ネットワーク管理
ONTAP 9

NetApp
February 12, 2026

目次

ネットワーク管理

始めましょう

System Manager を使用して ONTAP ネットワークを視覚化する

ONTAP 9.8以降では、System Managerを使用してネットワークのコンポーネントと構成を図で表示し、ホスト、ポート、SVM、ボリュームなどのネットワーク接続パスを確認できます。ONTAP 9.12.1以降では、[Network Interfaces]グリッドにLIFとサブネットの関連付けを表示できます。

グラフィックは、ネットワーク > 概要 を選択するか、ダッシュボードの ネットワーク セクションから → を選択すると表示されます。

図には次のカテゴリのコンポーネントが表示されます。

- ホスト
- ストレージ ポート
- ネットワーク インターフェイス
- Storage VM
- データ アクセス コンポーネント

各セクションでは、カーソルを合わせて詳細情報を表示したり、ネットワークの管理タスクや設定タスクを実行したりすることができます。

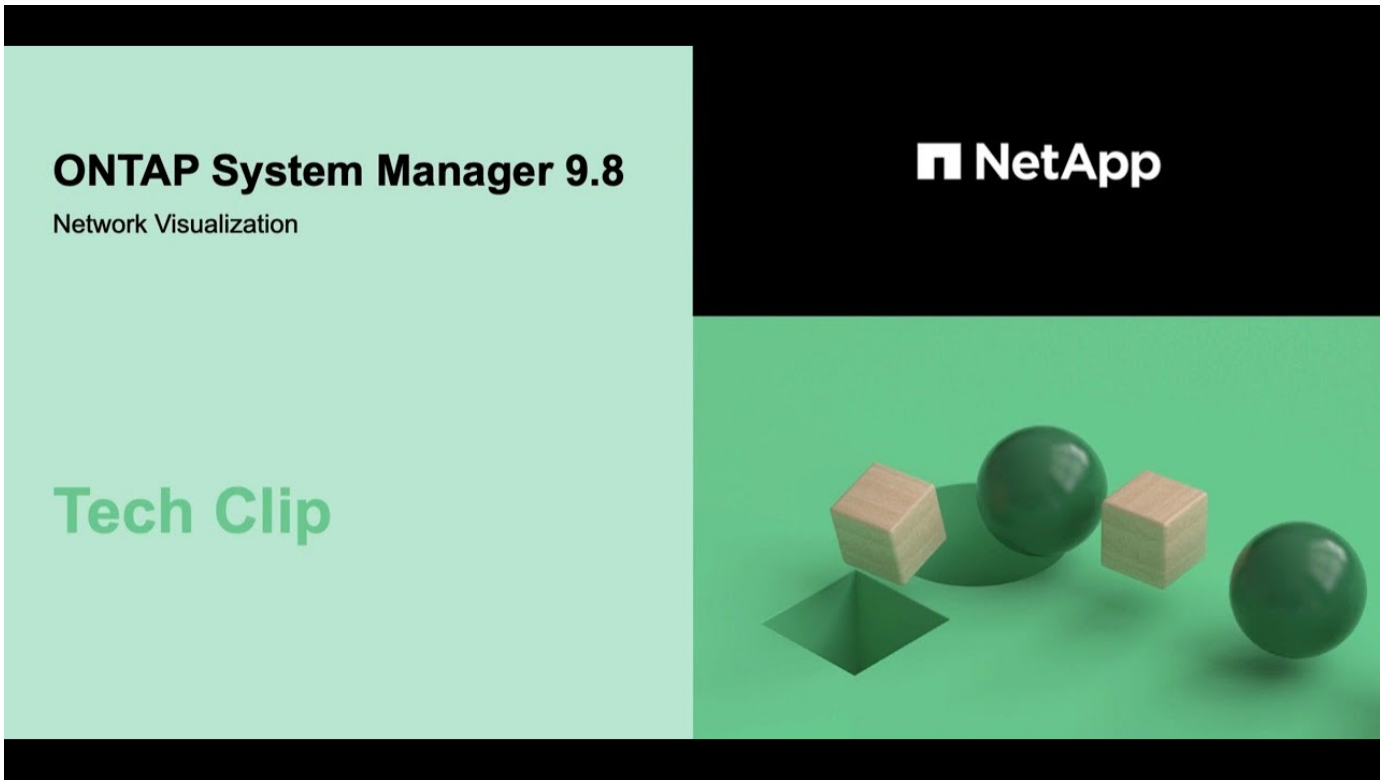
従来の System Manager（ONTAP 9.7 以前でのみ使用可能）を使用している場合は、"ネットワークの管理"を参照してください。

例

この図をさまざまに操作して、各コンポーネントの詳細を表示したり、ネットワークの管理操作を実行したりすることができます。以下はその一例です。

- ホストをクリックすると、その構成（関連付けられているポート、ネットワーク インターフェイス、ストレージVM、データ アクセス コンポーネント）が表示されます。
- Storage VM内のボリューム数にカーソルを合わせて、詳細を表示するボリュームを選択する。
- iSCSIインターフェイスを選択して、過去1週間のパフォーマンスを表示する。
- ⋮ をクリックすると、そのコンポーネントを変更するアクションが開始されます。
- 健全でないコンポーネントの横に表示される「X」から、ネットワークのどこで問題が発生しているかをすばやく突き止める。

System Managerのネットワーク可視化機能に関するビデオ



ONTAPクラスタのネットワークコンポーネントについて学習します

クラスタをセットアップする前に、クラスタのネットワーク コンポーネントについて理解しておく必要があります。クラスタの物理ネットワーク コンポーネントを論理コンポーネントに設定することで、ONTAPの持つ柔軟性とマルチテナンシー機能を活かせます。

次に、クラスタのさまざまなネットワーク コンポーネントについて説明します。

- 物理ポート

  ネットワーク インターフェイス カード（NIC）とホスト バス アダプタ（HBA）は、各ノードから物理ネットワーク（管理ネットワークとデータ ネットワーク）への物理接続（イーサネットおよびFibre Channel）を提供します。

  サイト要件、スイッチ情報、ポートケーブル情報、およびコントローラのオンボードポートケーブル接続については、Hardware Universe（ "hwu.netapp.com"）を参照してください。

- 論理ポート

  論理ポートは仮想ローカル エリア ネットワーク（VLAN）とインターフェイス グループで構成されます。インターフェイス グループは複数の物理ポートを1つのポートとして扱い、VLANは1つの物理ポートを複数の異なるポートに分割します。

- IPspace

  IPspaceを使用すると、クラスタ内のSVMごとに個別のIPアドレス スペースを作成できます。これにより、管理上分離されたネットワーク ドメインのクライアントが、IPアドレスの同じサブネット範囲内の重複したIPアドレスを使用してクラスタのデータにアクセスできるようになります。

- ブロードキャスト ドメイン

  ブロードキャスト ドメインはIPspace内に存在し、同じレイヤ2ネットワークに属する、クラスタ内の多数のノードからのネットワーク ポート グループを含んでいます。このグループのポートは、SVMでデータ トラフィック用に使用されます。

- サブネット

  サブネットはブロードキャスト ドメイン内に作成され、同じレイヤ3サブネットに属するIPアドレスのプールを含んでいます。このIPアドレス プールにより、LIF作成時にIPアドレスが簡単に割り当てられるようになります。

- 論理インターフェイス

  論理インターフェイス（LIF）は、ポートに関連付けられたIPアドレスまたはワールドワイド ポート名（WWPN）です。フェイルオーバー グループ、フェイルオーバー ルール、ファイアウォール ルールなどの属性があります。LIFは、現在バインドされているポート（物理または論理）からネットワーク経由で通信します。

  クラスタ内のLIFのタイプには、データLIF、クラスタ対象管理LIF、ノード対象管理LIF、クラスタ間LIF、クラスタLIFがあります。LIFの所有権は、LIFを実装するSVMによって異なります。データLIFはデータSVMによって、ノード対象管理LIF、クラスタ対象管理LIF、およびクラスタ間LIFは管理SVMによって、クラスタLIFはクラスタSVMによって所有されます。

- DNSゾーン

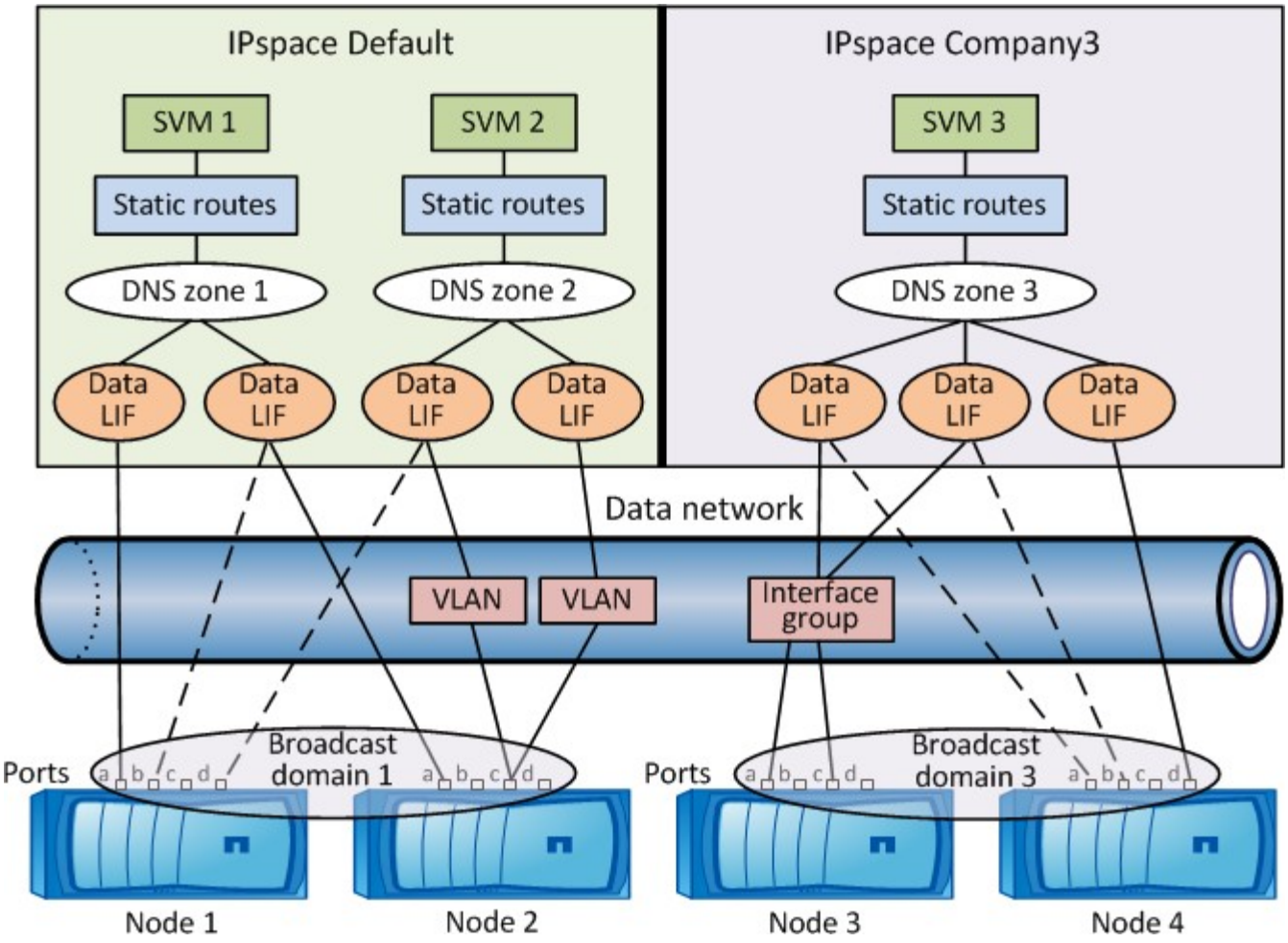
  DNSゾーンはLIFの作成時に指定でき、クラスタのDNSサーバ経由でエクスポートされるLIFの名前を提供します。複数のLIFで同じ名前を共有できるため、DNSロード バランシング機能を使用し、その名前のIPアドレスを負荷に従って分散させることができます。

  SVMには、複数のDNSゾーンを設定できます。

- ルーティング

  それぞれのSVMは、ネットワーク上で完全な機能を持つ独立した存在です。SVMは、LIFおよび設定済みの外部サーバに到達可能なルートを持っています。

  次の図は、4ノード クラスタにおける各種ネットワーク コンポーネントの関係を示しています。

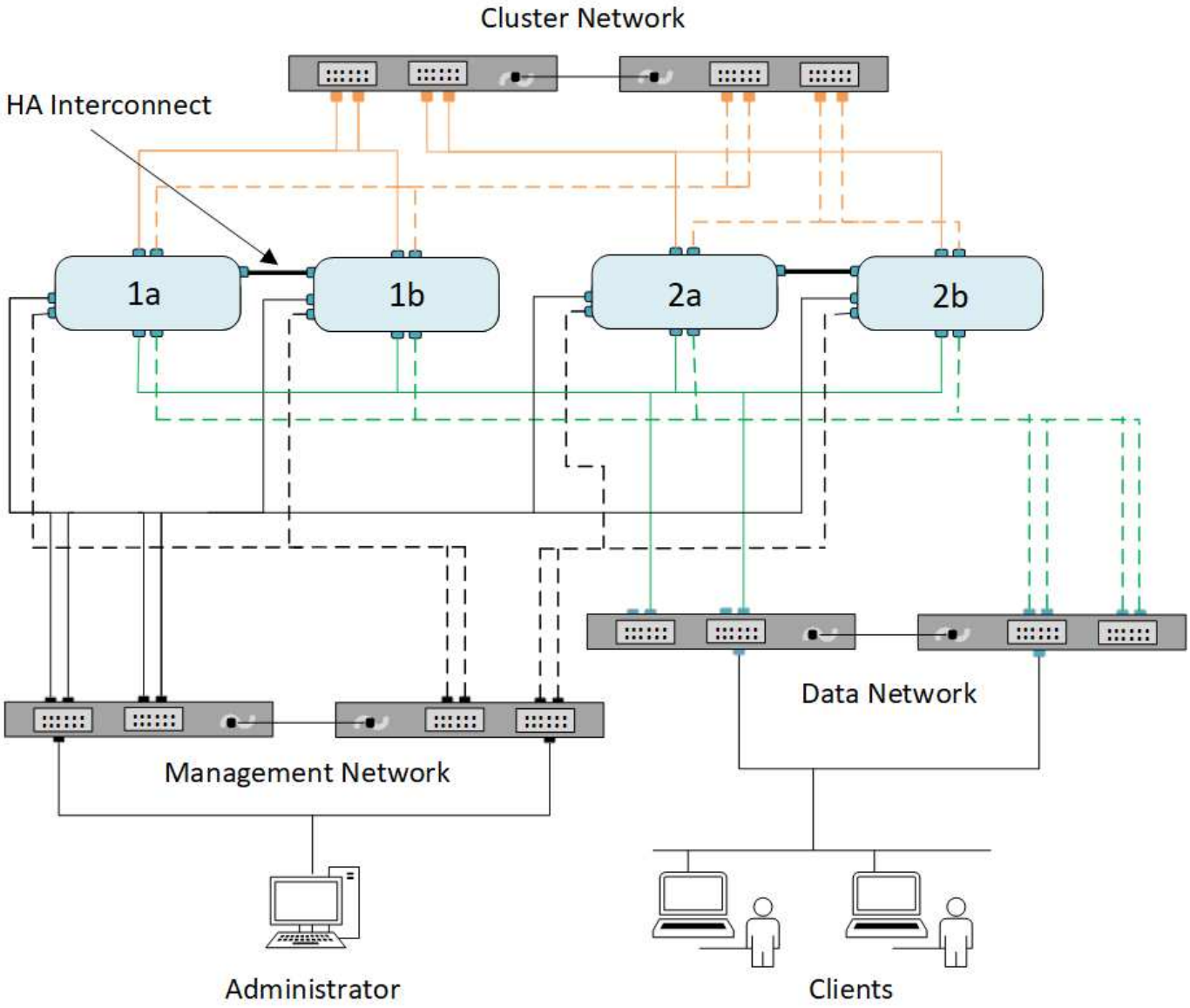


ONTAPネットワークケーブル配線のベストプラクティス

ネットワークのケーブル配線のベストプラクティスは、トラフィックをクラスタ、管理、データの各ネットワークに分離することです。

クラスタをケーブル配線するときは、クラスタのトラフィックが他のすべてのトラフィックとは別のネットワーク上にあるようにします。必須ではありませんが、ネットワーク管理トラフィックを、データとクラスタ内のトラフィックと分離することを推奨します。このようにネットワークを分離することにより、パフォーマンスとセキュリティが向上して管理しやすくなるだけでなく、ノードへの管理アクセスも簡単になります。

次の図は、3つのネットワークがある4ノードHAクラスタのネットワーク ケーブル配線を示しています。



ネットワークのケーブル配線を行うときは、次のガイドラインに従ってください。

- 各ノードを次の3つのネットワークに接続する必要があります。

  管理用、データ アクセス用、クラスタ内通信用のネットワークです。管理ネットワークとデータ ネットワークは論理的に分離できます。

- クライアント（データ）トラフィックのフローを改善するには、各ノードへのデータ ネットワーク接続を複数用意します。
- クラスタはデータ ネットワーク接続がなくても作成できますが、クラスタ インターコネクト接続は必須です。
- 各ノードへのクラスタ接続が常に2つ以上必要です。

ネットワークケーブル接続の詳細については、 "AFFおよびFASシステムドキュメントセンター"および"Hardware Universe"を参照してください。

ONTAPネットワークで使用するLIFフェイルオーバーポリシーを決定する

ブロードキャスト ドメイン、フェイルオーバー グループ、およびフェイルオーバー ポリシーの3つを組み合わせることで、LIFが設定されたノードまたはポートに障害が発生した場合にどのポートがテイクオーバーするかが決まります。

ブロードキャスト ドメインは、同じレイヤ2のイーサネット ネットワーク内にある到達可能なすべてのポートをリストします。いずれかのポートから送信されたイーサネット ブロードキャスト パケットは、ブロードキャスト ドメイン内の他のすべてのポートで認識されます。ブロードキャスト ドメインのこの特性はLIFにとって重要で、LIFがブロードキャスト ドメイン内の他のどのポートにフェイルオーバーしても、元のポートから到達できたすべてのローカル ホストとリモート ホストに引き続き到達できることを意味します。

フェイルオーバー グループは、相互にLIFフェイルオーバーが可能なブロードキャスト ドメイン内のポートを定義します。各ブロードキャスト ドメインには、すべてのポートを含むフェイルオーバー グループが1つあります。このフェイルオーバー グループは、LIF用に推奨されるデフォルトのフェイルオーバー グループです。ブロードキャスト ドメイン内の同じリンク速度のポートで構成されるフェイルオーバー グループなど、より限定的なフェイルオーバー グループも作成できます。

フェイルオーバー ポリシーは、ノードまたはポートが停止したときにLIFがフェイルオーバー グループのポートをどのように使用するかを規定します。フェイルオーバー グループに適用されるフィルタの一種と考えることができます。LIFのフェイルオーバー ターゲット（LIFがフェイルオーバーできるポートのセット）は、LIFのフェイルオーバー ポリシーをブロードキャスト ドメイン内のLIFのフェイルオーバー グループに適用することで決まります。

LIFのフェイルオーバー ターゲットは、次のCLIコマンドを使用して表示できます。

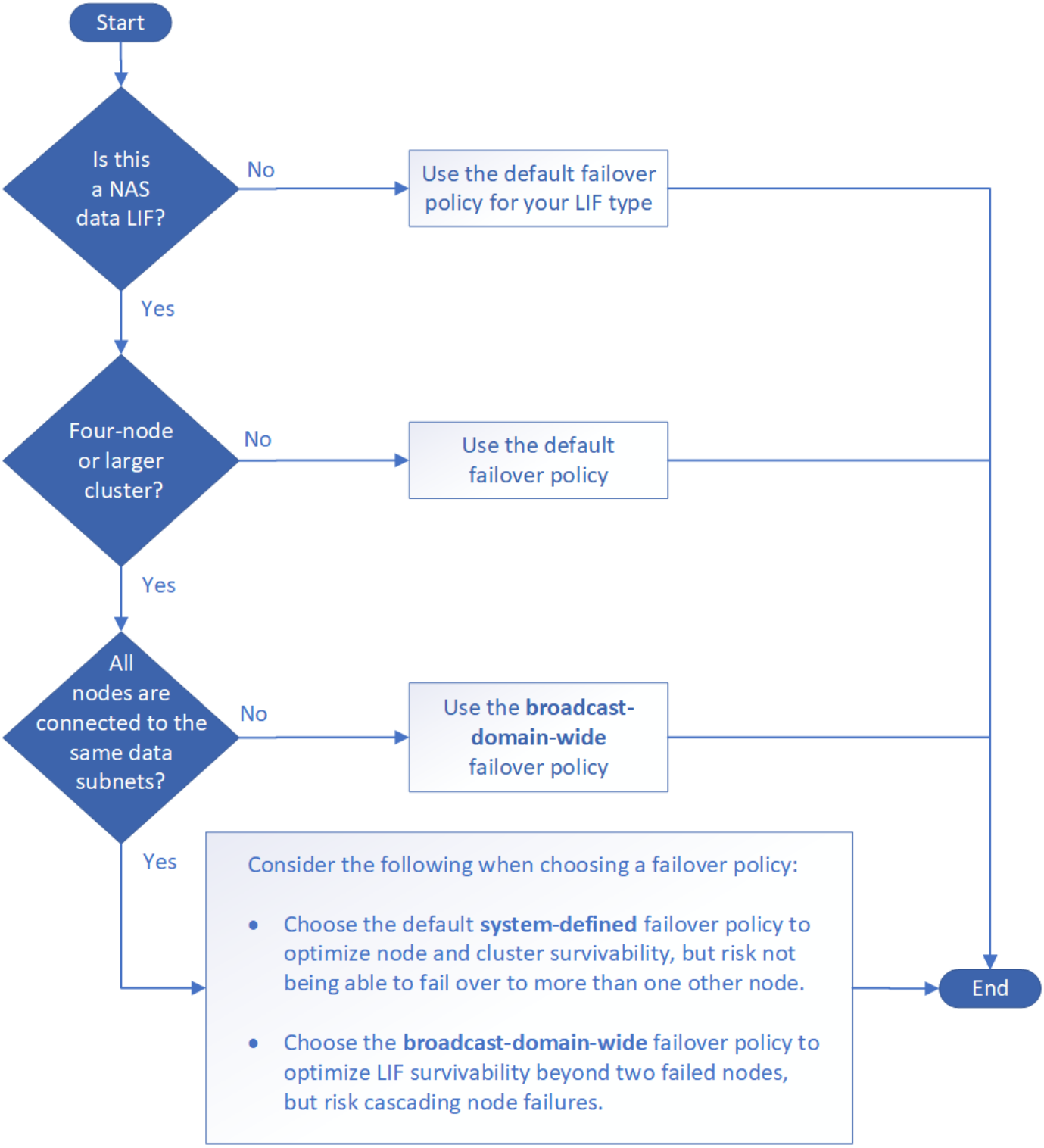
```
network interface show -failover
```

LIFのタイプに応じたデフォルトのフェイルオーバー ポリシーを使用することを強く推奨します。

使用するLIFフェイルオーバー ポリシーの決定

推奨されるデフォルトのフェイルオーバー ポリシーを使用するか、LIFのタイプと環境に基づいて変更するかを決定します。

フェイルオーバー ポリシーのデシジョン ツリー



LIFタイプ別のデフォルトのフェイルオーバー ポリシー

LIFタイプ	デフォルトのフェイルオーバー ポリシー	概要
BGPのLIF	無効	別のポートにフェイルオーバーしません。
クラスタLIF	local-only	同じノードのポートにのみフェイルオーバーします。

クラスタ管理LIF	broadcast-domain-wide	クラスタ内のすべてのノードの、同じブロードキャスト ドメイン内のポートにフェイルオーバーします。
クラスタ間LIF	local-only	同じノードのポートにのみフェイルオーバーします。
NASデータLIF	system-defined	HAパートナーでない他のいずれかのノードにフェイルオーバーします。
ノード管理LIF	local-only	同じノードのポートにのみフェイルオーバーします。
SANデータLIF	無効	別のポートにフェイルオーバーしません。

「sfo-partner-only」フェイルオーバー ポリシーはデフォルトではありませんが、LIFをホーム ノードまたはSFOパートナー上のポートのみにフェイルオーバーする場合に使用できます。

関連情報

- "network interface show"

NAS パス フェイルオーバー ワークフロー

ONTAPネットワーク上でNASパスフェイルオーバーを構成する

ネットワークの基本概念をすでに理解している場合は、NASパスのフェイルオーバー設定に関するこの「ハンズオン」ワークフローを確認することで、ネットワークの設定にかかる時間を節約できます。

ONTAP 9.7以前のバージョンでは、NASパスフェイルオーバーの設定ワークフローが異なります。ONTAP 9.7以前のバージョンを実行しているネットワークでNASフェイルオーバーを設定する必要がある場合は、ワークフロー"NASパスのフェイルオーバー ワークフロー（ONTAP 9.7以前）"を参照してください。

NAS LIFは、現在のポートでリンク障害が発生すると、稼働しているネットワーク ポートに自動的に移行します。ONTAPのデフォルトを利用してパスのフェイルオーバーを管理できます。

SAN LIFは移行されません（リンク障害発生後に手動で移動しない限り）。代わりに、ホストのマルチパス技術によってトラフィックが別のLIFに転送されます。詳細については、"SAN管理"を参照してください。

1 "ワークシートへの記入"

ワークシートを使用して、NASパスのフェイルオーバーの計画を立てます。

2 "IPspaceの作成"

クラスタ内のSVMごとに個別のIPアドレス スペースを作成します。

3 "IPspaceへのブロードキャスト ドメインの移動"

IPspaceにブロードキャスト ドメインを移動します。

4 **"SVMの作成"**

クライアントにデータを提供するSVMを作成します。

5 **"LIFの作成"**

データへのアクセスに使用するポートにLIFを作成します。

6 **"SVM用のDNSサービスの設定"**

NFS または SMB サーバーを作成する前に、SVM の DNS サービスを設定します。

ONTAPネットワーク上のNASパスフェイルオーバーのワークシート

NASパスのフェイルオーバーを設定する前に、ワークシートのすべてのセクションに記入しておく必要があります。

ONTAPネットワークにおけるNASフェイルオーバーに関する情報は、ONTAP 9.7以前のバージョンでは異なります。ONTAP 9.7以前のバージョンを実行しているネットワークでNASフェイルオーバーを設定する必要がある場合は、"NASパスのフェイルオーバー設定のワークシート（ONTAP 9.7以前）"を参照してください。

IPspace設定

IPspaceを使用すると、クラスタ内のSVMごとに個別のIPアドレス スペースを作成できます。これにより、管理上分離されたネットワーク ドメインのクライアントが、IPアドレスの同じサブネット範囲内の重複したIPアドレスを使用してクラスタのデータにアクセスできるようになります。

情報	必須？	値
IPspace 名 IPspace の一意の識別子。	はい	

ブロードキャスト ドメイン設定

ブロードキャスト ドメインは、同じレイヤ2ネットワークに属するポートをグループ化し、そのブロードキャスト ドメイン ポートにMTUを設定します。

ブロードキャスト ドメインは、IPspaceに割り当てられます。1つのIPspaceに複数のブロードキャスト ドメインを配置できます。

LIFのフェイルオーバー先のポートは、LIFのフェイルオーバー グループのメンバーである必要があります。ONTAPで作成されたブロードキャスト ドメインごとに同じ名前のフェイルオーバー グループが作成され、そのグループにブロードキャスト ドメインのすべてのポートが追加されます。

情報	必須？	値

IPspace 名 ブロードキャスト ドメインが割り当てられている IPspace。 既存のIPspaceを指定する必要があります。	はい	
ブロードキャスト ドメイン名：ブロードキャスト ドメインの名前。 この名前はIPspace内で一意である必要があります。	はい	
MTU ブロードキャスト ドメインの最大転送単位値。通常は **1500** または **9000** に設定されます。 MTU値は、ブロードキャスト ドメインのすべてのポートと、以降ブロードキャスト ドメインに追加されるすべてのポートに適用されます。 MTU値は、ネットワークに接続されているすべてのデバイスで同じである必要があります。管理トラフィックやサービス プロセッサのトラフィックを処理するe0Mポートについては、MTUを1500バイト以下に設定する必要があります。	はい	
ポート ポートは到達可能性に基づいてブロードキャストドメインに割り当てられます。ポートの割り当てが完了したら、 `network port reachability show`コマンドを実行して到達可能性を確認してください。 物理ポート、VLAN、またはインターフェイスグループを使用できます。 `network port reachability show`の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/network-port-reachability-show.html["ONTAPコマンドリファレンス"^]を参照してください。	はい	

サブネット構成

サブネットにはIPアドレスのプールとデフォルト ゲートウェイが1つ含まれ、IPspace内に配置されたSVMで使用するLIFに割り当てることができます。

- SVM上でLIFを作成する際には、IPアドレスとサブネットを指定する代わりにサブネット名を指定できま

す。

- サブネットはデフォルト ゲートウェイと一緒に設定できるため、SVMを作成する際に別途デフォルト ゲートウェイを作成する必要はありません。
- ブロードキャスト ドメインには、1つまたは複数のサブネットを含めることができます。
- 複数のサブネットをIPspaceのブロードキャスト ドメインと関連付けることによって、別のサブネット上にあるSVM LIFを設定できます。
- 各サブネットには、同じIPspace内の別のサブネットに割り当てられたIPアドレスと重複しないIPアドレスを含める必要があります。
- サブネットを使用する代わりに、SVMデータLIFに特定のIPアドレスを割り当ててSVM用のデフォルト ゲートウェイを作成することができます。

情報	必須？	値
IPspace 名 サブネットが割り当てられるIPspace。 既存のIPspaceを指定する必要があります。	はい	
サブネット名：サブネットの名前。 この名前はIPspace内で一意である必要があります。	はい	
ブロードキャスト ドメイン名 サブネットが割り当てられるブロードキャスト ドメイン。 指定したIPspaceに存在するブロードキャスト ドメインを指定する必要があります。	はい	
サブネット名とマスク IP アドレスが存在するサブネットとマスク。	はい	
ゲートウェイ サブネットのデフォルトゲートウェイを指定できます。 ゲートウェイはサブネットを作成する際に割り当てなくても、あとで割り当てることができます。	いいえ	

IP アドレスの範囲 IP アドレスの範囲または特定の IP アドレスを指定できます。 たとえば、次のような範囲を指定できます。 `192.168.1.1-192.168.1.100, 192.168.1.112, 192.168.1.145` IPアドレスの範囲を指定しない場合、指定したサブネット内のすべての範囲のIPアドレスがLIFに割り当て可能になります。	いいえ	
LIF 関連付けの強制更新既存の LIF 関連付けの更新を強制するかどうかを指定します。 デフォルトでは、サービス プロセッサ インターフェイスやネットワーク インターフェイスが指定された範囲のIPアドレスを使用している場合、サブネットの作成は失敗します。 このパラメータを使用すると、手動でアドレスを指定したすべてのインターフェイスがサブネットに関連付けられ、コマンドが成功します。	いいえ	

SVM構成

SVMを使用して、クライアントやホストにデータを提供します。

記録する値は、デフォルトのデータSVMを作成するためのものです。MetroClusterソースSVMを作成する場合は、"ファブリック接続のMetroClusterインストールおよび構成ガイド"または"Stretch MetroClusterのインストールと構成ガイド"を参照してください。

情報	必須？	値
SVM名 SVMの完全修飾ドメイン名（FQDN）。この名前はクラスタリーグ全体で一意である必要があります。	はい	
ルート ボリューム名 SVM ルート ボリュームの名前。	はい	
アグリゲート名 SVMルートボリュームを保持するアグリゲートの名前。このアグリゲートは存在している必要があります。	はい	
セキュリティ形式 SVM ルートボリュームのセキュリティ形式。指定できる値は **ntfs**、**unix**、**mixed** です。	はい	
IPspace名 SVMが割り当てられているIPspace。このIPspaceは存在している必要があります。	いいえ	

SVM言語設定 SVMとそのボリュームで使用するデフォルトの言語です。デフォルト言語を指定しない場合、デフォルトのSVM言語は*C.UTF-8*に設定されます。SVM言語設定は、SVM内のすべてのNASボリュームのファイル名とデータの表示に使用される文字セットを決定します。SVMの作成後に言語を変更できます。	いいえ	

LIFの構成

SVMは、1つ以上のネットワーク論理インターフェイス（LIF）を通じてクライアントとホストにデータを提供します。

情報	必須？	値
SVM 名 LIF の SVM の名前。	はい	
LIF名 LIFの名前。ノードごとに複数のデータLIFを割り当てることができます。また、ノードに使用可能なデータポートがあれば、クラスタ内の任意のノードにLIFを割り当てることができます。冗長性を確保するには、各データサブネットに少なくとも2つのデータLIFを作成し、特定のサブネットに割り当てられたLIFには、異なるノードのホームポートを割り当てる必要があります。**Important**： ノンストップオペレーションソリューションのためにSMB経由でHyper-VまたはSQL ServerをホストするようにSMBサーバを構成する場合、SVMにはクラスタ内のすべてのノードに少なくとも1つのデータLIFが必要です。	はい	
サービスポリシー LIF のサービスポリシー。サービスポリシーは、LIF を使用できるネットワークサービスを定義します。データ SVM とシステム SVM の両方で、データと管理トラフィックを管理するための組み込みサービスとサービスポリシーが利用できます。	はい	
許可されるプロトコル IPベースのLIFでは許可されるプロトコルを指定する必要はありません。代わりにサービスポリシーの行を使用してください。FibreChannelポート上のSAN LIFに許可されるプロトコルを指定します。これらは、そのLIFを使用できるプロトコルです。LIFの作成後は、LIFを使用するプロトコルを変更できません。LIFを設定する際には、すべてのプロトコルを指定する必要があります。	いいえ	
ホームノード LIFがホームポートに戻されたときに、LIFが戻るノード。データLIFごとにホームノードを記録する必要があります。	はい	

Home portまたはブロードキャストドメイン 次のいずれかを選択します：ポート：LIFがホームポートに戻された際に論理インターフェースが戻るポートを指定します。これはIPspaceのサブネット内の最初のLIFに対してのみ実行され、それ以外の場合は必須ではありません。ブロードキャストドメイン：ブロードキャストドメインを指定すると、LIFがホームポートに戻された際に論理インターフェースが戻る適切なポートがシステムによって選択されます。	はい	
サブネット名 SVM に割り当てるサブネット。アプリケーションサーバへの継続的な可用性を備えた SMB 接続を作成するために使用されるすべてのデータ LIF は、同じサブネット上に存在する必要があります。	○（サブネットを使用する場合）	

DNS設定

NFSまたはSMBサーバを作成する前に、SVMでDNSを設定する必要があります。

情報	必須？	値
SVM 名 NFS または SMB サーバーを作成する SVM の名前。	はい	
DNSドメイン名 ホストからIPアドレスへの名前解決を行う際にホスト名に追加するドメイン名のリスト。最初にローカルドメインをリストし、次にDNSクエリが最も頻繁に実行されるドメイン名をリストします。	はい	

DNS サーバの IP アドレス NFS または SMB サーバの名前解決を提供する DNS サーバの IP アドレスのリスト。リストされた DNS サーバには、SMB サーバが参加するドメインの Active Directory LDAP サーバおよびドメイン コントローラを見つけるために必要なサービス ロケーション レコード（SRV）が含まれている必要があります。SRV レコードは、サービスの名前を、そのサービスを提供するサーバの DNS コンピュータ名にマッピングするために使用されます。ONTAP がローカル DNS クエリを通じてサービス ロケーション レコードを取得できない場合、SMB サーバの作成は失敗します。ONTAP が Active Directory SRV レコードを見つけられるようにする最も簡単な方法は、Active Directory 統合 DNS サーバを SVM DNS サーバとして設定することです。DNS 管理者が Active Directory ドメイン コントローラに関する情報を含む DNS ゾーンに SRV レコードを手動で追加している場合は、Active Directory 非統合 DNS サーバを使用できます。Active Directory 統合 SRV レコードの詳細については、"Microsoft TechNet での Active Directory の DNS サポートの仕組み"のトピックを参照してください。	はい	

動的**DNS**設定

動的DNSを使用して自動的にActive Directory統合DNSサーバにDNSエントリを追加する前に、SVMに動的DNS（DDNS）を設定する必要があります。

SVM上にあるすべてのデータLIFについてDNSレコードが作成されます。SVM上に複数のデータLIFを作成することによって、割り当てられたデータIPアドレスへのクライアント接続の負荷を分散することができます。DNSは、そのホスト名を使用して、割り当てられたIPアドレスへの接続をラウンドロビン方式で確立することで、接続の負荷を分散します。

情報	必須？	値
SVM 名 NFS または SMB サーバーを作成する SVM。	はい	
DDNSを使用するかどうか DDNSを使用するかどうかを指定します。SVMに設定されているDNSサーバはDDNSをサポートしている必要があります。デフォルトではDDNSは無効になっています。	はい	

セキュアDDNSを使用するかどうか。セキュアDDNSは、Active Directory統合DNSでのみサポートされます。Active Directory統合DNSでセキュアDDNS更新のみが許可されている場合は、このパラメータの値をtrueに設定する必要があります。デフォルトでは、セキュアDDNSは無効になっています。セキュアDDNSは、SVM用のSMBサーバまたはActive Directoryアカウントを作成した後にのみ有効にできます。	いいえ	
DNSドメインのFQDN DNSドメインのFQDN。SVMのDNSネームサービスに設定されているドメイン名と同じドメイン名を使用する必要があります。	いいえ	

ネットワーク ポート

ONTAPネットワークポート構成について学ぶ

ポートは、物理ポート（NIC）と仮想ポート（インターフェイス グループやVLANなど）に分類されます。

仮想ポートは仮想ローカル エリア ネットワーク（VLAN）とインターフェイス グループで構成されます。インターフェイス グループは複数の物理ポートを1つのポートとして扱い、VLANは1つの物理ポートを複数の異なる論理ポートに分割します。

- 物理ポート：LIF は物理ポート上で直接設定できます。
- インターフェース グループ：単一のトランク ポートとして機能する 2 つ以上の物理ポートを含むポート アグリゲート。インターフェース グループには、シングル モード、マルチモード、ダイナミック マルチモードがあります。
- VLAN：VLANタグ付き（IEEE 802.1Q規格）トラフィックを送受信する論理ポート。VLANポートの特性には、ポートのVLAN IDが含まれます。基盤となる物理ポートまたはインターフェースグループポートはVLANトランクポートとみなされ、接続されたスイッチポートはVLAN IDをトランクするように設定する必要があります。

  VLANポートの基になる物理ポートまたはインターフェイス グループ ポートは引き続きLIFをホストし、タグなしのトラフィックを送受信できます。

- 仮想IP（VIP）ポート：VIP LIFのホームポートとして使用される論理ポート。VIPポートはシステムによって自動的に作成され、限られた数の操作のみをサポートします。VIPポートはONTAP 9.5以降でサポートされます。

ポートの命名規則は *enumberletter* です：

- 最初の文字はポートの種類です。「e」はイーサネットを表します。
- 2文字目はポート アダプタのスロット番号を示します。
- 3文字目は複数ポート アダプタ上のポートの位置を示します。「a」は最初のポート、「b」は2番目のポートを示し、以下同様です。

たとえば、 `e0b`は、イーサネット ポートがノードのマザーボード上の 2 番目のポートであることを示します。

VLAN は、構文 `port_name-vlan-id`を使用して名前を付ける必要があります。

`port_name` 物理ポートまたはインターフェイス グループを指定します。

`vlan-id`ネットワーク上のVLAN識別番号を指定します。たとえば、 `e1c-80`は有効なVLAN名です。

ネットワーク ポートの設定

物理ポートを組み合わせて**ONTAP**インターフェースグループを作成する

インターフェイス グループ（別名リンク アグリゲーション グループ[LAG]）は、同じノード上の2つ以上の物理ポートを1つの論理ポートに組み合わせて作成します。論理ポートを使用すると、耐障害性と可用性が向上し、負荷も共有できます。

インターフェイス グループの種類

ストレージ システムでは、シングルモード、スタティック マルチモード、およびダイナミック マルチモードという3種類のインターフェイス グループがサポートされています。各インターフェイス グループは、フォールト トレランスのレベルが異なります。マルチモード インターフェイス グループは、ネットワーク トラフィックのロード バランシング方法を提供します。

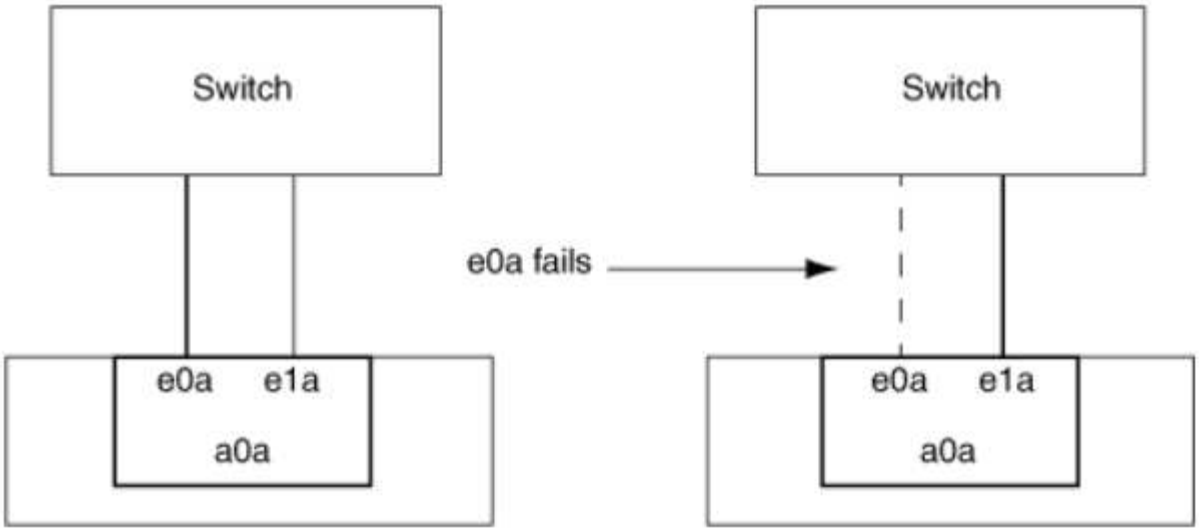
シングルモード インターフェイス グループの特性

シングルモード インターフェイス グループでは、インターフェイス グループの1つのインターフェイスだけがアクティブになります。他のインターフェイスはスタンバイで、アクティブなインターフェイスに障害が発生した場合に動作を引き継ぎます。

シングルモード インターフェイス グループの特性は、次のとおりです。

- フェイルオーバーでは、クラスタがアクティブ リンクを監視して、フェイルオーバーを制御します。クラスタがアクティブ リンクを監視するので、スイッチを設定する必要はありません。
- シングルモード インターフェイス グループには、複数のスタンバイ インターフェイスを設定できます。
- シングルモード インターフェイス グループが複数のスイッチをカバーする場合は、スイッチどうしをInter-Switch Link（ISL;スイッチ間リンク）で接続する必要があります。
- シングルモード インターフェイス グループでは、スイッチ ポートが同じブロードキャスト ドメインに属している必要があります。
- ポートが同じブロードキャスト ドメイン内にあるかどうかを確認するために、リンク監視用ARPパケット（送信元アドレスは0.0.0.0）がポートを介して送信されます。

次の図はシングルモード インターフェイス グループの例です。この例では、e0aとe1aがa0aというシングルモード インターフェイス グループを構成しています。アクティブ インターフェイスのe0aに障害が発生すると、スタンバイ インターフェイスのe1aが処理を引き継ぎ、スイッチとの接続を維持します。



シングルモード機能を実現するためには、フェイルオーバー グループを使用するアプローチが推奨されます。フェイルオーバー グループを使用すると、2番目のポートを引き続き他のLIFに使用でき、未使用のままにする必要がありません。またフェイルオーバー グループは、複数のポートにまたがることも、複数のノードのポートにまたがることも可能です。

スタティック マルチモード インターフェイス グループの特性

ONTAPに実装されているスタティック マルチモード インターフェイス グループは、IEEE 802.3ad（static）に準拠しています。スタティック マルチモード インターフェイス グループでは、アグリゲーションはサポートするがアグリゲーション設定のための制御パケット交換は行わないスイッチを使用できます。

スタティック マルチモード インターフェイス グループは、Link Aggregation Control Protocol（LACP）とも呼ばれるIEEE 802.3ad（dynamic）に準拠していません。LACPはポート アグリゲーション プロトコル（PAgP）と同等な、Cisco独自のリンク ポート アグリゲーション プロトコルです。

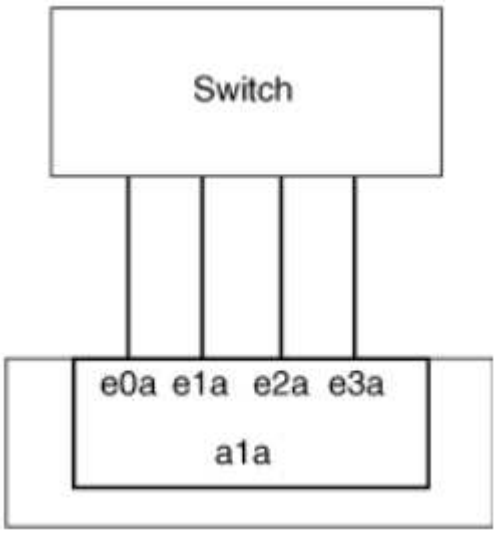
スタティック マルチモード インターフェイス グループの特性は、次のとおりです。

- インターフェイス グループ内のすべてのインターフェイスがアクティブで、単一のMACアドレスを共有します。
  - 複数の接続が、インターフェイス グループ内のインターフェイスに分散されます。
  - 各接続またはセッションが、インターフェイス グループ内の1つのインターフェイスを使用します。シーケンシャル ロード バランシング方式を使用する場合、すべてのセッションはパケット ベースで使用可能なリンク全体で分散され、インターフェイス グループの特定のインターフェイスにバインドされません。
- スタティック マルチモード インターフェイス グループは、最大「n-1」個のインターフェイスの障害から回復することができます。この「n」は、インターフェイス グループを構成しているインターフェイスの合計数です。
- あるポートで障害が発生した場合や切断された場合は、そのリンクを経由していたトラフィックが残りのインターフェイスの1つに自動的に再分散されます。
- スタティック マルチモード インターフェイス グループではリンクの喪失は検出できますが、クライアントへの接続の切断や、接続性とパフォーマンスに影響を及ぼす可能性があるスイッチの設定ミスは検出できません。
- スタティック マルチモード インターフェイス グループには、複数のスイッチ ポートでのリンク アグリ

ゲーションをサポートするスイッチが必要です。インターフェイス グループの各リンクの接続先ポートがすべて1つの論理ポートを構成するよう、そのスイッチを設定します。一部のスイッチは、ジャンボ フレーム用に構成されたポートのリンク アグリゲーションをサポートしていない場合があります。詳細については、スイッチ ベンダーのマニュアルを参照してください。

- スタティック マルチモード インターフェイス グループのインターフェイス間でのトラフィック分散には、いくつかのロード バランシング オプションを使用できます。

次の図はスタティック マルチモード インターフェイス グループの例を示したものです。インターフェイスe0a、e1a、e2a、およびe3aは、a1aというマルチモード インターフェイス グループの一部です。このa1aマルチモード インターフェイス グループの4つのインターフェイスはすべてアクティブです。



1つの集約リンク内のトラフィックを複数の物理スイッチに分散するテクノロジがいくつか存在します。この機能を有効にするテクノロジは、ネットワーキング製品によって異なります。ONTAPのスタティック マルチモード インターフェイス グループは、IEEE 802.3規格に準拠しています。IEEE 802.3規格に対応または準拠すると言われている複数スイッチ リンク アグリゲーション テクノロジであれば、ONTAPと一緒に使用できます。

IEEE 802.3規格には、集約リンク内の送信デバイスが、送信用の物理インターフェイスを決定することが規定されています。そのため、ONTAPが受け持つのは発信トラフィックの分散だけで、着信フレームの受信方法を制御することはできません。集約リンクでの着信トラフィックの転送を管理または制御するためには、直接接続されたネットワーク デバイス上でその転送を変更する必要があります。

ダイナミック マルチモード インターフェイス グループ

ダイナミック マルチモード インターフェイス グループは、Link Aggregation Control Protocol（LACP）を実装して、直接接続されたスイッチへのグループ メンバーシップの通信を行います。LACPを使用すると、リンク ステータスの喪失および直接接続されたスイッチ ポートと通信できないノードを検出できます。

ONTAPに実装されているダイナミック マルチモード インターフェイス グループは、IEEE 802.3 AD（802.1AX）に準拠しています。ONTAPは、Cisco独自のリンク アグリゲーション プロトコルであるPort Aggregation Protocol（PAgP）をサポートしていません。

ダイナミック マルチモード インターフェイス グループには、LACPをサポートするスイッチが必要です。

ONTAPは、アクティブまたはパッシブ モードに設定されているスイッチとの相性がよい、設定不可のアクティブ モードでLACPを実装します。ONTAPは、IEEE 802.3 AD（802.1AX）の規定に従い、longおよびshortのLACPタイマーを実装し、設定不可の値（3秒と90秒）で使用します。

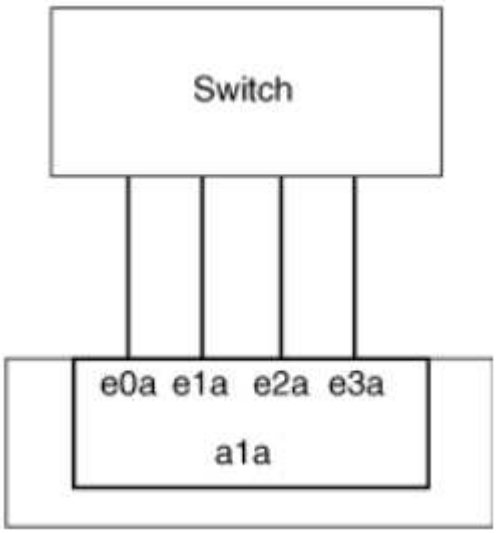
ONTAPのロード バランシング アルゴリズムは、発信トラフィックの転送に使用されるメンバー ポートを決定しますが、着信フレームの受信方法は制御しません。スイッチは、そのポート チャネル グループに設定されたロード バランシング アルゴリズムに基づいて、転送に使用されるポート チャネル グループのメンバー（個々の物理ポート）を決定します。したがって、スイッチの設定により、トラフィックを受信するストレージ システムのメンバー ポート（個々の物理ポート）が決まります。スイッチ設定の詳細については、スイッチ ベンダーのマニュアルを参照してください。

あるインターフェイスが、連続したLACPプロトコル パケットの受信に失敗すると、そのインターフェイスに対しては「ifgrp status」コマンドで「lag_inactive」と出力されます。既存のトラフィックは、他のアクティブなインターフェイスに自動的に再ルーティングされます。

ダイナミック マルチモード インターフェイス グループを使用する場合、以下のルールが適用されます。

- ダイナミック マルチモード インターフェイス グループは、ポートベース、IPベース、MACベース、またはラウンドロビンによるロード バランシング方式を使用するように設定する必要があります。
- ダイナミック マルチモード インターフェイス グループでは、すべてのインターフェイスをアクティブにして、1つのMACアドレスを共有する必要があります。

次の図は、ダイナミック マルチモード インターフェイス グループの例です。インターフェイスe0a、e1a、e2a、およびe3aは、a1aというマルチモード インターフェイス グループの一部です。a1aダイナミック マルチモード インターフェイス グループの4つのインターフェイスはすべてアクティブです。



マルチモード インターフェイス グループでのロード バランシング

IP アドレス、MAC アドレス、シーケンシャル、またはポートベース ロード バランシング方式を使用して、マルチモード インターフェイス グループのネットワーク ポートにネットワーク トラフィックを均等に分散することにより、マルチモード インターフェイス グループのすべてのインターフェイスが送信トラフィックに均等に使用されるようにすることができます。

マルチモード インターフェイス グループのロード バランシング方式を指定できるのは、インターフェイス グループの作成時だけです。

ベスト プラクティス：可能な限り、ポートベース ロード バランシングを推奨します。ネットワークに特別な理由や制限がない限り、ポートベース ロード バランシングを使用してください。

ポートベースのロード バランシング

ポートベースのロード バランシングは推奨される方式です。

ポートベースのロード バランシング方式を使用して、マルチモード インターフェイス グループのトラフィックをトランスポート レイヤ（TCPまたはUDP）ポートに基づいて均等に分散させることができます。

ポートベースのロード バランシング方式では、トランスポート レイヤのポート番号に加えて、送信元と受信側のIPアドレスに対して高速ハッシュ アルゴリズムを使用します。

