# Richtlinien zur ONTAP-Härtung

ONTAP 9

NetApp
July 19, 2024

# Inhalt

# Richtlinien zur ONTAP-Härtung

## Übersicht über die Erhöhung der Sicherheit durch ONTAP

ONTAP bietet eine Reihe von Kontrollmechanismen, mit denen Sie das Storage-Betriebssystem ONTAP, die branchenführende Datenmanagement-Software, absichern können. Mithilfe der Richtlinien- und Konfigurationseinstellungen für ONTAP kann Ihr Unternehmen die vorgegebenen Sicherheitsziele für Vertraulichkeit, Integrität und Verfügbarkeit von Informationssystemen erfüllen.

Die Entwicklung der aktuellen Bedrohungslandschaft stellt Unternehmen vor besondere Herausforderungen beim Schutz ihrer wertvollsten Ressourcen: Daten und Informationen. Die fortschrittlichen und dynamischen Bedrohungen und Schwachstellen, mit denen wir konfrontiert sind, werden immer raffinierter. Zusammen mit einer Steigerung der Effektivität von Verschleiss- und Aufklärungstechniken durch potenzielle Eindringlinge müssen sich die Systemmanager proaktiv mit der Sicherheit von Daten und Informationen befassen.

Ab Juli 2024 wurden die Inhalte aus zuvor als PDFs veröffentlichten technischen Berichten in die ONTAP Produktdokumentation integriert. Die ONTAP-Sicherheitsdokumentation enthält jetzt Inhalte aus *TR-4569: Security Hardening Guide for ONTAP*.

## Validierung von ONTAP-Images

ONTAP stellt Mechanismen bereit, die sicherstellen, dass das ONTAP-Image beim Upgrade und beim Booten gültig ist.

### Validierung von Upgrade Images

Mithilfe von Code-Signing kann sichergestellt werden, dass ONTAP Images über unterbrechungsfreie Image-Updates oder automatisierte unterbrechungsfreie Image-Updates, CLIs oder ONTAP APIs authentisch von NetApp erstellt und nicht manipuliert wurden. Die Validierung des Upgrade-Images wurde in ONTAP 9.3 eingeführt.

Diese Funktion ist eine automatische Sicherheitserweiterung für ONTAP-Upgrades oder -Reverversionen. Es wird nicht erwartet, dass der Benutzer etwas anderes tut, außer optional die Signatur der obersten Ebene „image.tgz“ zu überprüfen.

### Image-Validierung beim Booten

Ab ONTAP 9.4 ist sicheres Boot mit Unified Extensible Firmware Interface (UEFI) für NetApp AFF A800, AFF A220, FAS2750 und FAS2720 Systeme und nachfolgende Systeme der nächsten Generation mit UEFI BIOS aktiviert.

Während des Einschaltvorgangs validiert der Bootloader die Whitelist-Datenbank der sicheren Startschlüssel mit der Signatur, die jedem geladenen Modul zugeordnet ist. Nachdem jedes Modul validiert und geladen wurde, wird der Startvorgang mit der ONTAP-Initialisierung fortgesetzt. Wenn die Signaturüberprüfung für ein Modul fehlschlägt, wird das System neu gestartet.

Diese Optionen gelten für ONTAP-Images und das Plattform-BIOS.

# Lokale Storage-Administratorkonten

## Rollen, Applikationen und Authentifizierung

ONTAP bietet sicherheitsbewussten Unternehmen die Möglichkeit, verschiedenen Administratoren anhand verschiedener Anmeldeanwendungen und -Methoden granularen Zugriff zu gewähren. So können Kunden ein datenorientiertes Zero-Trust-Modell aufbauen.

Dies sind die Rollen, die Administratoren von Administratoren und Storage Virtual Machines zur Verfügung stehen. Die Methoden der Anmeldeanwendung und die Methoden der Anmeldeauthentifizierung werden angegeben.

### Rollen

Dank rollenbasierter Zugriffssteuerung (Role Based Access Control, RBAC) haben Benutzer nur Zugriff auf die Systeme und Optionen, die für ihre Rollen und Funktionen erforderlich sind. Die RBAC-Lösung in ONTAP beschränkt den administrativen Zugriff der Benutzer auf das Niveau, das für ihre Rolle festgelegt wurde. Administratoren können so Benutzer anhand der zugewiesenen Rolle managen. ONTAP bietet mehrere vordefinierte Rollen. Operatoren und Administratoren können benutzerdefinierte Zugriffskontrollrollen erstellen, ändern oder löschen und Kontobeschränkungen für bestimmte Rollen festlegen.

#### Vordefinierte Rollen für Cluster-Administratoren

| Diese Rolle… | Verfügt über diese Zugriffsebene… | Zu den folgenden Befehlen oder Befehlsverzeichnissen |
|---|---|---|
| `admin` | Alle | Alle Befehlsverzeichnisse (`DEFAULT`) |
| `admin-no-fsa` (Verfügbar ab ONTAP 9.12.1) | Lese-/Schreibzugriff | • Alle Befehlsverzeichnisse (`DEFAULT`)<br>• `security login rest-role`<br>• `security login role` |

| | | |
|---|---|---|
| Schreibgeschützt | • `security login rest-role create`<br>• `security login rest-role delete`<br>• `security login rest-role modify`<br>• `security login rest-role show`<br>• `security login role create`<br>• `security login role create`<br>• `security login role delete`<br>• `security login role modify`<br>• `security login role show`<br>• `volume activity-tracking`<br>• `volume analytics` | Keine |
| `volume file show-disk-usage` | `autosupport` | Alle |
| • `set`<br>• `system node autosupport` | Keine | Alle anderen Befehlsverzeichnisse (`DEFAULT`) |
| `backup` | Alle | `vserver services ndmp` |
| Schreibgeschützt | `volume` | Keine |
| Alle anderen Befehlsverzeichnisse (`DEFAULT`) | `readonly` | Alle |

| | | |
|---|---|---|
| • `security login password`<br><br>Nur zur Verwaltung des eigenen Benutzerkontos mit lokalem Passwort und Schlüsselinformationen<br><br>• `set` | Keine | `security` |
| Schreibgeschützt | Alle anderen Befehlsverzeichnisse (`DEFAULT`) | `none` |

Der `autosupport` Rolle ist dem vordefinierten zugewiesen `autosupport` Konto, das von AutoSupport OnDemand verwendet wird. ONTAP verhindert, dass Sie den ändern oder löschen können `autosupport` Konto. ONTAP verhindert darüber hinaus, dass Sie das zuweisen `autosupport` Rolle für andere Benutzerkonten.

**Vordefinierte Rollen für SVM-Administratoren (Storage Virtual Machine**

| Rollenname | Sorgen |
|---|---|
| `vsadmin` | • Verwalten Sie Ihr eigenes Benutzerkonto mit lokalen Kennwörtern und Schlüsselinformationen<br>• Verwalten von Volumes, mit Ausnahme von Volume-Verschiebungen<br>• Managen von Kontingenten, qtrees, Snapshot Kopien und Dateien<br>• LUNs managen<br>• Führen Sie SnapLock-Vorgänge aus, mit Ausnahme von privilegiertem Löschen<br>• Konfigurationsprotokolle: NFS, SMB, iSCSI, FC, FCoE, NVMe/FC und NVMe/TCP<br>• Services konfigurieren: DNS, LDAP und NIS<br>• Überwachen von Jobs<br>• Überwachen von Netzwerkverbindungen und Netzwerkschnittstellen<br>• Monitoring des Systemzustands der SVM |

| | |
|---|---|
| `vsadmin-volume` | • Verwalten Sie Ihr eigenes Benutzerkonto mit lokalen Kennwörtern und Schlüsselinformationen<br>• Managen von Volumes, einschließlich Volume-Verschiebungen<br>• Managen von Kontingenten, qtrees, Snapshot Kopien und Dateien<br>• LUNs managen<br>• Konfigurationsprotokolle: NFS, SMB, iSCSI, FC, FCoE, NVMe/FC und NVMe/TCP<br>• Services konfigurieren: DNS, LDAP und NIS<br>• Überwachung der Netzwerkschnittstelle<br>• Monitoring des Systemzustands der SVM |
| `vsadmin-protocol` | • Verwalten Sie Ihr eigenes Benutzerkonto mit lokalen Kennwörtern und Schlüsselinformationen<br>• Konfigurationsprotokolle: NFS, SMB, iSCSI, FC, FCoE, NVMe/FC und NVMe/TCP<br>• Services konfigurieren: DNS, LDAP und NIS<br>• LUNs managen<br>• Überwachung der Netzwerkschnittstelle<br>• Monitoring des Systemzustands der SVM |
| `vsadmin-backup` | • Verwalten Sie Ihr eigenes Benutzerkonto mit lokalen Kennwörtern und Schlüsselinformationen<br>• Management von NDMP-Vorgängen<br>• Lese-/Schreibzugriff auf ein wiederhergestelltes Volume erstellen<br>• Management von SnapMirror Beziehungen und Snapshot Kopien<br>• Anzeigen von Volumes und Netzwerkinformationen |

| | |
|---|---|
| `vsadmin-snaplock` | • Verwalten Sie Ihr eigenes Benutzerkonto mit lokalen Kennwörtern und Schlüsselinformationen<br>• Verwalten von Volumes, mit Ausnahme von Volume-Verschiebungen<br>• Managen von Kontingenten, qtrees, Snapshot Kopien und Dateien<br>• Führen Sie SnapLock-Vorgänge durch, einschließlich privilegiertem Löschen<br>• Protokolle konfigurieren: NFS und SMB<br>• Services konfigurieren: DNS, LDAP und NIS<br>• Überwachen von Jobs<br>• Überwachen von Netzwerkverbindungen und Netzwerkschnittstellen |
| `vsadmin-readonly` | • Verwalten Sie Ihr eigenes Benutzerkonto mit lokalen Kennwörtern und Schlüsselinformationen<br>• Monitoring des Systemzustands der SVM<br>• Überwachung der Netzwerkschnittstelle<br>• Zeigen Sie Volumes und LUNs an<br>• Services und Protokolle anzeigen |

**Anwendungsmethoden**

Die Anwendungsmethode gibt den Zugriffstyp der Anmeldemethode an. Mögliche Werte sind `console`, `http`, `ontapi`, `rsh`, `snmp`, `service-processor`, `ssh`, und `telnet`.

Durch Festlegen dieses Parameters wird `service-processor` dem Benutzer Zugriff auf den Service-Prozessor gewährt. Wenn dieser Parameter auf festgelegt `service-processor`ist, muss der `-authentication-method` Parameter auf festgelegt werden `password` , da der Service Processor nur die Kennwortauthentifizierung unterstützt. SVM-Benutzerkonten können nicht auf den Service-Prozessor zugreifen. Daher können Operatoren und Administratoren den Parameter nicht verwenden `-vserver` , wenn dieser Parameter auf eingestellt ist `service-processor`.

Um den Zugriff auf das weiter einzuschränken `service-processor` , verwenden Sie den Befehl `system service-processor ssh add-allowed-addresses`. Mit dem Befehl `system service-processor api-service` können die Konfigurationen und Zertifikate aktualisiert werden.

Aus Sicherheitsgründen sind Telnet und Remote Shell (RSH) standardmäßig deaktiviert, da NetApp Secure Shell (SSH) für sicheren Remote-Zugriff empfiehlt. Wenn Telnet oder RSH erforderlich ist oder nur einmalig benötigt wird, müssen diese aktiviert sein.

Mit dem `security protocol modify` Befehl wird die vorhandene Cluster-weite Konfiguration von RSH und Telnet geändert. Aktivieren Sie RSH und Telnet im Cluster, indem Sie das Feld aktiviert auf einstellen `true`.

### Authentifizierungsmethoden

Der Parameter für die Authentifizierungsmethode gibt die Authentifizierungsmethode an, die für Anmeldungen verwendet wird.

| Authentifizierungsmethode | Beschreibung |
|---|---|
| `cert` | SSL-Zertifikatauthentifizierung |
| `community` | SNMP-Community-Zeichenfolgen |
| `domain` | Active Directory-Authentifizierung |
| `nsswitch` | LDAP- oder NIS-Authentifizierung |
| `password` | Passwort |
| `publickey` | Authentifizierung über öffentlichen Schlüssel |
| `usm` | SNMP-Benutzersicherheitsmodell |

Die Verwendung von NIS wird aufgrund von Schwachstellen bei der Protokollsicherheit nicht empfohlen.

Ab ONTAP 9.3 steht die verkettete zwei-Faktor-Authentifizierung für lokale SSH-Konten mit und Passwort als die beiden Authentifizierungsmethoden zur Verfügung `admin` `publickey` . Zusätzlich zum Feld im Befehl wurde ein neues Feld mit dem `-authentication-method` `security login` Namen `-second -authentication-method` hinzugefügt. Der öffentliche Schlüssel oder das Kennwort können entweder als oder als angegeben werden `-authentication-method` `-second-authentication-method`. Während der SSH-Authentifizierung ist die Reihenfolge jedoch immer öffentlicher Schlüssel mit teilweiser Authentifizierung, gefolgt von der Kennwortaufforderung zur vollständigen Authentifizierung.

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

Ab ONTAP 9.4 `nsswitch` kann als zweite Authentifizierungsmethode mit verwendet werden `publickey`.

Ab ONTAP 9.12.1 kann FIDO2 auch für die SSH-Authentifizierung über ein YubiKey oder andere mit FIDO2 kompatible Geräte genutzt werden.

Ab ONTAP 9.13.1:

- `domain` Konten können als zweite Authentifizierungsmethode mit verwendet werden `publickey`.
- Time-Based One-time password (`totp`) ist ein temporärer Passcode, der von einem Algorithmus generiert wird, der die aktuelle Tageszeit als einen seiner Authentifizierungsfaktoren für die zweite Authentifizierungsmethode verwendet.
- Public Key Revocation wird mit SSH publickeys sowie Zertifikaten unterstützt, die während SSH auf Ablauf/Widerruf überprüft werden.

