Vorbereitung auf Cluster- und SVM-Peering

ONTAP 9

NetApp
September 09, 2026

This PDF was generated from https://docs.netapp.com/de-de/ontap/peering/peering-basics-concept.html on September 09, 2026. Always check docs.netapp.com for the latest.

Inhalt

Vorbereitung auf Cluster- und SVM-Peering . . . 1
- Grundlagen des ONTAP Peerings . . . 1
- ONTAP Voraussetzungen für ONTAP Peering . . . 1
  - Konnektivitätsanforderungen . . . 2
  - Port-Anforderungen . . . 2
  - Firewall-Anforderungen . . . 2
  - Cluster-Peer-Limits . . . 3
- Gemeinsam genutzte oder dedizierte ONTAP Ports verwenden . . . 3
  - Netzwerkbandbreite . . . 3
  - Replikationsintervall . . . 4
  - Portverfügbarkeit . . . 4
- Benutzerdefinierte ONTAP IPspaces ermöglichen die Isolierung des Replikationsverkehrs. . . . 4

Vorbereitung auf Cluster- und SVM-Peering

Grundlagen des ONTAP Peerings

Peer-Beziehungen zwischen Quell- und Ziel-Cluster sowie zwischen Quell- und Ziel-SVMs müssen erstellt werden, bevor Snapshots mithilfe von SnapMirror repliziert werden können. Eine Peer-Beziehung definiert Netzwerkverbindungen, die den sicheren Datenaustausch zwischen Clustern und SVMs ermöglichen.

Cluster und SVMs in Peer-Beziehungen kommunizieren über das Intercluster-Netzwerk mithilfe von *logischen Intercluster-Schnittstellen (LIFs).* Eine Intercluster-LIF ist eine LIF, die den Netzwerkschnittstellendienst „intercluster-core“ unterstützt und typischerweise mit der Netzwerkschnittstellendienstrichtlinie „default-intercluster“ erstellt wird. Intercluster-LIFs sind auf jedem Node der zu peerenden Cluster zu erstellen.

Intercluster-LIFs verwenden Routen, die zur System-SVM gehören, der sie zugewiesen sind. ONTAP erstellt automatisch eine System-SVM für Cluster-Kommunikation innerhalb eines IPspace.

Sowohl Fan-out- als auch Kaskadentopologien werden unterstützt. In einer Kaskadentopologie ist es nur erforderlich, Intercluster-Netzwerke zwischen dem primären und dem sekundären Cluster sowie zwischen dem sekundären und dem tertiären Cluster zu erstellen. Ein Intercluster-Netzwerk zwischen dem primären und dem tertiären Cluster ist nicht erforderlich.

Es ist möglich (aber nicht empfehlenswert), dass ein Administrator den intercluster-core Service aus der default-intercluster Service-Richtlinie entfernt. Falls dies geschieht, sind mit „default-intercluster“ erstellte LIFs tatsächlich keine Intercluster-LIFs. Zur Bestätigung, dass die default-intercluster Service-Richtlinie den intercluster-core Service enthält, kann folgender Befehl verwendet werden:

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

Weitere Informationen zu `network interface service-policy show` finden sich in der "ONTAP-Befehlsreferenz".

ONTAP Voraussetzungen für ONTAP Peering

Bevor Sie Cluster-Peering einrichten, sollten Sie sicherstellen, dass die Anforderungen an Konnektivität, Port, IP-Adresse, Subnetz, Firewall und Cluster erfüllt sind.

Ab ONTAP 9.6 bietet Cluster Peering standardmäßig Unterstützung für TLS 1.2 AES-256 GCM-Verschlüsselung bei der Datenreplizierung. Die standardmäßigen Sicherheitsverschlüsselungsverfahren („PSK-AES256-GCM-SHA384“) sind für die Funktion von Cluster Peering erforderlich, selbst wenn die Verschlüsselung deaktiviert ist.

Ab ONTAP 9.11.1 sind DHE-PSK Sicherheitsverschlüsselungsverfahren standardmäßig verfügbar.

Ab ONTAP 9.15.1 bietet Cluster Peering standardmäßig Unterstützung für TLS 1.3-Verschlüsselung bei der Datenreplizierung.

Konnektivitätsanforderungen

Jede Intercluster-LIF auf dem lokalen Cluster muss mit jeder Intercluster-LIF auf dem Remote-Cluster kommunizieren können.

Obwohl es nicht zwingend erforderlich ist, ist es in der Regel einfacher, die für die Intercluster-LIFs verwendeten IP-Adressen im selben Subnetz zu konfigurieren. Die IP-Adressen können sich im selben Subnetz wie die Daten-LIFs oder in einem anderen Subnetz befinden. Das in jedem Cluster verwendete Subnetz muss die folgenden Anforderungen erfüllen:

- Das Subnetz muss zur Broadcast-Domäne gehören, die die Ports enthält, die für die Intercluster-Verbindung verwendet werden.
- Das Subnetz muss über genügend verfügbare IP-Adressen verfügen, um einer Intercluster-LIF pro Knoten eine Adresse zuzuweisen.

