



クラスタと**SVM**のピアリングの準備

ONTAP 9

NetApp
February 12, 2026

目次

クラスタとSVMのピアリングの準備	1
ONTAPピアリングの基本	1
ONTAPピアリングの前提条件	1
接続要件	2
ポートの要件	2
ファイアウォールの要件	3
クラスタの要件	3
共有または専用のONTAPポートを使用する	3
ネットワーク帯域幅	3
レプリケーション間隔	4
ポートを使用可能か	4
カスタムONTAP IPspaceを使用してレプリケーショントラフィックを分離する	4

クラスタとSVMのピアリングの準備

ONTAPピアリングの基本

SnapMirrorを使用してスナップショットをレプリケートする前に、ソース クラスタとデスティネーション クラスタ間、およびソース SVM とデスティネーション SVM 間に_ピア関係_を作成する必要があります。ピア関係は、クラスタと SVM が安全にデータを交換できるようにするネットワーク接続を定義します。

ピア関係にあるクラスタとSVMは、_クラスタ間論理インターフェイス (LIF) _を使用してクラスタ間ネットワークを介して通信します。クラスタ間LIFは、「intercluster-core」ネットワーク・インターフェイス・サービスをサポートするLIFであり、通常は「default-intercluster」ネットワーク・インターフェイス・サービス・ポリシーを使用して作成されます。ピア関係にあるクラスタ内のすべてのノードにクラスタ間LIFを作成する必要があります。

クラスタ間LIFは、LIFが割り当てられているシステムSVMに属するルートを使用します。システムSVMは、クラスタレベルの通信用にIPspace内に自動的に作成されます。

ファンアウトとカスケードの両方のトポロジがサポートされます。カスケード トポロジの場合、クラスタ間ネットワークを作成する必要があるのは、プライマリ クラスタとセカンダリ クラスタの間、およびセカンダリ クラスタとターシャリ クラスタの間のみです。プライマリ クラスタとターシャリ クラスタの間にクラスタ間ネットワークを作成する必要はありません。

管理者は、default-interclusterサービス ポリシーからintercluster-coreサービスを削除することが可能です（ただし推奨されません）。この場合、「default-intercluster」を使用してLIFを作成しても、そのLIFはクラスタ間LIFにはなりません。default-interclusterサービス ポリシーにintercluster-coreサービスが含まれていることを確認するには、次のコマンドを使用します。

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



```
`network interface service-policy show`
```

の詳細については、[link:https://docs.netapp.com/us-en/ontap-cli/network-interface-service-policy-show.html](https://docs.netapp.com/us-en/ontap-cli/network-interface-service-policy-show.html) ["ONTAPコマンドリファレンス"^]を参照してください。

ONTAPピアリングの前提条件

クラスタ ピアリングを設定する前に、接続、ポート、IPアドレス、サブネット、ファイアウォール、およびクラスタの命名要件が下記の条件を満たしているか確認してください。



ONTAP 9.6以降では、クラスタ ピアリングで、データ レプリケーションに対するTLS 1.2 AES-256 GCM暗号化がデフォルトでサポートされます。デフォルトのセキュリティ暗号（「PSK-AES256-GCM-SHA384」）は、暗号化が無効になっていてもクラスタ ピアリングを機能させるために必要です。

ONTAP 9.11.1以降では、DHE-PSKセキュリティ暗号をデフォルトで使用できます。

ONTAP 9.15.1以降では、クラスタ ピアリングで、データ レプリケーションに対するTLS 1.3暗号化がデフォルトでサポートされます。

接続要件

ローカル クラスタのすべてのクラスタ間LIFが、リモート クラスタのすべてのクラスタ間LIFと通信可能であることが必要です。

必須ではありませんが、一般に、クラスタ間LIFには同じサブネットのIPアドレスを使用した方が構成がシンプルになります。使用するIPアドレスは、データLIFと同じサブネットのIPアドレスでも別のサブネットのIPアドレスでもかまいません。各クラスタで使用するサブネットは、次の要件を満たしている必要があります。

- サブネットがクラスタ間通信で使用するポートを含むブロードキャスト ドメインに属している。
- 1つのノードにつき1つのインタークラスタLIFが割り当てられるよう、サブネットに十分な数のIPアドレスを準備する。

たとえば、4ノード クラスタの場合、クラスタ間通信で使用するサブネットには使用可能なIPアドレスが4つ必要です。

クラスタ間ネットワークでは、ノードごとにインタークラスタLIFとIPアドレスが必要です。

クラスタ間LIFのアドレスにはIPv4またはIPv6のいずれかを使用できます。



ONTAPでは、必要に応じてIPv4プロトコルとIPv6プロトコルがクラスタ間LIFに共存することを許可し、IPv4からIPv6にピアリング ネットワークを移行できます。以前のリリースでは、クラスタ全体のすべてのクラスタ間関係がIPv4またはIPv6のどちらかだったため、プロトコルの変更はシステム停止を伴うイベントでした。