Weitere Informationen zur Multi-Faktor-Authentifizierung (MFA) für ONTAP System Manager, Active IQ Unified Manager und SSH finden Sie unter "TR-4647: Multifaktor-Authentifizierung in ONTAP 9".

## Standard-Administratorkonten

Das Administratorkonto sollte eingeschränkt sein, da die Rolle des Administrators Zugriff über alle Anwendungen erhält. Das Diagnose-Konto gewährt Zugriff auf die System-Shell und sollte nur für den technischen Support reserviert werden, um Fehlerbehebungsaufgaben durchzuführen.

Es gibt zwei standardmäßige Administratorkonten: `admin` Und `diag`.

Verwaiste Konten sind ein wichtiger Sicherheitsvektor und führen oft zu Schwachstellen, einschließlich der Eskalation von Berechtigungen. Dabei handelt es sich um unnötige und nicht genutzte Konten, die im Benutzerkonto-Repository verbleiben. Dabei handelt es sich in erster Linie um Standardkonten, die nie verwendet wurden oder für die Passwörter nie aktualisiert oder geändert wurden. Um dieses Problem zu beheben, unterstützt ONTAP das Entfernen und Umbenennen von Konten.

ONTAP kann integrierte Konten nicht entfernen oder umbenennen. NetApp empfiehlt jedoch, nicht benötigte integrierte Konten mit dem Sperrbefehl zu sperren.

Auch wenn verwaiste Konten ein erhebliches Sicherheitsproblem darstellen, empfiehlt NetApp dringend, die Auswirkungen des Entfernens von Konten aus dem lokalen Konto-Repository zu testen.

### Lokale Konten auflisten

Führen Sie zum Auflisten der lokalen Konten den Befehl aus `security login show .`

```
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.
```

### Entfernen Sie das Standard-Administratorkonto

Das `admin` Konto hat die Rolle des Administrators und ist über alle Anwendungen zugänglich.

#### Schritte

1. Weiteres Konto auf Administratorebene erstellen.

   Um das Standardkonto vollständig zu entfernen `admin` , müssen Sie zuerst ein anderes Administratorkonto erstellen, das die Anmeldeanwendung verwendet `console` .

Diese Änderungen können zu unerwünschten Auswirkungen führen. Testen Sie immer zuerst neue Einstellungen, die sich auf den Sicherheitsstatus der Lösung auf einem nicht produktiven Cluster auswirken können.

Beispiel:

```
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. Nachdem Sie das neue Administratorkonto erstellt haben, testen Sie den Zugriff auf dieses Konto mit der `NewAdmin` Anmeldung. Konfigurieren Sie mit der `NewAdmin` Anmeldung das Konto so, dass es die gleichen Anmeldeanwendungen hat wie das Standard- oder das vorherige Administratorkonto (z. B. `http`, `ontapi`, `service-processor`oder `ssh`). Dieser Schritt stellt sicher, dass die Zugriffssteuerung erhalten bleibt.

   Beispiel:

```
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. Nachdem alle Funktionen getestet wurden, können Sie das Administratorkonto für alle Anwendungen

deaktivieren, bevor Sie es aus ONTAP entfernen. Dieser Schritt dient als abschließender Test, um zu bestätigen, dass es keine anhaltenden Funktionen gibt, die auf das vorherige Administratorkonto angewiesen sind.

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

4. Führen Sie den folgenden Befehl aus, um das Standard-Administratorkonto und alle Einträge zu entfernen:

```
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.
```

### Legen Sie das Kennwort für das Diagnosekonto (diag) fest

Ein Diagnosekonto mit dem Namen `diag` wird im Lieferumfang des Speichersystems angegeben. Sie können das Konto verwenden `diag` , um Fehlerbehebungsaufgaben im durchzuführen `systemshell`. Das `diag` Konto ist das einzige Konto, mit dem über den privilegierten Befehl auf die Systemshell zugegriffen werden kann `diag systemshell`.

> ⚠ Die Systemshell und das zugehörige `diag` Konto sind für Low-Level-Diagnosezwecke vorgesehen. Ihr Zugriff erfordert die Berechtigungsebene für die Diagnose und darf nur unter Anleitung des technischen Supports verwendet werden, um Fehlerbehebungsaufgaben durchzuführen. Weder `diag` das Konto noch das `systemshell` sind für allgemeine administrative Zwecke bestimmt.

#### Bevor Sie beginnen

Bevor Sie auf den zugreifen `systemshell`, müssen Sie das Kontokennwort mit dem Befehl festlegen `diag security login password` . Verwenden Sie strenge Passwort-Prinzipien und ändern Sie das `diag` Passwort in regelmäßigen Abständen.

#### Schritte

1. Legen Sie das Kennwort für den Kontobenutzer fest `diag` :

```
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%
```

## Überprüfung durch mehrere Administratoren

Ab ONTAP 9.11.1 können Sie die Multi-Admin-Verifizierung (MAV) verwenden, um bestimmte Vorgänge, wie das Löschen von Volumes oder Snapshot Kopien, nur nach Genehmigungen von designierten Administratoren ausführen zu können. So werden gefährdete, böswillige oder unerfahrene Administratoren daran gehindert, unerwünschte Änderungen vorzunehmen oder Daten zu löschen.

Die Konfiguration der MAV besteht aus folgenden Komponenten:

- "Erstellen einer oder mehrerer Genehmigungsgruppen für Administratoren"
- "Aktivieren der Überprüfungsfunktion für mehrere Administratoren"
- "Hinzufügen oder Ändern von Regeln"

Nach der Erstkonfiguration können nur Administratoren einer MAV-Genehmigungsgruppe (MAV-Administratoren) diese Elemente ändern.

Wenn MAV aktiviert ist, sind für jeden geschützten Vorgang drei Schritte erforderlich:

1. Wenn ein Benutzer den Vorgang initiiert, wird ein angezeigt "Die Anforderung wird generiert."
2. Bevor es ausgeführt werden kann, muss die erforderliche Anzahl von angegeben werden "MAV-Administratoren müssen genehmigen."
3. Nach der Genehmigung schließt der Benutzer den Vorgang ab.

MAV ist nicht für den Einsatz bei Volumes oder Workflows mit hoher Automatisierung vorgesehen, da jede automatisierte Aufgabe vor Abschluss des Vorgangs eine Genehmigung erfordert. Wenn Sie Automatisierung und MAV gemeinsam nutzen möchten, empfiehlt NetApp, Abfragen für bestimmte MAV-Vorgänge zu verwenden. Sie können beispielsweise MAV-Regeln nur auf Volumes anwenden `volume delete` , auf die keine Automatisierung involviert ist. Sie können diese Volumes einem bestimmten Benennungsschema

zuweisen.

Weitere Informationen zum MAV finden Sie im "Dokumentation zur Verifizierung durch mehrere ONTAP Administratoren".

## Sperren von Snapshot-Kopien

Sperrung von Snapshot Kopien ist eine SnapLock Funktion. Hier können Snapshot Kopien manuell oder automatisch mit einer Aufbewahrungsfrist für die Snapshot Richtlinie des Volume unlöschbar gemacht werden. Durch das Sperren von Snapshot Kopien sollen böswillige oder nicht vertrauenswürdige Administratoren daran gehindert werden, Snapshots auf dem primären oder sekundären ONTAP System zu löschen.

Mit ONTAP 9.12.1 wurde die Snapshot Kopie gesperrt. Snapshot Kopien werden auch als manipulationssichere Snapshot Sperrung bezeichnet. Obwohl die SnapLock Lizenz und die Initialisierung der Compliance-Uhr erforderlich ist, hat die Sperrung von Snapshot Kopien keine Verbindung zu SnapLock Compliance oder SnapLock Enterprise. Es gibt keinen vertrauenswürdigen Storage-Administrator, wie bei SnapLock Enterprise und er schützt nicht die zugrunde liegende physische Storage-Infrastruktur, wie bei der SnapLock Compliance. Dies ist eine Verbesserung gegenüber der Snapshot-Kopien auf einem Sekundärsystem. Die schnelle Recovery von gesperrten Snapshots auf Primärsystemen kann ermöglicht werden, um durch Ransomware beschädigte Volumes wiederherzustellen.

Weitere Informationen zum Sperren von Snapshot Kopien finden Sie im "ONTAP-Dokumentation".

## Richten Sie den zertifikatbasierten API-Zugriff ein

Statt der Benutzer-ID- und Kennwortauthentifizierung für den REST-API- oder NetApp Manageability SDK-Zugriff auf ONTAP muss die zertifikatbasierte Authentifizierung verwendet werden.

Als Alternative zur zertifikatbasierten Authentifizierung für REST-API verwenden Sie "OAuth 2.0 Token-basierte Authentifizierung".)

Sie können ein selbstsigniertes Zertifikat auf ONTAP erstellen und installieren, wie in den folgenden Schritten beschrieben.

**Schritte**

1. Erstellen Sie mithilfe von OpenSSL ein Zertifikat, indem Sie den folgenden Befehl ausführen:

```
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'
```

Dieser Befehl erzeugt ein öffentliches Zertifikat mit dem Namen `test.pem` und einen privaten Schlüssel mit dem Namen `key.out`. Der allgemeine Name CN entspricht der ONTAP-Benutzer-ID.

2. Installieren Sie den Inhalt des öffentlichen Zertifikats im Format Privacy Enhanced Mail (pem) in ONTAP, indem Sie den folgenden Befehl ausführen und den Inhalt des Zertifikats einfügen, wenn Sie dazu aufgefordert werden:

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

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

3. Aktivieren Sie ONTAP, um den Clientzugriff über SSL zu erlauben, und definieren Sie die Benutzer-ID für den API-Zugriff.

```
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
```

Im folgenden Beispiel ist die Benutzer-ID `cert_user` nun für die Verwendung des zertifikatauthentifizierten API-Zugriffs aktiviert. Ein einfaches Manageability SDK Python-Skript, das zur Anzeige der ONTAP-Version verwendet `cert_user` wird, wird wie folgt angezeigt:

```
#!/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)
```

Die Ausgabe des Skripts zeigt die ONTAP-Version an.

```
./version.py

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

4. Führen Sie folgende Schritte durch, um eine zertifikatbasierte Authentifizierung mit der ONTAP REST API durchzuführen:
   a. Definieren Sie in ONTAP die Benutzer-ID für HTTP-Zugriff:

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

b. Führen Sie auf Ihrem Linux-Client den folgenden Befehl aus, der die ONTAP-Version als Ausgabe erzeugt:

```
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"
        }
    }
}
```

**Weitere Informationen**

- "Zertifikatbasierte Authentifizierung mit dem NetApp Manageability SDK für ONTAP".

## ONTAP OAuth 2.0 Token-basierte Authentifizierung für REST-API

Als Alternative zur zertifikatbasierten Authentifizierung können Sie die auf OAuth 2.0 Token-basierte Authentifizierung für REST-API verwenden.

Ab ONTAP 9.14.1 haben Sie die Möglichkeit, den Zugriff auf Ihre ONTAP-Cluster über das Open Authorization (OAuth 2.0)-Framework zu steuern. Sie können diese Funktion über jede der ONTAP-Administrationsschnittstellen konfigurieren, einschließlich der ONTAP-CLI, System Manager und REST-API. Die OAuth 2.0-Autorisierungs- und Zugriffskontrollentscheidungen können jedoch nur angewendet werden, wenn ein Client über die REST-API auf ONTAP zugreift.

OAuth 2.0-Token ersetzen Passwörter für die Benutzerkontoauthentifizierung.

Weitere Informationen zur Verwendung von OAuth 2.0 finden Sie im "ONTAP-Dokumentation zur Authentifizierung und Autorisierung mit OAuth 2.0".

## Anmelde- und Kennwortparameter

Eine effektive Sicherheitslage hält die festgelegten Unternehmensrichtlinien, Richtlinien und alle Governance- oder Standards ein, die für das Unternehmen gelten. Beispiele für diese Anforderungen sind die Lebensdauer des Benutzernamens, Anforderungen an die Länge des Passworts, Zeichenanforderungen und die Speicherung solcher Konten. Die ONTAP-Lösung bietet Funktionen für diese Sicherheitsstrukturen.

### Neue lokale Kontofunktionen

Zur Unterstützung der Richtlinien, Richtlinien oder Standards für Benutzerkonten eines Unternehmens, einschließlich Governance, wird in ONTAP die folgende Funktionalität unterstützt:

- Konfigurieren von Passwortrichtlinien zur Durchsetzung einer Mindestanzahl von Ziffern, Kleinbuchstaben oder Großbuchstaben
- Nach einem fehlgeschlagenen Anmeldeversuch ist eine Verzögerung erforderlich
- Definition des inaktiven Kontonormienlimits
- Ablaufen eines Benutzerkontos
- Eine Warnmeldung zum Ablauf des Kennworts wird angezeigt
- Benachrichtigung über eine ungültige Anmeldung

Konfigurierbare Einstellungen werden über den Befehl Security Login role config modify verwaltet.

### SHA-512-Unterstützung

Um die Passwortsicherheit zu verbessern, unterstützt ONTAP 9 die SHA-2-Passwort-Hash-Funktion und verwendet standardmäßig SHA-512, um neu erstellte oder geänderte Passwörter zu hashen. Operatoren und Administratoren können Konten auch nach Bedarf ablaufen lassen oder sperren.

Bereits vorhandene ONTAP 9-Benutzerkonten mit unveränderten Kennwörtern verwenden nach dem Upgrade auf ONTAP 9.0 oder höher weiterhin die MD5-Hash-Funktion. NetApp empfiehlt jedoch dringend, dass diese Benutzerkonten auf die sicherere SHA-512-Lösung migriert werden, indem Benutzer ihre Passwörter ändern müssen.

Mit der Passwort-Hash-Funktion können Sie die folgenden Aufgaben ausführen:

- Benutzerkonten anzeigen, die mit der angegebenen Hash-Funktion übereinstimmen:

```
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
```

- Konten ablaufen lassen, die eine bestimmte Hash-Funktion (z. B. MD5) verwenden, wodurch Benutzer bei der nächsten Anmeldung gezwungen werden, ihr Passwort zu ändern:

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

- Sperren Sie Konten mit Kennwörtern, die die angegebene Hash-Funktion verwenden.

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

Die Passwort-Hash-Funktion ist für den internen Benutzer in der Administrations-SVM des Clusters unbekannt `autosupport` . Dieses Problem ist kosmetisch. Die Hash-Funktion ist unbekannt, da dieser interne Benutzer standardmäßig kein konfiguriertes Passwort hat.

  - Um die Passwort-Hash-Funktion für den Benutzer anzuzeigen `autosupport` , führen Sie die folgenden Befehle aus:

```
::> 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
```

  - Um die Passwort-Hash-Funktion (Standard: sha512) einzustellen, führen Sie den folgenden Befehl aus:

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

Es spielt keine Rolle, auf welche Art das Passwort eingestellt ist.

