ネットワーク管理
ONTAP 9

NetApp
December 20, 2024

目次

ネットワーク管理

開始する

ネットワーク管理の概要

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示す図を表示し、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、LIFとサブネットの関連付けをネットワークインターフェイスグリッドで表示できます。

この図は、**[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]*セクションでを選択すると表示され → ます。

次のカテゴリのコンポーネントを図に示します。

- 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、を参照してください"ネットワークの管理"。

例

次に、各コンポーネントの詳細を表示したり、ネットワークを管理するためのアクションを開始したりするために図を操作する方法の例をいくつか示します。

- ホストをクリックすると、その構成（ポート、ネットワークインターフェイス、 Storage VM 、関連する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、ボリュームを選択して詳細を表示します。
- 過去1週間のパフォーマンスを表示するiSCSIインターフェイスを選択してください。
- コンポーネントの横にあるをクリックし ⋮ て、そのコンポーネントを変更するアクションを開始します。
- 正常でないコンポーネントの横に「X」が表示され、ネットワークで問題が発生する可能性がある場所をすばやく特定します。

System Managerネットワークの可視化ビデオ

クラスタのネットワークコンポーネントの概要

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構成することで、ONTAPの柔軟性とマルチテナンシー機能を活かすことができます。

クラスタのさまざまなネットワークコンポーネントは次のとおりです。

- 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。

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

- 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別 々 の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に属するクライアントは、同じIPアドレスサブネット範囲の重複するIPアドレスを使用してクラスタデータにアクセスできます。

- 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

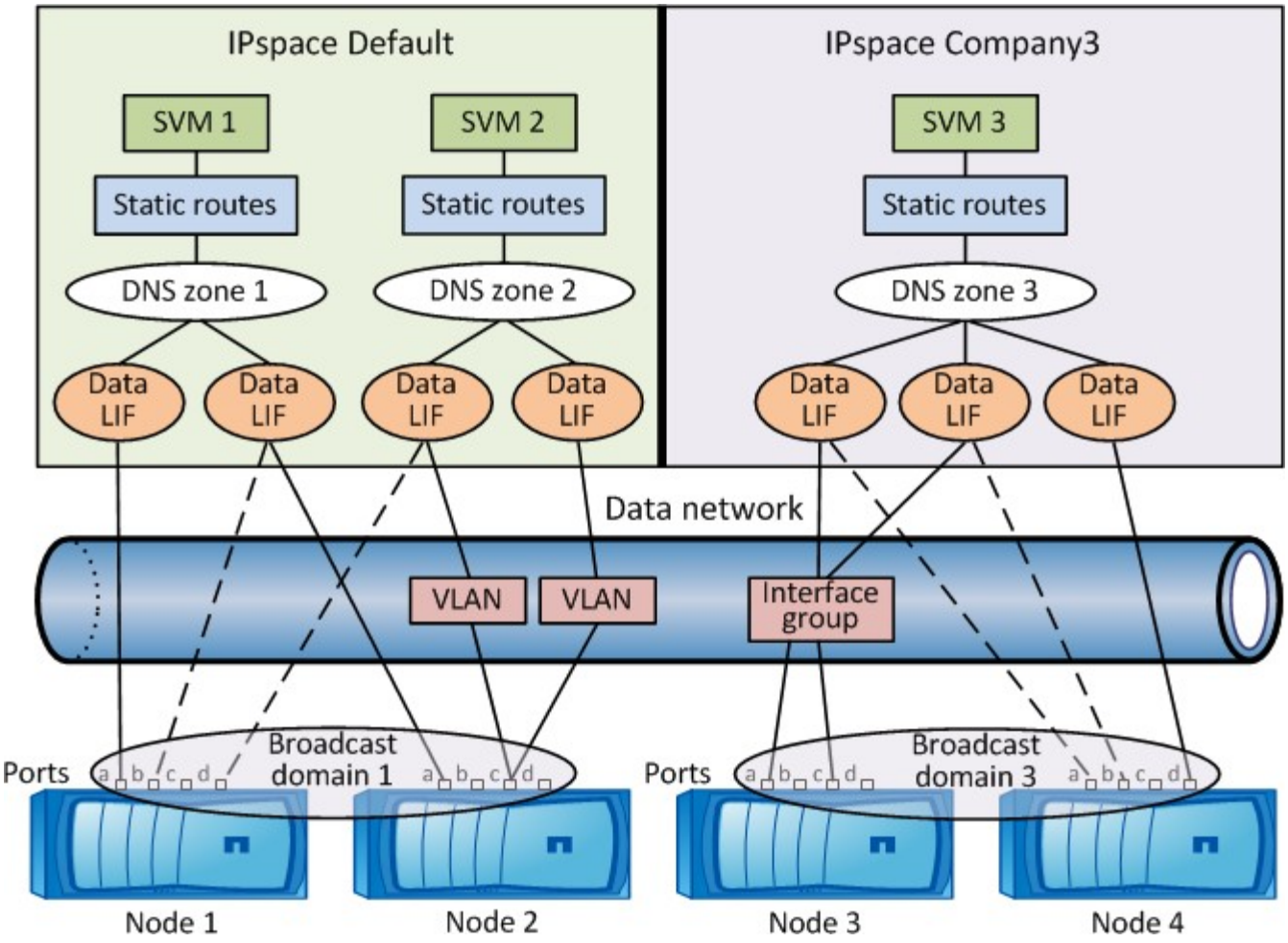
  DNSゾーンはLIFの作成時に指定でき、クラスタのDNSサーバ経由でエクスポートされるLIFの名前を提供します。複数のLIFで同じ名前を共有できるため、DNSロード バランシング機能を使用し、その名前のIPアドレスを負荷に従って分散させることができます。

