Sicherheit für das Netzwerk

ONTAP 9

NetApp
February 12, 2026

Inhalt

Sicherheit für das Netzwerk

Konfigurieren Sie die ONTAP-Netzwerksicherheit mit FIPS für alle SSL-Verbindungen

ONTAP erfüllt die Anforderungen des Federal Information Processing Standards (FIPS) 140-2 für alle SSL-Verbindungen. Sie können den SSL-FIPS-Modus ein- und ausschalten, SSL-Protokolle global festlegen und alle schwachen Verschlüsselungsverfahren innerhalb von ONTAP deaktivieren.

Bei SSL auf ONTAP ist die FIPS-Compliance standardmäßig deaktiviert und die folgenden TLS-Protokolle aktiviert:

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

In früheren ONTAP-Versionen waren standardmäßig die folgenden TLS-Protokolle aktiviert:

- TLSv1.1 (standardmäßig deaktiviert ab ONTAP 9.12.1)
- TLSv1 (standardmäßig deaktiviert, beginnend mit ONTAP 9.8)

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".

ONTAP 9.18.1 führt die Unterstützung für die Post-Quantum-Computing-Kryptographiealgorithmen ML-KEM, ML-DSA und SLH-DSA für SSL ein und bietet damit eine zusätzliche Sicherheitsebene gegen potenzielle zukünftige Quantencomputerangriffe. Diese Algorithmen sind nur verfügbar, wennFIPS ist deaktiviert Die Post-Quanten-Kryptographiealgorithmen werden ausgehandelt, wenn FIPS deaktiviert ist und der Peer sie unterstützt.

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 * -is-fips-enabled true
   ```

3. Wenn Sie dazu aufgefordert werden, fortzufahren, geben Sie ein `y`
4. Ab ONTAP 9.9.1 ist kein Neustart erforderlich. Wenn Sie ONTAP 9.8 oder früher ausführen, starten Sie jeden Knoten im Cluster einzeln manuell neu.

Beispiel

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

```
security config modify -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
```

Weitere Informationen zur `security config modify` Konfiguration des SSL-FIPS-Modus finden Sie in "ONTAP-Befehlsreferenz".

FIPS deaktivieren

Ab ONTAP 9.18.1 unterstützt SSL in ONTAP die Post-Quantum-Computing-Kryptographiealgorithmen ML-KEM, ML-DSA und SLH-DSA. Diese Algorithmen sind nur verfügbar, wenn FIPS deaktiviert ist und der Peer sie unterstützt.

Schritte

1. Ändern Sie die erweiterte Berechtigungsebene:

   ```
   set -privilege advanced
   ```

2. Deaktivieren Sie FIPS, indem Sie Folgendes eingeben:

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

3. Wenn Sie aufgefordert werden, fortzufahren, geben `y`Sie .
4. Ab ONTAP 9.9.1 ist kein Neustart erforderlich. Wenn Sie ONTAP 9.8 oder früher ausführen, starten Sie jeden Knoten im Cluster manuell neu.

Wenn Sie das SSLv3-Protokoll verwenden müssen, müssen Sie FIPS mit dem oben beschriebenen Verfahren deaktivieren. SSLv3 kann nur aktiviert werden, wenn FIPS deaktiviert ist.

Sie können SSLv3 mit folgendem Befehl aktivieren. Wenn Sie ONTAP 9.9.1 oder eine neuere Version verwenden, wird Ihnen diese Warnmeldung nicht angezeigt.

```
security config modify -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. Wenn Sie ONTAP 9.8 oder früher ausführen, starten Sie jeden Knoten im Cluster einzeln manuell neu.
2. Den aktuellen Compliance-Status anzeigen:

   ```
   security config show
   ```

```
cluster1::> security config show
Cluster    Supported
FIPS Mode  Protocols Supported Cipher Suites
---------- ---------
-----------------------------------------------------------
false      TLSv1.3,  TLS_RSA_WITH_AES_128_CCM,
TLS_RSA_WITH_AES_128_CCM_8,
           TLSv1.2   TLS_RSA_WITH_AES_128_GCM_SHA256,
                     TLS_RSA_WITH_AES_128_CBC_SHA,
                     TLS_RSA_WITH_AES_128_CBC_SHA256,
TLS_RSA_WITH_AES_256_CCM,
                     TLS_RSA_WITH_AES_256_CCM_8,
                     ...
```

Erfahren Sie mehr über `security config show` in der "ONTAP-Befehlsreferenz".