IPアドレスおよび**MAC**アドレスによるロード バランシング

IPアドレスおよびMACアドレスによるロード バランシングは、マルチモード インターフェイス グループのトラフィックを均等にする方式です。

これらのロード バランシング方式では、送信元アドレスと受信側アドレス（IPアドレスおよびMACアドレス）に対して高速ハッシュ アルゴリズムを使用します。ハッシュ アルゴリズムの結果が、リンク状態がUPでないインターフェイスに一致した場合は、次のアクティブなインターフェイスが使用されます。

> ルーターに直接接続しているシステムでインターフェイス グループを作成する場合は、MACアドレスによるロード バランシング方式を選択しないでください。このような構成では、すべての発信IPフレームの宛先MACアドレスはルーターのMACアドレスになります。そのため、使用されるインターフェイス グループのインターフェイスは1つだけになります。

IPアドレスによるロード バランシングは、IPv4アドレスとIPv6アドレスの両方で同様に機能します。

シーケンシャル ロード バランシング

シーケンシャル ロード バランシングでは、ラウンドロビン アルゴリズムを使用して複数のリンク間でパケットを均等に分散できます。単一の接続のトラフィックのロード バランシングによって負荷を複数のリンクに分散させて、単一の接続のスループットを向上させるには、シーケンシャル オプションを使用します。

ただし、シーケンシャル ロード バランシングでは、パケット配信の順序が乱れてパフォーマンスが大幅に低下する可能性があります。このため、一般にシーケンシャル ロード バランシングは推奨されません。

インターフェイス グループ（別名**LAG**）の作成

インターフェイス グループ（別名LAG）をシングルモード、スタティック マルチモード、またはダイナミック マルチモード（LACP）で作成すると、グループ内のネットワーク ポートの機能を組み合わせて1つのインターフェイスとしてクライアントに提供できます。

実行する手順は、System ManagerとCLIのどちらのインターフェイスを使用するかによって異なります。

System Manager

System Manager を使用して **LAG** を作成します

手順

1. LAG を作成するには、ネットワーク **> Ethernet** ポート **> + Link Aggregation Group** を選択します。
2. ドロップダウン リストからノードを選択します。
3. 次のいずれかを選択します。
   a. ONTAPで ブロードキャスト ドメインを自動的に選択（推奨） します。
   b. ブロードキャスト ドメインを手動で選択する。
4. LAGを構成するポートを選択します。
5. モードを選択します。
   a. シングル：一度に 1 つのポートのみが使用されます。
   b. 複数：すべてのポートを同時に使用できます。
   c. LACP：LACP プロトコルは使用できるポートを決定します。
6. 負荷分散を選択します。
   a. IP based
   b. MAC based
   c. ポート
   d. シーケンシャル
7. 変更を保存します。

CLI

CLI を使用してインターフェース グループを作成する

マルチモード インターフェイス グループを作成するときは、次のいずれかのロード バランシング方式を指定できます。

- `port`：ネットワーク トラフィックはトランスポート層（TCP/UDP）ポートに基づいて分散されます。これは推奨されるロード バランシング方法です。
- `mac`：ネットワーク トラフィックは MAC アドレスに基づいて分散されます。
- `ip`：ネットワーク トラフィックは IP アドレスに基づいて分散されます。
- `sequential`：ネットワーク トラフィックは受信されるとすぐに分散されます。

> インターフェイス グループのMACアドレスは、基盤のポートの順序およびそれらのポートがブートアップ時にどのように初期化されるかによって決まります。そのため、ifgrpのMACアドレスがリブート後やONTAPのアップグレード後に変わる可能性があることを想定しておいてください。

手順

`network port ifgrp create`コマンドを使用してインターフェース グループを作成します。

インターフェース グループには、`a<number><letter>`という構文を使用して名前を付ける必要があります。たとえば、a0a、a0b、a1c、a2aは有効なインターフェース グループ名です。

`network port ifgrp create`
の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/network-port-ifgrp-create.html["ONTAPコマンド リファレンス"^]をご覧ください。

次の例は、分散機能をportに、モードをmultimodeに設定して、a0aという名前のインターフェイス グループを作成する方法を示しています。

```
network port ifgrp create -node cluster-1-01 -ifgrp a0a -distr-func port -mode multimode
```

インターフェイス グループ（別名**LAG**）へのポートの追加

すべてのポート速度のインターフェイス グループ（別名LAG）に、最大16個の物理ポートを追加できます。

実行する手順は、System ManagerとCLIのどちらのインターフェイスを使用するかによって異なります。

System Manager

System Managerを使用してポートを**LAG**に追加します

手順

1. LAG を編集するには、ネットワーク **>** イーサネット ポート **> LAG** を選択します。
2. 同じノードからLAGに追加するポートを選択します。
3. 変更を保存します。

CLI

CLI を使用してインターフェイス グループにポートを追加する

手順

インターフェイス グループにネットワーク ポートを追加します。

```
network port ifgrp add-port
```

次の例は、a0aというインターフェイス グループにポートe0cを追加する方法を示しています。

```
network port ifgrp add-port -node cluster-1-01 -ifgrp a0a -port e0c
```

ONTAP 9.8以降では、最初の物理ポートがインターフェース グループに追加されてから約1分後に、インターフェース グループは適切なブロードキャスト ドメインに自動的に配置されます。ONTAPによるこの処理を希望せず、ifgrpを手動でブロードキャスト ドメインに配置する場合は、 `ifgrp add-port`コマンドの一部として `-skip-broadcast-domain-placement`パラメータを指定します。

"ONTAPコマンド リファレンス"のポート インターフェイス グループに適用される `network port ifgrp add-port`と設定制限の詳細については、こちらを参照してください。

インターフェイス グループ（別名**LAG**）からのポートの削除

LIFをホストするインターフェイス グループからポートを削除できます。ただし、削除するポートがインターフェイス グループ内の最後のポートでない場合に限ります。最後のポートをインターフェイス グループから削除しないという前提により、インターフェイス グループがLIFをホストできない、またはインターフェイス グループをLIFのホーム ポートに指定できないという要件はありません。ただし、最後のポートを削除する場合は、先にインターフェイス グループからLIFを移行または移動しておく必要があります。

タスク概要

インターフェイス グループ（別名LAG）からは最大16個のポート（物理インターフェイス）を削除できます。

実行する手順は、System ManagerとCLIのどちらのインターフェイスを使用するかによって異なります。

System Manager

System Managerを使用して**LAG**からポートを削除します

手順

1. LAG を編集するには、ネットワーク **>** イーサネット ポート **> LAG** を選択します。
2. LAGから削除するポートを選択します。
3. 変更を保存します。

CLI

CLI を使用してインターフェイス グループからポートを削除する

手順

インターフェイス グループからネットワーク ポートを削除します。

```
network port ifgrp remove-port
```

`network port ifgrp remove-port`
の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/network-port-ifgrp-remove-port.html["ONTAPコマンド リファレンス"^]をご覧ください。

次の例は、a0aというインターフェイス グループからポートe0cを削除する方法を示しています。

```
network port ifgrp remove-port -node cluster-1-01 -ifgrp a0a -port e0c
```

インターフェイス グループ（別名**LAG**）の削除

基盤となる物理ポートに直接LIFを設定する場合、またはインターフェイス グループ（別名LAG）のモードや分散機能を変更する場合は、インターフェイス グループ（別名LAG）を削除することができます。

開始する前に

- LIFをホストしているインターフェイス グループ（別名LAG）は削除できません。
- LIFのホーム ポートまたはフェイルオーバー ターゲットであるインターフェイス グループ（別名LAG）は削除できません。

実行する手順は、System ManagerとCLIのどちらのインターフェイスを使用するかによって異なります。

System Manager

System Managerを使用して**LAG**を削除します

手順

1. LAG を削除するには、ネットワーク **>** イーサネット ポート **> LAG** を選択します。
2. 削除するLAGを選択します。
3. LAGを削除します。

CLI

CLI を使用してインターフェース グループを削除する

手順

`network port ifgrp delete`コマンドを使用してインターフェース
グループを削除します。

`network port ifgrp delete`
の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/network-port-ifgrp-delete.html["ONTAPコマンド リファレンス"^]をご覧ください。

次に、a0bという名前のインターフェイス グループを削除する例を示します。

```
network port ifgrp delete -node cluster-1-01 -ifgrp a0b
```

物理ポート経由で**ONTAP VLAN**を設定する

ONTAPでVLANを使用し、分離されたブロードキャスト ドメインを作成することで、ネットワークを論理的にセグメント化できます。このブロードキャスト ドメインは、従来の物理的な境界ではなく、スイッチ ポートに基づいて定義されます。

1つのVLANは、複数の物理ネットワーク セグメントにまたがることができます。それぞれのVLANには、機能またはアプリケーションで関連性のあるエンド ステーションが属します。

たとえば、エンジニアリングや財務などの部門単位、またはリリース1やリリース2などのプロジェクト単位で、VLANのエンド ステーションをまとめることができます。VLANではエンド ステーションが物理的に近接した配置であることは重要ではないので、エンド ステーションを地理的に分散させても、スイッチ化されたネットワークにブロードキャスト ドメインを含めることができます。

ONTAP 9.14.1および9.13.1では、論理インターフェイス（LIF）で使用されていないタグなしポートで、接続されたネットワーク スイッチ上でネイティブVLAN接続が確立されていないポートは、デグレード状態としてマークされます。これは未使用ポートを識別するためのものであり、機能停止を示すものではありません。ネイティブVLANは、ONTAP CFMブロードキャストなど、ifgrpベース ポートでのタグなしトラフィックを許可します。タグなしトラフィックがブロックされないように、ネットワーク スイッチ上でネイティブVLANを設定してください。

管理者は、VLANを作成または削除したり、その情報を表示したりできます。

スイッチのネイティブVLANと同じ識別子のVLANをネットワーク インターフェイス上に作成しないでください。たとえば、ネットワーク インターフェイスe0bがネイティブVLAN 10に割り当てられている場合、そのインターフェイス上にVLAN e0b-10を作成しないでください。

VLANの作成

System Manager または `network port vlan create`コマンドを使用して、同じネットワーク ドメイン内で個別のブロードキャスト ドメインを維持するための VLAN を作成できます。

開始する前に

次の要件を満たしていることを確認します。

- ネットワーク上に配置されたスイッチが、IEEE 802.1Q規格に準拠しているか、ベンダー固有のVLANを実装している。
- 複数のVLANをサポートする場合、エンド ステーションが1つ以上のVLANに属するように静的に設定されている。
- VLANは、クラスタLIFをホストしているポートに接続されていない。
- VLANは、「Cluster」IPspaceに割り当てられているポートに接続されていない。
- VLANは、メンバー ポートのないインターフェイス グループ ポートに作成されていない。

タスク概要

VLANを作成すると、クラスタの指定したノードのネットワーク ポートにそのVLANが接続されます。

VLANを初めてポートに設定したときに、ポートが停止してネットワーク接続が一時的に切断されることがあります。その後同じポートにVLANを追加するときは、この問題は発生しません。

スイッチのネイティブVLANと同じ識別子のVLANをネットワーク インターフェイス上に作成しないでください。たとえば、ネットワーク インターフェイスe0bがネイティブVLAN 10に割り当てられている場合、そのインターフェイス上にVLAN e0b-10を作成しないでください。

実行する手順は、System ManagerとCLIのどちらのインターフェイスを使用するかによって異なります。

System Manager

System Managerを使用して**VLAN**を作成する

ONTAP 9.12.0以降では、ブロードキャスト ドメインを自動で選択することも、リストから手動で選択することもできます。以前は、ブロードキャスト ドメインはレイヤ2の接続に基づいて常に自動で選択されていました。ブロードキャスト ドメインを手動で選択すると、接続が失われる可能性があるという警告が表示されます。

手順

1. ネットワーク **>** イーサネット ポート **> + VLAN** を選択します。
2. ドロップダウン リストからノードを選択します。
3. 次のいずれかを選択します。
   a. ONTAPで ブロードキャスト ドメインを自動的に選択（推奨） します。
   b. リストからブロードキャスト ドメインを手動で選択する。
4. VLANを構成するポートを選択します。
5. VLAN IDを指定します。
6. 変更を保存します。

CLI

CLI を使用して **VLAN** を作成する

特定の状況では、ハードウェアの問題やソフトウェアの誤った構成を修正せずに、劣化したポートにVLAN ポートを作成する場合は、 `network port modify`コマンドの `-ignore-health-status`パラメータを`true`として設定できます。

`network port modify`の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/network-port-modify.html["ONTAPコマンド リファレンス"^]をご覧ください。

手順

1. `network port vlan create`コマンドを使用してVLANを作成します。
2. VLANを作成する際は、 `vlan-name`または `port`と `vlan-id`のいずれかのオプションを指定する必要があります。VLAN名は、ポート（またはインターフェース グループ）名とネットワーク スイッチVLAN識別子をハイフンで区切って組み合わせたものです。例えば、 `e0c-24`と `e1c-80`は有効なVLAN名です。

次の例は、ノード `cluster-1-01`上のネットワーク ポート `e1c`に接続された VLAN `e1c-80`を作成する方法を示しています：

```
network port vlan create -node cluster-1-01 -vlan-name e1c-80
```

ONTAP 9.8以降、VLANは作成後約1分で適切なブロードキャストドメインに自動的に配置されます。ONTAPによる自動配置を希望せず、VLANを手動でブロードキャストドメインに配置する場合は、

`vlan create`コマンドの一部として `-skip-broadcast-domain-placement`パラメータを指定します。

`network port vlan create`
の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/network-port-vlan-create.html["ONTAPコマンド リファレンス"^]をご覧ください。

VLANの編集

ブロードキャスト ドメインを変更したり、VLANを無効にしたりできます。

System Managerを使用したVLANの編集

ONTAP 9.12.0以降では、ブロードキャスト ドメインを自動で選択することも、リストから手動で選択することもできます。以前は、ブロードキャスト ドメインはレイヤ2の接続に基づいて常に自動で選択されていました。ブロードキャスト ドメインを手動で選択すると、接続が失われる可能性があるという警告が表示されます。

手順

1. ネットワーク **>** イーサネット ポート **> VLAN** を選択します。
2. 編集アイコンを選択します。
3. 次のいずれかを実行します。
   - 別のブロードキャスト ドメインをリストから選択して変更する。
   - *有効*チェック ボックスをオフにします。
4. 変更を保存します。

VLANの削除

NICをスロットから取り外す前に、VLANの削除が必要になることがあります。VLANを削除すると、そのVLANを使用しているすべてのフェイルオーバー ルールとフェイルオーバー グループから自動的に削除されます。

開始する前に

VLANに関連付けられているLIFがないことを確認します。

タスク概要

ポートの最後のVLANを削除すると、そのポートとネットワークの接続が一時的に切断される可能性があります。

実行する手順は、System ManagerとCLIのどちらのインターフェイスを使用するかによって異なります。

System Manager

System Managerを使用して**VLAN**を削除する

手順

1. ネットワーク **>** イーサネット ポート **> VLAN** を選択します。
2. 削除するVLANを選択します。
3. *削除*をクリックします。

CLI

CLI を使用して **VLAN** を削除する

手順

`network port vlan delete`コマンドを使用してVLANを削除します。

次の例は、ノード `cluster-1-01`のネットワーク ポート `e1c`から VLAN `e1c-80`を削除する方法を示しています：

```
network port vlan delete -node cluster-1-01 -vlan-name e1c-80
```

`network port vlan delete`
の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/network-port-vlan-delete.html["ONTAPコマンド リファレンス"^]をご覧ください。

ONTAPネットワークポート属性を変更する

物理ネットワーク ポートの自動ネゴシエーション、二重モード、フロー制御、速度、および健全性の設定を変更することができます。

開始する前に

LIFをホストしているポートは変更できません。

タスク概要

- 100GbE、40GbE、10GbE、または1GbEのネットワーク インターフェイスの管理設定は変更しないことをお勧めします。

  二重モードおよびポート速度の設定値のことを管理設定と呼びます。ネットワークの制限によっては、管理設定が運用設定（ポートで実際に使用されている二重モードおよび速度）と同じにならないことがあります。

- インターフェイス グループの基盤となる物理ポートの管理設定は変更しないことをお勧めします。

`-up-admin`パラメータ（advanced権限レベルで使用可能）は、ポートの管理設定を変更します。

- ノード上のすべてのポート、またはノード上で最後に稼働しているクラスタ LIF をホストするポートの `-up-admin`管理設定を false に設定することはお勧めしません。
- management interface の MTU サイズを変更することはお勧めしません e0M。
- ブロードキャスト ドメインのポートのMTUサイズを、そのブロードキャスト ドメイン用に設定されたMTU値以外に変更することはできません。
- VLANのMTUサイズがベース ポートのMTUサイズの値を超えることはできません。

手順

1. ネットワーク ポートの属性を変更します。

   ```
   network port modify
   ```

2. `-ignore-health-status`フィールドをtrueに設定すると、システムが指定されたポートのネットワークポートのヘルスステータスを無視できることを指定できます。

   ネットワークポートのヘルスステータスは自動的に「劣化」から「正常」に変更され、このポートはLIFのホスティングに使用できるようになりました。クラスタポートのフロー制御を `none`に設定する必要があります。デフォルトでは、フロー制御は `full`に設定されています。

次のコマンドは、フロー制御をnoneに設定してポートe0bのフロー制御を無効にします。

```
network port modify -node cluster-1-01 -port e0b -flowcontrol-admin none
```

`network port modify`の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/network-port-modify.html["ONTAPコマンド リファレンス"^]をご覧ください。

40GbE NICポートを変換して**ONTAP**ネットワーク用の**10GbE**ポートを作成する

X1144A-R6およびX91440A-R6 40GbEネットワーク インターフェイス カード（NIC）を変換して、4個の10GbEポートをサポートできます。

これらのNICのいずれかをサポートするハードウェア プラットフォームを、10GbEのクラスタ インターコネクトと顧客データ接続をサポートするクラスタに接続する場合は、NICを10GbE接続に対応するように変換する必要があります。

開始する前に

サポート対象のブレークアウト ケーブルを使用している必要があります。

タスク概要

NIC をサポートするプラットフォームの完全なリストについては、 "Hardware Universe"を参照してくださ

い。

X1144A-R6 NICでは、4つの10GbE接続をサポートするように変換できるのはポートAのみです。ポートAを変換すると、ポートEは使用できなくなります。

手順

1. 保守モードに切り替えます。
2. NICを40GbEサポートから10GbEサポートに変換します。

```
nicadmin convert -m [40G | 10G] [port-name]
```

3. convertコマンドを使用したあと、ノードを停止します。
4. ケーブルを取り付けるか変更します。
5. ハードウェア モデルに応じて、SP（サービス プロセッサ）またはBMC（ベースボード管理コントローラ）を使用してノードの電源を再投入し、変換を有効にします。

ONTAPネットワーク用に**UTA X1143A-R6**ポートを設定する

デフォルトでは、X1143A-R6統合ターゲット アダプタはFCターゲット モードに設定されていますが、ポートを10GbイーサネットおよびFCoE（CNA）ポート、または16Gb FCイニシエータ ポートまたはターゲット ポートとして設定できます。これには別のSFP+アダプタが必要です。

イーサネットおよびFCoE用に設定した場合、X1143A-R6アダプタは、同じ10GbEポートのNICおよびFCoEのターゲット トラフィックを同時にサポートします。FC用に設定した場合、同じASICを共有する2ポートの各ペアをFCターゲットまたはFCイニシエータ モード用に個別に設定できます。つまり、単一のX1143A-R6アダプタが、1つの2ポート ペアでFCターゲット モードをサポートし、もう1つの2ポート ペアでFCイニシエータ モードをサポートできます。同じASICに接続するポート ペアは、同じモードで構成する必要があります。

X1143A-R6アダプタは、FCモードでは既存のFCデバイスと同じように動作し、最大速度は16Gbpsになります。X1143A-R6アダプタをCNAモードで使用すると、同じ10GbEポートを共有するNICおよびFCoEのトラフィックを同時に処理することができます。CNAモードでは、FCoEの機能についてはFCターゲット モードのみがサポートされます。

統合ターゲット アダプタ（X1143A-R6）を設定するには、同じチップ上の隣接する2つのポートを同じパーソナリティ モードで設定する必要があります。

手順

1. ポート構成を表示します：

```
system hardware unified-connect show
```

2. ファイバー チャネル（FC）または統合ネットワーク アダプタ（CNA）に必要なポートを設定します：

```
system node hardware unified-connect modify -node <node_name> -adapter
<adapter_name> -mode {fcp|cna}
```

3. FC または 10 Gb Ethernet に適切なケーブルを接続します。
4. 正しい SFP+ がインストールされていることを確認します：

```
network fcp adapter show -instance -node -adapter
```

CNAの場合は、10Gb Ethernet SFPを使用する必要があります。FCの場合は、接続先のFCファブリックに応じて、8Gb SFPまたは16Gb SFPを使用する必要があります。

UTA2ポートを**ONTAP**ネットワークで使用するために変換する

UTA2ポートを、Converged Network Adapter（CNA）モードからFibre Channel（FC）モードに変換したり、その逆に変換したりできます。

ポートをネットワークに接続する物理メディアを変更する必要がある場合、または FC イニシエーターとターゲットをサポートする必要がある場合は、UTA2 パーソナリティを CNA モードから FC モードに変更する必要があります。

CNAモードから**FC**モードへ

手順

1. アダプタをオフラインにします。

```
network fcp adapter modify -node <node_name> -adapter <adapter_name>
-status-admin down
```

2. ポートのモードを変更します。

```
ucadmin modify -node <node_name> -adapter <adapter_name> -mode fcp
```

3. ノードをリブートし、アダプタをオンラインにします。

```
network fcp adapter modify -node <node_name> -adapter <adapter_name>
-status-admin up
```

4. 必要に応じて、管理者または VIF マネージャーにポートの削除または除去を通知します。
   - ポートが LIF のホーム ポートとして使用されている場合、インターフェイス グループ（ifgrp）のメンバーである場合、または VLAN をホストしている場合、管理者は次の操作を行う必要があります：
     - それぞれ、LIF を移動するか、ifgrp からポートを削除するか、VLAN を削除します。
     - `network port delete`コマンドを実行してポートを手動で削除します。 `network port delete`コマンドが失敗した場合、管理者はエラーに対処してから、コマンドを再度実行する必要があります。
   - ポートがLIFのホームポートとして使用されておらず、ifgrpのメンバーでもなく、VLANをホストしていない場合、VIFマネージャは再起動時にそのポートをレコードから削除する必要があります。VIFマネージャがポートを削除しない場合は、管理者は再起動後に `network port delete`コマンドを使用して手動でポートを削除する必要があります。

     `network port delete`
     の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/network-port-delete.html["ONTAPコマンド リファレンス "^]をご覧ください。

5. 正しい SFP+ がインストールされていることを確認します：

```
network fcp adapter show -instance -node -adapter
```

CNAの場合は、10Gb Ethernet SFPを使用する必要があります。FCの場合は、ノードの設定を変更する前に、8 Gb SFPまたは16 Gb SFPを使用する必要があります。

FCモードから**CNA**モードへ

手順

1. アダプタをオフラインにします。

```
network fcp adapter modify -node <node_name> -adapter <adapter_name>
-status-admin down
```

2. ポートのモードを変更します。

```
ucadmin modify -node <node_name> -adapter <adapter_name> -mode cna
```

3. ノードをリブートする
4. 正しい SFP+ がインストールされていることを確認します。

   CNAの場合は、10GbイーサネットSFPを使用する必要があります。

CNA/UTA2光モジュールを**ONTAP**ネットワーク用に変換する

ユニファイド ターゲット アダプタ（CNA / UTA2）用に選択したパーソナリティ モードをサポートするには、そのアダプタで光モジュールを変更する必要があります。

手順

1. カードで現在使用されているSFP+を確認してください。その後、現在のSFP+を、優先パーソナリティ（FCまたはCNA）に適したSFP+に交換してください。
2. X1143A-R6アダプタから現在の光モジュールを取り外します。
3. 優先して使用するパーソナリティ モード（FCまたはCNA）の光ファイバに適したモジュールを取り付けます。
4. 正しい SFP+ がインストールされていることを確認します：

```
network fcp adapter show -instance -node -adapter
```

   サポートされている SFP+ モジュールおよび Cisco ブランドの銅線（Twinax）ケーブルは、 "NetApp Hardware Universe"にリストされています。

ONTAPクラスタノードから**NIC**を削除する

障害の発生したNICをスロットから取り外したり、メンテナンス時にNICを別のスロットに移したりしなければならない場合があります。

ONTAP 9.7以前のバージョンでは、NICの削除手順が異なります。ONTAP 9.7以前を実行しているONTAPクラスタノードからNICを削除する必要がある場合は、手順"ノードからのNICの取り外し（ONTAP 9.7以前）"を参照してください。

手順

1. ノードの電源をオフにします。
2. NICをスロットから物理的に取り外します。
3. ノードの電源を投入します。
4. ポートが削除されたことを確認します。

```
network port show
```

ONTAPは、ポートをすべてのインターフェースグループから自動的に削除します。ポートがインターフェースグループの唯一のメンバーだった場合、インターフェースグループは削除されます。"ONTAPコマンド リファレンス"の `network port show`の詳細をご覧ください。

5. ポートにVLANが設定されていた場合は、VLANが孤立状態になります。孤立状態のVLANは、次のコマンドを使用して確認できます。

```
cluster controller-replacement network displaced-vlans show
```

`displaced-interface show`、`displaced-vlans show`、および `displaced-vlans restore`コマンドは一意であり、 `cluster controller-replacement network`で始まる完全修飾コマンド名を必要としません。

6. これらのVLANは削除されていますが、次のコマンドを使用してリストアできます。

```
displaced-vlans restore
```

7. ポートにLIFが設定されていた場合は、同じブロードキャスト ドメイン内の別のポートが新しいホーム ポートとして自動的に選択されます。同じストレージ コントローラに適切なホーム ポートが見つからなかったLIFは、孤立状態とみなされます。孤立状態のLIFは、次のコマンドを使用して確認できます。

```
displaced-interface show
```

8. 同じノードのブロードキャストドメインに新しいポートが追加されると、LIFのホームポートは自動的に復元されます。または、 `network interface modify -home-port -home-node or use the displaced- interface restore`コマンドを使用してホームポートを設定することもできます。

関連情報

- "cluster controller-replacement network displaced-interface delete"
- "network interface modify"

ONTAPネットワークポートの健全性を監視する

ONTAPによるネットワーク ポートの管理には、健全性の自動監視と一連のヘルスモニタが含まれており、LIFをホストするのに適していない可能性があるネットワーク ポートを特定するのに役立ちます。

タスク概要

ヘルスモニタによってネット ワークポートが正常でないと判断されると、EMSメッセージで管理者に警告が表示されるか、そのポートがデグレードとマークされます。LIFに対して別の健全なフェイルオーバー ターゲットが用意されている場合、ONTAPはデグレード状態のネットワーク ポートでのLIFのホストを回避します。リンク フラッピング（リンクの接続状態と切断状態が頻繁に切り替わる現象）やネットワーク パーティショニングなどのソフトな障害イベントが原因で、ポートがデグレード状態になることがあります。

- クラスタIPspace内のネットワーク ポートは、リンク フラッピングが発生した場合、またはブロードキャスト ドメイン内の他のネットワーク ポートへのレイヤ2（L2）の到達可能性が失われた場合にデグレードとマークされます。
- 非クラスタIPspace内のネットワーク ポートは、リンク フラッピングが発生するとデグレードとマークされます。

デグレード状態のポートについては、以下の動作に注意する必要があります。

- デグレード状態のポートをVLANやインターフェイス グループに含めることはできません。

  インターフェイス グループのメンバー ポートがデグレードとマークされていても、インターフェイス グループが正常とマークされている場合は、そのインターフェイス グループでLIFをホストできます。

- LIFは、デグレード状態のポートから健全なポートに自動的に移行されます。
- フェイルオーバー イベント時に、デグレード状態のポートはフェイルオーバー ターゲットとみなされません。健全なポートがない場合は、通常のフェイルオーバー ポリシーに従って、デグレード状態のポートがLIFをホストします。
- デグレード状態のポートにはLIFを作成、移行、リバートできません。

  ネットワークポートの `ignore-health-status`設定を `true`に変更できます。その後、正常なポートでLIFをホストできます。

手順

1. advanced権限モードにログインします。

```
set -privilege advanced
```

2. ネットワーク ポートの健全性の監視が有効になっているヘルスモニタを確認します。

```
network options port-health-monitor show
```

ポートのヘルス ステータスは、ヘルスモニタの値によって決まります。

ONTAPでは、以下のヘルスモニタを使用できます。これらのヘルスモニタは、デフォルトで有効になっています。

- Link-flappingヘルスモニター：Link-flappingを監視します

  ポートでリンク フラッピングが5分以内に複数回発生した場合に、そのポートがデグレードとマークされます。

- L2到達可能性ヘルスモニター：同じブロードキャストドメインに設定されているすべてのポートが相互にL2到達可能であるかどうかを監視します

  このヘルスモニタは、すべてのIPspaceのL2到達可能性の問題を報告しますが、デグレードとマークされるのはクラスタIPspace内のポートのみです。

- CRCモニター：ポートのCRC統計を監視します

  このヘルスモニタはポートをデグレードとマークしませんが、CRCエラー率が非常に高い場合にEMSメッセージを生成します。

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

3. 必要に応じて `network options port-health-monitor modify`コマンドを使用して、IPspaceのヘルスモニターを有効または無効にします。

   `network options port-health-monitor modify`
   の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/network-options-port-health-monitor-modify.html["ONTAPコマンド リファレンス"^]を参照してください。

4. ポートの詳細な健全性を表示します。

   ```
   network port show -health
   ```

コマンド出力には、ポートのヘルスステータス、 `ignore health status`設定、およびポートが劣化としてマークされている理由のリストが表示されます。

ポートのヘルス ステータスは `healthy`または `degraded`になります。

`ignore health status`設定が `true`の場合、ポートのヘルスステータスが管理者によって`degraded`から `healthy`に変更されたことを示します。

`ignore health status`設定が `false`の場合、ポートのヘルス
ステータスはシステムによって自動的に決定されます。

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

ONTAPネットワークポートの到達可能性を監視する

ONTAP 9.8以降には、到達可能性を監視する機能が搭載されています。この監視機能を使用して、物理的なネットワーク トポロジがONTAPの設定と一致していない状況を特定します。ONTAPでポートの到達可能性を修復できるケースもあります。できない場合は追加の手順が必要になります。

タスク概要

これらのコマンドを使用して、ONTAPの設定が物理的なケーブル接続またはネットワーク スイッチの設定に一致していないことに起因するネットワーク設定ミスを検証、診断、修復します。

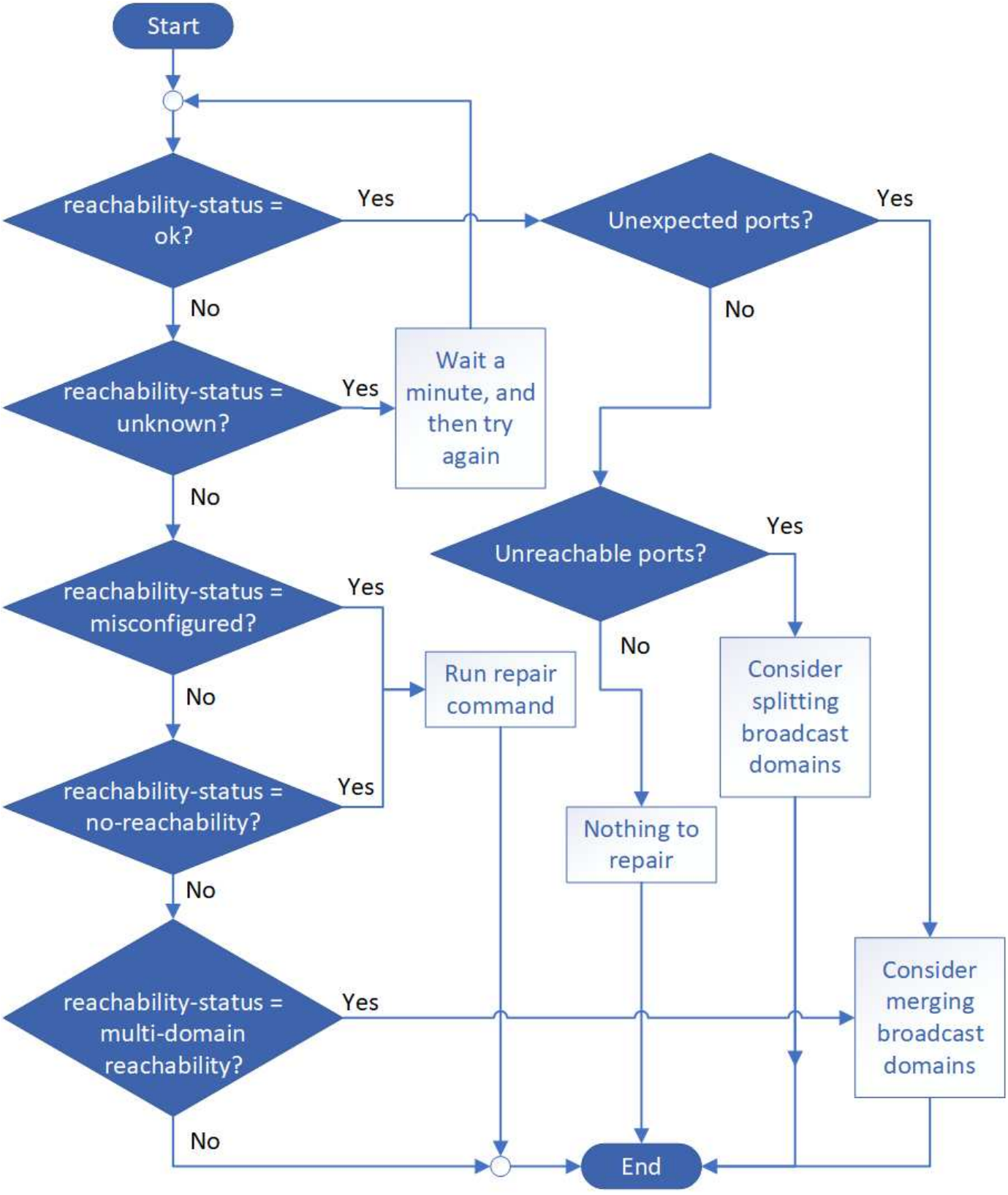
手順

1. ポートの到達可能性を表示します。

```
network port reachability show
```

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

2. 次のデシジョン ツリーと表を参照して、次に実行する手順を確認します。



到達可能性ステータス	概要

ok	ポートは割り当てられたブロードキャストドメインへのレイヤー2到達性を備えています。到達性ステータスが「ok」であっても「予期しないポート」がある場合は、1つ以上のブロードキャストドメインを統合することを検討してください。詳細については、次の_予期しないポート_の行を参照してください。 到達可能性ステータスが「ok」であるにもかかわらず、「到達不能ポート」が存在する場合は、1つ以上のブロードキャストドメインを分割することを検討してください。詳細については、次の_到達不能ポート_の行を参照してください。 到達可能性ステータスが「ok」で、かつ想定外のポートも到達不能なポートも存在しない場合、設定に問題はありません。
予期しないポート	ポートは割り当てられたブロードキャスト ドメインに対してレイヤ2到達可能性を持ちますが、少なくとも1つの他のブロードキャスト ドメインに対してもレイヤ2到達可能性を持ちます。 物理的な接続とスイッチの設定に間違いがないか、またはポートに割り当てられているブロードキャスト ドメインを1つ以上のブロードキャスト ドメインとマージする必要がないかを確認します。 詳細については、"ブロードキャスト ドメインのマージ"を参照してください。
到達不能なポート	単一のブロードキャストドメインが2つの異なる到達可能性セットに分割されている場合は、ブロードキャストドメインを分割してONTAP構成を物理ネットワークトポロジと同期できます。 通常、到達不能なポートは、物理的な構成とスイッチの設定に間違いがないことを確認したうえで、別のブロードキャスト ドメインにスプリットする必要があります。 詳細については、"ブロードキャスト ドメインのスプリット"を参照してください。
到達可能性の設定ミス	ポートは割り当てられたブロードキャスト ドメインに対してレイヤ2到達可能性を持ちませんが、別のブロードキャスト ドメインに対してはレイヤ2到達可能性を持ちます。 ポートの到達可能性を修復します。次のコマンドを実行すると、到達可能性があるブロードキャスト ドメインにポートが割り当てられます。 `network port reachability repair -node -port`詳細については、"ポートの到達可能性の修復"を参照してください。
到達不能	ポートには、既存のブロードキャストドメインへのレイヤー2到達可能性がありません。 ポートの到達可能性を修復します。次のコマンドを実行すると、デフォルトIPspaceに新しいブロードキャスト ドメインが自動的に作成され、ポートが割り当てられます。 `network port reachability repair -node -port`詳細については、"ポートの到達可能性の修復"を参照してください。"ONTAPコマンド リファレンス"の `network port reachability repair`の詳細を確認してください。

マルチドメイン到達可能性	ポートは割り当てられたブロードキャスト ドメインに対してレイヤ2到達可能性を持ちますが、少なくとも1つの他のブロードキャスト ドメインに対してもレイヤ2到達可能性を持ちます。 物理的な接続とスイッチの設定に間違いがないか、またはポートに割り当てられているブロードキャスト ドメインを1つ以上のブロードキャスト ドメインとマージする必要がないかを確認します。 詳細については、"ブロードキャスト ドメインのマージ"または"ポートの到達可能性の修復"を参照してください。
不明	到達可能性ステータスが「不明」の場合は、数分待ってからコマンドを再試行してください。

ポートを修復した後は、LIFとVLANの配置がずれていないか確認し、解決する必要があります。ポートがインターフェイスグループに属していた場合は、そのインターフェイスグループに何が起きたのかを把握する必要もあります。詳細については、"ポートの到達可能性の修復"を参照してください。

ONTAPネットワークでのポートの使用について学ぶ

ONTAPと特定のサービスとの通信用に、いくつかのウェルノウンポートが予約されています。ストレージ ネットワーク環境のポート値がONTAPポートの値と同じ場合、ポートの競合が発生します。

インバウンド トラフィック

ONTAPストレージの受信トラフィックでは、次のプロトコルとポートが使用されます：

プロトコル	ポート	目的
すべてのICMP	All	インスタンスにpingを実行する
TCP	22	クラスタ管理LIFまたはノード管理LIFのIPアドレスへのSecure Shellアクセス
TCP	80	クラスタ管理LIFのIPアドレスへのWebページアクセス
TCP/UDP	111	RPCBIND、NFS のリモート プロシージャ コール
UDP	123	NTP、ネットワーク タイム プロトコル
TCP	135	MSRPC、Microsoft リモート プロシージャ コール
TCP	139	NETBIOS-SSN、CIFSのNetBIOSサービス セッション
TCP/UDP	161-162	SNMP、Simple Network Management Protocol
TCP	443	クラスタ管理LIFのIPアドレスへのセキュアなWebページアクセス
TCP	445	MS Active Domain Services、NetBIOSフレーミングを使用したTCP経由のMicrosoft SMB/CIFS

TCP/UDP	635	NFSマウントは、リモートファイルシステムをローカルファイルシステムのように操作します。
TCP	749	Kerberos
UDP	953	名前daemon
TCP/UDP	2049	NFSサーバ デーモン
TCP	2050	NRV、NetApp リモートボリュームプロトコル
TCP	3260	iSCSI データ LIF を介した iSCSI アクセス
TCP/UDP	4045	NFSロック デーモン
TCP/UDP	4046	NFS のネットワーク ステータス モニター
UDP	4049	NFS RPC Rquotad
UDP	4444	KRB524、Kerberos 524
UDP	5353	マルチキャストDNS
TCP	10000	ネットワーク データ管理プロトコル（NDMP）を使用したバックアップ
TCP	11104	クラスタピアリング、SnapMirrorのクラスタ間通信セッションの双方向管理
TCP	11105	クラスタピアリング、クラスタ間LIFを使用した双方向SnapMirrorデータ転送
SSL/TLS	30000	DMAとNDMPサーバー間のセキュアソケット（SSL/TLS）経由のNDMPセキュア制御接続を受け入れます。セキュリティスキャナーはポート30000の脆弱性を報告する場合があります。

送信トラフィック

ONTAPストレージ上の送信トラフィックは、ビジネス ニーズに応じて基本ルールまたは詳細ルールを使用して設定できます。

基本的なアウトバウンドルール

すべてのポートは、ICMP、TCP、および UDP プロトコルを介したすべての送信トラフィックに使用できます。

プロトコル	ポート	目的
すべてのICMP	All	すべての送信トラフィック
すべてのTCP	All	すべての送信トラフィック
すべての UDP	All	すべての送信トラフィック

高度なアウトバウンドルール

アウトバウンド トラフィックに厳格なルールが必要な場合は、次の情報を使用して、ONTAPによるアウトバウンド通信に必要なポートのみを開くことができます。

Active Directory

プロトコル	ポート	ソース	デスティネーション	目的
TCP	88	ノード管理LIF、データLIF（NFS、CIFS、iSCSI）	Active Directoryフォレスト	Kerberos V認証
UDP	137	ノード管理LIF、データLIF（NFS、CIFS）	Active Directoryフォレスト	NetBIOSネーム サービス
UDP	138	ノード管理LIF、データLIF（NFS、CIFS）	Active Directoryフォレスト	NetBIOSデータグラムサービス
TCP	139	ノード管理LIF、データLIF（NFS、CIFS）	Active Directoryフォレスト	NetBIOSサービス セッション
TCP	389	ノード管理LIF、データLIF（NFS、CIFS）	Active Directoryフォレスト	LDAP
UDP	389	ノード管理LIF、データLIF（NFS、CIFS）	Active Directoryフォレスト	LDAP
TCP	445	ノード管理LIF、データLIF（NFS、CIFS）	Active Directoryフォレスト	NetBIOSフレームを使用したTCP経由のMicrosoft SMB/CIFS
TCP	464	ノード管理LIF、データLIF（NFS、CIFS）	Active Directoryフォレスト	Kerberos V パスワードの変更と設定（SET_CHANGE）
UDP	464	ノード管理LIF、データLIF（NFS、CIFS）	Active Directoryフォレスト	Kerberos鍵管理
TCP	749	ノード管理LIF、データLIF（NFS、CIFS）	Active Directoryフォレスト	Kerberos V パスワード（RPCSEC_GSS）の変更と設定

AutoSupport

プロトコル	ポート	ソース	デスティネーション	目的
TCP	80	ノード管理LIF	support.netapp.com	AutoSupport（トランスポート プロトコルがHTTPS から HTTP に変更された場合のみ）

SNMP

プロトコル	ポート	ソース	デスティネーション	目的
TCP/UDP	162	ノード管理LIF	監視サーバー	SNMPトラップによる監視

SnapMirror

プロトコル	ポート	ソース	デスティネーション	目的
TCP	11104	クラスタ間LIF	ONTAPクラスタ間LIF	SnapMirrorのクラスタ間通信セッションの管理

その他のサービス

プロトコル	ポート	ソース	デスティネーション	目的
TCP	25	ノード管理LIF	メール サーバ	SMTPアラートは、AutoSupportに使用できます
UDP	53	ノード管理LIFとデータLIF（NFS、CIFS）	DNS	DNS
UDP	67	ノード管理LIF	DHCP	DHCP サーバ
UDP	68	ノード管理LIF	DHCP	初回セットアップ用のDHCPクライアント
UDP	514	ノード管理LIF	syslogサーバ	Syslog転送メッセージ
TCP	5010	クラスタ間LIF	バックアップエンドポイントまたはリストアエンドポイント	S3へのバックアップ機能のバックアップおよびリストア処理
TCP	18600～18699	ノード管理LIF	宛先サーバー	NDMPコピー

ONTAP内部ポートについて学ぶ

次の表は、ONTAPが内部で使用するポートとその機能を示しています。ONTAPは、クラスタ内LIF通信の確立など、さまざまな機能にこれらのポートを使用します。

このリストは網羅的なものではなく、環境によって異なる場合があります。

ポート / プロトコル	コンポーネント/機能
514	syslog
900	NetAppクラスタRPC
902	NetAppクラスタRPC
904	NetAppクラスタRPC
905	NetAppクラスタRPC
910	NetAppクラスタRPC
911	NetAppクラスタRPC
913	NetAppクラスタRPC
914	NetAppクラスタRPC

915	NetAppクラスタRPC
918	NetAppクラスタRPC
920	NetAppクラスタRPC
921	NetAppクラスタRPC
924	NetAppクラスタRPC
925	NetAppクラスタRPC
927	NetAppクラスタRPC
928	NetAppクラスタRPC
929	NetAppクラスタRPC
930	カーネルサービスおよび管理機能（KSMF）
931	NetAppクラスタRPC
932	NetAppクラスタRPC
933	NetAppクラスタRPC
934	NetAppクラスタRPC
935	NetAppクラスタRPC
936	NetAppクラスタRPC
937	NetAppクラスタRPC
939	NetAppクラスタRPC
940	NetAppクラスタRPC
951	NetAppクラスタRPC
954	NetAppクラスタRPC
955	NetAppクラスタRPC
956	NetAppクラスタRPC
958	NetAppクラスタRPC
961	NetAppクラスタRPC
963	NetAppクラスタRPC
964	NetAppクラスタRPC
966	NetAppクラスタRPC
967	NetAppクラスタRPC
975	Key Management Interoperability Protocol（KMIP）
982	NetAppクラスタRPC
983	NetAppクラスタRPC
5125	ディスク用の代替制御ポート
5133	ディスク用の代替制御ポート

5144	ディスク用の代替制御ポート
65502	ノードを対象としたSSH
65503	LIFの共有
7700	Cluster Session Manager（CSM）
7810	NetAppクラスタRPC
7811	NetAppクラスタRPC
7812	NetAppクラスタRPC
7813	NetAppクラスタRPC
7814	NetAppクラスタRPC
7815	NetAppクラスタRPC
7816	NetAppクラスタRPC
7817	NetAppクラスタRPC
7818	NetAppクラスタRPC
7819	NetAppクラスタRPC
7820	NetAppクラスタRPC
7821	NetAppクラスタRPC
7822	NetAppクラスタRPC
7823	NetAppクラスタRPC
7824	NetAppクラスタRPC
7835-7839および7845-7849	クラスタ内通信用のTCPポート
8023	ノードを対象としたTelnet
8443	Amazon FSx 用 ONTAP S3 NAS ポート
8514	ノードを対象としたRSH
9877	KMIPクライアント ポート（内部ローカル ホストのみ）
10006	HAインターコネクト通信用のTCPポート

IPspace

ONTAP IPspace構成について学ぶ

IPspaceを使用すると、単一のONTAPクラスタを設定し、複数の管理上分離されたネットワーク ドメインのクライアントが、たとえ同じIPアドレス範囲を使用している場合でもアクセスできるようにすることができます。これにより、クライアント トラフィックを分離してプライバシーとセキュリティを確保することができます。

IPspaceは、Storage Virtual Machine（SVM）が実装される、個別のIPアドレス スペースを定義します。あるIPspaceに対して定義されたポートとIPアドレスは、そのIPspace内でのみ有効です。IPspace内のSVMごと

に個別のルーティング テーブルが保持されるため、SVMやIPspaceをまたがってトラフィックがルーティングされることはありません。

IPspaceのルーティング ドメインでは、IPv4およびIPv6のアドレスがサポートされます。

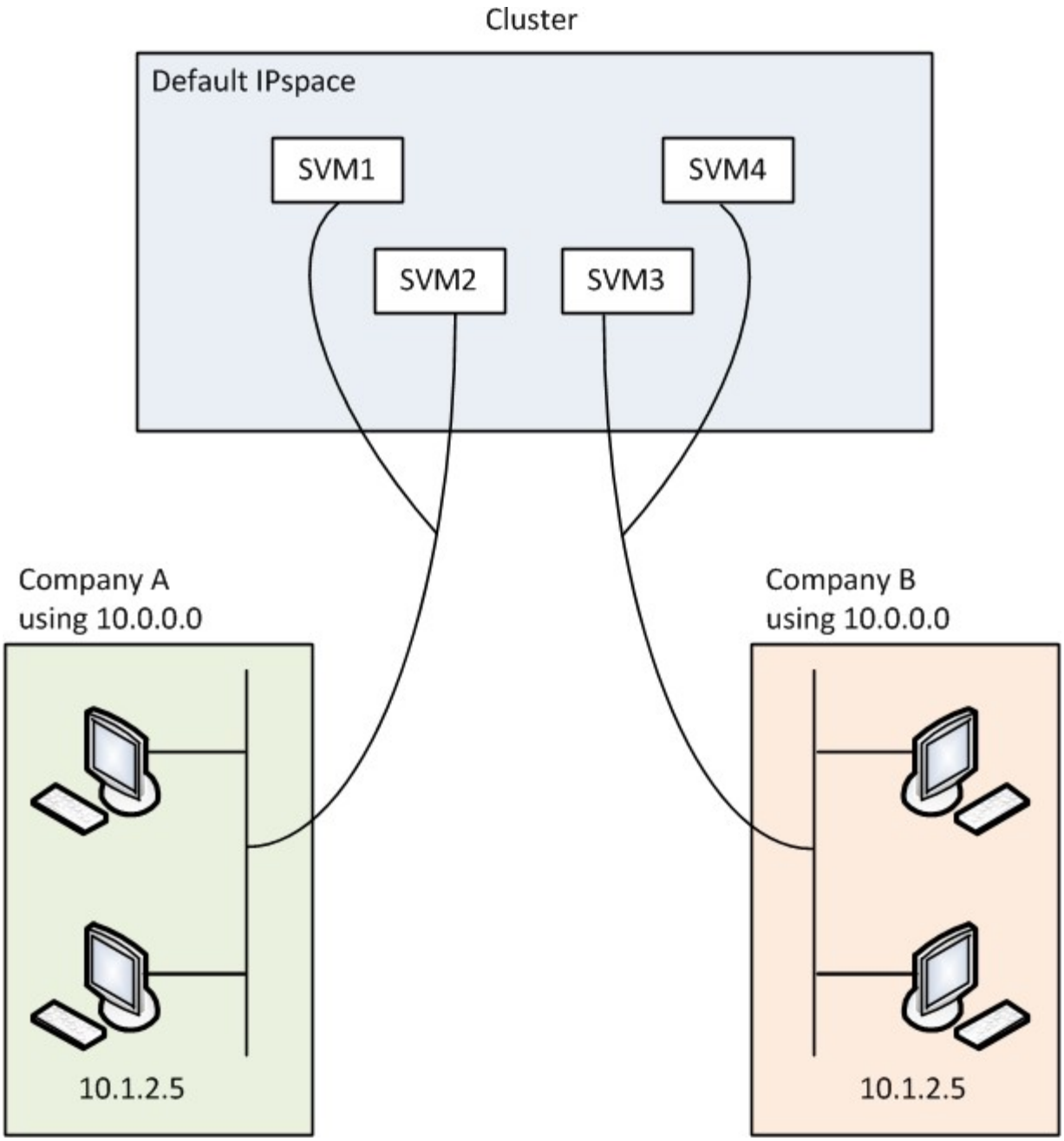
単一の組織のストレージを管理する場合は、IPspaceを設定する必要はありません。単一のONTAPクラスタで複数企業のストレージを管理していて、ユーザ間のネットワーク設定がないことが確実な場合も、IPspaceを使用する必要はありません。多くの場合、Storage Virtual Machine （SVM）を専用のIPルーティング テーブルと一緒に使用することで、IPspaceを使用しなくても固有のネットワーク設定を分離できます。

IPspaceの使用例

ここでは、IPspaceの一般的な用途として、ストレージ サービス プロバイダ（SSP）が、その顧客のA社とB社をSSPのONTAPクラスタに接続する必要があり、両方の会社が同じプライベートIPアドレスの範囲を使用する場合を取り上げます。

SSPは、クラスタに顧客用のSVMを作成し、2つのSVMからA社のネットワークへの専用ネットワーク パス、別の2つのSVMからB社のネットワークへの専用ネットワーク パスを提供します。

