# Sicherheit für das Netzwerk

ONTAP 9

NetApp
April 24, 2024

# Inhalt

# Sicherheit für das Netzwerk

## Konfiguration der Netzwerksicherheit mithilfe von FIPS (Federal Information Processing Standards)

ONTAP ist für alle SSL-Verbindungen konform in den Federal Information Processing Standards (FIPS) 140-2. Sie können den SSL-FIPS-Modus ein- und ausschalten, SSL-Protokolle global festlegen und alle schwachen Chiffren wie RC4 innerhalb von ONTAP deaktivieren.

SSL auf ONTAP wird standardmäßig mit deaktiviertem FIPS und mit dem folgenden SSL-Protokoll aktiviert:

- TLSv1.3 (ab ONTAP 9.11.1)
- TLSv1.2
- TLSv1.1
- TLSv1

Wenn der SSL-FIPS-Modus aktiviert ist, wird die SSL-Kommunikation von ONTAP mit externen Client- oder Serverkomponenten außerhalb von ONTAP FIPS-konforme Crypto for SSL verwendet.

Wenn Administratorkonten auf SVMs mit einem öffentlichen SSH-Schlüssel zugreifen möchten, müssen Sie vor Aktivierung des SSL-FIPS-Modus sicherstellen, dass der Host Key-Algorithmus unterstützt wird.

**Hinweis:** die Unterstützung des Host Key Algorithmus hat sich in ONTAP 9.11.1 und späteren Versionen geändert.

| Version von ONTAP | Unterstützte Schlüsseltypen | Nicht unterstützte Schlüsseltypen |
|---|---|---|
| 9.11.1 und höher | ecdsa-sha2-nistp256 | rsa-sha2-512 + rsa-sha2-256 + ssh-ed25519 + ssh-dss + ssh-rsa |
| 9.10.1 und früher | ecdsa-sha2-nistp256 + ssh-ed25519 | ssh-dss + SSH-rsa |

Bestehende öffentliche SSH-Konten ohne die unterstützten Schlüsselalgorithmen müssen vor der Aktivierung von FIPS mit einem unterstützten Schlüsseltyp neu konfiguriert werden oder die Administratorauthentifizierung schlägt fehl.

Weitere Informationen finden Sie unter "Aktivieren Sie SSH-Konten für öffentliche Schlüssel".

Weitere Informationen zur Konfiguration des SSL-FIPS-Modus finden Sie im `security config modify` Man-Page.

### Aktivieren Sie FIPS

Es wird empfohlen, dass alle sicheren Benutzer ihre Sicherheitskonfiguration unmittelbar nach der Installation oder Aktualisierung des Systems anpassen. Wenn der SSL-FIPS-Modus aktiviert ist, wird die SSL-Kommunikation von ONTAP mit externen Client- oder Serverkomponenten außerhalb von ONTAP FIPS-konforme Crypto for SSL verwendet.

Wenn FIPS aktiviert ist, können Sie kein Zertifikat mit einer RSA-Schlüssellänge von 4096 installieren oder erstellen.

**Schritte**

1. Ändern Sie die erweiterte Berechtigungsebene:

   ```
   set -privilege advanced
   ```

2. FIPS aktivieren:

   ```
   security config modify -interface SSL -is-fips-enabled true
   ```

3. Wenn Sie zum Fortfahren aufgefordert werden, geben Sie ein `y`
4. Wenn Sie ONTAP 9.8 oder früher ausführen, sollten Sie jeden Node im Cluster nacheinander neu booten. Ab ONTAP 9.9 ist ein Neubooten nicht erforderlich.

**Beispiel**

Wenn ONTAP 9.9.1 oder höher ausgeführt wird, wird die Warnmeldung nicht angezeigt.

```
security config modify -interface SSL -is-fips-enabled true

Warning: This command will enable FIPS compliance and can potentially
cause some non-compliant components to fail. MetroCluster and Vserver DR
require FIPS to be enabled on both sites in order to be compatible.
Do you want to continue? {y|n}: y

Warning: When this command completes, reboot all nodes in the cluster.
This is necessary to prevent components from failing due to an
inconsistent security configuration state in the cluster. To avoid a
service outage, reboot one node at a time and wait for it to completely
initialize before rebooting the next node. Run "security config status
show" command to monitor the reboot status.
Do you want to continue? {y|n}: y
```

## Deaktivieren Sie FIPS

Wenn Sie noch eine ältere Systemkonfiguration ausführen und ONTAP mit Abwärtskompatibilität konfigurieren möchten, können Sie SSLv3 nur aktivieren, wenn FIPS deaktiviert ist.

**Schritte**

1. Ändern Sie die erweiterte Berechtigungsebene:

   ```
   set -privilege advanced
   ```

2. Deaktivieren Sie FIPS, indem Sie Folgendes eingeben:

   ```
   security config modify -interface SSL -is-fips-enabled false
   ```

3. Wenn Sie zum Fortfahren aufgefordert werden, geben Sie ein `y`.
4. Wenn Sie ONTAP 9.8 oder älter ausführen, booten Sie jeden Node im Cluster manuell neu. Ab ONTAP 9.9 ist ein Neubooten nicht erforderlich.