ポートの要件

クラスタ間通信には専用のポートを使用することも、データ ネットワークで使用しているポートを共有することもできます。ポートは、次の要件を満たしている必要があります。

- 特定のリモート クラスタとの通信に使用するすべてのポートのIPspaceが同じである。

複数のクラスタとのピア関係の作成には複数のIPspaceを使用できます。ペアワイズのフルメッシュ接続はIPspace内でのみ必要になります。

- クラスタ間通信で使用されるブロードキャスト ドメインに、1ノードあたり最低2つのポートがあり、クラスタ間通信で別のポートへのフェイルオーバーが可能になっている。

ブロードキャスト ドメインに追加できるポートは、物理ネットワーク ポート、VLAN、インターフェイスグループ (ifgrps) です。

- すべてのポートが接続されている。
- すべてのポートが健全な状態である。
- ポートのMTU設定が一貫している。

ファイアウォールの要件



ONTAP 9.10.1以降、ファイアウォールポリシーは廃止され、LIFサービスポリシーに完全に置き換えられました。詳細については、"[LIFのファイアウォールポリシーの設定](#)"を参照してください。

ファイアウォールとクラスタ間ファイアウォール ポリシーでは、以下のプロトコルを許可する必要があります。

- 双方向ICMPトラフィック
- 双方向で開始され、すべてのクラスタ間LIFのIPアドレスを宛先とし、ポート11104および11105経由のTCPトラフィック
- クラスタ間LIF間の双方向HTTPS

HTTPSはCLIを使用したクラスタ ピアリングのセットアップ時には必要ありませんが、System Managerを使用してデータ保護を設定する場合にはあとで必要になります。

デフォルトの `intercluster` ファイアウォール ポリシーでは、HTTPSプロトコルとすべてのIPアドレス (0.0.0.0/0) からのアクセスが許可されます。必要に応じてポリシーを変更または置き換えることができます。

クラスタの要件

クラスタは、次の要件を満たす必要があります。

- 1つのクラスタに対してピア関係を設定できるクラスタは最大255個である。

共有または専用のONTAPポートを使用する

クラスタ間通信専用のポートを使用することも、データネットワークで使用するポートを共有することもできます。ポートを共有するかどうかを決定する際には、ネットワーク帯域幅、レプリケーション間隔、およびポートの可用性を考慮する必要があります。



一方のピア クラスタでポートを共有し、もう一方のクラスタでは専用ポートを使用することができます。

ネットワーク帯域幅

高速ネットワーク (10GbEなど) を採用している場合、データ アクセスに使用されるものと同じ10GbEポートでレプリケーションを実行しても、ローカルLANの帯域幅が不足することはあまりありません。

それでも、利用可能なWAN帯域幅とLAN帯域幅を比較する必要があります。利用可能なWAN帯域幅が10 GbEを大幅に下回る場合は、専用ポートの使用が必要になる可能性があります。



このルールの唯一の例外は、クラスタ内のすべてのノードまたは多くのノードがデータをレプリケートする場合です。この場合、帯域幅の使用率は通常、ノード間で分散されます。

専用ポートを使用していない場合は、通常、レプリケーション ネットワークの最大転送単位 (MTU) サイズは、データ ネットワークのMTUサイズと同じになります。

レプリケーション間隔

レプリケーションがオフピーク時に行われる場合、10GbE LAN接続がなくてもレプリケーションにデータ ポートを使用できるはずですが。

通常の営業時間中にレプリケーションを行う場合は、レプリケーションされるデータの量と、データプロトコルとの競争を引き起こすほどの帯域幅が必要かどうかを考慮する必要があります。データプロトコル (SMB、NFS、iSCSI) によるネットワーク使用率が50%を超える場合は、ノードフェイルオーバーが発生してもパフォーマンスが低下しないように、クラスタ間通信に専用ポートを使用する必要があります。

