Gestire la rete e la sicurezza

AFX

NetApp
February 10, 2026

Sommario

Gestire la rete e la sicurezza

Gestire la rete del cluster del sistema di archiviazione AFX

È necessario configurare la rete del sistema di archiviazione AFX. L'ambiente di rete supporta diversi scenari, tra cui l'accesso dei client ai dati sulle SVM e la comunicazione tra cluster.

Creare una risorsa di rete è un primo passo importante. È inoltre necessario eseguire ulteriori azioni amministrative, come la modifica o l'eliminazione delle definizioni di rete, a seconda delle necessità.

Crea un dominio di trasmissione

Un dominio broadcast semplifica la gestione della rete cluster raggruppando le porte che fanno parte della stessa rete di livello due. Alle macchine virtuali di archiviazione (SVM) possono quindi essere assegnate porte nel gruppo per il traffico dati o di gestione.

Durante la configurazione del cluster vengono creati diversi domini di broadcast, tra cui:

Predefinito
: Questo dominio di broadcast contiene porte nello spazio IP "Predefinito". Queste porte vengono utilizzate principalmente per la trasmissione dei dati. Sono incluse anche le porte di gestione dei cluster e dei nodi.

Grappolo
: Questo dominio di broadcast contiene porte nello spazio IP "Cluster". Queste porte vengono utilizzate per la comunicazione del cluster e includono tutte le porte del cluster da tutti i nodi nel cluster.

Dopo aver inizializzato il cluster, è possibile creare domini di broadcast aggiuntivi. Quando si crea un dominio broadcast, viene creato automaticamente un gruppo di failover contenente le stesse porte.

Informazioni su questo compito

Il valore dell'unità di trasmissione massima (MTU) delle porte definite per un dominio di broadcast viene aggiornato al valore MTU impostato nel dominio di broadcast.

Passi

1. In Gestione sistema, seleziona **Rete** e poi **Panoramica**.
2. In **Domini di trasmissione**, seleziona + Add .
3. Fornire il nome del dominio di trasmissione o accettare quello predefinito.

   Tutti i nomi di dominio broadcast devono essere univoci all'interno di uno spazio IP.

4. Fornire l'unità di trasmissione massima (MTU).

   L'MTU è il pacchetto dati più grande che può essere accettato nel dominio broadcast.

5. Selezionare le porte desiderate e selezionare **Salva**.

Crea uno spazio IP

Uno spazio IP è un dominio amministrativo per gli indirizzi IP e la relativa configurazione di rete. Questi spazi possono essere utilizzati per supportare le SVM tramite amministrazione e routing isolati. Ad esempio, sono utili quando i client hanno indirizzi IP sovrapposti provenienti dallo stesso intervallo di indirizzi IP e subnet.

Per poter creare una subnet è necessario disporre di uno spazio IP.

Passi

1. In Gestione sistema, seleziona **Rete** e poi **Panoramica**.
2. In **IPspaces**, seleziona + Add .
3. Fornire il nome dello spazio IP o accettare quello predefinito.

   Tutti i nomi IPspace devono essere univoci all'interno di un cluster.

4. Seleziona **Salva**.

Cosa c'è dopo?

È possibile utilizzare IPspace per creare una subnet.

Crea una sottorete

Una sottorete o subnet impone una divisione logica dello spazio degli indirizzi IP nella rete. Consente di allocare blocchi dedicati di indirizzi IP per la creazione di un'interfaccia di rete (LIF). Le subnet semplificano la creazione di LIF consentendo di utilizzare il nome della subnet anziché una combinazione specifica di indirizzo IP e maschera di rete.

Prima di iniziare

È necessario disporre di un dominio di broadcast e di uno spazio IP in cui verrà definita la subnet. Da notare inoltre:

- Tutti i nomi di subnet devono essere univoci all'interno di uno specifico spazio IP.
- L'intervallo di indirizzi IP utilizzato per una subnet non può sovrapporsi agli indirizzi IP di altre subnet.

Passi

1. In Gestione sistema, seleziona **Rete** e poi **Panoramica**.
2. Nella scheda **Sottoreti**, seleziona + Add .
3. Fornire i dettagli di configurazione, tra cui il nome della subnet, i dettagli dell'indirizzo IP e il dominio di broadcast.
4. Seleziona **Salva**.

Cosa c'è dopo?

La nuova subnet semplificherà la creazione delle interfacce di rete.