  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。

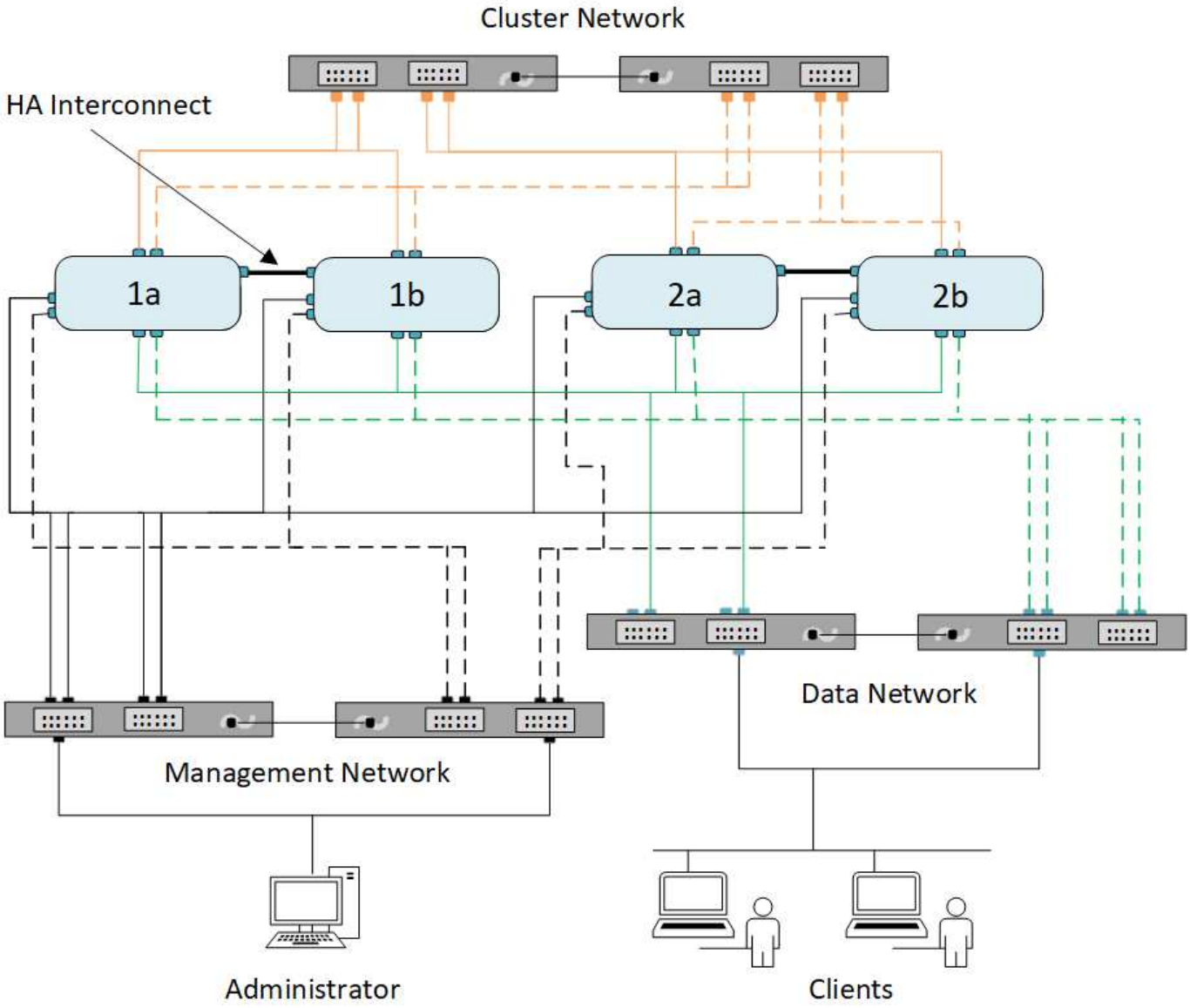


ネットワークノケーブルハイセンノガイドライン

ネットワークケーブル配線のベストプラクティスでは、トラフィックがクラスタ、管理、データのネットワークに分離されます。

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。



ネットワーク接続のケーブル配線を行う際は、次のガイドラインに従う必要があります。

- 各ノードを3つの異なるネットワークに接続する必要があります。

  1つは管理用、1つはデータアクセス用、もう1つはクラスタ内通信用です。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）のトラフィックフローを改善するために、各ノードに複数のデータネットワーク接続を確立できます。
- クラスタは、データネットワーク接続なしで作成できますが、クラスタインターコネクト接続が含まれている必要があります。
- 各ノードへのクラスタ接続は常に2つ以上にする必要があります。

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

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関係

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を組み合わせて、LIFが設定されているノードまたはポートで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を決定します。

ブロードキャストドメインは、同じレイヤ2イーサネットネットワーク内で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共通到達可能性はLIFにとって重要です。LIFがブロードキャストドメイン内の他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ためです。

フェイルオーバーグループは、相互にLIFフェイルオーバーのカバレッジを提供する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。ブロードキャストドメイン内のすべてのポートを含むこのフェイルオーバーグループが、LIFに対して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、定義するサブセットの数が少ないフェイルオーバーグループを作成できます。

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定義します。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して、フェイルオーバーポリシーが考えられます。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。

