Directrices de endurecimiento de ONTAP

ONTAP 9

NetApp
July 19, 2024

Tabla de contenidos

Directrices de endurecimiento de ONTAP

Información general sobre el refuerzo de la seguridad de ONTAP

ONTAP ofrece un conjunto de controles que permiten fortalecer el sistema operativo de almacenamiento de ONTAP, el software para la gestión de datos líder del sector. Utilice las directrices y los ajustes de configuración de ONTAP para ayudar a su organización a cumplir los objetivos de seguridad prescritos de confidencialidad, integridad y disponibilidad del sistema de información.

La evolución del panorama actual de amenazas presenta a una organización retos únicos para proteger sus activos más valiosos: Los datos y la información. Las amenazas y vulnerabilidades avanzadas y dinámicas a las que nos enfrentamos son cada vez más sofisticadas. Junto con un aumento en la eficacia de las técnicas de ofuscación y reconocimiento por parte de los posibles intrusos, los administradores de sistemas deben abordar la seguridad de los datos y la información de manera proactiva.

A partir de julio de 2024, el contenido de informes técnicos previamente publicados como archivos PDF se integró con la documentación de los productos de ONTAP. La documentación de seguridad de ONTAP ahora incluye contenido de *TR-4569: Guía de refuerzo de la seguridad para ONTAP*.

Validación de imágenes ONTAP

ONTAP proporciona mecanismos para garantizar que la imagen ONTAP sea válida durante la actualización y en el momento del inicio.

Renovación de la validación de imágenes

La firma de código ayuda a verificar que las imágenes ONTAP que se instalan mediante actualizaciones de imágenes no disruptivas o actualizaciones de imágenes, CLI o API de ONTAP automatizadas y no disruptivas se producen de forma auténtica mediante NetApp y no se han alterado. La validación de imágenes de actualización se introdujo en ONTAP 9,3.

Esta función es una mejora de la seguridad sin intervención para la actualización o reversión de ONTAP. No se espera que el usuario haga nada diferente excepto para verificar opcionalmente la firma “image.tgz” de nivel superior.

Validación de imagen en tiempo de arranque

A partir de ONTAP 9,4, el arranque seguro de la interfaz de firmware extensible unificada (UEFI) está habilitado para los sistemas NetApp AFF A800, AFF A220, FAS2750 y FAS2720 y los sistemas de próxima generación subsiguientes que utilizan BIOS UEFI.

Durante el encendido, el cargador de arranque valida la base de datos de la lista blanca de claves de inicio seguro con la firma asociada a cada módulo cargado. Después de validar y cargar cada módulo, el proceso de arranque continúa con la inicialización de ONTAP. Si la validación de firma falla para cualquier módulo, el sistema se reinicia.

Estos elementos se aplican a las imágenes ONTAP y a la plataforma BIOS.

Cuentas de administrador de almacenamiento local

Roles, aplicaciones y autenticación

ONTAP proporciona a la empresa condicionada por la seguridad la capacidad de brindar acceso granular a distintos administradores mediante diferentes métodos y aplicaciones de inicio de sesión. Esto ayuda a los clientes a crear un modelo de confianza cero centrado en los datos.

Estas son las funciones disponibles para los administradores de máquinas virtuales de almacenamiento y administradores. Se especifican los métodos de aplicación de inicio de sesión y los métodos de autenticación de inicio de sesión.

Funciones

Con el control de acceso basado en roles, los usuarios solo tienen acceso a los sistemas y las opciones requeridas para sus roles y funciones de trabajo. La solución RBAC de ONTAP limita el acceso administrativo de los usuarios al nivel permitido por el rol que tengan definido, lo que permite a los administradores gestionar usuarios según el rol asignado. ONTAP ofrece varios roles predefinidos. Los operadores y administradores pueden crear, modificar o suprimir roles de control de acceso personalizados, y pueden especificar restricciones de cuenta para roles específicos.

Roles predefinidos para 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`
Solo lectura	`volume`	Ninguno
Todos los demás directorios de comandos (`DEFAULT`)	`readonly`	Todo

• `security login password` Sólo para gestionar la contraseña local y la información de claves de la cuenta de usuario propia • `set`	Ninguno	`security`
Solo lectura	Todos los demás directorios de comandos (`DEFAULT`)	`none`

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

Roles predefinidos para administradores de máquinas virtuales de almacenamiento (SVM)

Nombre del rol	Funcionalidades
`vsadmin`	• Administrar la contraseña local y la información de clave de la cuenta de usuario propia • Gestionar volúmenes, excepto movimientos de volúmenes • Gestione cuotas, qtrees, copias Snapshot y archivos • Gestionar las LUN • Realice operaciones de SnapLock, excepto la supresión con privilegios • Configurar protocolos: NFS, SMB, iSCSI, FC, FCoE y NVMe/FC y NVMe/TCP • Configurar servicios: DNS, LDAP y NIS • Supervisar trabajos • Supervise las conexiones de red y la interfaz de red • Supervise el estado de la SVM

`vsadmin-volume`	• Administrar la contraseña local y la información de clave de la cuenta de usuario propia • Gestión de volúmenes, incluidos los movimientos de volúmenes • Gestione cuotas, qtrees, copias Snapshot y archivos • Gestionar las LUN • Configurar protocolos: NFS, SMB, iSCSI, FC, FCoE y NVMe/FC y NVMe/TCP • Configurar servicios: DNS, LDAP y NIS • Supervise la interfaz de red • Supervise el estado de la SVM
`vsadmin-protocol`	• Administrar la contraseña local y la información de clave de la cuenta de usuario propia • Configurar protocolos: NFS, SMB, iSCSI, FC, FCoE y NVMe/FC y NVMe/TCP • Configurar servicios: DNS, LDAP y NIS • Gestionar las LUN • Supervise la interfaz de red • Supervise el estado de la SVM
`vsadmin-backup`	• Administrar la contraseña local y la información de clave de la cuenta de usuario propia • Gestione las operaciones de NDMP • Haga que un volumen restaurado sea de lectura/escritura • Gestionar relaciones de SnapMirror y copias Snapshot • Ver información de volúmenes y redes

`vsadmin-snaplock`	• Administrar la contraseña local y la información de clave de la cuenta de usuario propia • Gestionar volúmenes, excepto movimientos de volúmenes • Gestione cuotas, qtrees, copias Snapshot y archivos • Realizar operaciones de SnapLock, incluida la supresión con privilegios • Configurar protocolos: NFS y SMB • Configurar servicios: DNS, LDAP y NIS • Supervisar trabajos • Supervise las conexiones de red y la interfaz de red
`vsadmin-readonly`	• Administrar la contraseña local y la información de clave de la cuenta de usuario propia • Supervise el estado de la SVM • Supervise la interfaz de red • Ver volúmenes y LUN • Ver servicios y protocolos

Métodos de aplicación

El método de aplicación especifica el tipo de acceso del método de inicio de sesión. Los valores posibles incluyen `console`, `http`, `ontapi`, `rsh`, `snmp`, `service-processor`, `ssh`, y `telnet`.

Configurar este parámetro `service-processor` para otorgar al usuario acceso a Service Processor. Cuando este parámetro se define en `service-processor`, el `-authentication-method` parámetro se debe definir en `password` porque el procesador de servicios sólo admite la autenticación de contraseña. Las cuentas de usuario de SVM no pueden acceder a Service Processor. Por lo tanto, los operadores y administradores no pueden utilizar el `-vserver` parámetro cuando este parámetro se define en `service-processor`.

Para restringir aún más el acceso al `service-processor` comando, utilice el comando `system service-processor ssh add-allowed-addresses`. El comando `system service-processor api-service` se puede utilizar para actualizar las configuraciones y los certificados.

Por motivos de seguridad, Telnet y el Shell remoto (RSH) están deshabilitados de forma predeterminada porque NetApp recomienda el shell seguro (SSH) para el acceso remoto seguro. Si hay un requisito o una necesidad única de Telnet o RSH, deben estar activados.

El `security protocol modify` comando modifica la configuración existente en todo el cluster de RSH y Telnet. Active RSH y Telnet en el cluster definiendo el campo Activado en `true`.

Métodos de autenticación

El parámetro del método de autenticación especifica el método de autenticación utilizado para inicios de

sesión.

Método de autenticación	Descripción
`cert`	Autenticación de certificado SSL
`community`	Cadenas de comunidad SNMP
`domain`	Autenticación de Active Directory
`nsswitch`	Autenticación LDAP o NIS
`password`	Contraseña
`publickey`	Autenticación de clave pública
`usm`	Modelo de seguridad de usuario SNMP

No se recomienda el uso de NIS debido a las debilidades de seguridad del protocolo.

A partir de ONTAP 9,3, la autenticación encadenada de dos factores está disponible para cuentas SSH locales `admin` que utilizan `publickey` y contraseña como los dos métodos de autenticación. Además del `-authentication-method` campo del `security login` comando, se ha agregado un nuevo campo denominado `-second-authentication-method` . La clave pública o la contraseña se pueden especificar como `-authentication-method` o la `-second-authentication-method`. Sin embargo, durante la autenticación SSH, el orden es siempre clave pública con autenticación parcial, seguido de la solicitud de contraseña para la autenticación completa.

```
[user@host01 ~]$ ssh ontap.netapp.local
Authenticated with partial success.
Password:
cluster1::>
```

A partir de ONTAP 9,4, `nsswitch` se puede utilizar como un segundo método de autenticación con `publickey`.

A partir de ONTAP 9.12.1, FIDO2 también se puede usar para la autenticación SSH usando un dispositivo de autenticación de hardware YubiKey u otros dispositivos compatibles con FIDO2.

A partir de ONTAP 9,13.1:

- `domain` las cuentas se pueden utilizar como un segundo método de autenticación con `publickey`.
- Contraseña de un solo uso basada en tiempo (`totp`) es un código de acceso temporal generado por un algoritmo que utiliza la hora actual del día como uno de sus factores de autenticación para el segundo método de autenticación.
- La revocación de claves públicas es compatible con claves públicas SSH, así como con certificados que se comprobarán para su caducidad/revocación durante SSH.

Para obtener más información sobre la autenticación multifactor (MFA) para el administrador del sistema de ONTAP, Active IQ Unified Manager y SSH, consulte "TR-4647: Autenticación multifactor en ONTAP 9".

Cuentas administrativas predeterminadas

Se debe restringir la cuenta de administrador porque se permite el acceso al rol de administrador mediante todas las aplicaciones. La cuenta de diagnóstico (diag) permite acceder al shell del sistema y se debe reservar solo para que el soporte técnico realice tareas de solución de problemas.

Hay dos cuentas administrativas predeterminadas `admin` : Y `diag`.

Las cuentas huérfanas son un vector de seguridad importante que a menudo conduce a vulnerabilidades, incluida la escalada de privilegios. Se trata de cuentas innecesarias y no utilizadas que permanecen en el repositorio de cuentas de usuario. Son principalmente cuentas predeterminadas que nunca se usaron o para las que las contraseñas nunca se actualizaron o cambiaron. Para solucionar este problema, ONTAP admite la eliminación y el cambio de nombre de las cuentas.

ONTAP no puede eliminar ni cambiar el nombre de las cuentas integradas. Sin embargo, NetApp recomienda bloquear cualquier cuenta incorporada innecesaria con el comando lock.

Aunque las cuentas huérfanas son un problema de seguridad importante, NetApp recomienda probar el efecto de eliminar cuentas del repositorio de cuentas local.

Enumerar las cuentas locales

Para mostrar las cuentas locales, ejecute `security login show` el comando.

```
cluster1::*> security login show -vserver cluster1

Vserver: cluster1
                              Authentication              Acct   Is-Nsswitch
User/Group Name  Application Method    Role Name         Locked Group
---------------- ----------- --------- ----------------- ------ -----------
admin            console     password  admin             no     no
admin            http        password  admin             no     no
admin            ontapi      password  admin             no     no
admin            service-processor password admin        no     no
admin            ssh         password  admin             no     no
autosupport      console     password  autosupport       no     no
6 entries were displayed.
```

Elimine la cuenta de administrador predeterminada

La `admin` cuenta tiene el rol de administrador y se le permite el acceso utilizando todas las aplicaciones.

Pasos

1. Cree otra cuenta de nivel de administrador.

   Para eliminar por completo la cuenta predeterminada `admin` , primero debe crear otra cuenta de nivel de administrador que utilice la `console` aplicación de inicio de sesión.

Hacer estos cambios puede causar algunos efectos no deseados. Pruebe siempre los nuevos ajustes que puedan afectar el estado de seguridad de la solución en un clúster que no sea de producción primero.