Creare un'interfaccia di rete

Un'interfaccia di rete logica (LIF) è costituita da un indirizzo IP e dai relativi parametri di configurazione di rete. Può essere associato a una porta fisica o logica e viene solitamente utilizzato dai client per accedere ai dati forniti da una SVM. I LIF garantiscono resilienza in caso di guasto e possono migrare tra le porte del nodo in modo che la comunicazione non venga interrotta.

Passi

1. In Gestione sistema, seleziona **Rete** e poi **Panoramica**.
2. Nella scheda **Interfacce di rete**, seleziona + Add .
3. Fornire i dettagli di configurazione, tra cui il nome dell'interfaccia, il tipo di interfaccia, i protocolli consentiti e i dettagli dell'indirizzo IP.
4. Seleziona **Salva**.

Informazioni correlate

- "Gestisci le porte Ethernet AFX"
- "Scopri di più sui domini di trasmissione ONTAP"
- "Scopri di più sulla configurazione di ONTAP IPspace"
- "Scopri di più sulle subnet per la rete ONTAP"
- "Panoramica dell'architettura di rete"

Gestire le porte Ethernet del sistema di archiviazione AFX

Le porte utilizzate dal sistema AFX costituiscono la base per la connettività e la comunicazione di rete. Sono disponibili diverse opzioni per personalizzare la configurazione di livello due della rete.

Creare un VLAN

Una VLAN è costituita da porte switch raggruppate in un dominio broadcast. Le VLAN consentono di aumentare la sicurezza, isolare potenziali problemi e limitare i percorsi disponibili all'interno dell'infrastruttura di rete IP.

Prima di iniziare

Gli switch distribuiti nella rete devono essere conformi agli standard IEEE 802.1Q oppure disporre di un'implementazione VLAN specifica del fornitore.

Informazioni su questo compito

Notare quanto segue:

- Non è possibile creare una VLAN su una porta di un gruppo di interfacce senza porte membro.
- Quando si configura una VLAN su una porta per la prima volta, la porta potrebbe non funzionare, causando una disconnessione temporanea della rete. Le successive aggiunte di VLAN alla stessa porta non influiscono sullo stato della porta.
- Non dovresti creare una VLAN su un'interfaccia di rete con lo stesso identificativo della VLAN nativa dello switch. Ad esempio, se l'interfaccia di rete e0b si trova sulla VLAN nativa 10, non è necessario creare una VLAN e0b-10 su tale interfaccia.

Passi

1. In Gestione sistema, seleziona **Rete** e poi **Porte Ethernet**.
2. Selezionare + VLAN .
3. Fornire i dettagli di configurazione, tra cui ID, dominio di broadcast e porte sui nodi desiderati.

La VLAN non può essere collegata a una porta che ospita un cluster LIF o a porte assegnate allo spazio IP del cluster.

4. Seleziona **Salva**.

Risultato

Hai creato una VLAN per aumentare la sicurezza, isolare i problemi e limitare i percorsi disponibili all'interno della tua infrastruttura di rete IP.

Creare un LAG

Un gruppo di aggregati di collegamenti (LAG) è una tecnica che combina più connessioni di rete fisiche in un'unica connessione logica. È possibile utilizzarlo per aumentare la larghezza di banda e garantire ridondanza tra i nodi.

Passi

1. In Gestione sistema, seleziona **Rete** e poi **Porte Ethernet**.
2. Seleziona **Collega gruppo aggregato**.
3. Fornire i dettagli di configurazione, tra cui nodo, dominio di broadcast, porte, modalità e distribuzione del carico.
4. Seleziona **Salva**.

Informazioni correlate

- "Gestire la rete del cluster AFX"
- "Scopri di più sulla configurazione delle porte di rete ONTAP"
- "Combina le porte fisiche per creare gruppi di interfacce ONTAP"

Preparare i servizi di autenticazione del sistema di archiviazione AFX

È necessario preparare i servizi di autenticazione e autorizzazione utilizzati dal sistema AFX per le definizioni degli account utente e dei ruoli.

Configurare LDAP

È possibile configurare un server LDAP (Lightweight Directory Access Protocol) per conservare le informazioni di autenticazione in una posizione centrale.

Prima di iniziare

È necessario aver generato una richiesta di firma del certificato e aggiunto un certificato digitale del server firmato da una CA.

Passi

1. In Gestione sistema, seleziona **Cluster** e poi **Impostazioni**.
2. Selezionare accanto a **LDAP**.
3. Selezionare + Add e fornire il nome o l'indirizzo IP del server LDAP.
4. Fornire le informazioni di configurazione necessarie, tra cui schema, DN di base, porta e binding.