  Beispielsweise muss in einem Cluster mit vier Knoten das für die Intercluster-Verbindung verwendete Subnetz über vier verfügbare IP-Adressen verfügen.

Jeder Knoten muss über eine Intercluster-LIF mit einer IP-Adresse im Intercluster-Netzwerk verfügen.

Intercluster LIFs können eine IPv4-Adresse oder eine IPv6-Adresse haben.

ONTAP ermöglicht die Migration Ihrer Peering-Netzwerke von IPv4 zu IPv6, indem optional beide Protokolle gleichzeitig auf den Intercluster-LIFs vorhanden sein können. In früheren Versionen waren alle Intercluster-Beziehungen eines gesamten Clusters entweder IPv4 oder IPv6. Dies bedeutete, dass ein Protokollwechsel potenziell zu Unterbrechungen führen konnte.

Port-Anforderungen

Sie können dedizierte Ports für die Intercluster-Verbindung verwenden oder Ports gemeinsam nutzen, die vom Datennetzwerk verwendet werden. Ports müssen die folgenden Anforderungen erfüllen:

- Alle Ports, die zur Kommunikation mit einem bestimmten Remote-Cluster verwendet werden, müssen sich im selben IPspace befinden.

  Sie können mehrere IPspaces verwenden, um mit mehreren Clustern ein Peering herzustellen. Eine paarweise vollständige Mesh-Konnektivität ist nur innerhalb eines IPspaces erforderlich.

- Die Broadcast-Domäne, die für die Intercluster-Verbindung verwendet wird, muss mindestens zwei Ports pro Knoten umfassen, damit die Intercluster-Verbindung von einem Port auf einen anderen umgeschaltet werden kann.

  Ports, die zu einer Broadcast-Domäne hinzugefügt werden, können physische Netzwerk-Ports, VLANs oder Schnittstellengruppen (ifgrps) sein.

- Alle Anschlüsse müssen verkabelt sein.
- Alle Ports müssen in einem einwandfreien Zustand sein.
- Die MTU-Einstellungen der Ports müssen einheitlich sein.

Firewall-Anforderungen

Ab ONTAP 9.10.1 sind Firewall-Richtlinien veraltet und vollständig durch LIF-Dienstrichtlinien

ersetzt. Weitere Informationen finden sich unter "Firewall-Richtlinien für LIFs konfigurieren".

Firewalls und die Intercluster-Firewall-Richtlinie müssen die folgenden Protokolle zulassen:

- Bidirektionaler ICMP-Verkehr
- Bidirektionaler initiierter TCP-Verkehr zu den IP-Adressen aller Intercluster-LIFs über die Ports 11104 und 11105
- Bidirektionales HTTPS zwischen den Intercluster-LIFs

  Obwohl HTTPS bei der Einrichtung des Cluster-Peerings über die CLI nicht erforderlich ist, ist HTTPS später erforderlich, wenn der System Manager zur Konfiguration des Datenschutzes verwendet wird.

Die Standard `intercluster`-Firewallrichtlinie erlaubt den Zugriff über das HTTPS-Protokoll und von allen IP-Adressen (0.0.0.0/0). Die Richtlinie kann bei Bedarf geändert oder ersetzt werden.

Cluster-Peer-Limits

Die unterstützte Anzahl von Cluster-Peers hängt von der ONTAP Version ab:

- ONTAP 9.14.1 und höher: Es werden bis zu 400 Cluster-Peers unterstützt.
- Frühere ONTAP Releases: Es werden bis zu 255 Cluster-Peers unterstützt.

```
[NOTE]
These values represent supported and validated limits. There is no
strictly enforced maximum cluster peer limit.
```

Gemeinsam genutzte oder dedizierte ONTAP Ports verwenden

Sie können dedizierte Ports für die Intercluster-Verbindung verwenden oder Ports gemeinsam nutzen, die vom Datennetzwerk verwendet werden. Bei der Entscheidung, ob Ports gemeinsam genutzt werden, sind die Netzwerkbandbreite, das Replikationsintervall und die Portverfügbarkeit zu berücksichtigen.

Ports können auf einem Peered-Cluster gemeinsam genutzt werden, während auf dem anderen dedizierte Ports verwendet werden.

Netzwerkbandbreite

Bei einem Hochgeschwindigkeitsnetzwerk wie beispielsweise 10 GbE steht möglicherweise genügend lokale LAN-Bandbreite zur Verfügung, um die Replikation über dieselben 10 GbE Ports durchzuführen, die auch für den Datenzugriff verwendet werden.

Auch dann sollte die verfügbare WAN-Bandbreite mit der LAN-Bandbreite verglichen werden. Liegt die verfügbare WAN-Bandbreite deutlich unter 10 GbE, kann der Einsatz dedizierter Ports erforderlich sein.

Eine Ausnahme von dieser Regel könnte bestehen, wenn alle oder viele Knoten im Cluster

Daten replizieren, in diesem Fall wird die Bandbreitennutzung typischerweise auf die Knoten verteilt.

Wenn Sie keine dedizierten Ports verwenden, sollte die maximale Übertragungseinheit (MTU) des Replikationsnetzwerks typischerweise der MTU des Datennetzwerks entsprechen.