Ejemplo:

```
cluster1::*> security login create -user-or-group-name NewAdmin
-application console -authentication-method password -vserver cluster1
```

```
cluster1::*> security login show -vserver cluster1

Vserver: cluster1
                             Authentication             Acct   Is-
Nsswitch
User/Group Name  Application Method    Role Name        Locked Group
---------------- ----------- --------- ---------------- ------
-----------
NewAdmin         console     password  admin            no     no
admin            console     password  admin            no     no
admin            http        password  admin            no     no
admin            ontapi      password  admin            no     no
admin            service-processor password admin       no     no
admin            ssh         password  admin            no     no
autosupport      console     password  autosupport      no     no
7 entries were displayed.
```

2. Después de crear la nueva cuenta de administrador, pruebe el acceso a esa cuenta con el `NewAdmin` inicio de sesión de la cuenta. Con la `NewAdmin` conexión, configure la cuenta para que tenga las mismas aplicaciones de conexión que la cuenta de administración predeterminada o anterior (por ejemplo, `http ontapi`, , `service-processor`o `ssh`). Este paso garantiza que se mantenga el control de acceso.

   Ejemplo:

```
cluster1::*> security login create -vserver cluster1 -user-or-group-name
NewAdmin -application ssh -authentication-method password
cluster1::*> security login create -vserver cluster1 -user-or-group-name
NewAdmin -application http -authentication-method password
cluster1::*> security login create -vserver cluster1 -user-or-group-name
NewAdmin -application ontapi -authentication-method password
cluster1::*> security login create -vserver cluster1 -user-or-group-name
NewAdmin -application service-processor -authentication-method password
```

3. Después de probar todas las funciones, puede desactivar la cuenta de administrador para todas las aplicaciones antes de eliminarla de ONTAP. Este paso sirve como prueba final para confirmar que no hay

funciones persistentes que se basen en la cuenta de administrador anterior.

```
cluster1::*> security login lock -vserver cluster1 -user-or-group-name
admin -application *
```

4. Para eliminar la cuenta de administrador predeterminada y todas las entradas para ella, ejecute el siguiente comando:

```
cluster1::*> security login delete -vserver cluster1 -user-or-group-name
admin -application *
cluster1::*> security login show -vserver cluster1

Vserver: cluster1
                             Authentication              Acct   Is-
Nsswitch
User/Group Name  Application Method    Role Name         Locked Group
---------------- ----------- --------- ----------------- ------
-----------
NewAdmin         console     password  admin             no     no
NewAdmin         http        password  admin             no     no
NewAdmin         ontapi      password  admin             no     no
NewAdmin         service-processor password admin        no     no
NewAdmin         ssh         password  admin             no     no
autosupport      console     password  autosupport       no     no
7 entries were displayed.
```

Establezca la contraseña de la cuenta de diagnóstico (diag)

El sistema de almacenamiento se proporciona una cuenta de diagnóstico llamada `diag` . Puede utilizar `diag` la cuenta para realizar tareas de solución de problemas en la `systemshell`. La `diag` cuenta es la única cuenta que se puede utilizar para acceder al systemshell a través del `diag` comando con privilegios `systemshell`.

> El systemshell y la cuenta asociada `diag` están pensados para fines de diagnóstico de bajo nivel. Su acceso requiere el nivel de privilegio de diagnóstico y se reserva solo para utilizarse con orientación del soporte técnico para realizar tareas de solución de problemas. Ni la `diag` cuenta ni la `systemshell` está destinada a fines administrativos generales.

Antes de empezar

Antes de acceder a `systemshell`, debe definir `diag` la contraseña de la cuenta mediante el `security login password` comando. Debe utilizar principios de contraseña seguros y cambiar la `diag` contraseña a intervalos regulares.

Pasos

1. Establezca `diag` la contraseña de usuario de la cuenta:

```
cluster1::> set -privilege diag

Warning: These diagnostic commands are for use by NetApp personnel only.
Do you want to continue? \{y|n}: y

cluster1::*> systemshell -node node-01
    (system node systemshell)
diag@node-01's password:

Warning: The system shell provides access to low-level
diagnostic tools that can cause irreparable damage to
the system if not used properly. Use this environment
only when directed to do so by support personnel.

node-01%
```

Verificación de varios administradores

A partir de ONTAP 9.11.1, puede usar la verificación multiadministrador (MAV) para permitir que ciertas operaciones, como la eliminación de volúmenes o copias de Snapshot, se ejecuten solo 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 MAV consiste en lo siguiente:

- "Crear uno o varios grupos de aprobación de administrador."
- "Habilitar la funcionalidad de verificación multi-administrador."
- "Adición o modificación de reglas."

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

Cuando MAV está activado, la realización de todas las operaciones protegidas requiere tres pasos:

1. Cuando un usuario inicia la operación, a. "se genera la solicitud."
2. Antes de que se pueda ejecutar, el número necesario de "Los administradores de MAV deben aprobar."
3. Después de la aprobación, el usuario completa la operación.

MAV no se ha diseñado para su uso con volúmenes o flujos de trabajo que implican una gran automatización, ya que cada tarea automatizada requiere aprobación antes de que se pueda completar la operación. Si desea utilizar la automatización y MAV conjuntamente, NetApp recomienda que utilice consultas para operaciones de MAV específicas. Por ejemplo, puede aplicar `volume delete` reglas MAV solo a volúmenes en los que la automatización no esté involucrada, y puede designar esos volúmenes con un esquema de nomenclatura particular.

Para obtener información más detallada sobre MAV, consulte la "Documentación de verificación

multiadministrador de ONTAP".

Bloqueo de copia de snapshot

El bloqueo de copia de Snapshot es una función de SnapLock en la que las copias de Snapshot se vuelven indelebles manual o automáticamente con un periodo de retención en la política de snapshots para volúmenes. El propósito del bloqueo de copias de Snapshot es impedir que los administradores malintencionados o que no sean de confianza eliminen snapshots en sistemas de ONTAP principales o secundarios.

Se introdujo el bloqueo de copias snapshot en ONTAP 9.12.1. El bloqueo de copia de SnapVault se conoce también como bloqueo de instantáneas a prueba de manipulaciones. Aunque requiere la licencia de SnapLock y la inicialización del reloj de cumplimiento de normativas, el bloqueo de copia de SnapShot no está relacionado con el cumplimiento de normativas de SnapLock ni con SnapLock Enterprise. No existe un administrador de almacenamiento de confianza, como sucede con SnapLock Enterprise y no protege la infraestructura de almacenamiento físico subyacente, como sucede con el cumplimiento de normativas de SnapLock. Esta es una mejora con respecto a la copia snapshot de SnapVault en un sistema secundario. Es posible lograr una rápida recuperación de copias Snapshot bloqueadas en sistemas principales para restaurar volúmenes dañados por el ransomware.

Si quiere más información sobre el bloqueo de copias snapshot, consulte "Documentación de ONTAP".

Configure el acceso de API basado en certificados

En lugar de utilizar la autenticación basada en certificado y el ID de usuario para la API de REST o el acceso de la API de SDK de capacidad de gestión de NetApp para ONTAP.

Como alternativa a la autenticación basada en certificados para la API de REST, utilice "Autenticación basada en token OAuth 2,0".)

Puede generar e instalar un certificado autofirmado en ONTAP, tal y como se describe en estos pasos.

Pasos

1. Con OpenSSL, genere un certificado ejecutando el siguiente comando:

```
openssl req -x509 -nodes -days 1095 -newkey rsa:2048 -keyout test.key
-out test.pem \> -subj "/C=US/ST=NC/L=RTP/O=NetApp/CN=cert_user"
Generating a 2048 bit RSA private key
..............+++
.........................+++
writing new private key to 'test.key'
```

   Este comando genera un certificado público denominado `test.pem` y una clave privada denominada `key.out`. El nombre común, CN, corresponde al ID de usuario de ONTAP.

2. Instale el contenido del certificado público en formato de correo mejorado de privacidad (pem) en ONTAP ejecutando el siguiente comando y pegando el contenido del certificado cuando se le solicite:

```
security certificate install -type client-ca -vserver cluster1

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

3. Active ONTAP para permitir el acceso del cliente a través de SSL y defina el ID de usuario para el acceso a la API.

```
security ssl modify -vserver cluster1 -client-enabled true
security login create -user-or-group-name cert_user -application ontapi
-authmethod cert -role admin -vserver cluster1
```

En el siguiente ejemplo, el ID de usuario `cert_user` ahora está habilitado para utilizar acceso a API autenticado con certificado. Un script de Python de SDK de gestión simple que utiliza `cert_user` para mostrar la versión de ONTAP aparece de la siguiente manera:

```
#!/usr/bin/python

import sys
sys.path.append("/home/admin/netapp-manageability-sdk-9.5/netapp-
manageability-sdk-9.5/lib/python/NetApp")
from NaServer import *

cluster = "cluster1"
transport = "HTTPS"
port = 443
style = "CERTIFICATE"
cert = "test.pem"
key = "test.key"

s = NaServer(cluster, 1, 30)
s.set_transport_type(transport)
s.set_port(port)
s.set_style(style)
s.set_server_cert_verification(0)
s.set_client_cert_and_key(cert, key)

api = NaElement("system-get-version")
output = s.invoke_elem(api)
if (output.results_status() == "failed"):
    r = output.results_reason()
    print("Failed: " + str(r))
    sys.exit(2)

ontap_version = output.child_get_string("version")
print ("V: " + ontap_version)
```

El resultado del script muestra la versión de ONTAP.

```
./version.py

V: NetApp Release 9.5RC1: Sat Nov 10 05:13:42 UTC 2018
```

4. Para realizar una autenticación basada en certificados con la API REST DE ONTAP, complete los siguientes pasos:
   a. En ONTAP, defina el ID de usuario para el acceso http:

```
security login create -user-or-group-name cert_user -application http
-authmethod cert -role admin -vserver cluster1
```

b. En su cliente Linux, ejecute el siguiente comando que genera la versión de ONTAP como resultado:

```
curl -k --cert-type PEM --cert ./test.pem --key-type PEM --key
./test.key -X GET "https://cluster1/api/cluster?fields=version"
{
    "version": {
        "full": "NetApp Release 9.7P1: Thu Feb 27 01:25:24 UTC 2020",
        "generation": 9,
        "major": 7,
        "minor": 0
    },
    "_links": {
        "self": {
            "href": "/api/cluster"
        }
    }
}
```

Más información

- "Autenticación basada en certificados con el SDK de capacidad de gestión de NetApp para ONTAP".

Autenticación basada en token OAuth 2,0 de ONTAP para la API de REST

Como alternativa a la autenticación basada en certificados, puede utilizar la autenticación basada en tokens OAuth 2,0 para la API REST.

A partir de ONTAP 9.14.1, 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.

Los tokens OAuth 2,0 reemplazan las contraseñas para la autenticación de cuentas de usuario.

Para obtener más información sobre el uso de OAuth 2,0, consulte la "Documentación de ONTAP sobre autenticación y autorización mediante OAuth 2,0".

Parámetros de inicio de sesión y contraseña

Una postura de seguridad efectiva se adhiere a las políticas organizativas establecidas, directrices y cualquier gobierno o estándares que se apliquen a la organización. Algunos ejemplos de estos requisitos incluyen la vida útil del nombre de usuario, los requisitos de longitud de contraseña, los requisitos de caracteres y el almacenamiento de dichas cuentas. La solución ONTAP ofrece características y funciones para abordar estos problemas de seguridad.

Nuevas funciones de cuenta local

Para admitir las políticas, directrices o estándares de cuentas de usuario de una organización, incluida la gobernanza, ONTAP admite las siguientes funciones:

- Configuración de políticas de contraseñas para aplicar un número mínimo de dígitos, caracteres en minúsculas o caracteres en mayúsculas
- Se requiere un retraso después de un intento fallido de inicio de sesión
- Definición del límite inactivo de la cuenta
- Vencimiento de una cuenta de usuario
- Mostrando un mensaje de advertencia de caducidad de contraseña
- Notificación de una conexión no válida

Los ajustes configurables se gestionan mediante el comando security login role config modify.

Compatibilidad con SHA-512

Para mejorar la seguridad de las contraseñas, ONTAP 9 admite la función hash de contraseña SHA-2 y utiliza por defecto SHA-512 para hash de contraseñas recién creadas o modificadas. Los operadores y administradores también pueden caducar o bloquear cuentas según sea necesario.

Las cuentas de usuario de ONTAP 9 preexistentes con contraseñas sin modificar siguen utilizando la función hash MD5 después de la actualización a ONTAP 9,0 o posterior. Sin embargo, NetApp recomienda encarecidamente que estas cuentas de usuario migren a la solución SHA-512 más segura al hacer que los usuarios cambien sus contraseñas.

La funcionalidad hash de contraseña le permite realizar las siguientes tareas:

- Muestra las cuentas de usuario que coinciden con la función hash especificada:

```
cluster1::*> security login show -user-or-group-name NewAdmin -fields
hash-function
vserver  user-or-group-name application authentication-method hash-
function
-------- ----------------- ----------- --------------------
-------------
cluster1 NewAdmin          console     password             sha512
cluster1 NewAdmin          ontapi      password             sha512
cluster1 NewAdmin          ssh         password             sha512
```

- Las cuentas Expire que utilizan una función hash especificada (por ejemplo, MD5), que obliga a los usuarios a cambiar sus contraseñas en el siguiente inicio de sesión:

```
cluster1::*> security login expire-password -vserver * -username * -hash
-function md5
```

- Bloquear cuentas con contraseñas que utilizan la función hash especificada.