5. Seleziona **Salva**.

Configurare l'autenticazione SAML

L'autenticazione Security Assertion Markup Language (SAML) consente agli utenti di essere autenticati da un provider di identità sicuro (IdP) anziché da provider che utilizzano altri protocolli come LDAP.

Prima di iniziare

- È necessario configurare il provider di identità che si intende utilizzare per l'autenticazione remota. Per i dettagli sulla configurazione, consultare la documentazione del provider.
- È necessario disporre dell'URI del provider di identità.

Passi

1. In Gestione sistema, seleziona **Cluster** e poi **Impostazioni**.
2. Selezionare in **Sicurezza** accanto a **Autenticazione SAML**.
3. Selezionare **Abilita autenticazione SAML**.
4. Fornire l'URL **IdP** e l'indirizzo IP del **sistema host** e selezionare **Salva**.

   Una finestra di conferma visualizza le informazioni sui metadati, che sono state automaticamente copiate negli appunti.

5. Accedi al sistema IdP specificato e copia i metadati dagli appunti per aggiornare i metadati del sistema.
6. Tornare alla finestra di conferma in System Manager e selezionare **Ho configurato l'IdP con l'URI host o i metadati**.
7. Selezionare **Disconnetti** per abilitare l'autenticazione basata su SAML.

   Il sistema IdP visualizzerà una schermata di autenticazione.

Informazioni correlate

- "Gestire gli utenti e i ruoli del cluster AFX"
- "Configurare l'autenticazione SAML per gli utenti ONTAP remoti"
- "Autenticazione e controllo degli accessi"

Gestire gli utenti e i ruoli del cluster del sistema di archiviazione AFX

È possibile definire account utente e ruoli in base ai servizi di autenticazione e autorizzazione disponibili con AFX.

A ciascun utente ONTAP deve essere assegnato un ruolo. Un ruolo include privilegi e determina quali azioni l'utente è in grado di eseguire.

Crea un ruolo di account

I ruoli per gli amministratori del cluster e gli amministratori delle VM di storage vengono creati automaticamente quando il cluster AFX viene configurato e inizializzato. È possibile creare ruoli di account

utente aggiuntivi per definire funzioni specifiche che gli utenti assegnati ai ruoli possono eseguire sul cluster.

Passi

1. In Gestione sistema, seleziona **Cluster** e poi **Impostazioni**.
2. Nella sezione **Sicurezza**, accanto a **Utenti e ruoli**, seleziona → .
3. In **Ruoli**, seleziona + Add .
4. Fornire il nome del ruolo e gli attributi.
5. Seleziona **Salva**.

Crea un account cluster

È possibile creare un account a livello di cluster da utilizzare durante l'amministrazione del cluster o della SVM.

Passi

1. In Gestione sistema, seleziona **Cluster** e poi **Impostazioni**.
2. Nella sezione **Sicurezza**, seleziona → accanto a **Utenti e ruoli**.
3. Selezionare + Add . in **Utenti**.
4. Inserisci un nome utente e poi seleziona il ruolo per l'utente.

   Il ruolo deve essere appropriato all'utente. Ad esempio, il ruolo **admin** è in grado di eseguire l'intera gamma di attività di configurazione sul cluster.

5. Selezionare il metodo di accesso dell'utente e il metodo di autenticazione; in genere sarà **Password**.
6. Inserisci una password per l'utente.
7. Seleziona **Salva**.

Risultato

Viene creato un nuovo account, disponibile per l'uso con il tuo cluster AFX.

Informazioni correlate

- "Preparare i servizi di autenticazione"
- "Amministrazione aggiuntiva AFX SVM"

Gestire i certificati su un sistema di archiviazione AFX

A seconda dell'ambiente, sarà necessario creare e gestire certificati digitali come parte dell'amministrazione di AFX. Ci sono diverse attività correlate che puoi svolgere.

Genera una richiesta di firma del certificato

Per iniziare a utilizzare un certificato digitale, è necessario generare una richiesta di firma del certificato (CSR). Una CSR viene utilizzata per richiedere un certificato firmato da un'autorità di certificazione (CA). A tale scopo, ONTAP crea una coppia di chiavi pubblica/privata e include la chiave pubblica nella CSR.