```
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
```

**Kennwortparameter**

Die ONTAP Lösung unterstützt Kennwortparameter, die die Anforderungen und Richtlinien des Unternehmens erfüllen und unterstützen.

| Attribut | Beschreibung | Standard | Bereich |
|---|---|---|---|
| `username-minlength` | Mindestlänge des Benutzernamens erforderlich | 3 | 3-16 |
| `username-alphanum` | Benutzername alphanumerisch | Deaktiviert | Aktiviert/deaktiviert |
| `passwd-minlength` | Mindestlänge des Passworts erforderlich | 8 | 3-64 |
| `passwd-alphanum` | Alphanumerisches Passwort | Aktiviert | Aktiviert/deaktiviert |
| `passwd-min-special-chars` | Mindestanzahl an Sonderzeichen im Passwort erforderlich | 0 | 0-64 |
| `passwd-expiry-time` | Passwortablaufzeit (in Tagen) | Unbegrenzt, d. h. die Passwörter laufen nie ab | 0-unbegrenzt<br><br>0 == Jetzt ablaufen lassen |
| `require-initial-passwd-update` | Erste Kennwortaktualisierung bei der ersten Anmeldung erforderlich | Deaktiviert | Aktiviert/deaktiviert<br><br>Änderungen sind über Konsole oder SSH zulässig |
| `max-failed-login-attempts` | Maximale Anzahl fehlgeschlagener Versuche | 0, Konto nicht sperren | - |

| Attribut | Beschreibung | Standard | Bereich |
|---|---|---|---|
| `lockout-duration` | Maximale Sperrzeit (in Tagen) | Der Standardwert ist 0, was bedeutet, dass das Konto für einen Tag gesperrt ist | - |
| `disallowed-reuse` | Letzte N-Kennwörter nicht zulassen | 6 | Der Mindestwert beträgt 6 |
| `change-delay` | Verzögerung zwischen Passwortänderungen (in Tagen) | 0 | - |
| `delay-after-failed-login` | Verzögerung nach jedem fehlgeschlagenen Anmeldeversuch (in Sekunden) | 4 | - |
| `passwd-min-lowercase-chars` | Mindestanzahl an Kleinbuchstaben im Passwort erforderlich | 0. Dies erfordert keine Kleinbuchstaben | 0-64 |
| `passwd-min-uppercase-chars` | Mindestanzahl an alphabetischen Großbuchstaben erforderlich | 0. Dies erfordert keine Großbuchstaben | 0-64 |
| `passwd-min-digits` | Mindestanzahl an Ziffern im Passwort erforderlich | 0, die keine Ziffern erfordert | 0-64 |
| `passwd-expiry-warn-time` | Warnmeldung vor Ablauf des Passworts anzeigen (in Tagen) | Unbegrenzt, was bedeutet, dass Sie nie vor Ablauf des Passworts warnen | 0. Dies bedeutet, dass der Benutzer bei jeder erfolgreichen Anmeldung über den Ablauf des Passworts informiert wird |
| `account-expiry-time` | Konto läuft in N Tagen ab | Unbegrenzt, d. h. die Konten laufen nie ab | Die Verfallszeit des Kontos muss größer sein als das Limit für inaktive Konten |
| `account-inactive-limit` | Maximale Dauer der Inaktivität vor Ablauf des Kontos (in Tagen) | Unbegrenzt. Das bedeutet, dass die inaktiven Konten nie ablaufen | Das Limit für inaktive Konten muss kleiner als die Ablaufdatum des Kontos sein |

**Beispiel**

```
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
```

Seit 9.14.1 gibt es eine erhöhte Komplexität und Sperrregeln für Passwörter. Dies gilt nur für Neuinstallationen von ONTAP.

# Methoden für die

Dies sind wichtige Parameter zur Stärkung der ONTAP-Systemadministration.

## Zugriff über die Befehlszeile

Die Einrichtung eines sicheren Zugriffs auf Systeme ist ein wichtiger Bestandteil der Aufrechterhaltung einer sicheren Lösung. Die häufigsten Optionen für den Zugriff auf die Befehlszeile sind SSH, Telnet und RSH. Davon ist SSH die sicherste, dem Branchenstandard entsprechende Best Practice für den Remote-Zugriff auf die Befehlszeile. NetApp empfiehlt die Verwendung von SSH für den Zugriff über die Befehlszeile auf die ONTAP-Lösung.

### SSH-Konfigurationen

Der `security ssh show` Befehl zeigt die Konfigurationen der SSH Schlüsselaustauschalgorithmen, Chiffren und MAC-Algorithmen für das Cluster und SVMs an. Die Schlüsselaustauschmethode verwendet diese Algorithmen und Chiffren, um festzulegen, wie die einmaligen Sitzungsschlüssel für die Verschlüsselung und

Authentifizierung generiert werden und wie die Serverauthentifizierung stattfindet.

