Proteggere la rete

ONTAP 9

NetApp
April 24, 2024

Sommario

Proteggere la rete

Configurare la sicurezza di rete utilizzando gli standard FIPS (Federal Information Processing Standards)

ONTAP è conforme agli standard federali sull'elaborazione delle informazioni (FIPS) 140-2 per tutte le connessioni SSL. È possibile attivare e disattivare la modalità SSL FIPS, impostare i protocolli SSL a livello globale e disattivare le crittografie deboli, ad esempio RC4, in ONTAP.

Per impostazione predefinita, SSL su ONTAP è impostato con la compliance FIPS disattivata e il protocollo SSL attivato con quanto segue:

- TLSv1.3 (a partire da ONTAP 9.11.1)
- TLSv1.2
- TLSv1.1
- TLSv1

Quando la modalità SSL FIPS è attivata, la comunicazione SSL da ONTAP a componenti client o server esterni a ONTAP utilizzerà la crittografia conforme a FIPS per SSL.

Se si desidera che gli account amministratore accedano alle SVM con una chiave pubblica SSH, assicurarsi che l'algoritmo della chiave host sia supportato prima di attivare la modalità SSL FIPS.

Nota: il supporto dell'algoritmo della chiave host è stato modificato in ONTAP 9.11.1 e versioni successive.

Release di ONTAP	Tipi di chiave supportati	Tipi di chiave non supportati
9.11.1 e versioni successive	ecdsa-sha2-nistp256	rsa-sha2-512 + rsa-sha2-256 + ssh-ed25519 + ssh-dss + ssh-rsa
9.10.1 e versioni precedenti	ecdsa-sha2-nistp256 + ssh-ed25519	ssh-dss + ssh-rsa

Gli account di chiave pubblica SSH esistenti senza gli algoritmi di chiave supportati devono essere riconfigurati con un tipo di chiave supportato prima di attivare FIPS, altrimenti l'autenticazione dell'amministratore non avrà esito positivo.

Per ulteriori informazioni, vedere "Abilitare gli account a chiave pubblica SSH".

Per ulteriori informazioni sulla configurazione della modalità SSL FIPS, consultare `security config modify` pagina man.

Abilitare FIPS

Si consiglia a tutti gli utenti sicuri di modificare la propria configurazione di sicurezza subito dopo l'installazione o l'aggiornamento del sistema. Quando la modalità SSL FIPS è attivata, la comunicazione SSL da ONTAP a componenti client o server esterni a ONTAP utilizzerà la crittografia conforme a FIPS per SSL.

Quando FIPS è attivato, non è possibile installare o creare un certificato con una chiave RSA di lunghezza pari a 4096.

Fasi

1. Passare al livello di privilegio avanzato:

   ```
   set -privilege advanced
   ```

2. Attiva FIPS:

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

3. Quando viene richiesto di continuare, immettere `y`
4. Se si utilizza ONTAP 9.8 o versioni precedenti, riavviare manualmente uno ad uno ogni nodo del cluster. A partire da ONTAP 9.9.1, non è necessario riavviare.

Esempio

Se si utilizza ONTAP 9.9.1 o versione successiva, il messaggio di avviso non viene visualizzato.

```
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
```

Disattiva FIPS

Se si esegue ancora una configurazione di sistema precedente e si desidera configurare ONTAP con compatibilità con le versioni precedenti, è possibile attivare SSLv3 solo quando FIPS è disattivato.

Fasi

1. Passare al livello di privilegio avanzato:

   ```
   set -privilege advanced
   ```

2. Disattivare FIPS digitando:

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

3. Quando viene richiesto di continuare, immettere `y`.
4. Se si utilizza ONTAP 9.8 o versioni precedenti, riavviare manualmente ciascun nodo del cluster. A partire da ONTAP 9.9.1, non è necessario riavviare.

Esempio

Se si utilizza ONTAP 9.9.1 o versione successiva, il messaggio di avviso non viene visualizzato.

```
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
```

Visualizza lo stato di conformità FIPS

È possibile verificare se l'intero cluster esegue le impostazioni di configurazione della protezione correnti.

