



Preparar-se para peering de cluster e SVM

ONTAP 9

NetApp
January 17, 2025

Índice

- Preparar-se para peering de cluster e SVM 1
 - Noções básicas de peering 1
 - Pré-requisitos para peering de cluster 1
 - Use portas compartilhadas ou dedicadas 3
 - Use IPspaces personalizados para isolar o tráfego de replicação 4

Preparar-se para peering de cluster e SVM

Noções básicas de peering

Você deve criar relacionamentos *peer* entre clusters de origem e destino e entre SVMs de origem e destino antes de poder replicar cópias Snapshot usando o SnapMirror. Um relacionamento de pares define conexões de rede que permitem que clusters e SVMs troquem dados com segurança.

Clusters e SVMs em relações entre pares se comunicam pela rede entre clusters usando *interfaces lógicas* (LIFs). um LIF entre clusters é um LIF que suporta o serviço de interface de rede "entre clusters-core" e é normalmente criado usando a política de serviço de interface de rede "default-clusters". É necessário criar LIFs entre clusters em cada nó nos clusters que estão sendo perados.

Os LIFs usam rotas que pertencem ao SVM do sistema ao qual são atribuídos. O ONTAP cria automaticamente um sistema SVM para comunicações em nível de cluster em um espaço de IPspace.

Topologias de fan-out e cascata são suportadas. Em uma topologia em cascata, você só precisa criar redes entre clusters primários e secundários e entre clusters secundários e secundários. Não é necessário criar uma rede entre clusters primário e terciário.



É possível (mas não aconselhável) que um administrador remova o serviço entre clusters da política de serviços padrão entre clusters. Se isso ocorrer, LIFs criadas usando "default-clusters" não serão, na verdade, LIFs entre clusters. Para confirmar que a política de serviço padrão contém o serviço entre clusters-core, use o seguinte comando:

```
network interface service-policy show -policy default-intercluster
```

Pré-requisitos para peering de cluster

Antes de configurar o peering de cluster, você deve confirmar se os requisitos de conectividade, porta, endereço IP, sub-rede, firewall e nomenclatura de cluster são atendidos.



A partir do ONTAP 9.6, o peering de cluster fornece suporte de criptografia TLS 1,2 AES-256 GCM para replicação de dados por padrão. As cifras de segurança padrão ("PSK-AES256-GCM-SHA384") são necessárias para que o peering de cluster funcione mesmo que a criptografia esteja desativada.

Começando com ONTAP 9.11,1, as cifras de segurança DHE-PSK estão disponíveis por padrão.

A partir do ONTAP 9.15,1, o peering de cluster fornece suporte de criptografia TLS 1,3 para replicação de dados por padrão.

Requisitos de conectividade

Cada LIF no cluster local deve ser capaz de se comunicar com cada LIF entre clusters no cluster remoto.

Embora não seja necessário, geralmente é mais simples configurar os endereços IP usados para LIFs entre

clusters na mesma sub-rede. Os endereços IP podem residir na mesma sub-rede que os LIFs de dados ou em uma sub-rede diferente. A sub-rede usada em cada cluster deve atender aos seguintes requisitos:

- A sub-rede deve pertencer ao domínio de broadcast que contém as portas usadas para comunicação entre clusters.
- A sub-rede deve ter endereços IP suficientes disponíveis para alocar a um LIF entre clusters por nó.

Por exemplo, em um cluster de quatro nós, a sub-rede usada para comunicação entre clusters deve ter quatro endereços IP disponíveis.

Cada nó deve ter um LIF entre clusters com um endereço IP na rede entre clusters.

LIFs podem ter um endereço IPv4 ou um endereço IPv6 entre clusters.



O ONTAP permite que você migre suas redes de peering de IPv4 para IPv6, permitindo opcionalmente que ambos os protocolos estejam presentes simultaneamente nas LIFs entre clusters. Em versões anteriores, todas as relações entre clusters para um cluster inteiro eram IPv4 ou IPv6. Isso significava que a mudança de protocolos era um evento potencialmente disruptivo.