```
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.
```

**Anmeldebanner**

Mithilfe von Anmeldebannern kann ein Unternehmen Bedienern, Administratoren und auch Benutzern mit eingeschränkten Berechtigungen die Bedingungen für eine akzeptable Nutzung anzeigen. Die Banner zeigen an, wer berechtigt ist, auf das System zuzugreifen. Dieser Ansatz ist hilfreich, um Erwartungen an den Zugriff und die Nutzung des Systems zu ermitteln. Mit dem `security login banner modify` Befehl wird das Anmeldebanner geändert. Das Anmeldebanner wird kurz vor dem Authentifizierungsschritt während der SSH- und Konsolengeräteanmeldung angezeigt. Der Bannertext muss in doppelten Anführungszeichen („ “) stehen, wie im folgenden Beispiel gezeigt.

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

**Anmeldebannerparameter**

| Parameter | Beschreibung |
|---|---|
| `vserver` | Verwenden Sie diesen Parameter, um die SVM mit dem geänderten Banner anzugeben. Verwenden Sie den Namen der Administrator-SVM des Clusters, um die Meldung auf Cluster-Ebene zu ändern. Meldung auf Cluster-Ebene wird als Standard für Daten-SVMs verwendet, für die keine Meldung definiert wurde. |

| Parameter | Beschreibung |
| --- | --- |
| `message` | Mit diesem optionalen Parameter kann eine Login-Banner-Meldung angegeben werden. Wenn auf dem Cluster eine Meldung zum Anmeldebanner gesetzt ist, wird das Cluster-Anmeldebanner-Banner von allen Daten-SVMs ebenfalls verwendet. Das Festlegen des Anmeldebanners einer Daten-SVM überschreibt die Anzeige des Cluster-Anmeldebanners. Verwenden Sie diesen Parameter mit dem Wert „-“, um ein Daten-SVM-Anmeldebanner zur Verwendung des Cluster-Anmeldebanners zurückzusetzen.<br><br>Wenn Sie diesen Parameter verwenden, darf das Anmeldebanner keine Zeilenumbrüche (auch als Zeilenende [EOLs] oder Zeilenumbrüche bezeichnet) enthalten. Geben Sie keine Parameter an, um eine Login-Banner-Nachricht mit Zeilenumbrüche einzugeben. Sie werden aufgefordert, die Nachricht interaktiv einzugeben. Interaktiv eingegebene Nachrichten können Zeilenumbrüche enthalten.<br><br>Nicht-ASCII-Zeichen müssen Unicode UTF-8 verwenden. |
| `uri` | `(ftp |
| http):///(hostname | IPv4`<br><br>Verwenden Sie diesen Parameter, um den URI anzugeben, von dem das Anmeldebanner heruntergeladen wird.<br><br>Die Länge der Nachricht darf 2048 Byte nicht überschreiten. Nicht-ASCII-Zeichen müssen als Unicode UTF-8 angegeben werden. |

**Nachricht des Tages**

Der `security login motd modify` Befehl aktualisiert die Nachricht des Tages (MOTD).

Es gibt zwei Kategorien von MOTD: Die Cluster-Level-MOTD und die Daten-SVM-Level-MOTD. Ein Benutzer, der sich bei der Clustershell einer Daten-SVM anmeldet, kann zwei Meldungen sehen: Die MOTD auf Cluster-Ebene gefolgt von der MOTD auf SVM-Ebene für diese SVM.

Der Clusteradministrator kann bei Bedarf die Clusterebene-MOTD auf jeder SVM einzeln aktivieren oder deaktivieren. Wenn der Clusteradministrator die MOTD auf Cluster-Ebene für eine SVM deaktiviert, kann ein Benutzer, der sich bei der SVM anmeldet, die Meldung auf Cluster-Ebene nicht sehen. Nur ein Clusteradministrator kann die Meldung auf Cluster-Ebene aktivieren oder deaktivieren.

| MOTD-Parameter | Beschreibung |
| --- | --- |
| Vserver | Verwenden Sie diesen Parameter, um die SVM anzugeben, für die die MOTD geändert wird. Verwenden Sie den Namen der Administrator-SVM des Clusters, um die Meldung auf Cluster-Ebene zu ändern. |

| MOTD-Parameter | Beschreibung |
| --- | --- |
| Nachricht | Mit diesem optionalen Parameter kann eine Meldung angegeben werden. Wenn Sie diesen Parameter verwenden, kann die MOTD keine Zeilenumbrüche enthalten. Wenn Sie außer dem Parameter keinen anderen Parameter angeben `-vserver` , werden Sie aufgefordert, die Meldung interaktiv einzugeben. Interaktiv eingegebene Nachrichten können Zeilenumbrüche enthalten. Nicht-ASCII-Zeichen müssen als Unicode UTF-8 angegeben werden. Die Nachricht kann dynamisch generierten Inhalt mit den folgenden Escape-Sequenzen enthalten:<br>• `\\` - Ein einziger Gegenspielcharakter<br>• `\b` - Keine Ausgabe (nur zur Kompatibilität mit Linux unterstützt)<br>• `\C` - Cluster-Name<br>• `\d` - Aktuelles Datum wie auf dem Login-Knoten eingestellt<br>• `\t` - Aktuelle Zeit wie auf dem Login-Knoten eingestellt<br>• `\I` - Eingehende LIF IP-Adresse (druckt Konsole für einen `console` Login)<br>• `\l` - Login-Gerätename (druckt Konsole für einen `console` Login)<br>• `\L` - Letzte Anmeldung für den Benutzer auf einem beliebigen Knoten im Cluster<br>• `\m` - Maschinenarchitektur<br>• `\n` - Knoten oder Daten-SVM-Name<br>• `\N` - Name des Benutzers, der sich anmeldet<br>• `\o` - Wie \O. Für Linux-Kompatibilität bereitgestellt.<br>• `\O` - DNS-Domain-Name des Knotens. Beachten Sie, dass die Ausgabe von der Netzwerkkonfiguration abhängt und möglicherweise leer ist.<br>• `\r` - Software-Release-Nummer<br>• `\s` - Name des Betriebssystems<br>• `\u` - Anzahl der aktiven Clustershell-Sitzungen auf dem lokalen Knoten. Für den Cluster-Admin: Alle clustershell-Benutzer. Für den Daten-SVM-Administrator: Nur aktive Sitzungen für diese Daten-SVM<br>• `\U` - Wie `\u`, aber hat `user` oder `users` angehängt<br>• `\v` - Effektive Cluster Version String<br>• `\W` - Aktive Sitzungen im Cluster für die Anmeldung des Benutzers (`who`) |

Weitere Informationen zum Konfigurieren der Tagesnachricht in ONTAP finden Sie im "ONTAP-Dokumentation über die Botschaft des Tages".

### Zeitüberschreitung für CLI-Sitzung

Das standardmäßige Timeout für die CLI-Sitzung beträgt 30 Minuten. Das Timeout ist wichtig, um veraltete Sitzungen und Session Huckepack zu verhindern.

Verwenden Sie den `system timeout show` Befehl, um das aktuelle Timeout für die CLI-Sitzung anzuzeigen.

Verwenden Sie den Befehl, um den Zeitüberschreitungswert festzulegen `system timeout modify -timeout <minutes>`.

## Webzugriff mit NetApp ONTAP System Manager

Wenn ein ONTAP Administrator für den Zugriff und das Management eines Clusters eine grafische Benutzeroberfläche anstelle der CLI verwenden möchte, verwenden Sie NetApp ONTAP System Manager. Sie ist in ONTAP als Webdienst enthalten, standardmäßig aktiviert und über einen Browser zugänglich. Zeigen Sie im Browser auf den Hostnamen, wenn Sie DNS oder die IPv4- oder IPv6-Adresse über verwenden `https://cluster-management-LIF`.

Wenn das Cluster ein selbstsigniertes digitales Zertifikat verwendet, wird im Browser möglicherweise eine Warnung angezeigt, dass das Zertifikat nicht vertrauenswürdig ist. Sie können entweder das Risiko bestätigen, den Zugriff fortzusetzen, oder ein digitales Zertifikat (CA) für die Serverauthentifizierung auf dem Cluster installieren.

Ab ONTAP 9.3 ist die SAML-Authentifizierung (Security Assertion Markup Language) eine Option für den ONTAP-System-Manager.

### SAML-Authentifizierung für ONTAP System Manager

SAML 2.0 ist ein weit verbreiteter Industriestandard, der es jedem SAML-konformen Identitätsanbieter (IdP) von Drittanbietern ermöglicht, MFA mithilfe von Mechanismen durchzuführen, die für das IdP der Unternehmenswahl einzigartig sind, und als Single Sign-On (SSO)-Quelle.

In der SAML-Spezifikation sind drei Rollen definiert: Der Principal, der IdP und der Service Provider. Bei der ONTAP-Implementierung ist der Clusteradministrator, der über ONTAP System Manager oder NetApp Active IQ Unified Manager auf ONTAP zugreifen kann. Das IdP ist eine IdP-Software von Drittanbietern. Ab ONTAP 9.3 werden Microsoft Active Directory Federated Services (ADFS) und das Open-Source-Shibboleth-IdP unterstützt. Ab ONTAP 9.12.1 wird Cisco DUO als IdP unterstützt. Bei dem Service-Provider handelt es sich um die in ONTAP integrierte SAML-Funktion, die vom ONTAP-System-Manager oder der Active IQ Unified Manager-Web-Applikation verwendet wird.

Im Gegensatz zum SSH-Zweifaktor-Konfigurationsprozess müssen sich nach Aktivierung der SAML-Authentifizierung alle vorhandenen Administratoren für den Zugriff auf ONTAP-System-Manager oder ONTAP-Serviceprozessor über das SAML-IdP authentifizieren. Es sind keine Änderungen an den Cluster-Benutzerkonten erforderlich. Wenn die SAML-Authentifizierung aktiviert ist, wird vorhandenen Benutzern mit Administratorrollen für und -Anwendungen eine neue Authentifizierungsmethode von `saml` hinzugefügt `http ontapi`.

Nachdem die SAML-Authentifizierung aktiviert ist, sollten in ONTAP weitere neue Konten definiert werden, die SAML-IdP-Zugriff erfordern, mit der Administratorrolle und der saml-Authentifizierungsmethode für `http` und-`ontapi` Anwendungen. Wenn die SAML-Authentifizierung zu einem bestimmten Zeitpunkt deaktiviert ist, muss für diese neuen Konten die Authentifizierungsmethode mit der Administratorrolle für und-Anwendungen definiert werden. Außerdem muss `password` `http` `ontapi` die Konsolenanwendung für die lokale ONTAP-Authentifizierung in ONTAP System Manager hinzugefügt werden.

Nachdem das SAML-IdP aktiviert wurde, führt das IdP eine Authentifizierung für den Zugriff auf ONTAP-System-Manager durch, indem es Methoden verwendet, die dem IdP zur Verfügung stehen, z. B. LDAP (Lightweight Directory Access Protocol), AD (Active Directory), Kerberos, Passwort usw. Die verfügbaren Methoden sind einzigartig für die IdP. Es ist wichtig, dass die in ONTAP konfigurierten Konten über Benutzer-IDs verfügen, die den IdP-Authentifizierungsmethoden zugeordnet sind.

Von NetApp validierte IDPs sind Microsoft ADFS, Cisco DUO und Open Source Shibboleth IdP.

Ab ONTAP 9.14.1 kann Cisco DUO als zweiter Authentifizierungsfaktor für SSH verwendet werden.

Weitere Informationen zu MFA für ONTAP System Manager, Active IQ Unified Manager und SSH finden Sie unter "TR-4647: Multifaktor-Authentifizierung in ONTAP 9".

### Einblicke in ONTAP System Manager

Ab ONTAP 9.11.1 bietet ONTAP System Manager Einblicke, die Cluster-Administratoren bei der Optimierung ihrer täglichen Aufgaben unterstützen. Die Erkenntnisse zur Sicherheit basieren auf den Empfehlungen dieses technischen Berichts.

| Security Insight | Entschlossenheit |
|---|---|
| Telnet ist aktiviert | NetApp empfiehlt Secure Shell (SSH) für den sicheren Remote-Zugriff. |
| Remote Shell (RSH) ist aktiviert | NetApp empfiehlt SSH für sicheren Remote-Zugriff. |
| AutoSupport verwendet ein unsicheres Protokoll | AutoSupport ist nicht für den Versand über Link:HTTPS konfiguriert. |
| Der Anmeldebanner ist auf Cluster-Ebene nicht konfiguriert | Warnung, wenn das Anmeldebanner für das Cluster nicht konfiguriert ist. |
| SSH verwendet unsichere Chiffren | Warnung, wenn SSH unsichere Chiffren verwendet. |
| Es sind zu wenige NTP-Server konfiguriert | Warnung, wenn die Anzahl der konfigurierten NTP-Server kleiner als drei ist. |
| Standard-Admin-Benutzer nicht gesperrt | Wenn Sie keine Standard-Administratorkonten (admin oder diag) für die Anmeldung bei System Manager verwenden und diese Konten nicht gesperrt sind, sollten Sie sie sperren. |
| Schutz vor Ransomware: Volumes haben keine Snapshot-Richtlinien | An ein oder mehrere Volumes ist keine angemessene Snapshot-Richtlinie gebunden. |
| Ransomware-Verteidigung: Deaktivieren Sie das automatische Löschen von Snapshots | Die automatische Löschung von Snapshots ist für ein oder mehrere Volumes festgelegt. |
| Volumes werden nicht auf Ransomware-Angriffe überwacht | Autonomer Ransomware-Schutz wird auf mehreren Volumes unterstützt, aber noch nicht konfiguriert. |
| SVMs sind nicht für autonomen Ransomware-Schutz konfiguriert | Autonomer Ransomware-Schutz wird auf mehreren SVMs unterstützt, aber noch nicht konfiguriert. |
| Native FPolicy ist nicht konfiguriert | FPolicy ist nicht für NAS SVMs festgelegt. |
| Aktivieren Sie den autonomen Ransomware-Schutz aktiv-Modus | Mehrere Volumes haben ihren Lernmodus abgeschlossen, und Sie können den aktiven Modus einschalten |
| Die globale FIPS 140-2-2-Compliance ist deaktiviert | Die globale FIPS 140-2-Compliance ist nicht aktiviert. |
| Das Cluster ist nicht für Benachrichtigungen konfiguriert | E-Mails, Webhooks oder SNMP-Traphosts sind nicht für den Empfang von Benachrichtigungen konfiguriert. |

Weitere Informationen zu den Einblicken in ONTAP System Manager finden Sie in der "ONTAP System Manager – Dokumentation zu den Einblicken".

# Autonomer Ransomware-Schutz von ONTAP

Als Ergänzung zur Analyse des Benutzerverhaltens für die Sicherheit von Storage-Workloads analysiert der autonome Ransomware-Schutz von ONTAP Volume-Workloads und Entropie, um Ransomware zu erkennen. Er erstellt einen Snapshot und benachrichtigt den Administrator, wenn der Verdacht eines Angriffs besteht.

ONTAP 9.10.1 bietet nicht nur Ransomware-Erkennung und -Vorbeugung mithilfe externer FPolicy User Behavioral Analytics (UBA) mit NetApp Cloud Insights/Cloud Secure und dem NetApp FPolicy Partner-Ecosystem, sondern auch autonomen Ransomware-Schutz. Der autonome Ransomware-Schutz von ONTAP nutzt eine integrierte Funktion für maschinelles Lernen (ML), die die Volume-Workload-Aktivität plus Daten-Entropie untersucht, um Ransomware automatisch zu erkennen. Es überwacht Aktivitäten, die sich von UBA unterscheiden, so dass es Angriffe erkennen kann, die UBA nicht unterstützt.

Weitere Informationen zu dieser Funktion finden Sie unter "TR-4572: Die NetApp Lösung für Ransomware" oder im "Dokumentation zum autonomen Ransomware-Schutz von ONTAP".

# Prüfung von Storage-Verwaltungssystemen

Stellen Sie die Integrität der Ereignisüberwachung sicher, indem Sie ONTAP-Ereignisse auf einen Remote-Syslog-Server laden. Bei diesem Server könnte es sich um ein Sicherheitsinformationsereignismanagementsystem wie Splunk handelt.

## Senden Sie Syslog

Protokoll- und Audit-Informationen sind für ein Unternehmen im Hinblick auf Support und Verfügbarkeit von unschätzbarem Wert. Zudem handelt es sich bei den in Protokollen (Syslog) und Audit-Berichten enthaltenen Informationen und Details in der Regel um sensible Daten. Um die Sicherheitskontrollen und das Sicherheitsniveau aufrechtzuerhalten, müssen Unternehmen die Protokoll- und Audit-Daten unbedingt sicher managen.

Das verlagern von Syslog-Informationen ist nötig, um den Umfang oder die Auswirkungen einer Sicherheitsverletzung auf ein einzelnes System oder eine einzelne Lösung zu beschränken. Daher empfiehlt NetApp, Syslog-Informationen sicher an einen sicheren Storage- oder Aufbewahrungsort zu verlagern.

### Erstellen Sie ein Ziel für die Protokollweiterleitung

Verwenden Sie den `cluster log-forwarding create` Befehl, um Protokollweiterleitungsziele für die Remote-Protokollierung zu erstellen.

#### Parameter

Verwenden Sie die folgenden Parameter, um den Befehl zu konfigurieren `cluster log-forwarding create`:

- **Ziel-Host.** Dieser Name ist der Hostname oder die IPv4- oder IPv6-Adresse des Servers, an den die Protokolle weitergeleitet werden sollen.

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

- **Zielport.** Dies ist der Port, an dem der Zielserver abhört.

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

- **Protokoll zur Protokollweiterleitung.** Dieses Protokoll wird zum Senden von Meldungen an das Ziel verwendet.

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

  Das Protokoll für die Protokollweiterleitung kann einen der folgenden Werte verwenden:

  - `udp-unencrypted`. Benutzer-Datagram-Protokoll ohne Sicherheit.
  - `tcp-unencrypted`. TCP ohne Sicherheit.
  - `tcp-encrypted`. TCP mit Transport Layer Security (TLS).
- * Überprüfen Sie die Identität des Zielservers.* Wenn dieser Parameter auf true gesetzt ist, wird die Identität des Protokollweiterleitungsziels durch Validierung des Zertifikats überprüft. Der Wert kann nur dann auf TRUE gesetzt werden, wenn der `tcpencrypted` Wert im Protokollfeld ausgewählt ist.

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

- **Syslog-Funktion.** Dieser Wert ist die Syslog-Funktion, die für die weitergeleiteten Protokolle verwendet werden soll.

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

- **Überspringen Sie den Verbindungstest.** Normalerweise überprüft der `cluster log-forwarding create` Befehl, ob das Ziel durch Senden eines ICMP-Ping (Internet Control Message Protocol) erreichbar ist, und schlägt fehl, wenn es nicht erreichbar ist. Wenn Sie diesen Wert so einstellen, `true` dass die Ping-Prüfung umgangen wird, können Sie das Ziel konfigurieren, wenn es nicht erreichbar ist.

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

NetApp empfiehlt, die Verbindung zu einem Typ mit dem `cluster log-forwarding` Befehl zu erzwingen `-tcp-encrypted` .

## Ereignisbenachrichtigung

Der Schutz der Informationen und Daten, die ein System verlassen, ist für die Aufrechterhaltung und das Management der Sicherheit des Systems von entscheidender Bedeutung. Die durch die ONTAP Lösung generierten Ereignisse bieten eine Fülle von Informationen über die Lösung, die verarbeiteten Informationen und vieles mehr. Die Vitalität dieser Daten macht deutlich, dass sie sicher gemanagt und migriert werden müssen.

Der `event notification create` Befehl sendet eine neue Benachrichtigung über eine Reihe von Ereignissen, die durch einen Ereignisfilter definiert wurden, an ein oder mehrere Benachrichtigungsziele. In den folgenden Beispielen werden die Konfiguration für Ereignisbenachrichtigungen und der `event notification show` Befehl dargestellt, mit dem die konfigurierten Filter und Ziele für Ereignisbenachrichtigungen angezeigt werden.