```
cluster1::*> security login lock -vserver * -username * -hash-function
md5
```

La función hash de contraseña es desconocida para el usuario interno `autosupport` de la SVM administrativa del clúster. Este problema es cosmético. La función hash es desconocida porque este usuario interno no tiene una contraseña configurada por defecto.

- Para ver la función hash de contraseña del `autosupport` usuario, ejecute los siguientes comandos:

```
::> set advanced
::> security login show -user-or-group-name autosupport -instance

                    Vserver: cluster1
      User Name or Group Name: autosupport
                  Application: console
        Authentication Method: password
     Remote Switch IP Address: -
                    Role Name: autosupport
               Account Locked: no
                 Comment Text: -
      Whether Ns-switch Group: no
       Password Hash Function: unknown
Second Authentication Method2: none
```

- Para establecer la función hash de contraseña (valor por defecto: SHA512), ejecute el siguiente comando:

```
::> security login password -username autosupport
```

  No importa en qué se establezca la contraseña.

```
security login show -user-or-group-name autosupport -instance

                      Vserver: cluster1
      User Name or Group Name: autosupport
                  Application: console
        Authentication Method: password
     Remote Switch IP Address: -
                    Role Name: autosupport
               Account Locked: no
                 Comment Text: -
      Whether Ns-switch Group: no
       Password Hash Function: sha512
Second Authentication Method2: none
```

Parámetros de contraseña

La solución de ONTAP admite parámetros de contraseña que abordan los requisitos y las directrices de las políticas de la organización y los respaldan.

Atributo	Descripción	Predeterminado	Rango
`username-minlength`	Longitud mínima de nombre de usuario requerida	3	3-16
`username-alphanum`	Nombre de usuario alfanumérico	deshabilitado	Activado/Desactivado
`passwd-minlength`	Longitud mínima requerida de contraseña	8	3-64
`passwd-alphanum`	Contraseña alfanumérica	activado	Activado/Desactivado
`passwd-min-special-chars`	Número mínimo de caracteres especiales requeridos en la contraseña	0	0-64
`passwd-expiry-time`	Tiempo de caducidad de la contraseña (en días)	Ilimitado, lo que significa que las contraseñas nunca caducan	0-ilimitado 0 == vence ahora
`require-initial-passwd-update`	Requerir la actualización inicial de la contraseña en el primer inicio de sesión	Deshabilitado	Activado/Desactivado Cambios permitidos a través de la consola o SSH
`max-failed-login-attempts`	Número máximo de intentos fallidos	0, no bloquee la cuenta	-

Atributo	Descripción	Predeterminado	Rango
`lockout-duration`	Período máximo de bloqueo (en días)	El valor predeterminado es 0, lo que significa que la cuenta está bloqueada durante un día	-
`disallowed-reuse`	No permitir las últimas N contraseñas	6	El mínimo es 6
`change-delay`	Retraso entre cambios de contraseña (en días)	0	-
`delay-after-failed-login`	Retraso tras cada intento de inicio de sesión fallido (en segundos)	4	-
`passwd-min-lowercase-chars`	Número mínimo de caracteres alfabéticos en minúscula necesarios en la contraseña	0, que no requiere caracteres en minúsculas	0-64
`passwd-min-uppercase-chars`	Núm. Mínimo de caracteres alfabéticos en mayúsculas necesario	0, que no requiere caracteres en mayúsculas	0-64
`passwd-min-digits`	Número mínimo de dígitos necesarios en la contraseña	0, que no requiere dígitos	0-64
`passwd-expiry-warn-time`	Mostrar mensaje de advertencia antes del vencimiento de la contraseña (en días)	Ilimitado, lo que significa que nunca advierta sobre la caducidad de la contraseña	0, lo que significa advertir al usuario sobre la caducidad de la contraseña cada vez que se inicia sesión correctamente
`account-expiry-time`	La cuenta caduca en N días	Ilimitado, lo que significa que las cuentas nunca caducan	La hora de vencimiento de la cuenta debe ser mayor que el límite inactivo de la cuenta
`account-inactive-limit`	Duración máxima de la inactividad antes del vencimiento de la cuenta (en días)	Ilimitado, lo que significa que las cuentas inactivas nunca caducan	El límite inactivo de la cuenta debe ser inferior al tiempo de vencimiento de la cuenta

Ejemplo

```
cluster1::*> security login role config show -vserver cluster1 -role admin

                                          Vserver: cluster1
                                        Role Name: admin
                  Minimum Username Length Required: 3
                            Username Alpha-Numeric: disabled
                  Minimum Password Length Required: 8
                            Password Alpha-Numeric: enabled
Minimum Number of Special Characters Required in the Password: 0
                       Password Expires In (Days): unlimited
   Require Initial Password Update on First Login: disabled
                Maximum Number of Failed Attempts: 0
                    Maximum Lockout Period (Days): 0
                      Disallow Last 'N' Passwords: 6
            Delay Between Password Changes (Days): 0
     Delay after Each Failed Login Attempt (Secs): 4
Minimum Number of Lowercase Alphabetic Characters Required in the
Password: 0
Minimum Number of Uppercase Alphabetic Characters Required in the
Password: 0
Minimum Number of Digits Required in the Password: 0
Display Warning Message Days Prior to Password Expiry (Days): unlimited
                        Account Expires in (Days): unlimited
Maximum Duration of Inactivity before Account Expiration (Days): unlimited
```

A partir de 9.14.1, se aumenta la complejidad y las reglas de bloqueo de las contraseñas. Esto se aplica solo a las nuevas instalaciones de ONTAP.

Métodos de administración del sistema

Estos son parámetros importantes para fortalecer la administración del sistema ONTAP.

Acceso en línea de comandos

Establecer un acceso seguro a los sistemas es una parte fundamental del mantenimiento de una solución segura. Las opciones de acceso a la línea de comandos más comunes son SSH, Telnet y RSH. De estos, SSH es la mejor práctica más segura y estándar en el sector para el acceso remoto en línea de comandos. NetApp recomienda encarecidamente el uso de SSH para el acceso de línea de comandos a la solución ONTAP.

Configuraciones de SSH

El `security ssh show` comando muestra las configuraciones de los algoritmos de intercambio de claves SSH, los cifrados y los algoritmos MAC para el clúster y las SVM. El método de intercambio de claves utiliza estos algoritmos y cifrados para especificar cómo se generan las claves de sesión única para el cifrado y la

autenticación y cómo se lleva a cabo la autenticación del servidor.

```
cluster1::> security ssh show

Vserver       Ciphers       Key Exchange Algorithms     MAC Algorithms
--------  ----------------  --------------------------  --------------
nsadhanacluster-2
                aes256-ctr,   diffie-helman-group-      hmac-sha2-256
                aes192-ctr,    exchange-sha256,         hmac-sha2-512
                aes128-ctr    ecdh-sha2-nistp384
vs0             aes128-gcm    curve25519-sha256         hmac-sha1
vs1             aes256-ctr,   diffie-hellman-group-     hmac-sha1-96
                aes192-ctr,   exchange-sha256           hmac-sha2-256
                aes128-ctr,   ecdh-sha2-nistp384        hmac-sha2-256-
                3des-cbc,     ecdh-sha2-nistp512        etm
                aes128-gcm                              hmac-sha2-512
3 entries were displayed.
```

Banners de inicio de sesión

Los banners de inicio de sesión permiten a una organización presentar a cualquier operador, administradores e incluso a los intrusos los términos y condiciones de uso aceptable, e indican a quién se le permite acceder al sistema. Este enfoque es útil para establecer las expectativas de acceso y uso del sistema. El `security login banner modify` comando modifica el banner de inicio de sesión. El banner de inicio de sesión se muestra justo antes del paso de autenticación durante el proceso de inicio de sesión del dispositivo de la consola y SSH. El texto del banner debe estar entre comillas dobles (“ ”), como se muestra en el siguiente ejemplo.