Requisitos portuários

Você pode usar portas dedicadas para comunicação entre clusters ou compartilhar portas usadas pela rede de dados. As portas devem atender aos seguintes requisitos:

- Todas as portas usadas para se comunicar com um determinado cluster remoto devem estar no mesmo espaço IPspace.

Você pode usar vários IPspaces para fazer pares com vários clusters. A conectividade de malha completa em pares é necessária apenas dentro de um espaço IPspace.

- O domínio de broadcast usado para comunicação entre clusters deve incluir pelo menos duas portas por nó para que a comunicação entre clusters possa fazer failover de uma porta para outra porta.

As portas adicionadas a um domínio de broadcast podem ser portas de rede físicas, VLANs ou grupos de interface (ifgrps).

- Todas as portas devem ser cabeadas.
- Todas as portas devem estar em um estado saudável.
- As configurações de MTU das portas devem ser consistentes.

Requisitos de firewall



A partir do ONTAP 9.10,1, as políticas de firewall são obsoletas e totalmente substituídas por políticas de serviço LIF. Para obter mais informações, "[Configurar políticas de firewall para LIFs](#)" consulte .

Os firewalls e a política de firewall entre clusters devem permitir os seguintes protocolos:

- Tráfego ICMP bidirecional
- Tráfego TCP iniciado bidirecional para os endereços IP de todas as LIFs entre clusters nas portas 11104 e

11105

- HTTPS bidirecional entre os LIFs entre clusters

Embora o HTTPS não seja necessário quando você configura o peering de cluster usando a CLI, o HTTPS é necessário mais tarde se você usar o System Manager para configurar a proteção de dados.

A política de firewall predefinida `intercluster` permite o acesso através do protocolo HTTPS e de todos os endereços IP (0,0.0,0/0). Você pode modificar ou substituir a política, se necessário.

Requisito de cluster

Os clusters precisam atender aos seguintes requisitos:

- Um cluster não pode estar em um relacionamento de pares com mais de 255 clusters.

Use portas compartilhadas ou dedicadas

Você pode usar portas dedicadas para comunicação entre clusters ou compartilhar portas usadas pela rede de dados. Ao decidir se deseja compartilhar portas, você precisa considerar a largura de banda da rede, o intervalo de replicação e a disponibilidade da porta.



Você pode compartilhar portas em um cluster com peered enquanto usa portas dedicadas no outro.

Largura de banda da rede

Se você tiver uma rede de alta velocidade, como 10 GbE, talvez tenha largura de banda local suficiente para executar a replicação usando as mesmas portas de 10 GbE usadas para acesso aos dados.

Mesmo assim, você deve comparar a largura de banda da WAN disponível com a largura de banda da LAN. Se a largura de banda da WAN disponível for significativamente menor que 10 GbE, talvez seja necessário usar portas dedicadas.



A única exceção a essa regra pode ser quando todos ou muitos nós no cluster replicarem dados, caso em que a utilização da largura de banda é normalmente espalhada pelos nós.

Se você não estiver usando portas dedicadas, o tamanho máximo da unidade de transmissão (MTU) da rede de replicação geralmente deve ser o mesmo que o tamanho da MTU da rede de dados.

Intervalo de replicação

Se a replicação ocorrer em horas fora do pico, você poderá usar portas de dados para replicação mesmo sem uma conexão LAN de 10 GbE.

Se a replicação ocorrer durante o horário comercial normal, você precisa considerar a quantidade de dados que serão replicados e se ela precisará de tanta largura de banda que poderia causar contenção com protocolos de dados. Se a utilização da rede por protocolos de dados (SMB, NFS, iSCSI) for superior a 50%, deverá utilizar portas dedicadas para comunicação entre clusters, para permitir uma performance não degradada se ocorrer failover de nó.