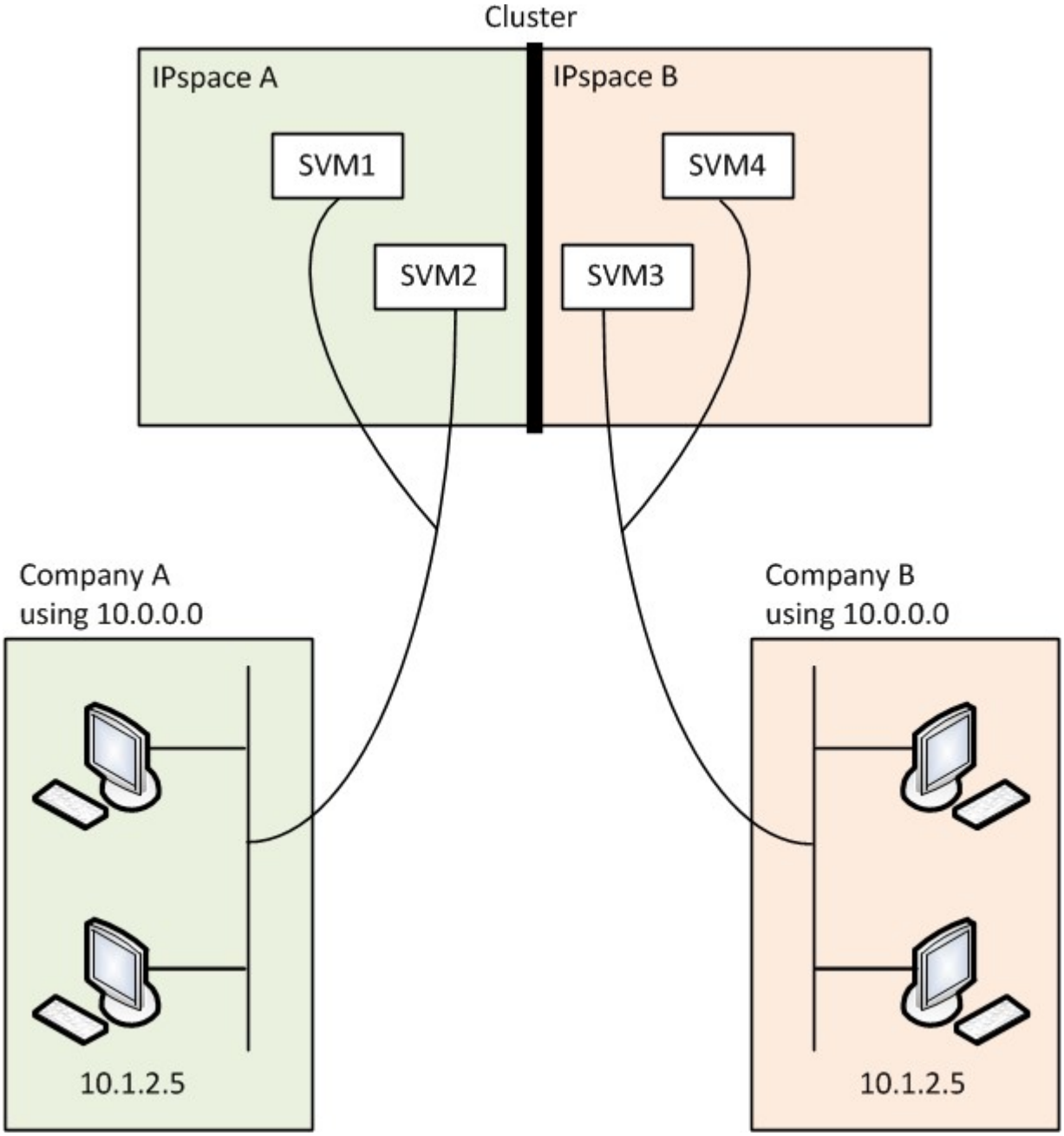
次の図に、この導入形態を示します。これは、両社で非プライベートIPアドレスの範囲を使用する場合に機能します。しかし、図に示すように両社が同じプライベートIPアドレスの範囲を使用すると問題が発生します。



両社がプライベートIPアドレスのサブネット10.0.0.0を使用すると、次のような問題が起こります。

- 両社がそれぞれのSVMに同じIPアドレスを使用した場合は、SSPにあるクラスタ内のSVMでIPアドレスの競合が発生します。
- 両社がそれぞれのSVMに別々のIPアドレスを使用することにした場合でも、まだ問題は残ります。
- たとえば、A社のネットワークのクライアントがB社のネットワークのクライアントと同じIPアドレスを持っている場合は、本来A社のアドレス スペースのクライアント宛てのパケットが、B社のアドレス スペースのクライアントにルーティングされる（またはその逆）可能性があります。
- 両社が互いに排他的なアドレス スペースを使用する（たとえば、A社がアドレス10.0.0.0とネットワーク マスク255.128.0.0を、B社がアドレス10.128.0.0とネットワーク マスク255.128.0.0を使用する）場合は、SSPがトラフィックをA社およびB社のネットワークに正しくルーティングするための静的ルートをクラスタに設定する必要があります。
- しかし、この方法は拡張性がなく（静的ルートであるため）、安全でもありません（ブロードキャスト ト

ラフィックがクラスタのすべてのインターフェイスに送信されるため）。この問題を解決するには、SSPが1社に1つずつ、2つのIPspaceをクラスタに定義する必要があります。トラフィックがIPspaceをまたがってルーティングされることはないので、すべてのSVMが10.0.0.0というアドレス スペースに設定されても、次の図に示すように、それぞれの会社のデータが該当するネットワークにセキュアにルーティングされます。



さらに、 `/etc/ hosts`ファイル、 `/etc/hosts.equiv`ファイル、 `the /etc/rc`ファイルなどの各種設定ファイルで参照されるIPアドレスは、そのIPspaceを基準とした相対的なものです。そのため、IPspaceを使用することで、SSPは複数のSVMの設定データと認証データに同じIPアドレスを設定でき、競合が発生することはありません。

IPspaceの標準プロパティ

クラスタの初回作成時に、特別なIPspaceがデフォルトで作成されます。さらに、IPspaceごとに特別なStorage Virtual Machine（SVM）が作成されます。

クラスタが初期化されると、次の2つのIPspaceが自動的に作成されます。

- 「Default」IPspace

  このIPspaceは、ポート、サブネット、およびデータ提供元SVMのコンテナです。クライアントごとに別々のIPspaceを作成する必要がない構成であれば、すべてのSVMをこのIPspaceに作成できます。このIPspaceにはクラスタ管理ポートとノード管理ポートも含まれます。

- 「Cluster」IPspace

  このIPspaceにはクラスタ内の全ノードのクラスタ ポートがすべて含まれ、クラスタの作成時に自動的に作成されます。このIPspaceは、内部のプライベート クラスタ ネットワークへの接続を提供します。ノードをクラスタに追加すると、追加したノードのクラスタ ポートが「Cluster」IPspaceに追加されます。

IPspaceごとに「システム」SVMが1つ存在します。IPspaceを作成すると、デフォルトのシステムSVMがIPspaceと同じ名前で作成されます。

- 「Cluster」IPspaceのシステムSVMは、内部プライベート クラスタ ネットワークのノード間でクラスタ トラフィックを伝送します。

  このSVMの管理はクラスタ管理者が担当し、「Cluster」という名前が割り当てられます。

- 「Default」IPspaceのシステムSVMは、クラスタ間トラフィックを含めた、クラスタとノードの管理トラフィックを伝送します。

  このSVMの管理はクラスタ管理者が担当し、クラスタと同じ名前が使用されます。

- ユーザが作成するカスタムIPspaceのシステムSVMは、そのSVMの管理トラフィックを伝送します。

  このSVMの管理はクラスタ管理者が担当し、IPspaceと同じ名前が使用されます。

1つのIPspaceにクライアント用のSVMを1つ以上配置できます。各クライアントSVMは専用のデータ ボリュームと設定を持ち、他のSVMからは独立して管理されます。

ONTAPネットワークのIPspaceを作成する

IPspaceは、Storage Virtual Machine（SVM）が属する個別のIPアドレス スペースです。SVMでセキュアなストレージ、管理、ルーティングを必要とする場合に、IPspaceを作成します。IPspaceを使用すると、クラスタ内のSVMごとに個別のIPアドレス スペースを作成できます。これにより、管理上分離されたネットワーク ドメインのクライアントが、IPアドレスの同じサブネット範囲内の重複したIPアドレスを使用してクラスタのデータにアクセスできるようになります。

タスク概要

IPspaceの数はクラスタ全体で最大512個です。この制限は、RAMが6GBのノードを含むクラスタでは256個に削減されます。お使いのプラットフォームに適用されるその他の制限を確認するには、Hardware Universeを参照してください。

"NetApp Hardware Universe"

「all」はシステムに予約されている名前なので、IPspace名を「all」にすることはできません。

開始する前に

このタスクを実行するには、クラスタ管理者である必要があります。

手順

1. IPspaceを作成します。

```
network ipspace create -ipspace ipspace_name
```

`ipspace_name`は、作成するIPspaceの名前です。次のコマンドは、クラスタ上にIPspace ipspace1を作成します：

```
network ipspace create -ipspace ipspace1
```

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

2. IPspaceを表示します。

```
network ipspace show
```

```
IPspace              Vserver List          Broadcast Domains
-------------------- --------------------- ------------------------------
Cluster              Cluster               Cluster
Default              Cluster1              Default
ipspace1             ipspace1              -
```

IPspaceが、そのIPspaceのシステムSVMとともに作成されます。システムSVMは管理トラフィックを伝送します。

終了後の操作

MetroCluster構成を使用しているクラスタ内にIPspaceを作成する場合は、IPspaceオブジェクトをパートナークラスタに手動でレプリケートする必要があります。IPspaceをレプリケートする前に作成されてIPspaceに割り当てられたSVMは、パートナー クラスタにレプリケートされません。

ブロードキャスト ドメインは「Default」IPspace内に自動的に作成され、次のコマンドを使用してIPspace間で移動できます。

```
network port broadcast-domain move
```

たとえば、ブロードキャスト ドメインを「Default」から「ips1」に移動する場合は、次のコマンドを使用します。

```
network port broadcast-domain move -ipspace Default -broadcast-domain
Default -to-ipspace ips1
```

ONTAPネットワーク上のIPspaceを表示する

クラスタに存在するIPspaceのリストを表示して、各IPspaceに割り当てられているStorage Virtual Machine（SVM）、ブロードキャスト ドメイン、およびポートを確認することができます。

手順

クラスタ内のIPspaceとSVMを表示します。

```
network ipspace show [-ipspace ipspace_name]
```

次のコマンドは、クラスタ内のすべてのIPspace、SVM、ブロードキャスト ドメインを表示します。

```
network ipspace show
IPspace        Vserver List             Broadcast Domains
-------------  -----------------------  -------------------
Cluster
               Cluster                  Cluster
Default
               vs1, cluster-1            Default
ipspace1
               vs3, vs4, ipspace1       bcast1
```

次のコマンドは、ipspace1というIPspaceに属するノードとポートを表示します。

```
network ipspace show -ipspace ipspace1
IPspace name: ipspace1
Ports: cluster-1-01:e0c, cluster-1-01:e0d, cluster-1-01:e0e, cluster-1-
02:e0c, cluster-1-02:e0d, cluster-1-02:e0e
Broadcast Domains: Default-1
Vservers: vs3, vs4, ipspace1
```

`network ipspace show`の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/network-ipspace-show.html["ONTAPコマンド リファレンス"^]をご覧ください。

ONTAPネットワークからIPspaceを削除する

不要になったIPspaceは削除できます。

開始する前に

削除するIPspaceに、関連付けられているブロードキャスト ドメイン、ネットワーク インターフェイス、SVMがないことを確認します。

システム定義の「Default」IPspaceと「Cluster」IPspaceは削除できません。

手順

IPspace を削除：

```
network ipspace delete -ipspace ipspace_name
```

次のコマンドでは、クラスタからipspace1というIPspaceを削除しています。

```
network ipspace delete -ipspace ipspace1
```

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

ブロードキャスト ドメイン

ONTAPブロードキャスト ドメインについて学ぶ

ブロードキャスト ドメインを使うと、同じレイヤ2ネットワークに属するネットワークポートをグループ化できます。グループ化したポートは、データまたは管理トラフィック用のStorage Virtual Machine（SVM）で使用できます。

ONTAP 9.7以前のバージョンでは、ブロードキャストドメインの管理方法が異なります。ONTAP 9.7以前のバージョンを実行しているネットワークでブロードキャストドメインを管理する必要がある場合は、"ブロードキャスト ドメインの概要（ONTAP 9.7以前）"を参照してください。

ブロードキャスト ドメインはIPspace内に配置されます。クラスタを初期化すると、デフォルトのブロードキャスト ドメインが2つ作成されます。

- 「Default」ブロードキャスト ドメインには、「Default」IPspace内にあるポートが含まれています。

  これらのポートは、主にデータの提供に使用されます。クラスタ管理ポートとノード管理ポートも、このブロードキャスト ドメインに含まれています。

- 「Cluster」ブロードキャスト ドメインには、「Cluster」IPspace内にあるポートが含まれています。

  これらのポートはクラスタ通信に使われ、クラスタの全ノードのすべてのクラスタ ポートが含まれています。

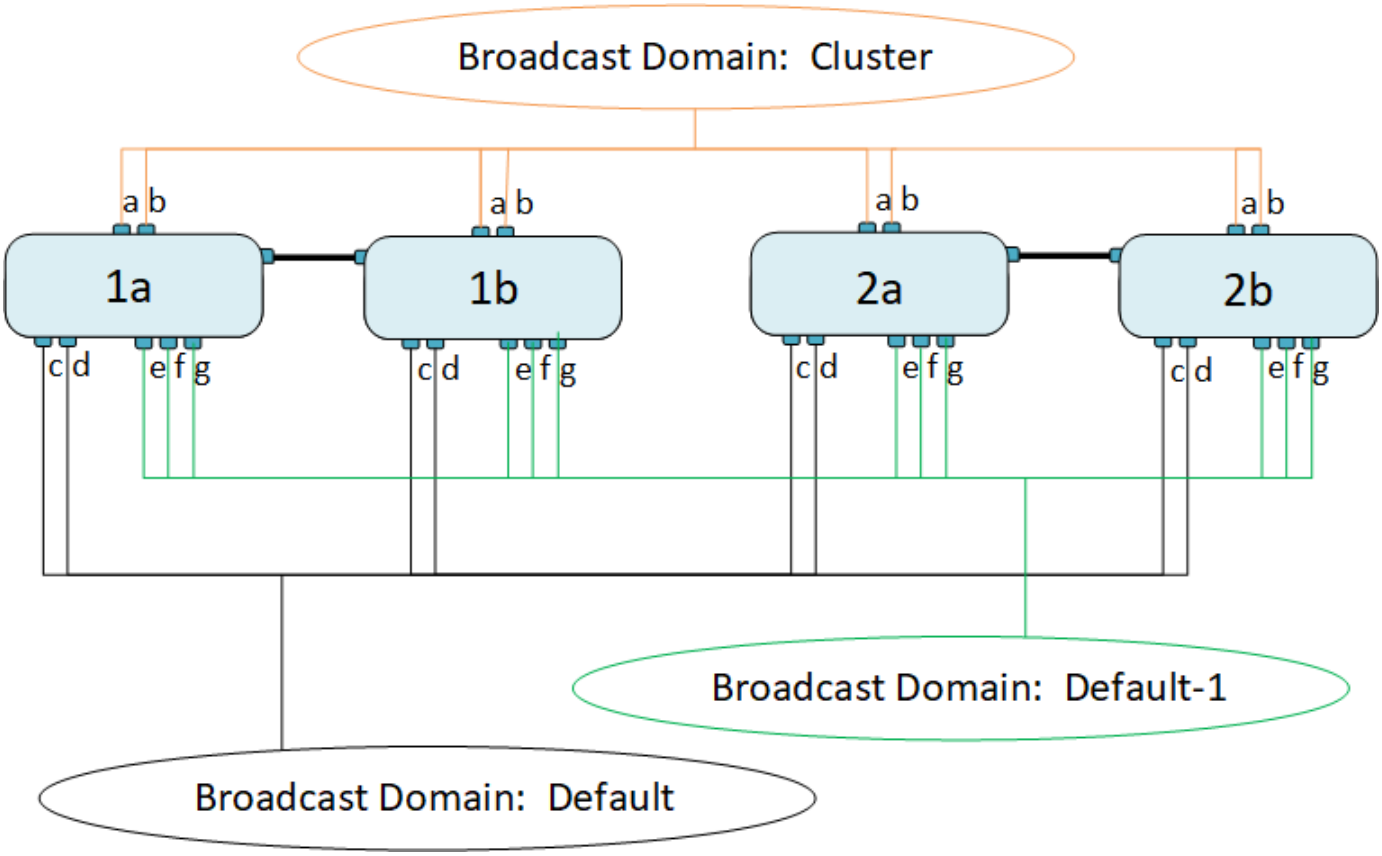
  必要に応じて、ブロードキャスト ドメインがDefault IPspaceに追加で作成されます。「Default」ブロードキャスト ドメインには、管理LIFのホーム ポートと、そのポートへのレイヤ2の到達可能性があるポートがすべて含まれています。追加のブロードキャスト ドメインの名前は、「Default-1」、「Default-2」などとなります。

ブロードキャスト ドメインの使用例

ブロードキャスト ドメインは、同じIPspace内にあり、相互にレイヤ2の到達可能性があるネットワーク ポートの集まりです。一般にクラスタ内の複数のノードのポートが含まれます。

次の図は、4ノード クラスタの3つのブロードキャスト ドメインにポートを割り当てている例を示します。

- 「Cluster」ブロードキャスト ドメインはクラスタの初期化中に自動的に作成され、クラスタ内の各ノードのポートaとbが含まれます。
- 「Default」ブロードキャスト ドメインもクラスタの初期化中に自動的に作成され、クラスタ内の各ノードのポートcとdが含まれます。
- レイヤ2ネットワークの到達可能性に基づいて、クラスタの初期化時にそれ以外のブロードキャスト ドメインが自動的に作成されます。これらのブロードキャスト ドメインの名前は、Default-1、Default-2のようになります。



それぞれのブロードキャスト ドメインと同じ名前で、同じネットワーク ポートを持つフェイルオーバー グループが自動的に作成されます。このフェイルオーバー グループはシステムによって自動的に管理されます。つまり、ブロードキャスト ドメインのポートが追加されたり削除されたりすると、フェイルオーバー グループのポートも同様に自動的に追加または削除されます。

ONTAPブロードキャスト ドメインを作成する

ブロードキャスト ドメインは、同じレイヤ2ネットワークに属するクラスタのネットワーク ポートをグループ化したものです。これらのポートは、SVMで使用されます。

ブロードキャスト ドメインはクラスタの作成時および追加時に自動的に作成されます。ONTAP 9.12.0以降では、自動的に作成されるブロードキャスト ドメインのほかに、ブロードキャスト ドメインをSystem Managerで手動で追加できます。

ONTAP 9.7以前のバージョンでは、ブロードキャストドメインの作成手順が異なります。ONTAP 9.7以前のバージョンを実行しているネットワークでブロードキャストドメインを作成する必要がある場合は、"ブロードキャスト ドメインの作成（ONTAP 9.7以前）"を参照してください。

開始する前に

ブロードキャスト ドメインに追加するポートは、他のブロードキャスト ドメインに属していないポートでなければなりません。使用するポートが別のブロードキャスト ドメインに属しているが、使用されていない場合は、元のブロードキャスト ドメインからそのポートを削除します。

タスク概要

- どのブロードキャスト ドメイン名もIPspace内で固有でなければなりません。

- 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、リンク アグリゲーション グループ / インターフェイス グループ（LAG / ifgrp）です。
- 使用するポートが別のブロードキャスト ドメインに属しているものの、使用されていない場合は、そのポートを新しいブロードキャスト ドメインに追加する前に既存のブロードキャスト ドメインから削除してください。
- ブロードキャスト ドメインに追加したポートの最大転送単位（MTU）は、ブロードキャスト ドメインに設定されているMTU値に更新されます。
- MTU値は、管理トラフィックを処理するe0Mポートを除き、そのレイヤ2ネットワークに接続されているすべてのデバイスで同じである必要があります。
- IPspace名を指定しない場合、ブロードキャスト ドメインは「Default」IPspaceに作成されます。

システムの設定を単純にするために、同じポートを含み、同じ名前の付いたフェイルオーバー グループが自動的に作成されます。

System Manager

手順

1. *ネットワーク > 概要 > ブロードキャスト ドメイン*を選択します。
2. ＋ Add をクリックします
3. ブロードキャスト ドメインの名前を指定します。
4. MTUを設定します。
5. IPspaceを選択します。
6. ブロードキャスト ドメインを保存します。

ブロードキャスト ドメインは追加後に編集または削除できます。

CLI

ONTAP 9.8以降を使用している場合、ブロードキャスト ドメインはレイヤ2の到達可能性に基づいて自動的に作成されます。詳細については、"ポートの到達可能性の修復"を参照してください。

ブロードキャスト ドメインを手動で作成することもできます。

手順

1. 現在ブロードキャスト ドメインに割り当てられていないポートを表示します。

   ```
   network port show
   ```

   表示が大きい場合は、 `network port show -broadcast-domain`コマンドを使用して、割り当てられていないポートのみを表示します。

2. ブロードキャスト ドメインを作成します。

   ```
   network port broadcast-domain create -broadcast-domain
   broadcast_domain_name -mtu mtu_value [-ipspace ipspace_name] [-ports
   ports_list]
   ```

   a. `broadcast_domain_name`は、作成するブロードキャスト ドメインの名前です。
   b. `mtu_value`はIPパケットのMTUサイズです。一般的な値は1500と9000です。

      この値は、このブロードキャスト ドメインに追加するすべてのポートに設定されます。

   c. `ipspace_name`は、このブロードキャスト ドメインが追加される IPspace の名前です。

      このパラメータの値を指定しないと、「Default」IPspaceが使われます。

   d. `ports_list`は、ブロードキャスト ドメインに追加されるポートのリストです。

      ポートは `node_name:port_number`の形式で追加されます（例： `node1:e0c`）。

3. 必要に応じて、ブロードキャスト ドメインが作成されたことを確認します。

   ```
   network port show -instance -broadcast-domain new_domain
   ```

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

例

次のコマンドは、「Default」IPspaceにブロードキャスト ドメインbcast1を作成し、MTUを1500に設定してポートを4つ追加します。

```
network port broadcast-domain create -broadcast-domain bcast1 -mtu 1500 -ports cluster1-01:e0e,cluster1-01:e0f,cluster1-02:e0e,cluster1-02:e0f
```

`network port broadcast-domain create`の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/network-port-broadcast-domain-create.html["ONTAPコマンド リファレンス"^]を参照してください。

終了後の操作

サブネットを作成することで、ブロードキャスト ドメインで使用可能なIPアドレスのプールを定義することも、この時点でSVMとインターフェイスをIPspaceに割り当てることもできます。詳細については、"クラスタとSVMのピアリング"を参照してください。

既存のブロードキャスト ドメインの名前を変更する必要がある場合は、 `network port broadcast-domain rename` コマンドを使用します。

`network port broadcast-domain rename`の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/network-port-broadcast-domain-rename.html["ONTAPコマンド リファレンス"^]を参照してください。

ONTAPブロードキャスト ドメインにポートを追加または削除する

ブロードキャスト ドメインはクラスタの作成時および追加時に自動的に作成されます。ブロードキャスト ドメインからポートを手動で削除する必要はありません。

物理的なネットワーク接続やスイッチ設定によってネットワーク ポートの到達可能性が変わり、ネットワーク ポートが属するブロードキャスト ドメインが変更になった場合は、次のトピックを参照してください。

"ポートの到達可能性の修復"

ONTAP 9.7以前のバージョンでは、ブロードキャストドメインのポートを追加または削除する手順が異なります。ONTAP 9.7以前のバージョンを実行しているネットワークでブロードキャストドメインのポートを追加または削除する必要がある場合は、"ブロードキャスト ドメインのポートの追加または削除（ONTAP 9.7以前）"を参照してください。

System Manager

ONTAP 9.14.1以降では、System Managerを使用してブロードキャスト ドメインにイーサネット ポートを再割り当てできます。イーサネット ポートはいずれも、ブロードキャスト ドメインに割り当てることを推奨します。そのため、あるブロードキャスト ドメインに対するイーサネット ポートの割り当てを解除した場合には、別のブロードキャスト ドメインに再割り当てする必要があります。

手順

イーサネット ポートを再割り当てするには、次の手順を実行します。

1. *ネットワーク > 概要*を選択します。
2. ブロードキャスト ドメイン セクションで、ドメイン名の横にある ⋮ を選択します。
3. ドロップダウン メニューで、*編集*を選択します。
4. *ブロードキャスト ドメインの編集*ページで、別のドメインに再割り当てするイーサネット ポートの選択を解除します。
5. 選択解除されたポートごとに、*イーサネット ポートの再割り当て*ウィンドウが表示されます。ポートを再割り当てするブロードキャスト ドメインを選択し、*再割り当て*を選択します。
6. 現在のブロードキャスト ドメインに割り当てるすべてのポートを選択し、変更を保存します。

CLI

物理的なネットワーク接続やスイッチ設定によってネットワーク ポートの到達可能性が変わり、ネットワーク ポートが属するブロードキャスト ドメインが変更になった場合は、次のトピックを参照してください。

"ポートの到達可能性の修復"

または、 `network port broadcast-domain add-ports`または `network port broadcast-domain remove-ports`コマンドを使用して、ブロードキャスト ドメインにポートを手動で追加または削除することもできます。

開始する前に

- このタスクを実行するには、クラスタ管理者である必要があります。
- ブロードキャスト ドメインに追加するポートは、他のブロードキャスト ドメインに属していないポートでなければなりません。
- すでにインターフェイス グループに属しているポートを個別にブロードキャスト ドメインに追加することはできません。

タスク概要

ネットワーク ポートの追加と削除には、次のルールがあります。

ポートを追加する場合…	ポートを削除する場合…
追加できるポートは、ネットワーク ポート、VLAN、インターフェイス グループ（ifgrp）です。	該当なし
ポートは、ブロードキャスト ドメインのシステム定義のフェイルオーバー グループに追加されます。	ポートは、ブロードキャスト ドメインのすべてのフェイルオーバー グループから削除されます。

ポートのMTUは、ブロードキャスト ドメインに設定されているMTU値に更新されます。	ポートのMTUは変更されません。
ポートのIPspaceは、ブロードキャスト ドメインのIPspace値に更新されます。	ポートは、ブロードキャスト ドメイン属性のない「Default」IPspaceに移動します。

`network port ifgrp remove-port`コマンドを使用してインターフェース グループの最後のメンバー ポートを削除すると、ブロードキャスト ドメインでは空のインターフェース グループ ポートは許可されないため、インターフェース グループ ポートがブロードキャスト ドメインから削除されます。 `network port ifgrp remove-port`の詳細については、"ONTAP コマンド リファレンス"を参照してください。

手順

1. `network port show`コマンドを使用して、ブロードキャスト ドメインに現在割り当てられているポートまたは割り当てられていないポートを表示します。
2. ブロードキャスト ドメインにポートを追加するか、ブロードキャスト ドメインからポートを削除します。

状況	方法
ブロードキャスト ドメインにポートを追加する	`network port broadcast-domain add-ports`
ブロードキャスト ドメインからポートを削除する	`network port broadcast-domain remove-ports`

3. ブロードキャスト ドメインのポートが追加または削除されたことを確認します。

```
network port show
```

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

ポートの追加と削除の例

次のコマンドは、Default IPspaceのブロードキャスト ドメインbcast1に、ノードcluster-1-01のポートe0gと、ノードcluster-1-02のe0gを追加します。

```
cluster-1::> network port broadcast-domain add-ports -broadcast-domain bcast1
-ports cluster-1-01:e0g,cluster1-02:e0g
```

次のコマンドは、Cluster IPspaceのブロードキャスト ドメインClusterに、クラスタ ポートを2つ追加します。

```
cluster-1::> network port broadcast-domain add-ports -broadcast-domain Cluster
-ports cluster-2-03:e0f,cluster2-04:e0f -ipspace Cluster
```

次のコマンドは、Default IPspaceのブロードキャスト ドメインbcast1から、ノードcluster1-01のポートe0eを削除します。

```
cluster-1::> network port broadcast-domain remove-ports -broadcast-domain
bcast1 -ports cluster-1-01:e0e
```

`network port broadcast-domain remove-ports`
の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/network-port-broadcast-domain-remove-ports.html["ONTAPコマンド リファレンス"^]をご覧ください。

関連情報

- "ONTAPコマンド リファレンス"

ONTAPポートの到達可能性を修復する

ブロードキャスト ドメインは自動的に作成されます。ただし、ポートのケーブル接続やスイッチの設定に変更があった場合は、ポートを別のブロードキャスト ドメイン（新規または既存）に修復しなければならないことがあります。

ONTAPは、ブロードキャスト ドメイン コンスティチュエントの（イーサネット ポートの）レイヤ2の到達可能性に基づいて、ネットワーク配線の問題を自動的に検出し、ソリューションを推奨します。

配線が正しくないと、ブロードキャスト ドメインのポートが想定どおりに割り当てられない可能性があります。ONTAP 9.10.1以降では、クラスタのセットアップ後や既存クラスタへの新しいノードの追加時にポートの到達可能性を確認することで、ネットワーク配線に問題がないかどうかが自動的に確認されます。

System Manager

ポートの到達可能性に問題が検出された場合、System Managerに問題を解決するための修復処理が提示されます。

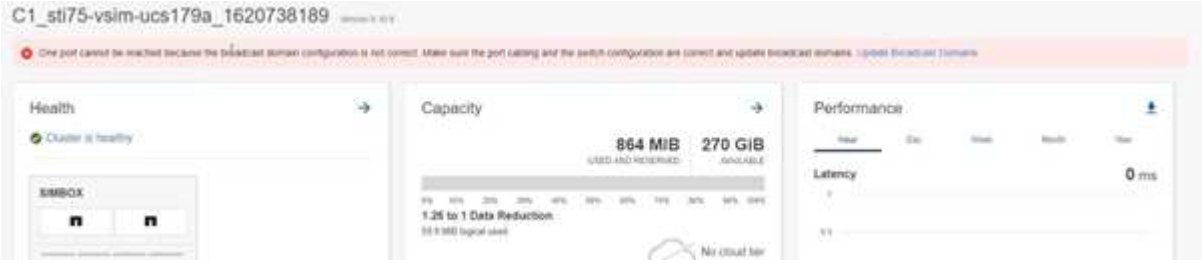
クラスタのセットアップ後は、ダッシュボードにネットワーク配線の問題が報告されます。

既存クラスタへの新しいノードの追加後は、[Nodes]ページにネットワーク配線の問題が表示されます。

ネットワーク図でネットワーク配線の状態を確認することもできます。ポートの到達可能性の問題があると、ネットワーク図に赤いエラー アイコンが表示されます。

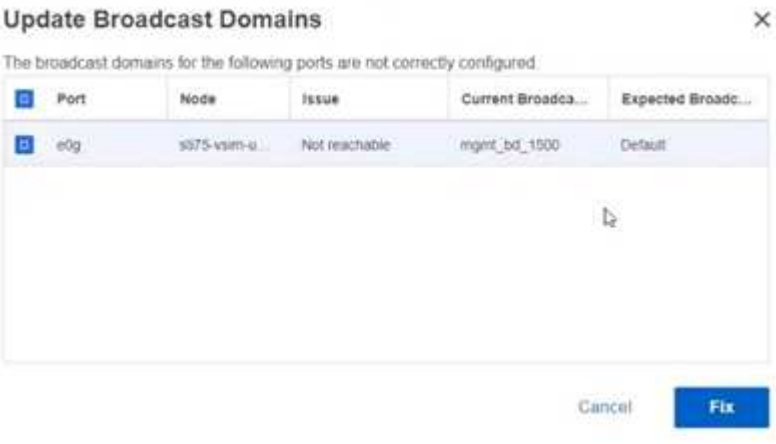
クラスタのセットアップ後

クラスタのセットアップ後にネットワーク配線の問題が検出されると、ダッシュボードにメッセージが表示されます。



手順

1. メッセージの指示に従って配線を修正します。
2. リンクをクリックすると、「ブロードキャストドメインの更新」ダイアログが起動します。「ブロードキャストドメインの更新」ダイアログが開きま

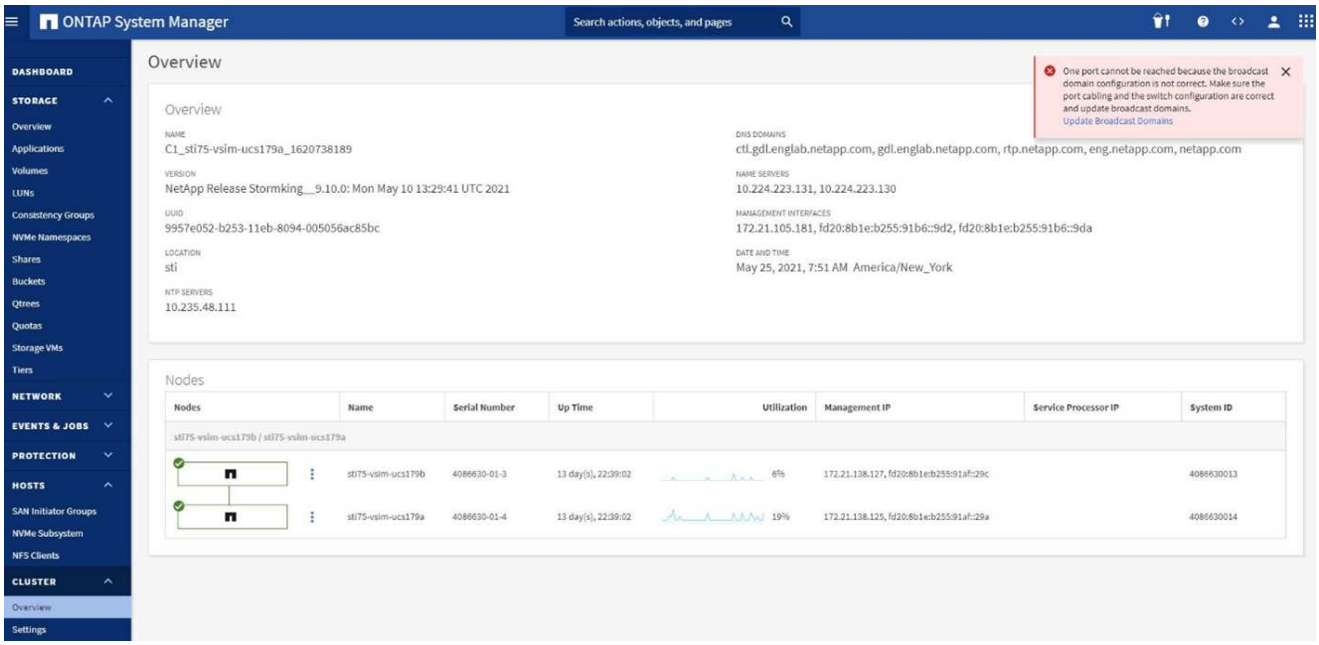


す。 ダイアログ"]

3. ノード、問題の内容、現在のブロードキャスト ドメイン、正しいブロードキャスト ドメインなど、ポートに関する情報を確認します。
4. 修復するポートを選択し、*Fix*をクリックします。システムはポートを現在のブロードキャストドメインから期待されるブロードキャストドメインに移動します。

ノードの追加後

クラスタに新しいノードを追加したあとにネットワーク配線の問題が検出されると、[Nodes]ページにメッセージが表示されます。



手順

1. メッセージの指示に従って配線を修正します。
2. リンクをクリックすると、「ブロードキャストドメインの更新」ダイアログが起動します。「ブロードキャストドメインの更新」ダイアログが開きま

す。 ダイアログ"]

3. ノード、問題の内容、現在のブロードキャスト ドメイン、正しいブロードキャスト ドメインなど、ポートに関する情報を確認します。
4. 修復するポートを選択し、**Fix** をクリックします。システムはポートを現在のブロードキャストドメインから期待されるブロードキャストドメインに移動します。

CLI

開始する前に

このタスクを実行するには、クラスタ管理者である必要があります。

タスク概要

検出されたレイヤ2の到達可能性に基づいてポートのブロードキャスト ドメイン設定を自動的に修復するコマンドが用意されています。

手順

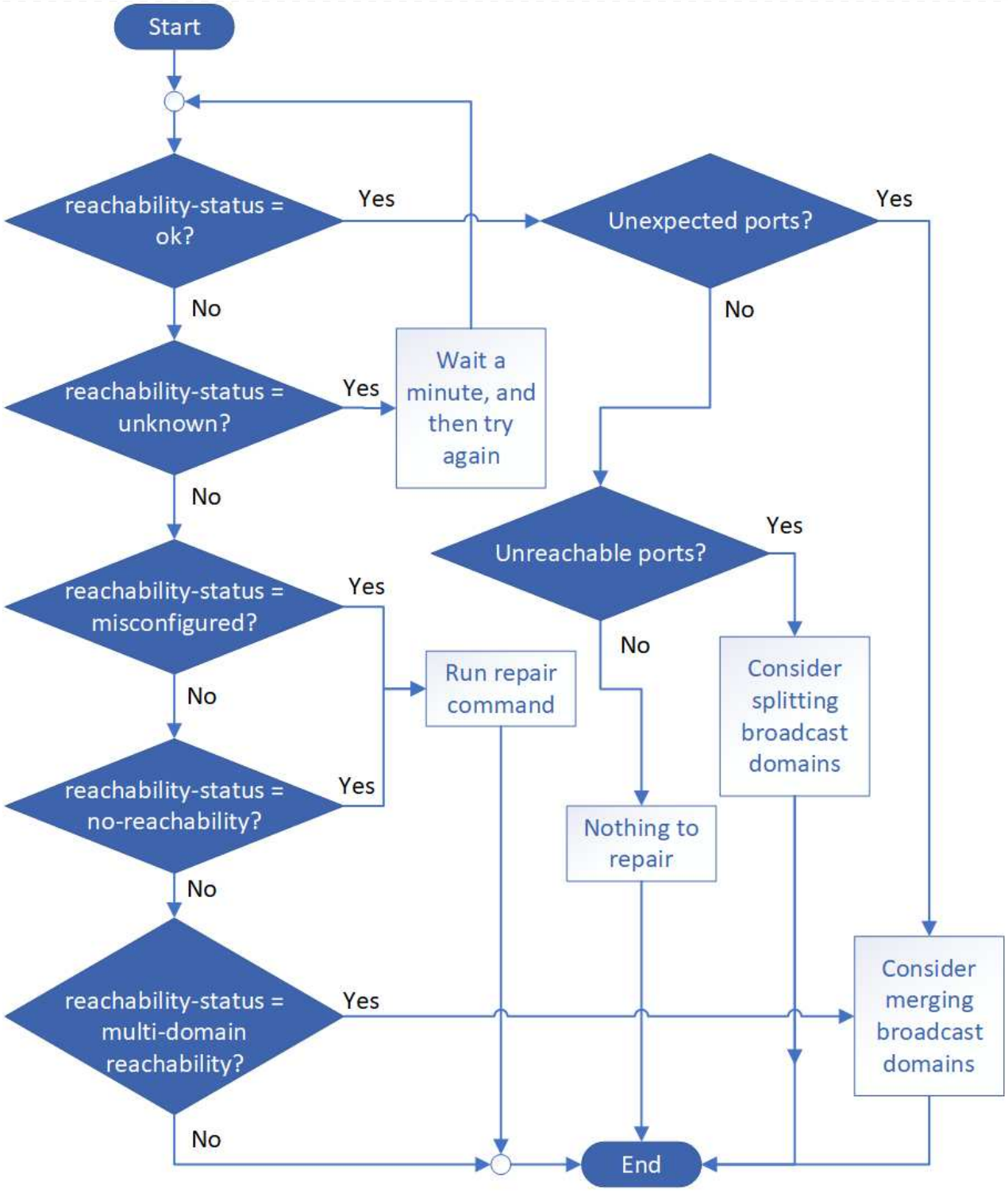
1. スイッチの設定とケーブル接続を確認します。
2. ポートの到達可能性を確認します。

   ```
   network port reachability show -detail -node -port
   ```

   コマンドの出力に到達可能性の結果が表示されます。

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

3. 次のデシジョン ツリーと表を参照して、到達可能性の結果を理解し、次に実行する手順を確認します。



到達可能性ステータス	概要

ok	ポートは割り当てられたブロードキャストドメインへのレイヤー2到達性を備えています。到達性ステータスが「ok」であっても「予期しないポート」がある場合は、1つ以上のブロードキャストドメインを統合することを検討してください。詳細については、次の_予期しないポート_の行を参照してください。 到達可能性ステータスが「ok」であるにもかかわらず、「到達不能ポート」が存在する場合は、1つ以上のブロードキャストドメインを分割することを検討してください。詳細については、次の_到達不能ポート_の行を参照してください。 到達可能性ステータスが「ok」で、かつ想定外のポートも到達不能なポートも存在しない場合、設定に問題はありません。
予期しないポート	ポートは割り当てられたブロードキャスト ドメインに対してレイヤ2到達可能性を持ちますが、少なくとも1つの他のブロードキャスト ドメインに対してもレイヤ2到達可能性を持ちます。 物理的な接続とスイッチの設定に間違いがないか、またはポートに割り当てられているブロードキャスト ドメインを1つ以上のブロードキャスト ドメインとマージする必要がないかを確認します。 詳細については、"ブロードキャスト ドメインのマージ"を参照してください。
到達不能なポート	単一のブロードキャストドメインが2つの異なる到達可能性セットに分割されている場合は、ブロードキャストドメインを分割してONTAP構成を物理ネットワークトポロジと同期できます。 通常、到達不能なポートは、物理的な構成とスイッチの設定に間違いがないことを確認したうえで、別のブロードキャスト ドメインにスプリットする必要があります。 詳細については、"ブロードキャスト ドメインのスプリット"を参照してください。
到達可能性の設定ミス	ポートは割り当てられたブロードキャスト ドメインに対してレイヤ2到達可能性を持ちませんが、別のブロードキャスト ドメインに対してはレイヤ2到達可能性を持ちます。 ポートの到達可能性を修復します。次のコマンドを実行すると、到達可能性があるブロードキャスト ドメインにポートが割り当てられます。 `network port reachability repair -node -port`

到達不能	ポートには、既存のブロードキャストドメインへのレイヤー2到達可能性がありません。
	
	ポートの到達可能性を修復します。次のコマンドを実行すると、デフォルトIPspaceに新しいブロードキャスト ドメインが自動的に作成され、ポートが割り当てられます。
	
	`network port reachability repair -node -port`
	
	注： すべてのインターフェースグループ（ifgrp）メンバーポートが `no-reachability`と報告されている場合、各メンバーポートで `network port reachability repair`コマンドを実行すると、各メンバーポートがifgrpから削除され、新しいブロードキャストドメインに配置され、最終的にはifgrp自体が削除されます。`network port reachability repair`コマンドを実行する前に、ポートの到達可能なブロードキャストドメインが、物理ネットワークトポロジに基づいて想定されるものであることを確認してください。
	
	`network port reachability repair`
	の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/network-port-reachability-repair.html["ONTAPコマンド リファレンス"^]をご覧ください。

マルチドメイン到達可能性	ポートは割り当てられたブロードキャスト ドメインに対してレイヤ2到達可能性を持ちますが、少なくとも1つの他のブロードキャスト ドメインに対してもレイヤ2到達可能性を持ちます。 物理的な接続とスイッチの設定に間違いがないか、またはポートに割り当てられているブロードキャスト ドメインを1つ以上のブロードキャスト ドメインとマージする必要がないかを確認します。 詳細については、"ブロードキャスト ドメインのマージ"を参照してください。
不明	到達可能性ステータスが「不明」の場合は、数分待ってからコマンドを再試行してください。

ポートを修復したあとに、孤立状態のLIFとVLANがないかを確認します。ポートがインターフェイス グループに属していた場合は、そのインターフェイス グループがどうなったかを把握する必要もあります。

LIF

ポートが修復されて別のブロードキャスト ドメインに移されると、そのポートに設定されていたLIFには新しいホーム ポートが自動的に割り当てられます。このホーム ポートは、同じノード上の同じブロードキャスト ドメインから選択されます（可能な場合）。または別のノードからホーム ポートが選択されることもあります。適切なホーム ポートがない場合、ホーム ポートはクリアされます。

LIFのホーム ポートが別のノードに移された場合、またはクリアされた場合、そのLIFは「孤立状態」とみなされます。孤立状態のLIFは次のコマンドで確認できます。

```
displaced-interface show
```

孤立状態のLIFがある場合は、次のいずれかを行う必要があります。

- 孤立状態のLIFのホームをリストアする。

  ```
  displaced-interface restore
  ```

- LIFのホームを手動で設定する。

  ```
  network interface modify -home-port -home-node
  ```

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

- 現在設定されているLIFのホームに問題がなければ、「displaced-interface」テーブルからエントリを削除する。

  ```
  displaced-interface delete
  ```

VLAN

修復されたポートにVLANがあった場合、それらのVLANは自動的に削除されますが、同時に「孤立状態（displaced）」として記録されます。孤立状態のVLANは次のコマンドで確認できます。

```
displaced-vlans show
```

孤立状態のVLANがある場合は、次のいずれかを行う必要があります。

- VLANを別のポートにリストアする。

  ```
  displaced-vlans restore
  ```

- 「displaced-vlans」テーブルからエントリを削除する。

  ```
  displaced-vlans delete
  ```

インターフェイス グループ

修復されたポートがインターフェイス グループに属していた場合は、そのインターフェイス グループから削除されます。このポートがインターフェイス グループに割り当てられていた唯一のメンバー ポートであった場合は、インターフェイス グループ自体が削除されます。

関連情報

- "Verify your network configuration after upgrading"
- "ネットワーク ポートの到達可能性の監視"
- "ONTAPコマンド リファレンス"

ONTAPブロードキャストドメインをIPspaceに移動する

ONTAP 9.8以降では、レイヤ2の到達可能性に基づいてシステムが作成したブロードキャストドメインを、作成したIPspaceに移動できます。

ブロードキャスト ドメインを移動する前に、ブロードキャスト ドメイン内のポートの到達可能性を確認する必要があります。

ポートの自動スキャンでは、相互に到達可能なポートを特定して同じブロードキャスト ドメインに配置することはできますが、適切なIPspaceを特定することはできません。ブロードキャスト ドメインがデフォルト以外のIPspaceに属している場合は、このセクションの手順に従ってそのドメインを手動で移動する必要があります。

開始する前に

ブロードキャストドメインは、クラスタの作成および参加操作の一環として自動的に設定されます。ONTAPは、「デフォルト」ブロードキャストドメインを、クラスタ内で最初に作成されたノードの管理インターフェイスのホームポートにレイヤー2接続されたポートのセットとして定義します。必要に応じて、他のブロードキャストドメインが作成され、**Default-1**、*Default-2*などの名前が付けられます。

既存のクラスタにノードを追加すると、そのネットワーク ポートはレイヤ2の到達可能性に基づいて既存のブロードキャスト ドメインに自動的に追加されます。既存のブロードキャスト ドメインに到達できない場合、ポートは1つ以上の新しいブロードキャスト ドメインに配置されます。

タスク概要

- クラスタLIFが設定されているポートは、自動的に「Cluster」IPspaceに配置されます。
- ノード管理LIFのホーム ポートに到達できるポートは、「Default」ブロードキャスト ドメインに配置されます。
- その他のブロードキャスト ドメインは、クラスタの作成時または追加時に自動的に作成されます。
- VLANやインターフェイス グループを追加すると、作成から約1分後に適切なブロードキャスト ドメインに自動的に配置されます。

手順

1. ブロードキャスト ドメイン内のポートの到達可能性を確認します。ONTAPはレイヤ2の到達可能性を自動で監視します。次のコマンドを使用して、各ポートがブロードキャスト ドメインに追加され、到達可能性が「ok」になっていることを確認します。

   ```
   network port reachability show -detail
   ```

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

2. 必要に応じて、ブロードキャスト ドメインを他のIPspaceに移動します。

   ```
   network port broadcast-domain move
   ```

   たとえば、ブロードキャスト ドメインを「Default」から「ips1」に移動する場合は、次のコマンドを使用します。

```
network port broadcast-domain move -ipspace Default -broadcast-domain Default
-to-ipspace ips1
```

関連情報

- "ネットワークポートのブロードキャストドメイン移動"

ONTAPブロードキャストドメインを分割する

物理的なネットワーク接続やスイッチ設定によってネットワーク ポートの到達可能性が変わり、単一のブロードキャスト ドメインに設定されていたネットワーク ポートのグループが到達可能性の異なる2つのグループに分かれた場合は、ブロードキャスト ドメインをスプリットしてONTAPの設定を物理的なネットワーク トポロジに合わせることができます。

ONTAP 9.7以前のバージョンでは、ブロードキャストドメインを分割する手順が異なります。ONTAP 9.7以前のバージョンを実行しているネットワークでブロードキャストドメインを分割する必要がある場合は、"ブロードキャスト ドメインのスプリット（ONTAP 9.7以前）"を参照してください。

ネットワークポートのブロードキャストドメインが複数の到達可能性セットに分割されているかどうかを確認するには、 `network port reachability show -details`コマンドを使用し、相互に接続されていないポート（「到達不能ポート」）に注目してください。通常、到達不能ポートのリストは、物理構成とスイッチ構成が正確であることを確認した後、別のブロードキャストドメインに分割する必要があるポートセットを定義します。"ONTAPコマンド リファレンス"の `network port reachability show`の詳細をご覧ください。

手順

ブロードキャスト ドメインを2つのブロードキャスト ドメインにスプリットします。

```
network port broadcast-domain split -ipspace <ipspace_name> -broadcast
-domain <broadcast_domain_name> -new-broadcast-domain
<broadcast_domain_name> -ports <node:port,node:port>
```

- `ipspace_name`は、ブロードキャストドメインが存在する ipspace の名前です。
- -`broadcast-domain`は、分割されるブロードキャスト ドメインの名前です。
- -`new-broadcast-domain`は、作成される新しいブロードキャスト ドメインの名前です。
- -`ports`は、新しいブロードキャスト ドメインに追加するノード名とポートです。

関連情報

- "network port broadcast-domain show"

ONTAPブロードキャストドメインをマージする

物理的なネットワーク接続やスイッチ設定によってネットワーク ポートの到達可能性が変わり、複数のブロードキャスト ドメインに設定されていた2つのグループのネットワーク ポートの到達可能性がすべて同じになった場合は、2つのブロードキャスト ドメイ

ンをマージしてONTAPの設定を物理的なネットワーク トポロジに合わせることができます。

> ONTAP 9.7以前のバージョンでは、ブロードキャストドメインをマージする手順が異なります。ONTAP 9.7以前のバージョンを実行しているネットワークでブロードキャストドメインをマージする必要がある場合は、"ブロードキャストドメインのマージ（ONTAP 9.7以前）"を参照してください。

複数のブロードキャストドメインが1つの到達可能性セットに属しているかどうかを確認するには、`network port reachability show -details`コマンドを使用し、別のブロードキャストドメインに設定されているポートのうち、実際に相互に接続されているポート（「予期しないポート」）に注目してください。通常、予期しないポートのリストは、物理構成とスイッチ構成が正確であることを確認した後、ブロードキャストドメインに統合する必要があるポートのセットを定義します。

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

手順

1つのブロードキャスト ドメインのポートを既存のブロードキャスト ドメインにマージします。

```
network port broadcast-domain merge -ipspace <ipspace_name> -broadcast
-domain <broadcast_domain_name> -into-broadcast-domain
<broadcast_domain_name>
```

- `ipspace_name`は、ブロードキャストドメインが存在するIPスペースの名前です。
- `-broadcast-domain`は、マージされるブロードキャストドメインの名前です。
- `-into-broadcast-domain`は、追加のポートを受信するブロードキャストドメインの名前です。

関連情報

- "ネットワークポートのブロードキャストドメイン統合"

ONTAPブロードキャストドメイン内のポートのMTU値を変更する

あるブロードキャスト ドメインのMTU値を変更することにより、そのブロードキャストドメインのすべてのポートのMTU値を変更できます。この操作は、ネットワークに加えられたトポロジの変更を反映させるために行います。

> ブロードキャスト ドメイン ポートのMTU値を変更する手順は、ONTAP 9.7以前のバージョンでは異なります。ONTAP 9.7以前を実行しているネットワークでブロードキャスト ドメイン ポートのMTU値を変更する必要がある場合は、"ブロードキャスト ドメインのポートのMTU値の変更（ONTAP 9.7以前）"を参照してください。

System Manager

ONTAP 9.12.1 以降では、System Manager を使用してブロードキャスト ドメインの MTU 値を変更し、そのブロードキャスト ドメイン内のすべてのポートの MTU 値を変更できます。

手順

1. *ネットワーク > ブロードキャスト ドメイン*を選択します。
2. ブロードキャスト ドメイン セクションで、MTU 値を変更するブロードキャスト ドメインの名前を選択します。
3. ブロードキャストドメイン内のすべてのポートの MTU 値を変更するかどうかを確認するプロンプトが表示されます。変更を続行するには、* Yes * をクリックします。
4. 必要に応じて MTU 値を変更し、変更を保存します。

   システムはブロードキャストドメイン内のすべてのポートに新しいMTU値を適用します。これにより、それらのポート上のトラフィックが短時間中断されます。

CLI

開始する前に

MTU値は、管理トラフィックを処理するe0Mポートを除き、そのレイヤ2ネットワークに接続されているすべてのデバイスで同じである必要があります。

タスク概要

MTU 値を変更すると、影響を受けるポート上のトラフィックが短時間中断されます。システムは、MTU を変更するには **y** と答える必要があるプロンプトを表示します。

手順

ブロードキャスト ドメインのすべてのポートのMTU値を変更します。

```
network port broadcast-domain modify -broadcast-domain
<broadcast_domain_name> -mtu <mtu_value> [-ipspace <ipspace_name>]
```

各値の意味は次のとおりです。

- `broadcast_domain` は、ブロードキャスト ドメインの名前です。
- `mtu`は IP パケットの MTU サイズです。一般的な値は 1500 と 9000 です。
- `ipspace`このブロードキャスト ドメインが存在する IPspace の名前です。このオプションに値を指定しない限り、「Default」IPspace が使用されます。