**Beispiel**

Wenn ONTAP 9.9.1 oder höher ausgeführt wird, wird die Warnmeldung nicht angezeigt.

```
security config modify -interface SSL -supported-protocols SSLv3

Warning: Enabling the SSLv3 protocol may reduce the security of the
interface, and is not recommended.
Do you want to continue? {y|n}: y

Warning: When this command completes, reboot all nodes in the cluster.
This is necessary to prevent components from failing due to an
inconsistent security configuration state in the cluster. To avoid a
service outage, reboot one node at a time and wait for it to completely
initialize before rebooting the next node. Run "security config status
show" command to monitor the reboot status.
Do you want to continue? {y|n}: y
```

## Den FIPS-Compliance-Status anzeigen

Sie sehen, ob im gesamten Cluster die aktuellen Sicherheitseinstellungen ausgeführt werden.

**Schritte**

1. Nacheinander: Jeden Node im Cluster neu booten

   Starten Sie nicht alle Cluster-Nodes gleichzeitig neu. Es ist ein Neustart erforderlich, um sicherzustellen, dass auf allen Applikationen im Cluster die neue Sicherheitskonfiguration und für alle Änderungen am FIPS-ein/aus-Modus, an Protokollen und Chiffren ausgeführt wird.

2. Den aktuellen Compliance-Status anzeigen:

   ```
   security config show
   ```

```
security config show

          Cluster                                                Cluster
Security
Interface FIPS Mode  Supported Protocols     Supported Ciphers Config
Ready
--------- ---------- ----------------------- -----------------
----------------
SSL       false      TLSv1_2, TLSv1_1, TLSv1 ALL:!LOW:!aNULL:  yes
                                             !EXP:!eNULL
```

# Konfigurieren Sie IP-Sicherheit (IPsec) über die Verschlüsselung über das Netzwerk

ONTAP verwendet im Transportmodus IPsec (Internet Protocol Security), um sicherzustellen, dass Daten auch während der Übertragung durchgehend sicher und verschlüsselt sind. IPsec bietet Datenverschlüsselung für den gesamten IP-Datenverkehr, einschließlich NFS-, iSCSI- und SMB-Protokollen.

Ab ONTAP 9.12.1 ist die IPsec-Unterstützung für das Front-End-Hostprotokoll in MetroCluster IP- und MetroCluster Fabric-Attached-Konfigurationen verfügbar.
Die IPsec-Unterstützung in MetroCluster-Clustern ist auf den Front-End-Host-Datenverkehr beschränkt und wird auf MetroCluster-Intercluster-LIFs nicht unterstützt.

Ab ONTAP 9.10.1 können Sie entweder vorfreigegebene Schlüssel (PSKs) oder Zertifikate für die Authentifizierung mit IPsec verwenden. Bisher wurden nur PSKs mit IPsec unterstützt.

Ab ONTAP 9.9 sind die von IPsec verwendeten Verschlüsselungsalgorithmen nach FIPS 140-2 zertifiziert. Die Algorithmen werden durch das NetApp Cryptographic Modul in ONTAP generiert, das die FIPS 140-2 Validierung durchführt.

Ab ONTAP 9.8 unterstützt ONTAP IPsec im Transportmodus.

Nach der Konfiguration von IPsec ist der Netzwerkverkehr zwischen dem Client und ONTAP durch vorbeugende Maßnahmen gegen Replay- und man-in-the-Middle (MITM)-Angriffe geschützt.

Für die Traffic-Verschlüsselung durch NetApp SnapMirror und Cluster-Peering (Cluster Peering Encryption, CPE) wird die Sicherheit der Transportschicht (TLS) für den sicheren Transport über das Netzwerk über IPsec empfohlen. Dies liegt daran, dass TLS eine bessere Leistung als IPsec hat.

Während die IPsec-Funktion auf dem Cluster aktiviert ist, erfordert das Netzwerk einen SPD-Eintrag (Security Policy Database), der dem zu schützenden Datenverkehr entspricht und Schutzdetails (wie Chiffre Suite und Authentifizierungsmethode) vor dem Datenfluss spezifiziert. Für jeden Client ist auch ein entsprechender SPD-Eintrag erforderlich.

## Aktivieren Sie IPsec auf dem Cluster

Sie können IPsec auf dem Cluster aktivieren, um sicherzustellen, dass Daten auch während der Übertragung ununterbrochen sicher und verschlüsselt sind.

**Schritte**

1. Ermitteln, ob IPsec bereits aktiviert ist:

   ```
   security ipsec config show
   ```

   Wenn das Ergebnis enthält `IPsec Enabled: false`Fahren Sie mit dem nächsten Schritt fort.

2. IPsec aktivieren:

   ```
   security ipsec config modify -is-enabled true
   ```

3. Führen Sie den Ermittlungsbefehl erneut aus:

   ```
   security ipsec config show
   ```

   Das Ergebnis umfasst jetzt `IPsec Enabled: true`.

