dos puntos y se codifican en base64. La

cadena se coloca en la cabecera de solicitud de autorización y se envía al servidor.

FAPI

Un grupo de trabajo de la Fundación OpenID que proporciona protocolos, esquemas de datos y recomendaciones de seguridad para el sector financiero. La API se conocía originalmente como la API de grado financiero.

INGLETE

Una compañía privada sin fines de lucro que proporciona orientación técnica y de seguridad a la Fuerza Aérea de los Estados Unidos y al gobierno de los Estados Unidos.

Recursos adicionales

A continuación se proporcionan varios recursos adicionales. Usted debe revisar estos sitios para obtener más información sobre OAuth 2,0 y los estándares relacionados.

Protocolos y estándares

- "RFC 6749: Marco de Autorización de OAuth 2,0"
- "RFC 7519: Tokens web JSON (JWT)"
- "RFC 7523: Perfil JSON Web Token (JWT) para la autenticación y autorización de cliente OAuth 2,0"
- "RFC 7662: Introspección del token OAuth 2,0"
- "RFC 7800: Clave de prueba de posesión para JWT"
- "RFC 8705: Autenticación de cliente Mutual-TLS de OAuth 2,0 y tokens de acceso vinculados a certificados"

Organizaciones

- "Fundación OpenID"
- "Grupo de trabajo de FAPI"
- "INGLETE"
- "IANA - JWT"

Productos y servicios

- "Auth0"
- "ID Entra"
- "Descripción general de ADFS"
- "Keycloak"

Herramientas y utilidades adicionales

- "JWT por Auth0"
- "OpenSSL"

Documentación y recursos de NetApp

- "Documentación de automatización de ONTAP"

Conceptos

Servidores de autorización OAuth 2.0 y tokens de acceso en ONTAP

Los servidores de autorización realizan varias funciones importantes como componente central dentro del marco de autorización de OAuth 2,0.

Servidores de autorización OAuth 2,0

Los servidores de autorización son los principales responsables de crear y firmar tokens de acceso. Estos tokens contienen información de identidad y autorización que permite a una aplicación cliente acceder selectivamente a los recursos protegidos. Los servidores generalmente están aislados entre sí y se pueden implementar de varias maneras diferentes, incluyendo como un servidor dedicado independiente o como parte de un producto de gestión de identidad y acceso más grande.

> En ocasiones, se puede utilizar una terminología diferente para un servidor de autorización, especialmente cuando la funcionalidad OAuth 2,0 está empaquetada dentro de un producto o solución de gestión de acceso e identidad más grande. Por ejemplo, el término **proveedor de identidad (IDP)** se utiliza con frecuencia indistintamente con **servidor de autorización**.

Administración

Además de emitir tokens de acceso, los servidores de autorización también proporcionan servicios administrativos relacionados, normalmente a través de una interfaz de usuario web. Por ejemplo, puede definir y administrar:

- Autenticación de usuarios y usuarios
- Ámbitos
- Segregación administrativa a través de inquilinos y dominios
- Aplicación de políticas
- Conexión a varios servicios externos
- Compatibilidad con otros protocolos de identidad (como SAML)

ONTAP es compatible con los servidores de autorización que cumplen con el estándar OAuth 2,0.

Definición a ONTAP

Debe definir uno o varios servidores de autorización para ONTAP. ONTAP se comunica de forma segura con cada servidor para verificar tokens y realizar otras tareas relacionadas en soporte de las aplicaciones cliente.

A continuación se presentan los principales aspectos de la configuración de ONTAP. Consulte también "Escenarios de despliegue de OAuth 2,0"para obtener más información.

Cómo y dónde se validan los tokens de acceso

Hay dos opciones para validar tokens de acceso.

- Validación local

  ONTAP puede validar los tokens de acceso localmente en función de la información proporcionada por el servidor de autorización que emitió el token. ONTAP almacena en caché la información recuperada del servidor de autorización y se actualiza periódicamente.

- Introspección remota

También puede utilizar la introspección remota para validar tokens en el servidor de autorización. La introspección es un protocolo que permite a las partes autorizadas consultar un servidor de autorización sobre un token de acceso. Proporciona a ONTAP una forma de extraer ciertos metadatos de un token de acceso y validar el token. ONTAP almacena en la caché algunos datos por razones de rendimiento.

Ubicación de red

ONTAP puede estar detrás de un firewall. En este caso, debe identificar un proxy como parte de la configuración.

Cómo se definen los servidores de autorización

Puede definir un servidor de autorización para ONTAP mediante cualquiera de las interfaces de administración, incluida la CLI, System Manager o la API DE REST. Por ejemplo, con la CLI utiliza el comando `security oauth2 client create`.

Obtenga más información sobre `security oauth2 client create` en el "Referencia de comandos del ONTAP".

Número de servidores de autorización

Puede definir hasta ocho servidores de autorización en un solo clúster de ONTAP. El mismo servidor de autorización se puede definir más de una vez en el mismo clúster de ONTAP, siempre y cuando las reclamaciones del emisor o del emisor/público sean únicas. Por ejemplo, con Keycloak esto siempre será el caso cuando se utilizan diferentes dominios.

Funciones de OAuth 2,0 admitidas en ONTAP

La compatibilidad con OAuth 2,0 estaba disponible inicialmente con ONTAP 9.14,1 y continúa mejorándose con las versiones posteriores. A continuación se describen las funciones de OAuth 2,0 compatibles con ONTAP.

> Las funciones introducidas con una versión específica de ONTAP se transfieren a futuras versiones.

ONTAP 9.16.1

ONTAP 9.16,1 amplía las características estándar de OAuth 2,0 para incluir extensiones específicas de Entra ID para grupos nativos de Entra ID. Esto implica el uso de GUID en el token de acceso en lugar de nombres. Además, la versión agrega compatibilidad con la asignación de roles externos para asignar los roles de proveedor de identidad nativos a los roles de ONTAP mediante el campo “roles” en el token de acceso.

ONTAP 9.14.1

A partir de ONTAP 9.14,1, los servidores de autorización son compatibles con las siguientes funciones estándar de OAuth 2,0 para aplicaciones que utilizan:

- OAuth 2,0 con los campos estándar incluyendo “iss”, “aud” y “exp” como se describe en "RFC6749: El Marco de Autorización OAuth 2,0" y "RFC 7519: Token web JSON (JWT)". Esto también incluye soporte para la identificación única de usuarios a través de campos en el token de acceso como “upn”, “appid”, “sub”, “username” o “preferred_username”.
- Extensiones específicas del proveedor de ADFS para nombres de grupo con el campo de grupo.
- Extensiones específicas del proveedor de Azure para UUID de grupo con el campo de grupo.
- Extensiones ONTAP para soporte de autorización mediante roles independientes y con nombre dentro del alcance del token de acceso OAuth 2,0. Esto incluye los campos “Alcance” y “scp”, así como los nombres

de grupo dentro del alcance.

Uso de tokens de acceso OAuth 2,0

Los tokens de acceso OAuth 2,0 emitidos por los servidores de autorización son verificados por ONTAP y utilizados para tomar decisiones de acceso basadas en roles para las solicitudes del cliente API REST.

Adquiriendo un token de acceso

Es necesario adquirir un token de acceso de un servidor de autorización definido en el clúster de ONTAP donde se utiliza la API DE REST. Para adquirir un token, debe ponerse en contacto directamente con el servidor de autorización.

ONTAP no emite tokens de acceso ni redirige las solicitudes de los clientes a los servidores de autorización.

La forma en que se solicita un token depende de varios factores, entre ellos:

- Servidor de autorización y sus opciones de configuración
- Tipo de concesión OAuth 2,0
- Cliente o herramienta de software utilizada para emitir la solicitud

Tipos de concesión

Un *grant* es un proceso bien definido, que incluye un conjunto de flujos de red, utilizado para solicitar y recibir un token de acceso OAuth 2,0. Se pueden utilizar varios tipos de concesión diferentes en función del cliente, el entorno y los requisitos de seguridad. En la tabla siguiente se presenta una lista de los tipos de subvención más populares.

Tipo de concesión	Descripción
Credenciales de cliente	Tipo de concesión popular basado en el uso de solo credenciales (como un ID y un secreto compartido). Se supone que el cliente tiene una relación de confianza cercana con el propietario del recurso.
Contraseña	El tipo de concesión de credenciales de contraseña de propietario del recurso se puede utilizar en los casos en que el propietario del recurso tenga una relación de confianza establecida con el cliente. También puede ser útil al migrar clientes HTTP heredados a OAuth 2,0.
Código de autorización	Este es un tipo de concesión ideal para clientes confidenciales y se basa en un flujo basado en redirección. Se puede utilizar para obtener un token de acceso y un token de refrescamiento.

Contenido de JWT

Un token de acceso OAuth 2,0 se formatea como JWT. El contenido es creado por el servidor de autorización en función de su configuración. Sin embargo, los tokens son opacos para las aplicaciones cliente. Un cliente no tiene ninguna razón para inspeccionar un token o para ser consciente de su contenido.

Cada token de acceso JWT contiene un juego de reclamaciones. Las reclamaciones describen las características del emisor y la autorización en función de las definiciones administrativas del servidor de autorización. Algunas de las reclamaciones registradas con el estándar se describen en la siguiente tabla. Todas las cadenas distinguen mayúsculas de minúsculas.

Reclamación	Palabra clave	Descripción
Emisor	iss	Identifica el principal que emitió el token. El procesamiento de la reclamación es específico de la aplicación.
Asunto	secundario	Asunto o usuario del token. El ámbito del nombre es global o localmente único.
Destinatarios	aud	Destinatarios para los que está destinado el token. Implementado como una matriz de cadenas.
Caducidad	esp	Hora después de la cual el token caduca y debe rechazarse.

Consulte "RFC 7519: Tokens web JSON" para obtener más información.

Autorización de cliente

Descripción general y opciones para la autorización del cliente de ONTAP

La implementación de ONTAP OAuth 2,0 está diseñada para ser flexible y robusta, proporcionando las características que necesita para proteger su entorno ONTAP. Hay varias opciones de configuración mutuamente excluyentes disponibles. Las decisiones de autorización se basan en última instancia en los roles REST DE ONTAP contenidos en o derivados de los tokens de acceso OAuth 2,0.

Sólo puede utilizarse "Roles DE REST de ONTAP" al configurar la autorización para OAuth 2,0. No se admiten los roles tradicionales de ONTAP anteriores.

ONTAP aplica la opción de autorización más adecuada en función de su configuración. Consulte "Cómo ONTAP determina el acceso" para obtener más información acerca de cómo ONTAP toma decisiones sobre el acceso de los clientes.

OAuth 2,0 ámbitos independientes

Estos ámbitos contienen uno o más roles REST personalizados, cada uno encapsulado dentro de una única cadena en el token de acceso. Son independientes de las definiciones de roles de ONTAP. Debe configurar las cadenas de ámbito en el servidor de autorización. Consulte "Alcances OAuth 2,0 autónomos" para obtener más información.

Roles DE REST DE ONTAP local

Se puede utilizar un único rol REST con nombre, ya sea Builtin o Custom. La sintaxis del ámbito para un rol con nombre es **ontap-role-**<URL-encoded-ONTAP-role-name>. Por ejemplo, si el rol ONTAP es `admin` la cadena de ámbito será `ontap-role-admin`.

Usuarios

Se puede utilizar el nombre de usuario en el token de acceso definido con acceso a la aplicación http. Un usuario se prueba en el siguiente orden según el método de autenticación definido: Contraseña, dominio (Active Directory), nsswitch (LDAP).

Grupos

Los servidores de autorización se pueden configurar para utilizar grupos ONTAP para su autorización. Si se examinan las definiciones de ONTAP locales pero no se puede tomar ninguna decisión de acceso, se utilizan los grupos de Active Directory («dominio») o LDAP («nsswitch»). La información del grupo se puede especificar de dos formas:

- Cadena de ámbito de OAuth 2,0

  Admite aplicaciones confidenciales mediante el flujo de credenciales de cliente donde no hay ningún usuario con una pertenencia a grupo. El ámbito debe denominarse **ontap-group-**<URL-encoded-ONTAP-group-name>. Por ejemplo, si el grupo está en «desarrollo», la cadena de alcance será «ontap-group-development».

- En el reclamo de “grupo”

  Esto está destinado a los tokens de acceso emitidos por ADFS mediante el flujo de propietario de recursos (concesión de contraseña).

Ver "Trabajar con grupos IdP de OAuth 2.0 o SAML en ONTAP" Para más información.

Ámbitos OAuth 2.0 autónomos en ONTAP

Los ámbitos autónomos son cadenas que se llevan en el token de acceso. Cada una de ellas es una definición de función personalizada completa e incluye todo lo que ONTAP necesita para tomar una decisión de acceso. El ámbito está separado y distinto de cualquiera de los roles de REST definidos en el propio ONTAP.

Formato de la cadena de ámbito

En un nivel base, el ámbito se representa como una cadena contigua y se compone de seis valores separados por dos puntos. Los parámetros utilizados en la cadena de ámbito se describen a continuación.

ONTAP literal

El ámbito debe comenzar con el valor literal `ontap` en minúscula. Identifica el ámbito como específico de ONTAP.

Clúster

Esto define al cluster de ONTAP al que se aplica el ámbito. Los valores pueden incluir:

- UUID del clúster

  Identifica un único clúster.

- Asterisco (*)

  Indica que el ámbito se aplica a todos los clusters.

Puede utilizar el comando de la CLI de ONTAP `cluster identity show` para mostrar el UUID de su clúster. Si no se especifica, el ámbito se aplica a todos los clusters. Obtenga más información sobre `cluster identity show` en el "Referencia de comandos del ONTAP".

Función

Nombre del rol REST contenido en el ámbito autónomo. ONTAP no examina este valor ni se relaciona con ningún rol de REST existente definido con ONTAP. El nombre se utiliza para el registro.

Nivel de acceso

Este valor indica el nivel de acceso aplicado a la aplicación cliente cuando se utiliza el punto final de API en el ámbito. Hay seis valores posibles, como se describe en la tabla siguiente.

Nivel de acceso	Descripción
ninguno	Deniega todo el acceso al punto final especificado.
sólo lectura	Permite solo el acceso de lectura mediante GET.
read_create	Permite el acceso de lectura, así como la creación de nuevas instancias de recursos mediante POST.
read_modify	Permite el acceso de lectura, así como la capacidad de actualizar los recursos existentes MEDIANTE PARCHE.
read_create_modify	Permite todos los accesos excepto eliminar. Las operaciones permitidas incluyen GET (READ), POST (CREATE) y PARCHE (UPDATE).
todo	Permite un acceso completo.

SVM

El nombre de la SVM dentro del clúster al que se aplica el ámbito. Utilice el valor * (asterisco) para indicar todas las SVM.

Esta función no es totalmente compatible con ONTAP 9.14.1. Puede ignorar el parámetro SVM y usar un asterisco como marcador de posición. Revise el "Notas de la versión de ONTAP" para comprobar si hay compatibilidad con SVM en el futuro.

URI DE LA API DE REST

Ruta de acceso completa o parcial a un recurso o juego de recursos relacionados. La cadena debe comenzar por `/api`. Si no especifica un valor, el alcance se aplica a todos los extremos de API en el clúster de ONTAP.