  次のコマンドは、ブロードキャスト ドメイン bcast1 内のすべてのポートの MTU を 9000 に変更します：

```
network port broadcast-domain modify -broadcast-domain <Default-1>
-mtu < 9000 >
Warning: Changing broadcast domain settings will cause a momentary
data-serving interruption.
Do you want to continue? {y|n}: <y>
```

関連情報

- "ネットワーク ポート ブロードキャスト ドメインの変更"

ONTAPブロードキャストドメインの表示

クラスタの各IPspace内にあるブロードキャスト ドメインのリストを表示できます。この出力には、それぞれのブロードキャスト ドメインのポートとMTU値のリストも含まれます。

ONTAP 9.7以前のバージョンでは、ブロードキャストドメインを表示する手順が異なります。ONTAP 9.7以前のバージョンを実行しているネットワークでブロードキャストドメインを表示する必要がある場合は、"ブロードキャストドメインを表示する（ONTAP 9.7以前）"を参照してください。

手順

クラスタのブロードキャスト ドメイン、および関連付けられているポートを表示します。

```
network port broadcast-domain show
```

次のコマンドは、クラスタのブロードキャスト ドメイン、および関連付けられているポートをすべて表示します。

```
network port broadcast-domain show
IPspace Broadcast                                 Update
Name    Domain Name  MTU   Port List              Status Details
------- ----------- -----  ---------------------- --------------
Cluster Cluster      9000
                            cluster-1-01:e0a       complete
                            cluster-1-01:e0b       complete
                            cluster-1-02:e0a       complete
                            cluster-1-02:e0b       complete
Default Default      1500
                            cluster-1-01:e0c       complete
                            cluster-1-01:e0d       complete
                            cluster-1-02:e0c       complete
                            cluster-1-02:e0d       complete
        Default-1    1500
                            cluster-1-01:e0e       complete
                            cluster-1-01:e0f       complete
                            cluster-1-01:e0g       complete
                            cluster-1-02:e0e       complete
                            cluster-1-02:e0f       complete
                            cluster-1-02:e0g       complete
```

次のコマンドは、Default-1というブロードキャスト ドメインのポートのうち、更新ステータスがerrorになっている（正しく更新されていない）ポートを表示します。

```
network port broadcast-domain show -broadcast-domain Default-1 -port
-update-status error

IPspace Broadcast                                 Update
Name    Domain Name  MTU   Port List              Status Details
------- ----------- -----  ---------------------- --------------
Default Default-1    1500
                            cluster-1-02:e0g       error
```

関連情報

- "network port broadcast-domain show"

ONTAPブロードキャストドメインを削除する

不要になったブロードキャスト ドメインは削除できます。削除することで、ブロードキャスト ドメインに関連付けられていたポートは「Default」IPspaceに移動します。

開始する前に

削除するブロードキャスト ドメインに、関連付けられているサブネット、ネットワーク インターフェイ

ス、SVMがないことを確認します。

タスク概要

- システムで作成された「Cluster」ブロードキャスト ドメインを削除することはできません。
- ブロードキャスト ドメインを削除すると、そのドメインに関連するフェイルオーバー グループもすべて削除されます。

実行する手順は、System ManagerとCLIのどちらのインターフェイスを使用するかによって異なります。

System Manager

ONTAP 9.12.0以降では、**System Manager**を使用してブロードキャストドメインを削除できます

ブロードキャスト ドメインにポートが含まれている場合やサブネットに関連付けられている場合は、削除オプションは表示されません。

手順

1. *ネットワーク > 概要 > ブロードキャスト ドメイン*を選択します。
2. 削除したいブロードキャスト ドメインの横にある *> 削除*を選択します。

CLI

CLIを使用してブロードキャスト ドメインを削除する

手順

ブロードキャスト ドメインを削除します。

```
network port broadcast-domain delete -broadcast-domain broadcast_domain_name
[-ipspace ipspace_name]
```

次のコマンドは、ipspace1というIPspaceのブロードキャスト ドメインDefault-1を削除します。

```
network port broadcast-domain delete -broadcast-domain Default-1 -ipspace
ipspace1
```

関連情報

- "network port broadcast-domain show"

フェイルオーバー グループとポリシー

ONTAPネットワーク上のLIFフェイルオーバーについて学ぶ

LIFのフェイルオーバーとは、LIFの現在のネットワーク ポートでリンク障害が発生したときに、別のネットワーク ポートにLIFを自動的に移行する機能のことです。これは、SVMとの接続の高可用性を実現するための重要な機能です。LIFのフェイルオーバーを設定する手順は、フェイルオーバー グループの作成、フェイルオーバー グループを使用するためのLIFの変更、およびフェイルオーバー ポリシーの指定に分かれています。

フェイルオーバー グループは、クラスタ内の1つ以上のノードのネットワーク ポート（物理ポート、VLAN、インターフェイス グループ）をまとめたものです。フェイルオーバー グループにあるネットワーク ポートによって、LIFで使用可能なフェイルオーバー ターゲットが決まります。フェイルオーバー グループには、クラスタ管理LIF、ノード管理LIF、クラスタ間LIF、およびNASデータLIFを割り当てることができます。

LIFが有効なフェイルオーバーターゲットなしで設定されている場合、LIFがフェイルオーバーを試行すると停止が発生します。 `network interface show -failover`コマンドを使用して、フェイルオーバー設定を確認できます。"ONTAPコマンド リファレンス"の `network interface show`の詳細をご覧ください。

ブロードキャスト ドメインを作成すると、同じネットワーク ポートを含み、同じ名前の付いたフェイルオーバー グループが自動的に作成されます。このフェイルオーバー グループはシステムによって自動的に管理されます。つまり、ブロードキャスト ドメインのポートが追加されたり削除されたりすると、フェイルオーバー グループのポートも同様に自動的に追加または削除されます。この機能によって、管理者が自分のフェイルオーバー グループを管理する手間を省くことができます。

ONTAPフェイルオーバー グループを作成する

ネットワーク ポートのフェイルオーバー グループを作成して、LIFの現在のポートでリンク障害が発生したときに、LIFが別のポートに自動的にフェイルオーバーされるようにします。これによりシステムは、ネットワーク トラフィックをクラスタの別の使用可能なポートに再ルーティングできます。

タスク概要

`network interface failover-groups create`コマンドを使用してグループを作成し、グループにポートを追加します。

- フェイルオーバー グループに追加できるポートは、ネットワーク ポート、VLAN、インターフェイス グループ（ifgrp）です。
- フェイルオーバー グループに追加するすべてのポートが、同じブロードキャスト ドメインに属している必要があります。
- 1つのポートを複数のフェイルオーバー グループで使用できます。
- 複数のLIFが異なるVLANやブロードキャスト ドメインに存在する場合は、VLANやブロードキャスト ドメインごとにフェイルオーバー グループを設定する必要があります。
- フェイルオーバー グループは、SANのiSCSI環境とFC環境には適用されません。

手順

フェイルオーバー グループを作成します。

```
network interface failover-groups create -vserver vserver_name -failover-group
failover_group_name -targets ports_list
```

- `*vserver_name*`は、フェイルオーバー グループを使用できる SVM の名前です。
- `*failover_group_name*`は、作成するフェイルオーバー グループの名前です。
- `*ports_list*`は、フェイルオーバー グループに追加されるポートのリストです。ポートは_node_name>:<port_number>_の形式で追加されます（例：node1:e0c）。

次のコマンドは、SVM vs3にフェイルオーバー グループfg3を作成してポートを2つ追加します。

```
network interface failover-groups create -vserver vs3 -failover-group fg3
-targets cluster1-01:e0e,cluster1-02:e0e
```

終了後の操作

- フェイル オーバーグループが作成されたら、フェイルオーバー グループをLIFに適用する必要があります。
- LIFに対応する有効なフェイルオーバー ターゲットがないフェイルオーバー グループを適用すると、警告メッセージが表示されます。

  有効なフェイルオーバー ターゲットのないLIFがフェイルオーバーしようとすると、システムが停止する可能性があります。

- `network interface failover-groups create`の詳細については、"ONTAPコマンド リファレンス"をご覧ください。

LIFでONTAPフェイルオーバー設定を構成する

フェイルオーバー ポリシーとフェイルオーバー グループをLIFに適用することにより、ネットワーク ポートの特定のグループにLIFがフェイルオーバーするように設定できます。また、LIFの別のポートへのフェイルオーバーを無効にすることもできます。

タスク概要

- LIFを作成するとLIFフェイルオーバーがデフォルトで有効になり、使用可能なターゲット ポートのリストが、LIFのタイプとサービス ポリシーに基づくデフォルトのフェイルオーバー グループとフェイルオーバー ポリシーによって決まります。

  9.5以降では、LIFを使用できるネットワーク サービスを定義するサービス ポリシーをLIFに指定できます。一部のネットワーク サービスでは、LIFのフェイルオーバーが制限されます。

  フェイルオーバーをそれまでよりも制限するようにLIFのサービス ポリシーを変更すると、LIFのフェイルオーバー ポリシーが自動的に更新されます。

- LIFのフェイルオーバーの動作は、network interface modifyコマンドの-failover-groupパラメータと-failover-policyパラメータの値を指定することによって変更できます。
- LIFの変更によって、LIFに有効なフェイルオーバー ターゲットがなくなる場合は警告メッセージが表示されます。

  有効なフェイルオーバー ターゲットのないLIFがフェイルオーバーしようとすると、システムが停止する可能性があります。

- ONTAP 9.11.1以降、オールフラッシュSANアレイ（ASA）プラットフォームでは、新規に作成したStorage VM上に新規に作成するiSCSI LIFで、iSCSI LIFフェイルオーバーが自動的に有効になります。

  さらに、"既存の iSCSI LIF で iSCSI LIF フェイルオーバーを手動で有効にする"ONTAP 9.11.1 以降にアップグレードする前に作成された LIF も対象となります。

- 次に、-failover-policyの設定によって、フェイルオーバー グループからどのターゲット ポートが選択されるかを示します。

> iSCSI LIF フェイルオーバーの場合、フェイルオーバーポリシー `local-only`、 `sfo-partner-only`、 `disabled`のみがサポートされます。

- `broadcast-domain-wide`フェイルオーバーグループ内のすべてのノードのすべてのポートに適用されます。
- `system-defined`LIF のホームノードと、クラスタ内の他の 1 つのノード（通常は SFO 以外のパートナー、存在する場合）のポートにのみ適用されます。
- `local-only`LIFのホームノード上のポートにのみ適用されます。
- `sfo-partner-only`LIFのホームノードとそのSFOパートナーのポートにのみ適用されます。
- `disabled` は、LIF がフェイルオーバー用に設定されていないことを示します。

手順

既存のインターフェイスのフェイルオーバーを設定します。

```
network interface modify -vserver <vserver_name> -lif <lif_name> -failover
-policy <failover_policy> -failover-group <failover_group>
```

フェイルオーバーの設定例、および無効化の例

次のコマンドは、フェイルオーバー ポリシーをbroadcast-domain-wideに設定し、SVM vs3のdata1というLIFのフェイルオーバー ターゲットとして、フェイルオーバー グループfg3のポートを使用します。

```
network interface modify -vserver vs3 -lif data1 -failover-policy
broadcast-domain-wide -failover-group fg3

network interface show -vserver vs3 -lif * -fields failover-
group,failover-policy

vserver lif              failover-policy       failover-group
------- -------------- ---------------        --------------
vs3     data1          broadcast-domain-wide  fg3
```

次のコマンドは、SVM vs3のdata1というLIFのフェイルオーバーを無効にします。

```
network interface modify -vserver vs3 -lif data1 -failover-policy disabled
```

関連情報

- "ネットワーク インターフェイス"

フェイルオーバー グループとポリシーを管理するためのONTAPコマンド

`network interface failover-groups`コマンドを使用してフェイルオーバー グループを管理できます。 `network interface modify`コマンドを使用して、LIFに適用されているフェイルオーバー グループとフェイルオーバー ポリシーを管理します。

状況	使用するコマンド
フェイルオーバー グループにネットワーク ポートを追加する	`network interface failover-groups add-targets`
フェイルオーバー グループからネットワーク ポートを削除する	`network interface failover-groups remove-targets`
フェイルオーバー グループのネットワーク ポートを変更する	`network interface failover-groups modify`
現在のフェイルオーバー グループを表示する	`network interface failover-groups show`
LIFのフェイルオーバーを設定する	`network interface modify -failover -group -failover-policy`
各LIFで使用されているフェイルオーバー グループとフェイルオーバー ポリシーを表示する	`network interface show -fields failover-group, failover-policy`
フェイルオーバー グループの名前を変更する	`network interface failover-groups rename`
フェイルオーバー グループを削除する	`network interface failover-groups delete`

フェイルオーバー グループを変更した結果、クラスタ内のどのLIFも有効なフェイルオーバー ターゲットを持たなくなってしまうと、LIFがフェイルオーバーしようとしたときにシステムが停止する可能性があります。

関連情報

- "ネットワーク インターフェイス"

サブネット（クラスタ管理者のみ）

ONTAPネットワークのサブネットについて学ぶ

サブネットを使用すると、ONTAPネットワーク設定用のIPアドレスの特定のブロックまたはプールを割り当てることができます。IPアドレスとネットワーク マスクの値を指定

しなくても、サブネット名を指定して簡単にLIFを作成できるようになります。

サブネットはブロードキャスト ドメイン内に作成され、同じレイヤ3サブネットに属するIPアドレスのプールを含んでいます。サブネット内のIPアドレスは、LIFの作成時にブロードキャスト ドメインのポートに割り当てられます。LIFを削除すると、そのIPアドレスはサブネット プールに返され、以降のLIFで使用できるようになります。

IPアドレスの管理が容易になり、LIFを簡単な手順で作成できるようになるため、サブネットを使用することをお勧めします。さらに、サブネットを定義するときにゲートウェイを指定した場合、そのサブネットを使用してLIFを作成すると、そのゲートウェイへのデフォルト ルートがSVMに自動的に追加されます。

ONTAPネットワークのサブネットを作成する

サブネットを作成してIPv4またはIPv6アドレスの特定のブロックを割り当てることができます。このサブネットは、あとでSVMのLIFを作成するときに使用します。

IPアドレスとネットワーク マスクの値をLIFごとに指定しなくても、サブネット名を指定して簡単にLIFを作成できるようになります。

開始する前に

このタスクを実行するには、クラスタ管理者である必要があります。

サブネットを追加するブロードキャスト ドメインとIPspaceが存在していなければなりません。

タスク概要

- すべてのサブネット名がIPspace内で一意である必要があります。
- IPアドレスの範囲をサブネットに割り当てるときは、別々のサブネットまたはホストで同じIPアドレスが使用されることのないように、ネットワーク内でIPアドレスの範囲が重複しないことを確認してください。
- サブネットの定義時にゲートウェイを指定すると、そのサブネットを使用してLIFを作成したときに、そのゲートウェイへのデフォルト ルートがSVMに自動的に追加されます。サブネットを使用しない場合、またはサブネットの定義時にゲートウェイを指定しない場合は、 `route create`コマンドを使用してSVMにルートを手動で追加する必要があります。
- NetApp は、データSVM上のすべてのLIFに対してサブネットオブジェクトを作成することを推奨しています。これは特にMetroCluster構成において重要です。サブネットオブジェクトには関連付けられたブロードキャストドメインがあるため、サブネットオブジェクトによってONTAPがデスティネーションクラスタ上のフェイルオーバーターゲットを判別できるようになります。

手順

ONTAP System Manager または ONTAP CLI を使用してサブネットを作成できます。

System Manager

ONTAP 9.12.0以降では、System Managerを使用してサブネットを作成できます。

手順

1. *Network > Overview > Subnets*を選択します。
2. + Add をクリックしてサブネットを作成します。
3. サブネットの名前を指定します。
4. サブネットのIPアドレスを指定します。
5. サブネット マスクを設定します。
6. サブネットを構成するIPアドレスの範囲を定義します。
7. 必要に応じて、ゲートウェイを指定します。
8. サブネットが属するブロードキャスト ドメインを選択します。
9. 変更を保存します。
   a. 入力したIPアドレスまたは範囲がすでにインターフェイスで使用されている場合は、次のメッセージが表示されます：
   `An IP address in this range is already in use by a LIF. Associate the LIF with this subnet?`
   b. *OK*をクリックすると、既存のLIFがサブネットに関連付けられます。

CLI

CLIを使用してサブネットを作成します。

```
network subnet create -subnet-name subnet_name -broadcast-domain
<broadcast_domain_name> [- ipspace <ipspace_name>] -subnet
<subnet_address> [-gateway <gateway_address>] [-ip-ranges
<ip_address_list>] [-force-update-lif-associations <true>]
```

- `subnet_name` は、作成するレイヤー 3 サブネットの名前です。

  「Mgmt」のようなテキスト文字列形式の名前を付けることも、192.0.2.0/24などのサブネットのIPアドレスの値にすることもできます。

- `broadcast_domain_name`は、サブネットが存在するブロードキャスト ドメインの名前です。
- `ipspace_name`は、ブロードキャスト ドメインが含まれる IPspace の名前です。

  このオプションの値を設定しないと、「Default」IPspaceが使われます。

- `subnet_address`は、サブネットのIPアドレスとマスクです（例：192.0.2.0/24）。
- `gateway_address`は、サブネットのデフォルト ルートのゲートウェイです（例：192.0.2.1）。
- `ip_address_list`は、サブネットに割り当てられる IP アドレスのリストまたは範囲です。

  個別のIPアドレス、IPアドレスの範囲、またはその組み合わせをカンマで区切って指定できます。

- `-force-update-lif-associations`オプションには `true`の値を設定できます。

  指定した範囲のIPアドレスを現在使用しているサービス プロセッサまたはネットワーク インターフェイスがある場合は、コマンドが失敗します。上記のオプションの値をtrueにすることで、手動でアドレスが指定されているインターフェイスが現在のサブネットに関連付けられ、コマンドは問題なく実行されます。

次のコマンドは、Default IPspaceのブロードキャスト ドメインDefault-1にsub1というサブネットを作成します。サブネットのIPv4アドレスとマスク、ゲートウェイ、IPアドレスの範囲を指定しています。

```
network subnet create -subnet-name sub1 -broadcast-domain Default-1
-subnet 192.0.2.0/24 - gateway 192.0.2.1 -ip-ranges 192.0.2.1-
192.0.2.100, 192.0.2.122
```

次のコマンドは、「Default」IPspaceのブロードキャスト ドメインDefaultにsub2というサブネットを作成します。IPv6アドレスの範囲を指定しています。

```
network subnet create -subnet-name sub2 -broadcast-domain Default
-subnet 3FFE::/64 - gateway 3FFE::1 -ip-ranges "3FFE::10-3FFE::20"
```

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

終了後の操作

サブネット内のアドレスを使用して、SVMとインターフェイスをIPspaceに割り当てることができます。

既存のサブネットの名前を変更する必要がある場合は、 `network subnet rename` コマンドを使用します。

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

ONTAPネットワークのサブネットにIPアドレスを追加または削除する

新しくサブネットを作成するときにIPアドレスを追加したり、既存のサブネットにIPアドレスを追加したりできます。また、既存のサブネットからIPアドレスを削除することもできます。このようにして、SVMに必要なIPアドレスだけが割り当てられるようにします。

実行する手順は、System ManagerとCLIのどちらのインターフェイスを使用するかによって異なります。

System Manager

ONTAP 9.12.0以降では、**System Manager**を使用してサブネットに**IP**アドレスを追加したり、サブネットから**IP**アドレスを削除したりすることができます。

手順

1. *Network > Overview > Subnets*を選択します。
2. **⋮ > Edit** を変更するサブネットの横で選択します。
3. IPアドレスを追加または削除します。
4. 変更を保存します。
   a. 入力したIPアドレスまたは範囲がすでにインターフェイスで使用されている場合は、次のメッセージが表示されます：
      `An IP address in this range is already in use by a LIF. Associate the LIF with this subnet?`
   b. *OK*をクリックすると、既存のLIFがサブネットに関連付けられます。

CLI

CLI を使用してサブネットに **IP** アドレスを追加または削除する

タスク概要

IPアドレスを追加する際、追加する範囲のIPアドレスをサービス プロセッサまたはネットワーク インターフェイスが使用している場合、エラーが発生します。手動でアドレスを指定したインターフェイスを現在のサブネットに関連付ける場合は、 `-force-update-lif-associations`オプションを `true`に設定してください。

IPアドレスを削除する際、削除するIPアドレスを使用しているサービス プロセッサまたはネットワーク インターフェイスがある場合はエラーが発生します。サブネットから削除された後もインターフェイスでIPアドレスを引き続き使用したい場合は、 `-force-update-lif-associations`オプションを `true`に設定してください。

手順

サブネットのIPアドレスを追加または削除します。

状況	使用するコマンド
サブネットにIPアドレスを追加する	ネットワークサブネットの範囲追加
サブネットからIPアドレスを削除する	ネットワーク サブネット削除範囲

次のコマンドは、192.0.2.82～192.0.2.85のIPアドレスをサブネットsub1に追加します。

```
network subnet add-ranges -subnet-name <sub1> -ip-ranges <192.0.2.82-
192.0.2.85>
```

次のコマンドは、IPアドレス198.51.100.9をサブネットsub3から削除します。

```
network subnet remove-ranges -subnet-name <sub3> -ip-ranges
<198.51.100.9>
```

現在のIPアドレスの範囲が1～10と20～40で、追加するアドレスが11～19と41～50（つまり、1～50を範囲にする）の場合は、次のコマンドを使って既存のアドレスの範囲に重複させることができます。このコマンドは新しい範囲のアドレスだけを追加し、既存のアドレスには影響しません。

```
network subnet add-ranges -subnet-name <sub3> -ip-ranges <198.51.10.1-
198.51.10.50>
```

`network subnet add-ranges`および `network subnet remove-ranges`の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/search.html?q=network+subnet["ONTAPコマンド リファレンス"^]をご覧ください。

ONTAPネットワークのサブネットプロパティを変更する

既存のサブネットのアドレスとマスク値、ゲートウェイ アドレス、IPアドレスの範囲を変更することができます。

タスク概要

- IPアドレスを変更するときは、別々のサブネットまたはホストで同じIPアドレスが使用されることのないように、ネットワーク内でIPアドレスの範囲が重複しないことを確認してください。
- ゲートウェイのIPアドレスを追加または変更した場合は、LIFを作成するときに、変更したゲートウェイがサブネットを使用して新しいSVMに設定されます。SVMのゲートウェイへのルートがない場合は、デフォルト ルートが作成されます。ゲートウェイのIPアドレスを変更した場合は、SVMに新しいルートを手動で追加する必要があります。

実行する手順は、System ManagerとCLIのどちらのインターフェイスを使用するかによって異なります。

System Manager

ONTAP 9.12.0以降では、**System Manager**を使用してサブネットのプロパティを変更できます

手順

1. *Network > Overview > Subnets*を選択します。
2. 変更したいサブネットの横にある*> 編集*を選択します。
3. 変更を行います。
4. 変更を保存します。
   a. 入力したIPアドレスまたは範囲がすでにインターフェイスで使用されている場合は、次のメッセージが表示されます：
   `An IP address in this range is already in use by a LIF. Associate the LIF with this subnet?`
   b. *OK*をクリックすると、既存のLIFがサブネットに関連付けられます。

CLI

CLI を使用してサブネットのプロパティを変更する

手順

サブネットのプロパティを変更します。

```
network subnet modify -subnet-name <subnet_name> [-ipspace
<ipspace_name>] [-subnet <subnet_address>] [-gateway <gateway_address>]
[-ip-ranges <ip_address_list>] [-force-update-lif-associations <true>]
```

- `subnet_name` は、変更するサブネットの名前です。
- `ipspace`は、サブネットが存在する IPspace の名前です。
- `subnet`は、該当する場合、サブネットの新しいアドレスとマスクです（例：192.0.2.0/24）。
- `gateway`は、該当する場合、サブネットの新しいゲートウェイです（例：192.0.2.1）。*""*と入力すると、ゲートウェイ エントリが削除されます。
- `ip_ranges`は、該当する場合、サブネットに割り当てられるIPアドレスの新しいリストまたは範囲です。IPアドレスは、個々のアドレス、IPアドレスの範囲、またはカンマ区切りのリストでの組み合わせを指定できます。ここで指定した範囲によって、既存のIPアドレスが置き換えられます。
- `force-update-lif-associations`は、IPアドレス範囲を変更する場合に必要です。IPアドレスの範囲を変更する際に、このオプションの値を*true*に設定できます。指定された範囲のIPアドレスをサービス プロセッサまたはネットワーク インターフェイスが使用している場合、このコマンドは失敗します。この値を*true*に設定すると、手動でアドレス指定されたインターフェイスが現在のサブネットに関連付けられ、コマンドが成功します。

次のコマンドは、sub3というサブネットのゲートウェイのIPアドレスを変更します。

```
network subnet modify -subnet-name <sub3> -gateway <192.0.3.1>
```

`network subnet modify`の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/network-subnet-modify.html["ONTAPコマンド リファレンス"^]をご覧ください。

ONTAPネットワークのサブネットを表示する

IPspace内の各サブネットに割り当てられているIPアドレスのリストを表示することができます。この出力には、各サブネットの使用可能なIPアドレスの総数、および現在使用されているIPアドレスの数も表示されます。

実行する手順は、System ManagerとCLIのどちらのインターフェイスを使用するかによって異なります。

System Manager

ONTAP 9.12.0以降では、**System Manager**を使用してサブネットを表示できます

手順

1. *Network > Overview > Subnets*を選択します。
2. サブネットのリストを確認します。

CLI

CLI を使用してサブネットを表示する

手順

サブネットのリスト、およびそれらのサブネットで使用されている関連付けられたIPアドレスの範囲を表示します。

```
network subnet show
```

次のコマンドは、サブネット、およびそのプロパティを表示します。

```
network subnet show

IPspace: Default
Subnet                  Broadcast               Avail/
Name    Subnet          Domain    Gateway       Total   Ranges
------  --------------- --------- ------------ --------
-----------------------
sub1    192.0.2.0/24     bcast1   192.0.2.1     5/9     192.0.2.92-
192.0.2.100
sub3    198.51.100.0/24  bcast3   198.51.100.1   3/3
198.51.100.7,198.51.100.9
```

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

ONTAPネットワークからサブネットを削除する

サブネットが不要になり、そのサブネットのIPアドレスの割り当てを解除したい場合は、サブネットを削除します。

実行する手順は、System ManagerとCLIのどちらのインターフェイスを使用するかによって異なります。

System Manager

ONTAP 9.12.0以降では、**System Manager**を使用してサブネットを削除できます

手順

1. *Network > Overview > Subnets*を選択します。
2. 削除するサブネットの横にある *> 削除*を選択します。
3. 変更を保存します。

CLI

CLI を使用してサブネットを削除する

タスク概要

指定した範囲のIPアドレスを現在使用しているサービス プロセッサまたはネットワーク インターフェイスがある場合は、エラーが表示されます。サブネットを削除したあとも、インターフェイスでそのIPアドレスを使用する場合は、-force-update-lif-associationsオプションをtrueに設定して、サブネットのLIFとの割り当てを解除します。

手順

サブネットを削除します。

```
network subnet delete -subnet-name subnet_name [-ipspace ipspace_name] [-
force-update-lif- associations true]
```

次のコマンドは、ipspace1というIPspaceのサブネットsub1を削除します。

```
network subnet delete -subnet-name sub1 -ipspace ipspace1
```

`network subnet delete`の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/network-subnet-delete.html["ONTAPコマンド リファレンス"^]をご覧ください。

ONTAPネットワーク用のSVMを作成する

クライアントにデータを提供するには、SVMを作成する必要があります。

開始する前に

- このタスクを実行するには、クラスタ管理者である必要があります。
- SVMのルート ボリュームに設定するセキュリティ形式を決めておく必要があります。

  このSVMにHyper-V over SMBまたはSQL Server over SMBソリューションを実装する予定がある場合は、ルート ボリュームにNTFSセキュリティ形式を使用してください。Hyper-VファイルまたはSQLデータベース ファイルを格納するボリュームは、作成時にNTFSセキュリティ形式に設定する必要があります。ルート ボリュームのセキュリティ形式をNTFSに設定することで、UNIXセキュリティ形式またはmixedセキュリティ形式のデータ ボリュームを誤って作成することがなくなります。

- ONTAP 9.13.1以降では、ストレージVMの最大容量を設定できます。また、SVMの容量がしきい値に近づいた場合にアラートを設定することもできます。詳細については、SVMの容量の管理を参照してください。

System Manager

System Managerを使用してStorage VMを作成できます。

手順

1. **Storage VM** を選択します。
2. + Add をクリックしてストレージ VM を作成します。
3. Storage VMの名前を指定します。
4. アクセス プロトコルを選択します。
   - SMB / CIFS、NFS
   - iSCSI
   - FC
   - NVMe
     i. **SMB/CIFS** を有効にする を選択した場合は、次の設定を完了します：

フィールドまたはチェックボックス	概要
管理者名	SMB/CIFS ストレージ VM の管理者ユーザ名を指定します。
パスワード	SMB/CIFS ストレージ VM の管理者パスワードを指定します。
サーバ名	SMB/CIFS ストレージ VM のサーバ名を指定します。
Active Directory ドメイン	SMB/CIFS ストレージ VM のユーザ認証を提供するための Active Directory ドメインを指定します。
組織単位	SMB/CIFS サーバに関連付けられている Active Directory ドメイン内の組織単位を指定します。「CN=Computers」はデフォルト値ですが、変更できます。
ストレージVM内の共有にアクセスする際にデータを暗号化します	SMB 3.0 を使用してデータを暗号化し、SMB/CIFS ストレージ VM 内の共有への不正なファイル アクセスを防ぐには、このチェック ボックスをオンにします。
ドメイン	SMB/CIFS ストレージ VM にリストされているドメインを追加、削除、または並べ替えます。
ネーム サーバ	SMB/CIFS ストレージ VM のネーム サーバーを追加、削除、または並べ替えます。

デフォルト言語	Storage VM とそのボリュームのデフォルトの言語エンコード設定を指定します。Storage VM内の個々のボリュームの設定を変更する場合はCLIを使用してください。
ネットワーク インターフェイス	ストレージVM用に設定するネットワークインターフェイスごとに、既存のサブネット（少なくとも1つ存在する場合）を選択するか、*Without a subnet*を指定して、*IP Address*と*Subnet Mask*のフィールドに入力します。必要に応じて、*Use the same subnet mask and gateway for all of the following interfaces*チェックボックスをオンにしてください。ホームポートはシステムによって自動的に選択されるようにすることも、リストから使用するポートを手動で選択することもできます。
管理者アカウントの管理	ストレージVM管理者アカウントを管理する場合は、このチェックボックスをオンにします。オンにした場合は、ユーザ名とパスワードを指定してパスワードを確認し、ストレージVM管理用のネットワーク インターフェイスを追加するかどうかを指定します。

1. **Enable NFS** を選択した場合は、次の設定を完了します。

フィールドまたはチェックボックス	概要
NFSクライアントアクセスを許可するチェックボックス	NFSストレージVM上に作成されたすべてのボリュームがマウントおよびトラバースにルートボリュームパス「/」を使用する場合は、このチェックボックスをオンにします。エクスポートポリシー「default」にルールを追加して、マウントトラバースが中断されないようにします。

ルール	+ Add をクリックしてルールを作成します。 • クライアント仕様：ホスト名、IP アドレス、ネットグループ、またはドメインを指定します。 • アクセス プロトコル：次のオプションの組み合わせを選択します。 ◦ SMB / CIFS ◦ FlexCache ◦ NFS ▪ NFSv3 ▪ NFSv4 • アクセス詳細：ユーザのタイプごとに、読み取り専用、読み取り/書き込み、スーパーユーザのいずれかのアクセス レベルを指定します。ユーザのタイプには次のものがあります： ◦ All ◦ All (as anonymous user) ◦ UNIX ◦ Kerberos 5 ◦ Kerberos 5i ◦ Kerberos 5p ◦ NTLM ルールを保存します。
デフォルト言語	Storage VM とそのボリュームのデフォルトの言語エンコード設定を指定します。Storage VM内の個々のボリュームの設定を変更する場合はCLIを使用してください。
ネットワーク インターフェイス	ストレージVM用に設定するネットワークインターフェイスごとに、既存のサブネット（少なくとも1つ存在する場合）を選択するか、*Without a subnet*を指定して、*IP Address*と*Subnet Mask*のフィールドに入力します。必要に応じて、*Use the same subnet mask and gateway for all of the following interfaces*チェックボックスをオンにしてください。ホームポートはシステムによって自動的に選択されるようにすることも、リストから使用するポートを手動で選択することもできます。

管理者アカウントの管理	ストレージVM管理者アカウントを管理する場合は、このチェックボックスをオンにします。オンにした場合は、ユーザ名とパスワードを指定してパスワードを確認し、ストレージVM管理用のネットワーク インターフェイスを追加するかどうかを指定します。

1. **iSCSI** を有効にする を選択した場合は、次の設定を完了します：

フィールドまたはチェックボックス	概要
ネットワーク インターフェイス	ストレージVM用に設定するネットワークインターフェイスごとに、既存のサブネット（少なくとも1つ存在する場合）を選択するか、*Without a subnet*を指定して、*IP Address*と*Subnet Mask*のフィールドに入力します。必要に応じて、*Use the same subnet mask and gateway for all of the following interfaces*チェックボックスをオンにしてください。ホームポートはシステムによって自動的に選択されるようにすることも、リストから使用するポートを手動で選択することもできます。
管理者アカウントの管理	ストレージVM管理者アカウントを管理する場合は、このチェックボックスをオンにします。オンにした場合は、ユーザ名とパスワードを指定してパスワードを確認し、ストレージVM管理用のネットワーク インターフェイスを追加するかどうかを指定します。

1. **FC** を有効にする を選択した場合は、次の設定を完了します：

フィールドまたはチェックボックス	概要
FCポートの設定	ストレージVMに含めるノード上のネットワークインターフェースを選択します。ノードごとに2つのネットワークインターフェースが推奨されます。
管理者アカウントの管理	ストレージVM管理者アカウントを管理する場合は、このチェックボックスをオンにします。オンにした場合は、ユーザ名とパスワードを指定してパスワードを確認し、ストレージVM管理用のネットワーク インターフェイスを追加するかどうかを指定します。

1. **NVMe/FC** を有効にする を選択した場合は、次の構成を完了します：

フィールドまたはチェックボックス	概要

FCポートの設定	ストレージVMに含めるノード上のネットワークインターフェースを選択します。ノードごとに2つのネットワークインターフェースが推奨されます。
管理者アカウントの管理	ストレージVM管理者アカウントを管理する場合は、このチェックボックスをオンにします。オンにした場合は、ユーザ名とパスワードを指定してパスワードを確認し、ストレージVM管理用のネットワーク インターフェイスを追加するかどうかを指定します。

1. **NVMe/TCP** を有効にする を選択した場合は、次の構成を完了します：

フィールドまたはチェックボックス	概要
ネットワーク インターフェイス	ストレージVM用に設定するネットワークインターフェイスごとに、既存のサブネット（少なくとも1つ存在する場合）を選択するか、*Without a subnet*を指定して、*IP Address*と*Subnet Mask*のフィールドに入力します。必要に応じて、*Use the same subnet mask and gateway for all of the following interfaces*チェックボックスをオンにしてください。ホームポートはシステムによって自動的に選択されるようにすることも、リストから使用するポートを手動で選択することもできます。
管理者アカウントの管理	ストレージVM管理者アカウントを管理する場合は、このチェックボックスをオンにします。オンにした場合は、ユーザ名とパスワードを指定してパスワードを確認し、ストレージVM管理用のネットワーク インターフェイスを追加するかどうかを指定します。

1. 変更を保存します。

CLI

ONTAP CLIを使用してサブネットを作成します。

手順

1. SVMのルート ボリュームを格納するためのアグリゲートを決定します。

   ```
   storage aggregate show -has-mroot false
   ```

   ルート ボリュームを格納するための空きスペースが1GB以上あるアグリゲートを選択する必要があります。SVMでNASの監査を設定する場合は、ルート アグリゲートに少なくとも3GBの追加の空きスペースと、監査を有効にしたときに監査ステージング ボリュームの作成に使用される追加のスペースが必要です。

既存のSVMでNASの監査がすでに有効になっている場合は、アグリゲートの作成が完了したあとすぐにアグリゲートのステージング ボリュームが作成されます。

2. SVMのルート ボリュームを作成するアグリゲートの名前を控えます。
3. SVMを作成するときに言語を指定する予定であり、使用する値がわからない場合は、指定する言語の値を確認し、その値を控えます。

   ```
   vserver create -language ?
   ```

4. SVMの作成時にSnapshotポリシーを指定する予定があり、ポリシーの名前がわからない場合は、使用可能なポリシーを一覧表示し、使用するSnapshotポリシーの名前を特定して記録します：

   ```
   volume snapshot policy show -vserver vserver_name
   ```

5. SVMを作成するときにクォータ ポリシーを指定する予定であり、ポリシーの名前がわからない場合は、使用可能なポリシーの一覧を表示し、使用するクォータ ポリシーの名前を確認して、その名前を控えます。

   ```
   volume quota policy show -vserver vserver_name
   ```

6. SVMを作成します。

   ```
   vserver create -vserver vserver_name -aggregate aggregate_name -rootvolume
   root_volume_name -rootvolume-security-style {unix|ntfs|mixed} [-ipspace
   IPspace_name] [-language <language>] [-snapshot-policy
   snapshot_policy_name] [-quota-policy quota_policy_name] [-comment comment]
   ```

   ```
   vserver create -vserver vs1 -aggregate aggr3 -rootvolume vs1_root
   -rootvolume-security-style ntfs -ipspace ipspace1 -language
   en_US.UTF-8
   ```

   ```
   [Job 72] Job succeeded: Vserver creation completed
   ```

7. SVMの設定が正しいことを確認します。

   ```
   vserver show -vserver vs1
   ```

```
Vserver: vs1
Vserver Type: data
Vserver Subtype: default
Vserver UUID: 11111111-1111-1111-1111-111111111111
Root Volume: vs1_root
Aggregate: aggr3
NIS Domain: -
Root Volume Security Style: ntfs
LDAP Client: -
Default Volume Language Code: en_US.UTF-8
Snapshot Policy: default
Comment:
Quota Policy: default
List of Aggregates Assigned: -
Limit on Maximum Number of Volumes allowed: unlimited
Vserver Admin State: running
Vserver Operational State: running
Vserver Operational State Stopped Reason: -
Allowed Protocols: nfs, cifs, ndmp
Disallowed Protocols: fcp, iscsi
QoS Policy Group: -
Config Lock: false
IPspace Name: ipspace1
Is Vserver Protected: false
```

この例では、コマンドを実行すると「vs1」という名前のSVMがIPspace「ipspace1」に作成されます。ルート ボリュームは、「vs1_root」という名前で、NTFSセキュリティ形式を使用してaggr3に作成されます。

ONTAP 9.13.1以降では、アダプティブQoSポリシーグループテンプレートを設定して、SVM内のボリュームにスループットの下限と上限を適用できます。このポリシーは、SVMを作成した後にのみ適用できます。このプロセスの詳細については、アダプティブ ポリシー グループ テンプレートの設定を参照してください。

論理インターフェイス（LIF）

LIFの概要

ONTAPクラスタのLIF構成について学ぶ

LIF（論理インターフェイス）は、クラスタ内のノードへのネットワーク アクセス ポイントを表します。LIFは、クラスタでネットワーク経由の通信の送受信に使用されるポートに設定できます。

クラスタ管理者は、LIFの作成、表示、変更、移行、リバート、削除を行うことができます。SVM管理者は、SVMに関連付けられているLIFだけを表示できます。

LIFは、サービス ポリシー、ホーム ポート、ホーム ノード、フェイルオーバー先のポートのリスト、ファイアウォール ポリシーなどの特性が関連付けられているIPアドレスまたはWWPNです。LIFは、クラスタでネットワーク経由の通信の送受信に使用されるポートに設定できます。

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。

LIFをホストできるポートは次のとおりです。

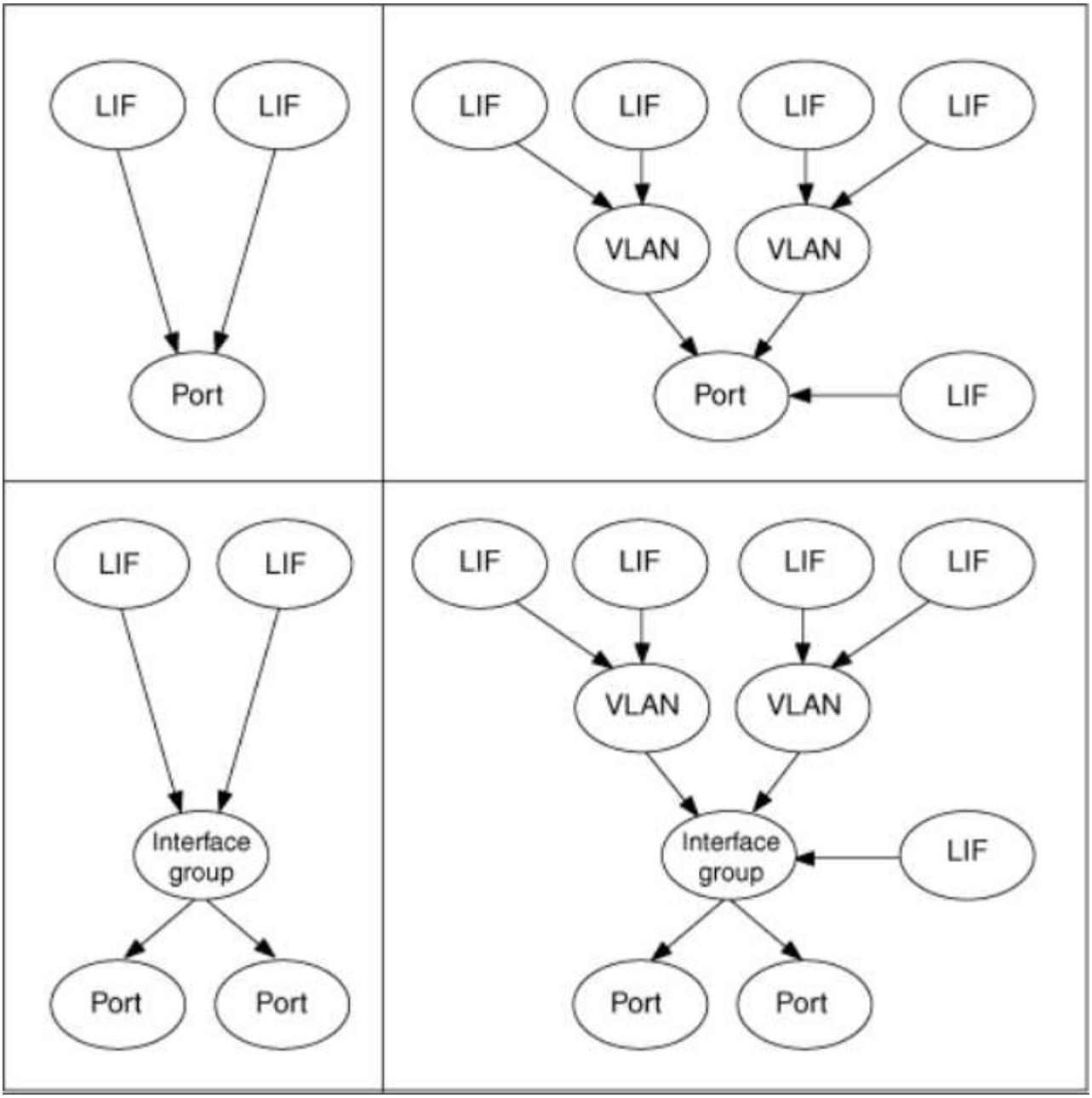
- インターフェイス グループに属していない物理ポート
- インターフェイス グループ
- VLAN
- VLANをホストする物理ポートまたはインターフェイス グループ
- 仮想IP（VIP）ポート

  ONTAP 9.5以降では、VIP LIFがサポートされており、VIPポートでホストされます。

LIFでFCなどのSANプロトコルを設定するときは、WWPNに関連付けられます。

"SAN管理"

次の図に、ONTAPシステムのポート階層を示します。



LIFのフェイルオーバーとギブバック

LIFのフェイルオーバーが発生すると、LIFがホーム ノードまたはポートからHAパートナー ノードまたはポートに移動します。LIFのフェイルオーバーは、物理イーサネット リンクが停止した場合や、ノードがレプリケートされたデータベース（RDB）クォーラムのメンバーでなくなった場合などの特定のイベント時に、ONTAPで自動的にトリガーすることも、クラスタ管理者が手動で開始することもできます。LIFのフェイルオーバーが発生した場合、フェイルオーバーの原因が解決されるまで、ONTAPはパートナー ノードで通常の動作を継続します。ホーム ノードまたはポートの健全性が回復すると、LIFはHAパートナーからホーム ノードまたはポートにリバートされます。このリバートはギブバックと呼ばれます。

LIFのフェイルオーバーとギブバックのためには、各ノードのポートが同じブロードキャスト ドメインに属している必要があります。各ノードの関連するポートが同じブロードキャスト ドメインに属していることを確認するには、以下を参照してください。

- ONTAP 9.8 以降："ポートの到達可能性の修復"

- ONTAP 9.7 以前："ブロードキャスト ドメインのポートの追加と削除"

LIFフェイルオーバーを（自動または手動で）有効にしたLIFには、以下のような処理が適用されます。

- データ サービス ポリシーを使用するLIFの場合は、次のフェイルオーバー ポリシーの制限事項を確認してください。
  - ONTAP 9.6 以降："LIFとサービス ポリシー（ONTAP 9.6以降）"
  - ONTAP 9.5 以前："ONTAP 9.5 以前の LIF ロール"
- LIF の自動復帰は、auto-revert が `true`に設定されており、LIF のホームポートが正常で LIF をホストできる場合に発生します。
- ノードの計画的テイクオーバーと計画外テイクオーバーでは、テイクオーバーされたノードのLIFがHAパートナーにフェイルオーバーされます。LIFのフェイルオーバー先ポートはVIFマネージャによって決定されます。
- フェイルオーバーが完了すると、LIFは正常に動作するようになります。
- ギブバックが開始されると、自動復帰が `true`に設定されている場合、LIF はホーム ノードとポートに戻ります。
- 1つ以上のLIFをホストするポートでイーサネットリンクがダウンした場合、VIFマネージャはダウンしたポートから同じブロードキャストドメイン内の別のポートにLIFを移行します。新しいポートは、同じノード内またはHAパートナー内のポートである可能性があります。リンクが回復し、自動復帰が `true`に設定されていると、VIFマネージャはLIFをホームノードとホームポートに戻します。
- ノードがレプリケートデータベース（RDB）クォーラムから外れると、VIFマネージャはクォーラム外ノードのLIFをHAパートナーに移行します。ノードがクォーラムに復帰し、自動復帰が `true`に設定されている場合、VIFマネージャはLIFをホームノードとホームポートに戻します。

ONTAPの**LIF**とポートタイプの互換性について学ぶ

LIFには、サポートするポートのタイプに応じて、それぞれ異なる特性があります。

クラスタ間LIFと管理LIFが同じサブネットに設定されている場合、管理トラフィックが外部ファイアウォールによってブロックされ、AutoSupportとNTP接続が失敗する可能性があります。`network interface modify -vserver *vserver name* -lif *intercluster LIF* -status-admin up|down`コマンドを実行してクラスタ間LIFを切り替えることで、システムを復旧できます。ただし、この問題を回避するには、クラスタ間LIFと管理LIFを異なるサブネットに設定する必要があります。

LIF	概要
Data LIF	Storage Virtual Machine（SVM）に関連付けられたLIFで、クライアントとの通信に使用します。1つのポートに複数のデータLIFを設定できます。これらのインターフェイスは、クラスタ全体で移行またはフェイルオーバーが可能です。ファイアウォール ポリシーをmgmtに変更すると、データLIFをSVM管理LIFとして使用できます。データLIFは、NIS、LDAP、Active Directory、WINS、およびDNSの各サーバに対するセッションで使用されます。

クラスタ LIF	クラスタ内のノード間トラフィックに使用されるLIFです。クラスタLIFは、必ずクラスタ ポートに作成する必要があります。クラスタLIFは、同じノードのクラスタ ポート間でフェイルオーバーできますが、リモート ノードに移行またはフェイルオーバーすることはできません。新しいノードがクラスタに追加されるとIPアドレスは自動的に生成されます。クラスタLIFにIPアドレスを手動で割り当てる場合は、新しいIPアドレスが既存のクラスタLIFと同じサブネット範囲に含まれるようにする必要があります。
クラスタ管理LIF	クラスタ全体に対する単一の管理インターフェイスを提供するLIFです。クラスタ管理LIFは、クラスタ内の任意のノードにフェイルオーバーできます。クラスタ ポートまたはクラスタ間ポートにはフェイルオーバーできません。
クラスタ間LIF	クラスタ間の通信、バックアップ、およびレプリケーションに使用されるLIFです。クラスタ ピア関係を確立するには、クラスタ内の各ノードにクラスタ間LIFを作成しておく必要があります。クラスタ間LIFは、同じノードのポートにのみフェイルオーバーできます。クラスタ内の別のノードに移行またはフェイルオーバーすることはできません。
ノード管理LIF	クラスタ内の特定のノードを管理するために専用のIPアドレスを提供するLIFです。クラスタの作成時またはクラスタへのノードの追加時に作成されます。ノード管理LIFは、クラスタからノードにアクセスできなくなった場合など、システムのメンテナンスに使用されます。
VIP LIF	VIP LIFとは、VIPポート上に作成されるデータLIFのことです。詳細については、"仮想IP（VIP）LIFの設定"をご覧ください。

関連情報

- "network interface modify"

ONTAPバージョンでサポートされている**LIF**サービスポリシーとロール

リリースを経るごとに、LIFでサポートされるトラフィック タイプをONTAPが管理する方法は変化しています。

- ONTAP 9.5以前のリリースでは、LIFのロールとファイアウォール サービスを使用します。
- ONTAP 9.6以降のリリースでは、LIFのサービス ポリシーを使用します。
  - ONTAP 9.5リリースで、LIFのサービス ポリシーが導入されました。
  - ONTAP 9.6で、LIFのロールがLIFのサービス ポリシーに置き換えられました。
  - ONTAP 9.10.1で、ファイアウォール サービスがLIFのサービス ポリシーに置き換えられました。

設定方法は、使用しているONTAPのバージョンによって異なります。

詳細については、以下を参照してください。

- ファイアウォール ポリシーについては、"コマンド：firewall-policy-show"を参照してください。
- LIF のロールについては、"LIFのロール（ONTAP 9.5以前）"を参照してください。
- LIFサービスポリシーについては、"LIFとサービス ポリシー（ONTAP 9.6以降）"を参照してください。

（LIFのロールまたはファイアウォール ポリシーの代わりに）サービス ポリシーをLIFに割り当てて、LIFでサポートされるトラフィックの種類を設定できます。サービス ポリシーは、LIFでサポートされる一連のネットワーク サービスを定義します。ONTAPには、LIFに関連付けることができる一連の組み込みのサービス ポリシーが用意されています。

ONTAP 9.7以前のバージョンでは、ネットワーク トラフィックの管理方法が異なります。ONTAP 9.7以前を実行しているネットワークでトラフィックを管理する必要がある場合は、"LIFのロール（ONTAP 9.5以前）"を参照してください。

FCP および NVMe/FCP プロトコルでは、現在、サービスポリシーは必要ありません。

次のコマンドを使用して、サービス ポリシーとその詳細を表示できます：
`network interface service-policy show`

`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["ONTAPコマンド リファレンス"^]を参照してください。

特定のサービスにバインドされていない機能では、システム定義の動作を使用してアウトバウンド接続用のLIFを選択します。

サービス ポリシーが空であるLIF上のアプリケーションは、予期しない動作をすることがあります。

システムSVMのサービス ポリシー

管理SVMとシステムSVMには、SVMのLIF（管理LIFやクラスタ間LIFなど）に使用できるサービス ポリシーが含まれています。これらのポリシーは、IPspaceの作成時にシステムによって自動的に作成されます。

次の表は、ONTAP 9.12.1以降のシステムSVMのLIFに組み込まれているポリシーの一覧です。その他のリリースの場合は、次のコマンドを使用してサービス ポリシーとその詳細を表示します：

`network interface service-policy show`

ポリシー	付属サービス	同等の役割	概要
デフォルトインタークラスタ	intercluster-core、management-https	intercluster	クラスタ間トラフィックを伝送する LIF によって使用されます。注：サービス intercluster-core は ONTAP 9.5 以降、net-intercluster サービス ポリシーという名前で使用できます。

デフォルトルートアナウンス	management-BGP	-	BGP ピア接続を伝送する LIF によって使用されます。注：ONTAP 9.5 以降では、net-route-announce サービス ポリシーという名前で使用できます。
デフォルト管理	management-core、management-https、management-http、management-ssh、management-autosupport、management-ems、management-dns-client、management-ad-client、management-ldap-client、management-nis-client、management-ntp-client、management-log-forwarding	node-mgmt、またはcluster-mgmt	このシステムスコープ管理ポリシーを使用して、システムSVMが所有するノードスコープおよびクラスタスコープの管理LIFを作成します。これらのLIFは、DNS、AD、LDAP、またはNISサーバへのアウトバウンド接続に加え、システム全体を代表して実行されるアプリケーションをサポートするための追加接続にも使用できます。ONTAP 9.12.1以降では、`management-log-forwarding`サービスを使用して、監査ログをリモートsyslogサーバに転送するために使用するLIFを制御できます。