Disponibilidade da porta

Se você determinar que o tráfego de replicação está interferindo no tráfego de dados, poderá migrar LIFs para qualquer outra porta compartilhada com capacidade para clusters no mesmo nó.

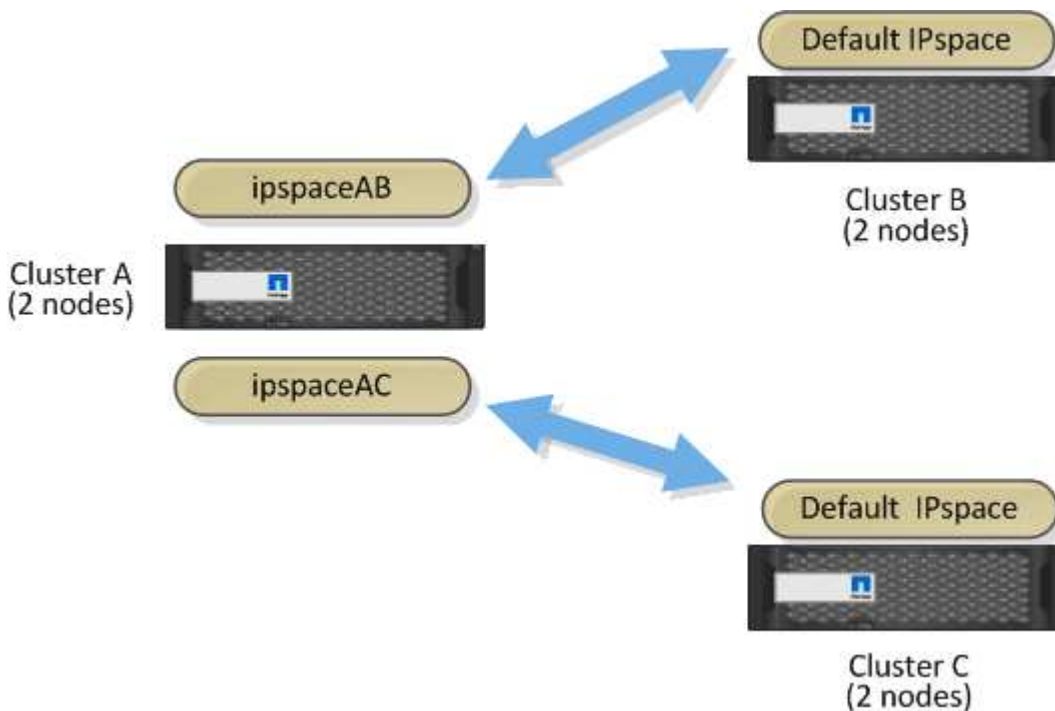
Você também pode dedicar portas VLAN para replicação. A largura de banda da porta é compartilhada entre todas as VLANs e a porta base.

Use IPspaces personalizados para isolar o tráfego de replicação

Você pode usar IPspaces personalizados para separar as interações que um cluster tem com seus pares. Chamada de *conetividade entre clusters designada*, essa configuração permite que os provedores de serviços isolem o tráfego de replicação em ambientes multitenant.

Suponha, por exemplo, que você deseja que o tráfego de replicação entre o Cluster A e o Cluster B seja separado do tráfego de replicação entre o Cluster A e o Cluster C. Para conseguir isso, você pode criar dois espaços IPspaces no Cluster A.

Um IPspace contém as LIFs entre clusters que você usa para se comunicar com o Cluster B. O outro contém as LIFs entre clusters que você usa para se comunicar com o Cluster C, como mostrado na ilustração a seguir.



Para a configuração de IPspace personalizada, consulte o *Network Management Guide*.

Informações sobre direitos autorais

Copyright © 2025 NetApp, Inc. Todos os direitos reservados. Impresso nos EUA. Nenhuma parte deste documento protegida por direitos autorais pode ser reproduzida de qualquer forma ou por qualquer meio — gráfico, eletrônico ou mecânico, incluindo fotocópia, gravação, gravação em fita ou storage em um sistema de recuperação eletrônica — sem permissão prévia, por escrito, do proprietário dos direitos autorais.