Fasi

1. Riavviare uno alla volta ciascun nodo del cluster.

   Non riavviare tutti i nodi del cluster contemporaneamente. È necessario riavviare il sistema per assicurarsi che tutte le applicazioni del cluster eseguano la nuova configurazione di sicurezza e per tutte le modifiche apportate alla modalità FIPS on/off, ai protocolli e ai cifrari.

2. Visualizza lo stato di conformità corrente:

   ```
   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
```

Configurare la crittografia IP Security (IPsec) over wire

ONTAP utilizza IPSec (Internet Protocol Security) in modalità di trasporto per garantire che i dati siano costantemente protetti e crittografati, anche durante il transito. IPSec offre la crittografia dei dati per tutto il traffico IP, inclusi i protocolli NFS, iSCSI e SMB.

A partire da ONTAP 9.12.1, il supporto IPSec del protocollo host front-end è disponibile nelle configurazioni MetroCluster IP e MetroCluster fabric-attached.
Il supporto di IPSec nei cluster MetroCluster è limitato al traffico host front-end e non è supportato dalle LIF intercluster MetroCluster.

A partire da ONTAP 9.10.1, è possibile utilizzare chiavi precondivise (PSK) o certificati per l'autenticazione con IPSec. In precedenza, solo gli PSK erano supportati con IPsec.

A partire da ONTAP 9.9.1, gli algoritmi di crittografia utilizzati da IPSec sono validati in FIPS 140-2. Gli algoritmi vengono generati dal modulo crittografico NetApp in ONTAP che riporta la convalida FIPS 140-2.

A partire da ONTAP 9.8, ONTAP supporta IPSec in modalità di trasporto.

Una volta configurato IPSec, il traffico di rete tra il client e ONTAP viene protetto con misure preventive per combattere gli attacchi di tipo play e man-in-the-middle (MITM).

Per NetApp SnapMirror e la crittografia del traffico di peering del cluster, la crittografia di peering del cluster (CPE) e la protezione TLS (Transport Layer Security) sono ancora consigliate su IPSec per garantire la sicurezza in transito via cavo. Questo perché TLS offre performance migliori rispetto a IPSec.

Mentre la funzionalità IPsec è attivata sul cluster, la rete richiede una voce del database dei criteri di protezione (SPD) che corrisponda al traffico da proteggere e che specifichi i dettagli di protezione (come la suite di crittografia e il metodo di autenticazione) prima che il traffico possa fluire. Su ciascun client è necessaria anche una voce SPD corrispondente.

Abilitare IPSec sul cluster

È possibile attivare IPsec sul cluster per garantire che i dati siano costantemente protetti e crittografati, anche durante il transito.

Fasi

1. Scopri se IPsec è già attivato:

```
security ipsec config show
```

Se il risultato include `IPsec Enabled: false`, passare alla fase successiva.

2. Attiva IPSec:

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

3. Eseguire nuovamente il comando di rilevamento:

```
security ipsec config show
```

Il risultato ora include `IPsec Enabled: true`.

Preparare la creazione del criterio IPsec con l'autenticazione del certificato

È possibile saltare questo passaggio se si utilizzano solo chiavi pre-condivise (PSK) per l'autenticazione e non si utilizza l'autenticazione del certificato.

Prima di creare un criterio IPsec che utilizza i certificati per l'autenticazione, è necessario verificare che siano soddisfatti i seguenti prerequisiti:

- Sia ONTAP che il client devono avere installato il certificato CA dell'altra parte in modo che i certificati dell'entità finale (ONTAP o client) siano verificabili da entrambe le parti
- Viene installato un certificato per il LIF ONTAP che partecipa al criterio

> Le LIF ONTAP possono condividere i certificati. Non è richiesta una mappatura uno-a-uno tra certificati e LIF.