```
cluster1::> security login banner modify -vserver cluster1 -message
“Authorized users ONLY!”
```

Parámetros del banner de inicio de sesión

Parámetro	Descripción
`vserver`	Use este parámetro para especificar la SVM con el banner modificado. Utilice el nombre de la SVM de administrador del clúster para modificar el mensaje de nivel del clúster. El mensaje del nivel del clúster se usa como predeterminado para las SVM de datos que no tienen un mensaje definido.

Parámetro	Descripción
`message`	Este parámetro opcional se puede usar para especificar un mensaje de banner de inicio de sesión. Si el clúster tiene establecido un mensaje de banner de inicio de sesión, todas las SVM de datos también utilizan el banner de inicio de sesión del clúster. Al configurar el banner de inicio de sesión de una SVM de datos, se anula la visualización del banner de inicio de sesión del clúster. Para restablecer un banner de inicio de sesión de SVM de datos y usar el banner de inicio de sesión del clúster, use este parámetro con el valor «-». Si utiliza este parámetro, el banner de inicio de sesión no puede contener nuevas líneas (también conocidas como ends of lines [EOLs] o saltos de línea). Para introducir un mensaje de banner de inicio de sesión con nuevas líneas, no especifique ningún parámetro. Se le pedirá que introduzca el mensaje de forma interactiva. Los mensajes introducidos de forma interactiva pueden contener nuevas líneas. Los caracteres no ASCII deben utilizar Unicode UTF-8.
`uri`	`(ftp
http):///(hostname	IPv4` Utilice este parámetro para especificar el URI desde el cual se descarga el banner de inicio de sesión. El mensaje no debe superar los 2048 bytes de longitud. Los caracteres no ASCII se deben proporcionar como Unicode UTF-8.

Mensaje del día

El `security login motd modify` comando actualiza el mensaje del día (MOTD).

Hay dos categorías de MOTD: El MOTD a nivel de clúster y el MOTD a nivel de SVM de datos. Un usuario que inicie sesión en el clustershell de una SVM de datos puede ver dos mensajes: El MOTD a nivel de clúster seguido por el MOTD a nivel de SVM para esa SVM.

El administrador del clúster puede habilitar o deshabilitar el MOTD a nivel de clúster en cada SVM de forma individual si es necesario. Si el administrador del clúster deshabilita el MOTD a nivel de clúster para una SVM, el usuario que inicie sesión en la SVM no verá el mensaje a nivel de clúster. Solo un administrador del clúster puede habilitar o deshabilitar el mensaje a nivel del clúster.

Parámetro MOTD	Descripción
Vserver	Utilice este parámetro para especificar la SVM para la que se modifica el MOTD. Utilice el nombre de la SVM de administrador del clúster para modificar el mensaje de nivel del clúster.

Parámetro MOTD	Descripción
mensaje	Este parámetro opcional se puede utilizar para especificar un mensaje. Si utiliza este parámetro, MOTD no puede contener nuevas líneas. Si no especifica ningún parámetro que no sea el `-vserver` parámetro, se le pedirá que introduzca el mensaje de forma interactiva. Los mensajes introducidos de forma interactiva pueden contener nuevas líneas. Los caracteres no ASCII se deben proporcionar como Unicode UTF-8. El mensaje puede contener contenido generado dinámicamente mediante las siguientes secuencias de escape: • `\\` - Un solo carácter de contragolpe • `\b` - Sin salida (compatible solo con Linux) • `\C` - Nombre del clúster • `\d` - Fecha actual como se establece en el nodo de inicio de sesión • `\t` - Hora actual como se establece en el nodo de inicio de sesión • `\I` - Dirección IP de LIF entrante (imprime la consola para un `console` inicio de sesión) • `\l` - Nombre del dispositivo de inicio de sesión (imprime la consola para un `console` inicio de sesión) • `\L` - Último login para el usuario en cualquier nodo del cluster • `\m` - Arquitectura de la máquina • `\n` - Nodo o nombre de SVM de datos • `\N` - Nombre del usuario que inicia sesión • `\o` - Igual que \O. Suministrado para compatibilidad con Linux. • `\O` - Nombre de dominio DNS del nodo. Tenga en cuenta que la salida depende de la configuración de red y puede estar vacía. • `\r` - Número de versión de software • `\s` - Nombre del sistema operativo • `\u` - Número de sesiones de clustershell activas en el nodo local. Para el administrador de clúster: Todos los usuarios de clustershell. Para el administrador de SVM de datos: Solo sesiones activas para esa SVM de datos. • `\U` - Igual que `\u`, pero tiene `user` o `users` anexado • `\v` - Cadena efectiva de la versión del clúster • `\W` - Sesiones activas en todo el clúster para el usuario que inicia sesión (`who`)

Para obtener más información sobre la configuración del mensaje del día en ONTAP, consulte la "Documentación de ONTAP sobre el mensaje del día".

Tiempo de espera de sesión de la CLI

El tiempo de espera predeterminado de la sesión de la CLI es de 30 minutos. El tiempo de espera es importante para evitar sesiones obsoletas y el respaldo continuo de sesiones.

Utilice `system timeout show` el comando para ver el tiempo de espera actual de la sesión de la CLI. Para configurar el valor de tiempo de espera, utilice `system timeout modify -timeout <minutes>` el comando.

Acceso web con System Manager de NetApp ONTAP

Si un administrador de ONTAP prefiere usar una interfaz gráfica en lugar de la CLI para acceder a un clúster y gestionarlo, use el administrador del sistema de NetApp ONTAP. Se incluye con ONTAP como servicio web, habilitado de forma predeterminada, y accesible mediante un navegador. Dirija el navegador al nombre de host si utiliza DNS o la dirección IPv4 o IPv6 a través de `https://cluster-management-LIF`.

Si el clúster utiliza un certificado digital autofirmado, es posible que el explorador muestre una advertencia que indica que el certificado no es de confianza. Puede reconocer el riesgo para continuar con el acceso o instalar un certificado digital firmado por una entidad de certificación (CA) en el clúster para la autenticación del servidor.

A partir de ONTAP 9,3, la autenticación del lenguaje de marcado de aserción de seguridad (SAML) es una opción para ONTAP System Manager.

Autenticación SAML para ONTAP System Manager

SAML 2,0 es un estándar de la industria ampliamente adoptado que permite a cualquier proveedor de identidad (IDP) que cumpla con SAML de terceros realizar MFA utilizando mecanismos únicos para el IDP que elija la empresa y como fuente de inicio de sesión único (SSO).

Hay tres roles definidos en la especificación SAML: El principal, el IdP y el proveedor de servicios. En la implementación de ONTAP, un principal es el administrador del clúster que obtiene acceso a ONTAP mediante ONTAP System Manager o NetApp Active IQ Unified Manager. El IdP es un software IdP de terceros. A partir de ONTAP 9,3, los Servicios Federados de Active Directory de Microsoft (ADFS) y el IdP de código abierto Shibboleth son compatibles. A partir de ONTAP 9.12.1, Cisco DUO es un IDP compatible. El proveedor de servicios es la funcionalidad SAML integrada en ONTAP que utiliza ONTAP System Manager o la aplicación web Active IQ Unified Manager.

A diferencia del proceso de configuración de dos factores de SSH, una vez que se activa la autenticación SAML, el acceso de ONTAP System Manager o Service Processor de ONTAP requiere que todos los administradores existentes se autentiquen mediante el IdP de SAML. No es necesario realizar cambios en las cuentas de usuario del clúster. Cuando se habilita la autenticación SAML, se añade un nuevo método de autenticación de `saml` a los usuarios existentes con roles de administrador para `http` y `ontapi` aplicaciones.

Una vez habilitada la autenticación SAML, es necesario definir cuentas nuevas adicionales que requieren acceso SAML IdP en ONTAP con el rol de administrador y el método de autenticación saml para `http` las aplicaciones y `ontapi` . Si la autenticación SAML está deshabilitada en algún momento, estas cuentas nuevas requieren que el `password` método de autenticación se defina con el rol de administrador para `http` las aplicaciones y `ontapi` y la adición de la aplicación de consola para la autenticación ONTAP local en el administrador de sistema de ONTAP.

Una vez habilitado el IdP de SAML, el IdP realiza la autenticación para el acceso de ONTAP System Manager mediante los métodos disponibles para IdP, como el protocolo ligero de acceso a directorios (LDAP), Active Directory (AD), Kerberos, contraseña, etc. Los métodos disponibles son únicos para el IdP. Es importante que las cuentas configuradas en ONTAP tengan ID de usuario que se asignen a los métodos de autenticación de IdP.

Los IDP validados por NetApp son Microsoft ADFS, Cisco DUO y Shibboleth IDP de código abierto.

A partir de ONTAP 9.14.1, Cisco DUO se puede utilizar como un segundo factor de autenticación para SSH.

Para obtener más información sobre MFA para el administrador del sistema de ONTAP, Active IQ Unified Manager y SSH, consulte "TR-4647: Autenticación multifactor en ONTAP 9".

Información de System Manager de ONTAP

A partir de ONTAP 9.11.1, System Manager de ONTAP proporciona información para ayudar a los administradores de clúster a simplificar sus tareas diarias. La información sobre seguridad se basa en las recomendaciones de este informe técnico.

Información sobre seguridad	Determinación
Telnet está activado	NetApp recomienda Secure Shell (SSH) para el acceso remoto seguro.
Shell remoto (RSH) está activado	NetApp recomienda SSH para un acceso remoto seguro.
AutoSupport está utilizando un protocolo no seguro	AutoSupport no está configurado para ser enviado a través de enlace:HTTPS.
El banner de inicio de sesión no está configurado en el clúster a nivel del clúster	Advertencia si el banner de inicio de sesión no está configurado para el clúster.
SSH está utilizando cifrados no seguros	Advertencia si SSH utiliza cifrados no seguros.
Hay muy pocos servidores NTP configurados	Advertencia si el número de servidores NTP configurados es inferior a tres.
El usuario administrador predeterminado no está bloqueado	Cuando no se utiliza ninguna cuenta administrativa predeterminada (admin o diag) para iniciar sesión en System Manager y estas cuentas no están bloqueadas, la recomendación es bloquearlas.
Defensa contra ransomware: Los volúmenes no tienen políticas Snapshot	No hay una política de Snapshot adecuada anexada a uno o varios volúmenes.
Protección contra ransomware: Desactiva la eliminación automática de SnapVault	La eliminación automática de Snapshot se establece para uno o varios volúmenes.
No se supervisan los volúmenes de ataques de ransomware	Diversos volúmenes son compatibles con la protección contra ransomware autónoma, pero no configurados todavía.
Las SVM no están configuradas para la protección autónoma contra ransomware	La protección autónoma contra ransomware es compatible con varias SVM, pero aún no configurada.
FPolicy nativo no configurado	FPolicy no está establecido para SVM NAS.
Habilita el modo activo de protección autónoma contra ransomware	Varios volúmenes completaron el modo de aprendizaje y se puede activar el modo activo
El cumplimiento de la normativa global FIPS 140-2 está desactivado	El cumplimiento de la normativa global FIPS 140-2 no está activado.
El clúster no está configurado para notificaciones	Los correos electrónicos, los WebHooks o los hosts de capturas de SNMP no están configurados para recibir notificaciones.

Para obtener más información acerca de los detalles de ONTAP System Manager, consulte la "Documentación de información de System Manager de ONTAP".

Protección autónoma contra ransomware de ONTAP

Para complementar el análisis del comportamiento de los usuarios para la Seguridad de las cargas de trabajo de almacenamiento, la protección autónoma frente al ransomware de ONTAP analiza las cargas de trabajo de volumen y la entropía para detectar el ransomware y realiza una copia Snapshot y notifica al administrador cuando se sospecha de un ataque.

Además de la detección y la prevención de ransomware mediante análisis externos de comportamiento del usuario de FPolicy (UBA) con NetApp Cloud Insights / Cloud Secure y el ecosistema de partners de FPolicy de NetApp, ONTAP 9.10.1 introduce una protección autónoma contra el ransomware. La protección autónoma frente al ransomware de ONTAP usa una funcionalidad de aprendizaje automático integrado (ML) que examina la actividad de carga de trabajo del volumen y la entropía de datos para detectar automáticamente el ransomware. Monitorea la actividad que es diferente de UBA para que pueda detectar ataques que UBA no lo hace.

Para obtener información más detallada sobre esta capacidad, consulte "TR-4572: La solución de NetApp para ransomware" o la "Documentación autónoma de protección contra ransomware de ONTAP"sección .

Auditoría del sistema de administración de almacenamiento

Asegure la integridad de la auditoría de eventos descargando eventos de ONTAP en un servidor syslog remoto. Este servidor podría ser un sistema de gestión de eventos de información de seguridad como Splunk.

Enviar syslog

La información de registro y auditoría es muy valiosa para las organizaciones desde el punto de vista del soporte y la disponibilidad. Además, la información y los detalles que contienen los registros (syslog) y los informes y resultados de auditorías suelen ser de carácter confidencial. Para mantener los controles y la política de seguridad, es imprescindible que las organizaciones gestionen los datos de registro y auditoría de forma segura.

Descargar la información de syslog es necesario para limitar el alcance o la huella de una intrusión en un solo sistema o solución. Por ello, NetApp recomienda descargar la información de syslog de forma segura en una ubicación segura de almacenamiento o retención.

Cree un destino de reenvío de logs

Utilice `cluster log-forwarding create` el comando para crear destinos de reenvío de registros para el registro remoto.

Parámetros

Use los siguientes parámetros para configurar `cluster log-forwarding create` el comando:

- **Destino host.** Este nombre es el nombre de host o la dirección IPv4 o IPv6 del servidor al que desea reenviar los logs.

```
-destination <Remote InetAddress>
```

- **Puerto de destino.** Este es el puerto en el que recibe el servidor de destino.

```
[-port <integer>]
```

- **Protocolo de reenvío de registros.** Este protocolo se utiliza para enviar mensajes al destino.

```
[-protocol \{udp-unencrypted|tcp-unencrypted|tcp-encrypted}]
```

  El protocolo de reenvío de registros puede usar uno de los valores siguientes:

  - `udp-unencrypted`. Protocolo de datagramas de usuario sin seguridad.
  - `tcp-unencrypted`. TCP sin seguridad.
  - `tcp-encrypted`. TCP con seguridad de la capa de transporte (TLS).
- **Verificar la identidad del servidor de destino.** Cuando este parámetro se define en TRUE, la identidad del destino de reenvío de logs se verifica validando su certificado. El valor se puede establecer en verdadero sólo cuando se selecciona el valor en `tcpencrypted` el campo de protocolo.

```
[-verify-server \{true|false}]
```

- **Instalación Syslog.** Este valor es la utilidad syslog que se debe utilizar para los registros reenviados.

```
[-facility <Syslog Facility>]
```

- **Salte la prueba de conectividad.** Normalmente, el `cluster log-forwarding create` comando comprueba que se puede acceder al destino enviando un ping de protocolo de mensajes de control de Internet (ICMP) y genera un error si no se puede acceder a él. Al definir este valor `true` se omite la comprobación de ping para que pueda configurar el destino cuando no se pueda acceder a él.

```
[-force [true]]
```

NetApp recomienda el uso `cluster log-forwarding` del comando para forzar la conexión a un `-tcp-encrypted` tipo.

Notificación de eventos

Proteger la información y los datos que salen de un sistema es vital para mantener y gestionar la política de seguridad del sistema. Los eventos generados por la solución de ONTAP ofrecen una gran cantidad de información acerca de qué se encuentra la solución, la información procesada y mucho más. La vitalidad de estos datos destaca la necesidad de gestionarlos y migrarlos de forma segura.

El `event notification create` comando envía una nueva notificación de un conjunto de eventos definidos por un filtro de eventos a uno o más destinos de notificación. Los siguientes ejemplos muestran la

configuración de notificaciones de eventos y `event notification show` el comando, que muestra los filtros y los destinos de notificación de eventos configurados.