次の表は、ONTAP 9.11.1 以降のシステム SVM で LIF が使用できるサービスを示しています：

サービス	フェイルオーバーの制限	概要
インタークラスタコア	ホーム ノードのみ	コアクラスタ間サービス
管理コア	-	コア管理サービス
管理-ssh	-	SSH管理アクセス用のサービス
管理-http	-	HTTP管理アクセス用のサービス
管理-https	-	HTTPS管理アクセス用のサービス
management-AutoSupport	-	AutoSupportペイロードの投稿に関連するサービス
management-BGP	母港のみ	BGP ピア インタラクションに関連するサービス
バックアップ NDMP コントロール	-	NDMPバックアップ制御のサービス
管理-ems	-	管理メッセージング アクセスのサービス

管理-NTPクライアント	-	ONTAP 9.10.1 で導入されました。NTP クライアントアクセス用のサービスです。
management-NTP サーバー	-	ONTAP 9.10.1で導入されました。NTPサーバ管理アクセスのサービス
管理-portmap	-	ポートマップ管理サービス
管理-rsh-サーバ	-	rshサーバー管理のサービス
管理-SNMP-サーバ	-	SNMPサーバー管理のサービス
管理-Telnet-サーバ	-	telnetサーバー管理のサービス
管理ログ転送	-	ONTAP 9.12.1で導入されました。監査ログ転送のサービス

データ**SVM**のサービス ポリシー

すべてのデータSVMに、そのSVMのLIFで使用できるサービス ポリシーが含まれています。

次の表は、ONTAP 9.11.1以降のデータSVMのLIFに組み込まれているポリシーの一覧です。その他のリリースの場合は、次のコマンドを使用してサービス ポリシーとその詳細を表示します：

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

ポリシー	付属サービス	同等のデータ プロトコル	概要
デフォルト管理	data-core、management-https、management-http、management-ssh、management-dns-client、management-ad-client、management-ldap-client、management-nis-client	なし	このSVMを対象とする管理ポリシーを使用して、データSVMが所有するSVM管理LIFを作成します。これらのLIFは、SVM管理者にSSHまたはHTTPSアクセスを提供するために使用できます。必要に応じて、これらのLIFは外部DNS、AD、LDAP、またはNISサーバーへのアウトバウンド接続にも使用できます。
デフォルトのデータブロック	data-core、data-iscsi	iscsi	ブロック指向SANデータトラフィックを伝送するLIFで使用されます。ONTAP 9.10.1以降、「default-data-blocks」ポリシーは非推奨です。代わりに「default-data-iscsi」サービスポリシーを使用してください。

デフォルトのデータファイル	data-core、data-fpolicy-client、data-dns-server、data-flexcache、data-cifs、data-nfs、management-dns-client、management-ad-client、management-ldap-client、management-nis-client	nfs、cifs、fcache	ファイルベースのデータプロトコルをサポートするNAS LIFを作成するには、default-data-filesポリシーを使用します。SVMにLIFが1つしか存在しない場合もあるため、このポリシーにより、LIFを外部DNS、AD、LDAP、またはNISサーバへのアウトバウンド接続に使用できます。これらの接続で管理LIFのみを使用する場合は、このポリシーからこれらのサービスを削除できます。
デフォルトデータiSCSI	data-core、data-iscsi	iscsi	iSCSI データ トラフィックを伝送する LIF によって使用されます。
デフォルトデータNVMe-TCP	data-core、data-nvme-tcp	nvme-tcp	NVMe/TCPデータトラフィックを伝送するLIFによって使用されます。

次の表は、ONTAP 9.11.1以降、データSVMで使用できるサービスと、各サービスがLIFのフェイルオーバーポリシーに課す制限を示しています：

サービス	フェイルオーバーの制限	概要
管理-ssh	-	SSH管理アクセス用のサービス
管理-http	-	ONTAP 9.10.1で導入されたHTTP管理アクセス用サービス
管理-https	-	HTTPS管理アクセス用のサービス
管理-portmap	-	portmap管理アクセス用のサービス
管理-SNMP-サーバ	-	ONTAP 9.10.1で導入されたSNMPサーバ管理アクセス用のサービス
data-core	-	コアデータサービス
data-nfs	-	NFSデータサービス
data-cifs	-	CIFSデータサービス
data-flexcache	-	FlexCacheデータサービス

データiSCSI	AFF/FASの場合はhome-port-only、ASAの場合はsfo-partner-only	iSCSIデータサービス
バックアップ NDMP コントロール	-	ONTAP 9.10.1で導入 バックアップNDMPによるデータサービスの制御
data-DNSサーバ	-	ONTAP 9.10.1で導入されたDNSサーバデータサービス
data-fpolicyクライアント	-	ファイルスクリーニングポリシーデータサービス
data-nvme-tcp	母港のみ	ONTAP 9.10.1で導入されたNVMe TCPデータサービス
data-s3-server	-	Simple Storage Service（S3）サーバデータサービス

データSVMのLIFに対するサービス ポリシーの割り当てについて、次の点に注意してください。

- データ サービスのリストを指定してデータSVMを作成した場合、そのSVMでは、指定したサービスを使用して組み込みの「default-data-files」サービス ポリシーと「default-data-blocks」サービス ポリシーが作成されます。
- データ サービスのリストを指定せずにデータSVMを作成した場合、そのSVMでは、デフォルトのデータ サービスのリストを使用して組み込みの「default-data-files」サービス ポリシーと「default-data-blocks」サービス ポリシーが作成されます。

  デフォルトのデータ サービスのリストには、iSCSI、NFS、NVMe、SMB、FlexCacheの各サービスが含まれます。

- データ プロトコルのリストを指定してLIFを作成した場合、指定したデータ プロトコルと同等のサービス ポリシーがLIFに割り当てられます。
- 同等のサービス ポリシーが存在しない場合は、カスタム サービス ポリシーが作成されます。
- サービス ポリシーまたはデータ プロトコルのリストを指定せずにLIFを作成した場合、デフォルトでdefault-data-filesサービス ポリシーがLIFに割り当てられます。

data-coreサービス

data-coreサービスは、LIFのロール（ONTAP 9.6で廃止）ではなくサービス ポリシーを使用してLIFを管理するようにアップグレードされたクラスタで、これまでdataロールのLIFを使用していたコンポーネントが想定どおりに機能するようにします。

data-coreをサービスとして指定してもファイアウォールのポートは開きませんが、データSVMのすべてのサービス ポリシーにこのサービスを含める必要があります。たとえば、default-data-filesサービス ポリシーには、デフォルトで次のサービスが含まれます。

- data-core
- data-nfs

- data-cifs
- data-flexcache

data-coreサービスはLIFを使用するすべてのアプリケーションが想定どおりに機能するために必要ですが、他の3つのサービスは不要であれば削除できます。

クライアント側の**LIF**サービス

ONTAP 9.10.1以降では、複数のアプリケーションに対してクライアント側のLIFサービスが提供されます。これらのサービスは、各アプリケーションに代わって、アウトバウンド接続に使用するLIFを制御します。

管理者は、次の新しいサービスを使用して、特定のアプリケーションのソース アドレスとして使用するLIFを制御できます。

サービス	SVMの制限	概要
管理ADクライアント	-	ONTAP 9.11.1以降、ONTAPは外部ADサーバへのアウトバウンド接続用にActive Directoryクライアントサービスを提供します。
management-dns-client	-	ONTAP 9.11.1 以降、ONTAP は外部 DNS サーバへのアウトバウンド接続用の DNS クライアントサービスを提供します。
management-ldap-client	-	ONTAP 9.11.1以降、ONTAPは外部LDAPサーバへのアウトバウンド接続用のLDAPクライアントサービスを提供します。
management-nis-client	-	ONTAP 9.11.1 以降、ONTAPは外部NISサーバへのアウトバウンド接続用のNISクライアントサービスを提供します。
管理-NTPクライアント	システムのみ	ONTAP 9.10.1 以降、ONTAP は外部 NTP サーバへのアウトバウンド接続用の NTP クライアント サービスを提供します。
data-fpolicyクライアント	data-only	ONTAP 9.8以降、ONTAPはアウトバウンドFPolicy接続用のクライアントサービスを提供します。

新しいサービスは一部の組み込みサービス ポリシーに自動的に含まれていますが、管理者はこれらのサービスを組み込みのポリシーから削除できます。またはカスタムのポリシーに追加して、各アプリケーションに代わってアウトバウンド接続に使用するLIFを制御することもできます。

関連情報

- "network interface service-policy show"

LIFの管理

LIFのサービス ポリシーを設定して、LIFを使用する単一のサービスまたは一連のサービスを指定することができます。

LIFのサービス ポリシーの作成

LIFのサービス ポリシーを作成することができます。1つ以上のLIFにサービス ポリシーを割り当てることで、1つまたは一連のサービスのトラフィックの処理をLIFに許可することができます。

`network interface service-policy create`コマンドを実行するには高度な権限が必要です。

タスク概要

データSVMとシステムSVM両方のデータ トラフィックと管理トラフィックの管理に、組み込みのサービスおよびサービス ポリシーを使用できます。ほとんどのユースケースでは、カスタム サービス ポリシーを作成するのではなく、組み込みのサービス ポリシーを使用して対応できます。

これらの組み込みのサービス ポリシーは必要に応じて変更できます。

手順

1. クラスタで使用できるサービスを確認します。

   ```
   network interface service show
   ```

   サービスとは、LIFがアクセスするアプリケーション、およびクラスタで提供されるアプリケーションです。各サービスには、アプリケーションがリスンしているTCPポートとUDPポートが0個以上含まれています。

   次の追加のデータ サービスと管理サービスを使用できます。

```
cluster1::> network interface service show

Service                      Protocol:Ports
-------                      --------------
cluster-core                 -
data-cifs                    -
data-core                    -
data-flexcache               -
data-iscsi                   -
data-nfs                     -
intercluster-core            tcp:11104-11105
management-autosupport       -
management-bgp               tcp:179
management-core              -
management-https             tcp:443
management-ssh               tcp:22
12 entries were displayed.
```

2. クラスタに存在するサービス ポリシーを確認します。

```
cluster1::> network interface service-policy show

Vserver   Policy                       Service: Allowed Addresses
--------- --------------------------
---------------------------------------
cluster1
          default-intercluster         intercluster-core: 0.0.0.0/0
                                       management-https: 0.0.0.0/0

          default-management           management-core: 0.0.0.0/0
                                       management-autosupport: 0.0.0.0/0
                                       management-ssh: 0.0.0.0/0
                                       management-https: 0.0.0.0/0

          default-route-announce       management-bgp: 0.0.0.0/0

Cluster
          default-cluster              cluster-core: 0.0.0.0/0

vs0
          default-data-blocks          data-core: 0.0.0.0/0
                                       data-iscsi: 0.0.0.0/0

          default-data-files           data-core: 0.0.0.0/0
                                       data-nfs: 0.0.0.0/0
                                       data-cifs: 0.0.0.0/0
                                       data-flexcache: 0.0.0.0/0

          default-management           data-core: 0.0.0.0/0
                                       management-ssh: 0.0.0.0/0
                                       management-https: 0.0.0.0/0

7 entries were displayed.
```

3. サービス ポリシーを作成します。

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support.
Do you wish to continue? (y or n): y

cluster1::> network interface service-policy create -vserver <svm_name>
-policy <service_policy_name> -services <service_name> -allowed
-addresses <IP_address/mask,...>
```

- 「service_name」には、ポリシーに含めるサービスのリストを指定します。
- 「IP_address/mask」には、サービス ポリシー内のサービスへのアクセスを許可するアドレスを、サブネット マスクのリストで指定します。デフォルトでは、指定したすべてのサービスが、デフォルトの許可アドレス リスト0.0.0.0/0（すべてのサブネットからのトラフィックを許可）で追加されます。デフォルト以外の許可アドレス リストを指定した場合、そのポリシーを使用するLIFは、指定したマスクと一致しないソース アドレスからの要求をすべてブロックするように設定されます。

  次の例は、*NFS* および *SMB* サービスを含む SVM のデータ サービス ポリシー *svm1_data_policy* を作成する方法を示しています：

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support.
Do you wish to continue? (y or n): y

cluster1::> network interface service-policy create -vserver svm1
-policy svm1_data_policy -services data-nfs,data-cifs,data-core
```

  次の例は、クラスタ間サービス ポリシーを作成する方法を示しています。

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support.
Do you wish to continue? (y or n): y

cluster1::> network interface service-policy create -vserver cluster1
-policy intercluster1 -services intercluster-core
```

4. サービス ポリシーが作成されたことを確認します。

```
cluster1::> network interface service-policy show
```

次の出力は、使用可能なサービス ポリシーを示しています。

```
cluster1::> network interface service-policy show

Vserver   Policy                       Service: Allowed Addresses
--------- --------------------------
---------------------------------------
cluster1
          default-intercluster         intercluster-core: 0.0.0.0/0
                                       management-https: 0.0.0.0/0

          intercluster1                intercluster-core: 0.0.0.0/0

          default-management           management-core: 0.0.0.0/0
                                       management-autosupport: 0.0.0.0/0
                                       management-ssh: 0.0.0.0/0
                                       management-https: 0.0.0.0/0

          default-route-announce       management-bgp: 0.0.0.0/0

Cluster
          default-cluster              cluster-core: 0.0.0.0/0

vs0
          default-data-blocks          data-core: 0.0.0.0/0
                                       data-iscsi: 0.0.0.0/0

          default-data-files           data-core: 0.0.0.0/0
                                       data-nfs: 0.0.0.0/0
                                       data-cifs: 0.0.0.0/0
                                       data-flexcache: 0.0.0.0/0

          default-management           data-core: 0.0.0.0/0
                                       management-ssh: 0.0.0.0/0
                                       management-https: 0.0.0.0/0

          svm1_data_policy             data-core: 0.0.0.0/0
                                       data-nfs: 0.0.0.0/0
                                       data-cifs: 0.0.0.0/0

9 entries were displayed.
```

終了後の操作

LIFの作成時または既存のLIFの変更時にサービス ポリシーを割り当てます。

LIFへのサービス ポリシーの割り当て

LIFの作成時または変更時に、LIFにサービス ポリシーを割り当てることができます。サービス ポリシーは、LIFで使用できる一連のサービスを定義します。

タスク概要

管理SVMとデータSVMのLIFにサービス ポリシーを割り当てることができます。

手順

LIFにサービス ポリシーをいつ割り当てるかに応じて、次のいずれかのコマンドを実行します。

状況	サービスポリシーを割り当てます...
NVMe LIFの設定	network interface create -vserver svm_name -lif <lif_name> -home-node <node_name> -home-port <port_name> {(-address <IP_address> -netmask <IP_address>) -subnet-name <subnet_name>} -service-policy <service_policy_name>
LIFの変更	network interface modify -vserver <svm_name> -lif <lif_name> -service-policy <service_policy_name>

LIFのサービス ポリシーを指定する際に、LIFのデータ プロトコルとロールを指定する必要はありません。ロールとデータ プロトコルを指定してLIFを作成することも可能です。

サービス ポリシーは、サービス ポリシーの作成時に指定した同じSVMに含まれるLIFでのみ使用できます。

例

次の例は、LIFのサービス ポリシーをdefault-managementに変更する方法を示しています。

```
cluster1::> network interface modify -vserver cluster1 -lif lif1 -service
-policy default-management
```

LIFのサービス ポリシーを管理するためのコマンド

`network interface service-policy`コマンドを使用して、LIFサービスポリシーを管理します。

`network interface service-policy`の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/search.html?q=network+interface+service-policy["ONTAPコマンドリファレンス"^]をご覧ください。

開始する前に

アクティブなSnapMirror関係にあるLIFのサービスポリシーを変更すると、レプリケーションスケジュールが

中断されます。LIFをインタークラスタから非インタークラスタ（またはその逆）に変換した場合、それらの変更はピアクラスタにレプリケートされません。LIFのサービスポリシーを変更した後にピアクラスタを更新するには、まず `snapmirror abort`操作を実行してからレプリケーション関係を再同期するを実行してください。

状況	使用するコマンド
サービスポリシーを作成する（高度な権限が必要）	`network interface service-policy create`
既存のサービスポリシーにサービスエントリを追加します（高度な権限が必要です）	`network interface service-policy add-service`
既存のサービスポリシーを複製する（高度な権限が必要）	`network interface service-policy clone`
既存のサービス ポリシー内のサービス エントリを変更する（高度な権限が必要）	`network interface service-policy modify-service`
既存のサービスポリシーからサービスエントリを削除します（高度な権限が必要です）	`network interface service-policy remove-service`
既存のサービスポリシーの名前を変更する（高度な権限が必要）	`network interface service-policy rename`
既存のサービスポリシーを削除します（高度な権限が必要です）	`network interface service-policy delete`
組み込みのサービスポリシーを元の状態に復元します（高度な権限が必要）	`network interface service-policy restore-defaults`
既存のサービス ポリシーを表示する	`network interface service-policy show`

関連情報

- "ネットワークインターフェイスサービスの表示"
- "ネットワークインターフェイス サービスポリシー"
- "snapmirror abort"

ONTAP LIFを作成する

SVMは、1つ以上のネットワーク論理インターフェイス（LIF）を通じてクライアントにデータを提供します。データへのアクセスに使用するポートにLIFを作成する必要があります。LIF（ネットワーク インターフェイス）は、物理ポートまたは論理ポートに関連付けられたIPアドレスです。コンポーネントに障害が発生しても、LIFは別の物理ポートにフェイルオーバーまたは移行できるので、引き続きネットワークと通信できます。

ベストプラクティス

ONTAPに接続されたスイッチ ポートは、LIFの移行時の遅延を軽減するために、スパニングツリー エッジ ポートとして設定する必要があります。

開始する前に

- このタスクを実行するには、クラスタ管理者である必要があります。
- 基盤となる物理または論理ネットワーク ポートの管理ステータスがupに設定されている必要があります。
- サブネット名を使用してLIFのIPアドレスとネットワーク マスク値を割り当てる場合は、そのサブネットが存在している必要があります。

  サブネットには、同じレイヤ 3 サブネットに属する IP アドレスのプールが含まれます。System Manager または `network subnet create`コマンドを使用して作成されます。

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

- LIFが処理するトラフィックのタイプを指定するメカニズムが変更されました。ONTAP 9.5以前ではロールで指定していました。ONTAP 9.6以降ではサービス ポリシーで指定します。

タスク概要

- 同じLIFにNASプロトコルやSANプロトコルを割り当てることはできません。

  サポートされるプロトコルは、SMB、NFS、FlexCache、iSCSI、およびFCです。iSCSIとFCを他のプロトコルと組み合わせることはできません。ただし、NASプロトコルとイーサネットベースのSANプロトコルは、同じ物理ポートで使用できます。

  - SMBトラフィックを伝送するLIFを、ホーム ノードに自動的にリバートするように設定しないでください。Hyper-V over SMBまたはSQL Server over SMBでノンストップ オペレーションを実現するソリューションをSMBサーバでホストする場合、これは必須です。
- 同じネットワーク ポート上にIPv4とIPv6の両方のLIFを作成できます。
- SVMで使用するすべてのネーム マッピング サービスとホスト名解決サービス（DNS、NIS、LDAP、Active Directoryなど）が、SVMのデータ トラフィックを処理する少なくとも1つのLIFから到達可能でなければなりません。
- クラスタ内のノード間トラフィックを処理するLIFは、管理トラフィックを処理するLIFまたはデータ トラフィックを処理するLIFと同じサブネット上には存在できません。
- 有効なフェイルオーバー ターゲットのないLIFを作成すると、警告メッセージが表示されます。
- クラスタ内のLIFの数が多い場合、クラスタでサポートされるLIFの最大数を確認できます。
  - System Manager：ONTAP 9.12.0以降では、ネットワーク インターフェイス グリッドでスループットを表示します。
  - CLI： `network interface capacity show`コマンドと `network interface capacity details show`コマンド（advanced権限レベル）を使用して、各ノードでサポートされているLIF容量を確認します。

`network interface capacity show`および `network interface capacity details show`の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/search.html?q=network+interface+capacity+show["ONTAPコマンド リファレンス"^]をご覧ください。

- ONTAP 9.7以降では、同じサブネットにSVM用の他のLIFがすでに存在していれば、LIFのホーム ポートを指定する必要はありません。同じサブネットにすでに設定されている他のLIFと同じブロードキャスト ドメインにあるホーム ノードから任意のポートが自動的に選択されます。

  ONTAP 9.4以降では、FC-NVMeがサポートされます。FC-NVMe LIFを作成する場合は、次の点に注意してください。

  - LIFを作成するFCアダプタでNVMeプロトコルがサポートされている必要があります。
  - データLIFで使用できるデータ プロトコルはFC-NVMeのみです。
- SANをサポートするStorage Virtual Machine（SVM）ごとに、管理トラフィックを処理するLIFを1つ設定する必要があります。
- NVMeのLIFとネームスペースは、同じノードでホストする必要があります。
- ノードごとに、SVM ごとに、データ トラフィックを処理する NVMe LIF を最大 2 つ設定できます。
- サブネットを使用してネットワーク インターフェイスを作成すると、使用可能なIPアドレスが選択したサブネットから自動的に選択され、ネットワーク インターフェイスに割り当てられます。複数のサブネットがある場合にサブネットを変更することはできますが、IPアドレスは変更できません。
- ネットワーク インターフェイス用のSVMを作成（追加）するときに、既存のサブネット範囲に含まれるIPアドレスを指定することはできません。サブネットの競合エラーが表示されます。この問題は、SVM設定やクラスタ設定でクラスタ間ネットワーク インターフェイスを作成または変更する場合など、ネットワーク インターフェイスの他のワークフローでも発生します。
- ONTAP 9.10.1以降、 `network interface` CLIコマンドには、NFS over RDMA構成用の `-rdma-protocols`パラメータが含まれています。NFS over RDMA構成用のネットワークインターフェイスの作成は、ONTAP 9.12.1以降のSystem Managerでサポートされています。詳細については、RDMA経由のNFS用にLIFを設定するを参照してください。
- ONTAP 9.11.1以降では、オールフラッシュSANアレイ（ASA）プラットフォームで自動iSCSI LIFフェイルオーバーを使用できます。

  指定されたSVMにiSCSI LIFが存在しない場合、または指定されたSVM内の既存のすべてのiSCSI LIFでiSCSI LIFフェイルオーバーがすでに有効になっている場合は、新しく作成されたiSCSI LIFでiSCSI LIFフェイルオーバーが自動的に有効になります（フェイルオーバー ポリシーが `sfo-partner-only`に設定され、自動復帰値が `true`に設定されます）。

  ONTAP 9.11.1 以降にアップグレードした後、iSCSI LIF フェイルオーバー機能が有効になっていない既存の iSCSI LIF が SVM 内に存在し、同じ SVM 内に新しい iSCSI LIF を作成した場合、新しい iSCSI LIF は SVM 内の既存の iSCSI LIF と同じフェイルオーバー ポリシー(`disabled`を適用します。

  "ASAプラットフォームのiSCSI LIFフェイルオーバー"

ONTAP 9.7以降では、LIFのホーム ポートは、そのIPspaceの同じサブネットに既存のLIFが1つでも存在していれば自動的に選択されます。ホーム ポートは、そのサブネットの他のLIFと同じブロードキャスト ドメインから選択されます。手動で指定することも引き続き可能です（指定したIPspaceの該当するサブネットにLIFが

ない場合）。

ONTAP 9.12.0以降では、実行する手順は、System ManagerとCLIのどちらのインターフェイスを使用するかによって異なります。

System Manager

System Managerを使用してネットワークインターフェイスを追加します

手順

1. *ネットワーク > 概要 > ネットワーク インターフェイス*を選択します。
2. + Add を選択します。
3. 次のいずれかのインターフェイス ロールを選択します。
   a. データ
   b. クラスタ間
   c. SVM管理
4. プロトコルを選択します。
   a. SMB/CIFS and NFS
   b. iSCSI
   c. FC
   d. NVMe/FC
   e. NVMe/TCP
5. LIFの名前を指定するか、ここまでの選択内容から生成された名前をそのまま使用します。
6. ホーム ノードをそのまま使用するか、ドロップダウンを使用して選択します。
7. 選択したSVMのIPspaceでサブネットが1つでも設定されている場合、サブネットのドロップダウンが表示されます。
   a. サブネットを選択する場合はドロップダウンから選択します。
   b. サブネットを選択せずに次に進むと、ブロードキャスト ドメインのドロップダウンが表示されます。
      i. IPアドレスを指定します。IPアドレスが使用中の場合は、警告メッセージが表示されます。
      ii. サブネット マスクを指定します。
8. ホーム ポートをブロードキャスト ドメインから自動で選択するか（推奨）、ドロップダウン メニューから選択します。ホーム ポートのオプションは、ブロードキャスト ドメインとサブネットの選択に基づいて表示されます。
9. ネットワーク インターフェイスを保存します。

CLI

CLIを使用して**LIF**を作成する

手順

1. LIFに使用するIPspaceブロードキャスト ドメインのポートを判断します。

```
network port broadcast-domain show -ipspace ipspace1
```

```
IPspace     Broadcast                         Update
Name        Domain name   MTU   Port List     Status Details
ipspace1
            default       1500
                                node1:e0d     complete
                                node1:e0e     complete
                                node2:e0d     complete
                                node2:e0e     complete
```

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

2. LIFに使用するサブネットに未使用のIPアドレスが十分にあることを確認します。

   `network subnet show -ipspace ipspace1`

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

3. データへのアクセスに使用するポートに1つ以上のLIFを作成します。

> NetAppでは、データSVM上のすべてのLIFに対してサブネットオブジェクトを作成することを推奨しています。これはMetroCluster構成では特に重要です。各サブネットオブジェクトにはブロードキャストドメインが関連付けられているため、サブネットオブジェクトによってONTAPがデスティネーション クラスタ上のフェイルオーバーターゲットを決定できるようになります。手順については、"サブネットの作成"を参照してください。

```
network interface create -vserver _SVM_name_ -lif _lif_name_
-service-policy _service_policy_name_ -home-node _node_name_ -home
-port port_name {-address _IP_address_ - netmask _Netmask_value_ |
-subnet-name _subnet_name_} -firewall- policy _policy_ -auto-revert
{true|false}
```

- `-home-node`は、 `network interface revert`コマンドがLIF上で実行されたときにLIFが戻るノードです。

  -auto-revertオプションを使用して、LIFをホーム ノードおよびホーム ポートに自動的にリバートするかどうかを指定することもできます。

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

- `-home-port`は、LIF上で `network interface revert`コマンドが実行されたときにLIFが戻る物理ポートまたは論理ポートです。
- `-address`および `-netmask`オプションを使用してIPアドレスを指定することも、 `-subnet_name`オプションを使用してサブネットからの割り当てを有効にすることもできます。
- サブネットを使用してIPアドレスとネットワーク マスクを指定した場合、サブネットにゲートウェイが定義されていると、そのサブネットを使用してLIFを作成するときにゲートウェイへのデフォルト ルートがSVMに自動的に追加されます。
- IPアドレスを手動で割り当てる場合（サブネットを使用せず）、クライアントまたはドメインコントローラが異なるIPサブネット上にある場合は、ゲートウェイへのデフォルトルートを設定する必要がある場合があります。"ONTAPコマンド リファレンス"の `network route create`の詳細をご覧ください。
- `-auto-revert`起動時、管理データベースのステータス変更時、ネットワーク接続時などの状況において、データLIFをホームノードに自動的に戻すかどうかを指定できます。デフォルト設定は `false`ですが、環境のネットワーク管理ポリシーに応じて `true`に設定することもできます。
- `-service-policy`ONTAP 9.5以降では、 `-service-policy`オプションを使用してLIFにサービスポリシーを割り当てることができます。LIFにサービスポリシーを指定すると、そのポリシーに基づいて、LIFのデフォルトロール、フェイルオーバーポリシー、およびデータプロトコルリストが作成されます。ONTAP 9.5では、サービスポリシーはクラスタ間サービスとBGPピアサービスでのみサポートされています。ONTAP 9.6では、複数のデータサービスと管理サービスに対してサービスポリシーを作成できます。
- `-data-protocol`FCPまたはNVMe/FCプロトコルをサポートするLIFを作成できます。IP LIFを作成する場合、このオプションは必要ありません。

4. オプション：-address オプションで IPv6 アドレスを割り当てます。
   a. `network ndp prefix show`コマンドを使用して、さまざまなインターフェースで学習された RA プレフィックスのリストを表示します。

      `network ndp prefix show`コマンドは、上級権限レベルで使用できます。

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

   b. `prefix::id`の形式を使用して、IPv6アドレスを手動で構築します。

      `prefix`は、さまざまなインターフェースで学習されたプレフィックスです。

`id`を導出するには、ランダムな64ビットの16進数を選択します。

5. LIFインターフェイスの設定が正しいことを確認します。

```
network interface show -vserver vs1
```

```
          Logical    Status     Network          Current   Current Is
Vserver   Interface  Admin/Oper Address/Mask     Node      Port
Home
--------- ---------- ---------- ---------------- --------- -------
----
vs1
           lif1       up/up      10.0.0.128/24   node1     e0d
true
```

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

6. フェイルオーバー グループの設定が適切であることを確認します。

```
network interface show -failover -vserver vs1
```

```
         Logical    Home       Failover        Failover
Vserver  interface  Node:Port  Policy          Group
-------- ---------- ---------  ---------       --------
vs1
         lif1       node1:e0d  system-defined  ipspace1
Failover Targets: node1:e0d, node1:e0e, node2:e0d, node2:e0e
```

7. 設定したIPアドレスに到達できることを確認します。

対象	方法
IPv4 アドレス	network ping
IPv6アドレス	network ping6

例

次のコマンドは、LIF を作成し、`-address`および`-netmask`パラメータを使用して IP アドレスとネットワーク マスクの値を指定します：

```
network interface create -vserver vs1.example.com -lif datalif1
-service-policy default-data-files -home-node node-4 -home-port e1c
-address 192.0.2.145 -netmask 255.255.255.0 -auto-revert true
```

次のコマンドは、LIFを作成し、IPアドレスとネットワーク マスク値を指定したサブネット（client1_sub）から割り当てています。

```
network interface create -vserver vs3.example.com -lif datalif3
-service-policy default-data-files -home-node node-3 -home-port e1c
-subnet-name client1_sub - auto-revert true
```

次のコマンドは、NVMe/FC LIFを作成し、 `nvme-fc`データ プロトコルを指定します：

```
network interface create -vserver vs1.example.com -lif datalif1 -data
-protocol nvme-fc -home-node node-4 -home-port 1c -address 192.0.2.145
-netmask 255.255.255.0 -auto-revert true
```

ONTAP LIFの変更

LIFの属性は変更することができます。これには、ホーム ノードや現在のノード、管理ステータス、IPアドレス、ネットマスク、フェイルオーバー ポリシー、ファイアウォール ポリシー、サービス ポリシーなどが含まれます。また、LIFのアドレス ファミリーをIPv4からIPv6に変更することもできます。

タスク概要

- LIFの管理ステータスをdownに変更すると、再びupに戻るまで、現行のNFSv4ロックが維持されたままになります。

  ロックされたファイルに他のLIFがアクセスしようとしたときにロックの競合が発生するのを防ぐには、LIFの管理ステータスをdownに設定する前に、NFSv4クライアントを別のLIFに移動する必要があります。

- FC LIFで使用されているデータ プロトコルを変更することはできません。ただし、サービス ポリシーに割り当てられているサービスや、IP LIFに割り当てられているサービス ポリシーは変更可能です。

  FC LIFで使用されているデータ プロトコルを変更するには、LIFを削除して作成し直す必要があります。IP LIFにサービス ポリシーの変更が適用される間、短時間の停止が発生します。

- 現在のノード、またはノードを対象とした管理LIFのホーム ノードを変更することはできません。
- LIFのIPアドレスとネットワーク マスクを変更するためにサブネットを使用すると、指定したサブネットからIPアドレスが割り当てられます。LIFの前のIPアドレスが別のサブネットから割り当てられた場合は、IPアドレスがそのサブネットに戻されます。
- LIF のアドレスファミリを IPv4 から IPv6 に変更するには、IPv6 アドレスにコロン表記を使用し、 `-netmask-length`パラメータに新しい値を追加する必要があります。

- 自動構成されたIPv6リンクローカル アドレスは変更できません。
- LIFの変更によって、LIFに有効なフェイルオーバー ターゲットがなくなる場合は警告メッセージが表示されます。

  有効なフェイルオーバー ターゲットのないLIFがフェイルオーバーしようとすると、システムが停止する可能性があります。

- ONTAP 9.5以降では、LIFに関連付けられているサービス ポリシーを変更できます。

  ONTAP 9.5では、クラスタ間およびBGPピアのサービスについてのみサービス ポリシーがサポートされます。ONTAP 9.6では、複数のデータ サービスおよび管理サービスについてサービス ポリシーを作成できます。

- ONTAP 9.11.1以降では、オールフラッシュSANアレイ（ASA）プラットフォームで自動iSCSI LIFフェイルオーバーを使用できます。

  既存のiSCSI LIF（9.11.1以降にアップグレードする前に作成されたLIF）の場合は、フェイルオーバーポリシーを"iSCSI LIFの自動フェイルオーバーを有効にする"に変更できます。

- ONTAPは、ネットワークタイムプロトコル（NTP）を使用してクラスタ全体の時刻を同期します。LIF IPアドレスを変更した後は、同期の失敗を防ぐためにNTP設定の更新が必要になる場合があります。詳細については、"NetAppナレッジベース：LIF IPの変更後にNTP同期が失敗する"を参照してください。

実行する手順は、System ManagerとCLIのどちらのインターフェイスを使用するかによって異なります。

System Manager

ONTAP 9.12.0以降では、**System Manager**を使用してネットワークインターフェイスを編集できます

手順

1. *ネットワーク > 概要 > ネットワーク インターフェイス*を選択します。
2. 変更したいネットワーク インターフェイスの横にある *> 編集*を選択します。
3. ネットワークインターフェイスの設定を1つ以上変更します。詳細については、"LIFの作成"を参照してください。
4. 変更を保存します。

CLI

CLIを使用して**LIF**を変更する

手順

1. `network interface modify`コマンドを使用してLIFの属性を変更します。

   次の例は、datalif2というLIFのIPアドレスとネットワーク マスクを、サブネットclient1_subのIPアドレスとネットワーク マスク値に変更する例を示しています。

   ```
   network interface modify -vserver vs1 -lif datalif2 -subnet-name
   client1_sub
   ```

   次の例は、LIFのサービス ポリシーを変更する方法を示しています。

   ```
   network interface modify -vserver siteA -lif node1_inter1 -service
   -policy example
   ```

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

2. IPアドレスに到達できることを確認します。

…を使用している場合	次に使用します…
IPv4アドレス	`network ping`
IPv6アドレス	`network ping6`

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

ONTAP LIFの移行

ポートで障害が発生した場合やメンテナンスを行う場合など、同じノードの別のポートやクラスタ内の別のノードにLIFを移行しなければならないことがあります。LIFの移行はLIFのフェイルオーバーと似ています。ただし、前者は手動で行う操作であるのに対し、後者はLIFの現在のネットワーク ポートのリンク障害に対処するために自動的に行われる移行です。

開始する前に

- LIFのフェイルオーバー グループを設定しておく必要があります。
- デスティネーションのノードおよびポートが動作していて、ソース ポートと同じネットワークにアクセスできる必要があります。

タスク概要

- BGP LIFはホーム ポートに配置され、他のノードやポートに移行することはできません。
- ノードからNICを削除する前に、NICに属しているポートでホストされているLIFをクラスタ内の他のポートに移行する必要があります。
- クラスタLIFを移行するコマンドは、そのクラスタLIFがホストされているノードで実行する必要があります。
- ノードを対象とした管理LIF、クラスタLIF、クラスタ間LIFなど、ノードを対象としたLIFをリモート ノードに移行することはできません。
- NFSv4のLIFをノード間で移行したときは、そのLIFが新しいポートで使用できるようになるまで、45秒ほどかかります。

  この問題を防ぐには、NFSv4.1を使用します。

- ONTAP 9.11.1以降を実行するオールフラッシュSANアレイ（ASA）プラットフォームのiSCSI LIFを移行できます。

  移行先は、ホーム ノードまたはHAパートナーのポートに限定されます。

- プラットフォームがONTAPバージョン9.11.1以降を実行するオールフラッシュSANアレイ（ASA）ではない場合、iSCSI LIFをノード間で移行することはできません。

  この制限を回避するには、宛先ノードにiSCSI LIFを作成する必要があります。"iSCSI LIFの作成"の詳細を確認してください。

- NFS over RDMAのLIF（ネットワークインターフェイス）を移行する場合は、移行先ポートがRoCE対応であることを確認する必要があります。CLIを使用してLIFを移行する場合はONTAP 9.10.1以降、System Managerを使用して移行する場合はONTAP 9.12.1を実行している必要があります。System ManagerでRoCE対応の移行先ポートを選択したら、*RoCEポートを使用する*の横にあるチェックボックスをオン

にして、移行を正常に完了する必要があります。"RDMA経由のNFS用のLIFの設定"の詳細を確認してください。

- VMware VAAIのコピー オフロード処理は、ソースLIFまたはデスティネーションLIFを移行すると失敗します。コピー オフロードの詳細については、以下を参照してください。
  - "NFS環境"
  - "SAN環境"

実行する手順は、System ManagerとCLIのどちらのインターフェイスを使用するかによって異なります。

System Manager

System Managerを使用してネットワークインターフェイスを移行する

手順

1. *ネットワーク > 概要 > ネットワーク インターフェイス*を選択します。
2. 変更するネットワーク インターフェイスの横にある *> Migrate*を選択します。

   iSCSI LIFの場合、[インターフェイスの移行]ダイアログボックスで、HAパートナーの宛先ノードとポートを選択します。

   iSCSI LIFを完全に移行する場合は、チェック ボックスをオンにします。完全な移行を行う前に、iSCSI LIFがオフラインになっている必要があります。また、完全に移行したiSCSI LIFは元に戻すことができません。リバートのオプションはありません。

3. *Migrate*をクリックします。
4. 変更を保存します。

CLI

CLIを使用して**LIF**を移行する

手順

特定のLIFを移行するかすべてのLIFを移行するかに応じて、該当する操作を実行します。

移行する項目	入力するコマンド
特定のLIF	`network interface migrate`
ノード上のすべてのデータLIFとクラスタ管理LIF	`network interface migrate-all`
ポートのすべてのLIF	`network interface migrate-all -node <node> -port <port>`

次の例は、SVM `vs0`上の `datalif1`という名前のLIFを `node0b`のポート `e0d`に移行する方法を示しています：

```
network interface migrate -vserver vs0 -lif datalif1 -dest-node node0b
-dest-port e0d
```

次の例は、現在（ローカル）のノードからすべてのデータおよびクラスタ管理LIFを移行する方法を示しています。

```
network interface migrate-all -node local
```

関連情報

- "network interface migrate"

ONTAPノードのフェイルオーバーまたはポート移行後に**LIF**をホームポートに戻す

別のポートにフェイルオーバーまたは移行されたLIFを、手動または自動でホーム ポートにリバートできます。特定のLIFのホーム ポートを利用できない場合、そのLIFは現在のポートにとどまり、リバートされません。

タスク概要

- 自動リバート オプションを設定する前にLIFのホーム ポートの状態をupにすると、LIFはホーム ポートにリバートされません。
- LIFは、「auto-revert」オプションの値をtrueに設定しないかぎり、自動的にリバートされることはありません。
- LIFのホーム ポートにリバートするには、LIFに対して「auto-revert」オプションを有効にする必要があります。

実行する手順は、System ManagerとCLIのどちらのインターフェイスを使用するかによって異なります。

System Manager

System Managerを使用してネットワーク インターフェイスをホーム ポートに戻す

手順

1. *ネットワーク > 概要 > ネットワーク インターフェイス*を選択します。
2. **⋮ > 元に戻す** を選択します（変更したいネットワーク インターフェイスの横）。
3. ネットワーク インターフェイスをホーム ポートに戻すには、*元に戻す*を選択します。

CLI

CLI を使用して **LIF** をホームポートに戻す

手順

LIFをホーム ポートに手動または自動でリバートします。

LIF をホームポートに戻す場合は…	次に、以下のコマンドを入力します…
手動	`network interface revert -vserver vserver_name -lif lif_name`
自動	`network interface modify -vserver vserver_name -lif lif_name -auto-revert true`

`network interface`の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/search.html?q=network+interface["ONTAPコマンド リファレンス"^]をご覧ください。

クラスタ ネットワークがスイッチにケーブル接続されていても、Cluster IPspaceに設定されているすべてのポートが相互に到達可能でない場合はクラスタを作成できません。

タスク概要

スイッチ クラスターでは、クラスター ネットワーク インターフェイス（LIF）が間違ったポートに設定されている場合、またはクラスター ポートが間違ったネットワークに接続されている場合、 `cluster create`コマンドは次のエラーで失敗する可能性があります：

```
Not all local cluster ports have reachability to one another.
Use the "network port reachability show -detail" command for more details.
```

`cluster create`の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/cluster-create.html["ONTAPコマンド リファレンス"^]をご覧ください。

`network port show`コマンドの結果には、クラスタLIFが設定されているポートに接続されているため、複数のポートがクラスタIPspaceに追加されたと表示されることがあります。ただし、 `network port reachability show -detail`コマンドの結果には、相互に接続されていないポートが表示されます。

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

クラスタLIFが設定されている他のポートに到達できないポートに設定されたクラスタLIFをリカバリするには、次の手順を実行します。

手順

1. クラスタLIFのホーム ポートを正しいポートにリセットします。

   ```
   network port modify -home-port
   ```

   `network port modify`の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/network-port-modify.html["ONTAPコマンド リファレンス"^]をご覧ください。

2. クラスタLIFが設定されていないポートをクラスタのブロードキャスト ドメインから削除します。

```
network port broadcast-domain remove-ports
```

`network port broadcast-domain remove-ports`
の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/network-port-broadcast-domain-remove-ports.html["ONTAPコマンド リファレンス"^]をご覧ください。

3. クラスタを作成します。

```
cluster create
```

結果

クラスタの作成が完了すると、正しい設定が検出され、正しいブロードキャスト ドメインにポートが配置されます。

関連情報

- "ネットワークポート到達性の表示"

ONTAP LIFを削除する

不要になったネットワーク インターフェイス（LIF）は削除できます。

開始する前に

削除するLIFが使用されていないことを確認します。

手順

1. 次のコマンドを使用して、削除するLIFを意図的に停止しているものとしてマークします。

```
network interface modify -vserver vserver_name -lif lif_name -status
-admin down
```

2. `network interface delete`コマンドを使用して、1つまたはすべてのLIFを削除します：

削除したい場合…	入力するコマンド
特定のLIF	`network interface delete -vserver vserver_name -lif lif_name`
すべてのLIF	`network interface delete -vserver vserver_name -lif *`

`network interface delete`
の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/network-interface-delete.html["ONTAPコマンド リファレンス"^]をご覧ください。

次のコマンドは、mgmtlif2というLIFを削除します。

```
network interface delete -vserver vs1 -lif mgmtlif2
```

3. `network interface show`コマンドを使用して、LIFが削除されたことを確認します。

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

ONTAP仮想IP（VIP）LIFの設定

一部の次世代データセンターでは、サブネットをまたぐLIFのフェイルオーバーを必要とする、レイヤ3（IP）ネットワークのメカニズムが使用されています。ONTAPでは、仮想IP（VIP）データLIFおよび関連するルーティング プロトコルであるBorder Gateway Protocol（BGP）がサポートされ、これらの次世代ネットワークのフェイルオーバー要件を満たすことができます。

タスク概要

VIPデータLIFは、いずれのサブネットにも属さない、同じIPspace内のBGP LIFをホストするすべてのポートから到達可能なLIFです。VIPデータLIFを使用すると、ホストは個別のネットワーク インターフェイスに依存しなくなります。複数の物理アダプタでデータ トラフィックが処理されるため、すべての負荷が単一のアダプタと関連するサブネットに集中することはありません。VIPデータLIFの存在は、ルーティング プロトコルであるBorder Gateway Protocol（BGP）を通じてピア ルーターに通知されます。

VIPデータLIFには次の利点があります。

- ブロードキャスト ドメインまたはサブネットを越えた LIF の移植性：VIP データ LIF は、各 VIP データ LIF の現在の場所を BGP 経由でルータに通知することにより、ネットワーク内の任意のサブネットにフェイルオーバーできます。
- 総スループット：VIP データ LIF は複数のサブネットまたはポートから同時にデータを送受信できるため、個々のポートの帯域幅を超える総スループットをサポートできます。

Border Gateway Protocol（BGP）のセットアップ

VIP LIFを作成する前にBGPをセットアップする必要があります。BGPは、VIP LIFの存在をピア ルーターに通知するためのルーティング プロトコルです。

ONTAP 9.9.1以降では、設定を簡単にするために、VIPのオプションとしてBGPピア グループを使用したデフォルト ルートの自動化が導入されています。

ONTAPには、BGPピアが同じサブネット上にある場合に、BGPピアをネクストホップルータとして使用してデフォルトルートを学習する簡単な方法があります。この機能を使用するには、 `-use-peer-as-next-hop`属性を `true`に設定します。デフォルトでは、この属性は `false`です。

静的ルートが設定されている場合は、これらの自動デフォルト ルートよりも優先されます。

開始する前に

ピア ルータは、設定された自律システム番号（ASN）の BGP LIF からの BGP 接続を受け入れるように設定する必要があります。

> ONTAPはルータからの着信ルートアナウンスメントを一切処理しません。そのため、ピアルータがクラスタにルート更新を送信しないように設定する必要があります。これにより、ピアとの通信が完全に機能するまでの時間が短縮され、ONTAP内部のメモリ使用量が削減されます。

タスク概要

BGPをセットアップする際には、必要に応じてBGP設定、BGP LIF、BGPピア グループを作成します。あるノードでBGPピア グループが最初に作成されると、デフォルト値を使用してデフォルトのBGP設定が自動的に作成されます。

BGP LIFは、ピア ルーターとのBGP TCPセッションを確立するために使用されます。ピア ルーターから見ると、BGP LIFはVIP LIFに到達するための次のホップです。BGP LIFではフェイルオーバーは無効になります。BGPピア グループは、ピア グループが使用するIPspaceにある、すべてのSVMのVIPルートを通知します。ピア グループが使用するIPspaceは、BGP LIFから継承されます。

ONTAP 9.16.1以降では、BGPセッションを保護するために、BGPピア グループでMD5認証がサポートされます。MD5が有効な状態では、BGPセッションは承認されたピア間でしか確立、処理できません。これにより、無許可ユーザによるセッションの中断を防げます。

`network bgp peer-group create`および `network bgp peer-group modify`コマンドに次のフィールドが追加されました：

- `-md5-enabled <true/false>`
- `-md5-secret <md5 secret in string or hex format>`

これらのパラメータを使用すれば、BGPピア グループにMD5署名を設定してセキュリティを強化できます。MD5認証を使用する際には、以下の要件が適用されます。

- `-md5-enabled`パラメータが `true`に設定されている場合にのみ、 `-md5-secret`パラメータを指定できます。
- MD5 BGP認証を有効にする前に、IPsecをグローバルに有効にする必要があります。BGP LIFにアクティブなIPsec設定は必要ありません。"IP Security（IPsec）のネットワーク上での暗号化設定"を参照してください。
- NetAppは、ONTAPコントローラでMD5を設定する前に、ルーターでMD5を設定することを推奨しています。

ONTAP 9.9.1以降では、次のフィールドが追加されています。

- `-asn`または `-peer-asn`（4 バイト値）属性自体は新しいものではありませんが、現在は 4 バイトの整数を使用します。

- `-med`
- `-use-peer-as-next-hop`

パスの優先順位付けでは、Multi-Exit Discriminator（MED）を使用して高度なルート選択を行うことができます。MEDはBGP更新メッセージのオプションの属性で、トラフィックに最適なルートを選択するようルーターに指示します。MEDは32ビットの符号なし整数（0～4294967295）で、値が小さい方が優先されます。

ONTAP 9.8 以降では、 `network bgp peer-group`コマンドに次のフィールドが追加されました：

- `-asn-prepend-type`
- `-asn-prepend-count`
- `-community`

これらのBGP属性を使用して、BGPピア グループのASパスとコミュニティを設定できます。

ONTAPは上記のBGP属性をサポートしていますが、必ずしもルーターに適用する必要はありません。ルーターでサポートされる属性を確認し、それに応じてBGPピア グループを設定することを強く推奨します。詳細については、ルーターに付属のBGPのドキュメントを参照してください。

手順

1. advanced権限レベルにログインします。

   ```
   set -privilege advanced
   ```

2. オプション：次のいずれかのアクションを実行して、BGP 構成を作成するか、クラスターのデフォルトの BGP 構成を変更します：

   a. BGP設定を作成する場合：

   ```
   network bgp config create -node {node_name | local} -asn <asn_number>
   -holdtime
   <hold_time> -routerid <router_id>
   ```

   - この `-routerid`パラメータは、ASドメイン内で一意である必要があるドット区切りの32ビット値を受け入れます。NetAppでは、一意性を保証する `<router_id>`にノード管理IP（v4）アドレスを使用することを推奨しています。
   - ONTAP BGPは32ビットASN数に対応していますが、サポートされるのは標準的な10進記数法のみです。4259840001ではなく65000.1などのドット付きASN表記は、プライベートASNではサポートされません。

   2バイトのASNの例：

   ```
   network bgp config create -node node1 -asn 65502 -holdtime 180
   -routerid 1.1.1.1
   ```

4バイトのASNの例：

```
network bgp config create -node node1 -asn 85502 -holdtime 180 -routerid
1.1.1.1
```

a. デフォルトのBGP設定を変更する場合：

```
network bgp defaults modify -asn <asn_number> -holdtime <hold_time>
network bgp defaults modify -asn 65502 -holdtime 60
```

- `<asn_number>`ASN番号を指定します。ONTAP 9.8以降、BGPのASNは2バイトの非負整数をサポートします。これは16ビットの数値（1～65534の値）です。ONTAP 9.9.1以降、BGPのASNは4バイトの非負整数（1～4294967295）をサポートします。デフォルトのASNは65501です。ASN 23456は、4バイトASN機能をアナウンスしないピアとのONTAPセッション確立用に予約されています。
- `<hold_time>`ホールド時間を秒単位で指定します。デフォルト値は180sです。

ONTAPは、複数のIPspaceにBGPを設定する場合でも、グローバル`<asn_number>`、`<hold_time>`、および`<router_id>`を1つだけサポートします。BGPとすべてのIPルーティング情報は、1つのIPspace内で完全に分離されます。IPspaceは、仮想ルーティングおよび転送（VRF）インスタンスに相当します。

3. システムSVM用のBGP LIFを作成します。

デフォルトのIPspaceでは、SVM名はクラスタ名になります。追加のIPspaceでは、SVM名はIPspace名と同じになります。

```
network interface create -vserver <system_svm> -lif <lif_name> -service
-policy default-route-announce -home-node <home_node> -home-port
<home_port> -address <ip_address> -netmask <netmask>
```

`default-route-announce`サービス ポリシーをBGP LIFに使用するか、「management-bgp」サービスを含む任意のカスタム サービス ポリシーを使用できます。

```
network interface create -vserver cluster1 -lif bgp1 -service-policy
default-route-announce -home-node cluster1-01 -home-port e0c -address
10.10.10.100 -netmask 255.255.255.0
```

4. リモート ピア ルータとの BGP セッションを確立するために使用される BGP ピア グループを作成し、ピア ルータにアドバタイズされる VIP ルート情報を設定します：

サンプル1：自動デフォルト ルートなしでピア グループを作成する

この場合、管理者がBGPピアへの静的ルートを作成する必要があります。

```
network bgp peer-group create -peer-group <group_name> -ipspace
<ipspace_name> -bgp-lif <bgp_lif> -peer-address <peer-router_ip_address>
-peer-asn <peer_asn_number> {-route-preference <integer>} {-asn-prepend-
type <ASN_prepend_type>} {-asn-prepend-count <integer>} {-med <integer>}
{-community BGP community list <0-65535>:<0-65535>}
```

```
network bgp peer-group create -peer-group group1 -ipspace Default -bgp
-lif bgp1 -peer-address 10.10.10.1 -peer-asn 65503 -route-preference 100
-asn-prepend-type local-asn -asn-prepend-count 2 -med 100 -community
9000:900,8000:800
```

サンプル2：自動デフォルト ルートを持つピア グループを作成する

```
network bgp peer-group create -peer-group <group_name> -ipspace
<ipspace_name> -bgp-lif <bgp_lif> -peer-address <peer-router_ip_address>
-peer-asn <peer_asn_number> {-use-peer-as-next-hop true} {-route-
preference <integer>} {-asn-prepend-type <ASN_prepend_type>} {-asn-
prepend-count <integer>} {-med <integer>} {-community BGP community list
<0-65535>:<0-65535>}
```