Verwandte Informationen

- "FIPS 203: Standard für einen modulgitterbasierten Schlüsselkapselungsmechanismus (ML-KEM)"
- "FIPS 204: Modulgitterbasierter digitaler Signaturstandard (ML-DSA)"
- "FIPS 205: Stateless Hash-Based Digital Signature Standard (SLH-DSA)"

Konfigurieren Sie die IPsec-Verschlüsselung während der Übertragung

Bereiten Sie die Verwendung der IP-Sicherheit im ONTAP-Netzwerk vor

Ab ONTAP 9.8 haben Sie die Möglichkeit, IP-Sicherheit (IPsec) zum Schutz Ihres Netzwerkverkehrs zu verwenden. IPsec ist eine von mehreren Data-in-Motion- oder in-Flight-Verschlüsselungsoptionen, die mit ONTAP verfügbar sind. Sie sollten die IPsec-Konfiguration vorbereiten, bevor Sie sie in einer Produktionsumgebung verwenden.

Implementierung der IP-Sicherheit in ONTAP

IPsec ist ein Internetstandard, der von der IETF verwaltet wird. Es bietet Datenverschlüsselung und -Integrität sowie Authentifizierung für den Datenverkehr, der auf IP-Ebene zwischen den Netzwerkendpunkten fließt.

Mit ONTAP sichert IPsec den gesamten IP-Datenverkehr zwischen ONTAP und den verschiedenen Clients, einschließlich der NFS-, SMB- und iSCSI-Protokolle. Neben Datenschutz und Datenintegrität ist der Netzwerkverkehr vor mehreren Angriffen wie Replay- und man-in-the-Middle-Angriffen geschützt. ONTAP verwendet die Implementierung des IPsec-Transportmodus. Er nutzt das IKE-Protokoll (Internet Key Exchange) Version 2 für die Verhandlung des Schlüsselmaterials zwischen ONTAP und den Clients, die entweder IPv4 oder IPv6 verwenden.

Wenn die IPsec-Funktion auf einem Cluster aktiviert ist, erfordert das Netzwerk einen oder mehrere Einträge in der ONTAP-Sicherheitsrichtliniendatenbank (SPD), die den verschiedenen Datenverkehrseigenschaften entsprechen. Diese Einträge werden den spezifischen Schutzdetails zugeordnet, die zum Verarbeiten und

Senden der Daten erforderlich sind (z. B. Chiffre Suite und Authentifizierungsmethode). Ein entsprechender SPD-Eintrag ist ebenfalls bei jedem Client erforderlich.

Für bestimmte Arten von Datenverkehr ist möglicherweise eine andere Option zur Verschlüsselung von Daten in Bewegung vorzuziehen. Für die Verschlüsselung von NetApp SnapMirror- und Cluster-Peering-Datenverkehr wird beispielsweise das TLS-Protokoll (Transport Layer Security) anstelle von IPsec empfohlen. Das liegt daran, dass TLS in den meisten Situationen eine bessere Leistung bietet.

Verwandte Informationen

- "Internet Engineering Task Force"
- "RFC 4301: Sicherheitsarchitektur für das Internet Protocol"

Weiterentwicklung der ONTAP IPsec-Implementierung

IPsec wurde erstmals mit ONTAP 9.8 eingeführt. Die Implementierung wurde in nachfolgenden ONTAP Versionen wie unten beschrieben weiterentwickelt.

ONTAP 9.18.1

Die Unterstützung für IPsec-Hardware-Offloading wurde auf IPv6-Datenverkehr erweitert.

ONTAP 9.17.1

Die Unterstützung für IPsec-Hardware-Offload wird erweitert auf "Link-Aggregationsgruppen" . "Postquanten-Pre-Shared Keys (PPKs)" werden für die IPsec-Pre-Shared Keys (PSK)-Authentifizierung unterstützt.

ONTAP 9.16.1

Mehrere kryptografische Vorgänge, wie Verschlüsselungs- und Integritätsprüfungen, können auf eine unterstützte NIC-Karte verlagert werden. Weitere Informationen finden Sie unter IPsec-Hardware-Offload-Funktion .