```
cluster1::> event notification create -filter-name filter1 -destinations
 email_dest,syslog_dest,snmp-traphost

cluster1::> event notification show
ID     Filter Name       Destinations
-----  ----------------  -----------------
1 filter1 email_dest, syslog_dest, snmp-traphost
```

Cifrado del almacenamiento

Para proteger los datos confidenciales en caso de que un disco sea robado, devuelto o reasignado mediante el cifrado de almacenamiento de NetApp basado en hardware o el cifrado de volúmenes de NetApp basado en software/el cifrado de agregados de NetApp. Ambos mecanismos son validados FIPS-140-2 y cuando se utilizan mecanismos basados en hardware con mecanismos basados en software, la solución califica para el programa de soluciones comerciales para clasificados (CSfC). Permite una protección de seguridad mejorada para los datos secretos y secretos en reposo, tanto a nivel de hardware como de software.

El cifrado de datos en reposo es importante para proteger los datos confidenciales en caso de robo, devolución o reasignación de un disco.

ONTAP 9 cuenta con tres soluciones de cifrado de datos en reposo conforme a la normativa FIPS 140-2:

- El cifrado en almacenamiento de NetApp (NSE) es una solución de hardware que usa unidades de autocifrado.
- El cifrado de volúmenes de NetApp (NVE) es una solución de software que permite el cifrado de cualquier volumen de datos en cualquier tipo de unidad, donde se habilita con una clave única para cada volumen.
- El cifrado de agregados de NetApp (NAE) es una solución de software que permite el cifrado de cualquier volumen de datos en cualquier tipo de unidad, donde se habilita con claves únicas para cada agregado.

NSe, NVE y NAE pueden usar la gestión de claves externa o el gestor de claves incorporado (OKM). El uso de NSE, NVE y NAE no afecta a las funciones de eficiencia del almacenamiento de ONTAP. Sin embargo, los volúmenes NVE se excluyen de la deduplicación de agregados. Los volúmenes NAE participan en la deduplicación agregada y se benefician de ella.

OKM proporciona una solución de cifrado independiente para datos en reposo con NSE, NVE o NAE.

NVE, NAE y OKM usan el CryptoMod de ONTAP. CryptoMod aparece en la lista CMVP de módulos validados FIPS 140-2-2. Consulte "Certificado FIPS 140-2 n.o 4144".

Para iniciar la configuración de OKM, utilice el `security key-manager onboard enable` comando. Para configurar gestores de claves del protocolo de interoperabilidad de gestión de claves (KMIP) externas, utilice `security key-manager external enable` el comando. A partir de ONTAP 9,6, se admite el multi-tenancy para los gestores de claves externos. Utilice el `-vserver <vserver name>` parámetro para

habilitar la gestión de claves externa para una SVM específica. Antes de 9,6, el `security key-manager setup` comando se utilizaba para configurar OKM y gestores de claves externos. Para la gestión de claves incorporada, esta configuración guía al operador o administrador a través de la configuración de la clave de acceso y los parámetros adicionales para la configuración de OKM.

En el siguiente ejemplo se proporciona una parte de la configuración:

```
cluster1::> security key-manager setup
Welcome to the key manager setup wizard, which will lead you through
the steps to add boot information.

Enter the following commands at any time
"help" or "?" if you want to have a question clarified,
"back" if you want to change your answers to previous questions, and
"exit" if you want to quit the key manager setup wizard. Any changes
you made before typing "exit" will be applied.

Restart the key manager setup wizard with "security key-manager setup". To
accept a default
or omit a question, do not enter a value.

Would you like to configure onboard key management? {yes, no} [yes]:
Enter the cluster-wide passphrase for onboard key management. To continue
the configuration, enter the passphrase, otherwise
type "exit":
Re-enter the cluster-wide passphrase:
After configuring onboard key management, save the encrypted configuration
data
in a safe location so that you can use it if you need to perform a manual
recovery
operation. To view the data, use the “security key-manager backup show”
command.
```

A partir de ONTAP 9,4, puede utilizar `-enable-cc-mode` la opción true con `security key-manager setup` para solicitar que los usuarios introduzcan la frase de acceso después de un reinicio. Para ONTAP 9,6 y versiones posteriores, la sintaxis del comando es `security key-manager onboard enable -cc -mode-enabled yes`.

A partir de ONTAP 9,4, se puede utilizar esta `secure-purge` función con privilegios avanzados para «restregar» datos de forma no disruptiva en los volúmenes habilitados para NVE. El barrido de datos en un volumen cifrado garantiza que no puedan recuperarse del medio físico. El siguiente comando purga de forma segura los archivos eliminados en vol1 en la SVM VS1:

```
cluster1::> volume encryption secure-purge start -vserver vs1 -volume vol1
```

A partir de ONTAP 9,7, NAE y NVE se habilitan de forma predeterminada si la licencia VE está vigente, se configuran OKM o los gestores de claves externos y NSE no se utiliza. Los volúmenes NAE se crean de forma

predeterminada en los agregados de NAE, y los volúmenes NVE se crean de forma predeterminada en agregados no NAE. Para anular esto, introduzca el siguiente comando:

```
cluster1::*> options -option-name
encryption.data_at_rest_encryption.disable_by_default true
```

A partir de ONTAP 9,6, se puede usar un ámbito de SVM para configurar la gestión de claves externa para una SVM de datos en el clúster. Esto es mejor para entornos multi-tenant en los que cada inquilino utiliza un SVM diferente (o un conjunto de SVM) para servir datos. Solo el administrador de SVM para un inquilino determinado tiene acceso a las claves de ese inquilino. Para obtener más información, consulte "Habilite la gestión de claves externa en ONTAP 9,6 y versiones posteriores" en la documentación de ONTAP.

A partir de ONTAP 9.11.1, puede configurar la conectividad con servidores de gestión de claves externos en clúster mediante la designación de servidores de claves primarios y secundarios en una SVM. Para obtener más información, consulte "configurar servidores de claves externas en clúster" en la documentación de ONTAP.

A partir de ONTAP 9.13.1, es posible configurar servidores del administrador de claves externos en System Manager. Para obtener más información, consulte "Gestione gestores de claves externos" en la documentación de ONTAP.

Cifrado de la replicación de datos

Para complementar el cifrado de datos en reposo, puede cifrar el tráfico de replicación de datos ONTAP entre clústeres usando TLS 1,2 con una clave precompartida para SnapMirror, SnapVault o FlexCache.

Al replicar datos para recuperación ante desastres, almacenamiento en caché o backup, debe proteger esos datos durante el transporte por el cable de un clúster de ONTAP a otro. De este modo, se evitan ataques maliciosos de tipo man-in-the-middle contra datos confidenciales mientras están en movimiento.

A partir de ONTAP 9,6, el cifrado de paridad de clústeres proporciona compatibilidad de cifrado TLS 1,2 AES-256 GCM para funciones de replicación de datos de ONTAP como SnapMirror, SnapVault y FlexCache. El cifrado se configura mediante una clave precompartida (PSK) entre dos pares de clústeres.

Los clientes que usan tecnologías como NSE, NVE y NAE para proteger los datos en reposo también pueden usar el cifrado de datos integral al actualizar a ONTAP 9,6 o una versión posterior para usar el cifrado de paridad de clústeres.

Cluster peering cifra todos los datos entre los pares de los clústeres. Por ejemplo, cuando se utiliza SnapMirror, toda la información de paridad y todas las relaciones de SnapMirror entre la paridad de clústeres de origen y de destino quedan cifradas. No se pueden enviar datos de texto claro entre pares de clústeres con el cifrado de interconexión de clústeres entre iguales habilitado.

A partir de ONTAP 9,6, las nuevas relaciones de paridad de clústeres tienen el cifrado habilitado de forma predeterminada. Para habilitar el cifrado en relaciones de paridad de clústeres que se crearon antes de ONTAP 9,6, debe actualizar el clúster de origen y de destino a 9,6. Además, debe usar el `cluster peer modify` comando para cambiar los pares de los clústeres de origen y de destino para usar el cifrado de interconexión de clústeres.

Puede convertir una relación entre iguales existente para usar el cifrado de interconexión de clústeres en ONTAP 9,6, como se muestra en el siguiente ejemplo:

```
On the Destination Cluster Peer

cluster2::> cluster peer modify cluster1 -auth-status-admin use-
authentication -encryption-protocol-proposed tls-psk

When prompted enter a passphrase.

On the Source Cluster Peer

cluster1::> cluster peer modify cluster2 -auth-status-admin use-
authentication -encryption-protocol-proposed tls-psk

When prompted enter the same passphrase you created in the previous step.
```

Cifrado de datos en tránsito IPsec

Los clientes que usan tecnologías de cifrado de datos en reposo como el cifrado del almacenamiento de NetApp (NSE) o el cifrado de volúmenes de NetApp (NVE) y el cifrado de paridad de clústeres (CPE) para el tráfico de replicación de datos ahora pueden utilizar el cifrado de extremo a extremo entre el cliente y el almacenamiento en su estructura de datos multicloud híbrida actualizando a ONTAP 9,8 o versiones posteriores, y utilizando IPSec. IPSec ofrece una alternativa al cifrado NFS o SMB/CIFS y es la única opción de cifrado en tránsito para el tráfico iSCSI.

En algunas situaciones, es posible que haya un requisito de proteger todos los datos de clientes transportados a través del cable (o en tránsito) hacia la SVM de ONTAP. De este modo, se evita la repetición y los ataques maliciosos de intermediario contra datos confidenciales mientras están en movimiento.

A partir de ONTAP 9,8, el protocolo de seguridad de Internet (IPsec) ofrece compatibilidad con cifrado integral para todo el tráfico IP entre un cliente y una SVM de ONTAP. El cifrado de datos IPSec para todo el tráfico IP incluye protocolos NFS, iSCSI y SMB/CIFS. IPSec proporciona la única opción de cifrado en vuelo para el tráfico iSCSI.

Proporcionar cifrado NFS por cable es uno de los casos de uso principales de IPsec. Antes de ONTAP 9,8, el cifrado por cable NFS requería la configuración y la configuración de Kerberos para utilizar krb5p para cifrar datos NFS en tránsito. No siempre es sencillo ni fácil de lograr en todos los entornos del cliente.

Los clientes que usan tecnologías de cifrado de datos en reposo como el cifrado del almacenamiento de NetApp (NSE) o el cifrado de volúmenes de NetApp (NVE) y el cifrado de paridad de clústeres (CPE) para el tráfico de replicación de datos ahora pueden utilizar el cifrado de extremo a extremo entre el cliente y el almacenamiento en su estructura de datos multicloud híbrida actualizando a ONTAP 9,8 o versiones posteriores, y utilizando IPSec.

IPSec es un estándar IETF. ONTAP utiliza IPsec en modo de transporte. También aprovecha la versión 2 del protocolo de intercambio de claves de Internet (IKE), que utiliza una clave precompartida (PSK) para negociar material clave entre el cliente y ONTAP con IPv4 o IPv6. De forma predeterminada, IPsec utiliza el cifrado Suite-B AES-GCM de 256 bits. Suite-B AES-GMAC256 y AES-CBC256 con cifrado de 256 bits también son compatibles.

Aunque la funcionalidad IPsec debe estar habilitada en el clúster, se aplica a direcciones IP de SVM individuales mediante el uso de una entrada de base de datos de política de seguridad (SPD). La entrada de directiva (SPD) contiene la dirección IP del cliente (subred IP remota), la dirección IP de SVM (subred IP local), el conjunto de cifrado que se va a utilizar y el secreto precompartido (PSK) necesario para autenticarse a través de IKEv2 y establecer la conexión IPsec. Además de la entrada de directiva IPsec, el cliente debe configurarse con la misma información (IP local y remota, PSK y conjunto de cifrado) antes de que el tráfico pueda fluir a través de la conexión IPsec. A partir de ONTAP 9.10.1, se añade el soporte de autenticación de certificados IPsec. Esto elimina los límites de la política IPsec y activa el soporte del sistema operativo Windows para IPsec.

Si hay un firewall entre el cliente y la dirección IP de SVM, debe permitir los protocolos ESP y UDP (puertos 500 y 4500), tanto de entrada (entrada) como de salida (salida), para que la negociación IKEv2 se realice correctamente y, por lo tanto, permita el tráfico IPsec.

Para el cifrado de tráfico de paridad de clústeres y SnapMirror de NetApp, se recomienda el cifrado de pares de clústeres (CPE) en IPsec para garantizar una seguridad en tránsito por la red. CPE tiene un mejor rendimiento para estas cargas de trabajo que IPsec. No necesita una licencia para IPsec y no hay restricciones de importación o exportación.

Puede habilitar IPsec en el clúster y crear una entrada SPD para un único cliente y una única dirección IP SVM, como se muestra en el siguiente ejemplo:

```
On the Destination Cluster Peer

cluster1::> security ipsec config modify -is-enabled true

cluster1::> security ipsec policy create -vserver vs1 -name test34 -local
-ip-subnets 192.168.134.34/32 -remote-ip-subnets 192.168.134.44/32