```
network bgp peer-group create -peer-group group1 -ipspace Default -bgp
-lif bgp1 -peer-address 10.10.10.1 -peer-asn 65503 -use-peer-as-next-hop
true -route-preference 100 -asn-prepend-type local-asn -asn-prepend
-count 2 -med 100 -community 9000:900,8000:800
```

サンプル3：MD5を有効にしたピアグループを作成する

a. IPsecを有効にします。

   ```
   security ipsec config modify -is-enabled true
   ```

b. MD5が有効なBGPピア グループを作成します。

   ```
   network bgp peer-group create -ipspace Default -peer-group
   <group_name> -bgp-lif bgp_lif -peer-address <peer_router_ip_address>
   {-md5-enabled true} {-md5-secret <md5 secret in string or hex format>}
   ```

   16進数キーを使用する例：

```
network bgp peer-group create -ipspace Default -peer-group peer1 -bgp
-lif bgp_lif1 -peer-address 10.1.1.100 -md5-enabled true -md5-secret
0x7465737420736563726574
```

文字列を使用する例：

```
network bgp peer-group create -ipspace Default -peer-group peer1 -bgp
-lif bgp_lif1 -peer-address 10.1.1.100 -md5-enabled true -md5-secret "test
secret"
```

BGPピアグループを作成した後、 `network port show`コマンドを実行すると仮想イーサネットポート（v0a..v0z、v1a…で始まる）が表示されます。このインターフェースのMTUは常に1500と報告されます。トラフィックに使用される実際のMTUは、トラフィックの送信時に決定される物理ポート（BGP LIF）から取得されます。"ONTAPコマンド リファレンス"の `network port show`の詳細をご覧ください。

仮想**IP**（**VIP**）データ**LIF**の作成

VIPデータLIFの存在は、ルーティング プロトコルであるBorder Gateway Protocol（BGP）を通じてピア ルーターに通知されます。

開始する前に

- BGPピア グループをセットアップし、LIFを作成するSVMのBGPセッションをアクティブにしておく必要があります。
- SVM のすべての送信 VIP トラフィックに対して、BGP ルータまたは BGP LIF のサブネット内の他のルータへの静的ルートを作成する必要があります。
- 送信 VIP トラフィックが利用可能なすべてのルートを使用できるように、マルチパス ルーティングをオンにする必要があります。

  マルチパス ルーティングを有効にしないと、すべての発信VIPトラフィックが1つのインターフェイスから送信されます。

手順

1. VIPデータLIFを作成します。

```
network interface create -vserver <svm_name> -lif <lif_name> -role data
-data-protocol
{nfs|cifs|iscsi|fcache|none|fc-nvme} -home-node <home_node> -address
<ip_address> -is-vip true -failover-policy broadcast-domain-wide
```

`network interface create`コマンドでホーム ポートを指定しない場合は、VIPポートが自動的に選択されます。

作成されたVIPデータLIFは、デフォルトで、各IPspaceに対してシステムで作成されるブロードキャストドメイン「Vip」に属します。VIPブロードキャスト ドメインを変更することはできません。

VIPデータLIFには、IPspaceのBGP LIFをホストするすべてのポートから同時に到達できます。ローカルノードにVIPのSVM用のアクティブなBGPセッションがない場合は、VIPデータLIFはそのSVM用のBGPセッションが確立されているノード上のVIPポートにフェイルオーバーします。

2. VIPデータLIFのSVMに対してBGPセッションがupステータスになっていることを確認します。

```
network bgp vserver-status show

Node        Vserver  bgp status
          ----------  -------- ---------
          node1       vs1      up
```

ノード上のSVMのBGPステータスが `down`の場合、VIPデータLIFは、SVMのBGPステータスがupである別のノードにフェイルオーバーします。すべてのノードでBGPステータスが `down`の場合、VIPデータLIFはどこにもホストできず、LIFステータスはdownになります。

BGPの管理用コマンド

ONTAP 9.5以降では、 `network bgp`コマンドを使用してONTAPのBGPセッションを管理します。

BGP設定の管理

状況	使用するコマンド
BGP設定を作成する	`network bgp config create`
BGP設定を変更する	`network bgp config modify`
BGP設定を削除する	`network bgp config delete`
BGP設定を表示する	`network bgp config show`
VIP LIFのSVMに対するBGPステータスを表示する	`network bgp vserver-status show`

BGPのデフォルト値の管理

状況	使用するコマンド
BGPのデフォルト値を変更する	`network bgp defaults modify`
BGPのデフォルト値を表示する	`network bgp defaults show`

BGPピア グループの管理

状況	使用するコマンド
BGPピア グループを作成する	`network bgp peer-group create`
BGPピア グループを変更する	`network bgp peer-group modify`

BGPピア グループを削除する	`network bgp peer-group delete`
BGPピア グループの情報を表示する	`network bgp peer-group show`
BGPピア グループの名前を変更する	`network bgp peer-group rename`

MD5を使用する**BGP**ピア グループの管理

ONTAP 9.16.1以降では、既存のBGPピア グループでMD5認証の有効と無効を切り替えることができます。

既存のBGPピア グループでMD5を有効または無効にすると、MD5設定の変更を適用するためにBGP接続が終了され、再作成されます。

状況	使用するコマンド
既存のBGPピア グループでMD5を有効にする	`network bgp peer-group modify -ipspace Default -peer-group <group_name> -bgp -lif <bgp_lif> -peer-address <peer_router_ip_address> -md5-enabled true -md5-secret <md5 secret in string or hex format>`
既存のBGPピア グループでMD5を無効にする	`network bgp peer-group modify -ipspace Default -peer-group <group_name> -bgp -lif <bgp_lif> -md5-enabled false`

関連情報

- "ONTAPコマンド リファレンス"
- "ネットワーク BGP"
- "ネットワーク インターフェイス"
- "security ipsec config modify"

ネットワーク負荷の分散

DNS ロード バランシングを使用した ONTAP ネットワーク トラフィックの最適化

負荷が適切に割り当てられたLIFでクライアント要求を処理するようにクラスタを設定することができます。この設定によって、LIFとポートがバランスよく使用されるようになり、クラスタのパフォーマンスが向上します。

DNSロード バランシングを使用すると、負荷が適切なデータLIFを選んで、使用可能なデータ ポートすべて（物理、インターフェイス グループ、VLAN）にユーザ ネットワークのトラフィックを分散させることができます。

DNSロード バランシングでは、LIFがSVMのロード バランシング ゾーンに関連付けられます。サイト規模のDNSサーバは、すべてのDNSリクエストを転送し、ネットワーク トラフィックとポートの利用可能なリソース（CPU使用率、スループット、開いている接続など）に基づいて負荷の最も少ないLIFを返すように設定されています。DNSロード バランシングのメリットは次のとおりです。

- 新しいクライアント接続が、使用可能なリソース全体に基づいて分散されます。
- 特定のSVMをマウントするときに使用するLIFを手動で決める必要がありません。
- NFSv3、NFSv4、NFSv4.1、SMB 2.0、SMB 2.1、SMB 3.0、およびS3をサポートしています。

ONTAP ネットワークの DNS ロード バランシングについて学ぶ

クライアントがSVMをマウントするには、（LIFに関連付けられた）IPアドレスか（複数のIPアドレスに関連付けられた）ホスト名を指定します。デフォルトでは、LIFはサイト全体のDNSサーバによってラウンドロビン方式で選択されます。これにより、すべてのLIF間にワークロードが分散されます。

ラウンドロビン方式の負荷分散では、一部のLIFが過負荷になることがあります。そのため、DNSロード バランシング ゾーンを使用して、SVMでホスト名解決を処理するオプションもあります。DNSロード バランシング ゾーンを使用すると、使用可能なリソース全体で新しいクライアント接続のバランスが改善され、クラスタのパフォーマンスが向上します。

DNSロード バランシング ゾーンは、すべてのLIFの負荷を動的に評価し、負荷が適切に割り当てられたLIFを返す、クラスタ内のDNSサーバです。ロード バランシング ゾーンでは、DNSによって負荷に基づく重み（指標）が各LIFに割り当てられます。

すべてのLIFに、ポートの負荷とホーム ノードのCPU利用率に基づく重みが割り当てられます。DNSクエリでは、負荷が少ないポートのLIFが返される可能性が高くなります。重みは手動で割り当てることもできます。

ONTAPネットワークのDNSロード バランシング ゾーンを作成する

DNSロード バランシング ゾーンを作成すると、負荷（LIFにマウントされているクライアントの数）に基づくLIFの動的選択が容易になります。ロード バランシング ゾーンはデータLIFを作成するときに作成できます。

開始する前に

サイト規模のDNSサーバ上に、設定したLIFにロード バランシング ゾーンに対するすべての要求を転送するDNSフォワーダを設定しておく必要があります。

"NetApp ナレッジ ベース：clustered Data ONTAP で DNS ロード バランシングを設定する方法"には、条件付き転送を使用した DNS ロード バランシングの設定に関する詳細情報が記載されています。

タスク概要

- どのデータLIFでも、DNSロード バランシング ゾーン名のDNSクエリに応答できます。
- DNSロード バランシング ゾーンの名前はクラスタ内で一意でなければなりません。ゾーン名の要件は次のとおりです。
  - 最大文字数は256文字です。
  - ピリオドが少なくとも1つ必要です。
  - 先頭および末尾の文字をピリオドなどの特殊文字にすることはできません。
  - 文字間にスペースを使用することはできません。
  - DNS名の各ラベルの最大文字数は63文字です。

ラベルは、ピリオドの前後のテキストです。たとえば、storage.company.comという名前のDNSゾーンは3つのラベルで構成されています。

手順

`network interface create`コマンドに `dns-zone`オプションを指定して、DNSロード バランシング ゾーンを作成します。link:https://docs.netapp.com/us-en/ontap-cli/network-interface-create.html["ONTAPコマンド リファレンス"^]の `network interface create`の詳細をご覧ください。

ロード バランシング ゾーンがすでに存在する場合は、LIFがそのロード バランシング ゾーンに追加されます。

次の例は、LIF `lif1`の作成時に storage.company.com という名前の DNS ロード バランシング ゾーンを作成する方法を示しています：

```
network interface create -vserver vs0 -lif lif1 -home-node node1
-home-port e0c -address 192.0.2.129 -netmask 255.255.255.128 -dns-zone
storage.company.com
```

ロード バランシング ゾーンへのONTAP LIFの追加または削除

Storage Virtual Machine（SVM）のDNSロード バランシング ゾーンに対してLIFを追加または削除できます。すべてのLIFをロード バランシング ゾーンから同時に削除することもできます。

開始する前に

- ロード バランシング ゾーンのLIFは、すべて同じSVMに属している必要があります。
- LIFは1つのDNSロード バランシング ゾーンだけに含めることができます。
- サブネットの異なるLIFがある場合は、サブネットごとのフェイルオーバー グループが設定されている必要があります。

タスク概要

管理ステータスがdownのLIFは一時的にDNSロード バランシング ゾーンから削除されます。LIFの管理ステータスがupに戻ると、自動的にDNSロード バランシング ゾーンに追加されます。

手順

ロード バランシング ゾーンに対してLIFを追加または削除します。

状況	入力する内容
LIFを追加する	`network interface modify -vserver` *`vserver_name`* `-lif` *`lif_name`* `-dns-zone` *`zone_name`* 例： `network interface modify -vserver vs1 -lif data1 -dns -zone cifs.company.com`

単一のLIFを削除する	`network interface modify -vserver vserver_name -lif lif_name -dns-zone none` 例：`network interface modify -vserver vs1 -lif data1 -dns-zone none`
すべてのLIFを削除する	`network interface modify -vserver vserver_name -lif * -dns-zone none` 例： `network interface modify -vserver vs0 -lif * -dns-zone none` ロード バランシング ゾーンから SVM を削除するには、そのゾーンから SVM 内のすべての LIF を削除します。

関連情報

- "network interface modify"

ONTAPネットワークのDNSサービスを設定する

NFSまたはSMBサーバを作成する前に、SVM用のDNSサービスを設定する必要があります。通常、DNSネーム サーバは、NFSまたはSMBサーバが参加するドメインのActive Directory統合DNSサーバです。

タスク概要

Active Directory統合DNSサーバには、ドメインLDAPおよびドメイン コントローラ サーバのサービス ロケーション レコード（SRV）が格納されます。SVMがActive Directory LDAPサーバおよびドメイン コントローラを見つけられない場合は、NFSまたはSMBサーバのセットアップに失敗します。

SVMは、ホストについての情報を検索する際に、hostsネーム サービスns-switchデータベースを使用してどのネーム サービスを使用するか、どの順番で使用するかを決定します。ホスト データベースとしてサポートされている2つのネーム サービスは、filesおよびdnsです。

SMBサーバを作成する前に、dnsがソースの1つであることを確認する必要があります。

mgwdプロセスとSecDプロセスについてDNSネーム サービスの統計を表示するには、統計画面を使用します。

手順

1. hostsネーム サービス データベースの現在の設定を確認します。この例では、hostsネーム サービス データベースはデフォルトの設定を使用しています。

   `vserver services name-service ns-switch show -vserver vs1 -database hosts`

   ```
   Vserver: vs1
   Name Service Switch Database: hosts
   Vserver: vs1 Name Service Switch Database: hosts
   Name Service Source Order: files, dns
   ```

2. 必要に応じて、次の操作を実行します。

a. DNSネーム サービスを希望の順番でhostsネーム サービス データベースに追加するか、ソースの順番を変更します。

   この例では、DNSおよびローカル ファイルをこの順番で使用するようにhostsデータベースを設定しています。

   ```
   vserver services name-service ns-switch modify -vserver vs1 -database hosts
   -sources dns,files
   ```

b. ネーム サービスの設定が正しいことを確認します。

   ```
   vserver services name-service ns-switch show -vserver vs1 -database hosts
   ```

```
Vserver: vs1
Name Service Switch Database: hosts
Name Service Source Order: dns, files
```

3. DNS サービスを設定します。

   ```
   vserver services name-service dns create -vserver vs1 -domains
   example.com,example2.com -name-servers 10.0.0.50,10.0.0.51
   ```

   vserver services name-service dns createコマンドによって設定が自動検証され、ONTAPがネーム サーバに接続できない場合はエラー メッセージが報告されます。

4. DNSの設定が正しいことと、サービスが有効になっていることを確認します。

```
Vserver: vs1
Domains: example.com, example2.com Name Servers: 10.0.0.50, 10.0.0.51
Enable/Disable DNS: enabled Timeout (secs): 2
Maximum Attempts: 1
```

5. ネーム サーバのステータスを検証します。

   ```
   vserver services name-service dns check -vserver vs1
   ```

```
Vserver  Name Server  Status  Status Details
vs1      10.0.0.50    up      Response time (msec): 2
vs1      10.0.0.51    up      Response time (msec): 2
```

SVMでの動的**DNS**の設定

Active Directory統合DNSサーバをDNSにあるNFSまたはSMBサーバのDNSレコードに動的に登録する場合は、SVMで動的DNS（DDNS）を設定する必要があります。

開始する前に

SVMでは、DNSネーム サービスが設定される必要があります。Secure DDNSを使用する場合は、Active Directory統合DNSネーム サーバを使用して、SVM用のNFSまたはSMBサーバあるいはActive Directoryアカウントを作成しておく必要があります。

タスク概要

一意の完全修飾ドメイン名（FQDN）を指定する必要があります。

一意の完全修飾ドメイン名（FQDN）を指定する必要があります。

- NFS の場合、 `vserver services name-service dns dynamic-update`コマンドの一部として `-vserver-fqdn` で指定された値は、LIF の登録済み FQDN になります。
- SMBの場合、CIFSサーバのNetBIOS名およびCIFSサーバの完全修飾ドメイン名として指定した値がLIFの登録済みFQDNになります。これはONTAPでは設定できません。次のシナリオでは、LIFのFQDNは「CIFS_VS1.EXAMPLE.COM」です。

```
cluster1::> cifs server show -vserver vs1

                                          Vserver: vs1
                        CIFS Server NetBIOS Name: CIFS_VS1
                    NetBIOS Domain/Workgroup Name: EXAMPLE
                      Fully Qualified Domain Name: EXAMPLE.COM
                              Organizational Unit: CN=Computers
Default Site Used by LIFs Without Site Membership:
                                   Workgroup Name: -
                                   Kerberos Realm: -
                                Authentication Style: domain
                CIFS Server Administrative Status: up
                          CIFS Server Description:
                          List of NetBIOS Aliases: -
```

DDNSアップデートのRFCルールに準拠していないSVM FQDNの設定エラーを回避するには、RFCに準拠したFQDN名を使用してください。詳細については、"RFC 1123"を参照してください。

手順

1. SVMでDDNSを設定します。

   ```
   vserver services name-service dns dynamic-update modify -vserver vserver_name
   -is- enabled true [-use-secure {true|false} -vserver-fqdn
   FQDN_used_for_DNS_updates

   vserver services name-service dns dynamic-update modify -vserver vs1 -is
   -enabled true - use-secure true -vserver-fqdn vs1.example.com
   ```

   カスタマイズされた FQDN の一部としてアスタリスクを使用することはできません。たとえば、`*.netapp.com`は無効です。

2. DDNSの設定が正しいことを確認します。

```
vserver services name-service dns dynamic-update show
```

```
Vserver  Is-Enabled Use-Secure Vserver FQDN      TTL
-------- ---------- ---------- ----------------- -------
vs1      true       true       vs1.example.com   24h
```

ONTAPネットワークのダイナミックDNSサービスを構成する

Active Directory統合DNSサーバをDNSにあるNFSまたはSMBサーバのDNSレコードに動的に登録する場合は、SVMで動的DNS（DDNS）を設定する必要があります。

開始する前に

SVMでは、DNSネーム サービスが設定される必要があります。Secure DDNSを使用する場合は、Active Directory統合DNSネーム サーバを使用して、SVM用のNFSまたはSMBサーバあるいはActive Directoryアカウントを作成しておく必要があります。

タスク概要

指定するFQDNは一意である必要があります。

> SVM FQDNの設定エラー（DDNS更新のためのRFCルールに準拠していない）を回避するには、RFC準拠のFQDN名を使用してください。

手順

1. SVMでDDNSを設定します。

```
vserver services name-service dns dynamic-update modify -vserver vserver_name
-is- enabled true [-use-secure {true|false} -vserver-fqdn
FQDN_used_for_DNS_updates

vserver services name-service dns dynamic-update modify -vserver vs1 -is
-enabled true - use-secure true -vserver-fqdn vs1.example.com
```

カスタマイズされた FQDN の一部としてアスタリスクを使用することはできません。たとえば、`*.netapp.com`は無効です。

2. DDNSの設定が正しいことを確認します。

```
vserver services name-service dns dynamic-update show
```

```
Vserver  Is-Enabled Use-Secure Vserver FQDN      TTL
-------- ---------- ---------- ----------------- -------
vs1      true       true       vs1.example.com   24h
```

ホスト名解決

ONTAPネットワークのホスト名解決について学ぶ

ONTAPでは、クライアントにアクセスを提供したりサービスにアクセスしたりするために、ホスト名を数値のIPアドレスに変換できなければなりません。Storage Virtual Machine（SVM）でローカルまたは外部のネーム サービスを使用してホスト情報を解決するように設定する必要があります。ONTAPでは、ホスト名を解決するために外部DNSサーバまたはローカルのhostsファイルを使用するように設定できます。

外部DNSサーバを使用する場合は、動的DNS（DDNS）を設定できます。これにより、新規または変更されたDNS情報がストレージ システムからDNSサーバに自動的に送信されます。動的DNS更新を使用しない場合は、新しいシステムがオンラインになったときや既存のDNS情報が変更されたときに、特定されたDNSサーバに手動でDNS情報（DNSの名前とIPアドレス）を追加する必要があります。このプロセスは時間がかかるだけでなく、エラーも起こりやすくなります。ディザスタ リカバリの際に手動で設定を行っていると、停止時間が長引くことにもなりかねません。

ONTAPネットワークのホスト名解決用にDNSを設定する

ホスト情報を取得するには、DNSを使用してローカル ソースまたはリモート ソースにアクセスします。これらのソースのいずれか、または両方にアクセスするためにDNSを設定する必要があります。

ONTAPがクライアントに適切なアクセスを許可するには、ホスト情報を検索できなければなりません。ネーム サービスを設定して、ONTAPがホスト情報を取得するためにローカルまたは外部のDNSサービスにアクセスできるようにします。

ONTAP は、UNIX システムの `/etc/nsswitch.conf` ファイルに相当するテーブルにネーム サービス構成情報を保存します。

外部DNSサーバを使用してホスト名を解決するためのSVMとデータLIFの設定

`vserver services name-service dns`コマンドを使用してSVMでDNSを有効にし、ホスト名の解決にDNSを使用するように設定できます。ホスト名は外部DNSサーバを使用して解決されます。

開始する前に

ホスト名を検索するために、サイト規模のDNSサーバが使用できなければなりません。

単一障害点を回避するため、複数のDNSサーバーを設定する必要があります。 `vserver services name-service dns create`コマンドは、DNSサーバー名を1つだけ入力した場合に警告を発します。

タスク概要

SVM での動的 DNS の設定の詳細については、ダイナミック DNS サービスを構成するを参照してください。

手順

1. SVMでDNSを有効にします。

```
vserver services name-service dns create -vserver <vserver_name>
-domains <domain_name> -name-servers <ip_addresses> -state enabled
```

次のコマンドは、vs1というSVMで外部DNSサーバを有効にします。

```
vserver services name-service dns create -vserver vs1.example.com
-domains example.com -name-servers 192.0.2.201,192.0.2.202 -state
enabled
```

> この `vserver services name-service dns create`コマンドは自動構成検証を実行し、ONTAPがネームサーバに接続できない場合はエラーメッセージを報告します。

2. `vserver services name-service dns check`コマンドを使用してネームサーバーのステータスを検証します。

```
vserver services name-service dns check -vserver vs1.example.com
                                    Name Server
Vserver             Name Server     Status       Status Details
-------------       --------------- ------------
--------------------------
vs1.example.com     10.0.0.50       up           Response time (msec): 2
vs1.example.com     10.0.0.51       up           Response time (msec): 2
```

DNS に関連するサービスポリシーの詳細については、"LIFとサービス ポリシー（ONTAP 9.6以降）"を参照してください。

ホスト名解決で使用するネーム サービス スイッチ テーブルの設定

ONTAPがホスト情報を取得するためにローカルまたは外部のネーム サービスにアクセスできるようにするには、ネーム サービス スイッチ テーブルを正しく設定する必要があります。

開始する前に

環境内のホストのマッピングでどのネーム サービスを使用するかを決めておく必要があります。

手順

1. ネーム サービス スイッチ テーブルに必要なエントリを追加します。

```
vserver services name-service ns-switch modify -vserver <vserver_name>
-database <database_name> -source <source_names>
```

2. ネーム サービス スイッチ テーブルに想定されるエントリが適切な順序で格納されていることを確認します。

```
vserver services name-service ns-switch show -vserver <vserver_name>
```

例

次の例は、SVM vs1のネーム サービス スイッチ テーブルで、ホスト名を解決するためにまずローカルのhostsファイルを使用し、次に外部DNSサーバを使用するようにエントリを変更しています。

```
vserver services name-service ns-switch modify -vserver vs1 -database
hosts -sources files,dns
```

ONTAPホストテーブルを管理するためのONTAPコマンド

クラスタ管理者は、管理Storage Virtual Machine（SVM）のhostsテーブルのホスト名エントリを追加、変更、削除、表示できます。SVM管理者が設定できるのは、割り当てられたSVMのホスト名エントリのみです。

ローカル ホスト名エントリの管理用コマンド

`vserver services name-service dns hosts`コマンドを使用して、DNSホストテーブルエントリを作成、変更、または削除できます。

DNSホスト名エントリを作成または変更するときは、複数のエイリアス アドレスをカンマで区切って指定できます。

状況	使用するコマンド
DNSホスト名エントリを作成する	`vserver services name-service dns hosts create`
DNSホスト名エントリを変更する	`vserver services name-service dns hosts modify`
DNSホスト名エントリを削除する	`vserver services name-service dns hosts delete`

`vserver services name-service dns hosts`コマンドの詳細については、https://docs.netapp.com/us-en/ontap-cli["ONTAPコマンド リファレンス"^]を参照してください。

ネットワークの保護

すべてのSSL接続に対してFIPSを使用してONTAPネットワークセキュリティを構成する

ONTAPは、すべてのSSL接続において連邦情報処理標準（FIPS）140-2に準拠しています。SSL FIPSモードのオン/オフを切り替えたり、SSLプロトコルをグローバルに設定したり、ONTAP内の脆弱な暗号を無効にしたりできます。

デフォルトでは、ONTAP の SSL は FIPS 準拠が無効に設定され、次の TLS プロトコルが有効になっています：

- TLSv1.3（ONTAP 9.11.1以降）
- TLSv1.2

以前のONTAPリリースでは、次のTLSプロトコルがデフォルトで有効になっていました：

- TLSv1.1（ONTAP 9.12.1以降ではデフォルトで無効）
- TLSv1（ONTAP 9.8以降ではデフォルトで無効）

SSL FIPSモードが有効な場合は、ONTAPからONTAP外部のクライアントまたはサーバ コンポーネントへのSSL通信に、FIPSに準拠したSSL用の暗号が使用されます。

管理者アカウントがSSH公開鍵を使用してSVMにアクセスできるようにする場合は、SSL FIPSモードを有効にする前に、ホスト キー アルゴリズムがサポートされていることを確認する必要があります。

注： ONTAP 9.11.1 以降のリリースでは、ホスト キー アルゴリズムのサポートが変更されました。

ONTAPリリース	サポートされているキーのタイプ	サポートされていないキー タイプ
9.11.1以降	ecdsa-sha2-nistp256	rsa-sha2-512 ＋ rsa-sha2-256 ＋ ssh-ed25519 ＋ ssh-dss ＋ ssh-rsa
9.10.1以前	ecdsa-sha2-nistp256 ＋ ssh-ed25519	ssh-dss ＋ ssh-rsa

サポートされるキー アルゴリズムを使用していない既存のSSH公開鍵アカウントは、FIPSを有効にする前に、サポートされるキー アルゴリズムで再設定する必要があります。この処理を実行しないと管理者認証は失敗します。

詳細については、"SSH公開鍵アカウントの有効化"を参照してください。

ONTAP 9.18.1では、SSLでML-KEM、ML-DSA、SLH-DSAといった量子コンピュータ耐性暗号アルゴリズムのサポートが導入され、将来起こり得る量子コンピュータ攻撃に対するセキュリティがさらに強化されます。これらのアルゴリズムはFIPSは無効ですの場合にのみ利用可能です。量子コンピュータ耐性暗号アルゴリズムは、FIPSが無効で、ピアがそれらをサポートしている場合にネゴシエートされます。

FIPS を有効にする

システムのインストールまたはアップグレードの直後に、すべてのセキュアなユーザがセキュリティ設定を調整することを推奨します。SSL FIPSモードが有効な場合は、ONTAPからONTAP外部のクライアントまたはサーバ コンポーネントへのSSL通信に、FIPSに準拠したSSL用の暗号が使用されます。

FIPSが有効な場合、4096ビットのRSAキーを使用する証明書をインストールまたは作成することはできません。

手順

1. advanced権限レベルに切り替えます。

   ```
   set -privilege advanced
   ```

2. FIPSを有効にします。

   ```
   security config modify * -is-fips-enabled true
   ```

3. 続行するように求められたら、 `y`を入力してください
4. ONTAP 9.9.1以降では、再起動は不要です。ONTAP 9.8以前を実行している場合は、クラスタ内の各ノードを1つずつ手動で再起動してください。

例

ONTAP 9.9.1以降を実行している場合、警告メッセージは表示されません。

```
security config modify -is-fips-enabled true

Warning: This command will enable FIPS compliance and can potentially
cause some non-compliant components to fail. MetroCluster and Vserver DR
require FIPS to be enabled on both sites in order to be compatible.
Do you want to continue? {y|n}: y

Warning: When this command completes, reboot all nodes in the cluster.
This is necessary to prevent components from failing due to an
inconsistent security configuration state in the cluster. To avoid a
service outage, reboot one node at a time and wait for it to completely
initialize before rebooting the next node. Run "security config status
show" command to monitor the reboot status.
Do you want to continue? {y|n}: y
```

`security config modify`および SSL FIPS モード構成の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/security-config-modify.html["ONTAPコマンド リファレンス"^]を参照してください。

FIPSの無効化

ONTAP 9.18.1以降、ONTAPのSSLはML-KEM、ML-DSA、およびSLH-DSAのポスト量子コンピューティング暗号化アルゴリズムをサポートします。これらのアルゴリズムは、FIPSが無効で、ピアがこれらのアルゴリズムをサポートしている場合にのみ使用できます。

手順

1. advanced権限レベルに切り替えます。

   ```
   set -privilege advanced
   ```

2. 次のように入力してFIPSを無効にします。

   ```
   security config modify -is-fips-enabled false
   ```

3. 続行するように求められたら、 `y`と入力します。
4. ONTAP 9.9.1以降では、再起動は不要です。ONTAP 9.8以前を実行している場合は、クラスタ内の各ノードを手動で再起動してください。

SSLv3 プロトコルを使用する必要がある場合は、上記の手順で FIPS を無効にする必要があります。SSLv3 は、FIPS が無効になっている場合にのみ有効にできます。

次のコマンドでSSLv3を有効にできます。ONTAP 9.9.1以降を実行している場合は、警告メッセージは表示されません。

```
security config modify -supported-protocols SSLv3

Warning: Enabling the SSLv3 protocol may reduce the security of the
interface, and is not recommended.
Do you want to continue? {y|n}: y

Warning: When this command completes, reboot all nodes in the cluster.
This is necessary to prevent components from failing due to an
inconsistent security configuration state in the cluster. To avoid a
service outage, reboot one node at a time and wait for it to completely
initialize before rebooting the next node. Run "security config status
show" command to monitor the reboot status.
Do you want to continue? {y|n}: y
```

FIPS準拠ステータスの表示

クラスタ全体が現在のセキュリティ設定を実行しているかどうかを確認できます。

手順

1. ONTAP 9.8 以前を実行している場合は、クラスタ内の各ノードを 1 つずつ手動で再起動します。
2. 現在の準拠ステータスを表示します。

   ```
   security config show
   ```

```
cluster1::> security config show
Cluster    Supported
FIPS Mode  Protocols Supported Cipher Suites
---------- ---------
-----------------------------------------------------------
false      TLSv1.3,  TLS_RSA_WITH_AES_128_CCM,
TLS_RSA_WITH_AES_128_CCM_8,
           TLSv1.2   TLS_RSA_WITH_AES_128_GCM_SHA256,
                     TLS_RSA_WITH_AES_128_CBC_SHA,
                     TLS_RSA_WITH_AES_128_CBC_SHA256,
TLS_RSA_WITH_AES_256_CCM,
                     TLS_RSA_WITH_AES_256_CCM_8,
                     ...
```

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

関連情報

- "FIPS 203：Module-Lattice-Based Key-Encapsulation Mechanism Standard（ML-KEM）"
- "FIPS 204：Module-Lattice-Based Digital Signature Standard（ML-DSA）"
- "FIPS 205：ステートレス ハッシュベース デジタル署名標準（SLH-DSA）"

IPSecの転送中暗号化の設定

ONTAPネットワークでIPセキュリティを使用するための準備

ONTAP 9.8以降では、必要に応じてIPセキュリティ（IPsec）を使用してネットワークトラフィックを保護できます。IPSecは、ONTAPで使用できるいくつかの移動中 / 転送中データ暗号化オプションの1つです。本番環境でIPSecを使用する前に、IPSecを設定する準備をしておく必要があります。

ONTAPでのIPセキュリティの実装

IPsecは、IETFによって管理されるインターネット標準です。ネットワーク エンドポイント間を流れるトラフィックの、IPレベルでのデータ暗号化、データ整合性、認証を実現します。

ONTAPでは、ONTAPとさまざまなクライアントの間のあらゆるIPトラフィック（NFS、SMB、iSCSIプロトコルなど）が、IPsecによって保護されます。プライバシーとデータ整合性を確保するだけでなく、リプレイ攻撃や中間者攻撃などの各種攻撃からネットワーク トラフィックを守ります。ONTAPでは、トランスポートモードのIPsec実装を使用します。IPv4かIPv6を使用してONTAPとクライアントの間でキー マテリアルをネゴシエートするために、Internet Key Exchange（IKE）プロトコル バージョン2を利用します。

クラスタでIPSec機能を有効にすると、さまざまなトラフィック特性に一致するONTAPセキュリティ ポリシ

ー データベース（SPD）のエントリが、ネットワークに1つ以上必要になります。これらのエントリは、データの処理と送信に必要な特定の保護の詳細（暗号スイートや認証方式など）にマッピングされます。各クライアントにも、対応するSPDエントリが必要です。

トラフィックの種類によっては、別の移動中データ暗号化オプションが望ましいものもあります。たとえば、NetApp SnapMirrorとクラスタ ピアリング トラフィックの暗号化については、IPsecではなくTransport Layer Security（TLS）プロトコルが一般的に推奨されます。これは、ほとんどの状況でTLSの方が高いパフォーマンスが得られるためです。

関連情報

- "Internet Engineering Task Force"
- "RFC 4301：インターネット プロトコルのセキュリティ アーキテクチャ"

ONTAP IPsec実装の進化

IPsecはONTAP 9.8で初めて導入されました。その実装は、以下に説明するように、その後のONTAPリリースで進化を続けています。

ONTAP 9.18.1

IPsec ハードウェア オフロードのサポートが IPv6 トラフィックに拡張されました。

ONTAP 9.17.1

IPsec ハードウェア オフロードのサポートが"リンク アグリゲーション グループ"に拡張されました。"耐量子事前共有鍵（PPK）"は IPsec 事前共有キー（PSK）認証でサポートされています。

ONTAP 9.16.1

暗号化や整合性チェックなどの暗号化操作の一部は、サポートされているNICカードにオフロードできます。詳細については、IPSecのハードウェア オフロード機能を参照してください。

ONTAP 9.12.1

MetroCluster IP構成とファブリック接続MetroCluster構成で、フロントエンドのホスト プロトコルとしてIPsecがサポートされました。MetroClusterクラスタでのIPsecのサポートはフロントエンドのホスト トラフィックに限定され、MetroClusterのクラスタ間LIFではサポートされません。

ONTAP 9.10.1

IPsec認証には、PSKに加えて証明書も使用できます。ONTAP 9.10.1より前のバージョンでは、認証にはPSKのみがサポートされています。

ONTAP 9.9.1

IPsecで使用される暗号化アルゴリズムが、FIPS 140-2準拠になりました。これらのアルゴリズムは、FIPS 140-2認定を受けたONTAPのNetApp Cryptographic Moduleで処理されています。

ONTAP 9.8

IPsecのサポートが、トランスポート モードの実装に基づいて初めて利用可能になりました。

IPSecのハードウェア オフロード機能

ONTAP 9.16.1以降を使用している場合、暗号化や整合性チェックなど、計算負荷の高い特定の処理を、ストレージ ノードにインストールされたネットワーク インターフェイス コントローラー（NIC）カードにオフロードするオプションがあります。NICカードにオフロードされた処理のスループットは約5%以下です。これにより、IPsecで保護されたネットワーク トラフィックのパフォーマンスとスループットが大幅に向上しま

す。

要件と推奨事項

IPsecのハードウェア オフロード機能を使用する前に、考慮しておくべき要件がいくつかあります。

サポートされるイーサネット カード

サポートされているイーサネット カードのみをインストールして使用する必要があります。ONTAP 9.16.1 以降では、次のイーサネット カードがサポートされています：

- X50131A（2p、40G/100G/200G/400G Ethernetコントローラ）
- X60132A（4p、10G/25G Ethernet Controller）

ONTAP 9.17.1 では、次のイーサネット カードのサポートが追加されました。

- X50135A（2p、40G/100G Ethernet Controller）
- X60135A（2p、40G/100G Ethernet Controller）

X50131A および X50135A カードは、次のプラットフォームでサポートされています：

- ASA A1K
- ASA A90
- ASA A70
- AFF A1K用
- AFF A90
- AFF A70

X60132A および X60135A カードは、次のプラットフォームでサポートされています：

- ASA A50
- ASA A30
- ASA A20
- AFF A50
- AFF A30
- AFF A20用

サポートされているプラットフォームとカードの詳細については、"NetApp Hardware Universe"を参照してください。

クラスタ スコープ

IPsecハードウェアオフロード機能はクラスタ全体でグローバルに設定されます。そのため、例えば `security ipsec config`コマンドはクラスタ内のすべてのノードに適用されます。

構成の一貫性

サポートされているNICカードが、クラスタ内のすべてのノードに取り付けられている必要があります。サポートされているNICカードが一部のノードでしか使用できない場合、一部のLIFがオフロード対応のNICにホストされていないと、フェイルオーバー後にパフォーマンスが大幅に低下することがあります。

アンチリプレイの無効化

ONTAP（デフォルト設定）およびIPsecクライアントでIPsecアンチリプレイ保護を無効にする必要があります。無効にしない場合、フラグメンテーションとマルチパス（冗長ルート）はサポートされません。

ONTAP IPsec 設定がデフォルトから変更され、アンチリプレイ保護が有効になっている場合は、次のコマンドを使用して無効にします：

```
security ipsec config modify -replay-window 0
```

クライアントでIPsecアンチリプレイ保護が無効になっていることを確認する必要があります。アンチリプレイ保護を無効にするには、クライアントのIPsecドキュメントを参照してください。

制限事項

IPsecのハードウェア オフロード機能を使用する前に、考慮しておくべき制限事項がいくつかあります。

IPv6

ONTAP 9.18.1以降では、IPsecハードウェアオフロード機能でIPv6がサポートされます。ONTAP 9.18.1より前のバージョンでは、IPsecハードウェアオフロードはIPv6をサポートしていません。

拡張シーケンス番号

IPSecの拡張シーケンス番号は、ハードウェア オフロード機能ではサポートされていません。通常の32ビットシーケンス番号のみが使用されます。

リンク アグリゲーション

ONTAP 9.17.1 以降では、IPsec ハードウェア オフロード機能を"リンク アグリゲーション グループ"で使用できます。

9.17.1より前のバージョンでは、IPsecハードウェアオフロード機能はリンクアグリゲーションをサポートしていません。ONTAP CLIの `network port ifgrp`コマンドで管理されるインターフェースまたはリンクアグリゲーショングループでは使用できません。

ONTAP CLIでの設定のサポート

ONTAP 9.16.1では、既存の3つのCLIコマンドが更新され、以下に説明するIPsecハードウェアオフロード機能がサポートされます。詳細については、"ONTAPでのIPセキュリティの設定"も参照してください。

ONTAPコマンド	更新
`security ipsec config show`	ブール型パラメータ `Offload Enabled`は、現在の NIC オフロード ステータスを表示します。
`security ipsec config modify`	このパラメータ `is-offload-enabled`を使用して、NIC オフロード機能を有効または無効にすることができます。
`security ipsec config show-ipsecsa`	インバウンド トラフィックとアウトバウンド トラフィックをバイト数とパケット数で表示するために、4つの新しいカウンタが追加されています。

ONTAP REST APIでの設定のサポート

ONTAP 9.16.1では、以下に説明するように、IPSecのハードウェア オフロード機能をサポートするために、既存の2つのREST APIエンドポイントが更新されています。

RESTエンドポイント	更新
`/api/security/ipsec`	パラメータ `offload_enabled`が追加され、PATCHメソッドで使用できるようになりました。
`/api/security/ipsec/security_association`	オフロード機能で処理された総バイト数とパケット数を追跡するために、2つの新しいカウンタ値が追加されています。

ONTAP REST APIの詳細（ "ONTAP REST APIの新機能"を含む）については、ONTAP自動化ドキュメントを参照してください。 "IPsecエンドポイント"の詳細については、ONTAP自動化ドキュメントも参照してください。

関連情報

- "セキュリティ IPsec"

ONTAPネットワークのIPセキュリティを構成する

ONTAPクラスタでIPSecの転送中暗号化を設定してアクティブ化するためには、いくつかのタスクを実行する必要があります。

IPsec を設定する前に、必ず"IPセキュリティを使用する準備"を確認してください。たとえば、ONTAP 9.16.1以降で使用可能なIPsecハードウェア オフロード機能を使用するかどうかを決定する必要がある場合があります。

クラスタでのIPsecの有効化

IPsecをクラスタで有効にすることで、転送中もデータの安全性と暗号化を維持できます。

手順

1. IPsecがすでに有効になっているかどうかを確認します。

   ```
   security ipsec config show
   ```

   結果に `IPsec Enabled: false`が含まれる場合は、次の手順に進みます。

2. IPsecを有効にします。

   ```
   security ipsec config modify -is-enabled true
   ```

   ブール型パラメータ `is-offload-enabled`を使用して、IPsec ハードウェア オフロード機能を有効にできます。

3. 検出コマンドをもう一度実行します。

   ```
   security ipsec config show
   ```

   結果には `IPsec Enabled: true`が含まれるようになりました。

証明書認証用の**IPsec**ポリシーの作成準備

この手順は、認証に事前共有キー（PSK）のみを使用しており、証明書認証を使用しない場合は省略できます。

認証に証明書を使用するIPsecポリシーを作成する前に、次の前提条件を満たしていることを確認する必要があります。

- ONTAPとクライアントの両方がエンド エンティティ（ONTAPまたはクライアント）の証明書を検証できるように、両方に相手側のCA証明書がインストールされている。
- ポリシーの対象になるONTAP LIFの証明書がインストールされている。

> ⓘ 証明書はONTAP LIF間で共有できます。証明書とLIFが1対1で対応している必要はありません。

手順

1. すでにインストールされている場合（ONTAPの自己署名ルートCAの場合）を除き、相互認証で使用するすべてのCA証明書（ONTAP側とクライアント側の両方のCAを含む）をONTAP証明書管理にインストールします。

   サンプル コマンド
   ```
   cluster::> security certificate install -vserver svm_name -type server-ca
   -cert-name my_ca_cert
   ```

2. 認証中にインストールされている CA が IPsec CA 検索パス内にあることを確認するには、 `security ipsec ca-certificate add`コマンドを使用して ONTAP 証明書管理 CA を IPsec モジュールに追加します。

   サンプル コマンド
   ```
   cluster::> security ipsec ca-certificate add -vserver svm_name -ca-certs
   my_ca_cert
   ```

3. ONTAP LIFで使用する証明書を作成してインストールします。この証明書の発行元CAがすでにONTAPにインストールされ、IPsecに追加されている必要があります。

   サンプル コマンド
   ```
   cluster::> security certificate install -vserver svm_name -type server -cert
   -name my_nfs_server_cert
   ```

ONTAPの証明書の詳細については、ONTAP 9のドキュメントのsecurity certificateコマンドを参照してください。

セキュリティ ポリシー データベース（**SPD**）の定義

IPsecでトラフィックをネットワーク上で転送するためにはSPDエントリが必要です。これは、認証にPSKと証明書のどちらを使用する場合にも当てはまります。

手順

1. `security ipsec policy create`コマンドを使用して次の操作を実行します：
   a. IPsec転送に参加するONTAPのIPアドレスまたはIPアドレスのサブネットを選択します。
   b. ONTAPのIPアドレスに接続するクライアントのIPアドレスを選択します。

クライアントでInternet Key Exchangeバージョン2（IKEv2）と事前共有キー（PSK）がサポートされている必要があります。

c. 必要に応じて、トラフィックを保護するための上位層プロトコル（UDP、TCP、ICMPなど）、ローカルポート番号、リモートポート番号などの詳細なトラフィックパラメータを選択します。対応するパラメータは、 `protocols`、 `local-ports`、 `remote-ports`です。

この手順は、ONTAPのIPアドレスとクライアントのIPアドレスの間のすべてのトラフィックを保護する場合は省略します。デフォルトでは、すべてのトラフィックが保護されます。

d. 希望する認証方法の `auth-method`パラメータとして、PSK または公開鍵インフラストラクチャ（PKI）を入力します。

i. PSK を入力する場合は、パラメータを含めて、<enter> を押して事前共有キーを入力して検証します。

ホストとクライアントの両方がstrongSwanを使用し、ホストまたはクライアントに対してワイルドカード ポリシーが選択されていない場合、 `local-identity`および`remote-identity`パラメータはオプションです。

ii. PKIを入力する場合は、 `cert-name`、 `local-identity`、 `remote-identity`パラメータも入力する必要があります。リモート側の証明書IDが不明な場合、または複数のクライアントIDが想定される場合は、特別なID `ANYTHING`を入力してください。

e. ONTAP 9.17.1以降では、 `ppk-identity`パラメータを使用して、オプションでポスト量子事前共有鍵（PPK）IDを入力できます。PPKは、将来起こりうる量子コンピュータ攻撃に対するセキュリティをさらに強化します。PPK IDを入力すると、PPKシークレットの入力を求められます。PPKはPSK認証でのみサポートされます。

`security ipsec policy create`
の詳細については、`link:https://docs.netapp.com/us-en/ontap-cli/security-ipsec-policy-create.html["ONTAPコマンド リファレンス"^]`をご覧ください。

```
security ipsec policy create -vserver vs1 -name test34 -local-ip-subnets
192.168.134.34/32 -remote-ip-subnets 192.168.134.44/32
Enter the preshared key for IPsec Policy _test34_ on Vserver _vs1_:
```

```
security ipsec policy create -vserver vs1 -name test34 -local-ip-subnets
192.168.134.34/32 -remote-ip-subnets 192.168.134.44/32 -local-ports 2049
-protocols tcp -auth-method PKI -cert-name my_nfs_server_cert -local
-identity CN=netapp.ipsec.lif1.vs0 -remote-identity ANYTHING
```

ONTAPとクライアントの両方で一致するIPsecポリシーが設定され、両方に認証クレデンシャル（PSKまたは証明書）がインストールされるまで、クライアントとサーバの間でIPトラフィックを転送することはできません。

IPsec IDの使用

事前共有キー認証方式では、ホストとクライアントの両方でstrongSwanを使用しており、ホストまたはクライアントに対してワイルドカード ポリシーが選択されていない場合、ローカルIDとリモートIDは任意です。

PKI/証明書認証方式では、ローカルIDとリモートIDの両方が必須です。これらのIDは、それぞれの証明書内で認証されるIDを指定し、検証プロセスで使用されます。リモートIDが不明な場合、または複数の異なるIDが使用される可能性がある場合は、特別なID `ANYTHING`を使用してください。

タスク概要

ONTAPでは、SPDエントリを変更するかSPDポリシーの作成時にIDを指定します。SPDには、IPアドレスまたは文字列形式のID名を使用できます。

手順

1. 次のコマンドを使用して、既存のSPD ID設定を変更します。

```
security ipsec policy modify
```

コマンド例

```
security ipsec policy modify -vserver vs1 -name test34 -local-identity
192.168.134.34 -remote-identity client.fooboo.com
```

IPsecの複数クライアント設定

IPsecを利用するクライアントの数が少ない場合は、クライアントごとにSPDエントリを1つ使用するだけで十分です。ただし、数百、数千のクライアントがIPsecを利用する必要がある場合は、IPsecの複数クライアント設定を使用することを推奨します。

タスク概要

ONTAPでは、IPsecを有効にした状態で、単一のSVM IPアドレスに複数のクライアントを多数のネットワーク経由で接続できます。そのためには、次のいずれかの方法を使用します。

- サブネット構成

  特定のサブネット（例：192.168.134.0/24）上のすべてのクライアントが単一のSPDポリシーエントリを使用して単一のSVM IPアドレスに接続できるようにするには、 `remote-ip-subnets`をサブネット形式で指定する必要があります。さらに、 `remote-identity`フィールドに正しいクライアント側IDを指定する必要があります。

  > サブネット設定で単一のポリシー エントリを使用する場合、そのサブネット内のIPsecクライアントはIPsec IDと事前共有キー（PSK）を共有します。ただし、これは証明書認証には当てはまりません。証明書を使用する場合は、各クライアントはそれぞれ固有の証明書か共有の証明書のいずれかを認証に使用できます。ONTAPのIPsecは、証明書の有効性をローカルの信頼ストアにインストールされているCAに基づいてチェックします。証明書失効リスト（CRL）のチェックもサポートされています。

- すべてのクライアント構成を許可する

  送信元 IP アドレスに関係なく、すべてのクライアントが SVM IPsec 対応 IP アドレスに接続できるようにするには、 `remote-ip-subnets`フィールドを指定するときに `0.0.0.0/0`ワイルドカードを使用します。

さらに、正しいクライアント側IDを `remote-identity`フィールドに指定する必要があります。証明書認証の場合は、 `ANYTHING`と入力できます。

また、 `0.0.0.0/0`ワイルドカードを使用する場合は、使用するローカルまたはリモートのポート番号を具体的に設定する必要があります。例： `NFS port 2049`

手順

a. 次のいずれかのコマンドを使用して、複数クライアント向けのIPsecを設定します。

i. 複数の IPsec クライアントをサポートするために サブネット構成 を使用している場合：

```
security ipsec policy create -vserver vserver_name -name policy_name
-local-ip-subnets IPsec_IP_address/32 -remote-ip-subnets
IP_address/subnet -local-identity local_id -remote-identity remote_id
```

コマンド例

```
security ipsec policy create -vserver vs1 -name subnet134 -local-ip-subnets
192.168.134.34/32 -remote-ip-subnets 192.168.134.0/24 -local-identity
ontap_side_identity -remote-identity client_side_identity
```

i. 複数の IPsec クライアントをサポートするために すべてのクライアントを許可する構成 を使用している場合：

```
security ipsec policy create -vserver vserver_name -name policy_name
-local-ip-subnets IPsec_IP_address/32 -remote-ip-subnets 0.0.0.0/0 -local
-ports port_number -local-identity local_id -remote-identity remote_id
```

コマンド例

```
security ipsec policy create -vserver vs1 -name test35 -local-ip-subnets
IPsec_IP_address/32 -remote-ip-subnets 0.0.0.0/0 -local-ports 2049 -local
-identity ontap_side_identity -remote-identity client_side_identity
```

IPSecの統計の表示

ネゴシエーションを通じて、ONTAP SVMのIPアドレスとクライアントのIPアドレスの間に、IKEセキュリティ アソシエーション（SA）と呼ばれるセキュリティ チャネルが確立されます。実際のデータの暗号化と復号化を実行するために、両方のエンドポイントにIPsec SAがインストールされます。統計コマンドを使用して、IPsec SAとIKE SAの両方のステータスを確認できます。

IPsec ハードウェア オフロード機能を使用している場合は、コマンド `security ipsec config show-ipsecsa`でいくつかの新しいカウンターが表示されます。

コマンド例

IKE SAのコマンドの例：

```
security ipsec show-ikesa -node hosting_node_name_for_svm_ip
```

IPsec SAのコマンドと出力の例：

```
security ipsec show-ipsecsa -node hosting_node_name_for_svm_ip
```

```
cluster1::> security ipsec show-ikesa -node cluster1-node1
            Policy Local           Remote
Vserver     Name   Address         Address         Initator-SPI     State
----------- ------ --------------- --------------- ----------------
-----------
vs1         test34
                   192.168.134.34  192.168.134.44  c764f9ee020cec69
ESTABLISHED
```

IPsec SAのコマンドと出力の例：

```
security ipsec show-ipsecsa -node hosting_node_name_for_svm_ip

cluster1::> security ipsec show-ipsecsa -node cluster1-node1
            Policy  Local           Remote          Inbound  Outbound
Vserver     Name    Address         Address         SPI      SPI
State
----------- ------- --------------- --------------- -------- --------
---------
vs1         test34
                    192.168.134.34  192.168.134.44  c4c5b3d6 c2515559
INSTALLED
```

関連情報

- "security certificate install"
- "セキュリティ IPsec"

ONTAPバックエンド クラスタ ネットワーク暗号化を設定する

ONTAP 9.18.1以降では、バックエンドクラスタネットワーク上の転送データにトランスポート層セキュリティ（TLS）暗号化を設定できます。この暗号化により、バックエンドクラスタネットワーク上のONTAPノード間で転送されるONTAPに保存されている顧客データが保護されます。

タスク概要

- バックエンド クラスタ ネットワークの暗号化は、デフォルトで無効になっています。
- バックエンド クラスタ ネットワークの暗号化を有効にすると、ONTAPに保存されているすべての顧客データは、バックエンド クラスタ ネットワーク上のONTAPノード間で送信される際に暗号化されます。制御パス データなど、一部のクラスタ ネットワーク トラフィックは暗号化されません。
- デフォルトでは、バックエンド クラスタのネットワーク暗号化では、クラスタ内の各ノードに対して自動生成された証明書が使用されます。クラスター ネットワーク暗号化証明書を管理する各ノードでカスタムインストールされた証明書を使用することもできます。

開始する前に

- 次のタスクを実行するには、 `admin`権限レベルの ONTAP 管理者である必要があります。
- バックエンド クラスタ ネットワークの暗号化を有効にするには、クラスタ内のすべてのノードでONTAP 9.18.1以降が実行されている必要があります。

クラスター ネットワーク通信の暗号化を有効または無効にする

手順

1. 現在のクラスター ネットワーク暗号化ステータスを表示します：