Fasi

1. Installare tutti i certificati CA utilizzati durante l'autenticazione reciproca, incluse le CA lato ONTAP e lato client, nella gestione dei certificati ONTAP, a meno che non sia già installato (come nel caso di una CA root autofirmata di ONTAP).

   Comando di esempio
   ```
   cluster::> security certificate install -vserver svm_name -type server-ca
   -cert-name my_ca_cert
   ```

2. Per assicurarsi che la CA installata rientri nel percorso di ricerca della CA IPSec durante l'autenticazione, aggiungere le CA di gestione dei certificati ONTAP al modulo IPSec utilizzando `security ipsec ca-certificate add` comando.

   Comando di esempio
   ```
   cluster::> security ipsec ca-certificate add -vserver svm_name -ca-certs
   my_ca_cert
   ```

3. Creare e installare un certificato per l'utilizzo da parte della LIF ONTAP. La CA emittente di questo certificato deve essere già installata in ONTAP e aggiunta a IPSec.

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

Per ulteriori informazioni sui certificati in ONTAP, vedere i comandi dei certificati di protezione nella documentazione di ONTAP 9 .

Definizione del database dei criteri di protezione (SPD)

IPSec richiede una voce SPD prima di consentire il flusso del traffico sulla rete. Ciò vale sia che si utilizzi un PSK o un certificato per l'autenticazione.

Fasi

1. Utilizzare `security ipsec policy create` comando a:
   a. Selezionare l'indirizzo IP ONTAP o la subnet degli indirizzi IP per partecipare al trasporto IPSec.
   b. Selezionare gli indirizzi IP del client che si connetteranno agli indirizzi IP ONTAP.

      > Il client deve supportare Internet Key Exchange versione 2 (IKEv2) con una chiave precondivisa (PSK).

   c. Opzionale. Selezionare i parametri di traffico a grana fine, ad esempio i protocolli di livello superiore (UDP, TCP, ICMP, ecc.)), i numeri delle porte locali e i numeri delle porte remote per proteggere il traffico. I parametri corrispondenti sono `protocols`, `local-ports` e. `remote-ports` rispettivamente.

      Ignorare questo passaggio per proteggere tutto il traffico tra l'indirizzo IP ONTAP e l'indirizzo IP del client. La protezione di tutto il traffico è l'impostazione predefinita.

   d. Immettere PSK o Public-Key Infrastructure (PKI) per `auth-method` parametro per il metodo di autenticazione desiderato.
      i. Se si immette una PSK, includere i parametri, quindi premere <enter> per visualizzare la richiesta di immissione e verifica della chiave precondivisa.

         > `local-identity` e. `remote-identity` I parametri sono facoltativi se sia l'host che il client utilizzano il metodo strongSwan e non è stato selezionato alcun criterio con caratteri jolly per l'host o il client.

      ii. Se si inserisce un'infrastruttura PKI, è necessario immettere anche il `cert-name`, `local-identity`, `remote-identity` parametri. Se l'identità del certificato lato remoto non è nota o se sono previste più identità client, inserire l'identità speciale `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
```

Il traffico IP non può passare tra il client e il server finché ONTAP e il client non hanno impostato i criteri IPSec

corrispondenti e le credenziali di autenticazione (PSK o certificato) non sono installate su entrambi i lati. Per ulteriori informazioni, vedere la configurazione IPSec lato client.

Utilizzare le identità IPsec

Per il metodo di autenticazione con chiave pre-condivisa, le identità locali e remote sono facoltative se host e client utilizzano il metodo di autenticazione con chiave strongSwan e non è stato selezionato alcun criterio con caratteri jolly per l'host o il client.

Per il metodo di autenticazione PKI/certificato, le identità locali e remote sono obbligatorie. Le identità specificano l'identità certificata all'interno del certificato di ciascun lato e vengono utilizzate nel processo di verifica. Se l'identità remota è sconosciuta o se può essere costituita da diverse identità, utilizzare l'identità speciale `ANYTHING`.

A proposito di questa attività

All'interno di ONTAP, le identità vengono specificate modificando la voce SPD o durante la creazione del criterio SPD. Il nome SPD può essere un indirizzo IP o un nome di identità in formato stringa.

Fase

Per modificare un'impostazione di identità SPD esistente, utilizzare il seguente comando:

```
security ipsec policy modify
```

Comando di esempio

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

Configurazione di più client IPSec

Quando un numero limitato di client deve sfruttare IPSec, è sufficiente utilizzare una singola voce SPD per ciascun client. Tuttavia, quando centinaia o addirittura migliaia di client devono sfruttare IPSec, NetApp consiglia di utilizzare una configurazione con più client IPSec.

A proposito di questa attività

ONTAP supporta la connessione di più client su molte reti a un singolo indirizzo IP SVM con IPSec attivato. È possibile eseguire questa operazione utilizzando uno dei seguenti metodi:

- **Configurazione subnet**

  Per consentire a tutti i client di una determinata subnet (ad esempio 192.168.134.0/24) di connettersi a un singolo indirizzo IP SVM utilizzando una singola voce di policy SPD, è necessario specificare `remote-ip-subnets` sotto forma di subnet. Inoltre, è necessario specificare `remote-identity` campo con l'identità lato client corretta.

  > Quando si utilizza una singola voce di criterio in una configurazione di subnet, i client IPSec in tale subnet condividono l'identità IPSec e la chiave precondivisa (PSK). Tuttavia, questo non è vero con l'autenticazione del certificato. Quando si utilizzano i certificati, ciascun client può utilizzare il proprio certificato univoco o un certificato condiviso per l'autenticazione. IPSec ONTAP verifica la validità del certificato in base alle CA installate nel relativo archivio di attendibilità locale. ONTAP supporta anche il controllo dell'elenco di revoche di certificati (CRL).

- **Consenti configurazione di tutti i client**

Per consentire a qualsiasi client, indipendentemente dall'indirizzo IP di origine, di connettersi all'indirizzo IP SVM abilitato a IPSec, utilizzare `0.0.0.0/0` carattere jolly quando si specifica `remote-ip-subnets` campo.

Inoltre, è necessario specificare `remote-identity` campo con l'identità lato client corretta. Per l'autenticazione del certificato, è possibile immettere `ANYTHING`.

Inoltre, quando `0.0.0.0/0` se si utilizza il carattere jolly, è necessario configurare un numero di porta locale o remota specifico da utilizzare. Ad esempio, `NFS port 2049`.

Fasi

a. Utilizzare uno dei seguenti comandi per configurare IPSec per più client.

   i. Se si utilizza la **configurazione della subnet** per supportare più client IPsec:

   ```
   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
   ```

   Comando di esempio

   ```
   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. Se si utilizza l'opzione **Allow all clients Configuration** (Consenti configurazione di tutti i client) per supportare più client IPsec:

   ```
   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
   ```

   Comando di esempio

   ```
   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
   ```

Statistiche IPsec

Attraverso la negoziazione, è possibile stabilire un canale di sicurezza denominato SA (IKE Security Association) tra l'indirizzo IP di ONTAP SVM e l'indirizzo IP del client. I SAS IPSec vengono installati su entrambi gli endpoint per eseguire le operazioni di crittografia e decrittografia dei dati.

È possibile utilizzare i comandi delle statistiche per controllare lo stato di IPSec SAS e IKE SAS.

Comandi di esempio

Comando di esempio IKE SA:

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

Comando e output di esempio SA IPSec:

```
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
```

Comando e output di esempio SA IPSec:

```
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
```

Configurare le policy firewall per le LIF

La configurazione di un firewall migliora la sicurezza del cluster e impedisce l'accesso non autorizzato al sistema di storage. Per impostazione predefinita, il firewall integrato è configurato in modo da consentire l'accesso remoto a un set specifico di servizi IP per le LIF di dati, gestione e intercluster.