When prompted enter and confirm the pre shared secret (PSK).
```

Gestión TLS y SSL

Puede habilitar el modo de cumplimiento de FIPS 140-2/3 para las interfaces del plano de control mediante el establecimiento del `is-fips-enabled` parámetro en true con el comando ONTAP `security config modify` .

A partir de ONTAP 9, puede habilitar el modo de cumplimiento normativo FIPS 140-2 para las interfaces en el plano de control de todo el clúster. De manera predeterminada, se deshabilita el modo FIPS 140-2-only. Puede habilitar el modo de cumplimiento de FIPS 140-2 estableciendo `is-fips-enabled` el parámetro en `true` para el `security config modify` comando. A continuación, puede utilizar `security config show command` para confirmar el estado en línea.

Cuando se habilita el cumplimiento FIPS 140-2, TLSv1 y SSLv3 están deshabilitados y solo TLSv1.1 y TLSv1.2 permanecen habilitados. ONTAP evita que habilite TLSv1 y SSLv3 cuando el cumplimiento de FIPS 140-2 está habilitado. Si habilita FIPS 140-2 y luego la deshabilita posteriormente, TLSv1 y SSLv3 seguirán deshabilitados, pero TLSv1,2 o TLSv1,1 y TLSv1,2 permanecerán habilitados, según la configuración anterior.

El `security config modify` comando modifica la configuración de seguridad existente en todo el clúster. Si habilita el modo conforme a FIPS, el clúster selecciona automáticamente solo los protocolos TLS. Utilice el

`-supported-protocols` parámetro para incluir o excluir protocolos TLS independientemente del modo FIPS. De forma predeterminada, el modo FIPS está deshabilitado y ONTAP admite los protocolos TLSv1,2, TLSv1,1 y TLSv1.

Para obtener compatibilidad con versiones anteriores, ONTAP admite añadir SSLv3 a la `supported-protocols` lista cuando se deshabilita el modo FIPS. Use `-supported-cipher-suites` el parámetro para configurar solo el estándar de cifrado avanzado (AES) o AES y 3DES. También puede desactivar los cifrados débiles como RC4 especificando !RC4. Por defecto, el valor de cifrado soportado es `ALL:!LOW:!aNULL:!EXP:!eNULL`. Esta configuración significa que todos los conjuntos de cifrado admitidos para los protocolos están habilitados, excepto los que no tienen autenticación, ningún cifrado, ninguna exportación y conjuntos de cifrado de bajo cifrado. Se trata de suites que utilizan algoritmos de cifrado de 64 o 56 bits.

Seleccione un conjunto de cifrado que esté disponible con el protocolo seleccionado correspondiente. Una configuración no válida puede provocar que algunas funcionalidades no funcionen correctamente.

Para obtener la sintaxis correcta de la cadena de cifrado, consulte la "cifrados" página en OpenSSL (publicada por la base de software OpenSSL). A partir de ONTAP 9.9.1 y versiones posteriores, ya no es necesario reiniciar todos los nodos manualmente después de modificar la configuración de seguridad.

La habilitación del cumplimiento FIPS 140-2 tiene efectos en otros sistemas y comunicaciones internos y externos a ONTAP 9. NetApp recomienda encarecidamente probar esta configuración en un sistema no de producción que tenga acceso a la consola.

Si se utiliza SSH para administrar ONTAP 9, debe utilizar un cliente OpenSSH 5,7 o posterior. Los clientes SSH deben negociar con el algoritmo de clave pública del algoritmo de firma digital de curva elíptica (ECDSA) para que la conexión sea exitosa.

La seguridad TLS puede reforzarse aún más si solo habilita TLS 1,2 y utiliza conjuntos de cifrado compatibles con el secreto directo perfecto (PFS). PFS es un método de intercambio de claves que, cuando se utiliza en combinación con protocolos de cifrado como TLS 1,2, ayuda a evitar que un atacante descifre todas las sesiones de red entre un cliente y un servidor. Para habilitar sólo conjuntos de cifrados compatibles con TLS 1,2 y PFS, utilice el `security config modify` comando del nivel de privilegio avanzado como se muestra en el siguiente ejemplo.

Antes de cambiar la configuración de la interfaz SSL, es importante recordar que el cliente debe admitir el cifrado mencionado (DHE, ECDHE) al conectarse a ONTAP. De lo contrario, no se permite la conexión.

```
cluster1::*> security config modify -interface SSL -supported-protocols
TLSv1.2 -supported-cipher-suites
PSK:DHE:ECDHE:!LOW:!aNULL:!EXP:!eNULL:!3DES:!kDH:!kECDH
```

Confirmar `y` para cada petición de datos. Para obtener más información sobre PFS, consulte "Este blog de NetApp".

Desde el soporte de ONTAP 9.11.1 y TLS 1,3, puede validar FIPS 140-3.

La configuración FIPS se aplica a ONTAP y a la plataforma BMC.

Cree un certificado digital firmado por CA

Para muchas organizaciones, el certificado digital autofirmado para el acceso web de ONTAP no cumple con sus políticas de InfoSec. En sistemas de producción, se recomienda que NetApp instale un certificado digital firmado por CA para utilizarlo en la autenticación del clúster o SVM como servidor SSL.

Puede usar `security certificate generate-csr` el comando para generar una solicitud de firma de certificación (CSR) y `security certificate install` el comando para instalar el certificado que recibe de la CA.

Pasos

1. Para crear un certificado digital firmado por la CA de la organización, realice lo siguiente:
   a. Generar una CSR.
   b. Siga el procedimiento de su organización para solicitar un certificado digital mediante la CSR de la CA de su organización. Por ejemplo, mediante la interfaz web de Microsoft Active Directory Certificate Services, vaya a `<CA_server_name>/certsrv` y solicite un certificado.
   c. Instale el certificado digital en ONTAP.

Protocolo de estado de certificado en línea

El protocolo de estado de certificados en línea (OCSP) permite que las aplicaciones de ONTAP que utilizan comunicaciones TLS, como LDAP o TLS, reciban el estado de certificado digital cuando OCSP está habilitado. La aplicación recibe una respuesta firmada que indica que el certificado solicitado es válido, revocado o desconocido.

OCSP permite determinar el estado actual de un certificado digital sin que sea necesario disponer de listas de revocación de certificados (CRL).

De manera predeterminada, la comprobación del estado de los certificados OCSP está deshabilitada. Se puede activar con el comando `security config ocsp enable -app name`, donde el nombre de la aplicación puede ser `autosupport`, , `audit_log`, , , , `fabricpool` `ems` `kmip` `ldap_ad` `ldap_nis_namemap`, o todo. El comando requiere un nivel de privilegio avanzado.

Gestión de SSHv2

El `security ssh modify` comando reemplaza las configuraciones existentes de los algoritmos de intercambio de claves SSH, los cifrados o los algoritmos MAC para el clúster o una SVM con los ajustes de configuración que especifique.

NetApp recomienda lo siguiente:

- Use contraseñas para las sesiones de usuario.
- Utilice una clave pública para el acceso a la máquina.

Cifrados e intercambios de claves compatibles

Cifrados	Intercambio de claves
aes256-ctr	diffie-hellman-group-exchange-sha256 (SHA-2)
aes192-ctr	diffie-hellman-group-exchange-sha1 (SHA-1)
aes128-ctr	diffie-hellman-group14-sha1 (SHA-1)
aes256-cbc	diffie-hellman-group1-sha1 (SHA-1)
aes192-cbc	-
aes128-cbc	-
aes128-gcm	-
aes256-gcm	-
3des-cbc	-

Compatibilidad con AES y 3DES cifrados simétricos

ONTAP también admite los siguientes tipos de cifrados simétricos AES y 3DES (también conocidos como cifrados):

- hmac-sha1
- hmac-sha1-96
- hmac-md5
- hmac-md5-96
- hmac-ripemd160
- umac-64
- umac-64
- umac-128
- hmac-sha2-256
- hmac-sha2-512
- hmac-sha1-etm
- hmac-sha1-96-etm
- hmac-sha2-256-etm
- hmac-sha2-512-etm
- hmac-md5-etm
- hmac-md5-96-etm
- hmac-ripemd160-etm
- umac-64-etm
- umac-128-etm

La configuración de gestión de SSH se aplica a ONTAP y a la plataforma BMC.

AutoSupport de NetApp

La función AutoSupport de ONTAP permite supervisar de manera proactiva el estado del sistema y enviar automáticamente mensajes y detalles al soporte técnico de NetApp, al equipo de soporte interno de su organización o a un partner de soporte. De manera predeterminada, los mensajes de AutoSupport en el soporte técnico de NetApp se habilitan cuando el sistema de almacenamiento se configura por primera vez. Además, AutoSupport comienza a enviar mensajes al soporte técnico de NetApp 24 horas después de que está habilitado. Este periodo de 24 horas se puede configurar. Para aprovechar la comunicación con el equipo de soporte interno de una organización, se debe completar la configuración del host de correo.

Solo el administrador del clúster puede realizar una gestión de AutoSupport (configuración). El administrador de SVM no tiene acceso a AutoSupport. Es posible deshabilitar la función AutoSupport. Sin embargo, NetApp recomienda habilitarlo porque AutoSupport ayuda a acelerar la identificación y la resolución de problemas en caso de que surja un problema en el sistema de almacenamiento. De forma predeterminada, el sistema recopila información de AutoSupport y la almacena localmente incluso si deshabilita AutoSupport.

Para obtener más detalles sobre los mensajes de AutoSupport, incluidos los contenidos en los distintos mensajes y los distintos tipos de mensajes, consulte "Asesor digital de Active IQ de NetApp" la documentación.

Los mensajes AutoSupport contienen datos confidenciales, incluidos, entre otros, los siguientes elementos:

- Archivos de registro
- Datos contextuales relativos a subsistemas específicos
- Datos de configuración y estado
- Datos de rendimiento

AutoSupport admite HTTPS, HTTP y SMTP para los protocolos de transporte. Debido a la naturaleza sensible de los mensajes de AutoSupport, NetApp recomienda encarecidamente utilizar HTTPS como protocolo de transporte predeterminado para enviar mensajes de AutoSupport a la compatibilidad de NetApp.

Además, debe aprovechar `system node autosupport modify` el comando para especificar los destinos de los datos de AutoSupport (por ejemplo, soporte técnico de NetApp, operaciones internas de una organización o partners). Este comando también permite especificar los detalles específicos de AutoSupport que se deben enviar (por ejemplo, datos de rendimiento, archivos de registro, etc.).

Para deshabilitar por completo AutoSupport, utilice `system node autosupport modify -state disable` el comando.

Protocolo de hora de red

Aunque ONTAP permite configurar manualmente la zona horaria, la fecha y la hora del clúster, debe configurar los servidores de protocolo de hora de redes (NTP) para sincronizar la hora del clúster con al menos tres servidores NTP externos.

Los problemas pueden surgir cuando la hora del clúster no es precisa. Aunque ONTAP permite configurar manualmente la zona horaria, la fecha y la hora en el clúster, debe configurar los servidores de protocolo de

tiempo de redes (NTP) para sincronizar la hora del clúster con servidores NTP externos.

A partir de ONTAP 9.5, puede configurar el servidor NTP con autenticación simétrica.

Puede asociar un máximo de 10 servidores NTP externos mediante el `cluster time-service ntp server create` comando. Para la redundancia y la calidad del servicio de tiempo, debe asociar al menos tres servidores NTP externos al clúster.

Para obtener detalles sobre la configuración de NTP en ONTAP, consulte "Gestionar la hora del clúster (solo administradores de clúster)".

Cuentas locales del sistema de archivos NAS (grupo de trabajo de CIFS)

La autenticación de clientes de grupo de trabajo proporciona una capa adicional de seguridad a la solución ONTAP que es consistente con una postura de autenticación de dominio tradicional. Utilice el `vserver cifs session show` comando para mostrar numerosos detalles relacionados con la postura, incluida la información de IP, el mecanismo de autenticación, la versión de protocolo y el tipo de autenticación.

A partir de ONTAP 9, puede configurar un servidor CIFS en un grupo de trabajo con clientes CIFS que se autentiquen en el servidor utilizando usuarios y grupos definidos localmente. La autenticación de clientes de grupo de trabajo proporciona una capa adicional de seguridad a la solución ONTAP que es consistente con una postura de autenticación de dominio tradicional. Para configurar el servidor CIFS, utilice `vserver cifs create` el comando. Tras crear el servidor CIFS, puede unirlo a un dominio CIFS o unirlo a un grupo de trabajo. Para unirse a un grupo de trabajo, utilice el `-workgroup` parámetro. A continuación se muestra un ejemplo de configuración:

```
cluster1::> vserver cifs create -vserver vs1 -cifs-server CIFSSERVER1
-workgroup Sales
```

Un servidor CIFS en modo grupo de trabajo solo es compatible con la autenticación de Windows NT LAN Manager (NTLM) y no admite la autenticación de Kerberos.

NetApp recomienda utilizar la función de autenticación NTLM con grupos de trabajo CIFS para mantener la política de seguridad de su organización. Para validar la política de seguridad CIFS, NetApp recomienda el uso `vserver cifs session show` del comando para mostrar numerosos detalles relacionados con la postura, incluida la información IP, el mecanismo de autenticación, la versión de protocolo y el tipo de autenticación.

Auditoría del sistema de archivos NAS

Los sistemas de archivos NAS ocupan un espacio más presente en el panorama de amenazas actual, las funciones de auditoría son cruciales para respaldar la visibilidad.

La seguridad requiere validación. ONTAP 9 ofrece más eventos y detalles de auditoría en toda la solución. Dado que los sistemas de archivos NAS ocupan un espacio cada vez mayor en el panorama de amenazas actual, las funciones de auditoría son cruciales para respaldar la visibilidad. Gracias a las funcionalidades de auditoría mejoradas que ofrece ONTAP 9, los detalles de auditoría CIFS son más abundantes que nunca. Los

detalles clave, incluidos los siguientes, se registran con eventos creados:

- Acceso a archivos, carpetas y recursos compartidos
- Archivos creados, modificados o eliminados
- Acceso de lectura a archivo realizado
- Intentos fallidos de leer o escribir archivos
- Cambios de permisos de carpeta

Cree una configuración de auditoría

Debe habilitar la auditoría de CIFS para generar eventos de auditoría. Utilice `vserver audit create` el comando para crear una configuración de auditoría. De forma predeterminada, el registro de auditoría utiliza un método de rotación según el tamaño. Puede utilizar una opción de rotación basada en el tiempo si se especifica en el campo Parámetros de rotación. Los detalles adicionales de configuración de rotación de auditoría de log incluyen el programa de rotación, los límites de rotación, los días de rotación de la semana y el tamaño de rotación. El siguiente texto proporciona una configuración de ejemplo que representa una configuración de auditoría mediante una rotación mensual basada en el tiempo programada para todos los días de la semana a las 12:30.