```
security cluster-network show
```

このコマンドは、クラスター ネットワーク暗号化の現在のステータスを表示します：

```
Cluster-1::*> security cluster-network show

Enabled: true

Mode: tls

Status: READY
```

2. TLS バックエンド クラスタ ネットワーク暗号化を有効または無効にします：

```
security cluster-network modify -enabled <true|false>
```

このコマンドは、バックエンド クラスタ ネットワーク上の顧客転送中データの暗号化通信を有効または無効にします。

クラスター ネットワーク暗号化証明書を管理する

1. 現在のクラスター ネットワーク暗号化証明書情報を表示します：

```
security cluster-network certificate show
```

このコマンドは、現在のクラスター ネットワーク暗号化証明書情報を表示します：

```
security cluster-network certificate show
Node                  Certificate Name                       CA
--------------------- -------------------------------------
--------------
node1                 -                                      Cluster-
1_Root_CA
node2                 -                                      Cluster-
1_Root_CA
node3                 google_issued_cert1                    Google_CA1
node4                 google_issued_cert2                    Google_CA1
```

クラスター内の各ノードの証明書と認証局（CA）の名前が表示されます。

2. ノードのクラスター ネットワーク暗号化証明書を変更します：

```
security cluster-network certificate modify -node <node_name> -name
<certificate_name>
```

このコマンドは、特定のノードのクラスタ ネットワーク暗号化証明書を変更します。このコマンドを実行する前に、証明書がインストールされ、インストール済みのCAによって署名されている必要があります。証明書管理の詳細については、"System ManagerでONTAP証明書を管理する"を参照してください。`-name`が指定されていない場合は、自動生成されたデフォルトの証明書が使用されます。

ONTAPネットワーク内のLIFのファイアウォールポリシーを設定する

ファイアウォールの設定は、クラスタのセキュリティを強化し、ストレージ システムへの不正アクセスを防止するのに役立ちます。デフォルトでは、オンボード ファイアウォールは、データLIF、管理LIF、クラスタ間LIFの特定のIPサービスに対するリモート アクセスを許可するように設定されています。

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 ポリシーに置き換えられました。以前は、オンボード ファイアウォールはファイアウォール ポリシーを使用して管理していました。今後はLIFサービス ポリシーを使用します。
- ファイアウォール ポリシーはすべて空であり、基盤となるファイアウォールでいずれのポートも開きません。代わりに、LIFのサービス ポリシーを使用してすべてのポートを開く必要があります。
- 9.10.1以降にアップグレードしたあとに、ファイアウォール ポリシーからLIFサービス ポリシーに移行するための操作は必要ありません。以前のリリースのONTAPで使用されていたファイアウォール ポリシーと整合性のあるLIFサービス ポリシーが自動的に構築されます。カスタム ファイアウォール ポリシーを作成および管理するスクリプトやその他のツールを使用している場合は、代わりにカスタム サービス ポリシーを作成するようにスクリプトのアップグレードが必要になることがあります。

詳細については、"LIFとサービス ポリシー（ONTAP 9.6以降）"を参照してください。

ファイアウォール ポリシーは、SSH、HTTP、HTTPS、Telnet、NTP、NDMP、NDMPS、RSH、DNS、SNMPなどの管理サービス プロトコルへのアクセスを制御するのに使用できます。NFSやSMBなどのデータ プロトコル用にファイアウォール ポリシーを設定することはできません。

ファイアウォール サービスとポリシーの管理には、次のような操作があります。

- ファイアウォール サービスを有効または無効にする
- 現在のファイアウォール サービスの設定を表示する
- ポリシー名とネットワーク サービスを指定して新しいファイアウォール ポリシーを作成する
- ファイアウォール ポリシーを論理インターフェイスに適用する
- 既存のファイアウォール ポリシーとまったく同一の新しいポリシーを作成する

  この機能は、同じSVM内でよく似たポリシーを作成するときや、別のSVMにポリシーをコピーするときに使用できます。

- ファイアウォール ポリシーについての情報を表示する
- ファイアウォール ポリシーで使用するIPアドレスおよびネットマスクを変更する
- LIFで使用していないファイアウォール ポリシーを削除する

ファイアウォール ポリシーと**LIF**

LIFのファイアウォール ポリシーは、各LIFを介したクラスタへのアクセスを制限するために使用します。デフォルトのファイアウォール ポリシーが、各タイプのLIFを介したシステムへのアクセスにどのように影響し、LIFのセキュリティを調節するためにファイアウォール ポリシーをどのようにカスタマイズできるかを理解する必要があります。

`network interface create`または `network interface modify` コマンドを使用してLIFを設定する場合、 `-firewall-policy`パラメータに指定された値によって、LIFへのアクセスが許可されるサービスプロトコルとIPアドレスが決まります。 `network interface` の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/search.html?q=network+interface["ONTAPコマンド リファレンス "^]を参照してください。

ほとんどの場合、デフォルトのファイアウォール ポリシーの値をそのまま使用できますが、特定のIPアドレスや管理サービス プロトコルへのアクセスを制限しなければならない場合もあります。設定可能な管理サービス プロトコルは、SSH、HTTP、HTTPS、Telnet、NTP、NDMP、NDMPS、RSH、DNS、およびSNMPです。

すべてのクラスタ LIF のファイアウォール ポリシーはデフォルトで `""`に設定されており、変更できません。

次の表に、LIFの作成時にそのロール（ONTAP 9.5以前）またはサービス ポリシー（ONTAP 9.6以降）に基づいてLIFに割り当てられるデフォルトのファイアウォール ポリシーを示します。

ファイアウォール ポリシー	デフォルトのサービス プロトコル	デフォルトのアクセス	割り当て対象のLIF

mgmt	dns、http、https、ndmp、ndmps、ntp、snmp、ssh	任意のアドレス（0.0.0.0/0）	クラスタ管理、SVM管理、ノード管理LIF
mgmt-nfs	dns、http、https、ndmp、ndmps、ntp、portmap、snmp、ssh	任意のアドレス（0.0.0.0/0）	SVM管理アクセスもサポートするデータLIF
intercluster	https、ndmp、ndmps	任意のアドレス（0.0.0.0/0）	すべてのインタークラスタLIF
data	dns、ndmp、ndmps、portmap	任意のアドレス（0.0.0.0/0）	すべてのデータLIF

portmapサービスの設定

portmapサービスは、RPCサービスをRPCサービスがリスンするポートにマップします。

portmapサービスはONTAP 9.3までは常にアクセス可能でしたが、ONTAP 9.4から設定対象となり、ONTAP 9.7からは自動で管理されるようになりました。

- ONTAP 9.3までは、サードパーティのファイアウォールではなく組み込みのONTAPファイアウォールを使用するネットワーク構成では、ポート111でportmapサービス（rpcbind）へのアクセスが常に許可されていました。
- ONTAP 9.4～ONTAP 9.6では、ファイアウォール ポリシーを変更してportmapサービスへのアクセスを許可するかどうかをLIFごとに制御できます。
- ONTAP 9.7以降ではportmapファイアウォール サービスは廃止され、代わりに、NFSサービスをサポートするすべてのLIFに対してportmapポートが自動的に開かれます。

Portmap サービスは、**ONTAP 9.4** から **ONTAP 9.6** のファイアウォールで設定できます。

ここからは、ONTAP 9.4～ONTAP 9.6リリースでportmapファイアウォール サービスを設定する方法について説明します。

構成に応じて、特定のタイプのLIF（管理LIFとクラスタ間LIFなど）にサービスへのアクセスを禁止することができます。状況によっては、データLIFからのアクセスも禁止できます。

想定される動作

ONTAP 9.4～ONTAP 9.6の動作は、アップグレード時にシームレスに移行できるように設計されています。portmapサービスにすでに特定のタイプのLIFからアクセスしている場合、それらのタイプのLIFからは引き続きサービスにアクセスできます。ONTAP 9.3以前と同様に、ファイアウォール内でアクセスを許可するサービスをLIFのタイプ別のファイアウォール ポリシーで指定できます。

この動作を有効にするには、クラスタ内のすべてのノードでONTAP 9.4～ONTAP 9.6が実行されている必要があります。影響するのはインバウンド トラフィックのみです。

新しいルールは次のとおりです。

- リリース9.4～9.6にアップグレードすると、既存のすべてのファイアウォール ポリシー（デフォルトまた

はカスタム）にportmapサービスが追加されます。

- 新しいクラスタやIPspaceを作成した場合、portmapサービスはデフォルトのデータ ポリシーにのみ追加され、デフォルトの管理ポリシーまたはクラスタ間ポリシーには追加されません。
- 必要に応じて、デフォルトまたはカスタムのポリシーにportmapサービスを追加したり削除したりできます。

portmapサービスを追加または削除する方法

SVMまたはクラスタのファイアウォール ポリシーにportmapサービスを追加する（ファイアウォール内でのアクセスを許可する）には、次のように入力します。

```
system services firewall policy create -vserver SVM -policy
mgmt|intercluster|data|custom -service portmap
```

SVMまたはクラスタのファイアウォール ポリシーからportmapサービスを削除する（ファイアウォール内でのアクセスを禁止する）には、次のように入力します。

```
system services firewall policy delete -vserver SVM -policy
mgmt|intercluster|data|custom -service portmap
```

network interface modifyコマンドを使用して、既存のLIFにファイアウォールポリシーを適用できます。この手順で説明するコマンドの詳細については、"ONTAPコマンド リファレンス"を参照してください。

ファイアウォール ポリシーの作成と**LIF**への割り当て

LIFを作成するときに、デフォルトのファイアウォール ポリシーが割り当てられます。多くの場合、ファイアウォールのデフォルト設定をそのまま使用でき、変更する必要はありません。ただし、LIFにアクセスできるネットワーク サービスやIPアドレスを変更したい場合は、カスタム ファイアウォール ポリシーを作成してLIFに割り当てます。

タスク概要

- `policy`名前 `data intercluster cluster`、または`mgmt`でファイアウォールポリシーを作成することはできません。

  これらの値は、システム定義のファイアウォール ポリシー用に予約されています。

- クラスタLIFのファイアウォール ポリシーを設定したり変更したりすることはできません。

  クラスタLIFのファイアウォール ポリシーは、どのサービス タイプでも0.0.0.0/0に設定されます。

- ポリシーからサービスを削除する必要がある場合は、既存のファイアウォール ポリシーを削除してから、新しいポリシーを作成する必要があります。
- クラスタでIPv6が有効になっている場合は、IPv6アドレスを指定してファイアウォール ポリシーを作成できます。

  IPv6 を有効にすると、 `data`、 `intercluster`、および`mgmt`ファイアウォール ポリシーの受け入れ可能なアドレスのリストに IPv6 ワイルドカードである ::/0 が含まれるようになります。

- System Managerを使用してクラスタ全体のデータ保護機能を設定するときは、必ず、許可されるアドレスのリストにクラスタ間LIFのIPアドレスを含め、クラスタ間LIFと会社所有のファイアウォールの両方でHTTPSサービスを許可してください。

デフォルトでは、 `intercluster`ファイアウォールポリシーはすべてのIPアドレス（0.0.0.0/0、またはIPv6の場合は::/0）からのアクセスを許可し、HTTPS、NDMP、およびNDMPSサービスを有効にします。このデフォルトポリシーを変更する場合、またはクラスタ間LIF用に独自のファイアウォールポリシーを作成する場合は、各クラスタ間LIFのIPアドレスを許可リストに追加し、HTTPSサービスを有効にする必要があります。

- ONTAP 9.6以降では、HTTPSおよびSSHのファイアウォール サービスはサポートされていません。

  ONTAP 9.6では、 `management-https`および `management-ssh`LIFサービスは、HTTPSおよびSSH管理アクセスに使用できます。

手順

1. 特定のSVMのLIFで使用可能なファイアウォール ポリシーを作成します。

   ```
   system services firewall policy create -vserver vserver_name -policy
   policy_name -service network_service -allow-list ip_address/mask
   ```

   ファイアウォール ポリシーに追加するネットワーク サービスごとに上記のコマンドを繰り返して、各サービスで許可されるIPアドレスを指定できます。

2. `system services firewall policy show`コマンドを使用して、ポリシーが正しく追加されたことを確認します。
3. ファイアウォール ポリシーをLIFに適用します。

   ```
   network interface modify -vserver vserver_name -lif lif_name -firewall-policy
   policy_name
   ```

4. `network interface show -fields firewall-policy`コマンドを使用して、ポリシーがLIFに正しく追加されたことを確認します。

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

ファイアウォール ポリシーを作成して**LIF**に割り当てる例

次のコマンドは、10.10サブネットのIPアドレスからのHTTPおよびHTTPSプロトコルによるアクセスを許可するdata_httpというファイアウォール ポリシーを作成し、SVM vs1のdata1というLIFに適用してから、クラスタのすべてのファイアウォール ポリシーを表示します。

```
system services firewall policy create -vserver vs1 -policy data_http
-service http - allow-list 10.10.0.0/16
```

```
system services firewall policy show

Vserver Policy       Service    Allowed
------- ------------ ---------- -------------------
cluster-1
        data
                     dns        0.0.0.0/0
                     ndmp       0.0.0.0/0
                     ndmps      0.0.0.0/0
cluster-1
        intercluster
                     https      0.0.0.0/0
                     ndmp       0.0.0.0/0
                     ndmps      0.0.0.0/0
cluster-1
        mgmt
                     dns        0.0.0.0/0
                     http       0.0.0.0/0
                     https      0.0.0.0/0
                     ndmp       0.0.0.0/0
                     ndmps      0.0.0.0/0
                     ntp        0.0.0.0/0
                     snmp       0.0.0.0/0
                     ssh        0.0.0.0/0
vs1
        data_http
                     http       10.10.0.0/16
                     https      10.10.0.0/16

network interface modify -vserver vs1 -lif data1 -firewall-policy
data_http

network interface show -fields firewall-policy

vserver  lif                  firewall-policy
-------  -------------------- ---------------
Cluster  node1_clus_1
Cluster  node1_clus_2
Cluster  node2_clus_1
Cluster  node2_clus_2
cluster-1 cluster_mgmt         mgmt
cluster-1 node1_mgmt1          mgmt
cluster-1 node2_mgmt1          mgmt
vs1      data1                data_http
vs3      data2                data
```

ファイアウォール サービスとポリシーを管理するための **ONTAP** コマンド

`system services firewall`コマンドを使用してファイアウォール サービスを管理し、`system services firewall policy`コマンドを使用してファイアウォール ポリシーを管理し、 `network interface modify`コマンドを使用してLIFのファイアウォール設定を管理できます。

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 ポリシーに置き換えられました。以前は、オンボード ファイアウォールはファイアウォール ポリシーを使用して管理していました。今後はLIFサービス ポリシーを使用します。
- ファイアウォール ポリシーはすべて空であり、基盤となるファイアウォールでいずれのポートも開きません。代わりに、LIFのサービス ポリシーを使用してすべてのポートを開く必要があります。
- 9.10.1以降にアップグレードしたあとに、ファイアウォール ポリシーからLIFサービス ポリシーに移行するための操作は必要ありません。以前のリリースのONTAPで使用されていたファイアウォール ポリシーと整合性のあるLIFサービス ポリシーが自動的に構築されます。カスタム ファイアウォール ポリシーを作成および管理するスクリプトやその他のツールを使用している場合は、代わりにカスタム サービス ポリシーを作成するようにスクリプトのアップグレードが必要になることがあります。

詳細については、"LIFとサービス ポリシー（ONTAP 9.6以降）"を参照してください。

状況	使用するコマンド
ファイアウォール サービスを有効または無効にする	`system services firewall modify`
ファイアウォール サービスの現在の設定を表示する	`system services firewall show`
ファイアウォール ポリシーを作成する、または既存のファイアウォール ポリシーにサービスを追加する	`system services firewall policy create`
LIFにファイアウォール ポリシーを適用する	`network interface modify -lif lifname -firewall-policy`
ファイアウォール ポリシーに関連付けられたIPアドレスとネットマスクを変更する	`system services firewall policy modify`
ファイアウォール ポリシーに関する情報を表示する	`system services firewall policy show`
既存のファイアウォール ポリシーとまったく同じ新しいポリシーを作成する	`system services firewall policy clone`
LIFで使用していないファイアウォール ポリシーを削除する	`system services firewall policy delete`

関連情報

- "システム サービス ファイアウォール"
- "network interface modify"

QoSマーキング（クラスタ管理者のみ）

ONTAPネットワークのQoS（Quality of Service）について学ぶ

ネットワークQoS（Quality of Service）マーキングは、ネットワークの状態に基づいて異なるトラフィックタイプに優先順位を付け、ネットワーク リソースを効果的に使用するのに役立ちます。IPspaceごとに、サポートされているトラフィックタイプに対して、送信IPパケットのDSCP（Differentiated Services Code Point）値を設定できます。

UC準拠のためのDSCPマーキング

デフォルトまたはユーザが指定したDSCPコードを使用して、特定のプロトコルの送信IPパケット トラフィックでDifferentiated Services Code Point（DSCP）マーキングを有効にすることができます。DSCPマーキングは、ネットワーク トラフィックを分類して管理するためのメカニズムであり、Unified Capabilities（UC）準拠のコンポーネントです。

DSCPマーキング（_QoSマーキング_または_Quality of Serviceマーキング_とも呼ばれます）は、IPspace、プロトコル、およびDSCP値を指定することによって有効化されます。DSCPマーキングを適用できるプロトコルは、NFS、SMB、iSCSI、SnapMirror、NDMP、FTP、HTTP/HTTPS、SSH、Telnet、およびSNMPです。

特定のプロトコルに対してDSCPマーキングを有効にする際にDSCP値を指定しない場合は、デフォルトが使用されます。

- データ プロトコル / トラフィックのデフォルト値は0x0A（10）です。
- 制御プロトコル / トラフィックのデフォルト値は0x30（48）です。

ONTAPネットワークQoSマーキング値を変更する

それぞれのIPspaceについて、さまざまなプロトコルのサービス品質（QoS）マーキング値を変更できます。

開始する前に

クラスタ内のすべてのノードで同じバージョンのONTAPが実行されている必要があります。

手順

`network qos-marking modify`コマンドを使用してQoSマーキング値を変更します。

- `–ipspace`パラメータは、QoS マーキングエントリを変更する IPspace を指定します。
- `–protocol`パラメータは、QoS マーキングエントリを変更するプロトコルを指定します。
- この `–dscp`パラメータは、Differentiated Services Code Point（DSCP）値を指定します。指定可能な値の範囲は0~63です。

- `-is-enabled`パラメータは、`–ipspace`パラメータによって提供されるIPspace内の指定されたプロトコルのQoSマーキングを有効または無効にするために使用されます。

次のコマンドは、デフォルトIPspaceのNFSプロトコルのQoSマーキングを有効にします。

```
network qos-marking modify -ipspace Default -protocol NFS -is-enabled true
```

次のコマンドは、デフォルトIPspaceのNFSプロトコルのDSCP値を20に設定します。

```
network qos-marking modify -ipspace Default -protocol NFS -dscp 20
```

`network qos-marking modify`
とプロトコルの可能な値の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/network-qos-marking-modify.html["ONTAPコマンド リファレンス
"^]を参照してください。

ONTAPネットワークQoSマーキング値を表示する

それぞれのIPspaceについて、さまざまなプロトコルのQoSマーキング値を表示できます。

手順

`network qos-marking show`コマンドを使用してQoSマーキング値を表示します。

次のコマンドは、デフォルトのIPspace内のすべてのプロトコルのQoSマーキングを表示します。

```
network qos-marking show -ipspace Default
IPspace              Protocol            DSCP  Enabled?
-------------------- ----------------- -----  --------
Default
                     CIFS                  10  false
                     FTP                   48  false
                     HTTP-admin            48  false
                     HTTP-filesrv          10  false
                     NDMP                  10  false
                     NFS                   10  true
                     SNMP                  48  false
                     SSH                   48  false
                     SnapMirror            10  false
                     Telnet                48  false
                     iSCSI                 10  false
11 entries were displayed.
```

`network qos-marking show`の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/network-qos-marking-show.html["ONTAPコマンド リファレンス"^]をご覧ください。

SNMPの管理（クラスタ管理者のみ）

ONTAPネットワーク上のSNMPについて学ぶ

クラスタのSVMを監視するようにSNMPを設定すると、問題を発生前に回避したり、発生時に対応したりすることができます。SNMPを管理するには、SNMPユーザを設定し、すべてのSNMPイベントのSNMPトラップの送信先（管理ワークステーション）を設定する必要があります。データLIFでは、SNMPはデフォルトで無効になっています。

データSVMに、読み取り専用SNMPユーザを作成して管理できます。データLIFは、SVMでSNMP要求を受信するように設定する必要があります。

SNMPネットワーク管理ワークステーションまたはマネージャは、SVM SNMPエージェントに情報を照会できます。SNMPエージェントは情報を収集し、SNMPマネージャに転送します。SNMPエージェントはまた、特定のイベントの発生時にトラップ通知を生成します。SVM上のSNMPエージェントの権限は読み取り専用権限であるため、設定操作や、トラップに応答して対処するために使用することはできません。ONTAPはSNMPバージョンv1、v2c、およびv3と互換性のあるSNMPエージェントを備えています。SNMPv3は、パスフレーズと暗号化を使用して高度なセキュリティを提供します。

ONTAPシステムでのSNMPサポートの詳細については、 "TR-4220：Data ONTAPにおけるSNMPサポート"を参照してください。

MIBの概要

管理情報ベース（MIB）は、SNMPのオブジェクトとトラップが記述されたテキスト ファイルです。

MIBは、ストレージ システムの管理データの構造を表し、オブジェクト識別子（OID）を含む階層状のネームスペースを使用します。各OIDは、SNMPを使用して読み取り可能な変数を識別します。

MIBは構成ファイルではなく、ONTAPはこれらのファイルを読み取らないため、SNMP機能はMIBによる影響を受けません。ONTAPには次のMIBファイルが用意されています。

- NetAppカスタムMIB(`netapp.mib`)

ONTAPは、IPv6（RFC 2465）、TCP（RFC 4022）、UDP（RFC 4113）、およびICMP（RFC 2466）のMIBをサポートします。これらのMIBではIPv4とIPv6の両方のデータが表示されます。

ONTAPでは、 `traps.dat`ファイル内のオブジェクト識別子（OID）とオブジェクトの短縮名の間の短い相互参照も提供されます。

> 最新バージョンのONTAP MIBおよび`traps.dat`ファイルはNetApp Support Siteから入手できます。ただし、サポートサイトにあるこれらのファイルのバージョンは、お使いのONTAPバージョンのSNMP機能と必ずしも一致しているわけではありません。これらのファイルは、最新のONTAPバージョンのSNMP機能を評価するのに役立つように提供されています。

SNMPトラップ

SNMPトラップは、SNMPエージェントからSNMPマネージャに非同期通知として送信されたシステム監視情報をキャプチャします。

SNMPトラップには、標準、ビルトイン、およびユーザ定義という3つの種類があります。ONTAPではユーザ定義トラップはサポートされていません。

トラップを使用して、MIBに定義された運用上のしきい値または障害を定期的にチェックすることができます。しきい値に到達するか、障害が検出されると、SNMPエージェントは、イベントを警告するメッセージ（トラップ）をトラップホストに送信します。

> ONTAPはSNMPv1およびSNMPv3トラップをサポートしています。ONTAPはSNMPv2cトラップとINFORMをサポートしていません。

標準SNMPトラップ

これらのトラップはRFC 1215で定義されています。ONTAPでサポートされているSNMPトラップは、coldStart、warmStart、linkDown、linkUp、およびauthenticationFailureの5つです。

> authenticationFailureトラップはデフォルトで無効になっています。トラップを有効にするには、 `system snmp authtrap`コマンドを使用する必要があります。"ONTAPコマンド リファレンス"の `system snmp authtrap`の詳細を確認してください。

ビルトインSNMPトラップ

ビルトイン トラップはONTAPに事前定義されたトラップで、イベントの発生時にトラップホスト リストのネットワーク管理ステーションに自動的に送信されます。これらのトラップ（diskFailedShutdown

、cpuTooBusy、volumeNearlyFullなど）はカスタムMIBで定義されています。

各ビルトイン トラップは、一意のトラップ コードで識別されます。

ONTAPネットワーク用のSNMPコミュニティを作成する

SNMPv1およびSNMPv2cを使用する場合に、管理ステーションとStorage Virtual Machine（SVM）間の認証メカニズムとして機能するSNMPコミュニティを作成できます。

データ SVM に SNMP コミュニティを作成すると、 `snmpwalk`や `snmpget`などのコマンドをデータ LIF で実行できます。

タスク概要

- ONTAPの新規インストールでは、SNMPv1とSNMPv2cはデフォルトで無効になっています。

  SNMPコミュニティを作成した後で、SNMPv1とSNMPv2cは有効になります。

- ONTAPでサポートされるのは、読み取り専用のコミュニティです。
- デフォルトでは、データ LIF に割り当てられている「データ」ファイアウォール ポリシーでは、SNMP サービスが `deny`に設定されています。

  データ SVM の SNMP ユーザを作成するときは、SNMP サービスが `allow`に設定された新しいファイアウォール ポリシーを作成する必要があります。

  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。

- 管理SVMとデータSVMの両方に、SNMPv1ユーザとSNMPv2cユーザのSNMPコミュニティを作成できます。
- SVM は SNMP 標準の一部ではないため、データ LIF に対するクエリにはNetAppルート OID（1.3.6.1.4.1.789）を含める必要があります（例： `snmpwalk -v 2c -c snmpNFS 10.238.19.14 1.3.6.1.4.1.789`）。

手順

1. `system snmp community add`コマンドを使用してSNMPコミュニティを作成します。次のコマンドは、管理SVM cluster-1にSNMPコミュニティを作成する方法を示しています：

   ```
   system snmp community add -type ro -community-name comty1 -vserver
   cluster-1
   ```

   次のコマンドは、データSVM vs1にSNMPコミュニティを作成する方法を示しています。

   ```
   system snmp community add -type ro -community-name comty2 -vserver vs1
   ```

2. system snmp community showコマンドを使用して、コミュニティが作成されたことを確認します。

   次のコマンドは、SNMPv1およびSNMPv2c用に作成された2つのコミュニティを表示します。

```
system snmp community show
cluster-1
rocomty1
vs1
rocomty2
```

3. `system services firewall policy`show`コマンドを使用して、「data」ファイアウォール ポリシーで SNMP がサービスとして許可されているかどうかを確認します。

   次のコマンドは、デフォルトの「data」ファイアウォール ポリシーではsnmpサービスが許可されていないことを示しています（snmpサービスは「mgmt」ファイアウォール ポリシーだけで許可されています）。

```
system services firewall policy show
Vserver Policy       Service    Allowed
------- ------------ ---------- --------------------
cluster-1
        data
                     dns        0.0.0.0/0
                     ndmp       0.0.0.0/0
                     ndmps      0.0.0.0/0
cluster-1
        intercluster
                     https      0.0.0.0/0
                     ndmp       0.0.0.0/0
                     ndmps      0.0.0.0/0
cluster-1
        mgmt
                     dns        0.0.0.0/0
                     http       0.0.0.0/0
                     https      0.0.0.0/0
                     ndmp       0.0.0.0/0
                     ndmps      0.0.0.0/0
                     ntp        0.0.0.0/0
                     snmp       0.0.0.0/0
                     ssh        0.0.0.0/0
```

4. `snmp`サービスを使用したアクセスを許可する新しいファイアウォール ポリシーを `system services firewall policy create`コマンドを使用して作成します。

   次のコマンドは、「data1」という名前の新しいデータファイアウォールポリシーを作成し、 `snmp`

```
system services firewall policy create -policy data1 -service snmp
-vserver  vs1 -allow-list 0.0.0.0/0

cluster-1::> system services firewall policy show -service snmp
Vserver  Policy       Service    Allowed
-------  ------------ ---------- -------------------
cluster-1
         mgmt
                      snmp       0.0.0.0/0
vs1
         data1
                      snmp       0.0.0.0/0
```

5. `network interface modify`コマンドに-firewall-policyパラメータを指定して、データLIFにファイアウォールポリシーを適用します。

   次のコマンドは、新しく作成した「data1」ファイアウォール ポリシーを「datalif1」というLIFに適用します。

```
network interface modify -vserver vs1 -lif datalif1 -firewall-policy
data1
```

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

ONTAPクラスタでSNMPv3ユーザーを構成する

SNMPv3は、SNMPv1やSNMPv2cに比べて安全なプロトコルです。SNMPv3を使用するには、SNMPマネージャからSNMPユーティリティを実行するためのSNMPv3ユーザを設定する必要があります。

手順

`security login create`コマンドを使用して、SNMPv3 ユーザーを作成します。

次の情報を指定するように求められます。

- エンジン ID：デフォルトおよび推奨値はローカル エンジン ID です
- 認証プロトコル
- 認証パスワード

- プライバシー プロトコル
- プライバシー プロトコルのパスワード

結果

SNMPv3ユーザは、ユーザ名とパスワードを使用してSNMPマネージャからログインし、SNMPユーティリティのコマンドを実行できます。

SNMPv3セキュリティ パラメータ

SNMPv3には認証機能が備わっており、この機能を選択すると、コマンドの呼び出し時に、ユーザ名、認証プロトコル、認証キー、および必要なセキュリティ レベルの入力が必要になります。

次の表に、SNMPv3セキュリティ パラメータを示します。

パラメータ	コマンドライン オプション	概要
engineID	-e EngineID	SNMPエージェントのエンジンID。デフォルト値はローカルエンジンID（推奨）です。
securityName	-u Name	ユーザー名は32文字を超えてはなりません。
authProtocol	-a {none	MD5
SHA	SHA-256}	認証タイプは、none、MD5、SHA、または SHA-256 になります。
authKey	-A パスフレーズ	最低 8 文字のパスフレーズ。
securityLevel	-l {authNoPriv	AuthPriv
noAuthNoPriv}	セキュリティ レベルは、認証、プライバシーなし、認証、プライバシーあり、または認証なし、プライバシーなしのいずれかになります。	privProtocol
-x { none	des	aes128}
プライバシー プロトコルは、none、des、またはaes128です。	privPassword	-X パスワード

さまざまなセキュリティ レベルの例

この例では、異なるセキュリティ レベルで作成された SNMPv3 ユーザーが `snmpwalk`などの SNMP クライアント側コマンドを使用してクラスタ オブジェクトを照会する方法を示します。

パフォーマンスを高めるには、テーブルから単一または少数のオブジェクトを取得するのではなく、テーブル内のすべてのオブジェクトを取得します。

認証プロトコルが SHA の場合は、 `snmpwalk` 5.3.1 以降を使用する必要があります。

セキュリティ レベル：**authPriv**

authPrivセキュリティ レベルのSNMPv3ユーザを作成した場合の出力を次に示します。

```
security login create -user-or-group-name snmpv3user -application snmp
-authentication-method usm
Enter the authoritative entity's EngineID [local EngineID]:
Which authentication protocol do you want to choose (none, md5, sha, sha2-
256) [none]: md5

Enter the authentication protocol password (minimum 8 characters long):
Enter the authentication protocol password again:
Which privacy protocol do you want to choose (none, des, aes128) [none]:
des
Enter privacy protocol password (minimum 8 characters long):
Enter privacy protocol password again:
```

FIPSモード

```
security login create -user-or-group-name snmpv3user -application snmp
-authmethod usm
Enter the authoritative entity's EngineID [local EngineID]:
Which authentication protocol do you want to choose (sha, sha2-256) [sha]

Enter authentication protocol password (minimum 8 characters long):
Enter authentication protocol password again:
Which privacy protocol do you want to choose (aes128) [aes128]:
Enter privacy protocol password (minimum 8 characters long):
Enter privacy protocol password again:
```

snmpwalkテスト

このSNMPv3ユーザがsnmpwalkコマンドを実行した場合の出力を次に示します。

パフォーマンスを高めるには、テーブルから単一または少数のオブジェクトを取得するのではなく、テーブル内のすべてのオブジェクトを取得します。

```
$ snmpwalk -v 3 -u snmpv3user -a SHA -A password1! -x DES -X password1! -l
authPriv 192.0.2.62 .1.3.6.1.4.1.789.1.5.8.1.2
Enterprises.789.1.5.8.1.2.1028 = "vol0"
Enterprises.789.1.5.8.1.2.1032 = "vol0"
Enterprises.789.1.5.8.1.2.1038 = "root_vs0"
Enterprises.789.1.5.8.1.2.1042 = "root_vstrap"
Enterprises.789.1.5.8.1.2.1064 = "vol1"
```

セキュリティ レベル：**authNoPriv**

authNoPrivセキュリティ レベルのSNMPv3ユーザを作成した場合の出力を次に示します。

```
security login create -user-or-group-name snmpv3user -application snmp
-authmethod usm -role read-only
Enter the authoritative entity's EngineID [local EngineID]:
Which authentication protocol do you want to choose (none, md5, sha)
[none]: md5
```

FIPSモード

FIPSでは、プライバシープロトコルに*none*を選択することはできません。そのため、FIPSモードでauthNoPriv SNMPv3ユーザーを設定することはできません。

snmpwalkテスト

このSNMPv3ユーザがsnmpwalkコマンドを実行した場合の出力を次に示します。

パフォーマンスを高めるには、テーブルから単一または少数のオブジェクトを取得するのではなく、テーブル内のすべてのオブジェクトを取得します。

```
$ snmpwalk -v 3 -u snmpv3user1 -a MD5 -A password1!  -l authNoPriv
192.0.2.62 .1.3.6.1.4.1.789.1.5.8.1.2
Enterprises.789.1.5.8.1.2.1028 = "vol0"
Enterprises.789.1.5.8.1.2.1032 = "vol0"
Enterprises.789.1.5.8.1.2.1038 = "root_vs0"
Enterprises.789.1.5.8.1.2.1042 = "root_vstrap"
Enterprises.789.1.5.8.1.2.1064 = "vol1"
```

セキュリティ レベル：**noAuthNoPriv**

noAuthNoPrivセキュリティ レベルのSNMPv3ユーザを作成した場合の出力を次に示します。

```
security login create -user-or-group-name snmpv3user -application snmp
-authmethod usm -role read-only
Enter the authoritative entity's EngineID [local EngineID]:
Which authentication protocol do you want to choose (none, md5, sha)
[none]: none
```

FIPSモード

FIPS では、プライバシー プロトコルに **none** を選択することはできません。

snmpwalkテスト

このSNMPv3ユーザがsnmpwalkコマンドを実行した場合の出力を次に示します。

パフォーマンスを高めるには、テーブルから単一または少数のオブジェクトを取得するのではなく、テーブル内のすべてのオブジェクトを取得します。

```
$ snmpwalk -v 3 -u snmpv3user2 -l noAuthNoPriv 192.0.2.62
.1.3.6.1.4.1.789.1.5.8.1.2
Enterprises.789.1.5.8.1.2.1028 = "vol0"
Enterprises.789.1.5.8.1.2.1032 = "vol0"
Enterprises.789.1.5.8.1.2.1038 = "root_vs0"
Enterprises.789.1.5.8.1.2.1042 = "root_vstrap"
Enterprises.789.1.5.8.1.2.1064 = "vol1"
```

`security login create`の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/security-login-create.html["ONTAPコマンド リファレンス"^]をご覧ください。

ONTAPネットワーク上でSNMP用のトラップホストを設定する

クラスタでSNMPトラップが生成されたときに通知（SNMPトラップPDU）が届くように、トラップホスト（SNMPマネージャ）を設定できます。SNMPトラップホストのホスト名かIPアドレス（IPv4またはIPv6）を指定できます。

開始する前に

- クラスタでSNMPとSNMPトラップが有効になっている必要があります。

  SNMPとSNMPトラップはデフォルトで有効になっています。

- クラスタでトラップホスト名を解決するようにDNSが設定されている必要があります。
- IPv6アドレスを使用してSNMPトラップホストを設定するには、クラスタでIPv6を有効にする必要があります。

- トラップホストを作成するときは、定義済みのユーザーベースのセキュリティ モデル（USM）の認証プロトコルとプライバシー資格情報を指定する必要があります。

手順

SNMPトラップホストを追加します。

```
system snmp traphost add
```

トラップを送信できるのは、1つ以上のSNMP管理ステーションがトラップホストとして指定されている場合だけです。

次のコマンドは、yyy.example.comという名前の新しいSNMPv3トラップホストを、既知のUSMユーザで追加します。

```
system snmp traphost add -peer-address yyy.example.com -usm-username
MyUsmUser
```

次のコマンドは、ホストのIPv6アドレスを使用してトラップホストを追加します。

```
system snmp traphost add -peer-address 2001:0db8:1:1:209:6bff:feae:6d67
```

ONTAPクラスタでのSNMPポーリングの検証

SNMPを設定したら、クラスタをポーリングできることを確認する必要があります。

タスク概要

クラスターをポーリングするには、 `snmpwalk`などのサードパーティ コマンドを使用する必要があります。

手順

1. SNMPコマンドを送信して、別のクラスタからクラスタをポーリングします。

   SNMPv1 を実行しているシステムの場合は、CLI コマンド `snmpwalk -v version -c community_stringip_address_or_host_name system`を使用して MIB（Management Information Base）の内容を検出します。

   この例では、ポーリングするクラスタ管理LIFのIPアドレスは10.11.12.123です。要求したMIB情報が表示されます。

```
C:\Windows\System32>snmpwalk -v 1 -c public 10.11.12.123 system

SNMPv1-MIB::sysDescr.0 = STRING: NetApp Release 8.3.0
            Cluster-Mode: Tue Apr 22 16:24:48 EDT 2014
SNMPv1-MIB::sysObjectID.0 = OID: SNMPv1-SMI::enterprises.789.2.5
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (162644448) 18 days,
19:47:24.48
SNMPv1-MIB::sysContact.0 = STRING:
SNMPv1-MIB::sysName.0 = STRING: systemname.testlabs.com
SNMPv1-MIB::sysLocation.0 = STRING: Floor 2 Row B Cab 2
SNMPv1-MIB::sysServices.0 = INTEGER: 72
```

SNMPv2c を実行しているシステムでは、CLI コマンド `snmpwalk -v version -c community_stringip_address_or_host_name system`を使用して MIB（Management Information Base）の内容を検出します。

この例では、ポーリングするクラスタ管理LIFのIPアドレスは10.11.12.123です。要求したMIB情報が表示されます。

```
C:\Windows\System32>snmpwalk -v 2c -c public 10.11.12.123 system

SNMPv2-MIB::sysDescr.0 = STRING: NetApp Release 8.3.0
            Cluster-Mode: Tue Apr 22 16:24:48 EDT 2014
SNMPv2-MIB::sysObjectID.0 = OID: SNMPv2-SMI::enterprises.789.2.5
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (162635772) 18 days,
19:45:57.72
SNMPv2-MIB::sysContact.0 = STRING:
SNMPv2-MIB::sysName.0 = STRING: systemname.testlabs.com
SNMPv2-MIB::sysLocation.0 = STRING: Floor 2 Row B Cab 2
SNMPv2-MIB::sysServices.0 = INTEGER: 72
```

SNMPv3 を実行しているシステムでは、CLI コマンド `snmpwalk -v 3 -a MD5 or SHA -l authnopriv -u username -A passwordip_address_or_host_name system`を使用して MIB（Management Information Base）の内容を検出します。

この例では、ポーリングするクラスタ管理LIFのIPアドレスは10.11.12.123です。要求したMIB情報が表示されます。

```
C:\Windows\System32>snmpwalk -v 3 -a MD5 -l authnopriv -u snmpv3
       -A password123 10.11.12.123 system

SNMPv3-MIB::sysDescr.0 = STRING: NetApp Release 8.3.0
       Cluster-Mode: Tue Apr 22 16:24:48 EDT 2014
SNMPv3-MIB::sysObjectID.0 = OID: SNMPv3-SMI::enterprises.789.2.5
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (162666569) 18 days,
19:51:05.69
SNMPv3-MIB::sysContact.0 = STRING:
SNMPv3-MIB::sysName.0 = STRING: systemname.testlabs.com
SNMPv3-MIB::sysLocation.0 = STRING: Floor 2 Row B Cab 2
SNMPv3-MIB::sysServices.0 = INTEGER: 72
```

SNMP、トラップ、トラップホストを管理するための ONTAP コマンド

`system snmp`コマンドを使用して、SNMP、トラップ、およびトラップホストを管理できます。
`security`コマンドを使用して、SVMごとのSNMPユーザを管理できます。
`event`コマンドを使用して、SNMPトラップに関連するイベントを管理できます。

SNMPを設定するコマンド

状況	使用するコマンド
クラスタでSNMPを有効にする	`options -option-name snmp.enable -option-value on` 管理（mgmt）ファイアウォール ポリシーでSNMPサービスが許可されている必要があります。SNMPが許可されているかどうかを確認するには、system services firewall policy showコマンドを使用します。
クラスタでSNMPを無効にする	`options -option-name snmp.enable -option-value off`

SNMPv1、**v2c**、**v3**ユーザを管理するコマンド

状況	使用するコマンド
SNMPユーザを設定する	`security login create`
SNMPユーザーを表示する	`security snmpusers` および `security login show -application snmp`

SNMPユーザーを削除する	`security login delete`
SNMPユーザのログイン方法のアクセス制御ロール名を変更する	`security login modify`

連絡先と場所の情報を提供するコマンド

状況	使用するコマンド
クラスタの連絡先の詳細を表示または変更する	`system snmp contact`
クラスタの場所の詳細を表示または変更する	`system snmp location`

SNMPコミュニティを管理するコマンド

状況	使用するコマンド
SVM またはクラスタ内のすべての SVM に読み取り専用（ro）コミュニティを追加します	`system snmp community add`
コミュニティまたはすべてのコミュニティを削除する	`system snmp community delete`
すべてのコミュニティのリストを表示する	`system snmp community show`

SVM は SNMP 標準の一部ではないため、データ LIF に対するクエリには NetApp ルート OID（1.3.6.1.4.1.789）を含める必要があります。例： `snmpwalk -v 2c -c snmpNFS 10.238.19.14 1.3.6.1.4.1.789`。

SNMPオプションの値を表示するコマンド

状況	使用するコマンド
SNMPの全オプションの値（クラスタの連絡先、連絡先の場所、クラスタからのトラップ送信の設定、トラップホストのリスト、コミュニティのリスト、アクセス制御の種類）を表示する	`system snmp show`

SNMPのトラップおよびトラップホストを管理するコマンド

状況	使用するコマンド
クラスタからのSNMPトラップの送信を有効にする	`system snmp init -init 1`
クラスタからのSNMPトラップの送信を無効にする	`system snmp init -init 0`

クラスタの特定のイベントに関するSNMP通知を受信するトラップホストを追加する	`system snmp traphost add`
トラップホストを削除する	`system snmp traphost delete`
トラップホストのリストを表示する	`system snmp traphost show`

SNMPトラップに関連するイベントを管理するコマンド

状況	使用するコマンド
SNMPトラップ（組み込み）が生成されるイベントを表示します	`event route show` `-snmp-support true`パラメータを使用して、SNMP関連のイベントのみを表示します。 `instance -messagename <message>`パラメータを使用して、イベントが発生した理由の詳細な説明と修正アクションを表示します。 個々のSNMPトラップ イベントを特定の送信先トラップホストにルーティングすることはできません。すべてのSNMPトラップ イベントが、すべての送信先トラップホストに送信されます。
SNMPトラップに送信されたイベント通知であるSNMPトラップ履歴レコードのリストを表示します	`event snmphistory show`
SNMPトラップ履歴レコードを削除する	`event snmphistory delete`

関連情報

- "システム SNMP"
- "セキュリティ snmpusers"
- "セキュリティ"
- "event"
- "セキュリティログイン"

SVMのルーティングの管理

ONTAPネットワーク上のSVMルーティングについて学ぶ

SVMのルーティング テーブルは、SVMがデスティネーションとの通信に使用するネットワーク パスを決めるものです。ネットワークの問題を未然に防ぐためには、ルーティング テーブルの仕組みを理解しておくことが重要です。

ルーティング ルールは次のとおりです。

- ONTAPは、最も限定的かつ使用可能なルートでトラフィックをルーティングします。
- より限定的なルートがない場合、最後の手段としてデフォルト ゲートウェイ ルート（0ビットのネットマスク）でトラフィックがルーティングされます。

デスティネーション、ネットマスク、メトリックが同じでルートが複数ある場合、リブート後またはアップグレード後に同じルートが使用される保証はありません。複数のデフォルト ルートを設定している場合は、この点が特に問題となります。

SVMにはデフォルトルートを1つだけ設定するのがベストプラクティスです。中断を避けるため、より具体的なルートでは到達できないネットワークアドレスにも、デフォルトルートが到達できることを確認してください。詳細については、"NetAppナレッジベース：SU134 - clustered ONTAPでの不適切なルーティング設定によりネットワークアクセスが中断される可能性があります"を参照してください。

ONTAPネットワークの静的ルートを作成する

Storage Virtual Machine（SVM）内で静的ルートを作成して、LIFが発信トラフィックをネットワークでどのように取り扱うかを制御できます。

SVMに関連するルート エントリを作成すると、そのルートが、ゲートウェイと同じサブネットにあり、指定したSVMに所有されているすべてのLIFで使用されます。

手順

`network route create`コマンドを使用してルートを作成します。

```
network route create -vserver vs0 -destination 0.0.0.0/0 -gateway
10.61.208.1
```

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

ONTAPネットワークのマルチパスルーティングを有効にする

複数のルートが同じ宛先に対して同じメトリックを持つ場合、送信トラフィックにはそのうちの1つのルートのみが選択されます。その結果、他のルートは送信トラフィックの送信に使用されません。マルチパス ルーティングを有効にすると、同じメトリックを持

つ利用可能なルート間でロード バランシングを行うECMPルーティングとは対照的に、利用可能なすべてのルート間でメトリックに比例したロード バランシングを行うことができます。

手順

1. advanced権限レベルにログインします。

   ```
   set -privilege advanced
   ```

2. マルチパス ルーティングを有効にします。

   ```
   network options multipath-routing modify -is-enabled true
   ```

   クラスタのすべてのノードでマルチパス ルーティングが有効になります。

```
network options multipath-routing modify -is-enabled true
```

`network options multipath-routing modify`の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/network-options-multipath-routing-modify.html["ONTAPコマンド リファレンス"^]をご覧ください。

ONTAPネットワークから静的ルートを削除する

不要な静的ルートをStorage Virtual Machine（SVM）から削除できます。

手順

`network route delete`コマンドを使用して静的ルートを削除します。

次の例は、SVM vs0に関連付けられている、ゲートウェイ10.63.0.1とデスティネーションIPアドレス0.0.0.0/0の静的ルートを削除します。

```
network route delete -vserver vs0 -gateway 10.63.0.1 -destination
0.0.0.0/0
```

`network route delete`の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/network-route-delete.html["ONTAPコマンド リファレンス"^]をご覧ください。

ONTAPルーティング情報を表示する

クラスタ上のそれぞれのSVMについて、ルーティング設定に関する情報を表示できます。この情報は、クライアント アプリケーションやサービスとクラスタ内のノード上のLIFとの接続に問題がある場合のルーティングの問題を診断するのに役立ちます。

手順

1. `network route show`コマンドを使用して、1つ以上のSVM内のルートを表示します。次の例は、vs0 SVMに設定されたルートを示しています：

```
network route show
  (network route show)
Vserver             Destination     Gateway         Metric
------------------- --------------- --------------- ------
vs0
                    0.0.0.0/0       172.17.178.1    20
```

2. `network route show-lifs`コマンドを使用して、1つ以上のSVM内のルートとLIFの関連付けを表示します。

   次の例では、vs0というSVMが所有するルートとLIFの関連付けを表示しています。

```
network route show-lifs
  (network route show-lifs)

Vserver: vs0
Destination             Gateway                 Logical Interfaces
----------------------  --------------          --------------------
0.0.0.0/0               172.17.178.1            cluster_mgmt,
                                                LIF-b-01_mgmt1,
                                                LIF-b-02_mgmt1
```

`network route show`および `network route show-lifs`の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/search.html?q=network+route+show["ONTAPコマンド リファレンス"^]をご覧ください。

3. `network route active-entry show`コマンドを使用して、1つ以上のノード、SVM、サブネット、または指定された宛先を持つルートにインストールされているルートを表示します。

   次の例では、特定のSVMに設定されたすべてのルートを表示しています。

```
network route active-entry show -vserver Data0
```

```
Vserver: Data0
Node: node-1
Subnet Group: 0.0.0.0/0
Destination             Gateway              Interface   Metric  Flags
----------------------  -------------------  ---------   ------  -----
127.0.0.1               127.0.0.1            lo              10  UHS
127.0.10.1              127.0.20.1           losk            10  UHS
127.0.20.1              127.0.20.1           losk            10  UHS

Vserver: Data0
Node: node-1
Subnet Group: fd20:8b1e:b255:814e::/64
Destination             Gateway              Interface   Metric  Flags
----------------------  -------------------  ---------   ------  -----
default                 fd20:8b1e:b255:814e::1
                                             e0d             20  UGS
fd20:8b1e:b255:814e::/64
                        link#4               e0d              0  UC

Vserver: Data0
Node: node-2
Subnet Group: 0.0.0.0/0
Destination             Gateway              Interface   Metric  Flags
----------------------  -------------------  ---------   ------  -----
127.0.0.1               127.0.0.1            lo              10  UHS

Vserver: Data0
Node: node-2
Subnet Group: 0.0.0.0/0
Destination             Gateway              Interface   Metric  Flags
----------------------  -------------------  ---------   ------  -----
127.0.10.1              127.0.20.1           losk            10  UHS
127.0.20.1              127.0.20.1           losk            10  UHS

Vserver: Data0
Node: node-2
Subnet Group: fd20:8b1e:b255:814e::/64
Destination             Gateway              Interface   Metric  Flags
----------------------  -------------------  ---------   ------  -----
default                 fd20:8b1e:b255:814e::1
                                             e0d             20  UGS
fd20:8b1e:b255:814e::/64
                        link#4               e0d              0  UC
fd20:8b1e:b255:814e::1  link#4               e0d              0  UHL
11 entries were displayed.
```

`network route active-entry show`
の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/network-route-active-entry-show.html["ONTAPコマンド リファレンス"^]をご覧ください。

ONTAPネットワークのルーティングテーブルから動的ルートを削除します

IPv4およびIPv6のICMPリダイレクトを受信すると、動的ルートがルーティング テーブルに追加されます。動的ルートはデフォルトで300秒後に削除されます。動的ルートが維持される時間を変更する場合は、タイムアウト値を変更してください。

タスク概要

タイムアウト値は0～65,535秒の範囲で設定できます。値を0に設定すると、ルートは無期限になります。動的ルートを削除すると、無効なルートが永続化されることによる接続の喪失を防ぐことができます。

手順

1. 現在のタイムアウト値を表示します。
   - IPv4：

     ```
     network tuning icmp show
     ```

   - IPv6：

     ```
     network tuning icmp6 show
     ```

2. タイムアウト値を変更します。
   - IPv4：

     ```
     network tuning icmp modify -node node_name -redirect-timeout
     timeout_value
     ```

   - IPv6：

     ```
     network tuning icmp6 modify -node node_name -redirect-v6-timeout
     timeout_value
     ```

3. タイムアウト値が正しく変更されたことを確認します。
   - IPv4：

```
network tuning icmp show
```

◦ IPv6：

```
network tuning icmp6 show
```

`network tuning icmp`の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/search.html?q=network+tuning+icmp["ONTAPコマンドリファレンス"^]を参照してください。

ONTAP ネットワーク情報

ONTAPネットワーク情報を表示する

CLIを使用して、ポート、LIF、ルート、フェイルオーバー ルール、フェイルオーバー グループ、ファイアウォール ルール、DNS、NIS、および接続に関する情報を表示することができます。ONTAP 9.8以降では、ネットワークに関してSystem Managerに表示されているデータをダウンロードすることもできます。

これらの情報は、ネットワークの再設定やクラスタのトラブルシューティングを行うときに便利です。

クラスタ管理者は、ネットワーク情報をすべて表示することができます。SVM管理者は、割り当てられているSVMに関連する情報のみを表示できます。

System Manager では、リスト ビュー に情報を表示しているときに ダウンロード をクリックすると、表示されているオブジェクトのリストがダウンロードされます。

- リストはコンマ区切り値（CSV）形式でダウンロードされます。
- 表示されている列のデータのみがダウンロードされます。
- CSV ファイル名は、オブジェクト名とタイムスタンプでフォーマットされます。

ONTAPネットワークポート情報を表示する

クラスタ内の特定のポート、またはすべてのノードのすべてのポートに関する情報を表示できます。

タスク概要

次の情報が表示されます。

- ノード名
- ポート名

- IPspace名
- ブロードキャスト ドメイン名
- リンクのステータス（upまたはdown）
- MTUの設定
- ポート速度の設定と動作ステータス（毎秒1ギガビットまたは10ギガビット）
- 自動ネゴシエーション設定（trueまたはfalse）
- 二重モードと動作ステータス（halfまたはfull）
- ポートのインターフェイス グループ（該当する場合）
- ポートのVLANタグの情報（該当する場合）
- ポートのヘルス ステータス（「正常」または「デグレード」）
- ポートがデグレードとマークされた理由

フィールドのデータが利用できない場合（たとえば、非アクティブなポートの動作デュプレックスと速度は利用できません）、フィールド値は `-`として表示されます。

手順

`network port show`コマンドを使用してネットワーク ポート情報を表示します。

`-instance`パラメータを指定して各ポートの詳細情報を表示したり、 `-fields`パラメータを使用してフィールド名を指定して特定の情報を取得したりできます。