## Bereiten Sie die IPsec-Richtlinienerstellung mit Zertifikatauthentifizierung vor

Sie können diesen Schritt überspringen, wenn Sie nur PSKs (Pre-Shared Keys) zur Authentifizierung verwenden und keine Zertifikatauthentifizierung verwenden.

Bevor Sie eine IPsec-Richtlinie erstellen, die Zertifikate für die Authentifizierung verwendet, müssen Sie überprüfen, ob die folgenden Voraussetzungen erfüllt sind:

- Sowohl ONTAP als auch der Client müssen das CA-Zertifikat der anderen Partei installiert haben, damit die Zertifikate der Endeinheit (entweder ONTAP oder der Client) von beiden Seiten verifiziert werden können
- Für die ONTAP LIF, die an der Richtlinie teilnimmt, wird ein Zertifikat installiert

> ONTAP LIFs können Zertifikate gemeinsam nutzen. Es ist keine 1:1-Zuordnung zwischen Zertifikaten und LIFs erforderlich.

**Schritte**

1. Installieren Sie alle während der gegenseitigen Authentifizierung verwendeten CA-Zertifikate, einschließlich ONTAP- und Client-seitiger CAS, in das ONTAP-Zertifikatsmanagement, sofern sie nicht bereits installiert ist (wie bei einer selbstsignierten ONTAP-Root-CA).

   **Beispielbefehl**
   ```
   cluster::> security certificate install -vserver svm_name -type server-ca
   -cert-name my_ca_cert
   ```

2. Um sicherzustellen, dass die installierte CA während der Authentifizierung innerhalb des IPsec-CA-Suchpfads ist, fügen Sie die ONTAP-Zertifizierungsstelle für die Zertifikatsverwaltung mithilfe des hinzu `security ipsec ca-certificate add` Befehl.

   **Beispielbefehl**
   ```
   cluster::> security ipsec ca-certificate add -vserver svm_name -ca-certs
   my_ca_cert
   ```

3. Erstellen und installieren Sie ein Zertifikat zur Verwendung durch die LIF von ONTAP. Die Emittent-CA dieses Zertifikats muss bereits in ONTAP installiert und zu IPsec hinzugefügt werden.

**Beispielbefehl**

```
cluster::> security certificate install -vserver svm_name -type server -cert
-name my_nfs_server_cert
```

Weitere Informationen zu Zertifikaten in ONTAP finden Sie in den Befehlen für Sicherheitszertifikate in der Dokumentation zu ONTAP 9 .

## Security Policy Database (SPD) definieren

IPsec erfordert einen SPD-Eintrag, bevor der Datenverkehr im Netzwerk fließen kann. Dies gilt unabhängig davon, ob Sie ein PSK oder ein Zertifikat zur Authentifizierung verwenden.

**Schritte**

1. Verwenden Sie die `security ipsec policy create` Befehl an:
   a. Wählen Sie die ONTAP-IP-Adresse oder das Subnetz der IP-Adressen aus, die am IPsec-Transport beteiligt werden sollen.
   b. Wählen Sie die Client-IP-Adressen aus, die eine Verbindung zu den ONTAP-IP-Adressen herstellen.

      Der Client muss Internet Key Exchange Version 2 (IKEv2) mit einem vorab freigegebenen Schlüssel (PSK) unterstützen.

   c. Optional Wählen Sie die feingranularen Datenverkehrsparameter aus, z. B. die Protokolle der oberen Ebene (UDP, TCP, ICMP usw.) ), die lokalen Port-Nummern und die Remote-Port-Nummern zum Schutz des Datenverkehrs. Die entsprechenden Parameter sind `protocols`, `local-ports` Und `remote-ports` Jeweils.

      Überspringen Sie diesen Schritt, um den gesamten Datenverkehr zwischen der ONTAP-IP-Adresse und der Client-IP-Adresse zu schützen. Der Schutz des gesamten Datenverkehrs ist die Standardeinstellung.

   d. Geben Sie entweder PSK oder Public-Key-Infrastruktur (PKI) für den ein `auth-method` Parameter für die gewünschte Authentifizierungsmethode.
      i. Wenn Sie eine PSK eingeben, fügen Sie die Parameter ein, und drücken Sie dann <enter>, um die Aufforderung zur Eingabe und Überprüfung der zuvor freigegebenen Taste zu drücken.