Ejemplos de ámbito

A continuación se presentan algunos ejemplos de ámbitos autónomos.

ontap:*:joes-role:read_create_modify:*:/api/cluster

Proporciona al usuario asignado a este rol acceso de lectura, creación y modificación al `/cluster` punto final.

Herramienta administrativa de la CLI

Para que la administración de los ámbitos autónomos sea más fácil y menos propensa a errores, ONTAP proporciona el comando CLI `security oauth2 scope` para generar cadenas de alcance basadas en los parámetros de entrada.

El comando `security oauth2 scope` tiene dos casos de uso basados en su entrada:

- Parámetros de CLI para la cadena de ámbito

  Puede utilizar esta versión del comando para generar una cadena de ámbito basada en los parámetros de entrada.

- Cadena de ámbito para parámetros de CLI

  Puede utilizar esta versión del comando para generar los parámetros del comando basados en la cadena de ámbito de entrada.

Ejemplo

El siguiente ejemplo genera una cadena de ámbito con la salida incluida después del siguiente ejemplo de comando. La definición se aplica a todos los clusters.

```
security oauth2 scope cli-to-scope -role joes-role -access readonly -api
/api/cluster
```

```
ontap:*:joes-role:readonly:*:/api/cluster
```

Obtenga más información sobre `security oauth2 scope` en el "Referencia de comandos del ONTAP".

Mapeo de roles externos de OAuth 2.0 en ONTAP

Un rol externo se define en un proveedor de identificación configurado para su uso por ONTAP. Es posible crear y administrar relaciones de asignación entre estos roles externos y los roles de ONTAP mediante la CLI de ONTAP.

> También es posible configurar la función de asignación de roles externos mediante la API DE REST DE ONTAP. Obtenga más información en el "Documentación de automatización de ONTAP".

Roles externos en un token de acceso

Aquí hay un fragmento de un token de acceso JSON que contiene dos roles externos.

```
...
"appidacr": "1",
"family_name": "User",
"name": "Test User 1",
"oid": "4c2215c7-6d52-40a7-ce71-096fa41379ba",
"roles": [
  "Global Administrator",
  "Application Administrator"
],
"ver": "1.0",
...
```

Configuración

Puede utilizar la interfaz de línea de comandos de ONTAP para administrar la función de asignación de roles externos.

Crear

Puede definir una configuración de asignación de roles con `security login external-role-mapping create` el comando. Debe estar en el nivel de privilegio **admin** de ONTAP para emitir este comando, así como las opciones relacionadas.

Parámetros

A continuación se describen los parámetros utilizados para crear una asignación de grupo.

Parámetro	Descripción
`external-role`	Nombre del rol definido en el proveedor de identidad externo.
`provider`	Nombre del proveedor de identidad. Este debe ser el identificador del sistema.
`ontap-role`	Indica el rol de ONTAP existente al que está asignado el rol externo.

Ejemplo

```
security login external-role-mapping create -external-role "Global
Administrator" -provider entra -ontap-role admin
```

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

Operaciones de CLI adicionales

El comando admite varias operaciones adicionales, entre las que se incluyen:

- Mostrar
- Modificar
- Eliminar

Información relacionada

- "Referencia de comandos del ONTAP"

Cómo determina ONTAP el acceso del cliente

Para diseñar e implementar correctamente OAuth 2,0, es necesario comprender cómo ONTAP utiliza su configuración de autorización para tomar decisiones de acceso para los clientes. Los pasos principales utilizados para determinar el acceso se presentan a continuación en función de la versión de ONTAP.

No hubo actualizaciones significativas de OAuth 2,0 con ONTAP 9.15,1. Si utiliza la versión 9.15.1, consulte la descripción de ONTAP 9.14,1.

Información relacionada

- "Funciones de OAuth 2,0 admitidas en ONTAP"

ONTAP 9.16.1

ONTAP 9.16,1 amplía la compatibilidad estándar con OAuth 2,0 para incluir extensiones específicas de Microsoft Entra ID para grupos nativos de Entra ID, así como la asignación de roles externos.

Determine el acceso de clientes para ONTAP 9.16,1

Paso 1: Ámbitos autónomos

Si el token de acceso contiene cualquier ámbito autónomo, ONTAP examina estos ámbitos primero. Si no hay ámbitos autónomos, vaya al paso 2.

Con uno o más ámbitos independientes presentes, ONTAP aplica cada ámbito hasta que se pueda tomar una decisión explícita de **PERMITIR** o **NEGAR**. Si se toma una decisión explícita, el procesamiento finaliza.

Si ONTAP no puede tomar una decisión de acceso explícita, continúe con el paso 2.

Paso 2: Compruebe el indicador de roles locales

ONTAP examina el parámetro booleano `use-local-roles-if-present` . El valor de este indicador se define por separado para cada servidor de autorización definido en ONTAP.

- Si el valor es `true`, continúe en el paso 3.
- Si el valor `false` finaliza el procesamiento y se deniega el acceso.

Paso 3: Se denomina rol REST ONTAP

Si el token de acceso contiene un rol REST con nombre en el `scope` campo o `scp`, o como una reclamación, ONTAP utiliza el rol para tomar la decisión de acceso. Esto siempre da como resultado una decisión **ALLOW** o **DENY** y el procesamiento termina.

Si no hay ningún rol REST con nombre o no se encuentra el rol, continúe con el paso 4.

Paso 4: Usuarios

Extraiga el nombre de usuario del token de acceso e intente hacer coincidir el nombre con los usuarios que tienen acceso a la aplicación «http». Los usuarios se examinan según el método de autenticación en el siguiente orden:

- contraseña
- Dominio (Active Directory)
- Conmutador ns(LDAP)

Si se encuentra un usuario coincidente, ONTAP utiliza el rol definido para el usuario para tomar una decisión de acceso. Esto siempre resulta en una decisión **ALLOW** o **DENY** y el procesamiento termina.

Si un usuario no coincide o no hay nombre de usuario en el token de acceso, continúe con el paso 5.

Paso 5: Grupos

Si se incluyen uno o más grupos, se examina el formato. Si los grupos se representan como UUID, se busca en una tabla interna de mapeo de grupos. Si hay una coincidencia de grupo y un rol asociado, ONTAP utiliza el rol definido para el grupo para tomar una decisión de acceso. Esto siempre resulta en una decisión **ALLOW** o **DENY** y el procesamiento finaliza. Para más información, consulte "Trabajar con grupos IdP de OAuth 2.0 o SAML en ONTAP" .

Si los grupos se representan como nombres y se configuran con autorización de dominio o nsswitch, ONTAP intenta relacionarlos con un grupo de Active Directory o LDAP, respectivamente. Si hay una coincidencia de grupo, ONTAP utiliza el rol definido para el grupo para tomar una decisión de acceso. Esto siempre resulta en una decisión **ALLOW** o **DENY** y el procesamiento termina.

Si no hay ninguna coincidencia de grupo o si no hay ningún grupo en el token de acceso, el acceso se deniega y el procesamiento finaliza.

ONTAP 9.14.1

OAuth 2,0 inicial admitido se introduce con ONTAP 9.14,1 basado en las características estándar de OAuth 2,0.

Determine el acceso de clientes para ONTAP 9.14,1

Paso 1: Ámbitos autónomos

Si el token de acceso contiene cualquier ámbito autónomo, ONTAP examina estos ámbitos primero. Si no hay ámbitos autónomos, vaya al paso 2.

Con uno o más ámbitos independientes presentes, ONTAP aplica cada ámbito hasta que se pueda tomar una decisión explícita de **PERMITIR** o **NEGAR**. Si se toma una decisión explícita, el procesamiento finaliza.

Si ONTAP no puede tomar una decisión de acceso explícita, continúe con el paso 2.

Paso 2: Compruebe el indicador de roles locales

ONTAP examina el parámetro booleano `use-local-roles-if-present` . El valor de este indicador se define por separado para cada servidor de autorización definido en ONTAP.

- Si el valor es `true`, continúe en el paso 3.
- Si el valor `false` finaliza el procesamiento y se deniega el acceso.

Paso 3: Se denomina rol REST ONTAP

Si el token de acceso contiene un rol REST con nombre en el `scope` campo OR `scp`, ONTAP utiliza el rol para tomar la decisión de acceso. Esto siempre da como resultado una decisión **ALLOW** o **DENY** y el procesamiento termina.

Si no hay ningún rol REST con nombre o no se encuentra el rol, continúe con el paso 4.

Paso 4: Usuarios

Extraiga el nombre de usuario del token de acceso e intente hacer coincidir el nombre con los usuarios que tienen acceso a la aplicación «http». Los usuarios se examinan según el método de autenticación en el siguiente orden:

- contraseña
- Dominio (Active Directory)
- Conmutador ns(LDAP)

Si se encuentra un usuario coincidente, ONTAP utiliza el rol definido para el usuario para tomar una decisión de acceso. Esto siempre resulta en una decisión **ALLOW** o **DENY** y el procesamiento termina.

Si un usuario no coincide o no hay nombre de usuario en el token de acceso, continúe con el paso 5.

Paso 5: Grupos

Si se incluyen uno o más grupos y se configuran con autorización de dominio o nsswitch, ONTAP intenta relacionarlos con un grupo LDAP o Active Directory, respectivamente.

Si hay una coincidencia de grupo, ONTAP utiliza el rol definido para el grupo para tomar una decisión de acceso. Esto siempre resulta en una decisión **ALLOW** o **DENY** y el procesamiento termina.

Si no hay ninguna coincidencia de grupo o si no hay ningún grupo en el token de acceso, el acceso se deniega y el procesamiento finaliza.

Escenarios de implementación de OAuth 2.0 con ONTAP

Hay varias opciones de configuración disponibles al definir un servidor de autorización en ONTAP. En función de estas opciones, puede definir un servidor de autorización adecuado para su entorno mediante uno de los varios escenarios de implementación.

Resumen de los parámetros de configuración

Hay varios parámetros de configuración disponibles al definir un servidor de autorización en ONTAP. Estos parámetros se admiten generalmente en todas las interfaces administrativas.

> El nombre utilizado para un parámetro o campo individual puede variar en función de la interfaz administrativa de ONTAP. Para acomodar las diferencias en las interfaces administrativas, se utiliza un único nombre genérico para cada parámetro de la tabla. El nombre exacto utilizado con una interfaz específica debe ser obvio basado en el contexto.

Parámetro	Descripción
Nombre	Nombre del servidor de autorización tal y como lo conoce ONTAP.
Cliente más	Aplicación interna de ONTAP a la que se aplica la definición. Debe ser **http**.
URI del emisor	El FQDN con ruta que identifica el sitio u organización que emite los tokens.
URI de JWKS de Proveedor	El FQDN con ruta y nombre de archivo donde ONTAP obtiene los conjuntos de claves web JSON utilizados para validar los tokens de acceso.
Intervalo de refrescamiento de JWKS	Intervalo de tiempo que determina la frecuencia con la que ONTAP refresca la información de certificado del URI JWKS del proveedor. El valor se especifica en formato ISO-8601.
Punto final de introspección	El FQDN con ruta que ONTAP utiliza para realizar la validación remota de tokens mediante introspección.
ID del cliente	El nombre del cliente tal y como se define en el servidor de autorización. Cuando se incluye este valor, también debe proporcionar el secreto de cliente asociado basado en la interfaz.
Proxy saliente	Esto es para proporcionar acceso al servidor de autorización cuando ONTAP está detrás de un firewall. El URI debe tener el formato cURL.
Utilice roles locales si están presentes	Un indicador booleano que determina si se usan las definiciones de ONTAP locales, incluido un rol REST con nombre y los usuarios locales.
Reclamación de usuario remoto	Nombre alternativo que utiliza ONTAP para coincidir con los usuarios locales. Utilice `sub` el campo del token de acceso para que coincida con el nombre de usuario local.
Destinatarios	Este campo define los puntos finales en los que se puede utilizar el token de acceso.

Escenarios de puesta en marcha

A continuación se presentan varios escenarios de implementación comunes. Se organizan en función de si ONTAP realiza la validación de tokens de forma local o remota mediante el servidor de autorización. Cada escenario incluye una lista de las opciones de configuración necesarias. Consulte "Desplegar OAuth 2,0 en ONTAP" para obtener ejemplos de los comandos de configuración.

Después de definir un servidor de autorización, puede mostrar su configuración a través de la interfaz administrativa de ONTAP. Por ejemplo, utilice el comando `security oauth2 client show` con la interfaz de línea de comandos de ONTAP.

Validación local

Los siguientes escenarios de implementación se basan en que ONTAP realiza la validación de tokens localmente.

Utilice ámbitos autónomos sin proxy

Esta es la implementación más sencilla utilizando solo los ámbitos autónomos de OAuth 2,0. No se utiliza ninguna definición de identidad ONTAP local. Debe incluir los siguientes parámetros:

- Nombre
- Aplicación (http)
- URI de JWKS de Proveedor
- URI del emisor

También debe añadir los ámbitos en el servidor de autorización.

Utilice ámbitos autónomos con un proxy

Este escenario de despliegue utiliza los ámbitos autónomos de OAuth 2,0. No se utiliza ninguna definición de identidad ONTAP local. Pero el servidor de autorización está detrás de un firewall y, por lo tanto, debe configurar un proxy. Debe incluir los siguientes parámetros:

- Nombre
- Aplicación (http)
- URI de JWKS de Proveedor
- Proxy saliente
- URI del emisor
- Destinatarios

También debe añadir los ámbitos en el servidor de autorización.

Use los roles de usuario local y la asignación predeterminada del nombre de usuario con un proxy

Este escenario de despliegue utiliza roles de usuario local con asignación de nombres por defecto. La reclamación de usuario remoto utiliza el valor predeterminado de `sub`, por lo que este campo del token de acceso se utiliza para coincidir con el nombre de usuario local. El nombre de usuario debe tener 40 caracteres o menos. El servidor de autorización está detrás de un firewall, por lo que también debe configurar un proxy. Debe incluir los siguientes parámetros:

- Nombre
- Aplicación (http)
- URI de JWKS de Proveedor
- Usar roles locales si están presentes (`true`)
- Proxy saliente
- Emisor

Debe asegurarse de que el usuario local esté definido en ONTAP.

Use roles de usuario local y una asignación de nombre de usuario alternativa con un proxy

Este escenario de despliegue utiliza roles de usuario local con un nombre de usuario alternativo que se utiliza para que coincida con un usuario local de ONTAP. El servidor de autorización está detrás de un firewall, por lo que debe configurar un proxy. Debe incluir los siguientes parámetros:

- Nombre
- Aplicación (http)
- URI de JWKS de Proveedor
- Usar roles locales si están presentes (`true`)
- Reclamación de usuario remoto
- Proxy saliente
- URI del emisor
- Destinatarios

Debe asegurarse de que el usuario local esté definido en ONTAP.

Introspección remota

Las siguientes configuraciones de implementación se basan en que ONTAP realiza la validación de tokens de forma remota a través de introspección.

Utilice ámbitos autónomos sin proxy

Esta es una implementación sencilla basada en el uso de los ámbitos autónomos OAuth 2,0. No se utiliza ninguna definición de identidad de ONTAP. Debe incluir los siguientes parámetros:

- Nombre
- Aplicación (http)
- Punto final de introspección
- ID del cliente
- URI del emisor

Debe definir los ámbitos, así como el secreto de cliente y cliente en el servidor de autorización.