```
network port show
Node: node1

Ignore
                                                  Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
--------- ------------ ---------------- ---- ---- ----------- --------
------
e0a       Cluster      Cluster          up   9000  auto/1000  healthy
false
e0b       Cluster      Cluster          up   9000  auto/1000  healthy
false
e0c       Default      Default          up   1500  auto/1000  degraded
false
e0d       Default      Default          up   1500  auto/1000  degraded
true
Node: node2

Ignore
                                                  Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
--------- ------------ ---------------- ---- ---- ----------- --------
------
e0a       Cluster      Cluster          up   9000  auto/1000  healthy
false
e0b       Cluster      Cluster          up   9000  auto/1000  healthy
false
e0c       Default      Default          up   1500  auto/1000  healthy
false
e0d       Default      Default          up   1500  auto/1000  healthy
false
8 entries were displayed.
```

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

ONTAP VLAN情報を表示する

特定のVLANやクラスタ内のすべてのVLANに関する情報を表示できます。

タスク概要

`-instance`パラメータを指定することで、各VLANの詳細情報を表示できます。 `-fields`パラメータを使用してフィールド名を指定することで、特定の情報を表示できます。

手順

`network port vlan show`コマンドを使用してVLANに関する情報を表示します。次のコマンドは、クラスタ内のすべてのVLANに関する情報を表示します：

```
network port vlan show
                  Network Network
Node   VLAN Name Port    VLAN ID  MAC Address
------ --------- ------- -------- -----------------
cluster-1-01
       a0a-10    a0a     10       02:a0:98:06:10:b2
       a0a-20    a0a     20       02:a0:98:06:10:b2
       a0a-30    a0a     30       02:a0:98:06:10:b2
       a0a-40    a0a     40       02:a0:98:06:10:b2
       a0a-50    a0a     50       02:a0:98:06:10:b2
cluster-1-02
       a0a-10    a0a     10       02:a0:98:06:10:ca
       a0a-20    a0a     20       02:a0:98:06:10:ca
       a0a-30    a0a     30       02:a0:98:06:10:ca
       a0a-40    a0a     40       02:a0:98:06:10:ca
       a0a-50    a0a     50       02:a0:98:06:10:ca
```

`network port vlan show`の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/network-port-vlan-show.html["ONTAPコマンド リファレンス"^]をご覧ください。

ONTAPインターフェース グループ情報を表示する

インターフェイス グループに関する情報を表示して、その設定を確認できます。

タスク概要

次の情報が表示されます。

- インターフェイス グループが配置されているノード
- インターフェイス グループに含まれているネットワーク ポートのリスト
- インターフェイス グループの名前
- 分散機能（MAC、IP、ポート、シーケンシャル）
- インターフェイス グループのMAC（メディア アクセス制御）アドレス
- ポートのアクティビティ・ステータス、つまりポート全体がアクティブ（完全参加）か、一部がアクティブ（部分参加）か、1つもアクティブでないか

手順

`network port ifgrp show`コマンドを使用してインターフェース グループに関する情報を表示します。

`-instance`パラメータを指定することで、各ノードの詳細情報を表示できます。 `-fields`パラメータを使用してフィールド名を指定することで、特定の情報を表示できます。

次のコマンドは、クラスタ内のすべてのインターフェイス グループに関する情報を表示します。

```
network port ifgrp show
          Port     Distribution                    Active
Node      IfGrp    Function     MAC Address        Ports   Ports
--------- -------- ------------ -----------------  ------- --------
cluster-1-01
          a0a      ip           02:a0:98:06:10:b2  full    e7a, e7b
cluster-1-02
          a0a      sequential   02:a0:98:06:10:ca  full    e7a, e7b
cluster-1-03
          a0a      port         02:a0:98:08:5b:66  full    e7a, e7b
cluster-1-04
          a0a      mac          02:a0:98:08:61:4e  full    e7a, e7b
```

次のコマンドは、1つのノードのインターフェイス グループに関する詳細情報を表示します。

```
network port ifgrp show -instance -node cluster-1-01

                  Node: cluster-1-01
 Interface Group Name: a0a
Distribution Function: ip
        Create Policy: multimode
          MAC Address: 02:a0:98:06:10:b2
   Port Participation: full
        Network Ports: e7a, e7b
             Up Ports: e7a, e7b
           Down Ports: -
```

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

ONTAP LIF情報を表示する

LIFに関する詳細情報を表示して、LIFの設定を確認できます。

この情報は、IPアドレスが重複していないか、ネットワーク ポートが正しいサブネットに属しているかなど、LIFの基本的な問題を診断するのにも便利です。Storage Virtual Machine（SVM）管理者は、SVMに関連付けられているLIFの情報だけを表示できます。

タスク概要

次の情報が表示されます。

- LIFに関連付けられているIPアドレス
- LIFの管理ステータス
- LIFの動作ステータス

  データLIFの動作ステータスは、そのデータLIFが関連付けられているSVMのステータスで決まります。SVMが停止すると、LIFの動作ステータスはdownに変わります。SVMが再び起動すると、動作ステータスはupに変わります。

- LIFが配置されているノードとポート

フィールドのデータが利用できない場合（たとえば、拡張ステータス情報がない場合）、フィールド値は `-` として表示されます。

手順

`network interface show`コマンドを使用してLIF情報を表示します。

各LIFの詳しい情報を表示するには、-instanceパラメータを指定します。特定の情報を表示するには、-fields

パラメータを使用してフィールド名を指定します。

次のコマンドは、クラスタ内のすべてのLIFに関する一般的な情報を表示します。

```
network interface show
           Logical    Status     Network          Current      Current Is
Vserver    Interface  Admin/Oper Address/Mask     Node         Port
Home
---------- ---------- ---------- ---------------- ------------ -------
----
example
           lif1         up/up    192.0.2.129/22   node-01
                                                               e0d
false
node
           cluster_mgmt up/up    192.0.2.3/20     node-02
                                                               e0c
false
node-01
           clus1        up/up    192.0.2.65/18    node-01
                                                               e0a
true
           clus2        up/up    192.0.2.66/18    node-01
                                                               e0b
true
           mgmt1        up/up    192.0.2.1/20     node-01
                                                               e0c
true
node-02
           clus1        up/up    192.0.2.67/18    node-02
                                                               e0a
true
           clus2        up/up    192.0.2.68/18    node-02
                                                               e0b
true
           mgmt2        up/up    192.0.2.2/20     node-02
                                                               e0d
true
vs1
           d1           up/up    192.0.2.130/21   node-01
                                                               e0d
false
           d2           up/up    192.0.2.131/21   node-01
                                                               e0d
true
           data3        up/up    192.0.2.132/20   node-02
                                                               e0c
true
```

次のコマンドは、1つのLIFに関する詳細情報を表示します。

```
network interface show -lif data1 -instance

                    Vserver Name: vs1
          Logical Interface Name: data1
                            Role: data
                   Data Protocol: nfs,cifs
                       Home Node: node-01
                       Home Port: e0c
                    Current Node: node-03
                    Current Port: e0c
               Operational Status: up
                  Extended Status: -
                          Is Home: false
                  Network Address: 192.0.2.128
                          Netmask: 255.255.192.0
            Bits in the Netmask: 18
                IPv4 Link Local: -
                    Subnet Name: -
             Administrative Status: up
                  Failover Policy: local-only
                  Firewall Policy: data
                      Auto Revert: false
   Fully Qualified DNS Zone Name: xxx.example.com
         DNS Query Listen Enable: false
             Failover Group Name: Default
                        FCP WWPN: -
                  Address family: ipv4
                         Comment: -
                  IPspace of LIF: Default
```

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

ONTAPネットワークのルーティング情報を表示する

SVMのルートに関する情報を表示できます。

手順

表示するルーティング情報の種類に応じて、適切なコマンドを入力します。

…に関する情報を表示するには	入力する内容

SVMごとの静的ルート	`network route show`
各ルートのLIF（SVMごと）	`network route show-lifs`

`-instance`パラメータを指定することで、各ルートの詳細情報を表示できます。次のコマンドは、cluster-1内のSVM内のスタティック ルートを表示します：

```
network route show
Vserver              Destination     Gateway         Metric
-------------------- --------------- --------------- ------
Cluster
                     0.0.0.0/0       10.63.0.1       10
cluster-1
                     0.0.0.0/0       198.51.9.1      10
vs1
                     0.0.0.0/0       192.0.2.1       20
vs3
                     0.0.0.0/0       192.0.2.1       20
```

次のコマンドは、cluster-1のすべてのSVM内の静的ルートと論理インターフェイス（LIF）の関連付けを表示します。

```
network route show-lifs
Vserver: Cluster
Destination             Gateway                 Logical Interfaces
----------------------  ----------------------  ------------------
0.0.0.0/0               10.63.0.1               -

Vserver: cluster-1
Destination             Gateway                 Logical Interfaces
----------------------  ----------------------  ------------------
0.0.0.0/0               198.51.9.1              cluster_mgmt,
                                                cluster-1_mgmt1,

Vserver: vs1
Destination             Gateway                 Logical Interfaces
----------------------  ----------------------  ------------------
0.0.0.0/0               192.0.2.1               data1_1, data1_2

Vserver: vs3
Destination             Gateway                 Logical Interfaces
----------------------  ----------------------  ------------------
0.0.0.0/0               192.0.2.1               data2_1, data2_2
```

`network route show`および `network route show-lifs`
の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/search.html?q=network+route+show["ONTAPコマンド リファレンス"^]をご覧ください。

ONTAP DNSホストテーブルエントリを表示する

DNS hostsテーブル エントリでは、ホスト名がIPアドレスにマッピングされています。クラスタ内のすべてのSVMについて、ホスト名とエイリアス名、そのマッピング先のIPアドレスを表示できます。

手順

vserver services name-service dns hosts showコマンドを使用して、すべてのSVMのホスト名エントリを表示します。

以下の例では、hostsテーブル エントリを表示しています。

```
vserver services name-service dns hosts show
Vserver    Address         Hostname        Aliases
---------- --------------- --------------- ---------------------
cluster-1
           10.72.219.36    lnx219-36       -
vs1
           10.72.219.37    lnx219-37       lnx219-37.example.com
```

`vserver services name-service dns`コマンドを使用してSVMでDNSを有効にし、ホスト名の解決にDNSを使用するように設定できます。ホスト名は外部DNSサーバを使用して解決されます。

ONTAP DNSドメイン構成情報を表示する

クラスタ内の1つ以上のStorage Virtual Machine（SVM）のDNSドメイン設定を表示して、正しく設定されているかどうかを確認できます。

手順

`vserver services name-service dns show`コマンドを使用してDNSドメイン構成を表示します。

次のコマンドは、クラスタ内のすべてのSVMのDNS設定を表示します。

```
vserver services name-service dns show
                                                  Name
Vserver         State     Domains                 Servers
--------------- --------- ----------------------- -------------
cluster-1        enabled   xyz.company.com         192.56.0.129,
                                                  192.56.0.130
vs1             enabled   xyz.company.com         192.56.0.129,
                                                  192.56.0.130
vs2             enabled   xyz.company.com         192.56.0.129,
                                                  192.56.0.130
vs3             enabled   xyz.company.com         192.56.0.129,
                                                  192.56.0.130
```

次のコマンドは、SVM vs1のDNS設定の詳細を表示します。

```
vserver services name-service dns show -vserver vs1
               Vserver: vs1
               Domains: xyz.company.com
          Name Servers: 192.56.0.129, 192.56.0.130
    Enable/Disable DNS: enabled
        Timeout (secs): 2
      Maximum Attempts: 1
```

ONTAPフェイルオーバーグループ情報を表示する

フェイルオーバー グループに関する情報を表示できます。表示できる情報には、各フェイルオーバー グループ内のノードとポートのリスト、フェイルオーバーの有効 / 無効、各LIFに適用されているフェイルオーバー ポリシーの種類などがあります。

手順

1. `network interface failover-groups show`コマンドを使用して、各フェイルオーバー グループのターゲット ポートを表示します。

   次のコマンドは、2ノード クラスタのすべてのフェイルオーバー グループの情報を表示します。

```
network interface failover-groups show
                                Failover
Vserver         Group           Targets
--------------- --------------- --------------------------------
Cluster
                Cluster
                                cluster1-01:e0a, cluster1-01:e0b,
                                cluster1-02:e0a, cluster1-02:e0b
vs1
                Default
                                cluster1-01:e0c, cluster1-01:e0d,
                                cluster1-01:e0e, cluster1-02:e0c,
                                cluster1-02:e0d, cluster1-02:e0e
```

```
`network interface failover-groups show`
の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/network-interface-failover-groups-show.html["ONTAPコマンド リファレンス
"^]をご覧ください。
```

2. `network interface failover-groups show`コマンドを使用して、特定のフェイルオーバー グループのターゲット ポートとブロードキャスト ドメインを表示します。

   次のコマンドは、SVM vs4のdata12というフェイルオーバー グループに関する詳細情報を表示します。

```
network interface failover-groups show -vserver vs4 -failover-group
data12

       Vserver Name: vs4
Failover Group Name: data12
   Failover Targets: cluster1-01:e0f, cluster1-01:e0g, cluster1-02:e0f,
                     cluster1-02:e0g
   Broadcast Domain: Default
```

3. `network interface show`コマンドを使用して、すべてのLIFで使用されるフェイルオーバー設定を表示します。

   次のコマンドは、各LIFで使用されているフェイルオーバー ポリシーとフェイルオーバー グループを表示します。

```
network interface show -vserver * -lif * -fields failover-
group,failover-policy
vserver   lif                  failover-policy         failover-group
--------  -------------------  ----------------------  --------------
Cluster   cluster1-01_clus_1  local-only              Cluster
Cluster   cluster1-01_clus_2  local-only              Cluster
Cluster   cluster1-02_clus_1  local-only              Cluster
Cluster   cluster1-02_clus_2  local-only              Cluster
cluster1  cluster_mgmt        broadcast-domain-wide   Default
cluster1  cluster1-01_mgmt1   local-only              Default
cluster1  cluster1-02_mgmt1   local-only              Default
vs1       data1               disabled                Default
vs3       data2               system-defined          group2
```

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

ONTAPLIFフェイルオーバーターゲットを表示する

LIFのフェイルオーバー ポリシーとフェイルオーバー グループが正しく設定されていることを確認する必要が生じる場合があります。フェイルオーバー ルールの設定ミスを防ぐために、1つまたはすべてのLIFのフェイルオーバー ターゲットを表示できます。

タスク概要

LIFのフェイルオーバー ターゲットを表示することで、以下のことを確認できます。

- LIFに正しいフェイルオーバー グループとフェイルオーバー ポリシーが設定されているか

- 表示されたフェイルオーバー ターゲット ポートのリストが、それぞれのLIFについて適切か
- データLIFのフェイルオーバー ターゲットが管理ポート（e0M）になっていないか

手順

`network interface show`コマンドの `failover`オプションを使用して、LIFのフェイルオーバー ターゲットを表示します。

次のコマンドは、2ノードクラスタ内のすべてのLIFのフェイルオーバーターゲットに関する情報を表示します。 `Failover Targets`行には、指定されたLIFのノードとポートの組み合わせの（優先順位付けされた）リストが表示されます。

```
network interface show -failover
         Logical       Home                  Failover        Failover
Vserver  Interface     Node:Port             Policy          Group
-------- ------------ --------------------- --------------- ---------
Cluster
         node1_clus1   node1:e0a             local-only      Cluster
                       Failover Targets: node1:e0a,
                                         node1:e0b
         node1_clus2   node1:e0b             local-only      Cluster
                       Failover Targets: node1:e0b,
                                         node1:e0a
         node2_clus1   node2:e0a             local-only      Cluster
                       Failover Targets: node2:e0a,
                                         node2:e0b
         node2_clus2   node2:e0b             local-only      Cluster
                       Failover Targets: node2:e0b,
                                         node2:e0a
cluster1
         cluster_mgmt  node1:e0c             broadcast-domain-wide
                                                             Default
                       Failover Targets: node1:e0c,
                                         node1:e0d,
                                         node2:e0c,
                                         node2:e0d
         node1_mgmt1   node1:e0c             local-only      Default
                       Failover Targets: node1:e0c,
                                         node1:e0d
         node2_mgmt1   node2:e0c             local-only      Default
                       Failover Targets: node2:e0c,
                                         node2:e0d
vs1
         data1         node1:e0e             system-defined  bcast1
                       Failover Targets: node1:e0e,
                                         node1:e0f,
                                         node2:e0e,
                                         node2:e0f
```

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

ロード バランシング ゾーン内の **ONTAP LIF** を表示する

ロード バランシング ゾーンに属するすべてのLIFを表示して、そのゾーンが正しく設定されているかを確認できます。特定のLIF、またはすべてのLIFのロード バランシング ゾーンを表示することもできます。

手順

次のコマンドを使用して、LIFとロード バランシングの詳細を表示します。

表示するには...	入力する内容
特定のロード バランシング ゾーン内のLIF	`network interface show -dns-zone zone_name` `zone_name` ロード バランシング ゾーンの名前を指定します。
特定のLIFのロード バランシング ゾーン	`network interface show -lif lif_name -fields dns-zone`
すべてのLIFのロード バランシング ゾーン	`network interface show -fields dns-zone`

LIFのロード バランシング ゾーンを表示する例

次のコマンドは、SVM vs0のstorage.company.comというロード バランシング ゾーンに属するすべてのLIFの詳細を表示します。

```
net int show -vserver vs0 -dns-zone storage.company.com

          Logical    Status     Network            Current   Current Is
Vserver   Interface  Admin/Oper Address/Mask       Node      Port    Home
--------- ---------- ---------- ------------------ --------- ------- ----
vs0
          lif3         up/up    10.98.226.225/20   ndeux-11  e0c     true
          lif4         up/up    10.98.224.23/20    ndeux-21  e0c     true
          lif5         up/up    10.98.239.65/20    ndeux-11  e0c     true
          lif6         up/up    10.98.239.66/20    ndeux-11  e0c     true
          lif7         up/up    10.98.239.63/20    ndeux-21  e0c     true
          lif8         up/up    10.98.239.64/20    ndeux-21  e0c     true
```

次のコマンドは、data3というLIFのDNSゾーンの詳細を表示します。

```
network interface show -lif data3 -fields dns-zone
Vserver  lif    dns-zone
-------  -----  --------
vs0      data3  storage.company.com
```

次のコマンドは、クラスタ内のすべてのLIF、および対応するDNSゾーンを表示します。

```
network interface show -fields dns-zone
Vserver   lif          dns-zone
-------   ------------ --------
cluster   cluster_mgmt none
ndeux-21  clus1        none
ndeux-21  clus2        none
ndeux-21  mgmt1        none
vs0       data1        storage.company.com
vs0       data2        storage.company.com
```

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

ONTAPクラスタ接続の表示

クラスタ内のすべてのアクティブな接続を表示したり、クライアント、論理インターフェイス、プロトコル、またはサービス別にノードのアクティブな接続を表示したりすることができます。また、クラスタ内のリスンしているすべての接続を表示することもできます。

クライアント別のアクティブな接続の表示（クラスタ管理者のみ）

クライアント別にアクティブな接続数を表示して、特定のクライアントで使用されているノードを確認したり、ノードあたりのクライアント数に不均衡がないかどうかを確認したりできます。

タスク概要

クライアント別のアクティブな接続数の情報は、次のような場合に役立ちます。

- ビジー状態や過負荷のノードを見つける。
- 特定のクライアントからのボリュームへのアクセスが低速になっている理由を確認する。

  クライアントがアクセスしているノードに関する詳細を表示し、ボリュームが配置されているノードと比較できます。ボリュームへのアクセスにクラスタ ネットワークのトラバースが必要な場合、オーバーサブスクライブされたリモート ノードにあるボリュームへのリモート アクセスにより、クライアントのパフォーマンスが低下することがあります。

- データ アクセスにすべてのノードが均等に使用されていることを確認する。
- 接続数が想定よりも多いクライアントを探す。
- 特定のクライアントがノードに接続しているかどうかを確認する。

手順

`network connections active show-clients`コマンドを使用して、ノード上のクライアントによるアクティブな接続の数を表示します。

`network connections active show-clients`の詳細については、link:http://docs.netapp.com/us-en/ontap-cli/network-connections-active-show-clients.html["ONTAPコマンド リファレンス"^]をご覧ください。

```
network connections active show-clients
Node    Vserver Name    Client IP Address     Count
------  --------------  -----------------     ------
node0   vs0             192.0.2.253                1
        vs0             192.0.2.252                2
        Cluster         192.10.2.124               5
node1   vs0             192.0.2.250                1
        vs0             192.0.2.252                3
        Cluster         192.10.2.123               4
node2   vs1             customer.example.com       1
        vs1             192.0.2.245                3
        Cluster         192.10.2.122               4
node3   vs1             customer.example.org       1
        vs1             customer.example.net       3
        Cluster         192.10.2.121               4
```

プロトコル別のアクティブな接続の表示（クラスタ管理者のみ）

ノードのアクティブな接続数をプロトコル（TCPまたはUDP）別に表示して、クラスタ内のプロトコルの使用状況を比較できます。

タスク概要

プロトコル別のアクティブな接続数の情報は、次のような場合に役立ちます。

- 接続が切断されているUDPクライアントを探す。

  ノードの接続数が制限に近づいたときに最初に接続が切断されるのはUDPクライアントです。

- 他のプロトコルが使用されていないことを確認する。

手順

`network connections active show-protocols`コマンドを使用して、ノード上のプロトコル別のアクティブな接続数を表示します。

`network connections active show-protocols`の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/network-connections-active-show-protocols.html["ONTAPコマンド リファレンス"^]をご覧ください。

```
network connections active show-protocols
Node     Vserver Name  Protocol   Count
-------  ------------  ---------  ------
node0
         vs0           UDP            19
         Cluster       TCP            11
node1
         vs0           UDP            17
         Cluster       TCP             8
node2
         vs1           UDP            14
         Cluster       TCP            10
node3
         vs1           UDP            18
         Cluster       TCP             4
```

サービス別のアクティブな接続の表示（クラスタ管理者のみ）

クラスタ内の各ノードのアクティブな接続数をサービス タイプ（NFS、SMB、マウントなど）別に表示できます。これによりクラスタ内のサービスの使用状況を比較でき、ノードのプライマリ ワークロードを確認するのに役立ちます。

タスク概要

サービス別のアクティブな接続数の情報は、次のような場合に役立ちます。

- すべてのノードが適切なサービス用に使用されていること、そのサービスのロード バランシングが機能していることを確認する。
- 他のサービスが使用されていないことを確認します。 `network connections active show-services`コマンドを使用して、ノード上のサービスごとのアクティブな接続数を表示します。

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

```
network connections active show-services
Node        Vserver Name    Service    Count
---------  --------------  ---------  ------
node0
            vs0             mount           3
            vs0             nfs            14
            vs0             nlm_v4          4
            vs0             cifs_srv        3
            vs0             port_map       18
            vs0             rclopcp        27
            Cluster         ctlopcp        60
node1
            vs0             cifs_srv        3
            vs0             rclopcp        16
            Cluster         ctlopcp        60
node2
            vs1             rclopcp        13
            Cluster         ctlopcp        60
node3
            vs1             cifs_srv        1
            vs1             rclopcp        17
            Cluster         ctlopcp        60
```

ノードおよび**SVM**の**LIF**別のアクティブな接続の表示

ノードおよびStorage Virtual Machine（SVM）のLIF別のアクティブな接続数を表示して、クラスタ内のLIF間で接続数の不均衡がないかどうかを確認できます。

タスク概要

LIF別のアクティブな接続数の情報は、次のような場合に役立ちます。

- 各LIFの接続数を比較することで、過負荷のLIFを探す。
- すべてのデータLIFに対してDNSロード バランシングが機能していることを確認する。
- さまざまなSVMへの接続数を比較して、最もよく使用されているSVMを特定する。

手順

`network connections active show-lifs`コマンドを使用して、SVM
およびノードごとに各LIFのアクティブな接続の数を表示します。

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

```
network connections active show-lifs
Node      Vserver Name  Interface Name  Count
--------  ------------  --------------- ------
node0
          vs0           datalif1             3
          Cluster       node0_clus_1         6
          Cluster       node0_clus_2         5
node1
          vs0           datalif2             3
          Cluster       node1_clus_1         3
          Cluster       node1_clus_2         5
node2
          vs1           datalif2             1
          Cluster       node2_clus_1         5
          Cluster       node2_clus_2         3
node3
          vs1           datalif1             1
          Cluster       node3_clus_1         2
          Cluster       node3_clus_2         2
```

クラスタ内のアクティブな接続の表示

クラスタ内のアクティブな接続に関する情報を表示して、それぞれの接続で使用されているLIF、ポート、リモート ホスト、サービス、Storage Virtual Machine（SVM）、およびプロトコルを確認できます。

タスク概要

クラスタ内のアクティブな接続の情報は、次のような場合に役立ちます。

- 個々のクライアントで正しいノードの正しいプロトコルやサービスを使用していることを確認する。
- クライアントで特定の組み合わせのノード、プロトコル、およびサービスを使用してデータにアクセスできない場合に、同様のクライアントを探して設定やパケット トレースを比較する。

手順

`network connections active show`コマンドを使用して、クラスタ内のアクティブな接続を表示します。

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

次のコマンドは、node1というノードのアクティブな接続の情報を表示します。

```
network connections active show -node node1
Vserver  Interface           Remote
Name     Name:Local Port     Host:Port           Protocol/Service
-------  ------------------  ------------------  ---------------
Node: node1
Cluster  node1_clus_1:50297  192.0.2.253:7700    TCP/ctlopcp
Cluster  node1_clus_1:13387  192.0.2.253:7700    TCP/ctlopcp
Cluster  node1_clus_1:8340   192.0.2.252:7700    TCP/ctlopcp
Cluster  node1_clus_1:42766  192.0.2.252:7700    TCP/ctlopcp
Cluster  node1_clus_1:36119  192.0.2.250:7700    TCP/ctlopcp
vs1      data1:111           host1.aa.com:10741  UDP/port-map
vs3      data2:111           host1.aa.com:10741  UDP/port-map
vs1      data1:111           host1.aa.com:12017  UDP/port-map
vs3      data2:111           host1.aa.com:12017  UDP/port-map
```

次のコマンドは、SVM vs1のアクティブな接続の情報を表示します。

```
network connections active show -vserver vs1
Vserver  Interface           Remote
Name     Name:Local Port     Host:Port           Protocol/Service
-------  ------------------  ------------------  ---------------
Node: node1
vs1      data1:111           host1.aa.com:10741  UDP/port-map
vs1      data1:111           host1.aa.com:12017  UDP/port-map
```

クラスタ内のリスンしている接続の表示

クラスタ内のリスンしている接続を表示して、特定のプロトコルとサービスの接続を受け入れているLIFとポートを確認することができます。

タスク概要

クラスタ内のリスンしている接続の表示は、次のような場合に役立ちます。

- 特定のLIFへのクライアント接続が必ず失敗する場合に、そのLIFを適切なプロトコルまたはサービスでリスンしていることを確認する。
- あるノードのボリュームのデータに別のノードのLIFを介してリモート アクセスできない場合に、それぞれのクラスタLIFでUDP / rclopcpリスナーが開いていることを確認する。
- 同じクラスタの2つのノード間でのSnapMirror転送に失敗した場合に、それぞれのクラスタLIFでUDP / rclopcpリスナーが開いていることを確認する。
- 異なるクラスタの2つのノード間でのSnapMirror転送に失敗した場合に、それぞれのクラスタ間LIFでTCP / ctlopcpリスナーが開いていることを確認する。

手順

`network connections listening show`コマンドを使用して、ノードごとのリスニング接続を表示します。

```
network connections listening show
Vserver Name     Interface Name:Local Port        Protocol/Service
---------------- -------------------------------  ----------------
Node: node0
Cluster          node0_clus_1:7700                TCP/ctlopcp
vs1              data1:4049                       UDP/unknown
vs1              data1:111                        TCP/port-map
vs1              data1:111                        UDP/port-map
vs1              data1:4046                       TCP/sm
vs1              data1:4046                       UDP/sm
vs1              data1:4045                       TCP/nlm-v4
vs1              data1:4045                       UDP/nlm-v4
vs1              data1:2049                       TCP/nfs
vs1              data1:2049                       UDP/nfs
vs1              data1:635                        TCP/mount
vs1              data1:635                        UDP/mount
Cluster          node0_clus_2:7700                TCP/ctlopcp
```

`network connections listening show`
の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/network-connections-listening-show.html["ONTAPコマンド リファレンス"^]をご覧ください。

ネットワークの問題を診断するための**ONTAP**コマンド

`ping, traceroute, ndp,`や
`tcpdump`などのコマンドを使用して、ネットワーク上の問題を診断できます。また、
`ping6`や `traceroute6`などのコマンドを使用してIPv6の問題を診断することもできます。

状況	コマンド
ノードがネットワーク上の他のホストに到達できるかどうかをテストする	`network ping`
ノードがIPv6ネットワーク上の他のホストに到達できるかどうかをテストする	`network ping6`
IPv4パケットがネットワーク ノードまでたどったルートをトレースする	`network traceroute`
IPv6パケットがネットワーク ノードまでたどったルートをトレースする	`network traceroute6`
近隣探索プロトコル（NDP）を管理する	`network ndp`
指定したネットワーク インターフェイスまたはすべてのネットワーク インターフェイスで送受信されたパケットの統計情報を表示する	`run -node node_name ifstat` 注：このコマンドはノードシェルから利用できます。
クラスタの各ノードとポートから検出した近隣デバイスの情報（リモート デバイスの種類とデバイスのプラットフォームを含む）を表示する	`network device-discovery show`
ノードのCDP近隣デバイスを表示する（ONTAPはCDPv1通知のみをサポート）	`run -node node_name cdpd show-neighbors` 注：このコマンドはノードシェルから利用できます。
ネットワークで送受信されたパケットをトレースする	`network tcpdump start -node node-name -port port_name` 注：このコマンドはノードシェルから利用できます。
クラスタ間のノードまたはクラスタ内のノード間のレイテンシとスループットを測定する	`network test -path -source-node source_nodename local -destination-cluster destination_clustername -destination-node destination_nodename -session -type Default, AsyncMirrorLocal, AsyncMirrorRemote, SyncMirrorRemote, or RemoteDataTransfer` 詳細については、"パフォーマンス管理"を参照してください。

関連情報

- "ONTAPコマンド リファレンス"
- "network ping"
- "network traceroute"
- "network device-discovery show"
- "network ndp"

ネイバー探索プロトコルを使用してネットワーク接続を表示する

ネイバー探索プロトコルを使用した **ONTAP** ネットワーク接続の表示

データセンターでは、ネイバー探索プロトコルを使用して、物理システムまたは仮想システムのペアとそのネットワークインターフェース間のネットワーク接続を表示できます。ONTAPは、Cisco Discovery Protocol（CDP）とLink Layer Discovery Protocol（LLDP）という2つのネイバー探索プロトコルをサポートしています。

近隣探索プロトコルによって、ネットワーク内の直接接続されているプロトコル対応デバイスが自動的に検出され、その情報が表示されるようになります。各デバイスがID、機能、および接続情報を通知します。この情報はイーサネット フレームでマルチキャストMACアドレスへ送信され、近隣のプロトコル対応デバイスで受信されます。

2つのデバイスどうしが近隣機器となるためには、各デバイスでプロトコルが有効で、正しく設定されている必要があります。探索プロトコルの機能は直接接続されたネットワークに限定されます。近隣機器には、スイッチ、ルーター、ブリッジなどのプロトコル対応デバイスが含まれます。ONTAPでは、2つの近隣探索プロトコルがサポートされます。これらは個別に使用することも一緒に使用することも可能です。

Cisco Discovery Protocol（CDP）

CDPは、Cisco Systemsが開発したリンク レイヤ プロトコルです。ONTAPでは、クラスタ ポートに対してこのプロトコルがデフォルトで有効になりますが、データ ポートに対しては明示的に有効にする必要があります。

Link Layer Discovery Protocol（LLDP）

LLDPは、ベンダーに依存しないプロトコルであり、IEEE 802.1AB規格のドキュメントで指定されています。このプロトコルは、すべてのポートに対して明示的に有効にする必要があります。

CDPを使用して**ONTAP**ネットワーク接続を検出する

CDPを使用したネットワーク接続の検出は、導入に関する考慮事項の確認、データ ポートでのCDPの有効化、近隣デバイスの表示、CDPの設定値の調整（必要な場合）で構成されます。クラスタ ポートでは、CDPはデフォルトで有効になります。

近隣デバイスに関する情報を表示するには、スイッチとルーターでもCDPを有効にする必要があります。

ONTAPリリース	概要
9.10.1以前	CDPは、クラスタ ネットワーク スイッチと管理ネットワーク スイッチを自動検出するためにクラスタ スイッチ ヘルスモニタでも使用されます。
9.11.1以降	CDP は、クラスタスイッチヘルスモニタによって、クラスタ、ストレージ、および管理ネットワークスイッチを自動的に検出するためにも使用されます。

関連情報

"システム管理"

CDPを使用する場合の考慮事項

デフォルトでは、CDP対応デバイスはCDPv2通知を送信します。CDP対応デバイスは、CDPv1通知を受信した場合にのみ、CDPv1通知を送信します。ONTAPはCDPv1のみをサポートします。したがって、ONTAPノードがCDPv1通知を送信すると、CDP対応の近隣デバイスがCDPv1通知を返します。

ノードでCDPを有効にする前に、次のことを考慮してください。

- CDPはすべてのポートでサポートされます。

- CDP通知は、up状態のポートから送受信されます。
- CDP通知を送信および受信するために、送信デバイスおよび受信デバイスの両方でCDPを有効にする必要があります。
- CDP通知は一定間隔で送信され、送信間隔は設定可能です。
- LIFのIPアドレスが変更されると、ノードは更新された情報を次のCDP通知で送信します。
- ONTAP 9.10.1以前：
  - CDPはクラスタ ポートで常に有効になります。
  - 非クラスタ ポートでは、CDPはデフォルトで無効になります。
- ONTAP 9.11.1以降：
  - CDPはクラスタ ポートとストレージ ポートで常に有効になります。
  - 非クラスタ ポートと非ストレージ ポートでは、CDPはデフォルトで無効になります。

ノードでLIFが変更された場合、スイッチなどの受信デバイス側でCDP情報が更新されないことがあります。このような問題が発生した場合は、ノードのネットワーク インターフェイスをいったんdown状態にしてから、up状態に設定してください。

- CDP通知で送信されるのはIPv4アドレスのみです。
- VLANが設定されている物理ネットワーク ポートの場合、VLANに設定されているすべてのLIFが通知されます。
- インターフェイス グループの一部となっている物理ポートの場合、そのインターフェイス グループに設定されているすべてのIPアドレスが、各物理ポートで通知されます。
- VLANをホストするインターフェイス グループの場合、インターフェイス グループおよびVLANに設定されているすべてのLIFが各ネットワーク ポートで通知されます。
- CDP パケットは 1500 バイト以下に制限されているため、多数の LIF が設定されているポートでは、隣接スイッチでこれらの IP アドレスのサブセットのみが報告される場合があります。

CDPの有効化または無効化

CDP対応の近隣デバイスを検出して通知を送信するには、クラスタの各ノードでCDPが有効になっている必要があります。

ONTAP 9.10.1以前では、CDPはデフォルトでノードのすべてのクラスタ ポートで有効に、非クラスタ ポートで無効になります。

ONTAP 9.11.1以降では、CDPはデフォルトでノードのすべてのクラスタ ポートとストレージ ポートで有効に、非クラスタ ポートと非ストレージ ポートで無効になります。

タスク概要

`cdpd.enable`オプションは、ノードのポート上で CDP を有効にするか無効にするかを制御します：

- ONTAP 9.10.1以前では、onにすると、非クラスタ ポートでCDPが有効になります。
- ONTAP 9.11.1以降では、onにすると、非クラスタ ポートと非ストレージ ポートでCDPが有効になりま

す。

- ONTAP 9.10.1以前では、offにすると、非クラスタ ポートでCDPが無効になります。クラスタ ポートのCDPを無効にすることはできません。
- ONTAP 9.11.1以降では、offにすると、非クラスタ ポートと非ストレージ ポートでCDPが無効になります。クラスタ ポートのCDPを無効にすることはできません。

CDP対応デバイスに接続されているポートでCDPを無効にすると、ネットワーク トラフィックが最適化されない可能性があります。

手順

1. クラスタ内の1つまたはすべてのノードの、現在のCDP設定を表示します。

…の CDP 設定を表示するには	入力する内容
1つのノード	`run - node <node_name> options cdpd.enable`
クラスタ内のすべてのノード	`options cdpd.enable`

2. クラスタ内の1つまたはすべてのノードで、すべてのポートのCDPを有効または無効に設定します。

CDPを有効または無効にする対象	入力する内容
1つのノード	`run -node node_name options cdpd.enable {on or off}`
クラスタ内のすべてのノード	`options cdpd.enable {on or off}`

CDP近隣情報の表示

クラスタノードの各ポートに接続されている隣接デバイスの情報を表示できます（ただし、ポートがCDP準拠デバイスに接続されている必要があります）。 `network device-discovery show -protocol cdp`コマンドを使用して隣接デバイス情報を表示できます。"ONTAPコマンド リファレンス"の `network device-discovery show`の詳細をご覧ください。

タスク概要

ONTAP 9.10.1以前の場合、クラスタ ポートではCDPが常に有効になっているため、これらのポートのCDP近隣情報は常に表示されます。非クラスタ ポートの近隣情報を表示するには、これらのポートでCDPを有効にする必要があります。

ONTAP 9.11.1以降の場合、クラスタ ポートとストレージ ポートではCDPが常に有効になっているので、これらのポートのCDP近隣情報は常に表示されます。非クラスタ ポートと非ストレージ ポートの近隣情報を表示するには、これらのポートでCDPを有効にする必要があります。

手順

クラスタ内のノードのポートに接続されているすべてのCDP対応デバイスの情報を表示します。

```
network device-discovery show -node node -protocol cdp
```

次のコマンドは、ノードsti2650-212のポートに接続されている近隣デバイスの情報を表示します。

```
network device-discovery show -node sti2650-212 -protocol cdp
Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface         Platform
----------- ------ ------------------------- ----------------
----------------
sti2650-212/cdp
            e0M    RTP-LF810-510K37.gdl.eng.netapp.com(SAL1942R8JS)
                                             Ethernet1/14      N9K-
C93120TX
            e0a    CS:RTP-CS01-510K35        0/8               CN1610
            e0b    CS:RTP-CS01-510K36        0/8               CN1610
            e0c    RTP-LF350-510K34.gdl.eng.netapp.com(FDO21521S76)
                                             Ethernet1/21      N9K-
C93180YC-FX
            e0d    RTP-LF349-510K33.gdl.eng.netapp.com(FDO21521S4T)
                                             Ethernet1/22      N9K-
C93180YC-FX
            e0e    RTP-LF349-510K33.gdl.eng.netapp.com(FDO21521S4T)
                                             Ethernet1/23      N9K-
C93180YC-FX
            e0f    RTP-LF349-510K33.gdl.eng.netapp.com(FDO21521S4T)
                                             Ethernet1/24      N9K-
C93180YC-FX
```

このコマンドの出力には、指定したノードの各ポートに接続されているCiscoデバイスが一覧表示されます。

CDPメッセージの保持時間の設定

保持時間は、CDP通知がCDP対応の近隣デバイスのキャッシュに格納される時間です。保持時間は各CDPv1パケットで通知され、ノードがCDPv1パケットを受信するたびに更新されます。

- `cdpd.holdtime`オプションの値は、HAペアの両方のノードで同じ値に設定する必要があります。
- デフォルトの保持時間は180ですが、10～255秒の値を入力できます。
- 保持時間が切れる前にIPアドレスが削除された場合、CDP情報は保持時間が切れるまでキャッシュされます。

手順

1. クラスタ内の1つまたはすべてのノードのCDPメッセージの現在の保持時間を表示します。

保持時間を表示する対象	入力する内容

1つのノード	`run -node node_name options cdpd.holdtime`
クラスタ内のすべてのノード	`options cdpd.holdtime`

2. クラスタ内の1つまたはすべてのノードで、すべてのポートのCDP通知の保持時間を設定します。

保持時間を設定する対象	入力する内容
1つのノード	`run -node node_name options cdpd.holdtime holdtime`
クラスタ内のすべてのノード	`options cdpd.holdtime holdtime`

CDP通知の送信間隔の設定

CDP通知は、一定の間隔でCDP近隣機器に送信されます。ネットワーク トラフィックの量やネットワーク トポロジの変化に応じて、CDP通知の送信間隔を調整することができます。

- `cdpd.interval`オプションの値は、HAペアの両方のノードで同じ値に設定する必要があります。
- デフォルトの送信間隔は60秒ですが、5～900秒の値を入力できます。

手順

1. クラスタ内の1つまたはすべてのノードについて、CDP通知の現在の送信間隔を表示します。

送信間隔を表示する対象	入力する内容
1つのノード	`run -node node_name options cdpd.interval`
クラスタ内のすべてのノード	`options cdpd.interval`

2. クラスタ内の1つまたはすべてのノードで、すべてのポートのCDP通知の送信間隔を設定します。

送信間隔を設定する対象	入力する内容
1つのノード	`run -node node_name options cdpd.interval interval`
クラスタ内のすべてのノード	`options cdpd.interval interval`

CDP統計情報の表示と消去

ネットワーク接続で発生する可能性のある問題を見つけるために、各ノードのクラスタ ポートと非クラスタ ポートのCDP統計情報を確認できます。CDP統計情報は、前回消去されたときからの累積値です。

タスク概要

ONTAP 9.10.1以前の場合、ポートでCDPが常に有効になっているので、これらのポートのトラフィックに関するCDP統計情報は常に表示されます。ポートのCDP統計情報を表示するには、ポートでCDPを有効にする

必要があります。

ONTAP 9.11.1以降の場合、クラスタ ポートとストレージ ポートではCDPが常に有効になっているので、これらのポートのトラフィックに関するCDP統計情報は常に表示されます。非クラスタ ポートと非ストレージ ポートのCDP統計情報を表示するには、これらのポートでCDPを有効にする必要があります。

手順

ノードのすべてのポートに関する現在のCDP統計情報を表示、または消去します。

状況	入力する内容
CDP統計情報を表示	`run -node node_name cdpd show-stats`
CDP統計情報を消去	`run -node node_name cdpd zero-stats`

統計情報の表示と消去の例

次のコマンドは、消去する前のCDP統計情報の例を示します。前回統計情報が消去されてから、送信および受信したパケットの総数が出力されています。

```
run -node node1 cdpd show-stats

RECEIVE
 Packets:          9116  | Csum Errors:       0  | Unsupported Vers:  4561
 Invalid length:      0  | Malformed:         0  | Mem alloc fails:      0
 Missing TLVs:        0  | Cache overflow:    0  | Other errors:         0

TRANSMIT
 Packets:          4557  | Xmit fails:        0  | No hostname:          0
 Packet truncated:    0  | Mem alloc fails:   0  | Other errors:         0

OTHER
 Init failures:       0
```

次のコマンドは、CDP統計情報を消去します。

```
run -node node1 cdpd zero-stats
```

```
run -node node1 cdpd show-stats

RECEIVE
 Packets:              0   | Csum Errors:         0   | Unsupported Vers:      0
 Invalid length:       0   | Malformed:           0   | Mem alloc fails:       0
 Missing TLVs:         0   | Cache overflow:      0   | Other errors:          0

TRANSMIT
 Packets:              0   | Xmit fails:          0   | No hostname:           0
 Packet truncated:     0   | Mem alloc fails:     0   | Other errors:          0

OTHER
 Init failures:        0
```

統計情報を消去すると、次にCDP通知が送信または受信された時点から情報が累積されていきます。

CDPがサポートされないイーサネット スイッチへの接続

一部のベンダーのスイッチはCDPをサポートしていません。詳細については、"NetApp ナレッジベース：ONTAP デバイス検出でスイッチではなくノードが表示される"をご覧ください。

この問題の解決方法は2つあります。

- CDPを無効にし、サポートされている場合はLLDPを有効にします。詳細については、"LLDPを使用したネットワーク接続の検出"を参照してください。
- CDP通知をドロップするように、スイッチにMACアドレス パケット フィルタを設定する

LLDPを使用してONTAPネットワーク接続を検出する

LLDPを使用したネットワーク接続の検出は、導入に関する考慮事項の確認、すべてのポートでのLLDPの有効化、近隣デバイスの表示、LLDPの設定値の調整（必要な場合）で構成されます。

近隣デバイスに関する情報を表示するには、スイッチとルーターでもLLDPを有効にする必要があります。

現時点では、ONTAPは次のType-Length-Value構造（TLV）を報告します。

- シャーシID
- ポートID
- Time-To-Live（TTL）
- システム名

  システム名TLVは、CNAデバイスでは送信されません。

X1143アダプタやUTA2オンボード ポートなどの特定の統合ネットワーク アダプタ（CNA）にはLLDPのオフロード サポートが含まれています。

- LLDPのオフロードは、Data Center Bridging（DCB）に使用されます。
- 表示される情報がクラスタとスイッチの間で異なる場合があります。

  スイッチで表示されるシャーシIDとポートIDのデータは、CNAポートとCNA以外のポートで異なる場合があります。

例：

- CNA以外のポート：
  - シャーシIDは、ノードのいずれかのポートの固定MACアドレスです。
  - ポートIDは、ノードの対応するポートのポート名です。
- CNAポート：
  - シャーシIDとポートIDは、ノードの対応するポートのMACアドレスです。

ただし、クラスタではこれらのポート タイプについて同じデータが表示されます。

LLDPの仕様では、SNMP MIBによる、収集された情報へのアクセスを定義します。ただし、現時点では、ONTAPはLLDP MIBをサポートしていません。

LLDPの有効化または無効化

LLDP対応の近隣デバイスを検出して通知を送信するには、クラスタの各ノードでLLDPが有効になっている必要があります。ONTAP 9.7以降では、ノードのすべてのポートでLLDPがデフォルトで有効になります。

タスク概要

ONTAP 9.10.1 以前では、この `lldp.enable`オプションはノードのポート上で LLDP を有効にするか無効にするかを制御します：

- `on` すべてのポートで LLDP を有効にします。
- `off` すべてのポートで LLDP を無効にします。

ONTAP 9.11.1 以降では、 `lldp.enable`オプションは、ノードの非クラスタポートおよび非ストレージポートで LLDP を有効にするか無効にするかを制御します：

- `on`すべての非クラスタポートおよび非ストレージポートで LLDP を有効にします。
- `off`すべての非クラスタポートおよび非ストレージポートで LLDP を無効にします。

手順

1. クラスタ内の1つまたはすべてのノードの、現在のLLDP設定を表示します。
   - 単一ノード： `run -node node_name options lldp.enable`
   - すべてのノード：オプション `lldp.enable`
2. クラスタ内の1つまたはすべてのノードで、すべてのポートのLLDPを有効または無効に設定します。

LLDPを有効または無効にする対象	入力する内容

1つのノード	`run -node node_name options lldp.enable {on
off}`	クラスタ内のすべてのノード
`options lldp.enable {on	off}`

- 1つのノード：

```
run -node node_name options lldp.enable {on|off}
```

- すべてのノード：

```
options lldp.enable {on|off}
```

LLDP近隣情報の表示

クラスタのノードのポートにLLDP対応デバイスが接続されている場合は、そのポートの近隣デバイスの情報を表示することができます。近隣情報を表示するには、network device-discovery showコマンドを使用します。

手順

1. クラスタ内のノードのポートに接続されているすべてのLLDP対応デバイスの情報を表示します。

```
network device-discovery show -node node -protocol lldp
```

次のコマンドは、ノード cluster-1_01 のポートに接続されているネイバーを表示します。出力には、指定されたノードの各ポートに接続されている LLDP 対応デバイスがリストされます。 `-protocol`オプションを省略すると、CDP 対応デバイスも出力されます。

```
network device-discovery show -node cluster-1_01 -protocol lldp
Node/       Local  Discovered
Protocol    Port   Device                    Interface         Platform
----------- ------ ------------------------- ----------------
----------------
cluster-1_01/lldp
            e2a    0013.c31e.5c60            GigabitEthernet1/36
            e2b    0013.c31e.5c60            GigabitEthernet1/35
            e2c    0013.c31e.5c60            GigabitEthernet1/34
            e2d    0013.c31e.5c60            GigabitEthernet1/33
```

LLDP通知の送信間隔の調整

LLDP通知は、一定の間隔でLLDP近隣機器に送信されます。ネットワーク トラフィックの量やネットワーク トポロジの変化に応じて、LLDP通知の送信間隔を調整することができます。

タスク概要

IEEEが推奨するデフォルトの送信間隔は30秒ですが、5～300秒の値を入力できます。

手順

1. クラスタ内の1つまたはすべてのノードについて、LLDP通知の現在の送信間隔を表示します。
   - 1つのノード：

     ```
     run -node <node_name> options lldp.xmit.interval
     ```

   - すべてのノード：

     ```
     options lldp.xmit.interval
     ```

2. クラスタ内の1つまたはすべてのノードで、すべてのポートのLLDP通知の送信間隔を調整します。
   - 1つのノード：

     ```
     run -node <node_name> options lldp.xmit.interval <interval>
     ```

   - すべてのノード：

     ```
     options lldp.xmit.interval <interval>
     ```

LLDP通知のTime-To-Live値の調整

Time-To-Live（TTL）とは、LLDP通知がLLDP対応の近隣デバイスのキャッシュに格納される時間です。TTLは各LLDPパケットで通知され、ノードがLLDPパケットを受信するたびに更新されます。発信LLDPフレームでTTLを変更できます。

タスク概要

- TTL は、送信間隔(`lldp.xmit.interval`とホールド乗数(`lldp.xmit.hold`の積に 1 を加えた計算値です。
- デフォルトの保持の乗数値は4ですが、1～100の値を入力できます。
- IEEEが推奨するデフォルトのTTLは121秒ですが、送信間隔と保持の乗数の値を調整することにより、発信フレームの値を6～30001秒に指定できます。
- TTLが期限切れになる前にIPアドレスが削除された場合、LLDP情報はTTLが期限切れになるまでキャッシュされます。

手順

1. クラスタ内の1つまたはすべてのノードの現在の保持の乗数値を表示します。
   - 1つのノード：

     ```
     run -node <node_name> options lldp.xmit.hold
     ```

   - すべてのノード：

     ```
     options lldp.xmit.hold
     ```

2. クラスタ内の1つまたはすべてのノードで、すべてのポートの保持の乗数値を調整します。
   - 1つのノード：

     ```
     run -node <node_name> options lldp.xmit.hold <hold_value>
     ```

   - すべてのノード：

     ```
     options lldp.xmit.hold <hold_value>
     ```

LLDP統計情報の表示と消去

ネットワーク接続で発生する可能性のある問題を見つけるために、各ノードのクラスタ ポートと非クラスタ ポートのLLDP統計情報を確認できます。LLDP統計情報は、前回消去されたときからの累積値です。

タスク概要

ONTAP 9.10.1以前の場合、クラスタ ポートではLLDPが常に有効になっているので、これらのポートのトラフィックに関するLLDP統計情報は常に表示されます。非クラスタ ポートのLLDP統計情報を表示するには、これらのポートでCDPを有効にする必要があります。

ONTAP 9.11.1以降の場合、クラスタ ポートとストレージ ポートではLLDPが常に有効になっているので、これらのポートのトラフィックに関するLLDP統計情報は常に表示されます。非クラスタ ポートと非ストレージ ポートのLLDP統計情報を表示するには、これらのポートでLLDPを有効にする必要があります。

手順

ノードのすべてのポートに関する現在のLLDP統計情報を表示、または消去します。

状況	入力する内容
LLDP統計情報を表示	`run -node node_name lldp stats`
LLDP統計情報を消去	`run -node node_name lldp stats -z`

統計情報の表示と消去の例

次のコマンドは、消去する前のLLDP統計情報の例を示します。前回統計情報が消去されてから、送信および受信したパケットの総数が出力されています。

```
cluster-1::> run -node vsim1 lldp stats

RECEIVE
 Total frames:     190k  | Accepted frames:   190k | Total drops:
0
TRANSMIT
 Total frames:     5195  | Total failures:      0
OTHER
 Stored entries:      64
```

次のコマンドは、LLDP統計情報を消去します。

```
cluster-1::> The following command clears the LLDP statistics:
run -node vsim1 lldp stats -z
run -node node1 lldp stats

RECEIVE
 Total frames:        0  | Accepted frames:     0  | Total drops:
0
TRANSMIT
 Total frames:        0  | Total failures:      0
OTHER
 Stored entries:      64
```

統計情報を消去すると、次にLLDP通知が送信または受信された時点から情報が累積されていきます。