A partire da ONTAP 9.10.1:

- Le policy firewall sono obsolete e vengono sostituite dalle policy di servizio LIF. In precedenza, il firewall integrato era gestito tramite policy firewall. Questa funzionalità viene ora eseguita utilizzando una policy di servizio LIF.
- Tutti i criteri firewall sono vuoti e non aprono porte nel firewall sottostante. Tutte le porte devono invece essere aperte utilizzando una policy di servizio LIF.
- Non è richiesta alcuna azione dopo un aggiornamento alla versione 9.10.1 o successiva per passare dalle policy firewall alle policy di servizio LIF. Il sistema crea automaticamente policy di servizio LIF coerenti con le policy firewall in uso nella release precedente di ONTAP. Se si utilizzano script o altri strumenti che creano e gestiscono policy firewall personalizzate, potrebbe essere necessario aggiornare tali script per creare policy di servizio personalizzate.

Per ulteriori informazioni, vedere "LIF e policy di servizio in ONTAP 9.6 e versioni successive".

Le policy firewall possono essere utilizzate per controllare l'accesso ai protocolli dei servizi di gestione come SSH, HTTP, HTTPS, Telnet, NTP, NDMP, NDMPS, RSH, DNS O SNMP. Non è possibile impostare policy firewall per protocolli dati come NFS o SMB.

È possibile gestire il servizio firewall e le policy nei seguenti modi:

- Attivazione o disattivazione del servizio firewall
- Visualizzazione della configurazione corrente del servizio firewall
- Creazione di un nuovo criterio firewall con il nome del criterio e i servizi di rete specificati
- Applicazione di un criterio firewall a un'interfaccia logica
- Creazione di una nuova policy firewall che sia una copia esatta di una policy esistente

  È possibile utilizzare questa opzione per creare una policy con caratteristiche simili all'interno della stessa SVM o per copiare la policy su una SVM diversa.

- Visualizzazione di informazioni sui criteri firewall
- Modifica degli indirizzi IP e delle netmask utilizzati da una policy firewall
- Eliminazione di una policy firewall non utilizzata da una LIF

Policy firewall e LIF

I criteri firewall LIF vengono utilizzati per limitare l'accesso al cluster su ogni LIF. È necessario comprendere in che modo la policy firewall predefinita influenza l'accesso al sistema su ciascun tipo di LIF e come è possibile personalizzare una policy firewall per aumentare o ridurre la sicurezza su una LIF.

Durante la configurazione di un LIF utilizzando `network interface create` oppure `network interface modify` il valore specificato per `-firewall-policy` Il parametro determina i protocolli di servizio e gli indirizzi IP ai quali è consentito l'accesso a LIF.

In molti casi è possibile accettare il valore predefinito del criterio firewall. In altri casi, potrebbe essere necessario limitare l'accesso a determinati indirizzi IP e a determinati protocolli dei servizi di gestione. I protocolli dei servizi di gestione disponibili includono SSH, HTTP, HTTPS, Telnet, NTP, NDMP, NDMPS, RSH, DNS E SNMP.

Per impostazione predefinita, il criterio firewall per tutte le LIF del cluster è `""` e non possono essere modificati.

La tabella seguente descrive i criteri firewall predefiniti assegnati a ciascun LIF, in base al ruolo (ONTAP 9.5 e versioni precedenti) o ai criteri di servizio (ONTAP 9.6 e versioni successive), quando si crea il LIF:

Policy del firewall	Protocolli di servizio predefiniti	Accesso predefinito	LIF applicati a.
gestione	dns, http, https, ndmp, ndmps, ntp, snmp, ssh	Qualsiasi indirizzo (0.0.0.0/0)	Gestione del cluster, gestione SVM e LIF di gestione dei nodi
mgmt-nfs	dns, http, https, ndmp, ndmps, ntp, portmap, snmp, ssh	Qualsiasi indirizzo (0.0.0.0/0)	Le LIF dei dati che supportano anche l'accesso alla gestione SVM

intercluster	https, ndmp, ndmps	Qualsiasi indirizzo (0.0.0.0/0)	Tutti i LIF intercluster
dati	dns, ndmp, ndmps, portmap	Qualsiasi indirizzo (0.0.0.0/0)	Tutti i dati LIF

Configurazione del servizio portmap

Il servizio portmap associa i servizi RPC alle porte su cui sono in ascolto.