Información relacionada

- "Mostrar cliente de seguridad OAuth2"

Autenticación de cliente ONTAP mediante OAuth 2.0 Mutual TLS

Dependiendo de sus necesidades de seguridad, puede configurar opcionalmente TLS mutuo (MTLS) para implementar una autenticación de cliente fuerte. Cuando se utiliza con ONTAP como parte de una implementación de OAuth 2,0, MTLS garantiza que los tokens de acceso solo son utilizados por los clientes a los que se emitieron originalmente.

TLS Mutuo con OAuth 2,0

La seguridad de la capa de transporte (TLS) se utiliza para establecer un canal de comunicación seguro entre dos aplicaciones, normalmente un explorador de cliente y un servidor web. El TLS Mutuo amplía esto proporcionando una identificación sólida del cliente a través de un certificado de cliente. Cuando se utiliza en un clúster de ONTAP con OAuth 2,0, la funcionalidad MTLS base se amplía mediante la creación y el uso de tokens de acceso restringidos por el remitente.

Un token de acceso restringido por remitente solo puede ser utilizado por el cliente para el que se emitió originalmente. Para admitir esta función, (`cnf`se inserta una nueva reclamación de confirmación) en el token. El campo contiene la propiedad `x5t#S256` que contiene un resumen del certificado de cliente utilizado al solicitar el token de acceso. ONTAP verifica este valor como parte de la validación del token. Los tokens de acceso emitidos por los servidores de autorización que no están restringidos por el remitente no incluyen la reclamación de confirmación adicional.

Debe configurar ONTAP para que utilice MTLS por separado para cada servidor de autorización. Por ejemplo, el comando CLI `security oauth2 client` incluye el parámetro `use-mutual-tls` para controlar el procesamiento MTLS basado en tres valores como se muestra en la tabla siguiente.

> En cada configuración, el resultado y la acción de ONTAP dependen del valor del parámetro de configuración, así como del contenido del token de acceso y del certificado del cliente. Los parámetros de la tabla se organizan desde el más mínimo hasta el más restrictivo.

Parámetro	Descripción
ninguno	La autenticación TLS mutua OAuth 2,0 está completamente desactivada para el servidor de autorización. ONTAP no realizará la autenticación del certificado de cliente MTLS incluso si la reclamación de confirmación está presente en el token o si se proporciona un certificado de cliente con la conexión TLS.
petición	OAuth 2,0 La autenticación TLS mutua se aplica si el cliente presenta un token de acceso restringido por el remitente. Es decir, MTLS se aplica sólo si la reclamación de confirmación (con propiedad `x5t#S256`) está presente en el token de acceso. Esta es la configuración predeterminada.
obligatorio	La autenticación TLS mutua OAuth 2,0 se aplica a todos los tokens de acceso emitidos por el servidor de autorización. Por lo tanto, todos los tokens de acceso deben estar restringidos por el remitente. Se producen errores en la autenticación y la solicitud de API de REST si la reclamación de confirmación no está presente en el token de acceso o si existe un certificado de cliente no válido.

Flujo de implantación de alto nivel

A continuación se presentan los pasos típicos que implica el uso de MTLS con OAuth 2,0 en un entorno ONTAP. Consulte "RFC 8705: Autenticación de cliente Mutual-TLS de OAuth 2,0 y tokens de acceso vinculados a certificados" para obtener más información.

Paso 1: Crear e instalar un certificado de cliente

El establecimiento de la identidad del cliente se basa en demostrar el conocimiento de una clave privada del cliente. La clave pública correspondiente se coloca en un certificado X,509 firmado presentado por el cliente. En un nivel alto, los pasos involucrados en la creación del certificado de cliente incluyen:

1. Generar un par de claves públicas y privadas
2. Cree una solicitud de firma de certificación

3. Envíe el archivo CSR a una CA conocida
4. CA verifica la solicitud y emite el certificado firmado

Normalmente, puede instalar el certificado de cliente en su sistema operativo local o usarlo directamente con una utilidad común, como cURL.

Paso 2: Configure ONTAP para usar MTLS

Debe configurar ONTAP para que utilice MTLS. Esta configuración se realiza por separado para cada servidor de autorización. Por ejemplo, con la CLI el comando `security oauth2 client` se utiliza con el parámetro opcional `use-mutual-tls` . Consulte "Desplegar OAuth 2,0 en ONTAP" para obtener más información.

Paso 3: El cliente solicita un token de acceso

El cliente necesita solicitar un token de acceso desde el servidor de autorización configurado en ONTAP. La aplicación cliente debe utilizar MTLS con el certificado creado e instalado en el paso 1.

Paso 4: El servidor de autorización genera el token de acceso

El servidor de autorización verifica la solicitud del cliente y genera un token de acceso. Como parte de esto, crea un resumen de mensaje del certificado de cliente que se incluye en el token como una reclamación de confirmación (campo `cnf`).

Paso 5: La aplicación cliente presenta el token de acceso a ONTAP

La aplicación cliente realiza una llamada a la API REST al clúster de ONTAP e incluye el token de acceso en el encabezado de solicitud de autorización como un token **portador**. El cliente debe utilizar MTLS con el mismo certificado utilizado para solicitar el token de acceso.

Paso 6: ONTAP verifica el cliente y el token.

ONTAP recibe el token de acceso en una solicitud HTTP, así como el certificado de cliente utilizado como parte del procesamiento MTLS. ONTAP valida primero la firma en el token de acceso. En función de la configuración, ONTAP genera un resumen de mensaje del certificado de cliente y lo compara con la reclamación de confirmación **cnf** en el token. Si los dos valores coinciden, ONTAP ha confirmado que el cliente que hace la solicitud API es el mismo cliente al que se emitió originalmente el token de acceso.

Información relacionada

- "cliente de seguridad oauth2"

Configurar e implementar

Prepárese para implementar OAuth 2,0 con ONTAP

Antes de configurar OAuth 2,0 en un entorno ONTAP, debe prepararse para el despliegue. A continuación se incluye un resumen de las principales tareas y decisiones. La disposición de las secciones generalmente está alineada con el orden que debe seguir. Sin embargo, si bien es aplicable a la mayoría de las implementaciones, debe adaptarlo a su entorno según sea necesario. También debe considerar la creación de un plan de despliegue formal.

En función del entorno, puede seleccionar la configuración de los servidores de autorización definidos en ONTAP. Esto incluye los valores de parámetros que necesita especificar para cada tipo de despliegue. Consulte "Escenarios de despliegue de OAuth 2,0" para obtener más información.

Recursos protegidos y aplicaciones cliente

OAuth 2,0 es un marco de autorización para controlar el acceso a los recursos protegidos. Dado esto, un primer paso importante en cualquier implementación es determinar cuáles son los recursos disponibles y qué clientes necesitan acceder a ellos.

Identificar aplicaciones cliente

Debe decidir qué clientes utilizarán OAuth 2,0 al emitir llamadas a la API REST y a qué puntos finales API necesitan acceso.

Revisar los roles DE REST DE ONTAP y los usuarios locales existentes

Debe revisar las definiciones de identidad ONTAP existentes, incluidos los roles REST y los usuarios locales. Dependiendo de cómo configure OAuth 2,0, estas definiciones se pueden utilizar para tomar decisiones de acceso.

Transición global a OAuth 2,0

Aunque puede implementar la autorización OAuth 2,0 gradualmente, también puede mover todos los clientes de la API REST a OAuth 2,0 inmediatamente estableciendo un indicador global para cada servidor de autorización. Esto permite tomar decisiones de acceso según la configuración de ONTAP existente sin necesidad de crear ámbitos independientes.

Servidores de autorización

Los servidores de autorización desempeñan un papel importante en su implementación de OAuth 2,0 mediante la emisión de tokens de acceso y la aplicación de la política administrativa.

Seleccione e instale el servidor de autorización

Debe seleccionar e instalar uno o más servidores de autorización. Es importante familiarizarse con las opciones de configuración y los procedimientos de sus proveedores de identidad, incluido cómo definir ámbitos. Tenga en cuenta que algunos servidores de autorización, incluido Microsoft Entra ID, representan grupos que utilizan UID en lugar de nombres.

Determine si es necesario instalar el certificado de CA raíz de autorización

ONTAP utiliza el certificado del servidor de autorización para validar los tokens de acceso firmados presentados por los clientes. Para hacerlo, ONTAP necesita el certificado de CA raíz y todos los certificados intermedios. Estos pueden preinstalarse con ONTAP. Si no es así, debe instalarlos.

Evalúe la ubicación y la configuración de la red

Si el servidor de autorización está detrás de un firewall, ONTAP debe configurarse para utilizar un servidor proxy.

Autenticación y autorización de clientes

Hay varios aspectos de la autenticación y autorización del cliente que debe considerar.

Ámbitos autónomos o definiciones de identidad locales de ONTAP

En un nivel superior, puede definir ámbitos independientes definidos en el servidor de autorización o basarse en las definiciones de identidad de ONTAP local existentes, incluidos los roles y los usuarios.

Opciones con procesamiento ONTAP local

Si utiliza las definiciones de identidad de ONTAP, debe decidir cuáles aplicar, entre ellas:

- Rol REST con nombre

- Coincide con los usuarios locales
- Grupos de Active Directory o LDAP

Validación local o introspección remota

Debe decidir si los tokens de acceso serán validados localmente por ONTAP o en el servidor de autorización mediante introspección. También hay varios valores relacionados que se deben tener en cuenta, como el intervalo de refrescamiento.

Tokens de acceso restringidos por el remitente

Para entornos que requieren un alto nivel de seguridad, puede utilizar tokens de acceso con restricciones de envío basados en MTLS. Esto requiere un certificado para cada cliente.

Agrupa como UUID y asignación de identidad

Si está utilizando un servidor de autorización que representa grupos que utilizan UUID, debe planificar cómo asignarlos a nombres de grupo y, posiblemente, a roles asociados.

Interfaz administrativa

Puede realizar la administración de OAuth 2,0 a través de cualquiera de las interfaces ONTAP, incluyendo:

- Interfaz de línea de comandos
- System Manager
- API REST

Cómo solicitan los clientes tokens de acceso

Las aplicaciones cliente deben solicitar tokens de acceso directamente desde el servidor de autorización. Debe decidir cómo se hará esto, incluido el tipo de subvención.

Configurar ONTAP

Debe realizar varias tareas de configuración de ONTAP.

Defina los roles REST y los usuarios locales

En función de la configuración de autorización, se puede utilizar el procesamiento de identificación de ONTAP local. En este caso, debe revisar y definir los roles REST y las definiciones de usuario. Y dependiendo del servidor de autorización, esto también puede incluir la administración de grupos basados en valores UUID.

Configuración central

Hay tres pasos principales necesarios para llevar a cabo la configuración principal de ONTAP, incluyendo los siguientes:

- Opcionalmente, instale el certificado raíz (y cualquier certificado intermedio) para la CA que firmó el certificado del servidor de autorización.
- Defina el servidor de autorización.
- Habilite el procesamiento de OAuth 2,0 para el clúster.

Desplegar OAuth 2,0 en ONTAP

La implementación de la funcionalidad principal de OAuth 2,0 implica tres pasos principales.

Antes de empezar

Debe prepararse para el despliegue de OAuth 2,0 antes de configurar ONTAP. Por ejemplo, debe evaluar el servidor de autorización, incluido cómo se firmó su certificado y si está detrás de un firewall. Consulte "Prepárese para implementar OAuth 2,0 con ONTAP" para obtener más información.

Paso 1: Instale los certificados de CA raíz del servidor de autorización

ONTAP incluye un gran número de certificados de CA raíz preinstalados. Por lo tanto, en muchos casos, el certificado para su servidor de autorización será reconocido inmediatamente por ONTAP sin configuración adicional. Pero dependiendo de cómo se haya firmado el certificado del servidor de autorización, es posible que necesite instalar un certificado de CA raíz y cualquier certificado intermedio.

Siga las instrucciones proporcionadas a continuación para instalar el certificado si es necesario. Debe instalar todos los certificados necesarios en el nivel de clúster.

Elija el procedimiento correcto en función de cómo acceda a ONTAP.

Ejemplo 1. Pasos

System Manager

1. En System Manager, selecciona **Clúster** > **Configuración**.
2. Desplácese hacia abajo hasta la sección **Seguridad**.
3. Haga clic en → junto a **Certificados**.
4. En la pestaña **Autoridades de certificación de confianza**, haga clic en **Agregar**.
5. Haga clic en **Importar** y seleccione el archivo de certificado.
6. Complete los parámetros de configuración del entorno.
7. Haga clic en **Agregar**.

CLI

1. Comience la instalación:

   ```
   security certificate install -type server-ca
   ```

2. Busque el siguiente mensaje de la consola:

   ```
   Please enter Certificate: Press <Enter> when done
   ```

3. Abra el archivo de certificado con un editor de texto.
4. Copie todo el certificado, incluidas las siguientes líneas:

   ```
   -----BEGIN CERTIFICATE-----
   <certificate_value>
   -----END CERTIFICATE-----
   ```

5. Pegue el certificado en el terminal después del símbolo del sistema.
6. Presione **Enter** para completar la instalación.
7. Confirme la instalación del certificado mediante uno de los siguientes métodos:

   ```
   security certificate show-user-installed
   ```

   ```
   security certificate show
   ```

Paso 2: Configure el servidor de autorización

Debe definir al menos un servidor de autorización para ONTAP. Debe elegir los valores de los parámetros en función de su plan de configuración e implementación. Revise "Situaciones de puesta en marcha de OAuth2" para determinar los parámetros exactos necesarios para su configuración.

Para modificar una definición de servidor de autorización, puede suprimir la definición existente y crear una nueva.

El ejemplo que se proporciona a continuación se basa en el primer escenario de despliegue sencillo en

"Validación local". Los ámbitos autónomos se utilizan sin un proxy.

Elija el procedimiento correcto en función de cómo acceda a ONTAP. El procedimiento de la CLI utiliza variables simbólicas que hay que reemplazar antes de emitir el comando.

Ejemplo 2. Pasos

System Manager

1. En System Manager, selecciona **Clúster** > **Configuración**.
2. Desplácese hacia abajo hasta la sección **Seguridad**.
3. Haga clic en **+** junto a **Autorización OAuth 2,0**.
4. Selecciona **Más opciones**.
5. Proporcione los valores necesarios para el despliegue, como:
   - Nombre
   - Aplicación (http)
   - URI de JWKS de Proveedor
   - URI del emisor
6. Haga clic en **Agregar**.

CLI

1. Vuelva a crear la definición:

   ```
   security oauth2 client create -config-name <NAME> -provider-jwks-uri
   <URI_JWKS> -application http -issuer <URI_ISSUER>
   ```

   Por ejemplo:

   ```
   security oauth2 client create \
   -config-name auth0 \
   -provider-jwks-uri https://superzap.dev.netapp.com:8443/realms/my-
   realm/protocol/openid-connect/certs \
   -application http \
   -issuer https://superzap.dev.netapp.com:8443/realms/my-realm
   ```

   Obtenga más información sobre `security oauth2 client create` en el "Referencia de comandos del ONTAP".

Paso 3: Habilite OAuth 2,0

El paso final es habilitar OAuth 2,0. Se trata de una configuración global para el clúster de ONTAP.

> No habilite el procesamiento de OAuth 2,0 hasta que confirme que ONTAP, los servidores de autorización y los servicios de soporte se han configurado correctamente.