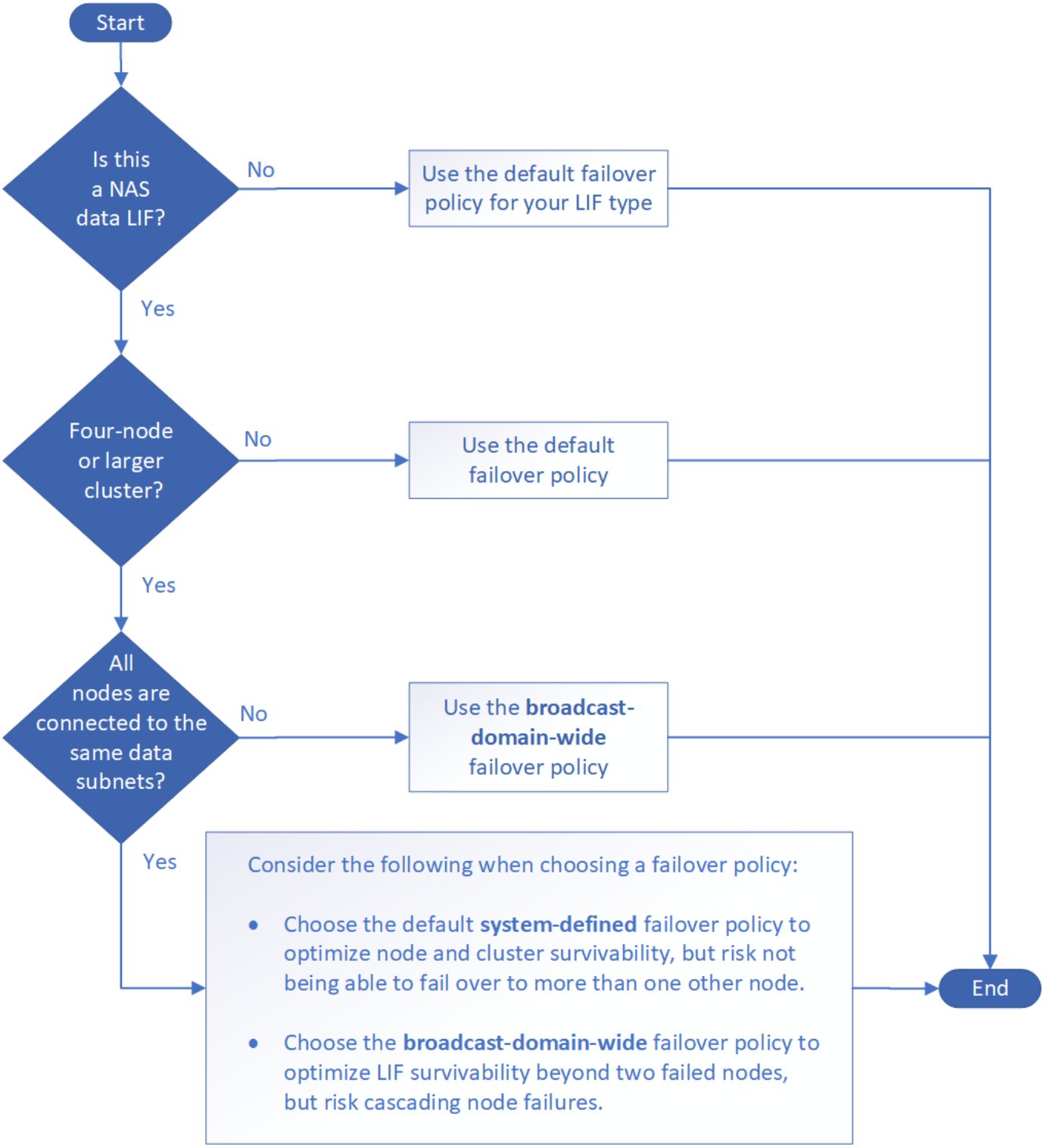
```
network interface show -failover
```

NetAppでは、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ています。

使用する**LIF**フェイルオーバーポリシーを決定する

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	説明
BGPのLIF	無効	別のポートにフェイルオーバーしない。
クラスタLIF	ローカルのみ	LIFは、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	ローカルのみ	LIFは、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	システム定義	HAパートナーではないもう一方のノードにフェイルオーバーします。
ノード管理LIF	ローカルのみ	LIFは、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ない。

「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パートナーのポートにのみフェイルオーバーする場合に使用できます。

NASパスのフェイルオーバーワークフロー（ONTAP 9 .8以降）

NASパスのフェイルオーバーについて（ONTAP 9.8以降）

このワークフローでは、ONTAP 9.8以降でNASパスのフェイルオーバーを設定するためのネットワーク設定手順を示します。このワークフローは次のことを前提としています。

- NASパスのフェイルオーバーに関するベストプラクティスを使用してネットワーク設定を簡易化したい。
- System ManagerではなくCLIを使用する必要がある。
- ONTAP 9.8以降が稼働している新しいシステムでネットワークを設定しようとしている。

9.8より前のリリースのONTAPを実行している場合は、ONTAP 9.0～9.7でのNASパスのフェイルオーバー手順を使用してください。

- "NASパスのフェイルオーバー ワークフロー（ONTAP 9.0～9.7での）"

ネットワーク管理の詳細については、ネットワーク管理に関する参考資料を参照してください。

- ネットワーク管理の概要

ワークフロー（ONTAP 9.8以降）

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。

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（リンク障害後に手動で移動しないかぎり）。代わりに、ホストのマルチパステクノロジ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、を参照してください "SAN管理"。

1 "ワークシートに記入する"

ワークシートを使用して、NASパスのフェイルオーバーを計画します。

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"**

ブロードキャストドメインをIPspaceに移動します。

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サーバを作成する前に、SVM用のDNSサービスを設定します。

NASパスのフェイルオーバー設定用ワークシート（ONTAP 9 .8以降）

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情報を入力する必要があります。

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に属するクライアントは、同じIPアドレスサブネット範囲の重複するIPアドレスを使用してクラスタデータにアクセスできます。

情報	必須	自分の価値観

IPspace 名 IPspace の一意の識別子。	○	

ブロードキャストドメインの設定

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、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。IPspaceには1つ以上のブロードキャストドメインを含めることができます。

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で作成したブロードキャストドメインごとに、ブロードキャストドメイン内のすべてのポートを含む同じ名前のフェイルオーバーグループも作成されます。

情報	必須	自分の価値観
IPspace 名：ブロードキャストドメインを割り当てる IPspace 。 既存のIPspaceを指定する必要があります。	○	
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を指定します。 この名前はIPspace内で一意である必要があります。	○	
MTUブロードキャストドメインの最大伝送ユニット値。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内のすべてのポートと、あとで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。	○	
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。ポート割り当てが完了したら、コマンドを実行して到達可能性を確認します `network port reachability show`。 これらのポートには、物理ポート、VLAN、インターフェイスグループがあります。	○	

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含まれ、IPspace内のSVMで使用されるLIFに割り当てることができます。

- SVMでLIFを作成するときは、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の名前を指定できます。
- 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の作成時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つ以上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に関連付けることで、異なる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内の他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	自分の価値観
IPspace 名：サブネットを割り当てる IPspace 。 既存のIPspaceを指定する必要があります。	○	
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。	○	
ブロードキャストドメイン名サブネットを割り当てるブロードキャストドメインです。 このブロードキャストドメインは指定したIPspaceに存在する必要があります。	○	
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を指定します。	○	
Gateway ：サブネットのデフォルトゲートウェイを指定できます。 サブネットの作成時にゲートウェイを割り当てなかった場合は、あとでゲートウェイを割り当てることができます。	いいえ	