```
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
```

# Storage-Verschlüsselung

Verwenden Sie zur Sicherung sensibler Daten im Falle einer gestohlenen, zurückgegebenen oder umgewandten Festplatte die hardwarebasierte Storage-Verschlüsselung von NetApp oder die softwarebasierte Volume-Verschlüsselung/NetApp Aggregatverschlüsselung. Beide Mechanismen sind nach FIPS-140-2 validiert. Wenn hardwarebasierte Mechanismen mit softwarebasierten Mechanismen verwendet werden, ist die Lösung für das Commercial Solutions for Classified (CSfC)-Programm qualifiziert. Die Lösung bietet erweiterten Schutz für geheime und streng geheime Daten im Ruhezustand sowohl auf der Hardware- als auch auf der Softwareebene.

Die Verschlüsselung ruhender Daten ist wichtig, um sensible Daten bei Diebstahl, Rückgabe oder neuer Verwendung einer Festplatte zu schützen.

ONTAP 9 bietet drei FIPS 140-2-konforme Verschlüsselungslösungen für Daten im Ruhezustand:

- NetApp Storage Encryption (NSE) ist eine Hardwarelösung, die Self-Encrypting Drives verwendet.
- NetApp Volume Encryption (NVE) ist eine Softwarelösung, die die Verschlüsselung beliebiger Daten-Volumes auf jedem Laufwerkstyp ermöglicht, bei dem sie aktiviert wird, mit einem eindeutigen Schlüssel für jedes Volume.
- NetApp Aggregate Encryption (NAE) ist eine Softwarelösung, die die Verschlüsselung beliebiger Daten-Volumes auf beliebigen Laufwerken ermöglicht, wobei sie mit eindeutigen Schlüsseln für jedes Aggregat aktiviert wird.

NSE, NVE und NAE können entweder externes Verschlüsselungsmanagement oder den Onboard Key Manager (OKM) verwenden. Die Verwendung von NSE, NVE und NAE wirkt sich nicht auf die ONTAP Storage-Effizienzfunktionen aus. NVE Volumes sind jedoch von der Aggregatdeduplizierung ausgeschlossen. NAE Volumes werden in die Aggregatdeduplizierung einbezogen und profitieren von ihnen.

OKM bietet eine eigenständige Verschlüsselungslösung für Daten im Ruhezustand mit NSE, NVE oder NAE.

NVE, NAE und OKM verwenden den ONTAP CryptoMod. CryptoMod ist in der nach FIPS 140-2 validierten CMVP-Modulliste aufgeführt. Siehe "FIPS 140-2 Cert# 4144".

Verwenden Sie zum Starten der OKM-Konfiguration den `security key-manager onboard enable` Befehl. Um externe KMIP-Schlüsselmanager (Key Management Interoperability Protocol) zu konfigurieren, verwenden Sie den `security key-manager external enable` Befehl. Ab ONTAP 9.6 wird die Mandantenfähigkeit für externe Schlüsselmanager unterstützt. Verwenden Sie den `-vserver <vserver name>` Parameter, um das externe Verschlüsselungsmanagement für eine bestimmte SVM zu aktivieren. Vor 9.6 wurde der `security key-manager setup` Befehl verwendet, um sowohl OKM als auch externe Schlüsselmanager zu konfigurieren. Für das Onboard-Verschlüsselungsmanagement leitet diese Konfiguration den Bediener oder Administrator durch die Passphrase-Einrichtung und zusätzliche Parameter für die Konfiguration von OKM.

Ein Teil der Konfiguration wird im folgenden Beispiel dargestellt:

```
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.
```

Ab ONTAP 9.4 können Sie die Option true mit verwenden `-enable-cc-mode` `security key-manager setup` , um die Eingabe der Passphrase nach einem Neustart durch Benutzer zu verlangen. Für ONTAP 9.6 und höher lautet die Befehlssyntax `security key-manager onboard enable -cc-mode-enabled yes`.

Ab ONTAP 9.4 können Sie die Funktion mit erweiterten Berechtigungen verwenden `secure-purge` , um Daten auf NVE-fähigen Volumes unterbrechungsfrei zu „Scrub“. Durch das Scrubbing von Daten auf einem verschlüsselten Volume wird sichergestellt, dass sie nicht von den physischen Medien wiederhergestellt werden können. Mit dem folgenden Befehl werden die gelöschten Dateien auf vol1 auf SVM vs1 sicher gelöscht:

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

Ab ONTAP 9.7 sind NAE und NVE standardmäßig aktiviert, wenn die VE-Lizenz vorhanden ist, OKM- oder externe Schlüsselmanager konfiguriert werden und NSE nicht verwendet wird. NAE-Volumes werden auf NAE-Aggregaten standardmäßig erstellt und NVE-Volumes werden standardmäßig auf nicht-NAE-Aggregaten erstellt. Sie können diesen umgehen, indem Sie den folgenden Befehl eingeben:

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

Ab ONTAP 9.6 können Sie mithilfe eines SVM-Umfangs externes Verschlüsselungsmanagement für eine Daten-SVM im Cluster konfigurieren. Dies ist insbesondere für mandantenfähige Umgebungen geeignet, in denen jeder Mandant eine andere SVM (oder einen Satz SVMs) zur Bereitstellung von Daten verwendet. Nur der SVM-Administrator für einen bestimmten Mandanten hat Zugriff auf die Schlüssel für den jeweiligen Mandanten. Weitere Informationen finden Sie unter "Aktivieren Sie das externe Schlüsselmanagement in ONTAP 9.6 und höher" in der ONTAP-Dokumentation.

Ab ONTAP 9.11.1 können Sie die Konnektivität zu geclusterten externen Schlüsselmanagementservern konfigurieren, indem Sie primäre und sekundäre Schlüsselserver auf einer SVM festlegen. Weitere Informationen finden Sie unter "Konfiguration von geclusterten externen Schlüsselservern" in der ONTAP-Dokumentation.

Ab ONTAP 9.13.1 können Sie externe Schlüsselmanager-Server im System Manager konfigurieren. Weitere Informationen finden Sie unter "Management externer Schlüsselmanager" in der ONTAP-Dokumentation.

# Datenreplizierung Verschlüsselung

## Als Ergänzung zur Verschlüsselung von Daten im Ruhezustand können Sie den ONTAP-Datenverkehr zwischen Clustern mithilfe von TLS 1.2 mit einem vorab gemeinsam genutzten Schlüssel für SnapMirror, SnapVault oder FlexCache verschlüsseln.

Bei der Replizierung von Daten für Disaster Recovery, Caching oder Backup müssen die Daten während der Übertragung über das Netzwerk von einem ONTAP Cluster zum anderen gesichert werden. Auf diese Weise werden böswillige man-in-the-Middle-Angriffe auf sensible Daten während der Übertragung verhindert.

Ab ONTAP 9.6 bietet Cluster-Peering-Verschlüsselung TLS 1.2 AES-256 GCM-Verschlüsselung für ONTAP Datenreplizierungsfunktionen wie SnapMirror, SnapVault und FlexCache. Die Verschlüsselung wird über einen vorab freigegebenen Schlüssel (PSK) zwischen zwei Cluster-Peers eingerichtet.

Unternehmen, die Technologien wie NSE, NVE und NAE zur Sicherung von Daten im Ruhezustand einsetzen, können außerdem die End-to-End-Datenverschlüsselung durch Upgrade auf ONTAP 9.6 oder höher zur Verwendung der Cluster-Peering-Verschlüsselung nutzen.

Cluster-Peering verschlüsselt alle Daten zwischen den Cluster-Peers. Wenn Sie beispielsweise SnapMirror verwenden, werden alle Peering-Informationen sowie alle SnapMirror Beziehungen zwischen dem Quell- und Ziel-Cluster-Peer verschlüsselt. Sie können keine Klartextdaten zwischen Cluster-Peers senden, für die die Cluster-Peering-Verschlüsselung aktiviert ist.

Ab ONTAP 9.6 ist bei neuen Cluster-Peer-Beziehungen standardmäßig die Verschlüsselung aktiviert. Um die Verschlüsselung für Cluster-Peer-Beziehungen zu aktivieren, die vor ONTAP 9.6 erstellt wurden, müssen Sie

das Quell- und Ziel-Cluster auf 9.6 aktualisieren. Darüber hinaus müssen Sie den Befehl verwenden `cluster peer modify` , um die Quell- und Ziel-Cluster-Peers zu ändern, um Cluster-Peering-Verschlüsselung zu verwenden.

Sie können eine vorhandene Peer-Beziehung in ONTAP 9.6 umwandeln, um die Cluster-Peering-Verschlüsselung zu verwenden, wie im folgenden Beispiel gezeigt:

```
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.
```

# IPsec-Verschlüsselung von aktiven Daten

Unternehmen, die Verschlüsselungstechnologien für ruhende Daten wie NetApp Storage Encryption (NSE) oder NetApp Volume Encryption (NVE) und Cluster Peering Encryption (CPE) für den Datenreplizierungsverkehr verwenden, können jetzt durch ein Upgrade auf ONTAP 9.8 oder höher die End-to-End-Verschlüsselung zwischen Client und Storage in ihrer hybriden Multi-Cloud-Data Fabric nutzen IPsec: IPsec bietet eine Alternative zur NFS- oder SMB/CIFS-Verschlüsselung und ist die einzige Option für die Verschlüsselung bei iSCSI-Datenverkehr.

In manchen Situationen müssen möglicherweise alle Client-Daten geschützt werden, die über das Netzwerk (oder bei der Übertragung) zu der ONTAP SVM übertragen werden. Dadurch werden Replay- und böswillige man-in-the-Middle-Angriffe auf sensible Daten während der Übertragung verhindert.

Ab ONTAP 9.8 bietet die Internetprotokollsicherheit (IPsec) End-to-End-Verschlüsselungsunterstützung für den gesamten IP-Datenverkehr zwischen einem Client und einer ONTAP SVM. Die IPsec-Datenverschlüsselung für den gesamten IP-Datenverkehr umfasst NFS-, iSCSI- und SMB/CIFS-Protokolle. IPsec bietet die einzige Verschlüsselung im Flug für iSCSI-Datenverkehr.

Die Bereitstellung von NFS-Verschlüsselung über das Netzwerk ist einer der wichtigsten Anwendungsfälle für IPsec. Vor ONTAP 9.8 war für die NFS-Verschlüsselung über das Netzwerk die Einrichtung und Konfiguration von Kerberos erforderlich, damit die aktiven NFS-Daten über krb5p verschlüsselt werden. Dies ist nicht immer einfach oder leicht in jeder Kundenumgebung zu erreichen.

Unternehmen, die Verschlüsselungstechnologien für ruhende Daten wie NetApp Storage Encryption (NSE) oder NetApp Volume Encryption (NVE) und Cluster Peering Encryption (CPE) für den Datenreplizierungsverkehr verwenden, können jetzt durch ein Upgrade auf ONTAP 9.8 oder höher die End-to-End-Verschlüsselung zwischen Client und Storage in ihrer hybriden Multi-Cloud-Data Fabric nutzen IPsec:

IPsec ist ein IETF-Standard. ONTAP verwendet IPsec im Transportmodus. Es nutzt auch das IKE-Protokoll (Internet Key Exchange) Version 2, das einen Pre-Shared Key (PSK) verwendet, um Schlüsselmaterial zwischen dem Client und ONTAP entweder mit IPv4 oder IPv6 auszuhandeln. Standardmäßig verwendet IPsec Suite-B AES-GCM 256-Bit-Verschlüsselung. Suite-B AES-GMAC256 und AES-CBC256 mit 256-Bit-Verschlüsselung werden ebenfalls unterstützt.

Obwohl die IPsec-Funktion auf dem Cluster aktiviert werden muss, wird sie durch Verwendung eines SPD-Eintrags (Security Policy Database) auf einzelne SVM-IP-Adressen angewendet. Der Richtlinieneintrag (SPD) enthält die Client-IP-Adresse (Remote-IP-Subnetz), die SVM-IP-Adresse (lokales IP-Subnetz), die zu verwendende Verschlüsselungssuite und den Pre-Shared-Schlüssel (PSK), der für die Authentifizierung über IKEv2 und den Aufbau der IPsec-Verbindung benötigt wird. Zusätzlich zum IPsec-Richtlinieneintrag muss der Client mit denselben Informationen (lokale und Remote-IP, PSK und Chiffre-Suite) konfiguriert werden, bevor der Datenverkehr über die IPsec-Verbindung fließen kann. Ab ONTAP 9.10.1 wird die IPsec-Zertifikatauthentifizierung unterstützt. Dadurch werden IPsec-Richtlinienbeschränkungen entfernt und Windows-Betriebssystemunterstützung für IPsec aktiviert.

Wenn zwischen dem Client und der SVM-IP-Adresse eine Firewall vorhanden ist, muss die ESP- und UDP-Protokolle (Port 500 und 4500) sowohl Inbound (Ingress) als auch Outbound (Egress) zugelassen werden, damit die IKEv2-Verhandlung erfolgreich ist und damit IPsec-Datenverkehr ermöglicht wird.

Für die Verkehrsverschlüsselung mit NetApp SnapMirror und Cluster-Peering wird die Cluster-Peering-Verschlüsselung (CPE) für die sichere Übertragung über das Netzwerk weiterhin über IPsec empfohlen. CPE bietet für diese Workloads eine bessere Performance als IPsec. Sie benötigen keine Lizenz für IPsec und es gibt keine Import- oder Exportbeschränkungen.

Sie können IPsec auf dem Cluster aktivieren und einen SPD-Eintrag für einen einzelnen Client und eine einzelne SVM-IP-Adresse erstellen, wie im folgenden Beispiel gezeigt:

```
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).
```

# TLS und SSL-Management

## Sie können den FIPS 140-2/3-Compliance-Modus für Schnittstellen der Kontrollebene aktivieren, indem Sie den Parameter mit dem ONTAP-Befehl auf „true“ setzen `is-fips-enabled` `security config modify`.

Ab ONTAP 9 können Sie den FIPS 140-2-Compliance-Modus für Cluster-weite Kontrollebene-Schnittstellen aktivieren. Standardmäßig ist der reine FIPS 140-2-Modus deaktiviert. Sie können den FIPS 140-2-Compliance-Modus aktivieren, indem Sie den Parameter für den Befehl auf setzen `is-fips-enabled` `true` `security config modify`. Sie können dann den Online-Status mithilfe des `security config show command` bestätigen.

Wenn die FIPS 140-2-Konformität aktiviert ist, sind TLSv1 und SSLv3 deaktiviert, und nur TLSv1.1 und

TLSv1.2 bleiben aktiviert. ONTAP verhindert, dass Sie TLSv1 und SSLv3 aktivieren, wenn die FIPS 140-2-Compliance aktiviert ist. Wenn Sie FIPS 140-2 aktivieren und anschließend deaktivieren, bleiben TLSv1 und SSLv3 deaktiviert, TLSv1.2 oder TLSv1.1 und TLSv1.2 bleiben jedoch aktiviert, je nach vorheriger Konfiguration.

Mit dem `security config modify` Befehl wird die vorhandene Cluster-weite Sicherheitskonfiguration geändert. Wenn Sie den FIPS-konformen Modus aktivieren, wählt das Cluster automatisch nur TLS-Protokolle aus. Verwenden Sie den `-supported-protocols` Parameter, um TLS-Protokolle unabhängig vom FIPS-Modus ein- oder auszuschließen. Standardmäßig ist der FIPS-Modus deaktiviert, und ONTAP unterstützt die Protokolle TLSv1.2, TLSv1.1 und TLSv1.

Zur Rückwärtskompatibilität unterstützt ONTAP das Hinzufügen von SSLv3 zur Liste, wenn der `supported-protocols` FIPS-Modus deaktiviert ist. Verwenden Sie den `-supported-cipher-suites` Parameter, um nur den Advanced Encryption Standard (AES) oder AES und 3DES zu konfigurieren. Sie können auch schwache Chiffren wie RC4 deaktivieren, indem Sie !RC4 angeben. Standardmäßig ist die unterstützte Chiffre-Einstellung `ALL:!LOW:!aNULL:!EXP:!eNULL`. Diese Einstellung bedeutet, dass alle unterstützten Cipher-Suites für die Protokolle aktiviert sind, mit Ausnahme der Suiten ohne Authentifizierung, ohne Verschlüsselung, ohne Exporte und mit geringer Verschlüsselung. Diese Suiten verwenden 64-Bit- oder 56-Bit-Verschlüsselungsalgorithmen.

Wählen Sie eine Verschlüsselungssuite aus, die mit dem entsprechenden ausgewählten Protokoll verfügbar ist. Eine ungültige Konfiguration kann dazu führen, dass einige Funktionen nicht ordnungsgemäß funktionieren.

Die korrekte Syntax der Chiffren-Zeichenketten finden Sie auf der "Verschlüsselung" Seite zu OpenSSL (veröffentlicht von OpenSSL Software Foundation). Ab ONTAP 9.9.1 und neueren Versionen müssen Sie nach Änderung der Sicherheitskonfiguration nicht mehr alle Nodes manuell neu booten.

Die Aktivierung der FIPS 140-2-2-Konformität hat Auswirkungen auf andere interne und externe Systeme und die Kommunikation mit ONTAP 9. NetApp empfiehlt dringend, diese Einstellungen auf einem nicht-produktiven System mit Konsolenzugriff zu testen.

> Wenn SSH zur Verwaltung von ONTAP 9 verwendet wird, müssen Sie einen OpenSSH 5.7 oder höher-Client verwenden. SSH-Clients müssen mit dem öffentlichen Schlüsselalgorithmus Elliptic Curve Digital Signature Algorithm (ECDSA) verhandeln, damit die Verbindung erfolgreich hergestellt werden kann.

TLS-Sicherheit kann weiter gehärtet werden, indem nur TLS 1.2 aktiviert und Perfect Forward Secrecy (PFS)-fähige Chiffre Suites verwendet werden. PFS ist eine Methode des Schlüsselaustauschs, die in Kombination mit Verschlüsselungsprotokollen wie TLS 1.2 einen Angreifer daran hindert, alle Netzwerksitzungen zwischen einem Client und einem Server zu entschlüsseln. Um nur TLS 1.2- und PFS-fähige Chiffren-Suites zu aktivieren, verwenden Sie den `security config modify` Befehl von der erweiterten Berechtigungsebene aus, wie im folgenden Beispiel gezeigt.

> Bevor Sie die Konfiguration der SSL-Schnittstelle ändern, ist es wichtig zu beachten, dass der Client die erwähnte Verschlüsselung (DHE, ECDHE) bei der Verbindung mit ONTAP unterstützen muss. Andernfalls ist die Verbindung nicht zulässig.

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

Bestätigen Sie `y` für jede Eingabeaufforderung. Weitere Informationen zu PFS finden Sie unter "In diesem NetApp Blog".

Ab ONTAP 9.11.1 und TLS 1.3-Unterstützung können Sie FIPS 140-3 validieren.

Die FIPS-Konfiguration gilt für ONTAP und die Plattform BMC.

# Erstellen Sie ein CA-signiertes digitales Zertifikat

Für viele Unternehmen ist das selbstsignierte digitale Zertifikat für den ONTAP-Webzugriff nicht mit den InfoSec-Richtlinien kompatibel. Auf Produktionssystemen ist es eine NetApp Best Practice, ein CA-signiertes digitales Zertifikat zu installieren, das zur Authentifizierung des Clusters oder der SVM als SSL-Server verwendet wird.

Sie können den Befehl verwenden `security certificate generate-csr` , um eine Zertifikatsignierungsanforderung (CSR) zu generieren, und den `security certificate install` Befehl, um das Zertifikat zu installieren, das Sie von der Zertifizierungsstelle zurückerhalten.

**Schritte**

1. Gehen Sie wie folgt vor, um ein digitales Zertifikat zu erstellen, das von der Zertifizierungsstelle des Unternehmens signiert wurde:
   a. CSR erstellen.
   b. Befolgen Sie die Anweisungen Ihres Unternehmens, um ein digitales Zertifikat über die CSR von der Zertifizierungsstelle Ihres Unternehmens anzufordern. Gehen Sie beispielsweise über die Microsoft Active Directory-Zertifikatdienste-Webschnittstelle zu `<CA_server_name>/certsrv` und fordern Sie ein Zertifikat an.
   c. Installieren Sie das digitale Zertifikat in ONTAP.

# Online-Protokoll für den Zertifikatsstatus

Mit dem Online Certificate Status Protocol (OCSP) können ONTAP-Applikationen, die TLS-Kommunikation wie LDAP oder TLS verwenden, einen digitalen Zertifikatsstatus erhalten, wenn OCSP aktiviert ist. Die Applikation erhält eine signierte Antwort, die angibt, ob das angeforderte Zertifikat in Ordnung, annulliert oder unbekannt ist.

OCSP ermöglicht die Ermittlung des aktuellen Status eines digitalen Zertifikats, ohne dass Zertifikatsperrlisten (Certificate Revocation Lists, CRLs) erforderlich sind.

Standardmäßig ist die Überprüfung des OCSP-Zertifikatsstatus deaktiviert. Es kann mit dem Befehl eingeschaltet werden `security config ocsp enable -app name`, wo der App-Name sein kann `autosupport`, , `audit_log` `fabricpool` `ems`, , , `kmip`, `ldap_ad` `ldap_nis_namemap`, oder alle. Für den Befehl ist eine erweiterte Berechtigungsebene erforderlich.

# SSHv2-Management

Mit dem `security ssh modify` Befehl werden die vorhandenen Konfigurationen der SSH-Schlüsselaustauschalgorithmen, Chiffren oder MAC-Algorithmen für das Cluster oder eine SVM durch die von Ihnen angegebenen Konfigurationseinstellungen ersetzt.

NetApp empfiehlt Folgendes:

- Verwenden Sie Passwörter für Benutzersitzungen.
- Verwenden Sie einen öffentlichen Schlüssel für den Maschinenzugriff.

## Unterstützte Chiffren und Schlüsselaustausch

| Verschlüsselung | Schlüsselaustausch |
|---|---|
| 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 | - |

## Unterstützte symmetrische AES- und 3DES-Verschlüsselungen

ONTAP unterstützt auch die folgenden Arten von symmetrischen AES- und 3DES-Verschlüsselungen (auch als Chiffren bezeichnet):

- 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

Die SSH-Verwaltungskonfiguration gilt für ONTAP und die Plattform BMC.

# NetApp AutoSupport

Mit der AutoSupport Funktion von ONTAP überwachen Sie proaktiv den Zustand Ihres Systems und senden automatisch Nachrichten und Details an den technischen Support von NetApp, das interne Support-Team Ihres Unternehmens oder einen Support-Partner. Standardmäßig sind AutoSupport Meldungen an den technischen Support von NetApp aktiviert, wenn das Storage-System zum ersten Mal konfiguriert wird. Darüber hinaus sendet AutoSupport 24 Stunden nach Aktivierung Nachrichten an den technischen Support von NetApp. Dieser Zeitraum von 24 Stunden ist konfigurierbar. Um die Kommunikation mit dem internen Support-Team eines Unternehmens nutzen zu können, muss die Konfiguration des Mail-Hosts abgeschlossen sein.

Das AutoSupport-Management (Konfiguration) kann nur vom Clusteradministrator durchgeführt werden. Der SVM-Administrator hat keinen Zugriff auf AutoSupport. Die AutoSupport-Funktion kann deaktiviert werden. NetApp empfiehlt jedoch die Aktivierung, da mit AutoSupport Probleme schneller identifiziert und gelöst werden können, sollte auf dem Storage-System ein Problem auftreten. Standardmäßig erfasst das System AutoSupport-Informationen und speichert diese lokal, selbst wenn Sie AutoSupport deaktivieren.

Weitere Details zu AutoSupport Meldungen, einschließlich der Inhalte in den verschiedenen Meldungen und wo verschiedene Meldungstypen gesendet werden, finden Sie in der "NetApp Active IQ Digital Advisor" Dokumentation.

AutoSupport-Meldungen enthalten sensible Daten, wie z. B. die folgenden Elemente:

- Log-Dateien
- Kontextsensitive Daten zu spezifischen Subsystemen
- Konfigurations- und Statusdaten
- Performance-Daten

AutoSupport unterstützt HTTPS, HTTP und SMTP für Transportprotokolle. Aufgrund der sensible Natur von AutoSupport Meldungen empfiehlt NetApp dringend, HTTPS als Standard-Transportprotokoll für das Senden von AutoSupport Meldungen an die NetApp Unterstützung zu verwenden.

Zusätzlich sollten Sie den Befehl nutzen `system node autosupport modify`, um die Ziele von AutoSupport-Daten anzugeben (z. B. technischer Support von NetApp, interne Vorgänge eines Unternehmens oder Partner). Mit diesem Befehl können Sie auch angeben, welche spezifischen AutoSupport-Details gesendet werden sollen (z. B. Performance-Daten, Log-Dateien usw.).

Um AutoSupport vollständig zu deaktivieren, verwenden Sie den `system node autosupport modify -state disable` Befehl.

# Network Time Protocol

Obwohl Sie mit ONTAP die Zeitzone, das Datum und die Uhrzeit auf dem Cluster manuell festlegen können, müssen Sie die NTP-Server (Network Time Protocol) konfigurieren, damit die Cluster-Zeit mit mindestens drei externen NTP-Servern synchronisiert wird.

Wenn die Cluster-Zeit nicht stimmt, können Probleme auftreten. ONTAP ermöglicht Ihnen zwar das manuelle Einstellen der Zeitzone, des Datums und der Uhrzeit auf dem Cluster, Sie müssen jedoch die NTP-Server (Network Time Protocol) konfigurieren, damit die Cluster-Zeit mit externen NTP-Servern synchronisiert wird.

Ab ONTAP 9.5 können Sie Ihren NTP-Server mit symmetrischer Authentifizierung konfigurieren.

Mit dem Befehl können Sie maximal 10 externe NTP-Server verknüpfen `cluster time-service ntp server create` . Um Redundanz und Qualität des Zeitdienstes zu gewährleisten, sollten Sie mindestens drei externe NTP-Server mit dem Cluster verbinden.

Details zur Konfiguration von NTP in ONTAP finden Sie unter "Verwalten der Cluster-Zeit (nur Cluster-Administratoren)".

# Lokale NAS-Dateisystemkonten (CIFS-Arbeitsgruppe)

Die Workgroup-Client-Authentifizierung bietet eine zusätzliche Sicherheitsebene für die ONTAP-Lösung, die mit der herkömmlichen Domänenauthentifizierung konsistent ist. Verwenden Sie den `vserver cifs session show` Befehl, um zahlreiche Details zu den Positionen anzuzeigen, einschließlich IP-Informationen, des Authentifizierungsmechanismus, der Protokollversion und des Authentifizierungstyps.

Ab ONTAP 9 können Sie einen CIFS-Server in einer Arbeitsgruppe mit CIFS-Clients konfigurieren, die sich mithilfe lokal definierter Benutzer und Gruppen beim Server authentifizieren. Die Workgroup-Client-Authentifizierung bietet eine zusätzliche Sicherheitsebene für die ONTAP-Lösung, die mit der herkömmlichen Domänenauthentifizierung konsistent ist. Verwenden Sie zum Konfigurieren des CIFS-Servers den `vserver cifs create` Befehl. Nachdem der CIFS-Server erstellt wurde, können Sie ihn einer CIFS-Domäne hinzufügen oder einer Arbeitsgruppe beitreten. Um einer Arbeitsgruppe beizutreten, verwenden Sie den `-workgroup` Parameter. Hier ist eine Beispielkonfiguration:

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

Ein CIFS-Server im Arbeitsgruppenmodus unterstützt nur die NTLM-Authentifizierung (Windows NT LAN Manager) und unterstützt keine Kerberos-Authentifizierung.

NetApp empfiehlt die Verwendung der NTLM-Authentifizierungsfunktion mit CIFS-Arbeitsgruppen, um die Sicherheit Ihres Unternehmens aufrechtzuerhalten. Zum Validieren der CIFS-Sicherheitslage empfiehlt NetApp, mithilfe des `vserver cifs session show` Befehls zahlreiche Details zum Thema Haltung anzuzeigen, einschließlich IP-Informationen, des Authentifizierungsmechanismus, der Protokollversion und des Authentifizierungstyps.

# NAS-Filesystem-Auditing

NAS-Dateisysteme nehmen in der heutigen Bedrohungslandschaft einen größeren Platz ein, Audit-Funktionen sind für die Transparenz von entscheidender Bedeutung.

Sicherheit erfordert Validierung. ONTAP 9 bietet mehr Auditing-Ereignisse und Details in der gesamten Lösung. Da NAS-Dateisysteme in der heutigen Bedrohungslandschaft einen größeren Platz einnehmen, sind Audit-Funktionen für die Transparenz von entscheidender Bedeutung. Dank der verbesserten Audit-Funktion von ONTAP 9 sind CIFS-Audit-Details zahlreicher als je zuvor. Wichtige Details, einschließlich folgender, werden mit erstellten Ereignissen protokolliert:

- Datei-, Ordner- und Freigabezugriff
- Erstellte, bearbeitete oder gelöschte Dateien
- Erfolgreicher Lesezugriff auf die Datei
- Fehlgeschlagene Versuche, Dateien zu lesen oder zu schreiben
- Geänderte Ordnerrechte

## Erstellen Sie eine Überwachungskonfiguration

Sie müssen CIFS-Überwachung aktivieren, um Auditing-Ereignisse zu generieren. Erstellen Sie mit dem `vserver audit create` Befehl eine Überwachungskonfiguration. Standardmäßig verwendet das Audit-Protokoll eine auf Größe basierende Rotationsmethode. Sie können eine zeitbasierte Rotationsoption verwenden, wenn sie im Feld Rotationsparameter angegeben ist. Weitere Konfigurationsdetails für die Protokollaudit-Rotation sind der Rotationszeitplan, die Rotationsgrenzen, die Rotationstage der Woche und die Rotationsgröße. Der folgende Text enthält eine Beispielkonfiguration, die eine Überwachungskonfiguration mit einer monatlichen, zeitbasierten Rotation darstellt, die für alle Wochentage um 12:30 Uhr geplant ist.