Elija el procedimiento correcto en función de cómo acceda a ONTAP.

Ejemplo 3. Pasos

System Manager

1. En System Manager, selecciona **Clúster** > **Configuración**.
2. Desplácese hacia abajo hasta la sección **Seguridad**.
3. Haga clic en → junto a **OAuth 2,0 AUTORIZATION**.
4. Habilita **OAuth 2,0 autorización**.

CLI

1. Activar OAuth 2,0:

   ```
   security oauth2 modify -enabled true
   ```

2. Confirme que OAuth 2,0 está activado:

   ```
   security oauth2 show
   Is OAuth 2.0 Enabled: true
   ```

Información relacionada

- "instalación del certificado de seguridad"
- "Mostrar certificado de seguridad"
- "modificar seguridad oauth2"
- "seguridad oauth2 mostrar"

Emitir una llamada a la API REST de ONTAP mediante OAuth 2.0

La implementación de OAuth 2,0 en ONTAP es compatible con las aplicaciones del cliente API de REST. Puede emitir una llamada a la API de REST simple usando cURL para comenzar a usar OAuth 2,0. El ejemplo que se presenta a continuación recupera la versión del cluster de ONTAP.

Antes de empezar

Tiene que configurar y habilitar la función OAuth 2,0 para el clúster de ONTAP. Esto incluye la definición de un servidor de autorización.

Paso 1: Adquiera un token de acceso

Debe adquirir un token de acceso para utilizarlo con la llamada de la API de REST. La solicitud de token se realiza fuera de ONTAP y el procedimiento exacto depende del servidor de autorización y de su configuración. Puede solicitar el token a través de un navegador web, con un comando curl o utilizando un lenguaje de programación.

Para fines ilustrativos, a continuación se presenta un ejemplo de cómo se puede solicitar un token de acceso desde Keycloak usando curl.

Ejemplo de Keycloak

```
curl --request POST \
--location
'https://superzap.dev.netapp.com:8443/realms/peterson/protocol/openid-
connect/token' \
--header 'Content-Type: application/x-www-form-urlencoded' \
--data-urlencode 'client_id=dp-client-1' \
--data-urlencode 'grant_type=client_credentials' \
--data-urlencode 'client_secret=5iTUf9QKLGxAoYa1iR33vlD5A2xq09V7'
```

Debe copiar y guardar el token devuelto.

Paso 2: Emita la llamada a la API de REST

Una vez que tenga un token de acceso válido, puede usar un comando cURL con el token de acceso para emitir una llamada a la API de REST.

Parámetros y variables

Las dos variables del ejemplo de curl se describen en la tabla siguiente.

Variable	Descripción
$FQDN_IP	El nombre de dominio completo o la dirección IP de la LIF de gestión de ONTAP.
$ACCESS_TOKEN	El token de acceso OAuth 2,0 emitido por el servidor de autorización.

Primero debe definir estas variables en el entorno de shell de Bash antes de emitir el ejemplo de cURL. Por ejemplo, en la CLI de Linux escriba el siguiente comando para establecer y mostrar la variable FQDN:

```
FQDN_IP=172.14.31.224
echo $FQDN_IP
172.14.31.224
```

Después de definir ambas variables en el shell Bash local, puede copiar el comando cURL y pegarlo en la CLI. Presione **Enter** para sustituir las variables y emitir el comando.

Ejemplo de curl

```
curl --request GET \
--location "https://$FQDN_IP/api/cluster?fields=version" \
--include \
--header "Accept: */*" \
--header "Authorization: Bearer $ACCESS_TOKEN"
```

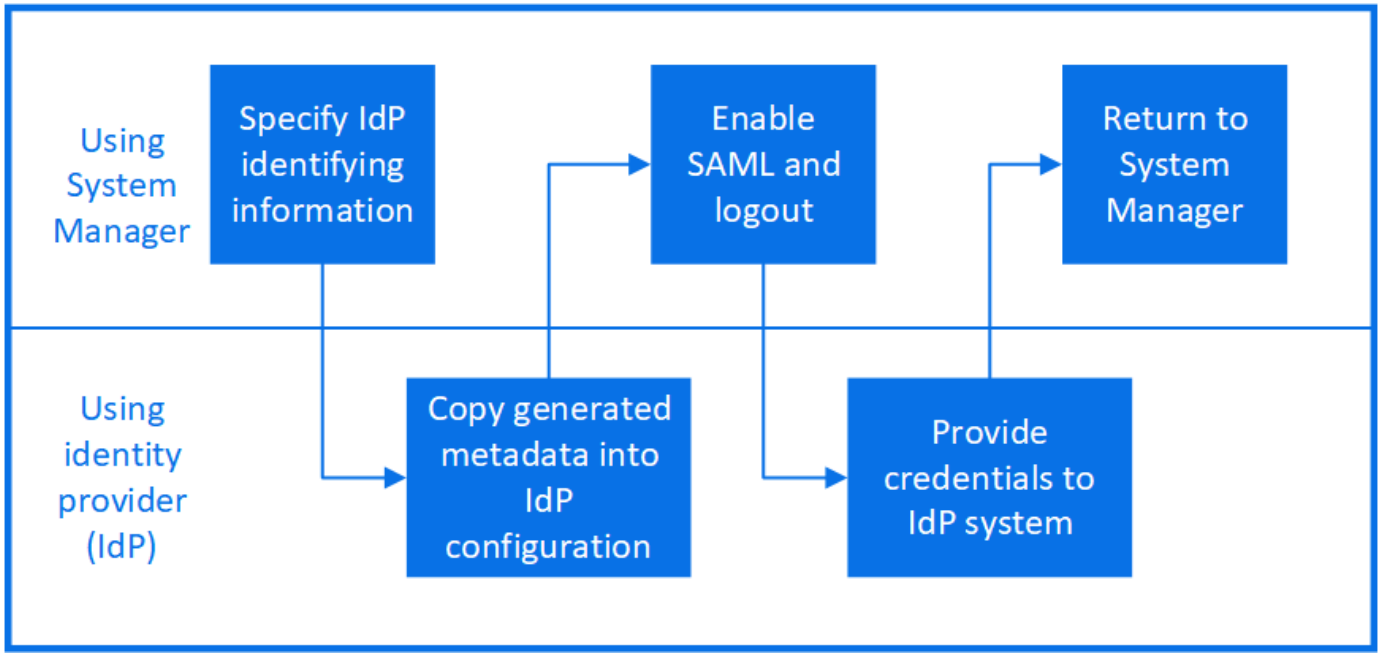
Configurar la autenticación SAML para usuarios remotos de ONTAP

A partir de ONTAP 9.3, puede configurar la autenticación SAML (Lenguaje de Marcado para Aserciones de Seguridad) para servicios web. Cuando la autenticación SAML está configurada y habilitada, los usuarios se autentican mediante un proveedor de identidad (IdP) externo en lugar de proveedores de servicios de directorio como Active Directory y LDAP. Cuando la autenticación SAML está deshabilitada, se utilizan los proveedores de servicios de directorio configurados, como Active Directory y LDAP, para la autenticación.

Habilite la autenticación SAML

Para habilitar la autenticación SAML con System Manager o con la CLI, realice los siguientes pasos. Si el clúster ejecuta ONTAP 9,7 o una versión anterior, los pasos que debe seguir son diferentes. Consulte la ayuda en línea de System Manager disponible en su sistema.

> Tras habilitar la autenticación SAML, solo los usuarios remotos configurados para la autenticación SAML podrán acceder a la GUI del Administrador del Sistema. Los usuarios locales no podrán acceder a la GUI del Administrador del Sistema una vez habilitada la autenticación SAML.



Acerca de esta tarea

- La autenticación SAML se aplica únicamente a ONTAP `http` y `ontapi` aplicaciones.

  El `http` y `ontapi` Las aplicaciones son utilizadas por los siguientes servicios web: Infraestructura del procesador de servicios, API de ONTAP y Administrador del sistema.

- La autenticación SAML solo se aplica para acceder a la SVM de administrador.
- A partir de ONTAP 9.17.1, la información de grupo proporcionada por el IdP se puede asignar a roles de ONTAP . Esto permite asignar roles a los usuarios según los grupos definidos en el IdP. Para obtener más información, consulte "Trabajar con grupos IdP de OAuth 2.0 o SAML en ONTAP" .

Los siguientes IDP se han validado con System Manager:

- ID de Microsoft Entra (validado con ONTAP 9.17.1 y versiones posteriores)
- Servicios de federación de Active Directory
- Cisco Duo (validado con las siguientes versiones de ONTAP :)
  - 9.7P21 y versiones posteriores de 9,7 (consulte la "Documentación de System Manager Classic")
  - Versiones del parche 9.8P17 y posteriores
  - Versiones del parche 9.9.1P13 y posteriores
  - Versiones del parche 9.10.1P9 y posteriores 9.10.1
  - Versiones del parche 9.11.1P4 y posteriores
  - 9.12.1 y versiones posteriores
- Shibboleth

Antes de empezar

- El IdP que planea utilizar para la autenticación remota debe ser configurado. Debe tener la URI del IdP. La URI del IdP es la dirección web a la que ONTAP envía las solicitudes de autenticación y de la que recibe las respuestas
- El puerto 443 debe estar abierto entre el clúster ONTAP y el IdP.
- El clúster de ONTAP y el IdP deben poder hacer ping al nombre de dominio completo del otro. Asegúrese de que el DNS esté configurado correctamente y que el certificado del clúster no esté caducado.
- Si es necesario, agregue la autoridad de certificación (CA) de confianza del IdP a ONTAP. Puede "Administrar certificados ONTAP con el Administrador del sistema" Es posible que necesite configurar el certificado del clúster ONTAP en el IdP.
- Debe poder acceder al clúster ONTAP "Procesador de servicios (SP)" consola. Si SAML está mal configurado, deberá deshabilitarlo desde la consola del SP .
- Si utiliza Entra ID (validado a partir de ONTAP 9.17.1), debe configurarlo con los metadatos de ONTAP antes de crear la configuración SAML de ONTAP . Entra ID no proporcionará la URI del IdP hasta que se configure con los metadatos de ONTAP . La URI del IdP es necesaria para crear la configuración SAML de ONTAP .
  - Si utiliza el Administrador del sistema para configurar SAML, deje el campo URI del IdP en blanco hasta que el Administrador del sistema proporcione los metadatos de ONTAP . Configure el ID de Entra con los metadatos de ONTAP y, a continuación, copie el URI del IdP en el Administrador del sistema antes de habilitar la configuración de SAML.
  - Si utiliza la CLI de ONTAP para configurar SAML, debe generar los metadatos de ONTAP antes de habilitar la configuración de SAML de ONTAP . Puede generar el archivo de metadatos de ONTAP con el siguiente comando:

    ```
    security saml-sp default-metadata create -sp-host <ontap_host_name>
    ```

    `ontap_host_name` Es el nombre de host o la dirección IP del host del proveedor de servicios SAML, que en este caso es el sistema ONTAP . De forma predeterminada, se utiliza la dirección IP de administración del clúster. Opcionalmente, puede proporcionar la información del certificado del servidor ONTAP . De forma predeterminada, se utiliza la información del certificado del servidor web ONTAP .

Configure Entra ID con los metadatos proporcionados. Debe configurar Entra ID antes de crear la configuración SAML de ONTAP . Una vez configurado Entra, siga el siguiente procedimiento de la CLI.

- No se pueden generar los metadatos de ONTAP para Entra ID hasta que todos los nodos del clúster tengan la versión 9.17.1.

Pasos

Siga estos pasos en función de su entorno:

System Manager

1. Haga clic en **clúster > Configuración**.
2. Junto a **Autenticación SAML**, haga clic en .
3. Asegúrese de que haya una Marca en la casilla de verificación **Habilitar autenticación SAML**.
4. Introduzca la URL del URI del IdP (incluido "https://"). Si está utilizando Entra ID, omita este paso.
5. Modifique la dirección del sistema host, si es necesario. Esta es la dirección a la que el IdP dirigirá tras la autenticación. La dirección IP predeterminada es la de administración del clúster.
6. Asegúrese de utilizar el certificado correcto:
   - Si su sistema sólo se ha asignado con un certificado con el tipo "servidor", ese certificado se considera el predeterminado y no se muestra.
   - Si su sistema estaba asignado con varios certificados como tipo "servidor", se muestra uno de los certificados. Para seleccionar un certificado diferente, haga clic en **Cambiar**.
7. Haga clic en **Guardar**. Una ventana de confirmación muestra la información de metadatos, que se ha copiado automáticamente en el portapapeles.
8. Vaya al sistema IdP que especificó y copie los metadatos del portapapeles para actualizarlos. Si usa Entra ID, copie la URI del IdP en ONTAP después de configurar Entra ID con los metadatos del sistema.
9. Vuelva a la ventana de confirmación (en System Manager) y marque la casilla de verificación **he configurado el IDP con el URI de host o metadatos**.
10. Haga clic en **Cerrar sesión** para activar la autenticación basada en SAML. El sistema IDP mostrará una pantalla de autenticación.
11. En la página de inicio de sesión del IdP, introduzca sus credenciales basadas en SAML. Una vez verificadas, accederá a la página principal de System Manager.

CLI

1. Cree una configuración de SAML para que ONTAP pueda acceder a los metadatos de IDP:

   ```
   security saml-sp create -idp-uri <idp_uri> -sp-host <ontap_host_name>
   ```

   `idp_uri` Es la dirección FTP o HTTP del host de IdP desde el que se pueden descargar los metadatos de IdP.

   > Algunas URL incluyen el signo de interrogación (?). Este signo activa la ayuda activa de la línea de comandos de ONTAP . Para introducir una URL con un signo de interrogación, primero debe desactivar la ayuda activa con el comando. `set -active -help false` La ayuda activa se puede volver a habilitar posteriormente con el comando `set -active-help true` . Obtenga más información en el "Referencia de comandos del ONTAP" .

   `ontap_host_name` Es el nombre de host o la dirección IP del host del proveedor de servicios SAML que, en este caso, es el sistema ONTAP. De manera predeterminada, se utiliza la dirección IP de la LIF de administración del clúster.

   Opcionalmente, puede proporcionar la información de certificado del servidor ONTAP. De manera predeterminada, se utiliza la información de certificado de servidor web ONTAP.

```
cluster_12::> security saml-sp create -idp-uri
https://example.url.net/idp/shibboleth

Warning: This restarts the web server. Any HTTP/S connections that
are active
         will be disrupted.
Do you want to continue? {y|n}: y
[Job 179] Job succeeded: Access the SAML SP metadata using the URL:
https://10.0.0.1/saml-sp/Metadata

Configure the IdP and ONTAP users for the same directory server
domain to ensure that users are the same for different
authentication methods. See the "security login show" command for
the ONTAP user configuration.
```

Se muestra la URL para acceder a los metadatos del host ONTAP.

2. Desde el host IdP, configurar el IdP Con los metadatos del host de ONTAP . Si usa Entra ID, ya ha completado este paso.
3. Una vez configurado el IdP, habilite la configuración de SAML:

   `security saml-sp modify -is-enabled true`

   Cualquier usuario existente que acceda a la `http` `ontapi` aplicación o se configura automáticamente para la autenticación SAML.