IP アドレス範囲： 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 の関連付けを強制的に更新既存の LIF との関連付けを強制的に更新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またはネットワークインターフェイスが指定した範囲の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。

記録した値は、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、またはを参照してください"Fabric-attached MetroCluster Installation and Configuration Guide""ストレッチ MetroCluster インストールおよび設定ガイド"。

情報	必須	自分の価値観
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。	○	
ルートボリューム名 SVM ルートボリュームの名前。	○	
アグリゲート名は、 SVM ルートボリュームを保持するアグリゲートの名前です。既存のアグリゲートを指定する必要があります	○	
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 * 、および * mixed * です。	○	
IPspace 名： SVM を割り当てる IPspace 。既存のIPspaceを指定する必要があります。	いいえ	

SVM の言語： SVM とそのボリュームで使用されるデフォルトの言語。ボリュームの言語を指定しなかった場合は、 SVM のデフォルトの言語設定は * C.UTF-8 * になります。SVMの言語の設定によって、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が決まります。言語はSVMの作成後に変更できます。	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）を介し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	自分の価値観
SVM 名 LIF の SVM の名前。	○	
LIF の名前 LIF の名前。ノードに使用可能なデータポートがある場合は、ノードごとに複数のデータLIFを割り当てたり、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、データサブネットごとに少なくとも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。*重要：ノンストップオペレーションソリューション用に Hyper-V または SQL Server over SMB をホストする SMB サーバを設定する場合、クラスタ内の SVM のすべてのノードに少なくとも 1 つのデータ LIF が存在する必要があります。	○	
LIF のサービスポリシーサービスポリシー。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とサービスポリシーを使用できます。	○	
許可されたプロトコル IP ベースの LIF では、許可されたプロトコルは必要ありません。代わりにサービスポリシーの行を使用してください。FibreChannelポートでSAN LIFに許可するプロトコルを指定してください。これらは、そのLIFを使用できるプロトコルです。LIFを使用するプロトコルは、LIFの作成後は変更できません。LIFの設定時に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 がホームポートにリバートされるときに LIF が戻るノード。各データLIFのホームノードを記録する必要があります。	○	

ホームポートまたはブロードキャストドメインから次のいずれかを選択しました。 * Port * ：LIF がホームポートにリバートされるときに論理インターフェイスが戻るポートを指定します。この処理は、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要ありません。* 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します。LIF がホームポートにリバートされるときに論理インターフェイ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。	○	
SVM に割り当てるサブネットの名前を指定します。アプリケーションサーバへの継続的可用性を備えたSMB接続を確立するために使用されるデータLIFは、すべて同じサブネット上にある必要があります。	○（サブネットを使用する場合）	

DNS構成

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	自分の価値観
SVM 名： NFS または SMB サーバを作成する SVM の名前。	○	
DNS ドメイン名ホストと IP の名前解決を行う際に、ホスト名に付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。	○	

DNS サーバの IP アドレス NFS サーバまたは 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。これらのDNSサーバには、Active DirectoryのLDAPサーバとSMBサーバが参加するドメインの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クエリを介し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サーバの作成に失敗します。ONTAPがActive Directory SRVレコードを確実に見つけることができ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に統合されていないDNSサーバを使用できます。Active Directoryに統合されたSRVレコードの詳細については、のトピックを参照してください"Microsoft TechNet での Active Directory の DNS サポートのしくみ"。	○	

動的**DNS**設定

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

SVM上のすべてのデータ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を作成することで、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できます。DNSは、ホスト名を使用して確立された接続を、割り当てられたIPアドレスにラウンドロビン方式で負荷分散します。

情報	必須	自分の価値観
SVM 名： NFS または SMB サーバを作成する SVM 。	○	
DDNS を使用するかどうかで、 DDNS を使用するかどうかを指定します。SVMで設定されているDNSサーバが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。	○	

Secure DDNS を使用するかどうかは、 Active Directory 統合 DNS でのみサポートされます。Active Directory統合DNSでセキュアな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にする必要があります。デフォルトでは、Secure DDNSは無効になっています。Secure DDNSは、SVM用のSMBサーバまたはActive Directoryアカウントが作成されたあと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 です。SVMのDNSネームサービス用に設定されているドメイン名と同じ名前を使用する必要があります。	いいえ	

NASパスのフェイルオーバー ワークフロー（ONTAP 9.7以前）

NASパスのフェイルオーバーのセットアップ（ONTAP 9 .7以前）

このワークフローは、ONTAP 9 .0~9.7のNASパスフェイルオーバーをセットアップするためのネットワーク設定手順を示しています。このワークフローは次のことを前提としています。

- NASパスのフェイルオーバーに関するベストプラクティスを使用してネットワーク設定を簡易化したい。
- System ManagerではなくCLIを使用する必要がある。
- ONTAP 9 .0から9.7を実行する新しいシステムでネットワークを設定する。