```
cluster1::> vserver audit create -vserver vs1 -destination /audit_log
-rotate-schedule-month all -rotate-schedule-dayofweek all -rotate-schedule
-hour 12 -rotate-schedule-minute 30
```

Eventos de auditoría CIFS

Los eventos de auditoría CIFS son los siguientes:

- **File Share**: Genera un evento de auditoría cuando se agrega, modifica o elimina un recurso compartido de red CIFS mediante los comandos relacionados `vserver cifs share` .
- **Cambio de política de auditoría**: Genera un evento de auditoría cuando la política de auditoría está deshabilitada, habilitada o modificada usando los comandos relacionados `vserver audit` .
- **Cuenta de usuario**: Genera un evento de auditoría cuando se crea o elimina un usuario local de CIFS o UNIX; se habilita, deshabilita o modifica una cuenta de usuario local; o se restablece o cambia una contraseña. Este evento utiliza `vserver cifs users-and-groups local-group` el comando o el comando relacionado `vserver services name-service unix-user` .
- **Grupo de seguridad**: Genera un evento de auditoría cuando se crea o elimina un grupo de seguridad local CIFS o UNIX mediante el `vserver cifs users-and-groups local-group` comando o el comando relacionado `vserver services name-service unix-group` .
- **Cambio de política de autorización**: Genera un evento de auditoría cuando se otorgan o revocan derechos para un usuario de CIFS o un grupo CIFS mediante el `vserver cifs users-and-groups privilege` comando.

> Esta funcionalidad se basa en la función de auditoría del sistema, que permite a un administrador revisar lo que el sistema permite y realiza desde la perspectiva de un usuario de datos.

Efecto de las API de REST en la auditoría NAS

ONTAP incluye la capacidad de las cuentas de administrador de acceder a archivos SMB/CIFS o NFS y manipularlos usando las API de REST. Aunque los administradores de ONTAP solo pueden ejecutar las API de REST, los comandos de la API de REST omiten el registro de auditoría del sistema NAS. Además, los administradores de ONTAP también pueden omitir los permisos de archivos cuando utilizan las API DE REST. Sin embargo, las acciones del administrador con API REST en los archivos se capturan en el registro del historial de comandos del sistema.

Crear rol de API de REST sin acceso

Puede evitar que los administradores de ONTAP utilicen las API DE REST para acceder a los archivos mediante la creación de un rol de API DE REST que no tiene acceso a volúmenes de ONTAP mediante REST. Para provisionar este rol, realice los siguientes pasos.

Pasos

1. Crear un nuevo rol DE REST que no tenga acceso a los volúmenes de almacenamiento, pero que tenga acceso a la API de REST.

```
cluster1::> security login rest-role create nofiles -vserver cluster1
"/api/storage/volumes" -access none
cluster1::> security login rest-role create nofiles -vserver cluster1
"/api" -access all
```

2. Asigne la cuenta de administrador al nuevo rol de API DE REST que creó en el paso anterior.

```
cluster1::> security login modify -user-or-group-name user1 -application
http -authentication-method password -vserver cluster1 -role nofile
```

Si desea impedir que la cuenta de administrador de clúster de ONTAP integrada utilice las API DE REST para acceder a los archivos, primero debe "cree una nueva cuenta de administrador y desactive o elimine la cuenta integrada".

Configure y habilite la firma y el sellado CIFS SMB

Puede configurar y habilitar la firma SMB que proteja la seguridad del Data Fabric garantizando que el tráfico entre clientes y sistemas de almacenamiento no se vea comprometido por ataques de reinyección y de intermediario. La firma SMB protege al verificar que los mensajes SMB tengan firmas válidas.

Acerca de esta tarea

El protocolo SMB constituye un vector de amenazas para las arquitecturas y los sistemas de archivos. Para abordar este vector, la solución ONTAP 9 utiliza firma y sellado SMB estándar del sector. La firma SMB protege la seguridad del Data Fabric al garantizar que el tráfico entre clientes y los sistemas de almacenamiento no se vea comprometido por ataques de reinyección y de intermediario. Para ello, verifica que los mensajes SMB tengan firmas válidas.

Aunque la firma SMB está deshabilitada de forma predeterminada en interés del rendimiento, NetApp recomienda encarecidamente habilitarla. Además, la solución de ONTAP admite el cifrado SMB, que también se conoce como sellado. Este enfoque permite el transporte seguro de datos de recurso por recurso. De manera predeterminada, el cifrado SMB está deshabilitado. Sin embargo, NetApp recomienda que habilite el cifrado SMB.

La firma y el sellado LDAP ahora son compatibles con SMB 2,0 y versiones posteriores. La firma (protección contra manipulación) y el sellado (cifrado) permiten una comunicación segura entre SVM y los servidores de Active Directory. El cifrado acelerado AES nuevas instrucciones (Intel AES NI) ahora es compatible con SMB 3,0 y versiones posteriores. AES-NI mejora el algoritmo de AES y acelera el cifrado de datos en las familias de procesadores compatibles.

Pasos

1. Para configurar y habilitar la firma SMB, utilice `vserver cifs security modify` el comando y verifique que el `-is-signing-required` parámetro se establezca en `true`. Consulte el siguiente ejemplo de configuración:

```
cluster1::> vserver cifs security modify -vserver vs1 -kerberos-clock
-skew 3 -kerberos-ticket-age 8 -is-signing-required true
```

2. Para configurar y habilitar el sellado y el cifrado SMB, utilice `vserver cifs security modify` el comando y verifique que el `-is-smb-encryption-required` parámetro se haya establecido en `true`. Consulte el siguiente ejemplo de configuración:

```
cluster1::> vserver cifs security modify -vserver vs1 -is-smb-encryption
-required true

cluster1::> vserver cifs security show -vserver vs1 -fields is-smb-
encryption-required
vserver  is-smb-encryption-required
-------- --------------------------
vs1      true
```

Protección para NFS

Las reglas de exportación son los elementos funcionales de una política de exportación. Las reglas de exportación coinciden con las solicitudes de acceso de cliente de un volumen con los parámetros específicos que configura para determinar cómo se manejan las solicitudes de acceso de clientes. La política de exportación debe contener al menos una regla de exportación para permitir el acceso a los clientes. Si una política de exportación contiene más de una regla, se procesan las reglas en el orden en que aparecen en la política de exportación.

El control de acceso es fundamental para mantener una postura segura. Por lo tanto, ONTAP utiliza la función de políticas de exportación para limitar el acceso al volumen NFS a los clientes que coincidan con parámetros específicos. Las políticas de exportación contienen una o varias reglas de exportación que procesan cada solicitud de acceso de cliente. Cada volumen tiene asociada una política de exportación para configurar el

acceso de clientes al volumen. El resultado de este proceso determina si al cliente se le otorga o se deniega (con un mensaje de denegación de permiso) el acceso al volumen. En este proceso también se determina el nivel de acceso al volumen.

Debe haber una política de exportación con reglas de exportación en una máquina virtual de almacenamiento para que los clientes accedan a los datos. Una SVM puede contener varias políticas de exportación.

El orden de las reglas viene determinado por el número de índice de reglas. Si una regla coincide con un cliente, se utilizan los permisos de esa regla y no se procesan más reglas. Si no hay reglas que coincidan, se deniega el acceso al cliente.

Las reglas de exportación determinan los permisos de acceso del cliente aplicando los siguientes criterios:

- Protocolo de acceso a archivos utilizado por el cliente que envía la solicitud (por ejemplo, NFSv4 o SMB)
- Un identificador de cliente (por ejemplo, nombre de host o dirección IP)
- Tipo de seguridad utilizado por el cliente para autenticar (por ejemplo, Kerberos v5, NTLM o AUTH_SYS)

Si una regla especifica varios criterios y el cliente no coincide con uno o más de ellos, la regla no se aplica.

Un ejemplo de política de exportación contiene una regla de exportación con los parámetros siguientes:

- `-protocol nfs`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule any`

El tipo de seguridad determina el nivel de acceso que recibe un cliente. Los tres niveles de acceso son de sólo lectura, de lectura y escritura y de superusuario (para clientes con ID de usuario `0`). Dado que el nivel de acceso determinado por el tipo de seguridad se evalúa en este orden, debe observar las reglas enumeradas:

Reglas para parámetros de nivel de acceso en reglas de exportación

Para que un cliente obtenga los siguientes niveles de acceso	Estos parámetros de acceso deben coincidir con el tipo de seguridad del cliente
Usuario normal de solo lectura	Solo lectura (`-rorule`)
Lectura y escritura normal del usuario	Solo lectura (`-rorule`) y lectura y escritura (`-rwrule`)
Sólo lectura de superusuario	Solo lectura (`-rorule`) y. `-superuser`
Lectura y escritura de superusuario	Solo lectura (`-rorule`) y lectura y escritura (`-rwrule`) y. `-superuser`

A continuación, se muestran tipos de seguridad válidos para cada uno de estos tres parámetros de acceso:

- Cualquiera
- Ninguno
- Nunca

Estos tipos de seguridad no son válidos para su uso con el `-superuser` parámetro:

- krb5
- ntlm
- act

Reglas para los resultados de los parámetros de acceso

Si el tipo de seguridad del cliente…	Entonces…
Coincide con un tipo de seguridad especificado en el parámetro de acceso.	El cliente recibe acceso para ese nivel con su propio ID de usuario.
No coincide con un tipo de seguridad especificado, pero el parámetro de acceso incluye la opción `none`.	El cliente recibe acceso para ese nivel y recibe el usuario anónimo con el ID de usuario especificado por el `-anon` parámetro.
No coincide con un tipo de seguridad especificado y el parámetro de acceso no incluye la opción `none`.	El cliente no recibe ningún acceso para ese nivel. Esta restricción no se aplica al `-superuser` parámetro porque este parámetro siempre incluye ninguno, incluso cuando no se ha especificado.

Kerberos 5 y Krb5p

A partir de ONTAP 9, se admite la autenticación Kerberos 5 con servicio de privacidad (krb5p). El modo de autenticación krbp5 es seguro y protege contra la manipulación y la escucha de datos empleando sumas de comprobación para cifrar todo el tráfico entre cliente y servidor. La solución ONTAP es compatible con el cifrado AES de 128 bits y 256 bits para Kerberos. El servicio de privacidad incluye la verificación de la integridad de los datos recibidos, la autenticación de los usuarios y el cifrado de los datos antes de la transmisión.

La opción krb5p está más presente en la función de política de exportación, donde se establece como una opción de cifrado. El método de autenticación krb5p se puede usar como parámetro de autenticación, tal como se muestra en el ejemplo siguiente:

```
cluster1::> vserver export-policy check-access -vserver vs1 -client-ip
10.22.32.42 -volume flex_vol -authentication-method krb5p -protocol nfs3
-access- type read
```

Active la firma y el sellado del protocolo ligero de acceso a directorios

Se admiten la firma y el sellado para habilitar la seguridad de la sesión en consultas enviadas a un servidor LDAP. Este enfoque proporciona una alternativa a la seguridad de sesión LDAP-over-TLS.

La firma comprueba la integridad de la carga de datos LDAP mediante una tecnología de clave secreta. El sellado cifra la carga de datos LDAP para impedir la transmisión de información confidencial en texto sin cifrar. La configuración de seguridad de sesiones en una SVM se corresponde con las disponibles en el servidor LDAP. De forma predeterminada, la firma y el sellado LDAP están deshabilitados.

Pasos

1. Para habilitar esta función, ejecute `vserver cifs security modify` el comando con `session-security-for-ad-ldap` el parámetro.

   Opciones para las funciones de seguridad de LDAP:

   - **Ninguno**: Por defecto, sin firma o sellado
   - **Signo**: Firmar tráfico LDAP
   - **Sello**: Firma y cifra el tráfico LDAP

   > Los parámetros de signo y sello son acumulativos, lo que significa que si se utiliza la opción de signo, el resultado es LDAP con firma. Sin embargo, si se utiliza la opción de sellado, el resultado es tanto el signo como el sello. Además, si no se especifica un parámetro para este comando, el valor predeterminado es none.

   A continuación se muestra un ejemplo de configuración:

```
cluster1::> vserver cifs security modify -vserver vs1 -kerberos-clock
-skew 3 -kerberos-ticket-age 8 -session-security-for-ad-ldap seal
```

Cree y utilice una instancia de NetApp FPolicy

Puede crear y utilizar un FPolicy, un componente de infraestructura de la solución ONTAP que permite a las aplicaciones de los partners supervisar y establecer permisos de acceso a archivos. Una de las aplicaciones más potentes es la seguridad de cargas de trabajo de almacenamiento, una aplicación SaaS de NetApp que proporciona visibilidad y control centralizados de todos los accesos a los datos corporativos en entornos de cloud híbrido para garantizar que se cumplan los objetivos de seguridad y cumplimiento de normativas.

El control de acceso es un concepto clave de la seguridad. La visibilidad y la capacidad de responder al acceso a archivos y a las operaciones con archivos son cruciales para mantener su política de seguridad. Para proporcionar visibilidad y control de acceso a los archivos, la solución ONTAP usa la función FPolicy de NetApp.

Se pueden establecer políticas de archivo por tipos de archivo. FPolicy determina la forma en que el sistema de almacenamiento maneja las solicitudes de sistemas cliente individuales en operaciones como crear, abrir, cambiar nombre y eliminar. A partir de ONTAP 9, el marco de notificaciones de acceso a archivos de FPolicy se ha mejorado con controles de filtrado y resiliencia ante breves interrupciones de red.

Pasos

1. Para aprovechar la función FPolicy, primero debe crear la política de FPolicy con `vserver fpolicy policy create` el comando.

Además, debe usar el `-events` parámetro si utiliza FPolicy para obtener visibilidad y colección de eventos. La granularidad adicional que proporciona ONTAP permite filtrar y acceder a él según el nivel de control de los nombres de usuario. Para controlar los privilegios y el acceso con nombres de usuario, especifique el `-privilege-user-name` parámetro.

En el siguiente texto, se proporciona un ejemplo de creación de FPolicy:

```
cluster1::> vserver fpolicy policy create -vserver vs1.example.com
-policy-name vs1_pol -events cserver_evt,v1e1 -engine native -is
-mandatory true -allow-privileged-access no -is-passthrough-read-enabled
false
```

2. Después de crear la política de FPolicy, debe habilitarla con `vserver fpolicy enable` el comando. Este comando también establece la prioridad o la secuencia de la entrada de FPolicy.

La secuencia de FPolicy es importante porque, si varias políticas se han suscrito al mismo evento de acceso a archivos, la secuencia dicta el orden en que se otorga o deniega el acceso.

El siguiente texto proporciona una configuración de ejemplo para habilitar la política de FPolicy y validar la configuración con `vserver fpolicy show` el comando:

```
cluster1::> vserver fpolicy enable -vserver vs2.example.com -policy-name
vs2_pol -sequence-number 5

cluster1::> vserver fpolicy show
Vserver                 Policy Name                  Sequence  Status
Engine
----------------------- ---------------------------- --------  -------
-------
vs1.example.com         vs1_pol
vs2.example.com         vs2_pol
 external
2 entries were displayed.
```

Mejoras de FPolicy

ONTAP 9 incluye las mejoras de FPolicy descritas en las siguientes secciones.

Controles de filtrado

Hay nuevos filtros disponibles para `SetAttr` y para eliminar notificaciones en las actividades del directorio.

Resiliencia asincrónica

Si un servidor de FPolicy que funciona en modo asíncrono experimenta una interrupción de la red, las notificaciones de FPolicy generadas durante la interrupción se almacenan en el nodo de almacenamiento. Cuando el servidor FPolicy vuelve a estar conectado, recibe alertas de las notificaciones almacenadas y pueden recogerlas del nodo de almacenamiento. El tiempo que las notificaciones se pueden almacenar durante una interrupción se puede configurar hasta 10 minutos.

Seguridad de LIF

Una LIF es una dirección IP o un nombre de puerto a nivel mundial (WWPN) con características asociadas, como un rol, un puerto de inicio, un nodo de inicio, una lista de puertos a los que se deben conmutar por error y una política de firewall. Puede configurar las LIF en los puertos a través de los que el clúster envía y recibe comunicaciones a través de la red. Es crucial comprender las características de seguridad de cada rol de LIF.

Roles LIF

Los roles de LIF pueden ser los siguientes:

- **Data LIF**: Una LIF asociada a una SVM y utilizada para comunicarse con los clientes.
- **Cluster LIF**: Una LIF utilizada para transportar tráfico intraclúster entre nodos de un cluster.
- **Node management LIF**: Una LIF que proporciona una dirección IP dedicada para administrar un nodo en particular en un clúster.
- **Cluster management LIF**: Un LIF que proporciona una única interfaz de gestión para todo el clúster.
- **Intercluster LIF**: Una LIF utilizada para la comunicación entre clústeres, la copia de seguridad y la replicación.

Características de seguridad de cada rol de LIF

	LIF de datos	LIF de clúster	LIF de gestión de nodos	LIF de gestión del clúster	LIF entre clústeres
¿Requiere subred IP privada?	No	Sí	No	No	No
¿Necesita una red segura?	No	Sí	No	No	Sí
Política de firewall predeterminada	Muy restrictivo	Completamente abierto	Mediano	Mediano	Muy restrictivo
¿Es personalizable el firewall?	Sí	No	Sí	Sí	Sí

- Dado que la LIF de clúster está completamente abierta sin política de firewall configurable, debe estar en una subred IP privada en una red aislada segura.
- Bajo ninguna circunstancia se debe exponer ningún rol de LIF a Internet.

Obtenga más información sobre la protección de las LIF, consulte el "Configurar políticas de firewall para LIF".

Protocolo y seguridad de puertos

Además de realizar operaciones y funciones de seguridad integradas, el endurecimiento de una solución también debe incluir mecanismos de seguridad externos. El aprovechamiento de dispositivos de infraestructura adicionales, como firewalls, sistemas de prevención de intrusiones (IPSs) y otros dispositivos de seguridad, para filtrar y limitar el acceso a ONTAP es una forma eficaz de establecer y mantener una postura de seguridad estricta. Esta información es un componente clave para filtrar y limitar el acceso al entorno y sus recursos.

Los protocolos y puertos comúnmente utilizados

Servicio	Puerto/protocolo	Descripción
SSH	22/TCP	Inicio de sesión SSH
telnet	23/TCP	Inicio de sesión remoto
Domain	53/TCP	Servidor de nombres de dominio
HTTP	80/TCP 80/UDP	HTTP
rpcbind	111/TCP 111/UDP	Llamada a procedimiento remoto
NTP	123/UDP	Protocolo de hora de red
msrpc	135/UDP	Llamada a procedimiento remoto de Microsoft
Netbios-name	137/TCP 137/UDP	Servicio de nombres NetBIOS
netbios-ssn	139/TCP	Sesión de servicio NetBIOS
SNMP	161/UDP	SNMP
HTTPS	443/TCP	Enlace seguro:http
microsoft-ds	445/TCP	Servicios de directorio de Microsoft
IPsec	500/UDP	Seguridad del protocolo de Internet
mount	635/UDP	Montaje NFS
named	953/UDP	Daemon de nombres
NFS	2049/UDP 2049/TCP	Daemon del servidor NFS
nrv	2050/TCP	Protocolo de volumen remoto de NetApp
iscsi	3260/TCP	Puerto de destino iSCSI
Lockd	4045/TCP 4045/UDP	Daemon de bloqueo NFS

Servicio	Puerto/protocolo	Descripción
NFS	4046/TCP	Protocolo NFS mountd
acp-proto	4046/UDP	Protocolo de contabilidad
rquotad	4049/UDP	Protocolo rquotad NFS
krb524	4444/UDP	Kerberos 524
IPsec	4500/UDP	Seguridad del protocolo de Internet
acp	5125/UDP 5133/UDP 5144/TCP	Puerto de control alternativo para el disco
Mdns	5353/UDP	DNS de multidifusión
HTTPS	5986/UDP	Puerto HTTPS: Protocolo binario de escucha
TELNET	8023/TCP	Telnet de ámbito de nodo
HTTPS	8443/TCP	7MTT herramienta GUI a través de xref:./ontap-hardening/HTTPS
RSH	8514/TCP	RSH de ámbito de nodo
KMIP	9877/TCP	Puerto de cliente KMIP (solo host local interno)
ndmp	10000/TCP	NDMP
cifs puerto de testigo	40001/TCP	Puerto de testigo CIFS
TLS	50000/TCP	Seguridad de la capa de transporte
Iscsi	65200/TCP	Puerto iSCSI
SSH	65502/TCP	Shell seguro
vsun	65503/TCP	vsun

Puertos internos de NetApp

Puerto/protocolo	Descripción
900	RPC del clúster de NetApp
902	RPC del clúster de NetApp
904	RPC del clúster de NetApp
905	RPC del clúster de NetApp
910	RPC del clúster de NetApp
911	RPC del clúster de NetApp
913	RPC del clúster de NetApp
914	RPC del clúster de NetApp
915	RPC del clúster de NetApp
918	RPC del clúster de NetApp

Puerto/protocolo	Descripción
920	RPC del clúster de NetApp
921	RPC del clúster de NetApp
924	RPC del clúster de NetApp
925	RPC del clúster de NetApp
927	RPC del clúster de NetApp
928	RPC del clúster de NetApp
929	RPC del clúster de NetApp
931	RPC del clúster de NetApp
932	RPC del clúster de NetApp
933	RPC del clúster de NetApp
934	RPC del clúster de NetApp
935	RPC del clúster de NetApp
936	RPC del clúster de NetApp
937	RPC del clúster de NetApp
939	RPC del clúster de NetApp
940	RPC del clúster de NetApp
951	RPC del clúster de NetApp
954	RPC del clúster de NetApp
955	RPC del clúster de NetApp
956	RPC del clúster de NetApp
958	RPC del clúster de NetApp
961	RPC del clúster de NetApp
963	RPC del clúster de NetApp
964	RPC del clúster de NetApp
966	RPC del clúster de NetApp
967	RPC del clúster de NetApp
7810	RPC del clúster de NetApp
7811	RPC del clúster de NetApp
7812	RPC del clúster de NetApp
7813	RPC del clúster de NetApp
7814	RPC del clúster de NetApp
7815	RPC del clúster de NetApp
7816	RPC del clúster de NetApp

Puerto/protocolo	Descripción
7817	RPC del clúster de NetApp
7818	RPC del clúster de NetApp
7819	RPC del clúster de NetApp
7820	RPC del clúster de NetApp
7821	RPC del clúster de NetApp
7822	RPC del clúster de NetApp
7823	RPC del clúster de NetApp
7824	RPC del clúster de NetApp

Recursos de seguridad

Para obtener más información sobre la información descrita en esta documentación de seguridad de ONTAP, consulte la siguiente información adicional y conceptos de seguridad.

Para obtener información sobre la creación de informes sobre vulnerabilidades e incidentes, las respuestas de seguridad de NetApp y la confidencialidad del cliente, consulte la "Portal de seguridad de NetApp".

- "Notas de la versión de ONTAP 9"
- "Referencias de comandos de ONTAP 9"
- "Administración del sistema"
- "Autenticación de administrador y RBAC"
- "Cifrado NetApp"
- "TR-4647: Autenticación multifactor en ONTAP 9,3"
- "Cifrados OPENSSL"
- "CryptoMod FIPS-140-2 Nivel 1"
- "Autenticación basada en certificados con el SDK de capacidad de gestión de NetApp para ONTAP"
- "Gestión de redes"