         `local-identity` Und `remote-identity` Parameter sind optional, wenn sowohl Host als auch Client strongSwan verwenden und keine Platzhalterrichtlinie für den Host oder Client ausgewählt ist.

      ii. Wenn Sie eine PKI eingeben, müssen Sie auch die eingeben `cert-name`, `local-identity`, `remote-identity` Parameter. Wenn die Identität des externen Zertifikats unbekannt ist oder mehrere Clientidentitäten erwartet werden, geben Sie die spezielle Identität ein `ANYTHING`.

```
security ipsec policy create -vserver vs1 -name test34 -local-ip-subnets
192.168.134.34/32 -remote-ip-subnets 192.168.134.44/32
Enter the preshared key for IPsec Policy _test34_ on Vserver _vs1_:
```

```
security ipsec policy create -vserver vs1 -name test34 -local-ip-subnets
192.168.134.34/32 -remote-ip-subnets 192.168.134.44/32 -local-ports 2049
-protocols tcp -auth-method PKI -cert-name my_nfs_server_cert -local
-identity CN=netapp.ipsec.lif1.vs0 -remote-identity ANYTHING
```

Der IP-Verkehr kann erst zwischen Client und Server übertragen werden, wenn sowohl ONTAP als auch der Client die entsprechenden IPsec-Richtlinien eingerichtet haben und die Authentifizierungsdaten (entweder PSK oder Zertifikat) auf beiden Seiten vorhanden sind. Weitere Informationen finden Sie in der clientseitigen IPsec-Konfiguration.

## Verwenden Sie IPsec-Identitäten

Bei der Authentifizierungsmethode für vorinstallierte Schlüssel sind lokale und Remote-Identitäten optional, wenn sowohl Host als auch Client strongSwan verwenden und keine Platzhalterrichtlinie für den Host oder Client ausgewählt ist.

Für die PKI/Zertifikat-Authentifizierungsmethode sind sowohl lokale als auch Remote-Identitäten zwingend erforderlich. Die Identitäten geben an, welche Identität innerhalb des Zertifikats jeder Seite zertifiziert ist und für den Überprüfungsprozess verwendet wird. Wenn die Remote-Identität unbekannt ist oder viele verschiedene Identitäten vorliegen, verwenden Sie die spezielle Identität `ANYTHING`.

#### Über diese Aufgabe

Innerhalb von ONTAP werden Identitäten durch Ändern des SPD-Eintrags oder während der Erstellung der SPD-Richtlinie festgelegt. Beim SPD kann es sich um einen Identitätsnamen im IP-Adressenformat oder String-Format handelt.

#### Schritt

Verwenden Sie den folgenden Befehl, um eine vorhandene SPD-Identitätseinstellung zu ändern:

```
security ipsec policy modify
```

#### Beispielbefehl

security ipsec policy modify -vserver *vs1* -name *test34* -local-identity *192.168.134.34* -remote-identity *client.fooboo.com*

## IPsec Konfiguration für mehrere Clients

Wenn eine kleine Anzahl von Clients IPsec nutzen muss, reicht die Verwendung eines einzelnen SPD-Eintrags für jeden Client aus. Wenn jedoch Hunderte oder gar Tausende von Clients IPsec nutzen müssen, empfiehlt NetApp die Verwendung einer IPsec Konfiguration für mehrere Clients.

#### Über diese Aufgabe

ONTAP unterstützt die Verbindung mehrerer Clients über mehrere Netzwerke mit einer einzelnen SVM-IP-Adresse, wobei IPsec aktiviert ist. Dies lässt sich mit einer der folgenden Methoden erreichen:

- **Subnetz-Konfiguration**

  Um allen Clients in einem bestimmten Subnetz (z. B. 192.168.134.0/24) zu erlauben, über einen einzigen SPD-Richtlinieneintrag eine Verbindung mit einer einzelnen SVM-IP-Adresse herzustellen, müssen Sie die angeben `remote-ip-subnets` Im Subnetz-Formular. Darüber hinaus müssen Sie die angeben `remote-`

`identity` Feld mit der korrekten clientseitigen Identität.

> Bei der Verwendung eines einzelnen Richtlinieneintrags in einer Subnetzkonfiguration teilen IPsec-Clients in diesem Subnetz die IPsec-Identität und den vorab gemeinsam genutzten Schlüssel (PSK). Dies gilt jedoch nicht für die Zertifikatauthentifizierung. Bei der Verwendung von Zertifikaten kann jeder Client sein eigenes eindeutiges Zertifikat oder ein freigegebenes Zertifikat zur Authentifizierung verwenden. ONTAP IPsec überprüft die Gültigkeit des Zertifikats auf der Grundlage des CAS, das auf seinem lokalen Vertrauensspeicher installiert ist. ONTAP unterstützt auch die Überprüfung der Zertifikatsperrliste (Certificate Revocation List, CRL).

- **Alle Clients konfigurieren** zulassen

  Damit jeder Client unabhängig von seiner Quell-IP-Adresse eine Verbindung zur SVM IPsec-fähigen IP-Adresse herstellen kann, verwenden Sie den `0.0.0.0/0` Platzhalterzeichen bei der Angabe des `remote-ip-subnets` Feld.

  Darüber hinaus müssen Sie die angeben `remote-identity` Feld mit der korrekten clientseitigen Identität. Zur Zertifikatauthentifizierung können Sie eingeben `ANYTHING`.

  Auch, wenn der `0.0.0.0/0` Platzhalterzeichen wird verwendet. Sie müssen eine bestimmte lokale oder Remote-Portnummer konfigurieren, die verwendet werden soll. Beispiel: `NFS port 2049`.