9.7よりも新しいONTAPリリースを実行している場合は、ONTAP 9 .8以降でNASパスのフェイルオーバー手順を使用する必要があります。

- ONTAP 9 .8以降のNASパスのフェイルオーバーワークフロー

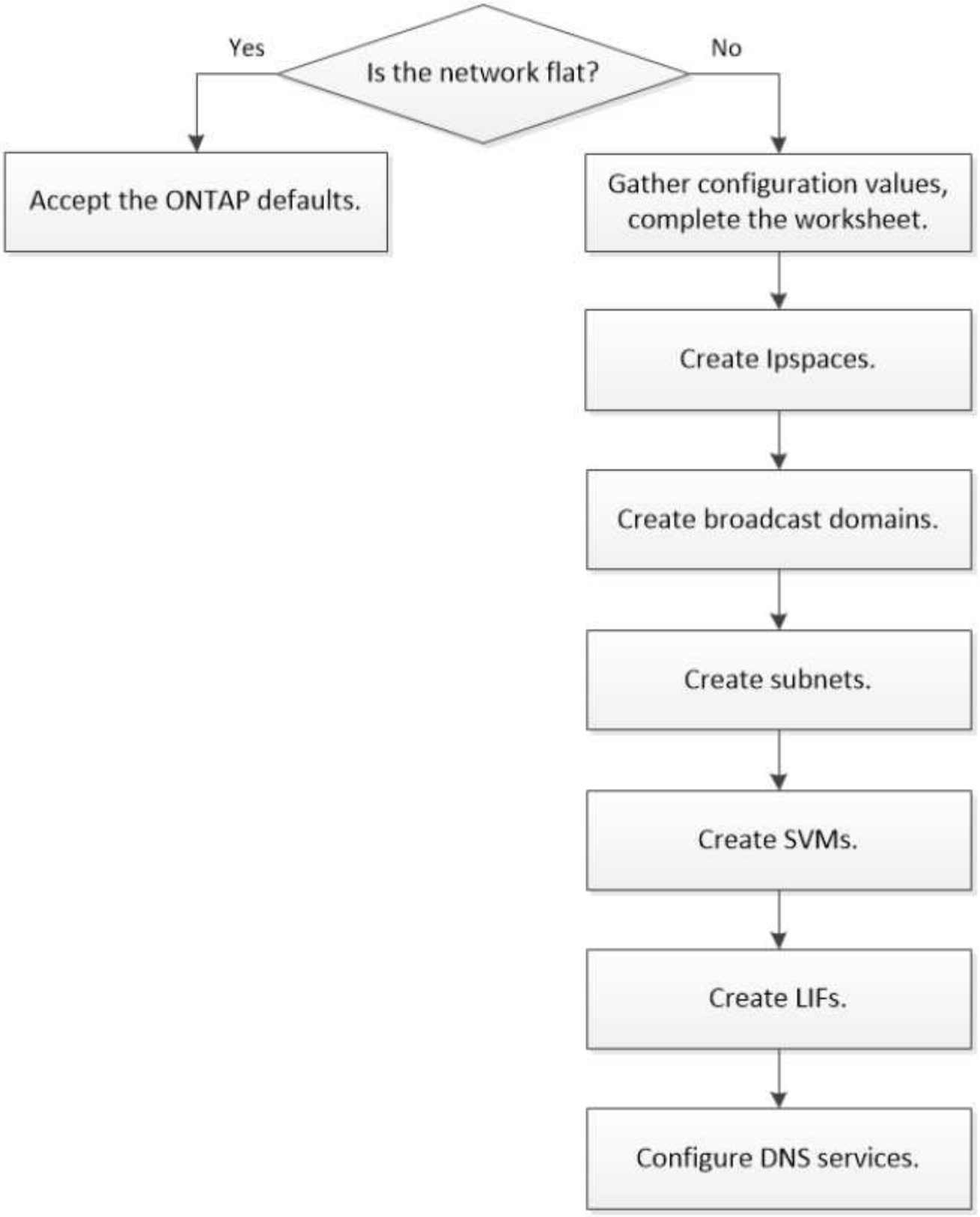
ネットワークコンポーネントと管理の詳細が必要な場合は、ネットワーク管理の参考資料を参照してください。

- ネットワーク管理の概要

ワークフロー（ONTAP 9.7以前）

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。

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。ネットワークがフラットな場合は、ONTAPのデフォルトを使用してパスのフェイルオーバーを管理できます。それ以外の場合は、このワークフローの手順に従ってパスのフェイルオーバーを設定する必要があります。



SAN LIFは移行されません（リンク障害後に手動で移動しないかぎり）。代わりに、ホストのマルチパステクノロジ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、を参照してください "SAN管理"。

1 "ワークシートに記入する"

ワークシートを使用して、NASパスのフェイルオーバーを計画します。

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 "ブロードキャストドメインの作成"

ブロードキャストドメインを作成する

4 "サブネットの作成"

サブネットを作成する。

5 "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。

6 "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。

7 "SVM用のDNSサービスの設定"

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

NASパスのフェイルオーバー設定用ワークシート（ONTAP 9 .7以前）

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情報を入力する必要があります。

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に属するクライアントは、同じIPアドレスサブネット範囲の重複するIPアドレスを使用してクラスタデータにアクセスできます。

情報	必須	自分の価値観

IPspaceメイ • IPspaceの名前。 • この名前はクラスタ内で一意である必要があります。	○	

ブロードキャストドメインの設定

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、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。IPspaceには1つ以上のブロードキャストドメインを含めることができます。

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。ブロードキャストドメインを作成すると、同じ名前のフェイルオーバーグループがONTAPによって自動的に作成されます。フェイルオーバーグループには、ブロードキャストドメインに割り当てられているすべてのポートが含まれます。

情報	必須	自分の価値観
IPspaceメイ • ブロードキャストドメインの割り当て先のIPspaceを指定します。 • 既存のIPspaceを指定する必要があります。	○	
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を指定します。 • この名前はIPspace内で一意である必要があります。	○	

MTU • ブロードキャストドメインのMTU。 • 一般的には* 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内のすべてのポートと、あとで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。	○	
ポート • ブロードキャストドメインに追加するネットワークポートを指定します。 • ブロードキャストドメインには、物理ポート、VLAN、インターフェイスグループ（ifgroup）を割り当てることができます。 • ポートが別のブロードキャストドメインにある場合は、そのドメインに追加する前に削除する必要があります。 • ポートは、ノード名とポートの両方を指定して割り当てます（例：node1：e0d）。	○	

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含まれ、IPspace内のSVMで使用されるLIFに割り当てることができます。

- SVMでLIFを作成するときは、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の名前を指定できます。
- 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の作成時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つ以上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に関連付けることで、異なる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内の他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	自分の価値観
IPspaceメイ • サブネットを割り当てるIPspace。 • 既存のIPspaceを指定する必要があります。	○	
サブネット名 • サブネットの名前を指定します。 • 名前はIPspace内で一意である必要があります。	○	
ブロードキャストドメイン名 • サブネットを割り当てるブロードキャストドメインを指定します。 • ブロードキャストドメインは指定したIPspaceに存在している必要があります。	○	
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。	○	

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。 • サブネットの作成時にゲートウェイを割り当てなかった場合は、いつでもゲートウェイを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 との関連付けを強制的に更新します • 既存のLIFの関連付けを強制的に更新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またはネットワークインターフェイスが指定した範囲の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。

記録した値は、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、またはを参照してください"ファブリック接続 MetroCluster をインストール""ストレッチMetroCluster を