Il servizio portmap era sempre accessibile in ONTAP 9.3 e versioni precedenti, è diventato configurabile in ONTAP 9.4 fino a ONTAP 9.6 e viene gestito automaticamente a partire da ONTAP 9.7.

- In ONTAP 9.3 e versioni precedenti, il servizio portmap (rpcbind) era sempre accessibile sulla porta 111 nelle configurazioni di rete che si basavano sul firewall ONTAP integrato anziché su un firewall di terze parti.
- Da ONTAP 9.4 a ONTAP 9.6, è possibile modificare i criteri del firewall per controllare se il servizio portmap è accessibile su specifiche LIF.
- A partire da ONTAP 9.7, il servizio firewall portmap viene eliminato. La porta portmap viene invece aperta automaticamente per tutti i LIF che supportano il servizio NFS.

Il servizio Portmap è configurabile nel firewall in ONTAP 9.4 fino a ONTAP 9.6.

Il resto di questo argomento illustra come configurare il servizio firewall portmap per le versioni da ONTAP 9.4 a ONTAP 9.6.

A seconda della configurazione, potrebbe essere possibile non consentire l'accesso al servizio su specifici tipi di LIF, in genere LIF di gestione e di intercluster. In alcuni casi, potresti persino essere in grado di impedire l'accesso alle LIF dei dati.

Quale comportamento ci si può aspettare

Il comportamento da ONTAP 9.4 a ONTAP 9.6 è progettato per fornire una transizione perfetta all'aggiornamento. Se si accede già al servizio portmap su specifici tipi di LIF, questo continuerà ad essere accessibile attraverso questi tipi di LIF. Come in ONTAP 9,3 e versioni precedenti, nella policy di firewall per il tipo di LIF è possibile specificare i servizi a cui accedere.

Tutti i nodi del cluster devono eseguire ONTAP 9.4 fino a ONTAP 9.6 per rendere effettivo il comportamento. Viene influenzato solo il traffico in entrata.

Le nuove regole sono le seguenti:

- All'aggiornamento alla versione 9.4 fino alla 9.6, ONTAP aggiunge il servizio portmap a tutte le policy firewall esistenti, predefinite o personalizzate.
- Quando si crea un nuovo cluster o un nuovo IPSpace, ONTAP aggiunge il servizio portmap solo al criterio dati predefinito, non ai criteri di gestione predefiniti o di intercluster.
- È possibile aggiungere il servizio portmap alle policy predefinite o personalizzate in base alle necessità e rimuovere il servizio in base alle necessità.

Come aggiungere o rimuovere il servizio portmap

Per aggiungere il servizio portmap a una policy SVM o del firewall del cluster (renderlo accessibile all'interno del firewall), immettere:

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

Per rimuovere il servizio portmap da una policy SVM o del firewall del cluster (rendendolo inaccessibile all'interno del firewall), immettere:

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

È possibile utilizzare il comando di modifica dell'interfaccia di rete per applicare il criterio firewall a una LIF esistente. Per la sintassi completa dei comandi, vedere "Comandi di ONTAP 9".

Creare una policy firewall e assegnarla a una LIF

I criteri firewall predefiniti vengono assegnati a ciascun LIF quando si crea il LIF. In molti casi, le impostazioni predefinite del firewall funzionano correttamente e non è necessario modificarle. Se si desidera modificare i servizi di rete o gli indirizzi IP che possono accedere a una LIF, è possibile creare una policy firewall personalizzata e assegnarla alla LIF.

A proposito di questa attività

- Non è possibile creare un criterio firewall con `policy` nome `data`, `intercluster`, `cluster`, o. `mgmt`.

  Questi valori sono riservati ai criteri firewall definiti dal sistema.