  **Schritte**

  a. Verwenden Sie einen der folgenden Befehle, um IPsec für mehrere Clients zu konfigurieren.

     i. Wenn Sie **Subnetz-Konfiguration** zur Unterstützung mehrerer IPsec-Clients verwenden:

     ```
     security ipsec policy create -vserver vserver_name -name policy_name
     -local-ip-subnets IPsec_IP_address/32 -remote-ip-subnets
     IP_address/subnet -local-identity local_id -remote-identity remote_id
     ```

     **Beispielbefehl**

     ```
     security ipsec policy create -vserver vs1 -name subnet134 -local-ip-subnets
     192.168.134.34/32 -remote-ip-subnets 192.168.134.0/24 -local-identity
     ontap_side_identity -remote-identity client_side_identity
     ```

     i. Wenn Sie **allow all Clients Configuration** verwenden, um mehrere IPsec-Clients zu unterstützen:

     ```
     security ipsec policy create -vserver vserver_name -name policy_name
     -local-ip-subnets IPsec_IP_address/32 -remote-ip-subnets 0.0.0.0/0 -local
     -ports port_number -local-identity local_id -remote-identity remote_id
     ```

     **Beispielbefehl**

     ```
     security ipsec policy create -vserver vs1 -name test35 -local-ip-subnets
     IPsec_IP_address/32 -remote-ip-subnets 0.0.0.0/0 -local-ports 2049 -local
     -identity ontap_side_identity -remote-identity client_side_identity
     ```

## IPsec-Statistiken

Während der Verhandlung kann ein Sicherheitskanal, der als IKE-Sicherheitszuordnung (SA) bezeichnet wird, zwischen der ONTAP SVM-IP-Adresse und der Client-IP-Adresse eingerichtet werden. IPsec SAS werden auf

beiden Endpunkten installiert, um die eigentliche Datenverschlüsselung und -Entschlüsselung zu ermöglichen.

Sie können Statistikbefehle verwenden, um den Status von IPsec SAS und IKE SAS zu überprüfen.

**Beispielbefehle**

IKE SA-Beispielbefehl:

```
security ipsec show-ikesa -node hosting_node_name_for_svm_ip
```

IPsec SA-Beispielbefehl und -Ausgabe:

```
security ipsec show-ipsecsa -node hosting_node_name_for_svm_ip
```

```
cluster1::> security ipsec show-ikesa -node cluster1-node1
            Policy Local           Remote
Vserver     Name   Address         Address         Initator-SPI     State
----------- ------ --------------- --------------- ----------------
-----------
vs1         test34
                   192.168.134.34  192.168.134.44  c764f9ee020cec69
ESTABLISHED
```

IPsec SA-Beispielbefehl und -Ausgabe:

```
security ipsec show-ipsecsa -node hosting_node_name_for_svm_ip

cluster1::> security ipsec show-ipsecsa -node cluster1-node1
            Policy  Local           Remote          Inbound  Outbound
Vserver     Name    Address         Address         SPI      SPI
State
----------- ------- --------------- --------------- -------- --------
---------
vs1         test34
                    192.168.134.34  192.168.134.44  c4c5b3d6 c2515559
INSTALLED
```

# Konfigurieren Sie Firewallrichtlinien für LIFs

Die Einrichtung einer Firewall verbessert die Clustersicherheit und hilft, unbefugten Zugriff auf das Storage-System zu verhindern. Standardmäßig ist die integrierte Firewall so konfiguriert, dass der Remote-Zugriff auf einen bestimmten Satz von IP-Services für Daten, Management und logische Intercluster-Schnittstellen möglich ist.

Ab ONTAP 9.10.1:

- Firewallrichtlinien sind veraltet und werden durch LIF-Servicerichtlinien ersetzt. Zuvor wurde die integrierte

Firewall mithilfe von Firewallrichtlinien gemanagt. Diese Funktion wird nun mithilfe einer LIF-Service-Richtlinie realisiert.

- Alle Firewall-Richtlinien sind leer und öffnen keine Ports in der zugrunde liegenden Firewall. Stattdessen müssen alle Ports mithilfe einer LIF-Service-Richtlinie geöffnet werden.
- Nach einem Upgrade auf 9.10.1 oder höher ist keine Aktion erforderlich, da die Umstellung von Firewallrichtlinien auf LIF-Servicrichtlinien erfolgt. Das System erstellt automatisch die LIF-Servicrichtlinien entsprechend den in der früheren ONTAP Version verwendeten Firewall-Richtlinien. Wenn Sie Skripts oder andere Tools verwenden, mit denen benutzerdefinierte Firewallrichtlinien erstellt und gemanagt werden, müssen Sie diese Skripte möglicherweise aktualisieren, um stattdessen benutzerdefinierte Service-Richtlinien zu erstellen.

Weitere Informationen finden Sie unter "LIFs und Service-Richtlinien in ONTAP 9.6 und höher".