ONTAP 9.12.1

Die Unterstützung von IPsec-Front-End-Hostprotokollen ist in MetroCluster-IP- und MetroCluster-Fabric-Attached-Konfigurationen verfügbar. Die durch MetroCluster Cluster bereitgestellte IPsec-Unterstützung für Cluster ist auf Front-End-Host-Datenverkehr beschränkt und wird auf MetroCluster LIFs nicht unterstützt.

ONTAP 9.10.1

Zusätzlich zu den PSKs können Zertifikate für die IPsec-Authentifizierung verwendet werden. Vor ONTAP 9.10.1 werden nur PSKs für die Authentifizierung unterstützt.

ONTAP 9.9.1

Die von IPsec verwendeten Verschlüsselungsalgorithmen sind nach FIPS 140-2 validiert. Diese Algorithmen werden vom NetApp Cryptographic Module in ONTAP verarbeitet, das die FIPS 140-2-2-Validierung führt.

ONTAP 9,8

Die Unterstützung für IPsec wird basierend auf der Implementierung des Transportmodus zunächst verfügbar.

IPsec-Hardware-Offload-Funktion

Wenn Sie ONTAP 9.16.1 oder höher verwenden, haben Sie die Möglichkeit, bestimmte rechenintensive Vorgänge, wie z. B. Verschlüsselungs- und Integritätsprüfungen, auf eine am Storage-Node installierte NIC-Karte (Network Interface Controller) zu übertragen. Der Durchsatz für auf die NIC-Karte ausgelagerte Vorgänge beträgt etwa 5 % oder weniger. Dies kann die Leistung und den Durchsatz des durch IPsec geschützten Netzwerkverkehrs erheblich verbessern.

Anforderungen und Empfehlungen

Vor der Verwendung der IPsec-Hardware-Offload-Funktion sollten Sie mehrere Anforderungen beachten.

Unterstützte Ethernet-Karten

Sie dürfen nur unterstützte Ethernet-Karten installieren und verwenden. Die folgenden Ethernet-Karten werden ab ONTAP 9.16.1 unterstützt:

- X50131A (2P, 40G/100G/200G/400G Ethernet-Controller)
- X60132A (4p, 10G/25G Ethernet-Controller)

ONTAP 9.17.1 fügt Unterstützung für die folgenden Ethernet-Karten hinzu:

- X50135A (2p, 40G/100G Ethernet-Controller)
- X60135A (2p, 40G/100G Ethernet-Controller)

Die Karten X50131A und X50135A werden auf den folgenden Plattformen unterstützt:

- ASA A1K
- ASA A90
- ASA A70
- AFF A1K
- AFF A90
- AFF A70

Die Karten X60132A und X60135A werden auf den folgenden Plattformen unterstützt:

- ASA A50
- ASA A30
- ASA A20
- AFF A50
- AFF A30
- AFF A20

Sehen Sie sich die "NetApp Hardware Universe" für weitere Informationen zu den unterstützten Plattformen und Karten.

Umfang des Clusters

Die IPsec-Hardware-Offload-Funktion ist global für den Cluster konfiguriert. Und so wird der Befehl beispielsweise `security ipsec config` auf alle Nodes im Cluster angewendet.

Konsistente Konfiguration

Unterstützte NIC-Karten sollten auf allen Knoten im Cluster installiert werden. Wenn eine unterstützte NIC-Karte nur auf einigen Nodes verfügbar ist, wird nach einem Failover eine deutliche Performance-Verschlechterung angezeigt, wenn einige der LIFs nicht auf einer Offload-fähigen NIC gehostet werden.

Anti-Replay deaktivieren

Sie müssen den IPsec-Anti-Replay-Schutz auf ONTAP (Standardkonfiguration) und den IPsec-Clients deaktivieren. Wenn diese Option nicht deaktiviert ist, werden Fragmentierung und Multi-Path (redundante

Route) nicht unterstützt.

Wenn die ONTAP-IPsec-Konfiguration von der Standardeinstellung auf Anti-Replay-Schutz aktivieren geändert wurde, verwenden Sie diesen Befehl, um sie zu deaktivieren:

```
security ipsec config modify -replay-window 0
```

Sie müssen sicherstellen, dass der IPsec-Anti-Replay-Schutz auf Ihrem Client deaktiviert ist. Informationen zur Deaktivierung des Anti-Replay-Schutzes finden Sie in der IPsec-Dokumentation für Ihren Client.