O software derivado do material da NetApp protegido por direitos autorais está sujeito à seguinte licença e isenção de responsabilidade:

ESTE SOFTWARE É FORNECIDO PELA NETAPP "NO PRESENTE ESTADO" E SEM QUAISQUER GARANTIAS EXPRESSAS OU IMPLÍCITAS, INCLUINDO, SEM LIMITAÇÕES, GARANTIAS IMPLÍCITAS DE COMERCIALIZAÇÃO E ADEQUAÇÃO A UM DETERMINADO PROPÓSITO, CONFORME A ISENÇÃO DE RESPONSABILIDADE DESTES DOCUMENTOS. EM HIPÓTESE ALGUMA A NETAPP SERÁ RESPONSÁVEL POR QUALQUER DANO DIRETO, INDIRETO, INCIDENTAL, ESPECIAL, EXEMPLAR OU CONSEQUENCIAL (INCLUINDO, SEM LIMITAÇÕES, AQUISIÇÃO DE PRODUTOS OU SERVIÇOS SOBRESSALIENTES; PERDA DE USO, DADOS OU LUCROS; OU INTERRUPÇÃO DOS NEGÓCIOS), INDEPENDENTEMENTE DA CAUSA E DO PRINCÍPIO DE RESPONSABILIDADE, SEJA EM CONTRATO, POR RESPONSABILIDADE OBJETIVA OU PREJUÍZO (INCLUINDO NEGLIGÊNCIA OU DE OUTRO MODO), RESULTANTE DO USO DESTES SOFTWARES, MESMO SE ADVERTIDA DA RESPONSABILIDADE DE TAL DANO.

A NetApp reserva-se o direito de alterar quaisquer produtos descritos neste documento, a qualquer momento e sem aviso. A NetApp não assume nenhuma responsabilidade nem obrigação decorrentes do uso dos produtos descritos neste documento, exceto conforme expressamente acordado por escrito pela NetApp. O uso ou a compra deste produto não representam uma licença sob quaisquer direitos de patente, direitos de marca comercial ou quaisquer outros direitos de propriedade intelectual da NetApp.

O produto descrito neste manual pode estar protegido por uma ou mais patentes dos EUA, patentes estrangeiras ou pedidos pendentes.

LEGENDA DE DIREITOS LIMITADOS: o uso, a duplicação ou a divulgação pelo governo estão sujeitos a restrições conforme estabelecido no subparágrafo (b)(3) dos Direitos em Dados Técnicos - Itens Não Comerciais no DFARS 252.227-7013 (fevereiro de 2014) e no FAR 52.227- 19 (dezembro de 2007).

Os dados aqui contidos pertencem a um produto comercial e/ou serviço comercial (conforme definido no FAR 2.101) e são de propriedade da NetApp, Inc. Todos os dados técnicos e software de computador da NetApp fornecidos sob este Contrato são de natureza comercial e desenvolvidos exclusivamente com despesas privadas. O Governo dos EUA tem uma licença mundial limitada, irrevogável, não exclusiva, intransferível e não sublicenciável para usar os Dados que estão relacionados apenas com o suporte e para cumprir os contratos governamentais desse país que determinam o fornecimento de tais Dados. Salvo disposição em contrário no presente documento, não é permitido usar, divulgar, reproduzir, modificar, executar ou exibir os dados sem a aprovação prévia por escrito da NetApp, Inc. Os direitos de licença pertencentes ao governo dos Estados Unidos para o Departamento de Defesa estão limitados aos direitos identificados na cláusula 252.227-7015(b) (fevereiro de 2014) do DFARS.

Informações sobre marcas comerciais

NETAPP, o logotipo NETAPP e as marcas listadas em <http://www.netapp.com/TM> são marcas comerciais da NetApp, Inc. Outros nomes de produtos e empresas podem ser marcas comerciais de seus respectivos proprietários.