インストールします"。

情報	必須	自分の価値観
SVM名 • SVMの名前。 • SVM名がクラスタ リーグ全体で一意になるように、完全修飾ドメイン名（FQDN）を使用します。	○	
ルートボリューム名 • SVMルートボリュームの名前。	○	
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。 • 既存のアグリゲートを指定する必要があります	○	
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 * 、および * mixed * です。	○	
IPspaceメイ • SVM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。	いいえ	

SVMの言語設定 • SVMとそのボリュームで使用されるデフォルトの言語。 • ボリュームの言語を指定しなかった場合は、 SVM のデフォルトの言語設定は * C.UTF-8 * になります。 • SVMの言語の設定によって、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が決まります。言語はSVMの作成後に変更できます。	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）を介し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	自分の価値観
SVM名 • LIFのSVMの名前。	○	

LIF名 • LIFの名前。 • ノードに利用可能なデータ ポートがある場合は、ノードごとに複数のデータLIFを割り当てたり、クラスタ内の任意のノードにLIFを割り当てたりすることができます。 • 冗長性を確保するには、データ サブネットごとに2つ以上のデータLIFを作成する必要があり、特定のサブネットに割り当てられたLIFには、異なるノード上のホーム ポートを割り当てる必要があります。* 重要：ノンストップオペレーションソリューション用に Hyper-V または SQL Server over SMB をホストする SMB サーバを設定する場合、クラスタ内の SVM のすべてのノードに少なくとも 1 つのデータ LIF が存在する必要があります。	○	
LIFのロール • LIFのロール。 • データLIFにはデータロールが割り当てられます。	はい、 ONTAP 9.6 から廃止されました	データ
LIF のサービスポリシーサービスポリシー。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とサービスポリシーを使用できます。	はい、 ONTAP 9.6 以降でサポートされています	

キョカスルプロトコル • LIFを使用できるプロトコル。 • デフォルトでは、SMB、NFS、およびFlexCacheが許可されています。FlexCacheプロトコルを使用するボリュームは、Data ONTAP 7-Modeを実行しているシステムのFlexCacheボリュームの元のボリュームにすることができます。 LIFを使用するプロトコルは、LIFが作成されたあとは変更できません。LIFの設定時に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がホームポートにリバートされるときにLIFが戻るノード。 • 各データLIFのホームノードを記録する必要があります。	○	
ホームポートまたはブロードキャストドメイン • LIFがホームポートにリバートされるときに論理インターフェイスが戻るポート。 • 各データLIFのホームポートを記録する必要があります。	○	
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可用性を備えたSMB接続を確立するために使用されるデータLIFは、すべて同じサブネット上にある必要があります。	○（サブネットを使用する場合）	

DNS構成

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	自分の価値観
SVM名 • NFSサーバまたはSMBサーバを作成するSVMの名前。	○	
DNSトメインメイ • ホストとIPの名前解決を実行するときにホスト名に付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。	○	

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。 • これらのDNSサーバには、Active DirectoryのLDAPサーバと、SMBサーバが参加するドメインのドメイン 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プするために使用されます。ローカルのDNSクエリを介してサービス ロケーション レコードを取得できない場合は、SMBサーバの作成に失敗します。ONTAPがActive Directory SRVレコードを確実に見つけることができるようにする最も簡単な方法は、Active Directory統合DNSサーバをSVMのDNSサーバとして構成することです。DNS管理者が手動で、Active Directoryドメイン コントローラに関する情報を含んだDNSゾーンにSRVのレコードを追加した場合は、Active Directoryを統合していないDNSサーバを使用することができます。 • Active Directoryに統合されたSRVレコードの詳細については、のトピックを参照してください"Microsoft TechNet での Active Directory の DNS サポートのしくみ"。	○	

動的**DNS**設定

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

SVM上のすべてのデータ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を作成することで、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できます。DNSは、ホスト名を使用して確立された接続を、割り当てられたIPアドレスにラウンドロビン方式で負荷分散します。

情報	必須	自分の価値観
SVM名 • NFSサーバまたはSMBサーバを作成するSVM。	○	
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で設定されているDNSサーバが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。	○	
セキュアなDDNSを使用するかどうか • Secure DDNSは、Active Directory統合DNSでのみサポートされます。 • Active Directory統合DNSでセキュアな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にする必要があります。 • デフォルトでは、Secure DDNSは無効になっています。 • Secure DDNSは、SVM用のSMBサーバまたはActive Directoryアカウントが作成されたあと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ネームサービス用に設定されているドメイン名と同じ名前を使用する必要があります。	いいえ	

ネットワークポート

ネットワークポート設定の概要

ポートは、物理ポート（NIC）または仮想ポート（インターフェイスグループやVLANなど）です。

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別々 の論理ポートに分割します。

- 物理ポート： LIF は物理ポートに直接設定できます。
- インターフェイスグループ：複数の物理ポートを含むポートアグリゲートで、 1 つのトランクポートとして機能します。インターフェイスグループには、シングルモード、マルチモード、または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です。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イスグループポートはVLANトランクポートとみなされ、接続するスイッチポートはVLAN IDをトランクするように設定する必要があります。

  VLANポートの基盤と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、タグなしトラフィックを送受信するLIFを引き続きホストできます。

- 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、サポートされる処理は限られています。VIPポートはONTAP 9以降でサポートされています。5.

