Preparatevi per il peering di cluster e SVM

ONTAP 9

NetApp
April 24, 2024

Sommario

Preparatevi per il peering di cluster e SVM

Nozioni di base sul peering

È necessario creare *relazioni peer* tra cluster di origine e di destinazione e tra SVM di origine e di destinazione prima di poter replicare le copie Snapshot utilizzando SnapMirror. Una relazione peer definisce le connessioni di rete che consentono a cluster e SVM di scambiare dati in modo sicuro.

I cluster e le SVM nelle relazioni tra pari comunicano sulla rete intercluster utilizzando *LIF (Intercluster Logical Interface)*. Una LIF intercluster è una LIF che supporta il servizio di interfaccia di rete "intercluster-core" e viene generalmente creata utilizzando la policy del servizio di interfaccia di rete "intercluster predefinito". È necessario creare LIF intercluster su ogni nodo dei cluster sottoposti a peering.

Le LIF di intercluster utilizzano i percorsi che appartengono alla SVM di sistema a cui sono assegnate. ONTAP crea automaticamente una SVM di sistema per le comunicazioni a livello di cluster all'interno di un IPSpace.

Sono supportate entrambe le topologie fan-out e cascata. In una topologia a cascata, è necessario creare solo reti di intercluster tra i cluster primario e secondario e tra i cluster secondario e terziario. Non è necessario creare una rete di intercluster tra il cluster primario e il cluster terzo.

> È possibile (ma non consigliabile) che un amministratore rimuova il servizio intercluster-core dalla policy di servizio intercluster predefinita. In questo caso, i LIF creati utilizzando "intercluster predefinito" non saranno effettivamente LIF intercluster. Per confermare che la policy di servizio dell'intercluster predefinito contiene il servizio intercluster-core, utilizzare il seguente comando:
>
> ```
> network interface service-policy show -policy default-intercluster
> ```

Prerequisiti per il peering del cluster

Prima di configurare il peering del cluster, verificare che la connettività, la porta, l'indirizzo IP, la subnet, il firewall, e i requisiti di naming dei cluster sono soddisfatti.

> A partire da ONTAP 9.6, la crittografia peer del cluster fornisce il supporto per la crittografia GCM TLS 1.2 AES-256 per la replica dei dati per impostazione predefinita. I cifrari di sicurezza predefiniti ("PSK-AES256-GCM-SHA384") sono necessari per il funzionamento del peering del cluster anche se la crittografia è disattivata.
>
> A partire da ONTAP 9.11.1, le crittografia di sicurezza DHE-PSK sono disponibili per impostazione predefinita.

Requisiti di connettività

Ogni LIF di intercluster sul cluster locale deve essere in grado di comunicare con ogni LIF di intercluster sul cluster remoto.

Sebbene non sia necessario, è in genere più semplice configurare gli indirizzi IP utilizzati per le LIF di intercluster nella stessa subnet. Gli indirizzi IP possono risiedere nella stessa sottorete dei file LIF dei dati o in una sottorete diversa. La subnet utilizzata in ciascun cluster deve soddisfare i seguenti requisiti:

- La subnet deve appartenere al dominio di trasmissione che contiene le porte utilizzate per la comunicazione tra cluster.
- La subnet deve disporre di un numero sufficiente di indirizzi IP da allocare a un LIF intercluster per nodo.

  Ad esempio, in un cluster a quattro nodi, la subnet utilizzata per la comunicazione tra cluster deve avere quattro indirizzi IP disponibili.

Ciascun nodo deve disporre di una LIF intercluster con un indirizzo IP sulla rete intercluster.

Le LIF di intercluster possono avere un indirizzo IPv4 o IPv6.

> ONTAP consente di migrare le reti peering da IPv4 a IPv6, consentendo la presenza simultanea di entrambi i protocolli nelle LIF dell'intercluster. Nelle versioni precedenti, tutte le relazioni tra cluster per un intero cluster erano IPv4 o IPv6. Ciò significava che la modifica dei protocolli era un evento potenzialmente disgregativo.