4. Si desea crear usuarios para el `http` o `ontapi` Una vez configurada la aplicación SAML, especifique SAML como método de autenticación para los nuevos usuarios. Antes de ONTAP 9.17.1, se creaba automáticamente un inicio de sesión SAML para los usuarios existentes. `http` o `ontapi` usuarios cuando SAML está habilitado. Los nuevos usuarios deben configurarse para SAML. A partir de ONTAP 9.17.1, todos los usuarios creados con `password` , `domain` , o `nsswitch` Los métodos de autenticación se autentican automáticamente contra el IdP cuando SAML está habilitado.

   a. Cree un método de inicio de sesión para nuevos usuarios con autenticación SAML . `user_name` debe coincidir con el nombre de usuario configurado en el IdP:

      > El `user_name` valor distingue mayúsculas de minúsculas. A menos que estés usando Entra ID, incluye solo el nombre de usuario y no incluyas ninguna parte del dominio. Si estás usando Entra ID, puedes crear el nombre de usuario con el dominio, por ejemplo *user_name@domain.com*.

      `security login create -user-or-group-name <user_name> -application [http | ontapi] -authentication-method saml -vserver <svm_name>`

      Ejemplo:

```
cluster_12::> security login create -user-or-group-name admin1
-application http -authentication-method saml -vserver cluster_12
```

b. Compruebe que se ha creado la entrada de usuario:

`security login show`

Ejemplo:

```
cluster_12::> security login show

Vserver: cluster_12

Second
User/Group                 Authentication                 Acct
Authentication
Name           Application Method        Role Name        Locked
Method
-------------- ----------- ------------- ---------------- ------
--------------
admin          console     password      admin            no
none
admin          http        password      admin            no
none
admin          http        saml          admin            -
none
admin          ontapi      password      admin            no
none
admin          ontapi      saml          admin            -
none
admin          service-processor
                           password      admin            no
none
admin          ssh         password      admin            no
none
admin1         http        password      backup           no
none
admin1         http        saml          backup           -
none
```

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

Deshabilitar la autenticación SAML

Puede deshabilitar la autenticación SAML si desea dejar de autenticar usuarios remotos de System Manager con un proveedor de identidad (IdP) externo. Cuando la autenticación SAML está deshabilitada, se utiliza la autenticación de usuarios locales o los proveedores de servicios de directorio configurados, como Active Directory y LDAP, para autenticar a los usuarios.

Siga estos pasos en función de su entorno:

Ejemplo 4. Pasos

System Manager

1. Haga clic en **clúster > Configuración**.
2. En **autenticación SAML**, haga clic en el botón de alternar **Activado**.
3. *Opcional*: También puede hacer clic junto a **Autenticación SAML**, y luego desmarcar la casilla de verificación **Habilitar Autenticación SAML**.

CLI

1. Deshabilitar la autenticación SAML:

   ```
   security saml-sp modify -is-enabled false
   ```

2. Si ya no desea usar autenticación SAML o si desea modificar el IDP, elimine la configuración de SAML:

   ```
   security saml-sp delete
   ```

Configurar IdP de terceros

Acerca de esta tarea

Para autenticarse con ONTAP, es posible que deba cambiar la configuración de su proveedor de identidad (IdP). Las siguientes secciones proporcionan información de configuración para los IdP compatibles.

ID Entra

Al configurar Entra ID, cree una nueva aplicación y configure el inicio de sesión SAML con los metadatos proporcionados por ONTAP. Una vez creada la aplicación, edite la sección "Atributos y notificaciones" de la configuración SAML de la aplicación para que coincida con lo siguiente:

Ajuste	Valor
Nombre	urna:oid:0.9.2342.19200300.100.1.1
Espacio de nombres	*Dejar en blanco*
Formato de nombre	URI
Origen	Atributo
Atributo de origen	usuario.nombreprincipaldelusuario

Si desea utilizar grupos con Entra ID, agregue un reclamo de grupo con la siguiente configuración:

Ajuste	Valor
Nombre	urna:oid:1.3.6.1.4.1.5923.1.5.1.1
Espacio de nombres	*Dejar en blanco*
Atributo de origen	ID de grupo

Entra ID proporciona información de grupo en formato UUID. Para obtener más información sobre el uso de grupos con Entra ID, consulte "Gestionar grupos con UUID" .

La *URL de metadatos de federación de la aplicación* proporcionada en la sección "Certificado SAML" de la configuración SAML de la aplicación es la URI del IdP que ingresará en ONTAP.

Para obtener información sobre cómo configurar la autenticación multifactor de Entra ID, consulte "Planificar una implementación de autenticación multifactor de Microsoft Entra" .

Para obtener más información, consulte la "Documentación de identificación de entrada" .

Servicios de federación de Active Directory

Al configurar los Servicios de Federación de Active Directory (AD FS), debe agregar una nueva confianza de usuario autenticado que admita notificaciones con los metadatos del proveedor de servicios proporcionados por ONTAP. Una vez creada la confianza de usuario autenticado, agregue las siguientes reglas de notificación a su Política de Emisión de Notificaciones mediante la plantilla "Enviar Atributos LDAP como Notificaciones":

Tienda de atributos	Atributo LDAP	Tipo de reclamación saliente
Active Directory	Nombre de la cuenta SAM	Identificación del nombre
Active Directory	Nombre de la cuenta SAM	urna:oid:0.9.2342.19200300.100.1.1
Active Directory	Formato del nombre	urna:oasis:nombres:tc:SAML:2.0:attrname-format:uri
Active Directory	Grupos de tokens: calificados por nombre de dominio	urna:oid:1.3.6.1.4.1.5923.1.5.1.1

Tienda de atributos	Atributo LDAP	Tipo de reclamación saliente
Active Directory	nombreDeCuentaSAMA	urna:oid:1.2.840.113556.1.4.221

AD FS proporciona información de grupo en formato de nombre. Para obtener más información sobre el uso de grupos con AD FS, consulte "Gestionar grupos con nombres" .

Para obtener más información, consulte la "Documentación de AD FS" .

Cisco Duo

Consulte la "Documentación de Cisco Duo" para obtener información de configuración.

Shibboleth

Antes de configurar el IdP de Shibboleth, debe haber configurado un servidor LDAP.

Al habilitar SAML en ONTAP, guarde el XML de metadatos del host proporcionado. En el host donde esté instalado Shibboleth, reemplace el contenido de `metadata/sp-metadata.xml` con los metadatos del host XML dentro del directorio de inicio de Shibboleth IdP.

Para obtener más información, consulte "Shibboleth" .

Solucione problemas de la configuración de SAML

Si se produce un error al configurar la autenticación del lenguaje de marcado de aserción de seguridad (SAML), puede reparar manualmente cada nodo en el que falló la configuración de SAML y recuperarse del error. Durante el proceso de reparación, se reinicia el servidor web y se interrumpen todas las conexiones HTTP o HTTPS activas.

Acerca de esta tarea

Cuando se configura la autenticación SAML, ONTAP aplica la configuración de SAML por nodo. Cuando habilita la autenticación SAML, ONTAP intenta reparar automáticamente cada nodo si existen problemas de configuración. Si hay problemas con la configuración de SAML en cualquier nodo, puede deshabilitar la autenticación SAML y luego volver a habilitar la autenticación SAML. Puede haber situaciones en las que la configuración de SAML no pueda aplicarse en uno o varios nodos incluso después de volver a habilitar la autenticación SAML. Puede identificar el nodo en el que falló la configuración de SAML y reparar manualmente ese nodo.

Pasos

1. Inicie sesión en el nivel de privilegio avanzado:

   ```
   set -privilege advanced
   ```

2. Identifique el nodo en el que no pudo realizarse la configuración de SAML:

   ```
   security saml-sp status show -instance
   ```

   Ejemplo:

```
cluster_12::*> security saml-sp status show -instance

                          Node: node1
                Update Status: config-success
               Database Epoch: 9
   Database Transaction Count: 997
                   Error Text:
SAML Service Provider Enabled: false
        ID of SAML Config Job: 179

                          Node: node2
                Update Status: config-failed
               Database Epoch: 9
   Database Transaction Count: 997
                   Error Text: SAML job failed, Reason: Internal error.
Failed to receive the SAML IDP Metadata file.
SAML Service Provider Enabled: false
        ID of SAML Config Job: 180
2 entries were displayed.
```

Obtenga más información sobre `security saml-sp status show` en el "Referencia de comandos del ONTAP".

3. Repare la configuración de SAML en el nodo con errores:

   `security saml-sp repair -node <node_name>`

   Ejemplo:

```
cluster_12::*> security saml-sp repair -node node2

Warning: This restarts the web server. Any HTTP/S connections that are
active
         will be disrupted.
Do you want to continue? {y|n}: y
[Job 181] Job is running.
[Job 181] Job success.
```

   Se reinicia el servidor web y se interrumpen las conexiones HTTP o HTTPS activas.

   Obtenga más información sobre `security saml-sp repair` en el "Referencia de comandos del ONTAP".

4. Compruebe que SAML se haya configurado correctamente en todos los nodos:

   `security saml-sp status show -instance`

Ejemplo:

```
cluster_12::*> security saml-sp status show -instance

                          Node: node1
                 Update Status: config-success
                Database Epoch: 9
    Database Transaction Count: 997
                    Error Text:
SAML Service Provider Enabled: false
         ID of SAML Config Job: 179

                          Node: node2
                 Update Status: config-success
                Database Epoch: 9
    Database Transaction Count: 997
                    Error Text:
SAML Service Provider Enabled: false
         ID of SAML Config Job: 180
2 entries were displayed.
```

Obtenga más información sobre `security saml-sp status show` en el "Referencia de comandos del ONTAP".

Información relacionada

- "Referencia de comandos del ONTAP"
- "saml-SP de seguridad"
- "seguridad de inicio de sesión creado"

Trabajar con grupos IdP de OAuth 2.0 o SAML en ONTAP

ONTAP ofrece varias opciones para configurar grupos según su servidor de autorización OAuth 2.0 o proveedor de identidad (IdP) SAML. Los grupos se pueden asignar a roles que ONTAP utiliza para determinar el acceso.

A partir de ONTAP 9.17.1, la información de grupo proporcionada por el IdP de SAML se puede asignar a roles de ONTAP . Esto permite asignar roles a los usuarios según los grupos definidos en el IdP. Para más información, consulte "Configurar la autenticación SAML". A partir de ONTAP 9.14.1, ONTAP admite la autenticación por nombre de grupo para OAuth 2.0. partir de ONTAP 9.16.1, ONTAP admite la autenticación por UUID de grupo y la asignación de roles de OAuth 2.0. Para obtener más información, consulte "Descripción general de la implementación de ONTAP OAuth 2,0" .

Cómo se identifican los grupos

Al configurar un grupo en un servidor de autorización o un proveedor de identidades SAML, este se identifica y se incluye en un token de acceso OAuth 2.0 o una aserción SAML mediante un nombre o UUID. Debe saber

cómo su servidor de autorización o proveedor de identidades SAML gestiona los grupos antes de configurar ONTAP.

> Si se incluyen varios grupos en un token de acceso, ONTAP intentará utilizar cada uno hasta que haya una coincidencia.

Nombres de grupo

Muchos servidores de autorización e IdP SAML, como el Servicio de Federación de Active Directory (ADFS), identifican y representan grupos mediante un nombre. Aquí se muestra un fragmento de un token de acceso JSON OAuth 2.0 generado por ADFS que contiene varios grupos. Consulte Gestionar grupos con nombres Para más información.

```
...
"sub": "User1_TestDev@NICAD5.COM",
"group": [
  "NICAD5\\Domain Users",
  "NICAD5\\Development Group",
  "NICAD5\\Production Group"
],
"apptype": "Confidential",
"appid": "3bff3b2b-8e40-44ba-7c11-d73c3b76e3e8",
...
```

UUID de grupo

Algunos servidores de autorización e IdP SAML, como Microsoft Entra ID, identifican y representan grupos mediante un UUID. Aquí se muestra un fragmento de un token de acceso OAuth 2.0 generado por Entra ID que contiene varios grupos. Consulte Gestionar grupos con UUID Para más información.

```
...
"appid": "4aff4b4b-8e40-44ba-7c11-d73c3b76e3d7",
"appidacr": "1",
"groups": [
  "8ea4c5b0-bcad-4e66-8f1e-cd395474a448",
  "a8558fc2-a1b2-4cb7-cc41-59bd831840cc"],
"name": "admin007 with group membership",
...
```

Gestionar grupos con nombres

Si su servidor de autorización o proveedor de identidades SAML utiliza nombres para identificar grupos, debe asegurarse de que cada grupo esté definido para su clúster de ONTAP . Dependiendo de su entorno de seguridad, es posible que ya tenga el grupo definido.

Aquí hay un ejemplo de comando CLI que define un grupo de ONTAP . Observe que utiliza un grupo con nombre del token de acceso de ejemplo. Debe tener privilegios de administrador de ONTAP para ejecutar el

comando.

Ejemplo

```
security login create -user-or-group-name "NICAD5\\Domain Users"
-application http -authentication-method domain -role admin
```

Usar `-authentication-method domain` o `nsswitch` para grupos de servidores de autorización SAML IdP y OAuth 2.0.

También puede configurar esta función mediante la API REST de ONTAP . Obtenga más información en "Documentación de automatización de ONTAP" .

Gestionar grupos con UUID

Si su servidor de autorización o proveedor de identidades SAML representa grupos mediante valores UUID, debe realizar una configuración de dos pasos antes de usar un grupo. A partir de ONTAP 9.16.1, hay dos funciones de mapeo disponibles, probadas con Entra ID. Entra ID para OAuth 2.0 es compatible a partir de ONTAP 9.16.1, y Entra ID para SAML es compatible a partir de ONTAP 9.17.1. Debe tener privilegios de administrador de ONTAP para ejecutar los comandos de la CLI.

También es posible configurar estas funciones mediante la API de REST DE ONTAP. Obtenga más información en el "Documentación de automatización de ONTAP".

Asignar un UUID de grupo a un nombre de grupo

Si utiliza un servidor de autorización o un proveedor de identidades SAML que representa grupos mediante valores UUID, debe asignar los UUID de grupo a los nombres de grupo. Las principales operaciones de la CLI de ONTAP se describen a continuación.

Crear

Puede definir una nueva configuración de mapeo de grupo con el `security login group create` Comando. El UUID y el nombre del grupo deben coincidir con la configuración del servidor de autorización o del proveedor de identidades SAML. Más información sobre `security login group create` en el "Referencia de comandos del ONTAP" .

Parámetros

A continuación se describen los parámetros utilizados para crear una asignación de grupo.

Parámetro	Descripción
`vserver`	De manera opcional especifica el nombre de la SVM (Vserver) a la que está asociado el grupo. Si se omite, el grupo está asociado con el clúster de ONTAP.
`name`	Nombre único del grupo que utilizará ONTAP.
`type`	Este valor indica el proveedor de identidad del que se origina el grupo.
`uuid`	Especifica el identificador único universal del grupo proporcionado por el servidor de autorización o el IdP SAML.

A continuación, se muestra un ejemplo de comando CLI que define un grupo para ONTAP. Observe que utiliza un grupo UUID del token de acceso de ejemplo.

Ejemplo

```
security login group create -vserver ontap-cls-1 -name IAM_Dev -type entra
-uuid 8ea4c5b0-bcad-4e66-8f1e-cd395474a448
```

Después de crear el grupo, se genera un identificador entero único de solo lectura para el grupo.