Einschränkungen

Vor der Verwendung der IPsec-Hardware-Offload-Funktion sollten Sie mehrere Einschränkungen berücksichtigen.

IPv6

Ab ONTAP 9.18.1 wird IPv6 für die IPsec-Hardware-Offload-Funktion unterstützt. Vor ONTAP 9.18.1 unterstützt die IPsec-Hardware-Auslagerung kein IPv6.

Erweiterte Sequenznummern

Die erweiterten IPsec-Sequenznummern werden von der Hardware-Offload-Funktion nicht unterstützt. Es werden nur die normalen 32-Bit-Sequenznummern verwendet.

Link-Aggregation

Ab ONTAP 9.17.1 können Sie die IPsec-Hardware-Offload-Funktion mit einem "Link-Aggregationsgruppe" .

Vor Version 9.17.1 unterstützt die IPsec-Hardware-Offload-Funktion keine Link-Aggregation. Sie kann nicht mit einer Schnittstelle oder Link-Aggregationsgruppe verwendet werden, die über das `network port ifgrp` Befehle an der ONTAP CLI.

Konfigurationsunterstützung in der ONTAP-CLI

In ONTAP 9.16.1 werden drei vorhandene CLI-Befehle aktualisiert, um die IPsec-Hardware-Offload-Funktion wie unten beschrieben zu unterstützen. "Konfigurieren Sie die IP-Sicherheit in ONTAP"Weitere Informationen finden Sie unter.

ONTAP-Befehl	Aktualisieren
`security ipsec config show`	Der boolesche Parameter `Offload Enabled` zeigt den aktuellen NIC-Offload-Status an.
`security ipsec config modify`	Mit dem Parameter `is-offload-enabled` kann die NIC-Offload-Funktion aktiviert oder deaktiviert werden.
`security ipsec config show-ipsecsa`	Vier neue Zähler wurden hinzugefügt, um den ein- und ausgehenden Datenverkehr in Byte und Paketen anzuzeigen.

Konfigurationsunterstützung in der ONTAP-REST-API

Zwei vorhandene REST-API-Endpunkte werden in ONTAP 9.16.1 aktualisiert, um die IPsec-Hardware-Offload-Funktion wie unten beschrieben zu unterstützen.

REST-Endpunkt	Aktualisieren
`/api/security/ipsec`	Der Parameter `offload_enabled` wurde hinzugefügt und ist mit der PATCH-Methode verfügbar.
`/api/security/ipsec/security_association`	Zwei neue Zählerwerte wurden hinzugefügt, um die Gesamtzahl der von der Offload-Funktion verarbeiteten Bytes und Pakete zu verfolgen.

Weitere Informationen zur ONTAP REST-API einschließlich "Neuerungen an der ONTAP REST-API"finden Sie in der Dokumentation zur ONTAP Automatisierung. Weitere Informationen zu finden Sie auch in der Dokumentation zur ONTAP-Automatisierung "IPsec-Endpunkte".

Verwandte Informationen

- "Sicherheit IPSec"

Konfigurieren Sie die IP-Sicherheit für das ONTAP-Netzwerk

Zum Konfigurieren und Aktivieren der IPsec-Verschlüsselung während der Übertragung auf Ihrem ONTAP-Cluster sind mehrere Aufgaben erforderlich.

Überprüfen Sie die "Bereiten Sie sich auf die Verwendung der IP-Sicherheit vor"Einstellungen, bevor Sie IPsec konfigurieren. Sie müssen beispielsweise entscheiden, ob Sie die ab ONTAP 9.16.1 verfügbare IPsec-Hardware-Offload-Funktion verwenden möchten.