Replikationsintervall

Wenn die Replikation außerhalb der Spitzenzeiten erfolgt, sollte es möglich sein, die Datenports auch ohne 10-GbE-LAN-Verbindung für die Replikation zu verwenden.

Erfolgt die Datenreplizierung während der regulären Geschäftszeiten, ist die Menge der zu replizierenden Daten sowie die Frage zu berücksichtigen, ob dafür so viel Bandbreite benötigt wird, dass es zu Konflikten mit den Datenprotokollen kommen könnte. Liegt die Netzwerkauslastung durch Datenprotokolle (SMB, NFS, iSCSI) über 50 %, empfiehlt sich die Nutzung dedizierter Ports für die Intercluster-Verbindung, um eine nicht beeinträchtigte Performance im Falle eines Knotenausfalls zu ermöglichen.

Portverfügbarkeit

Wenn Sie feststellen, dass der Replikationsverkehr den Datenverkehr beeinträchtigt, können Intercluster-LIFs auf einen beliebigen anderen Intercluster-fähigen gemeinsam genutzten Port auf demselben Knoten migriert werden.

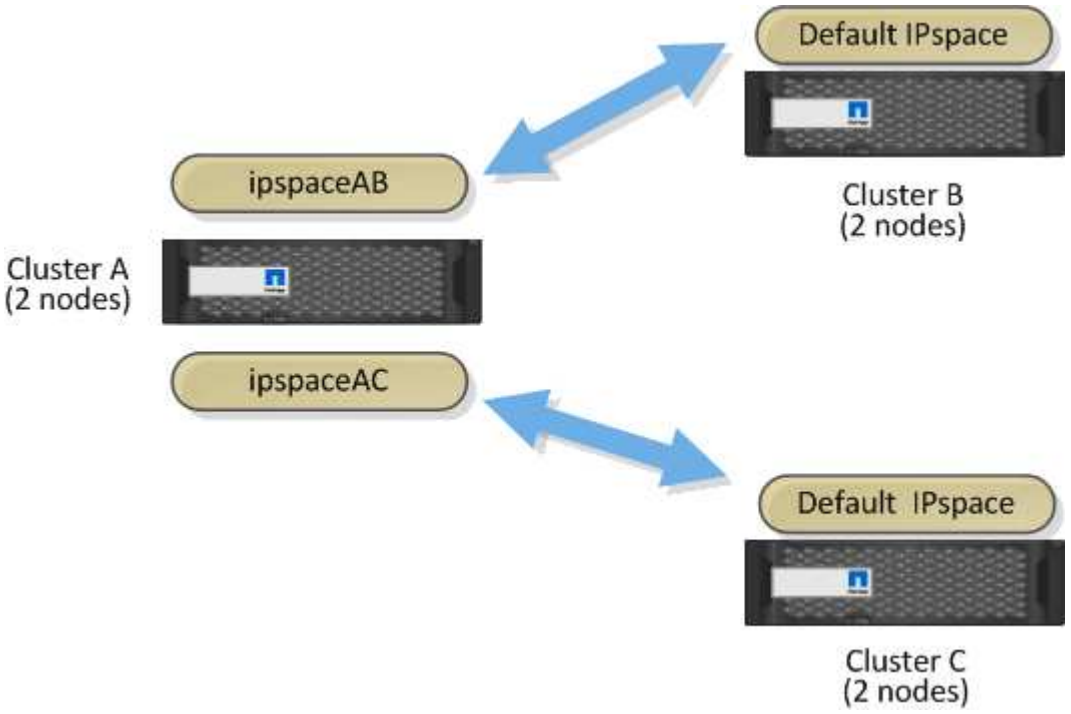
Sie können auch VLAN-Ports für die Replikation reservieren. Die Bandbreite des Ports wird zwischen allen VLANs und dem Basis-Port gemeinsam genutzt.

Benutzerdefinierte ONTAP IPspaces ermöglichen die Isolierung des Replikationsverkehrs.

Mithilfe benutzerdefinierter IPspaces lassen sich die Interaktionen eines Clusters mit seinen Peers trennen. Diese als *designated intercluster connectivity* bezeichnete Konfiguration ermöglicht es Dienstanbietern, den Replikationsverkehr in mandantenfähigen Umgebungen zu isolieren.

Angenommen, Sie möchten beispielsweise den Replikationsverkehr zwischen Cluster A und Cluster B vom Replikationsverkehr zwischen Cluster A und Cluster C trennen. Zu diesem Zweck können zwei IPspaces auf Cluster A erstellt werden.

Ein IPspace enthält die Intercluster-LIFs, die Sie zur Kommunikation mit Cluster B verwenden. Der andere enthält die Intercluster-LIFs, die Sie zur Kommunikation mit Cluster C verwenden, wie in der folgenden Abbildung zu sehen ist.



Verwandte Informationen

- "Informationen zur ONTAP IPspace Konfiguration"

Copyright-Informationen

Copyright © 2026 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGENDEINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter http://www.netapp.com/TM aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.