Operaciones de CLI adicionales

El comando admite varias operaciones adicionales, entre las que se incluyen:

- Mostrar
- Modificar
- Eliminar

Puede utilizar `show` la opción para recuperar el ID de grupo único generado para un grupo. Obtenga más información sobre `show` en el "Referencia de comandos del ONTAP".

Asignar un UUID de grupo a un rol

Si utiliza un servidor de autorización o un proveedor de identidades SAML que representa grupos mediante valores UUID, puede asignar el grupo a un rol. Para obtener más información sobre el control de acceso basado en funciones en ONTAP, consulte "Obtenga más información sobre la gestión de roles de control de acceso de ONTAP". Las operaciones principales de la CLI de ONTAP se describen a continuación. tener privilegios de administrador de ONTAP para ejecutar los comandos.

Primero necesitas Asignar un UUID de grupo a un nombre de grupo y recuperar el ID entero único generado para el grupo. Necesitará el ID para asignar el grupo a un rol.

Crear

Puede definir una nueva asignación de roles con el `security login group role-mapping create` comando. Obtenga más información sobre `security login group role-mapping create` en el "Referencia de comandos del ONTAP" .

Parámetros

A continuación se describen los parámetros utilizados para asignar un grupo a un rol.

Parámetro	Descripción
`group-id`	Especifica el ID único generado para el grupo mediante el comando `security login group create`.
`role`	Nombre del rol de ONTAP al que está asignado el grupo.

Ejemplo

```
security login group role-mapping create -group-id 1 -role admin
```

Operaciones de CLI adicionales

El comando admite varias operaciones adicionales, entre las que se incluyen:

- Mostrar
- Modificar
- Eliminar

Obtenga más información sobre los comandos descritos en este procedimiento en el "Referencia de comandos del ONTAP".

Información relacionada

- "Asignación de roles externos"

Autenticación y autorización mediante WebAuthn MFA

Obtenga información sobre la autenticación multifactor WebAuthn para los usuarios de ONTAP System Manager

A partir de ONTAP 9.16,1, los administradores pueden habilitar la autenticación multifactor (MFA) de WebAuthn para los usuarios que inician sesión en System Manager. Esto permite los inicios de sesión de System Manager mediante una clave FIDO2 (como YubiKey) como segunda forma de autenticación. De forma predeterminada, WebAuthn MFA está desactivado para los usuarios de ONTAP nuevos y existentes.

WebAuthn MFA es compatible con usuarios y grupos que utilizan los siguientes tipos de autenticación para el primer método de autenticación:

- Usuarios: Contraseña, dominio o nsswitch
- Grupos: Domain o nsswitch

Después de habilitar WebAuthn MFA como el segundo método de autenticación para un usuario, se solicita al usuario que registre un autenticador de hardware al iniciar sesión en System Manager. Después del registro, la clave privada se almacena en el autenticador y la clave pública se almacena en ONTAP.

ONTAP admite una credencial WebAuthn por usuario. Si un usuario pierde un autenticador y necesita reemplazarlo, el administrador de ONTAP debe eliminar la credencial WebAuthn del usuario para que el usuario pueda registrar un nuevo autenticador en el siguiente inicio de sesión.

> Los usuarios que tienen WebAuthn MFA habilitado como segundo método de autenticación necesitan usar el FQDN (por ejemplo, "https://myontap.example.com") en lugar de la dirección IP (por ejemplo, "https://192.168.100.200") para acceder a System Manager. Para los usuarios con MFA de WebAuthn habilitado, se rechazan los intentos de iniciar sesión en System Manager con la dirección IP.

Habilite WebAuthn MFA para los usuarios o grupos de ONTAP System Manager

Como administrador de ONTAP, puede habilitar WebAuthn MFA para un usuario o grupo de System Manager agregando un nuevo usuario o grupo con la opción MFA de

WebAuthn habilitada o habilitando la opción para un usuario o grupo existente.

> Después de habilitar WebAuthn MFA como el segundo método de autenticación para un usuario o grupo, se solicitará al usuario (o a todos los usuarios de ese grupo) que registre un dispositivo de hardware FIDO2 en el siguiente inicio de sesión en System Manager. El sistema operativo local del usuario gestiona este registro y, por lo general, consiste en insertar la clave de seguridad, crear una clave de acceso y tocar la clave de seguridad (si es compatible).

Habilite WebAuthn MFA al crear un nuevo usuario o grupo

Puede crear un nuevo usuario o grupo con MFA de WebAuthn habilitado mediante System Manager o la CLI de ONTAP.

System Manager

1. Seleccione **Cluster > Settings**.
2. Seleccione el icono de flecha junto a **Usuarios y Roles**.
3. Seleccione **Agregar** en **Usuarios**.
4. Especifique un nombre de usuario o grupo y seleccione un rol en el menú desplegable para **Rol**.
5. Especifique un método de inicio de sesión y una contraseña para el usuario o el grupo.

   WebAuthn MFA soporta métodos de inicio de sesión de “contraseña”, “dominio” o “nsswitch” para los usuarios, y “dominio” o “nsswitch” para los grupos.
6. En la columna **MFA for HTTP**, selecciona **enabled**.
7. Seleccione **Guardar**.

CLI

1. Cree un nuevo usuario o grupo con WebAuthn MFA activado.

   En el siguiente ejemplo, WebAuthn MFA se habilita eligiendo “publickey” para el segundo método de autenticación:

   ```
   security login create -user-or-group-name <user_or_group_name> \
                         -authentication-method domain \
                         -second-authentication-method publickey \
                         -application http \
                         -role admin
   ```

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

Habilite WebAuthn MFA para un usuario o grupo existente

Puede habilitar WebAuthn MFA para un usuario o grupo existente.

System Manager

1. Seleccione **Cluster > Settings**.
2. Seleccione el icono de flecha junto a **Usuarios y Roles**.
3. En la lista de usuarios y grupos, seleccione el menú de opciones para el usuario o grupo que desea editar.

   WebAuthn MFA soporta métodos de inicio de sesión de “contraseña”, “dominio” o “nsswitch” para los usuarios, y “dominio” o “nsswitch” para los grupos.
4. En la columna **MFA for HTTP** para ese usuario, seleccione **enabled**.
5. Seleccione **Guardar**.

CLI

1. Modifique un usuario o grupo existente para habilitar WebAuthn MFA para ese usuario o grupo.

   En el siguiente ejemplo, WebAuthn MFA se habilita eligiendo “publickey” para el segundo método de autenticación:

   ```
   security login modify -user-or-group-name <user_or_group_name> \
                         -authentication-method domain \
                         -second-authentication-method publickey \
                         -application http \
                         -role admin
   ```

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

Desactive WebAuthn MFA para usuarios de ONTAP System Manager

Como administrador de ONTAP, puede deshabilitar la MFA de WebAuthn para un usuario o grupo editando el usuario o grupo con System Manager o la interfaz de línea de comandos de ONTAP.

Desactive WebAuthn MFA para un usuario o grupo existente

Puede deshabilitar WebAuthn MFA para un usuario o grupo existente en cualquier momento.

> Si deshabilita las credenciales registradas, se conservan las credenciales. Si vuelve a activar las credenciales en el futuro, se utilizarán las mismas credenciales, por lo que el usuario no tendrá que volver a registrarse al iniciar sesión.

System Manager

1. Seleccione **Cluster > Settings**.
2. Seleccione el icono de flecha junto a **Usuarios y Roles**.
3. En la lista de usuarios y grupos, seleccione el usuario o grupo que desea editar.
4. En la columna **MFA for HTTP** para ese usuario, seleccione **Disabled**.
5. Seleccione **Guardar**.

CLI

1. Modifique un usuario o grupo existente para desactivar WebAuthn MFA para ese usuario o grupo.

   En el siguiente ejemplo, WebAuthn MFA se deshabilita seleccionando “none” para el segundo método de autenticación.

   ```
   security login modify -user-or-group-name <user_or_group_name> \
                         -authentication-method domain \
                         -second-authentication-method none \
                         -application http \
                         -role admin
   ```

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

Vea la configuración MFA de ONTAP WebAuthn y administre las credenciales

Como administrador de ONTAP, puede ver la configuración MFA de WebAuthn para todo el clúster y administrar las credenciales de usuario y grupo para WebAuthn MFA.

Ver la configuración del clúster para WebAuthn MFA

La configuración del clúster de la MFA de WebAuthn se puede ver mediante la CLI de ONTAP.

Pasos

1. Vea la configuración del clúster para WebAuthn MFA. De manera opcional, puede especificar una máquina virtual de almacenamiento con `vserver` el argumento:

   ```
   security webauthn show -vserver <storage_vm_name>
   ```

   Obtenga más información sobre `security webauthn show` en el "Referencia de comandos del ONTAP".

Ver los algoritmos MFA de clave pública soportados de WebAuthn

Es posible ver los algoritmos de clave pública compatibles con la MFA de WebAuthn para una máquina virtual de almacenamiento o para un clúster.

Pasos

1. Enumere los algoritmos MFA de WebAuthn de clave pública admitidos. De manera opcional, puede especificar una máquina virtual de almacenamiento con `vserver` el argumento:

```
security webauthn supported-algorithms show -vserver <storage_vm_name>
```

Obtenga más información sobre `security webauthn supported-algorithms show` en el "Referencia de comandos del ONTAP".

Vea las credenciales MFA registradas de WebAuthn

Como administrador de ONTAP, puede ver las credenciales de WebAuthn registradas para todos los usuarios. Los usuarios que no sean administradores que utilicen este procedimiento sólo pueden ver sus propias credenciales de WebAuthn registradas.

Pasos

1. Vea las credenciales MFA registradas de WebAuthn:

```
security webauthn credentials show
```

Obtenga más información sobre `security webauthn credentials show` en el "Referencia de comandos del ONTAP".

Quitar una credencial MFA de WebAuthn registrada

Puede quitar una credencial MFA de WebAuthn registrada. Esto es útil cuando la clave de hardware de un usuario se perdió, fue robada o ya no está en uso. También puede eliminar una credencial registrada cuando el usuario aún tiene el autenticador de hardware original, pero desea reemplazarla por una nueva. Después de eliminar la credencial, se le pedirá al usuario que registre el autenticador de reemplazo.

> Al quitar una credencial registrada para un usuario, no se deshabilita WebAuthn MFA para el usuario. Si un usuario pierde un autenticador de hardware y necesita iniciar sesión antes de reemplazarlo, debe eliminar la credencial mediante estos pasos y también "Desactive WebAuthn MFA" para el usuario.

System Manager

1. Seleccione **Cluster > Settings**.
2. Seleccione el icono de flecha junto a **Usuarios y Roles**.
3. En la lista de usuarios y grupos, seleccione el menú de opciones para el usuario o grupo cuyas credenciales desea eliminar.
4. Seleccione **Remove MFA for HTTP credentials**.
5. Seleccione **Quitar**.

CLI

1. Elimine las credenciales registradas. Tenga en cuenta lo siguiente:
   - Opcionalmente, puede especificar una máquina virtual de almacenamiento del usuario. Si se omite, la credencial se elimina en el nivel de clúster.
   - Opcionalmente, puede especificar un nombre de usuario del usuario para el que va a suprimir la credencial. Si se omite, la credencial se elimina del usuario actual.

     ```
     security webauthn credentials delete -vserver <storage_vm_name>
     -username <username>
     ```

     Obtenga más información sobre `security webauthn credentials delete` en el "Referencia de comandos del ONTAP".

Gestionar servicios web

Información general sobre los servicios web de Manage

Puede habilitar o deshabilitar un servicio web para el clúster o una máquina virtual de almacenamiento (SVM), mostrar la configuración de los servicios web y controlar si los usuarios de un rol pueden acceder a un servicio web.

Puede gestionar los servicios web para el clúster o una SVM de las siguientes formas:

- Activación o desactivación de un servicio Web específico
- Especificar si el acceso a un servicio Web está restringido a sólo HTTP (SSL) cifrado
- Mostrar la disponibilidad de los servicios web
- Permitir o rechazar a los usuarios de una función acceder a un servicio web
- Mostrar los roles que pueden tener acceso a un servicio Web

Para que un usuario pueda acceder a un servicio web, se deben cumplir todas las siguientes condiciones:

- Se debe autenticar al usuario.

  Por ejemplo, un servicio Web puede solicitar un nombre de usuario y una contraseña. La respuesta del usuario debe coincidir con una cuenta válida.

- Debe configurarse el usuario con el método de acceso correcto.

  La autenticación sólo se realiza correctamente para los usuarios con el método de acceso correcto para el servicio web dado. Para el servicio web de la API de ONTAP `ontapi`), los usuarios deben tener el `ontapi` método de acceso. Para todos los demás servicios web, los usuarios deben tener el `http` método de acceso.

  > `security login`Los comandos se usan para gestionar los métodos de acceso y los métodos de autenticación de los usuarios.

- El servicio web debe estar configurado para permitir la función de control de acceso del usuario.

  > Los `vserver services web access` comandos se utilizan para controlar el acceso de un rol a un servicio web.

Si hay un firewall habilitado, la política de firewall para el LIF que se utilizará para los servicios web debe configurarse para permitir HTTP o HTTPS.

Si utiliza HTTPS para el acceso a servicios web, debe habilitar SSL para el clúster o la SVM que ofrece el servicio web, y debe proporcionar un certificado digital para el clúster o la SVM.

Administrar el acceso a los servicios web de ONTAP

Un servicio web es una aplicación a la que los usuarios pueden acceder mediante HTTP o HTTPS. El administrador de clúster puede configurar el motor de protocolo web, configurar SSL, habilitar un servicio web y permitir que los usuarios de un rol accedan a un servicio web.

A partir de ONTAP 9.6, se admiten los siguientes servicios web:

- Infraestructura de Procesador de Servicios (`spi`)

  Este servicio hace que los archivos de registro, volcado de memoria y MIB de un nodo estén disponibles para el acceso HTTP o HTTPS a través de la LIF de gestión de clústeres o de una LIF de gestión de nodos. El valor predeterminado es `enabled`.

  Cuando se recibe una solicitud para acceder a los archivos de registro o a los archivos de volcado de núcleo de un nodo, el `spi` El servicio web crea automáticamente un punto de montaje desde un nodo al volumen raíz de otro nodo donde residen los archivos. No es necesario crear el punto de montaje manualmente.

- API de ONTAP (`ontapi`)

  Este servicio le permite ejecutar API de ONTAP para ejecutar funciones administrativas con un programa remoto. El valor predeterminado es `enabled`.

  Es posible que este servicio sea necesario para algunas herramientas de administración externas. Por ejemplo, si utiliza System Manager, debe dejar este servicio habilitado.

- Descubrimiento Data ONTAP (`disco`)

  Este servicio permite que las aplicaciones de administración externas puedan detectar el clúster en la red. El valor predeterminado es `enabled`.

- Diagnósticos de Soporte (`supdiag`)

  Este servicio controla el acceso a un entorno privilegiado en el sistema para ayudar al análisis y resolución de problemas. El valor predeterminado es `disabled`. Debe habilitar este servicio solo cuando lo indique el soporte técnico.

- System (`sysmgr`Manager)

  Este servicio controla la disponibilidad de System Manager, que se incluye con ONTAP. El valor predeterminado es `enabled`. Este servicio solo es compatible en el clúster.