Über Firewallrichtlinien kann der Zugriff auf Management-Serviceprotokolle wie SSH, HTTP, HTTPS, Telnet, NTP, gesteuert werden. NDMP, NDMPS, RSH, DNS ODER SNMP Firewallrichtlinien können nicht für Datenprotokolle wie NFS oder SMB eingerichtet werden.

Für Firewallservices und -Richtlinien gibt es folgende Managementoptionen:

- Aktivieren oder Deaktivieren des Firewallservice
- Anzeigen der aktuellen Konfiguration des Firewallservice
- Erstellen einer neuen Firewallrichtlinie unter Angabe von Richtliniennamen und Netzwerkservices
- Anwenden einer Firewallrichtlinie auf eine logische Schnittstelle
- Erstellen einer neuen Firewallrichtlinie als exakte Kopie einer vorhandenen Richtlinie

  Verwenden einer Richtlinienkopie zum Erstellen einer Richtlinie mit ähnlichen Merkmalen innerhalb derselben SVM oder zum Kopieren dieser Richtlinie zu einer anderen SVM

- Anzeigen von Informationen zu Firewallrichtlinien
- Ändern der IP-Adressen und Netmasks, die von einer Firewallrichtlinie verwendet werden
- Löschen einer Firewallrichtlinie, die von keinem LIF verwendet wird

## Firewall-Richtlinien und LIFs

Mithilfe von LIF-Firewallrichtlinien wird der Zugriff auf das Cluster über jede logische Schnittstelle beschränkt. Sie müssen verstehen, wie sich die Standard-Firewall-Richtlinie auf den Systemzugriff über jeden logischen Typ auswirkt, und wie Sie eine Firewall-Richtlinie anpassen können, um die Sicherheit über LIF zu erhöhen oder zu verringern.

Wenn Sie ein LIF mit dem konfigurieren `network interface create` Oder `network interface modify` Befehl, der für das angegebene Wert `-firewall-policy` Der Parameter bestimmt die Service-Protokolle und IP-Adressen, die auf das LIF zugreifen dürfen.

In vielen Fällen können Sie den standardmäßigen Firewallrichtlinienwert akzeptieren. In anderen Fällen müssen Sie den Zugriff auf bestimmte IP-Adressen und bestimmte Management-Service-Protokolle einschränken. Die verfügbaren Management-Service-Protokolle umfassen SSH, HTTP, HTTPS, Telnet, NTP, NDMP, NDMPS, RSH, DNS UND SNMP

Die Firewallrichtlinie für alle Cluster-LIFs ist standardmäßig aktiviert `""` Und kann nicht geändert werden.

In der folgenden Tabelle werden die Standard-Firewall-Richtlinien beschrieben, die jeder logischen

Schnittstelle zugewiesen werden. Dies ist abhängig von ihrer Rolle (ONTAP 9.5 und früher) oder Service-Richtlinie (ONTAP 9.6 und höher) bei der Erstellung des logischen Schnittstelle.

| Firewallrichtlinie | Standard-Service-Protokolle | Standardzugriff | LIFs werden angewendet auf |
|---|---|---|---|
| Management | dns, http, https, ndmp, NDMPs, ntp, snmp, SSH | Beliebige Adresse (0.0.0.0/0) | Cluster-Management, SVM-Management und Node-Management-LIFs |
| management nfs | dns, http, https, ndmp, NDMPs, ntp, portmap, snmp, SSH | Beliebige Adresse (0.0.0.0/0) | Daten-LIFs unterstützen zudem den SVM-Managementzugriff |
| Intercluster | https, ndmp, NDMPs | Beliebige Adresse (0.0.0.0/0) | Alle LIFs zwischen Clustern |
| Daten | dns, ndmp, NDMPs, Port-Map | Beliebige Adresse (0.0.0.0/0) | Alle Daten-LIFs |

## Konfiguration des Portmap-Dienstes

Der Portmap-Dienst ordnet RPC-Dienste den Ports zu, auf denen sie zuhören.

Der Portmap-Service war in ONTAP 9.3 und früher immer zugänglich, war von ONTAP 9.4 bis ONTAP 9.6 konfigurierbar und wird ab ONTAP 9.7 automatisch gemanagt.

- In ONTAP 9.3 und früher war der portmap-Dienst (rpcbind) in Netzwerkkonfigurationen, die sich auf die integrierte ONTAP-Firewall statt auf eine Firewall eines Drittanbieters stützten, immer über Port 111 zugänglich.
- Von ONTAP 9.4 bis ONTAP 9.6 können Sie Firewallrichtlinien ändern, um zu steuern, ob der Portmap-Service auf bestimmten LIFs zugegriffen werden kann.
- Ab ONTAP 9.7 wird der Port Map Firewall-Service eingestellt. Stattdessen wird der Port-Map automatisch für alle LIFs geöffnet, die den NFS-Service unterstützen.

**Portmap-Dienst ist in der Firewall in ONTAP 9.4 bis ONTAP 9.6 konfigurierbar.**

Der restliche Teil dieses Themas erläutert, wie der Port Map Firewall-Service für ONTAP 9.4 bis ONTAP 9.6 Versionen konfiguriert wird.