```
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
```

## CIFS-Audit-Ereignisse

CIFS-Audit-Ereignisse sind wie folgt:

- **Dateifreigabe**: Erzeugt ein Audit-Ereignis, wenn eine CIFS-Netzwerkfreigabe mit den zugehörigen Befehlen hinzugefügt, geändert oder gelöscht wird `vserver cifs share .`
- **Änderung der Überwachungsrichtlinie**: Erzeugt ein Audit-Ereignis, wenn die Überwachungsrichtlinie mit den zugehörigen Befehlen deaktiviert, aktiviert oder geändert wird `vserver audit .`
- **Benutzerkonto**: Erzeugt ein Audit-Ereignis, wenn ein lokaler CIFS- oder UNIX-Benutzer erstellt oder gelöscht wird; ein lokales Benutzerkonto aktiviert, deaktiviert oder geändert wird; oder ein Passwort zurückgesetzt oder geändert wird. Dieses Ereignis verwendet den `vserver cifs users-and-groups local-group` Befehl oder den entsprechenden `vserver services name-service unix-user` Befehl.
- **Sicherheitsgruppe**: Erzeugt ein Auditereignis, wenn eine lokale CIFS- oder UNIX-Sicherheitsgruppe mit dem Befehl oder dem entsprechenden Befehl erstellt oder gelöscht wird `vserver cifs users-and-groups local-group vserver services name-service unix-group .`

- **Änderung der Autorisierungsrichtlinie**: Erzeugt ein Auditereignis, wenn Rechte für einen CIFS-Benutzer oder eine CIFS-Gruppe mit dem Befehl gewährt oder aufgehoben werden `vserver cifs users-and-groups privilege`.

> Diese Funktion basiert auf der Systemaudit-Funktion, mit der ein Administrator aus Sicht eines Datenbenutzers überprüfen kann, was das System erlaubt und was es ausführt.

## Auswirkungen von REST-APIs auf NAS-Auditing

ONTAP bietet Administratorkonten die Möglichkeit, über REST-APIs auf SMB/CIFS- oder NFS-Dateien zuzugreifen und diese zu bearbeiten. Obwohl REST-APIs nur von ONTAP Administratoren ausgeführt werden können, umgehen REST-API-Befehle das NAS-Revisionsprotokoll des Systems. Darüber hinaus können Dateiberechtigungen von ONTAP-Administratoren bei Verwendung von REST-APIs ignoriert werden. Die Aktionen des Administrators mit REST-APIs für Dateien werden jedoch im Verlaufsprotokoll des Systembefehls erfasst.

### REST-API-Rolle ohne Zugriff erstellen

Sie können verhindern, dass ONTAP-Administratoren REST-APIs für den Dateizugriff verwenden, indem Sie eine REST-API-Rolle erstellen, die über REST keinen Zugriff auf ONTAP Volumes hat. Führen Sie die folgenden Schritte aus, um diese Rolle bereitzustellen.

#### Schritte

1. Erstellen einer neuen REST-Rolle, die keinen Zugriff auf Storage-Volumes hat, aber über alle anderen REST-API-Zugriff verfügt

```
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. Weisen Sie das Administratorkonto der neuen REST-API-Rolle zu, die Sie im vorherigen Schritt erstellt haben.

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

> Wenn Sie verhindern möchten, dass das integrierte ONTAP-Cluster-Administratorkonto REST-APIs für den Dateizugriff verwendet, müssen Sie zuerst "Erstellen Sie ein neues Administratorkonto, und deaktivieren oder löschen Sie das integrierte Konto".

# Konfigurieren und aktivieren Sie das CIFS-SMB-Signing and Sealing

Sie können SMB-Signaturen konfigurieren und aktivieren, die die Sicherheit der Data-Fabric-Architektur schützen, indem dafür gesorgt wird, dass der Datenverkehr zwischen

den Storage-Systemen und den Clients nicht durch Replay- oder man-in-the-Middle-Angriffe beeinträchtigt wird. SMB-Signaturen schützen durch Überprüfung, ob SMB-Nachrichten über gültige Signaturen verfügen.

**Über diese Aufgabe**

Ein gängiger Bedrohungsvektor für Filesysteme und Architekturen ist das SMB-Protokoll. Um diesen Vektor anzugehen, verwendet die ONTAP 9 Lösung das branchenübliche SMB-Signing and Sealing. SMB-Signaturen schützen die Sicherheit der Data-Fabric-Architektur, indem sichergestellt wird, dass der Datenverkehr zwischen den Storage-Systemen und den Clients nicht durch Replay- oder man-in-the-Middle-Angriffe beeinträchtigt wird. Dazu wird sichergestellt, dass SMB-Nachrichten über gültige Signaturen verfügen.

Obwohl die SMB-Signatur im Hinblick auf die Performance standardmäßig deaktiviert ist, empfiehlt NetApp dringend, sie zu aktivieren. Zudem unterstützt die ONTAP Lösung SMB-Verschlüsselung, die auch als Sealing bezeichnet wird. Dieser Ansatz ermöglicht einen sicheren Share-by-Share-Transport der Daten. Die SMB-Verschlüsselung ist standardmäßig deaktiviert. NetApp empfiehlt jedoch, die SMB-Verschlüsselung zu aktivieren.

LDAP-Signing und Sealing werden jetzt in SMB 2.0 und höher unterstützt. Das Signieren (Schutz vor Manipulation) und Sealing (Verschlüsselung) ermöglichen eine sichere Kommunikation zwischen SVMs und Active Directory-Servern. Beschleunigte AES New Instructions (Intel AES NI)-Verschlüsselung wird jetzt in SMB 3.0 und höher unterstützt. Intel AES NI verbessert den AES-Algorithmus und beschleunigt die Datenverschlüsselung mit unterstützten Prozessorfamilien.

**Schritte**

1. Verwenden Sie zum Konfigurieren und Aktivieren von SMB-Signaturen den `vserver cifs security modify` Befehl und überprüfen Sie, ob der `-is-signing-required` Parameter auf festgelegt ist `true`. Siehe folgendes Beispiel:

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

2. Verwenden Sie zum Konfigurieren und Aktivieren von SMB-Sealing und -Verschlüsselung den `vserver cifs security modify` Befehl und überprüfen Sie, ob der `-is-smb-encryption-required` Parameter auf festgelegt ist `true`. Siehe folgendes Beispiel:

```
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
```

# NFS-Sicherung

Exportregeln sind die funktionalen Elemente einer Exportrichtlinie. Die Exportregeln

richten sich nach Client-Zugriffsanforderungen für ein Volume anhand bestimmter Parameter, die Sie konfigurieren, um zu bestimmen, wie mit den Clientzugriffsanfragen umzugehen ist. Eine Exportrichtlinie muss mindestens eine Exportregel enthalten, um den Zugriff auf Clients zu ermöglichen. Wenn eine Exportrichtlinie mehrere Regeln enthält, werden die Regeln in der Reihenfolge verarbeitet, in der sie in der Exportrichtlinie angezeigt werden.

Zugriffssteuerung ist ein zentraler Bestandteil des Sicherheitsstatus. Daher verwendet ONTAP die Funktion für die Exportrichtlinie, um den Zugriff auf NFS-Volumes auf Clients zu beschränken, die mit bestimmten Parametern übereinstimmen. Exportrichtlinien enthalten mindestens eine Exportregel, die jede Clientzugriffsanforderung verarbeitet. Jedem Volume ist eine Exportrichtlinie zugeordnet, um den Client-Zugriff auf das Volume zu konfigurieren. Das Ergebnis dieses Prozesses legt fest, ob dem Client (mit einer Meldung, dass ihm die Berechtigung verweigert wird) der Zugriff auf das Volume gewährt oder verweigert wird. Dieser Prozess bestimmt auch, welche Zugriffsebene auf das Volume bereitgestellt wird.

Für den Zugriff auf Daten durch Clients muss auf einer SVM eine Exportrichtlinie mit Exportrichtlinien vorhanden sein. Eine SVM kann mehrere Exportrichtlinien enthalten.

Die Regelreihenfolge wird durch die Indexnummer der Regel vorgegeben. Wenn eine Regel mit einem Client übereinstimmt, werden die Berechtigungen dieser Regel verwendet und keine weiteren Regeln verarbeitet. Stimmen keine Regeln überein, wird dem Client der Zugriff verweigert.

Exportregeln bestimmen Clientzugriffsberechtigungen, indem die folgenden Kriterien angewendet werden:

- Das Dateizugriffsprotokoll, das vom Client verwendet wird, der die Anforderung sendet (z. B. NFSv4 oder SMB)
- Eine Client-Kennung (z. B. Hostname oder IP-Adresse)
- Der vom Client zur Authentifizierung verwendete Sicherheitstyp (z. B. Kerberos v5, NTLM oder AUTH_SYS)

Wenn in einer Regel mehrere Kriterien angegeben sind und der Client einem oder mehreren Kriterien nicht entspricht, gilt die Regel nicht.

Eine Beispielrichtlinie für den Export enthält eine Exportregel mit den folgenden Parametern:

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

Der Sicherheitstyp legt fest, welche Zugriffsebene ein Client erhält. Die drei Zugriffsebenen sind schreibgeschützt, Lesen/Schreiben und Superuser (für Clients mit der Benutzer-ID `0`). Da die vom Sicherheitstyp festgelegte Zugriffsebene in dieser Reihenfolge bewertet wird, müssen Sie die folgenden Regeln beachten:

## Regeln für Parameter auf Zugriffsebene in Exportregeln

| Für einen Client, um die folgenden Zugriffsebenen zu erhalten | Diese Zugriffsparameter müssen mit dem Sicherheitstyp des Clients übereinstimmen |
|---|---|
| Normaler Benutzer schreibgeschützt | Schreibgeschützt (`-rorule`) |
| Normaler Benutzer Lese-/Schreibzugriff | Schreibgeschützt (`-rorule`) Und lesen-schreiben ( `-rwrule`) |
| Schreibgeschützt für Superuser | Schreibgeschützt (`-rorule`) Und `-superuser` |
| Superuser lesen und schreiben | Schreibgeschützt (`-rorule`) Und lesen-schreiben ( `-rwrule`) Und `-superuser` |

Die folgenden Sicherheitstypen sind für jeden der folgenden drei Zugriffsparameter gültig:

- Alle
- Keine
- Nie

Diese Sicherheitstypen sind für die Verwendung mit dem `-superuser` Parameter:

- Krb5
- ntlm
- Sys

## Regeln für Zugriffsparameter-Ergebnisse

| Wenn der Sicherheitstyp des Clients … | Dann … |
|---|---|
| Stimmt mit einem Sicherheitstyp überein, der im Zugriffsparameter angegeben wurde. | Der Client erhält Zugriff auf diese Ebene mit seiner eigenen Benutzer-ID. |
| Stimmt nicht mit einem angegebenen Sicherheitstyp überein, aber der Zugriffsparameter enthält die Option `none`. | Der Client erhält Zugriff auf diese Ebene und erhält den anonymen Benutzer mit der vom Parameter angegebenen Benutzer-ID `-anon` . |
| Stimmt nicht mit einem angegebenen Sicherheitstyp überein, und der Zugriffsparameter enthält nicht die Option `none`. | Der Client erhält keinen Zugriff auf diese Ebene.<br>Diese Einschränkung gilt nicht für den `-superuser` Parameter, da dieser Parameter auch dann keine enthält, wenn er nicht angegeben ist. |

## Kerberos 5 und Krb5p

Ab ONTAP 9 wird die Kerberos 5-Authentifizierung mit dem Datenschutzdienst (krb5p) unterstützt. Der krbp5-Authentifizierungsmodus ist sicher und schützt mithilfe von Prüfsummen vor Datenmanipulation und -Ausspähung, um den gesamten Verkehr zwischen Client und Server zu verschlüsseln. Die ONTAP-Lösung unterstützt 128-Bit- und 256-Bit-AES-Verschlüsselung für Kerberos. Der Datenschutzservice umfasst die Überprüfung der Integrität der empfangenen Daten, die Authentifizierung von Benutzern und die Verschlüsselung von Daten vor der Übertragung.

Die krb5p-Option ist am häufigsten in der Exportrichtlinie vorhanden, wo sie als Verschlüsselungsoption festgelegt ist. Die krb5p-Authentifizierungsmethode kann als Authentifizierungsparameter verwendet werden, wie im folgenden Beispiel gezeigt:

```
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
```

# Aktivieren Sie Lightweight Directory Access Protocol Signing and Sealing

Das Signieren und Versiegeln wird unterstützt, um die Sitzungssicherheit bei Anfragen an einen LDAP-Server zu ermöglichen. Dieser Ansatz bietet eine Alternative zur LDAP-über-TLS-Sitzungssicherheit.

Das Signieren bestätigt die Integrität der LDAP-Nutzlastdaten mithilfe der Geheimschlüsseltechnologie. Das Sealing verschlüsselt die LDAP-Nutzlastdaten, um das Übertragen sensibler Informationen als unverschlüsselten Text zu vermeiden. Die Sitzungssicherheitseinstellungen auf einer SVM entsprechen denen auf dem LDAP-Server. Standardmäßig sind LDAP-Signing und Sealing deaktiviert.

**Schritte**

1. Um diese Funktion zu aktivieren, führen Sie den `vserver cifs security modify` Befehl mit dem `session-security-for-ad-ldap` Parameter aus.