Aktivieren Sie IPsec auf dem Cluster

Sie können IPsec auf dem Cluster aktivieren, um sicherzustellen, dass Daten während der Übertragung kontinuierlich verschlüsselt und sicher 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
   ```

   Sie können die IPsec-Hardware-Offload-Funktion mit dem booleschen Parameter aktivieren `is-offload-enabled`.

3. Führen Sie den Ermittlungsbefehl erneut aus:

   ```
   security ipsec config show
   ```

   Das Ergebnis enthält nun `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 sich die installierte CA während der Authentifizierung im IPsec-CA-Suchpfad befindet, fügen Sie mithilfe des `security ipsec ca-certificate add` Befehls die ONTAP-Zertifizierungsstelle für die Zertifikatsverwaltung zum IPsec-Modul hinzu.

   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. Mit dem `security ipsec policy create` Befehl können Sie:
   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. Wählen Sie optional die detaillierten Datenverkehrsparameter aus, z. B. die Protokolle der oberen Schicht (UDP, TCP, ICMP usw.), die lokalen Portnummern und die Remote-Portnummern, um den Datenverkehr zu schützen. 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 `auth-method` Parameter für die gewünschte Authentifizierungsmethode ein.

   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.

   > Die `local-identity` Parameter und `remote-identity` 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 `cert-name` `local-identity` `remote-identity` Parameter , , eingeben. Wenn die Identität des externen Zertifikats unbekannt ist oder mehrere Client-Identitäten erwartet werden, geben Sie die spezielle Identität ein `ANYTHING`.

e. Ab ONTAP 9.17.1 können Sie optional eine Post-Quantum Pre-Shared Key (PPK)-Identität mit dem `ppk-identity` Parameter. PPKs bieten eine zusätzliche Sicherheitsebene gegen potenzielle zukünftige Quantencomputerangriffe. Wenn Sie eine PPK-Identität eingeben, werden Sie aufgefordert, das PPK-Geheimnis einzugeben. PPKs werden nur für die PSK-Authentifizierung unterstützt.

Erfahren Sie mehr über `security ipsec policy create` im "ONTAP-Befehlsreferenz" .

```
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.

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 wenn es viele verschiedene Identitäten sein könnte, 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.

Schritte

1. 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**

  Damit alle Clients in einem bestimmten Subnetz (z. B. 192.168.134.0/24) über einen einzigen SPD-Richtlinieneintrag eine Verbindung zu einer einzelnen SVM-IP-Adresse herstellen `remote-ip-subnets` können, müssen Sie das im Subnetz-Formular angeben. Außerdem müssen Sie das `remote-identity` Feld mit der korrekten clientseitigen Identität angeben.

  > 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 IPsec-fähigen SVM-IP-

Adresse `0.0.0.0/0` herstellen kann, verwenden Sie bei der Angabe des `remote-ip-subnets` Felds den Platzhalter.

Außerdem müssen Sie das `remote-identity` Feld mit der korrekten clientseitigen Identität angeben. Für die Zertifikatauthentifizierung können Sie eingeben `ANYTHING`.

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

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
```

Zeigt IPsec-Statistiken an

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.

Wenn Sie die IPsec-Hardware-Offload-Funktion verwenden, werden mit dem Befehl mehrere neue Zähler angezeigt `security ipsec config show-ipsecsa`.

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
```

Verwandte Informationen

- "Sicherheitszertifikat installieren"
- "Sicherheit IPSec"

Konfigurieren der ONTAP Backend-Cluster-Netzwerkverschlüsselung

Ab ONTAP 9.18.1 können Sie die Transport Layer Security (TLS)-Verschlüsselung für Daten während der Übertragung im Backend-Cluster-Netzwerk konfigurieren. Diese Verschlüsselung schützt Kundendaten, die in ONTAP gespeichert sind, während der Übertragung zwischen ONTAP Knoten im Backend-Clusternetzwerk.

Über diese Aufgabe

- Die Backend-Cluster-Netzwerkverschlüsselung ist standardmäßig deaktiviert.
- Wenn die Verschlüsselung des Backend-Cluster-Netzwerks aktiviert ist, werden alle in ONTAP gespeicherten Kundendaten bei der Übertragung zwischen ONTAP Knoten im Backend-Cluster-Netzwerk verschlüsselt. Bestimmte Netzwerkdaten im Cluster, wie z. B. Daten des Kontrollpfads, sind nicht verschlüsselt.
- Standardmäßig verwendet die Backend-Cluster-Netzwerkverschlüsselung automatisch generierte Zertifikate für jeden Knoten im Cluster. Du kannstCluster-Netzwerkverschlüsselungszertifikate verwalten Auf jedem Knoten soll ein benutzerdefiniertes Zertifikat verwendet werden.

Bevor Sie beginnen

- Sie müssen ONTAP Administrator sein. `admin` Berechtigungsstufe zum Ausführen der folgenden Aufgaben.
- Auf allen Knoten im Cluster muss ONTAP 9.18.1 oder höher ausgeführt werden, um die Backend-Cluster-Netzwerkverschlüsselung zu aktivieren.