Je nach Konfiguration können Sie den Zugriff auf den Service für bestimmte Arten von LIFs, in der Regel Management-Schnittstellen und Intercluster LIFs, unzulassen. In manchen Fällen kann der Zugriff auf Daten-LIFs sogar unzulässig sein.

#### Welches Verhalten können Sie erwarten

Das Verhalten von ONTAP 9.4 bis ONTAP 9.6 ermöglicht einen nahtlosen Übergang bei einem Upgrade. Wenn bereits über bestimmte LIFs auf den Portmap-Service zugegriffen wird, ist dieser über diese LIFs hinweg weiterhin zugänglich. Wie in ONTAP 9.3 und früheren Versionen können Sie die Services angeben, auf die in der Firewall-Richtlinie für den LIF-Typ zugegriffen werden kann.

Alle Nodes im Cluster müssen ONTAP 9.4 bis ONTAP 9.6 ausführen, damit das Verhalten wirksam wird. Nur der eingehende Datenverkehr ist betroffen.

Die neuen Regeln lauten wie folgt:

- Bei einem Upgrade auf Version 9.4 bis 9.6 fügt ONTAP den Portmap-Service allen vorhandenen Firewall-Richtlinien hinzu – Standard oder benutzerdefiniert.
- Wenn Sie ein neues Cluster oder einen neuen IPspace erstellen, fügt ONTAP den Portmap-Service nur der Standarddatenrichtlinie hinzu, nicht jedoch den standardmäßigen Management- oder Cluster-Richtlinien.
- Sie können den Portmap-Dienst je nach Bedarf den Standard- oder benutzerdefinierten Richtlinien hinzufügen und den Dienst nach Bedarf entfernen.

**So fügen Sie den Portmap-Dienst hinzu oder entfernen ihn**

Um den Portmap-Service einer SVM oder Cluster-Firewallrichtlinie hinzuzufügen (Zugriff innerhalb der Firewall), geben Sie ein:

```
system services firewall policy create -vserver SVM -policy
mgmt|intercluster|data|custom -service portmap
```

Um den Portmap-Service von einer SVM oder einer Cluster-Firewallrichtlinie zu entfernen (Zugriff innerhalb der Firewall), geben Sie ein:

```
system services firewall policy delete -vserver SVM -policy
mgmt|intercluster|data|custom -service portmap
```

Sie können mit dem Befehl „Ändern“ der Netzwerkschnittstelle die Firewallrichtlinie auf eine vorhandene LIF anwenden. Eine vollständige Befehlssyntax finden Sie unter "ONTAP 9-Befehle".

## Erstellen Sie eine Firewallrichtlinie und weisen Sie sie einem LIF zu

Jedem LIF werden Standard-Firewallrichtlinien zugewiesen, wenn Sie das LIF erstellen. In vielen Fällen funktionieren die Standard-Firewall-Einstellungen gut und Sie müssen sie nicht ändern. Wenn Sie die Netzwerkservices oder IP-Adressen ändern möchten, die auf eine LIF zugreifen können, können Sie eine benutzerdefinierte Firewallrichtlinie erstellen und dieser LIF zuweisen.

**Über diese Aufgabe**

- Sie können keine Firewallrichtlinie mit dem erstellen `policy` Name `data`, `intercluster`, `cluster`, Oder `mgmt`.

  Diese Werte sind den systemdefinierten Firewallrichtlinien vorbehalten.

- Sie können keine Firewallrichtlinie für Cluster-LIFs festlegen oder ändern.

  Die Firewallrichtlinie für Cluster-LIFs ist für alle Service-Typen auf 0.0.0.0/0 festgelegt.

- Wenn Sie einen Dienst aus einer Richtlinie entfernen müssen, müssen Sie die vorhandene Firewallrichtlinie löschen und eine neue Richtlinie erstellen.
- Wenn IPv6 auf dem Cluster aktiviert ist, können Sie Firewallrichtlinien mit IPv6-Adressen erstellen.

  Nach Aktivierung von IPv6 `data`, `intercluster`, und `mgmt` Firewall-Richtlinien beinhalten ::/0, den IPv6-Platzhalter, in ihrer Liste der akzeptierten Adressen.

- Wenn Sie zur Konfiguration der Datensicherungsfunktionen in allen Clustern System Manager verwenden, müssen Sie sicherstellen, dass die Cluster-übergreifenden LIF-IP-Adressen in der Liste „zulässig“ aufgeführt sind und dass HTTPS-Service sowohl auf den Intercluster LIFs als auch auf den Firewalls Ihres

Unternehmens zulässig ist.

Standardmäßig wird der verwendet `intercluster` Firewall-Richtlinie ermöglicht den Zugriff aus allen IP-Adressen (0.0.0.0/0 oder ::/0 für IPv6) und aktiviert HTTPS-, NDMP- und NDMPS-Dienste. Wenn Sie diese Standardrichtlinie ändern oder eine eigene Firewallrichtlinie für Intercluster-LIFs erstellen, müssen Sie der Liste „zulässig“ jede Intercluster-LIF-IP-Adresse hinzufügen und den HTTPS-Service aktivieren.