ポートの命名規則は *enumberletter* ：

- 最初の文字はポートタイプを表します。「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、マルチポートアダプタでのポートの位置を示します。「a」は最初のポートを示し、「b」は2番目のポートを示します。以下同様に続きます。

たとえば、 `e0b`は、イーサネットポートであり、ノードのマザーボード上にある2番目のポートです。

VLANの名前には、という構文を使用する必要があり `port_name-vlan-id`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示します。

`vlan-id`ネットワーク上のVLAN ID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インターフェイスグループを作成

インターフェイスグループはLink Aggregation Group（LAG；リンクアグリゲーショングループ）とも呼ばれ、同じノード上の複数の物理ポートを1つの論理ポートにまとめることで作成されます。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。

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。

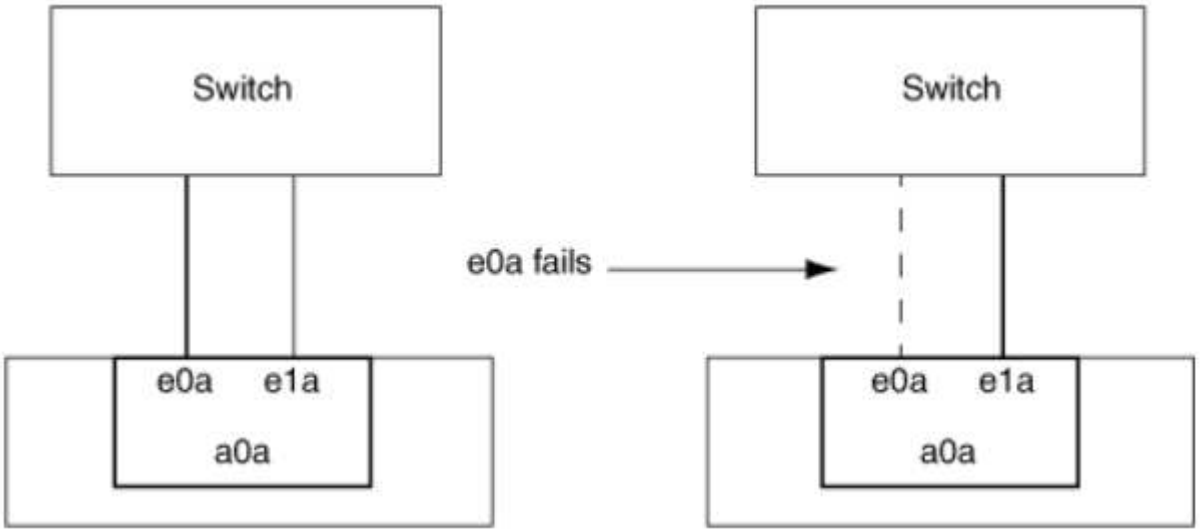
シングルモード インターフェイス グループの特性

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ことを推奨します。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はありません。さらに、フェイルオーバーグループは3つ以上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

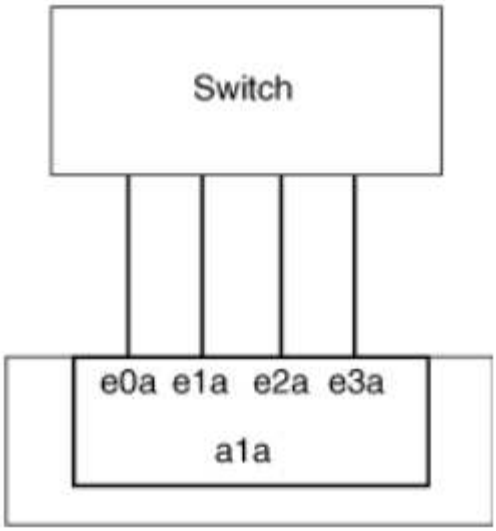
ONTAPに実装されているスタティックマルチモードインターフェイスグループは、IEEE 802.3ad（static）に準拠しています。スタティックマルチモードインターフェイスグループでは、アグリゲートをサポートしているが、アグリゲートを設定するための制御パケット交換が行われていないスイッチを使用できます。

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、Cisco独自のリンクアグリゲーションプロトコルであるポートアグリゲーションプロトコル（PAgP）に相当します。

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、1つの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は、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と、すべてのセッションがパケット単位で使用可能なリンクに分散され、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、最大で「n-1」個のインターフェイスの障害から回復できます。nは、インターフェイスグループを構成するインターフェイスの総数です。
- ポートに障害が発生した場合、またはポートが接続されていない場合、障害が発生したリンクを通過していたトラフィックは、残りのインターフェイスの1つに自動的に再配布されます。
- 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喪失や、接続とパフォーマンスに影響する可能性の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。スイッチは、インターフェイスグループの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に設定されています。一部のスイッチでは、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がサポートされ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トラフィックを分散するために、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です。インターフェイスe0a、e1a、e2a、およびe3aは、a1aマルチモードインターフェイスグループの一部です。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。



単一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できるようにするテクノロジーがいくつか存在します。この機能を有効にするために使用されるテクノロジは、ネットワーク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。特定のマルチスイッチリンクアグリゲーションテクノロジがIEEE 802.3規格と相互運用または準拠していると言われている場合は、ONTAPと連携して動作する必要があります。

IEEE 802.3規格では、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と規定されています。したがって、ONTAPは発信トラフィックの配信のみを担当し、着信フレームの着信方法を制御することはできません。集約リンク上の着信トラフィックの送信を管理または制御する場合は、直接接続されたネットワークデバイスでその送信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にグループメンバーシップを通信します。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（802.1 AX）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ポートアグリゲーションプロトコル（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は設定不可のアクティブモードでLACPを実装します。これは、アクティブモードまたはパッシブモードに設定されたスイッチと連動します。ONTAPは、IEEE 802.3 AD（802.1AX）で規定されているように、longおよびshortのLACPタイマーを実装します（3秒および90秒の設定不可の値で使用します）。

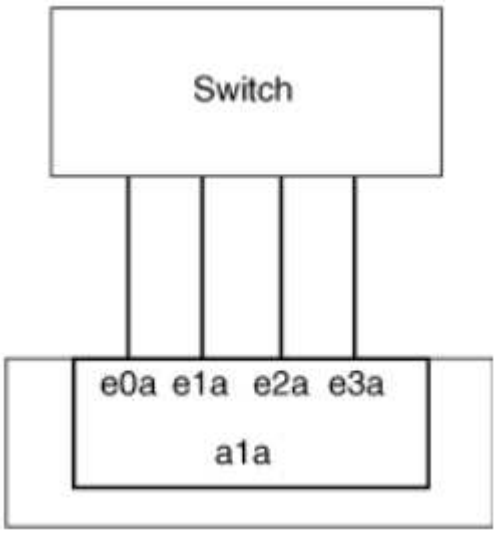
ONTAPロードバランシングアルゴリズムは、発信トラフィックの送信に使用されるメンバーポートを決定しますが、着信フレームの受信方法は制御しません。スイッチは、スイッチのポートチャネルグループに設定されたロードバランシングアルゴリズムに基づいて、送信に使用されるポートチャネルグループのメンバー（個々 の物理ポート）を決定します。したがって、スイッチの設定によって、トラフィックを受信するストレージシステムのメンバーポート（個 々 の物理ポート）が決まります。スイッチの設定の詳細については、スイッチベンダーのマニュアルを参照してください。