Verschlüsselung für die Cluster-Netzwerkkommunikation aktivieren oder deaktivieren

Schritte

1. Den aktuellen Verschlüsselungsstatus des Clusternetzwerks anzeigen:

   ```
   security cluster-network show
   ```

   Dieser Befehl zeigt den aktuellen Status der Cluster-Netzwerkverschlüsselung an:

   ```
   Cluster-1::*> security cluster-network show

   Enabled: true

   Mode: tls

   Status: READY
   ```

2. Aktivieren oder Deaktivieren der TLS-Backend-Cluster-Netzwerkverschlüsselung:

   ```
   security cluster-network modify -enabled <true|false>
   ```

   Dieser Befehl aktiviert oder deaktiviert die verschlüsselte Kommunikation für Kundendaten, die sich während der Übertragung im Backend-Cluster-Netzwerk befinden.

Cluster-Netzwerkverschlüsselungszertifikate verwalten

1. Aktuelle Informationen zum Cluster-Netzwerkverschlüsselungszertifikat anzeigen:

   ```
   security cluster-network certificate show
   ```

   Dieser Befehl zeigt die aktuellen Informationen zum Cluster-Netzwerkverschlüsselungszertifikat an:

```
security cluster-network certificate show
Node                  Certificate Name                       CA
--------------------- -------------------------------------
--------------
node1                 -                                      Cluster-
1_Root_CA
node2                 -                                      Cluster-
1_Root_CA
node3                 google_issued_cert1                    Google_CA1
node4                 google_issued_cert2                    Google_CA1
```

Für jeden Knoten im Cluster werden die Zertifikats- und Zertifizierungsstellennamen (CA-Namen) angezeigt.

2. Ändern des Clusternetzwerk-Verschlüsselungszertifikats für einen Knoten:

```
security cluster-network certificate modify -node <node_name> -name
<certificate_name>
```

Dieser Befehl ändert das Clusternetzwerk-Verschlüsselungszertifikat für einen bestimmten Knoten. Das Zertifikat muss vor Ausführung dieses Befehls installiert und von einer installierten Zertifizierungsstelle signiert werden. Weitere Informationen zur Zertifikatsverwaltung finden Sie unter"Managen Sie ONTAP Zertifikate mit System Manager" Die Wenn `-name` Wenn kein Zertifikat angegeben ist, wird das automatisch generierte Standardzertifikat verwendet.

Konfiguration von Firewallrichtlinien für LIFs im ONTAP Netzwerk

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.

Beim Konfigurieren einer LIF mit dem `network interface create` `network interface modify` Befehl oder `-firewall-policy` bestimmt der für den Parameter angegebene Wert die Service-Protokolle und IP-Adressen, die Zugriff auf die LIF erlauben. Erfahren Sie mehr über `network interface` in der "ONTAP-Befehlsreferenz".

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. Erfahren Sie mehr über die in diesem Verfahren beschriebenen Befehle im "ONTAP-Befehlsreferenz".

Erstellen Sie eine Firewallrichtlinie und weisen Sie sie einer logischen Schnittstelle 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 `policy` Namen `data`, , `intercluster` `cluster`oder erstellen `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.

  Nachdem IPv6 aktiviert ist, `data` `intercluster` `mgmt`enthalten , und Firewallrichtlinien ::/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 `intercluster` erlaubt die Firewallrichtlinie den Zugriff von 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 `management-https` `management-ssh` sind die und LIF-Services 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 mit dem `system services firewall policy show` Befehl, ob die Richtlinie ordnungsgemäß hinzugefügt wurde.
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 mit dem `network interface show -fields firewall-policy` Befehl, ob die Richtlinie korrekt zum LIF hinzugefügt wurde.

   Erfahren Sie mehr über `network interface show` in der "ONTAP-Befehlsreferenz".

Beispiel zum Erstellen einer Firewallrichtlinie und Zuweisen zu einer logischen Schnittstelle

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
```

ONTAP-Befehle zum Managen von Firewallservices und -Richtlinien

Sie können den `system services firewall` Firewall-Service mit den Befehlen managen, die `system services firewall policy` Befehle zum Verwalten von Firewallrichtlinien und den `network interface modify` Befehl zum Verwalten von Firewalleinstellungen für LIFs.

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".

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`

Verwandte Informationen

- "Firewall für Systemdienste"
- "Änderung der Netzwerkschnittstelle"