- Ab ONTAP 9.6 werden die HTTPS- und SSH-Firewall-Services nicht unterstützt.

  In ONTAP 9.6 werden die `management-https` Und `management-ssh` LIF-Services sind für HTTPS- und SSH-Managementzugriff verfügbar.

**Schritte**

1. Erstellen Sie eine Firewallrichtlinie, die für LIFs auf einer bestimmten SVM zur Verfügung steht:

   `system services firewall policy create -vserver` *`vserver_name`* `-policy` *`policy_name`* `-service` *`network_service`* `-allow-list` *`ip_address/mask`*

   Mit diesem Befehl können Sie mehrere Male mehr als einen Netzwerkdienst und eine Liste zulässiger IP-Adressen für jeden Dienst in der Firewall-Richtlinie hinzufügen.

2. Überprüfen Sie mithilfe des, ob die Richtlinie korrekt hinzugefügt wurde `system services firewall policy show` Befehl.
3. Wenden Sie die Firewallrichtlinie auf ein LIF an:

   `network interface modify -vserver` *`vserver_name`* `-lif` *`lif_name`* `-firewall-policy` *`policy_name`*

4. Überprüfen Sie mithilfe der, ob die Richtlinie korrekt zum LIF hinzugefügt wurde `network interface show -fields firewall-policy` Befehl.

**Beispiel für die Erstellung einer Firewallrichtlinie und ihre Anwendung auf LIF**

Mit dem folgenden Befehl wird eine Firewall-Richtlinie namens Data_http erstellt, die den HTTP- und HTTPS-Protokollzugriff über IP-Adressen im Subnetz 10.10 ermöglicht, diese Richtlinie auf die LIF namens data1 in SVM vs1 anwendet und dann alle Firewallrichtlinien des Clusters zeigt:

```
system services firewall policy create -vserver vs1 -policy data_http
-service http - allow-list 10.10.0.0/16
```

```
system services firewall policy show

Vserver Policy       Service    Allowed
------- ------------ ---------- -------------------
cluster-1
        data
                     dns        0.0.0.0/0
                     ndmp       0.0.0.0/0
                     ndmps      0.0.0.0/0
cluster-1
        intercluster
                     https      0.0.0.0/0
                     ndmp       0.0.0.0/0
                     ndmps      0.0.0.0/0
cluster-1
        mgmt
                     dns        0.0.0.0/0
                     http       0.0.0.0/0
                     https      0.0.0.0/0
                     ndmp       0.0.0.0/0
                     ndmps      0.0.0.0/0
                     ntp        0.0.0.0/0
                     snmp       0.0.0.0/0
                     ssh        0.0.0.0/0
vs1
        data_http
                     http       10.10.0.0/16
                     https      10.10.0.0/16

network interface modify -vserver vs1 -lif data1 -firewall-policy
data_http

network interface show -fields firewall-policy

vserver  lif                  firewall-policy
-------  -------------------- ---------------
Cluster  node1_clus_1
Cluster  node1_clus_2
Cluster  node2_clus_1
Cluster  node2_clus_2
cluster-1 cluster_mgmt         mgmt
cluster-1 node1_mgmt1          mgmt
cluster-1 node2_mgmt1          mgmt
vs1      data1                data_http
vs3      data2                data
```

# Befehle zum Management von Firewallservice und -Richtlinien

Sie können das verwenden `system services firewall` Befehle zum Verwalten des Firewallservice, die `system services firewall policy` Befehle zum Management von Firewall-Richtlinien und das `network interface modify` Befehl zum Verwalten von Firewall-Einstellungen für LIFs.

| Ihr Ziel ist | Befehl |
|---|---|
| Aktivieren oder Deaktivieren des Firewallservice | `system services firewall modify` |
| Zeigt die aktuelle Konfiguration für den Firewallservice an | `system services firewall show` |
| Erstellen Sie eine Firewallrichtlinie oder fügen Sie einen Service zu einer vorhandenen Firewallrichtlinie hinzu | `system services firewall policy create` |
| Wenden Sie eine Firewallrichtlinie auf ein LIF an | `network interface modify -lif lifname -firewall-policy` |
| Ändern Sie die IP-Adressen und Netmasks, die einer Firewallrichtlinie zugeordnet sind | `system services firewall policy modify` |
| Zeigt Informationen zu Firewallrichtlinien an | `system services firewall policy show` |
| Erstellen Sie eine neue Firewallrichtlinie als exakte Kopie einer vorhandenen Richtlinie | `system services firewall policy clone` |
| Löschen Sie eine Firewallrichtlinie, die von keinem LIF verwendet wird | `system services firewall policy delete` |

Weitere Informationen finden Sie auf den man-Pages für die `system services firewall`, `system services firewall policy`, und `network interface modify` Befehle in "ONTAP 9-Befehle".