- Actualización del controlador de administración de la placa base (BMC) del firmware (`FW_BMC`)

  Este servicio le permite descargar archivos de firmware de BMC. El valor predeterminado es `enabled`.

- Documentación de ONTAP (`docs`)

  Este servicio proporciona acceso a la documentación de ONTAP. El valor predeterminado es `enabled`.

- API RESTful de ONTAP (`docs_api`)

  Este servicio proporciona acceso a la documentación de la API RESTful de ONTAP. El valor predeterminado es `enabled`.

- Carga y descarga de archivos (`fud`)

  Este servicio ofrece carga y descarga de archivos. El valor predeterminado es `enabled`.

- Mensajería ONTAP (`ontapmsg`)

  Este servicio admite una interfaz de publicación y suscripción que le permite suscribirse a eventos. El valor predeterminado es `enabled`.

- Portal ONTAP (`portal`)

  Este servicio implementa la puerta de enlace en un servidor virtual. El valor predeterminado es `enabled`.

- Interfaz ONTAP RESTful (`rest`)

  Este servicio es compatible con una interfaz RESTful que se utiliza para gestionar de forma remota todos los elementos de la infraestructura de clúster. El valor predeterminado es `enabled`.

- Soporte del proveedor de servicios de lenguaje de marcado de aserción de seguridad (SAML) (`saml`)

  Este servicio proporciona recursos para admitir el proveedor de servicios SAML. El valor predeterminado es `enabled`.

- Proveedor de Servicios SAML (`saml-sp`)

Este servicio ofrece servicios como metadatos del SP y el servicio de consumidor de aserción al proveedor de servicios. El valor predeterminado es `enabled`.

A partir de ONTAP 9.7, se admiten los siguientes servicios adicionales:

- Archivos de Copia de Seguridad de Configuración (`backups`)

  Este servicio permite descargar archivos de copia de seguridad de configuración. El valor predeterminado es `enabled`.

- Seguridad ONTAP (`security`)

  Este servicio admite la gestión de token de CSRF para una autenticación mejorada. El valor predeterminado es `enabled`.

Administre el motor de protocolo web en ONTAP

Puede configurar el motor de protocolo web en el clúster para controlar si se permite el acceso web y qué versiones SSL se pueden utilizar. También puede mostrar los ajustes de configuración del motor de protocolo web.

Puede gestionar el motor de protocolo web en el nivel de clúster de las siguientes formas:

- Puede especificar si los clientes remotos pueden utilizar HTTP o HTTPS para acceder al contenido del servicio web mediante `system services web modify` el comando con el `-external` parámetro.
- Puede especificar si se debe utilizar SSLv3 para un acceso web seguro mediante `security config modify` el comando con el `-supported-protocol` parámetro. De forma predeterminada, SSLv3 está deshabilitado. La seguridad de la capa de transporte 1.0 (TLSv1.0) está habilitada y se puede desactivar si es necesario.

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

- Puede habilitar el modo de cumplimiento del estándar de procesamiento de información federal (FIPS) 140-2 para las interfaces de servicio web del plano de control de todo el clúster.

  De manera predeterminada, el modo de cumplimiento de FIPS 140-2 está deshabilitado.

  - **Cuando el modo de cumplimiento FIPS 140-2 está desactivado**, puede habilitar el modo de cumplimiento FIPS 140-2 estableciendo el `is-fips-enabled` parámetro en `true` para el `security config modify` comando y, a continuación, usando el `security config show` comando para confirmar el estado en línea.
  - **Cuando el modo de cumplimiento FIPS 140-2 está activado**
    - A partir de ONTAP 9.11.1, TLSv1, TLSv1,1 y SSLv3 están deshabilitados, y solo TSLv1,2 y TSLv1,3 permanecen habilitados. Afecta a otros sistemas y comunicaciones internos y externos a ONTAP 9. Si habilita el modo de cumplimiento FIPS 140-2 y, a continuación, se deshabilita TLSv1, TLSv1.1 y SSLv3. TLSv1,2 o TLSv1,3 permanecerán habilitados según la configuración anterior.
    - Para las versiones de ONTAP anteriores a 9.11.1, tanto TLSv1 como SSLv3 están deshabilitados y sólo TLSv1.1 y TLSv1.2 permanecen habilitados. ONTAP evita que habilite TLSv1 y SSLv3 cuando el modo de cumplimiento FIPS 140-2 está habilitado. Si activa el modo de cumplimiento FIPS 140-

2 y lo deshabilita posteriormente, TLSv1 y SSLv3 permanecen deshabilitados, pero TLSv1.2 o TLSv1.1 y TLSv1.2 se habilitan en función de la configuración anterior.

- Puede mostrar la configuración de la seguridad de todo el clúster mediante `system security config show` el comando.

  Obtenga más información sobre `security config show` en el "Referencia de comandos del ONTAP".

Si el firewall está habilitado, debe configurarse la política de firewall de la interfaz lógica (LIF) que se utilizará para los servicios web para permitir el acceso HTTP o HTTPS.

Si utiliza HTTPS para acceder a servicios web, debe habilitar también SSL para el clúster o la máquina virtual de almacenamiento (SVM) que ofrezca el servicio web, y debe proporcionar un certificado digital para el clúster o la SVM.

En las configuraciones de MetroCluster, los cambios de configuración que realice para el motor de protocolo web de un clúster no se replican en el clúster de partners.

Comandos ONTAP para administrar el motor de protocolo web

Los `system services web` comandos se utilizan para administrar el motor del protocolo web. Utilice los `system services firewall policy create` `network interface modify` comandos y para permitir que las solicitudes de acceso web pasen por el firewall.

Si desea…	Se usa este comando…
Configure el motor de protocolo web en el nivel de clúster: • Habilite o deshabilite el motor de protocolo web del clúster • Habilite o deshabilite SSLv3 para el clúster • Habilitar o deshabilitar el cumplimiento de la normativa FIPS 140-2 para servicios web seguros (HTTPS)	`system services web modify`
Muestre la configuración del motor de protocolo web en el nivel del clúster, determine si los protocolos web son funcionales en todo el clúster y muestre si el cumplimiento con FIPS 140-2 está habilitado y en línea	`system services web show`
Muestre la configuración del motor de protocolo web en el nivel del nodo y la actividad de la manipulación del servicio web de los nodos del clúster	`system services web node show`

Si desea…	Se usa este comando…
Cree una política de firewall o agregue un servicio de protocolo HTTP o HTTPS a una política de firewall existente para permitir que las solicitudes de acceso web se atraviese por el firewall	`system services firewall policy create` La configuración `-service` del parámetro en `http` o `https` permite que las solicitudes de acceso web pasen por el firewall.
Asociar una política de firewall a una LIF	`network interface modify` Puede usar el `-firewall-policy` parámetro para modificar la política de firewall de una LIF.

Información relacionada

- "modificación de la interfaz de red"

Configurar el acceso a los servicios web de ONTAP

Al configurar el acceso a los servicios web, los usuarios autorizados pueden usar HTTP o HTTPS para acceder al contenido del servicio en el clúster o una máquina virtual de almacenamiento (SVM).

Pasos

1. Si hay un firewall habilitado, asegúrese de que el acceso HTTP o HTTPS esté configurado en la política de firewall para la LIF que se utilizará para los servicios web:

   Puede comprobar si un firewall está activado mediante el `system services firewall show` comando.

   a. Para verificar que HTTP o HTTPS está configurado en la política de firewall, utilice el `system services firewall policy show` comando.

      `-service`El parámetro `system services firewall policy create` del comando se establece en `http` o `https` para habilitar la política para admitir el acceso web.

   b. Para verificar que la política de firewall que admite HTTP o HTTPS está asociada a la LIF que proporciona servicios web, utilice `network interface show` el comando con el `-firewall-policy` parámetro.

      Obtenga más información sobre `network interface show` en el "Referencia de comandos del ONTAP".

      Utilice `network interface modify` el comando con `-firewall-policy` el parámetro para poner la política de firewall en vigencia para una LIF.

   Obtenga más información sobre `network interface modify` en el "Referencia de comandos del ONTAP".

2. Para configurar el motor de protocolo web a nivel de clúster y hacer que el contenido del servicio web sea accesible, utilice el `system services web modify` comando.
3. Si planea utilizar servicios web seguros (HTTPS), habilite SSL y proporcione información de certificado digital para el clúster o la SVM mediante `security ssl modify` el comando.

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

4. Para habilitar un servicio web para el clúster o la SVM, utilice `vserver services web modify` el comando.

   Debe repetir este paso para cada servicio que desee habilitar para el clúster o la SVM.

5. Para autorizar un rol para acceder a servicios web en el clúster o SVM, utilice `vserver services web access create` el comando.

   La función que concede acceso ya debe existir. Puede mostrar los roles existentes mediante `security login role show` el comando o crear roles nuevos mediante `security login role create` el comando.

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

6. Para un rol autorizado a acceder a un servicio web, asegúrese de que sus usuarios también estén configurados con el método de acceso correcto comprobando la salida del `security login show` comando.

   Para acceder al servicio web de la API de ONTAP `ontapi`), se debe configurar un usuario con el `ontapi` método de acceso. Para acceder a todos los demás servicios web, se debe configurar un usuario con el `http` método de acceso.

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

> Utilice `security login create` el comando para agregar un método de acceso para un usuario. Obtenga más información sobre `security login create` en el "Referencia de comandos del ONTAP".

Comandos ONTAP para administrar servicios web

Los `vserver services web` comandos se utilizan para gestionar la disponibilidad de servicios web para el clúster o una máquina virtual de almacenamiento (SVM). Los `vserver services web access` comandos se utilizan para controlar el acceso de un rol a un servicio web.

Si desea…	Se usa este comando…
Configure un servicio web para el clúster o ANSVM: • Activar o desactivar un servicio Web • Especifique si sólo se puede utilizar HTTPS para acceder a un servicio web	`vserver services web modify`
Muestre la configuración y la disponibilidad de servicios web del clúster o ANSVM	`vserver services web show`
Autorice a un rol para acceder a un servicio web en el clúster o anSVM	`vserver services web access create`
Muestre los roles que están autorizados a acceder a los servicios web en el clúster o anSVM	`vserver services web access show`
Evite que un rol acceda a un servicio web en el clúster o anSVM	`vserver services web access delete`

Información relacionada

"Referencia de comandos del ONTAP"

Comandos para administrar puntos de montaje en nodos ONTAP

`spi`El servicio web crea automáticamente un punto de montaje desde un nodo al volumen raíz de otro nodo tras una solicitud para acceder a los archivos de registro o los archivos principales del nodo. Aunque no necesita gestionar manualmente los puntos de montaje, puede hacerlo mediante los `system node root-mount` comandos.

Si desea…	Se usa este comando…
Crear manualmente un punto de montaje desde un nodo al volumen raíz de otro nodo	`system node root-mount create` Sólo puede existir un único punto de montaje entre un nodo y otro.
Muestra los puntos de montaje existentes en los nodos del clúster, incluida la hora en la que se creó un punto de montaje y su estado actual	`system node root-mount show`
Elimine un punto de montaje de un nodo a el volumen raíz de otro nodo y obligue las conexiones al punto de montaje a cerrarse	`system node root-mount delete`

Información relacionada

"Referencia de comandos del ONTAP"

Administrar SSL en ONTAP

Utilice `security ssl` los comandos para gestionar el protocolo SSL para el clúster o una máquina virtual de almacenamiento (SVM). El protocolo SSL mejora la seguridad del acceso web mediante el uso de un certificado digital para establecer una conexión cifrada entre un servidor web y un navegador.

Puede gestionar SSL para el clúster o una máquina virtual de almacenamiento (SVM) de las siguientes maneras:

- Habilitar SSL
- Generar e instalar un certificado digital y asociarlo con el clúster o SVM
- Mostrar la configuración SSL para ver si SSL se ha habilitado y, si está disponible, el nombre del certificado SSL
- Configurar políticas de firewall para el clúster o SVM para que las solicitudes de acceso web puedan atravesarse
- Definición de las versiones SSL que se pueden utilizar
- Restringir el acceso sólo a solicitudes HTTPS para un servicio Web

Comandos para gestionar SSL

Los `security ssl` comandos se utilizan para gestionar el protocolo SSL para el clúster o una máquina virtual de almacenamiento (SVM).

Si desea…	Se usa este comando…
Habilite SSL para el clúster o una SVM y asocie un certificado digital con él	`security ssl modify`
Muestre la configuración de SSL y el nombre de certificado para el clúster o una SVM	`security ssl show`

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

Utilice HSTS para servicios web de ONTAP

La Seguridad de Transporte Estricta HTTP (HSTS) es un mecanismo de política de seguridad web que ayuda a proteger los sitios web contra ataques de intermediario, como la degradación de protocolos y el secuestro de cookies. Al implementar el uso de HTTPS, HSTS garantiza el cifrado de todas las comunicaciones entre el navegador del usuario y el servidor. A partir de ONTAP 9.17.1, ONTAP puede implementar conexiones HTTPS para ONTAP servicios web.

El navegador web solo aplica HSTS tras establecer una conexión HTTPS segura inicial con ONTAP. Si el navegador no establece una conexión segura inicial, no se aplicará HSTS. Consulte la documentación de su navegador para obtener información sobre la administración de HSTS.

Acerca de esta tarea

- Para la versión 9.17.1 y posteriores, HSTS está habilitado de forma predeterminada para los clústeres de ONTAP recién instalados. Al actualizar a la versión 9.17.1, HSTS no está habilitado de forma predeterminada. Debe habilitar HSTS después de la actualización.
- HSTS es compatible con todos "Servicios web de ONTAP" .

Antes de empezar

- Se requieren privilegios avanzados para las siguientes tareas.

Mostrar configuración de HSTS

Puede mostrar la configuración actual de HSTS para verificar si está habilitada y ver la configuración de edad máxima.

Pasos

1. Utilice el `system services web show` Comando para mostrar la configuración actual de los servicios web, incluida la configuración HSTS:

```
cluster-1::system services web*> show

                    External Web Services: true
                                HTTP Port: 80
                               HTTPS Port: 443
                          Protocol Status: online
                       Per Address Limit: 80
                     Wait Queue Capacity: 192
                            HTTP Enabled: true
                  CSRF Protection Enabled: true
Maximum Number of Concurrent CSRF Tokens: 500
       CSRF Token Idle Timeout (Seconds): 900
   CSRF Token Absolute Timeout (Seconds): 0
          Allow Web Management via Cloud: true
Enforce Network Interface Service-Policy: -
                            HSTS Enabled: true
                   HSTS max age (Seconds): 63072000
```

Habilitar HSTS y establecer la edad máxima

A partir de ONTAP 9.17.1, HSTS está habilitado de forma predeterminada en los nuevos clústeres de ONTAP . Si actualiza un clúster existente a la versión 9.17.1 o posterior, deberá habilitar HSTS manualmente para forzar el uso de HTTPS. Puede habilitar HSTS y establecer la antigüedad máxima. Puede cambiar la antigüedad máxima en cualquier momento si HSTS está habilitado. Una vez habilitado HSTS, los

navegadores comenzarán a forzar las conexiones seguras solo después de establecer una conexión segura inicial.

Pasos

1. Utilice el `system services web modify` Comando para habilitar HSTS o modificar la edad máxima:

```
system services web modify -hsts-enabled true -hsts-max-age <seconds>
```

`-hsts-max-age` Especifica el tiempo en segundos que el navegador recordará aplicar HTTPS. El valor predeterminado es 63072000 segundos (dos años).