Passi

1. In Gestione sistema, seleziona **Cluster** e poi **Impostazioni**.

2. In **Sicurezza** e accanto a **Certificati**, seleziona →
3. Selezionare + Generate CSR .
4. Fornire il nome comune dell'oggetto e il paese; facoltativamente, fornire l'organizzazione e l'unità organizzativa.
5. Per modificare i valori predefiniti che definiranno il certificato, selezionare ↙↗ More options e apportare gli aggiornamenti desiderati.
6. Seleziona **Genera**.

Risultato

Hai generato una CSR che può essere utilizzata per richiedere un certificato a chiave pubblica.

Aggiungi un'autorità di certificazione attendibile

ONTAP fornisce un set predefinito di certificati radice attendibili da utilizzare con Transport Layer Security (TLS) e altri protocolli. È possibile aggiungere altre autorità di certificazione attendibili in base alle esigenze.

Passi

1. In Gestione sistema, seleziona **Cluster** e poi **Impostazioni**.
2. In **Sicurezza** e accanto a **Certificati**, seleziona → .
3. Selezionare la scheda **Autorità di certificazione attendibili** e quindi selezionare + Add .
4. Fornire le informazioni di configurazione, tra cui nome, ambito, nome comune, tipo e dettagli del certificato; è possibile importare il certificato selezionando **Importa**.
5. Selezionare **Aggiungi**.

Risultato

Hai aggiunto un'autorità di certificazione attendibile al tuo sistema AFX.

Rinnovare o eliminare un'autorità di certificazione attendibile

Le autorità di certificazione attendibili devono essere rinnovate annualmente. Se non si desidera rinnovare un certificato scaduto, è necessario eliminarlo.

Passi

1. Selezionare **Cluster** e poi **Impostazioni**.
2. In **Sicurezza** e accanto a **Certificati**, seleziona → .
3. Selezionare la scheda **Autorità di certificazione attendibili**.
4. Selezionare l'autorità di certificazione attendibile che si desidera rinnovare o eliminare.
5. Rinnovare o eliminare l'autorità di certificazione.

Per rinnovare l'autorità di certificazione, procedere come segue:	**Per eliminare l'autorità di certificazione, procedere come segue:**
a. Selezionare ⋮ e poi seleziona **Rinnova**. b. Inserisci o importa le informazioni del certificato e seleziona **Rinnova**.	a. Selezionare ⋮ e quindi seleziona **Elimina**. b. Conferma che vuoi eliminare e seleziona **Elimina**.

Risultato

Hai rinnovato o eliminato un'autorità di certificazione attendibile esistente sul tuo sistema AFX.

Aggiungere un certificato client/server o un'autorità di certificazione locale

È possibile aggiungere un certificato client/server o un'autorità di certificazione locale per abilitare servizi Web sicuri.

Passi

1. In Gestione sistema, seleziona **Cluster** e poi **Impostazioni**.
2. In **Sicurezza** e accanto a **Certificati**, seleziona → .
3. Selezionare **Certificati client/server** o **Autorità di certificazione locali**, a seconda delle esigenze.
4. Aggiungi le informazioni del certificato e seleziona **Salva**.

Risultato

Hai aggiunto un nuovo certificato client/server o autorità locali al tuo sistema AFX.

Rinnovare o eliminare un certificato client/server o autorità di certificazione locali

I certificati client/server e le autorità di certificazione locali devono essere rinnovati annualmente. Se non si desidera rinnovare un certificato scaduto o le autorità di certificazione locali, è necessario eliminarli.

Passi

1. Selezionare **Cluster** e poi **Impostazioni**.
2. In **Sicurezza** e accanto a Certificati, seleziona → .
3. Selezionare **Certificati client/server** o **Autorità di certificazione locali**, a seconda delle esigenze.
4. Seleziona il certificato che desideri rinnovare o eliminare.
5. Rinnovare o eliminare l'autorità di certificazione.

Per rinnovare l'autorità di certificazione, procedere come segue:	**Per eliminare l'autorità di certificazione, procedere come segue:**
a. Selezionare ⋮ e poi seleziona **Rinnova**. b. Inserisci o importa le informazioni del certificato e seleziona **Rinnova**.	Selezionare ⋮ e quindi seleziona **Elimina**.

Risultato

Hai rinnovato o eliminato un certificato client/server esistente o un'autorità di certificazione locale sul tuo sistema AFX.

Informazioni correlate

- "Generare e installare un certificato server firmato da CA in ONTAP"
- "Gestire i certificati ONTAP con System Manager"

Informazioni sul copyright

Informazioni sul marchio commerciale