   Optionen für LDAP-Sicherheitsfunktionen:

   - **None**: Standard, keine Signatur oder Versiegelung
   - **Zeichen**: LDAP-Verkehr signieren
   - **Seal**: LDAP-Verkehr signieren und verschlüsseln

   > ⓘ Die Parameter für Zeichen und Siegel sind kumulativ, d. h. wenn die Option Zeichen verwendet wird, ist das Ergebnis LDAP mit Signing. Wenn jedoch die Option „Siegel“ verwendet wird, ist das Ergebnis sowohl Zeichen als auch Siegel. Wenn für diesen Befehl kein Parameter angegeben wird, ist der Standardwert „none“.

   Im Folgenden finden Sie eine Beispielkonfiguration:

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

# NetApp FPolicy erstellen und verwenden

Sie können eine FPolicy erstellen und verwenden, eine Infrastrukturkomponente der ONTAP-Lösung, mit der Partnerapplikationen Dateizugriffsberechtigungen überwachen und festlegen können. Eine der leistungsstärksten Anwendungen ist Storage Workload

Security, eine NetApp-SaaS-Anwendung, die über Hybrid-Cloud-Umgebungen hinweg einen zentralen Überblick und eine zentrale Kontrolle über den Zugriff auf alle Unternehmensdaten bietet und so die Einhaltung von Sicherheits- und Compliance-Zielen sicherstellt.

Die Zugriffssteuerung ist ein zentrales Sicherheitskonzept. Sichtbarkeit und die Fähigkeit, auf Dateizugriff und Dateivorgänge zu reagieren, sind wichtig, um die Sicherheit aufrechtzuerhalten. Um Sichtbarkeit und Zugriffssteuerung für Dateien zu ermöglichen, verwendet die ONTAP Lösung die Funktion NetApp FPolicy.

Dateirichtlinien können basierend auf dem Dateityp festgelegt werden. FPolicy legt fest, wie das Storage-System Anfragen von einzelnen Client-Systemen für Vorgänge wie Erstellen, Öffnen, Umbenennen und Löschen verarbeitet. Mit ONTAP 9 wurde das FPolicy Dateizugriffs-Benachrichtigungs-Framework durch Filterkontrollen und Ausfallsicherheit bei kurzen Netzwerkausfällen verbessert.

**Schritte**

1. Um die FPolicy Funktion nutzen zu können, müssen Sie zunächst die FPolicy Richtlinie mit dem Befehl erstellen `vserver fpolicy policy create`.

   Verwenden Sie außerdem den `-events` Parameter, wenn Sie FPolicy für die Sichtbarkeit und das Sammeln von Ereignissen verwenden. Die zusätzliche Granularität durch ONTAP ermöglicht Filterung und Zugriff bis hinunter auf die Kontrollebene für Benutzernamen. Um Berechtigungen und Zugriff mit Benutzernamen zu steuern, geben Sie den Parameter an `-privilege-user-name`.

   Der folgende Text zeigt ein Beispiel für die FPolicy-Erstellung:

   ```
   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. Nachdem Sie die FPolicy-Richtlinie erstellt haben, müssen Sie sie mit dem Befehl aktivieren `vserver fpolicy enable`. Mit diesem Befehl wird auch die Priorität oder Sequenz des FPolicy-Eintrags festgelegt.

   Die FPolicy-Sequenz ist wichtig, da, wenn mehrere Richtlinien dasselbe Dateizugriffsereignis abonniert haben, die Sequenz die Reihenfolge vorgibt, in der der Zugriff gewährt oder verweigert wird.

   Der folgende Text enthält eine Beispielkonfiguration zum Aktivieren der FPolicy-Richtlinie und zum Validieren der Konfiguration mit dem `vserver fpolicy show` Befehl:

```
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.
```

### Verbesserungen von FPolicy

ONTAP 9 umfasst die in den folgenden Abschnitten beschriebenen Verbesserungen von FPolicy.

#### Filterkontrollen

Für und zum Entfernen von Benachrichtigungen zu Verzeichnisaktivitäten stehen neue Filter zur Verfügung `SetAttr`.

#### Asynchrone Ausfallsicherheit

Wenn bei einem FPolicy-Server im asynchronen Modus ein Netzwerkausfall auftritt, werden FPolicy Benachrichtigungen, die während des Ausfalls generiert wurden, auf dem Storage-Node gespeichert. Wenn der FPolicy-Server wieder online geschaltet wird, wird er über die gespeicherten Benachrichtigungen benachrichtigt und kann sie vom Speicher-Node abrufen. Die Länge der Speicherung der Benachrichtigungen während eines Ausfalls kann so bis zu 10 Minuten betragen.

# LIF-Sicherheit

Eine LIF ist eine IP-Adresse oder ein WWPN (Worldwide Port Name) mit zugehörigen Merkmalen, beispielsweise eine Rolle, einen Home Port, einen Home Node, eine Liste der Failover-Ports sowie eine Firewallrichtlinie. Sie können LIFs an Ports konfigurieren, über die das Cluster Kommunikation über das Netzwerk sendet und empfängt. Es ist wichtig, die Sicherheitsmerkmale der einzelnen LIF-Rollen zu kennen.

## LIF-Rollen

Dies sind die folgenden LIF-Rollen:

- **Data LIF**: Eine mit einer SVM verknüpfte LIF, die zur Kommunikation mit Clients verwendet wird.
- **Cluster LIF**: Eine LIF zur Durchführung von Intracluster-Datenverkehr zwischen Knoten in einem Cluster.
- **Node Management LIF**: Eine LIF, die eine dedizierte IP-Adresse zur Verwaltung eines bestimmten Knotens in einem Cluster bereitstellt.

- **Cluster-Management-LIF**: Eine LIF, die eine einzige Managementoberfläche für den gesamten Cluster bereitstellt.
- **Intercluster LIF**: Eine LIF, die für Cluster-übergreifende Kommunikation, Backup und Replikation verwendet wird.

### Sicherheitsmerkmale der einzelnen LIF-Rolle

| | Daten-LIF | Cluster-LIF | Node Management-LIF | Cluster-Management-LIF | Intercluster-LIF |
|---|---|---|---|---|---|
| Privates IP-Subnetz erforderlich? | Nein | Ja. | Nein | Nein | Nein |
| Erfordert ein sicheres Netzwerk? | Nein | Ja. | Nein | Nein | Ja. |
| Standardmäßige Firewallrichtlinie | Sehr restriktiv | Vollständig geöffnet | Mittel | Mittel | Sehr restriktiv |
| Ist die Firewall anpassbar? | Ja. | Nein | Ja. | Ja. | Ja. |

- Da die Cluster-LIF vollständig geöffnet ist und keine konfigurierbare Firewall-Richtlinie enthält, muss sie sich in einem privaten IP-Subnetz in einem sicheren, isolierten Netzwerk befinden.
- Unter keinen Umständen sollten LIF-Rollen dem Internet zugänglich gemacht werden.

Weitere Informationen zum Sichern von LIFs finden Sie im "Konfigurieren Sie Firewallrichtlinien für LIFs".

# Protokoll- und Portsicherheit

Neben der Durchführung von integrierten Sicherheitsvorgängen und -Funktionen muss die Härtung einer Lösung auch Off-Box-Sicherheitsmechanismen beinhalten. Die Nutzung zusätzlicher Infrastrukturgeräte wie Firewalls, Intrusion Prevention-Systeme (IPSs) und andere Sicherheitsgeräte zum Filtern und Einschränken des Zugriffs auf ONTAP ist eine effiziente Möglichkeit, ein strenges Sicherheitsniveau zu definieren und aufrechtzuerhalten. Diese Informationen sind eine wichtige Komponente zum Filtern und Einschränken des Zugriffs auf die Umgebung und ihre Ressourcen.

### Häufig verwendete Protokolle und Ports

| Service | Port/Protokoll | Beschreibung |
|---|---|---|
| `SSH` | 22/TCP | SSH-Anmeldung |
| `telnet` | 23/TCP | Remote-Anmeldung |
| `Domain` | 53/TCP | Domain Name Server |

| Service | Port/Protokoll | Beschreibung |
| --- | --- | --- |
| HTTP | 80/TCP<br>80/UDP | HTTP |
| rpcbind | 111/TCP 111/UDP | Remote-Prozeduraufruf |
| NTP | 123/UDP | Network Time Protocol |
| msrpc | 135/UDP | Microsoft Remote Procedure Call |
| Netbios-name | 137/TCP 137/UDP | NetBIOS-Namensdienst |
| netbios-ssn | 139/TCP | Sitzung für den NETBIOS-Dienst |
| SNMP | 161/UDP | SNMP |
| HTTPS | 443/TCP | Sicherer Link:http |
| microsoft-ds | 445/TCP | Microsoft Verzeichnisdienste |
| IPsec | 500/UDP | Sicherheit Des Internetprotokolls |
| mount | 635/UDP | NFS-Mount |
| named | 953/UDP | Name Daemon |
| NFS | 2049/UDP 2049/TCP | NFS-Server-Daemon |
| nrv | 2050/TCP | NetApp Remote Volume-Protokoll |
| iscsi | 3260/TCP | ISCSI-Zielport |
| Lockd | 4045/TCP 4045/UDP | NFS-Sperr-Daemon |
| NFS | 4046/TCP | NFS-Mountd-Protokoll |
| acp-proto | 4046/UDP | Buchhaltungsprotokoll |
| rquotad | 4049/UDP | NFS rquotad-Protokoll |
| krb524 | 4444/UDP | Kerberos 524 |
| IPsec | 4500/UDP | Sicherheit Des Internetprotokolls |
| acp | 5125/UDP 5133/UDP<br>5144/TCP | Alternativer Kontrollport für Festplatte |
| Mdns | 5353/UDP | Multicast-DNS |
| HTTPS | 5986/UDP | HTTPS-Port: Hören binäres Protokoll |
| TELNET | 8023/TCP | Node-Scope-Telnet |
| HTTPS | 8443/TCP | 7MTT GUI-Tool über Link:HTTPS |
| RSH | 8514/TCP | Knoten-Umfang RSH |
| KMIP | 9877/TCP | KMIP-Client-Port (nur interner lokaler Host) |

| Service | Port/Protokoll | Beschreibung |
|---|---|---|
| `ndmp` | 10000/TCP | NDMP |
| `cifs` Witness-Port | 40001/TCP | CIFS-Witness-Port |
| `TLS` | 50000/TCP | Sicherheit der Datenübertragungsschicht |
| `Iscsi` | 65200/TCP | ISCSI-Port |
| `SSH` | 65502/TCP | Sichere Shell |
| `vsun` | 65503/TCP | Vsun |

## Interne NetApp-Ports

| Port/Protokoll | Beschreibung |
|---|---|
| 900 | NetApp-Cluster-RPC |
| 902 | NetApp-Cluster-RPC |
| 904 | NetApp-Cluster-RPC |
| 905 | NetApp-Cluster-RPC |
| 910 | NetApp-Cluster-RPC |
| 911 | NetApp-Cluster-RPC |
| 913 | NetApp-Cluster-RPC |
| 914 | NetApp-Cluster-RPC |
| 915 | NetApp-Cluster-RPC |
| 918 | NetApp-Cluster-RPC |
| 920 | NetApp-Cluster-RPC |
| 921 | NetApp-Cluster-RPC |
| 924 | NetApp-Cluster-RPC |
| 925 | NetApp-Cluster-RPC |
| 927 | NetApp-Cluster-RPC |
| 928 | NetApp-Cluster-RPC |
| 929 | NetApp-Cluster-RPC |
| 931 | NetApp-Cluster-RPC |
| 932 | NetApp-Cluster-RPC |
| 933 | NetApp-Cluster-RPC |
| 934 | NetApp-Cluster-RPC |
| 935 | NetApp-Cluster-RPC |
| 936 | NetApp-Cluster-RPC |
| 937 | NetApp-Cluster-RPC |

| Port/Protokoll | Beschreibung |
| --- | --- |
| 939 | NetApp-Cluster-RPC |
| 940 | NetApp-Cluster-RPC |
| 951 | NetApp-Cluster-RPC |
| 954 | NetApp-Cluster-RPC |
| 955 | NetApp-Cluster-RPC |
| 956 | NetApp-Cluster-RPC |
| 958 | NetApp-Cluster-RPC |
| 961 | NetApp-Cluster-RPC |
| 963 | NetApp-Cluster-RPC |
| 964 | NetApp-Cluster-RPC |
| 966 | NetApp-Cluster-RPC |
| 967 | NetApp-Cluster-RPC |
| 7810 | NetApp-Cluster-RPC |
| 7811 | NetApp-Cluster-RPC |
| 7812 | NetApp-Cluster-RPC |
| 7813 | NetApp-Cluster-RPC |
| 7814 | NetApp-Cluster-RPC |
| 7815 | NetApp-Cluster-RPC |
| 7816 | NetApp-Cluster-RPC |
| 7817 | NetApp-Cluster-RPC |
| 7818 | NetApp-Cluster-RPC |
| 7819 | NetApp-Cluster-RPC |
| 7820 | NetApp-Cluster-RPC |
| 7821 | NetApp-Cluster-RPC |
| 7822 | NetApp-Cluster-RPC |
| 7823 | NetApp-Cluster-RPC |
| 7824 | NetApp-Cluster-RPC |

# Sicherheitsressourcen

Weitere Informationen zu den in dieser ONTAP-Sicherheitsdokumentation beschriebenen Daten finden Sie in den folgenden zusätzlichen Informationen und Sicherheitskonzepten.

Informationen zur Meldung von Schwachstellen und Vorfällen, NetApp Sicherheitsreaktionen und Vertraulichkeit der Kundenvertraulichkeit finden Sie im "Sicherheitsportal von NetApp".

- "Versionshinweise zu ONTAP 9"
- "ONTAP 9 Befehlsreferenzen"
- "Systemadministration"
- "Administratorauthentifizierung und RBAC"
- "NetApp-Verschlüsselung"
- "TR-4647: Multifaktor-Authentifizierung in ONTAP 9.3"
- "OPENSSL-Chiffren"
- "CryptoMod FIPS-140-2 Level 1"
- "Zertifikatbasierte Authentifizierung mit dem NetApp Manageability SDK für ONTAP"
- "Netzwerkmanagement"