Requisiti delle porte

È possibile utilizzare porte dedicate per la comunicazione tra cluster o condividere le porte utilizzate dalla rete dati. Le porte devono soddisfare i seguenti requisiti:

- Tutte le porte utilizzate per comunicare con un determinato cluster remoto devono trovarsi nello stesso IPSpace.

  È possibile utilizzare più IPspaces per eseguire il peer con più cluster. La connettività full-mesh a coppie è necessaria solo all'interno di un IPSpace.

- Il dominio di broadcast utilizzato per la comunicazione tra cluster deve includere almeno due porte per nodo in modo che la comunicazione tra cluster possa eseguire il failover da una porta a un'altra.

  Le porte aggiunte a un dominio di broadcast possono essere porte di rete fisiche, VLAN o gruppi di interfacce (ifgrps).

- Tutte le porte devono essere cablate.
- Tutte le porte devono essere in buono stato.
- Le impostazioni MTU delle porte devono essere coerenti.

Requisiti del firewall

> A partire da ONTAP 9.10.1, le policy firewall sono obsolete e completamente sostituite con le policy di servizio LIF. Per ulteriori informazioni, vedere "Configurare le policy firewall per le LIF".

I firewall e i criteri di firewall tra cluster devono consentire i seguenti protocolli:

- Traffico ICMP bidirezionale
- Traffico TCP avviato in modo bidirezionale verso gli indirizzi IP di tutti i LIF intercluster sulle porte 11104 e 11105
- HTTPS bidirezionale tra le LIF dell'intercluster

  Sebbene HTTPS non sia richiesto quando si imposta il peering del cluster utilizzando la CLI, HTTPS è richiesto in seguito se si utilizza System Manager per configurare la protezione dei dati.

L'impostazione predefinita `intercluster` La policy firewall consente l'accesso tramite il protocollo HTTPS e da tutti gli indirizzi IP (0.0.0.0/0). Se necessario, è possibile modificare o sostituire la policy.

Requisito del cluster

I cluster devono soddisfare i seguenti requisiti:

- Un cluster non può trovarsi in una relazione peer con più di 255 cluster.

Utilizzare porte condivise o dedicate

È possibile utilizzare porte dedicate per la comunicazione tra cluster o condividere le porte utilizzate dalla rete dati. Per decidere se condividere le porte, è necessario considerare la larghezza di banda della rete, l'intervallo di replica e la disponibilità delle porte.

È possibile condividere le porte su un cluster peered utilizzando le porte dedicate sull'altro.

Larghezza di banda della rete

Se si dispone di una rete ad alta velocità, ad esempio 10 GbE, potrebbe essere disponibile una larghezza di banda LAN locale sufficiente per eseguire la replica utilizzando le stesse porte 10 GbE utilizzate per l'accesso ai dati.

Anche in questo caso, è necessario confrontare la larghezza di banda WAN disponibile con la larghezza di banda della LAN. Se la larghezza di banda WAN disponibile è significativamente inferiore a 10 GbE, potrebbe essere necessario utilizzare porte dedicate.

L'unica eccezione a questa regola potrebbe essere rappresentata dal fatto che tutti o molti nodi del cluster replicano i dati, nel qual caso l'utilizzo della larghezza di banda è in genere distribuito tra i nodi.

Se non si utilizzano porte dedicate, le dimensioni massime dell'unità di trasmissione (MTU) della rete di replica dovrebbero essere le stesse della dimensione MTU della rete dati.

Intervallo di replica

Se la replica avviene in ore non di punta, dovresti essere in grado di utilizzare le porte dati per la replica anche senza una connessione LAN a 10 GbE.

Se la replica avviene durante il normale orario di lavoro, è necessario considerare la quantità di dati che verranno replicati e se richiede una larghezza di banda così elevata da causare conflitti con i protocolli dati. Se l'utilizzo della rete da parte dei protocolli di dati (SMB, NFS, iSCSI) è superiore al 50%, è necessario utilizzare porte dedicate per la comunicazione tra cluster, per consentire prestazioni non degradate in caso di failover del nodo.