Deshabilitar HSTS

Los navegadores guardan la configuración de edad máxima de HSTS con cada conexión y continúan implementando HSTS durante todo el proceso, incluso si HSTS está deshabilitado en ONTAP. El navegador tardará hasta alcanzar la edad máxima configurada para dejar de implementar HSTS después de su deshabilitación. Si durante este tiempo no se puede establecer una conexión segura, los navegadores que implementan HSTS no permitirán el acceso a los servicios web de ONTAP hasta que se resuelva el problema o expire la edad máxima del navegador.

Pasos

1. Desactivar HSTS mediante el `system services web modify` dominio:

```
system services web modify -hsts-enabled false
```

Información relacionada

"RFC 6797 - Seguridad de transporte estricta HTTP (HSTS)"

Solucionar problemas de acceso al servicio web de ONTAP

Los errores de configuración provocan problemas de acceso al servicio web. Puede resolver los errores garantizando que la LIF, la política de firewall, el motor de protocolo web, los servicios web, los certificados digitales, y la autorización de acceso del usuario está configurada correctamente.

La tabla siguiente le ayuda a identificar y solucionar errores de configuración del servicio web:

Este problema de acceso…	Se produce debido a este error de configuración…	Para solucionar el error…
Su navegador web devuelve un `unable to connect failure to establish a connection` error OR cuando intenta acceder a un servicio web.	Es posible que el LIF se haya configurado incorrectamente.	Asegúrese de que puede hacer ping al LIF que proporciona el servicio web. Usted utiliza `network ping` el comando para hacer ping a una LIF.
Es posible que el firewall esté configurado incorrectamente.	Asegúrese de que se haya configurado una política de firewall para que sea compatible con HTTP o HTTPS y de que la política esté asignada a la LIF que proporciona el servicio web. Los `system services firewall policy` comandos se utilizan para administrar las políticas de firewall. Puede utilizar `network interface modify` el comando con `-firewall-policy` el parámetro para asociar una política a una LIF.	Es posible que el motor de protocolo web esté desactivado.

Este problema de acceso…	Se produce debido a este error de configuración…	Para solucionar el error…
Asegúrese de que el motor de protocolo web está activado para que los servicios web estén accesibles. `system services web`Los comandos se usan para administrar el motor de protocolo web del clúster.	Su navegador web devuelve un `not found` error cuando intenta acceder a un servicio web.	Es posible que el servicio web esté desactivado.
Asegúrese de que todos los servicios web a los que desea permitir el acceso están habilitados individualmente. El `vserver services web modify` comando se utiliza para habilitar un servicio web para el acceso.	El explorador Web no puede iniciar sesión en un servicio Web con el nombre de cuenta y la contraseña de un usuario.	El usuario no se puede autenticar, el método de acceso no es correcto o el usuario no está autorizado a acceder al servicio web.

Este problema de acceso…	Se produce debido a este error de configuración…	Para solucionar el error…
Asegúrese de que la cuenta de usuario exista y esté configurada con el método de acceso y el método de autenticación correctos. Asimismo, asegúrese de que la función del usuario está autorizada para acceder al servicio web. Los `security login` comandos se utilizan para administrar las cuentas de usuario y sus métodos de acceso y métodos de autenticación. Para acceder al servicio web de la API de ONTAP se requiere `ontapi` el método de acceso. El acceso a todos los demás servicios web requiere el `http` método de acceso. Los `vserver services web access` comandos se utilizan para gestionar el acceso de un rol a un servicio web.	Se conecta al servicio web con HTTPS y el explorador web indica que la conexión se ha interrumpido.	Es posible que no tenga habilitado SSL en el clúster ni la SVM que proporciona el servicio web.

Este problema de acceso…	Se produce debido a este error de configuración…	Para solucionar el error…
Compruebe que el clúster o la SVM tengan habilitada SSL y que el certificado digital sea válido. Los `security ssl` comandos se utilizan para administrar la configuración SSL para servidores HTTP y `security certificate show` el comando para mostrar información de certificados digitales.	Se conecta al servicio web mediante HTTPS y el navegador web indica que la conexión no es de confianza.	Es posible que utilice un certificado digital autofirmado.

Información relacionada

- "¿Cuáles son las mejores prácticas para la configuración de red para ONTAP?"
- "ping de red"
- "modificación de la interfaz de red"
- "Generación de certificado de seguridad CSR"
- "instalación del certificado de seguridad"
- "Mostrar certificado de seguridad"
- "seguridad SSL"

Compruebe la identidad de los servidores remotos mediante certificados

Obtenga información sobre cómo verificar la identidad de servidores remotos mediante certificados en ONTAP

ONTAP admite características de certificado de seguridad para verificar la identidad de los servidores remotos.

El software ONTAP permite conexiones seguras utilizando las siguientes funciones y protocolos de certificados digitales:

- El protocolo de estado de certificados en línea (OCSP) valida el estado de las solicitudes de certificados digitales de los servicios de ONTAP mediante conexiones SSL y de seguridad de la capa de transporte (TLS). Esta función está deshabilitada de forma predeterminada.
- Con el software ONTAP se incluye un conjunto predeterminado de certificados raíz de confianza.
- Los certificados de protocolo de interoperabilidad de gestión de claves (KMIP) permiten la autenticación mutua de un clúster y de un servidor KMIP.

Verificar que los certificados digitales sean válidos usando OCSP en ONTAP

El Protocolo de estado de certificado en línea (OCSP) permite que las aplicaciones ONTAP que utilizan comunicaciones de seguridad de la capa de transporte (TLS) reciban el estado del certificado digital cuando OCSP está habilitado. Es posible habilitar o deshabilitar las comprobaciones de estado de certificados de OCSP para aplicaciones específicas en cualquier momento. De manera predeterminada, la comprobación del estado de los certificados OCSP está deshabilitada.

Antes de empezar

Necesita acceso de nivel de privilegio avanzado para realizar esta tarea.

Acerca de esta tarea

OCSP admite las siguientes aplicaciones:

- AutoSupport
- Sistema de gestión de eventos (EMS)
- LDAP sobre TLS
- Protocolo de interoperabilidad de gestión de claves (KMIP)
- Registro de auditoría
- FabricPool
- SSH (a partir de ONTAP 9.13.1)

Pasos

1. Establezca el nivel de privilegio en AVANZADO `set -privilege advanced`: .
2. Para habilitar o deshabilitar las comprobaciones de estado de certificados de OCSP para aplicaciones de ONTAP específicas, utilice el comando correspondiente.

Si desea que las comprobaciones del estado del certificado OCSP para que algunas aplicaciones sean…	Usar el comando…
Activado	`security config ocsp enable -app app name`
Deshabilitado	`security config ocsp disable -app app name`

El siguiente comando habilita la compatibilidad de OCSP para AutoSupport y EMS.

```
cluster::*> security config ocsp enable -app asup,ems
```

Cuando OCSP está habilitado, la aplicación recibe una de las siguientes respuestas:

- Correcto: El certificado es válido y la comunicación continúa.

- Revocado: La autoridad emisora de certificados considera permanentemente que el certificado no es de confianza y la comunicación no continúa.
- Unknown: El servidor no tiene ninguna información de estado sobre el certificado y la comunicación no continúa.
- Falta información del servidor OCSP en el certificado: El servidor actúa como si OCSP está deshabilitado y continúa con la comunicación TLS, pero no se produce ninguna comprobación de estado.
- Sin respuesta del servidor OCSP: La aplicación no puede continuar.

3. Para habilitar o deshabilitar las comprobaciones de estado de certificados OCSP para todas las aplicaciones que utilizan comunicaciones TLS, utilice el comando correspondiente.

Si desea que las comprobaciones del estado del certificado OCSP para que todas las aplicaciones sean…	**Usar el comando…**
Activado	`security config ocsp enable -app all`
Deshabilitado	`security config ocsp disable -app all`

Cuando se habilita, todas las aplicaciones reciben una respuesta firmada que significa que el certificado especificado es correcto, revocado o desconocido. En el caso de un certificado revocado, la solicitud no continuará. Si la aplicación no recibe una respuesta del servidor OCSP o si no se puede acceder al servidor, la aplicación no podrá continuar.

4. Utilice `security config ocsp show` el comando para mostrar todas las aplicaciones que admiten OCSP y su estado de soporte.

```
cluster::*> security config ocsp show
         Application                     OCSP Enabled?
         --------------------            ---------------------
         autosupport                     false
         audit_log                       false
         fabricpool                      false
         ems                             false
         kmip                            false
         ldap_ad                         true
         ldap_nis_namemap                true
         ssh                             true

         8 entries were displayed.
```

Información relacionada

- "configuración de seguridad ocsp habilitar"
- "configuración de seguridad ocsp deshabilitada"
- "configuración de seguridad ocsp show"

Ver certificados predeterminados para aplicaciones basadas en TLS en ONTAP

ONTAP proporciona un conjunto predeterminado de certificados raíz confiables para aplicaciones ONTAP que utilizan Seguridad de la capa de transporte (TLS).

Antes de empezar

Los certificados predeterminados se instalan solo en el SVM de administrador durante su creación o durante una actualización.

Acerca de esta tarea

Las aplicaciones actuales que funcionan como cliente y requieren validación de certificados son AutoSupport, EMS, LDAP, Registro de auditoría, FabricPool, Y KMIP.

Cuando los certificados caducan, se invoca un mensaje EMS que solicita al usuario que elimine los certificados. Los certificados predeterminados solo se pueden eliminar en el nivel de privilegios avanzados.

> La eliminación de los certificados predeterminados puede provocar que algunas aplicaciones ONTAP no funcionen como se esperaba (por ejemplo, AutoSupport y Registro de auditoría).

Paso

1. Puede ver los certificados predeterminados que se instalan en la SVM de administrador mediante el comando Security certificate show:

   `security certificate show -vserver -type server-ca`

   ```
   cluster1::> security certificate show

   Vserver    Serial Number   Certificate Name
   Type
   ---------- --------------- ----------------------------------------
   ---------
   vs0        4F4E4D7B         www.example.com
   server
       Certificate Authority:  www.example.com
             Expiration Date: Thu Feb 28 16:08:28 2013
   ```

   Obtenga más información sobre `security certificate show` en el "Referencia de comandos del ONTAP".

Autentique mutuamente el clúster y un servidor KMIP

Descripción general de la autenticación mutua del clúster ONTAP y un servidor KMIP

Al autenticar mutuamente el clúster y un gestor de claves externo, como un servidor de protocolo de interoperabilidad de gestión de claves (KMIP), el administrador de claves puede comunicarse con el clúster mediante KMIP a través de SSL. Esto se hace cuando una aplicación o determinada funcionalidad (por ejemplo, la funcionalidad de cifrado del almacenamiento) requieren claves seguras para ofrecer un acceso seguro a los datos.

Genere una solicitud de firma de certificación para el clúster en ONTAP

Es posible usar `generate-csr` el comando security certificate 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 un administrador 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
```

Obtenga más información sobre `security certificate generate-csr` en el "Referencia de comandos del ONTAP".

El siguiente comando crea una CSR con una clave privada de 2,048 bits generada por la función de hashing SHA256 para que la utilice el grupo Software del departamento DE TI de una empresa cuyo nombre común personalizado es server1.companyname.com, ubicado en Sunnyvale, California, EE. UU. La dirección de correo electrónico del administrador de contacto de la SVM es web@example.com. El sistema muestra la CSR y la clave privada en la salida.

```
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-----
<certificate_value>
-----END CERTIFICATE REQUEST-----
Private Key :
24 | Administrator Authentication and RBAC
-----BEGIN RSA PRIVATE KEY-----
<key_value>
-----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.

Instalar un certificado de servidor firmado por CA para el clúster ONTAP

Para habilitar un servidor SSL que autentique el clúster o la máquina virtual de almacenamiento (SVM) como cliente SSL, se instala un certificado digital con el tipo de cliente en el clúster o la SVM. A continuación, proporcionará el certificado de CA de cliente al administrador del servidor SSL para su instalación en el servidor.

Antes de empezar

Ya debe haber instalado el certificado raíz del servidor SSL en el clúster o en la SVM con el `server-ca` tipo de certificado.

Pasos

1. Si desea utilizar un certificado digital autofirmado para la autenticación de cliente, utilice `security certificate create` el comando con `type client` el parámetro.

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

2. Para utilizar un certificado digital firmado por CA para la autenticación de clientes, complete los siguientes pasos:

   a. Genere una solicitud de firma de certificación (CSR) digital mediante `generate-csr` el comando security certificate.

      ONTAP muestra el resultado de CSR, que incluye una solicitud de certificado y una clave privada, y le recuerda que debe copiar el resultado en un archivo para futura referencia.

b. Envíe la solicitud de certificado de la salida de CSR en un formulario electrónico (como por ejemplo, correo electrónico) a una CA de confianza para su firma.

   Debe conservar una copia de la clave privada y el certificado firmado por CA para referencia futura.

Después de procesar la solicitud, la CA envía el certificado digital firmado.

a. Instale el certificado firmado por CA mediante `security certificate install` el comando con el `-type client` parámetro.
b. Introduzca el certificado y la clave privada cuando se le solicite y, a continuación, pulse **Intro**.
c. Introduzca cualquier certificado raíz o intermedio adicional cuando se le solicite y, a continuación, pulse **Intro**.

   Puede instalar un certificado intermedio en el clúster o la SVM si a una cadena de certificados que comienza en la CA raíz de confianza y finaliza con el certificado SSL emitido para usted, le faltan los certificados intermedios. Un certificado intermedio es un certificado subordinado emitido por el raíz de confianza específicamente para emitir certificados de servidor de entidades finales. El resultado es una cadena de certificados que comienza en la CA raíz de confianza, atraviesa el certificado intermedio y termina con el certificado SSL que se le emitió.

3. Proporcione `client-ca` el certificado del clúster o SVM al administrador del servidor SSL para su instalación en el servidor.

   El comando security certificate show con los `-instance` `-type client-ca` parámetros y muestra `client-ca` la información de certificados.

Información relacionada

- "instalación del certificado de seguridad"
- "Mostrar certificado de seguridad"

Instalar un certificado de cliente firmado por CA para el servidor KMIP en ONTAP

El subtipo de certificado del protocolo de interoperabilidad de gestión de claves (KMIP) (el parámetro -subtipo kmip-cert), junto con los tipos de CA del cliente y del servidor, especifica que el certificado se utiliza para autenticar mutuamente el clúster y un gestor de claves externo, como un servidor KMIP.

Acerca de esta tarea

Instale un certificado KMIP para autenticar un servidor KMIP como servidor SSL en el clúster.

Pasos

1. Utilice `security certificate install` el comando con `-type server-ca` `-subtype kmip-cert` los parámetros y para instalar un certificado KMIP para el servidor KMIP.
2. Cuando se le solicite, introduzca el certificado y pulse Intro.

   ONTAP le recuerda que debe conservar una copia del certificado para futuras consultas.

```
cluster1::> security certificate install -type server-ca -subtype kmip-
cert
-vserver cluster1

Please enter Certificate: Press <Enter> when done
-----BEGIN CERTIFICATE-----
<certificate_value>
-----END CERTIFICATE-----


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

cluster1::>
```

Información relacionada

- "instalación del certificado de seguridad"