ポートを使用可能か

レプリケーショントラフィックがデータトラフィックに干渉していると判断した場合は、クラスタ間LIFを同じノード上の他のクラスタ間対応共有ポートに移行できます。

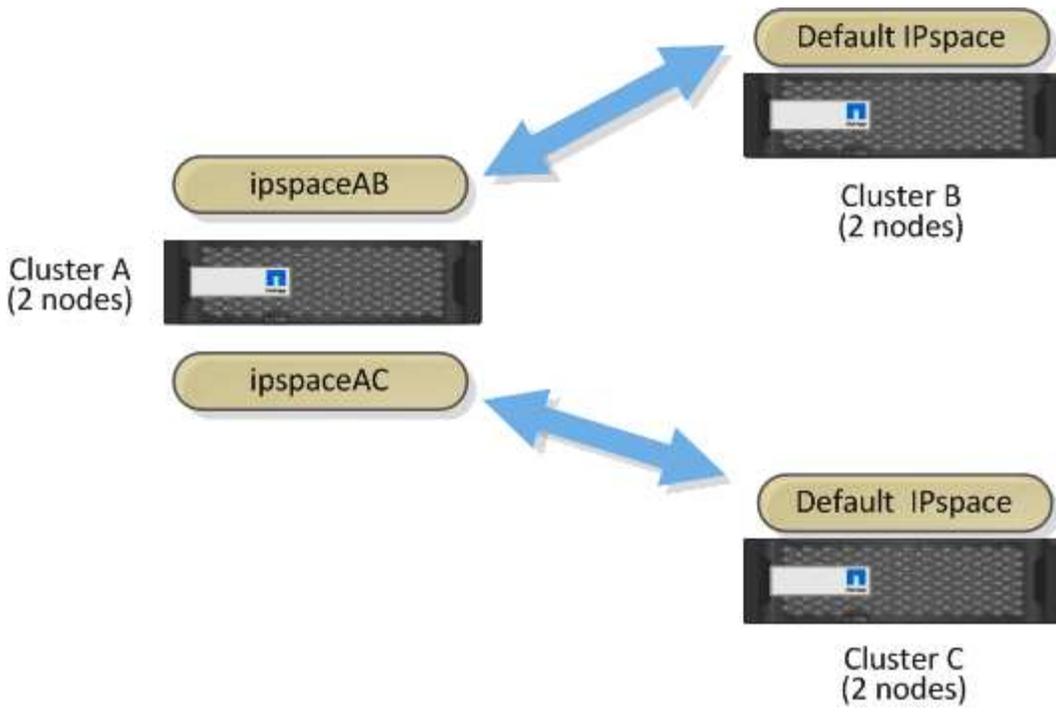
VLANポートをレプリケーション専用にすることもできます。ポートの帯域幅は、すべてのVLANとベースポートで共有されます。

カスタムONTAP IPspaceを使用してレプリケーショントラフィックを分離する

カスタムIPspaceを使用することで、クラスタとピア間の通信を分離できます。この構成は「指定クラスタ間接続」と呼ばれ、サービスプロバイダーはマルチテナント環境におけるレプリケーショントラフィックを分離できます。

たとえば、クラスタAとクラスタBの間のレプリケーショントラフィックをクラスタAとクラスタCの間のレプリケーショントラフィックから切り離すためには、クラスタAにIPspaceを2つ作成します。

次の図に示すように、一方のIPspaceにはクラスタBとの通信に使用するクラスタ間LIFを、もう一方のIPspaceにはクラスタCとの通信に使用するクラスタ間LIFを含めます。



関連情報

- ["ONTAP IPspace構成について学ぶ"](#)

著作権に関する情報

Copyright © 2026 NetApp, Inc. All Rights Reserved. Printed in the U.S.このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

ネットアップの著作物から派生したソフトウェアは、次に示す使用許諾条項および免責条項の対象となります。

このソフトウェアは、ネットアップによって「現状のまま」提供されています。ネットアップは明示的な保証、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないいかなる暗示的な保証も行いません。ネットアップは、代替品または代替サービスの調達、使用不能、データ損失、利益損失、業務中断を含み、かつこれに限定されない、このソフトウェアの使用により生じたすべての直接的損害、間接的損害、偶発的損害、特別損害、懲罰的損害、必然的損害の発生に対して、損失の発生の可能性が通知されていたとしても、その発生理由、根拠とする責任論、契約の有無、厳格責任、不法行為（過失またはそうでない場合を含む）にかかわらず、一切の責任を負いません。

ネットアップは、ここに記載されているすべての製品に対する変更を随時、予告なく行う権利を保有します。ネットアップによる明示的な書面による合意がある場合を除き、ここに記載されている製品の使用により生じる責任および義務に対して、ネットアップは責任を負いません。この製品の使用または購入は、ネットアップの特許権、商標権、または他の知的所有権に基づくライセンスの供与とはみなされません。

このマニュアルに記載されている製品は、1つ以上の米国特許、その他の国の特許、および出願中の特許によって保護されている場合があります。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7013（2014年2月）およびFAR 5252.227-19（2007年12月）のRights in Technical Data -Noncommercial Items（技術データ - 非商用品目に関する諸権利）条項の(b)(3)項、に規定された制限が適用されます。

本書に含まれるデータは商用製品および/または商用サービス（FAR 2.101の定義に基づく）に関係し、データの所有権はNetApp, Inc.にあります。本契約に基づき提供されるすべてのネットアップの技術データおよびコンピュータソフトウェアは、商用目的であり、私費のみで開発されたものです。米国政府は本データに対し、非独占的かつ移転およびサブライセンス不可で、全世界を対象とする取り消し不能の制限付き使用权を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc.の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用权については、DFARS 252.227-7015(b)項（2014年2月）で定められた権利のみが認められます。

商標に関する情報

NetApp、NetAppのロゴ、<http://www.netapp.com/TM>に記載されているマークは、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。