Disponibilità delle porte

Se si determina che il traffico di replica interferisce con il traffico dati, è possibile migrare le LIF di intercluster su qualsiasi altra porta condivisa compatibile con intercluster sullo stesso nodo.

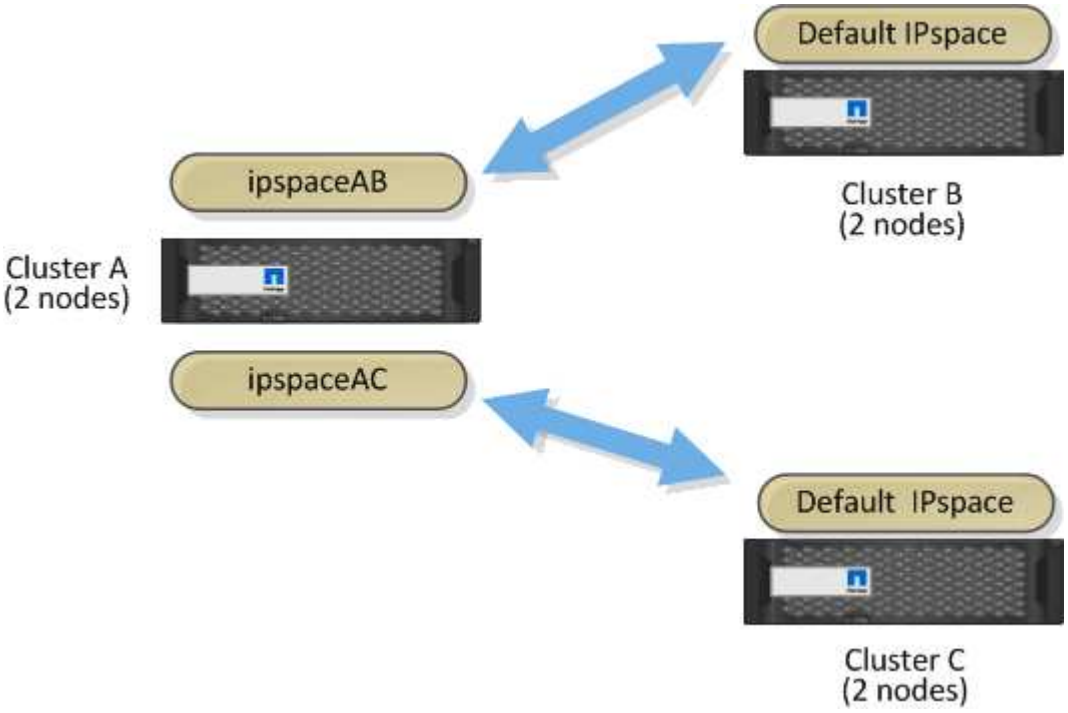
È inoltre possibile dedicare le porte VLAN per la replica. La larghezza di banda della porta è condivisa tra tutte le VLAN e la porta base.

Utilizzare IPspaces personalizzati per isolare il traffico di replica

È possibile utilizzare IPspaces personalizzati per separare le interazioni di un cluster con i peer. Detta *connettività intercluster designata*, questa configurazione consente ai service provider di isolare il traffico di replica in ambienti multi-tenant.

Si supponga, ad esempio, di voler separare il traffico di replica tra il cluster A e il cluster B dal traffico di replica tra il cluster A e il cluster C. A tale scopo, è possibile creare due IPspaces sul cluster A.

Un IPSpace contiene le LIF intercluster utilizzate per comunicare con il cluster B. L'altro contiene le LIF di intercluster utilizzate per comunicare con il cluster C, come mostrato nell'illustrazione seguente.



Per una configurazione IPSpace personalizzata, consultare la *Guida alla gestione di rete*.