- Non è possibile impostare o modificare un criterio firewall per le LIF del cluster.

  Il criterio del firewall per le LIF del cluster è impostato su 0.0.0.0/0 per tutti i tipi di servizi.

- Se è necessario rimuovere un servizio da un criterio, è necessario eliminare il criterio firewall esistente e crearne uno nuovo.
- Se IPv6 è attivato nel cluster, è possibile creare policy firewall con indirizzi IPv6.

  Dopo aver attivato IPv6, `data`, `intercluster`, e. `mgmt` I criteri firewall includono ::/0, il carattere jolly IPv6, nell'elenco degli indirizzi accettati.

- Quando si utilizza System Manager per configurare la funzionalità di protezione dei dati tra cluster, è necessario assicurarsi che gli indirizzi IP LIF tra cluster siano inclusi nell'elenco consentito e che il servizio HTTPS sia consentito sia per le LIF tra cluster che per i firewall di proprietà dell'azienda.

  Per impostazione predefinita, il `intercluster` La policy firewall consente l'accesso da tutti gli indirizzi IP (0.0.0.0/0, o ::/0 per IPv6) e abilita i servizi HTTPS, NDMP e NDMPS. Se si modifica questo criterio predefinito o si crea un criterio firewall personalizzato per le LIF tra cluster, è necessario aggiungere ciascun indirizzo IP LIF tra cluster all'elenco consentito e attivare il servizio HTTPS.

- A partire da ONTAP 9.6, i servizi firewall HTTPS e SSH non sono supportati.

  In ONTAP 9.6, il `management-https` e. `management-ssh` I servizi LIF sono disponibili per l'accesso alla gestione HTTPS e SSH.

Fasi

1. Creare una policy firewall che sarà disponibile per i LIF su una SVM specifica:

   ```
   system services firewall policy create -vserver vserver_name -policy
   ```

policy_name -service *network_service* -allow-list *ip_address/mask*

È possibile utilizzare questo comando più volte per aggiungere più di un servizio di rete e un elenco di indirizzi IP consentiti per ciascun servizio nella policy del firewall.

2. Verificare che il criterio sia stato aggiunto correttamente utilizzando `system services firewall policy show` comando.
3. Applicare il criterio firewall a una LIF:

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

4. Verificare che il criterio sia stato aggiunto correttamente alla LIF utilizzando `network interface show -fields firewall-policy` comando.

Esempio di creazione e applicazione di un criterio firewall a una LIF

Il seguente comando crea una policy firewall denominata data_http che abilita l'accesso ai protocolli HTTP e HTTPS dagli indirizzi IP sulla subnet 10.10, applica tale policy alla LIF denominata data1 su SVM vs1, quindi mostra tutte le policy firewall sul cluster:

```
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
```

Comandi per la gestione del servizio firewall e delle policy

È possibile utilizzare `system services firewall` comandi per la gestione del servizio firewall, il `system services firewall policy` comandi per la gestione delle policy firewall e di `network interface modify` Comando per gestire le impostazioni del firewall per le LIF.

Se si desidera…	Utilizzare questo comando…
Attiva o disattiva il servizio firewall	`system services firewall modify`
Visualizza la configurazione corrente per il servizio firewall	`system services firewall show`
Creare una policy firewall o aggiungere un servizio a una policy firewall esistente	`system services firewall policy create`
Applicare un criterio firewall a una LIF	`network interface modify -lif lifname -firewall-policy`
Modificare gli indirizzi IP e le netmask associate a un criterio firewall	`system services firewall policy modify`
Visualizza informazioni sui criteri firewall	`system services firewall policy show`
Creare una nuova policy firewall che sia una copia esatta di una policy esistente	`system services firewall policy clone`
Eliminare una policy firewall non utilizzata da una LIF	`system services firewall policy delete`

Per ulteriori informazioni, consultare le pagine man del `system services firewall`, `system services firewall policy`, e. `network interface modify` comandi in "Comandi di ONTAP 9".