あるインターフェイスが連続する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は「ifgrp status」コマンドの出力で「lag_inactive」と表示されます。既存のトラフィックは、残りのアクティブ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は、次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、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アドレスベース、MACアドレスベース、シーケンシャルベース、または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ネットワークポート上で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利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は、インターフェイスグループの作成時にのみ指定できます。

- ベストプラクティス * ：可能なかぎりポートベースのロードバランシングを推奨します。ポートベースのロードバランシングは、ネットワークに特定の理由または制限がないかぎり使用してください。

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が推奨されます。

ポートベースのロードバランシング方式を使用すると、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 / UDP）ポートに基づいて均等に分散できます。

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、ソースとデスティネーションの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分散する方法です。

これらのロードバランシング方式では、送信元アドレスと宛先アドレス（IPアドレスとMACアドレス）に対して高速ハッシュアルゴリズムが使用されます。ハッシュアルゴリズムの結果がupリンクステートにないインターフェイスにマッピングされる場合、次のアクティブインターフェイスが使用されます。

> ルータに直接接続す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。このような設定では、すべての発信IPフレームの宛先MACアドレスがルータのMACアドレスになります。そのため、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使用されます。

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じように機能します。

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を使用すると、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。シーケンシャルオプションを使用すると、単一の接続のトラフィックを複数のリンクに分散して、単一の接続のスループットを向上させることができます。

ただし、シーケンシャルロードバランシングはパケット配信の順序が乱れてしまう可能性があるため、パフォーマンスが極端に低下する可能性があります。したがって、シーケンシャルロードバランシングは一般に推奨されません。

インターフェイスグループまたはLAGの作成

インターフェイスグループまたはLAG（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））を作成すると、集約されたネットワークポートの機能を組み合わせて単一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。

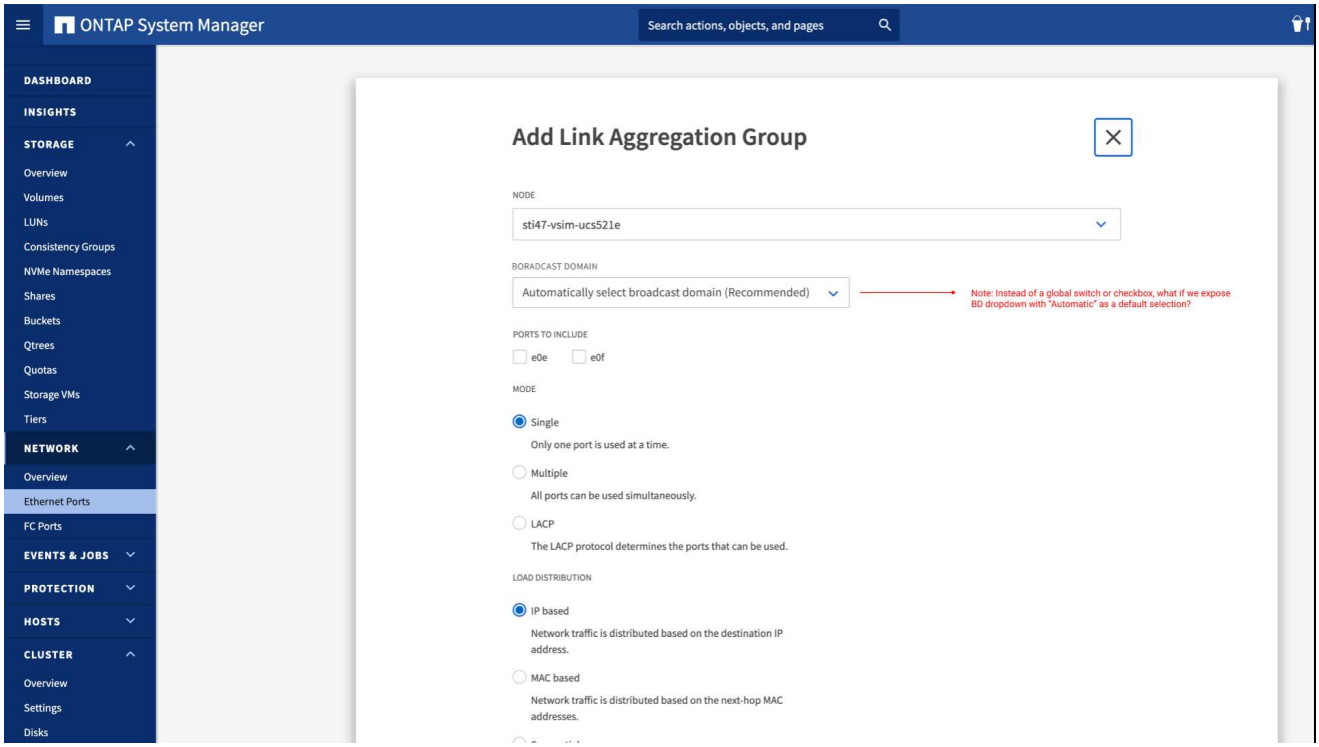
実行する手順は、使用するインターフェイス（System ManagerまたはCLI）によって異なります。

System Manager

- System Managerを使用してLAGを作成します。*

手順

1. [*Network]>[Ethernet port]>[+ Link Aggregation Group]を選択して、LAGを作成します。
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 to * automatically select broadcast domain（推奨）*。
   b. ブロードキャストドメインを手動で選択するには、をクリックします。
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. Single：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プロトコルによって、使用できるポートが決まります。
6. ロードバランシングを選択します。
   a. IPベース
   b. MACベース
   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イスグループを作成*

ポートインターフェイスグループに適用される設定上の制限事項の一覧については、のマニュアルページを参照して `network port ifgrp add-port`ください。

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、トランスポートレイヤ（TCP / UDP）ポートに基づいて分散されます。これが推奨されるロードバランシング方式です。
- `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したとおりに分散されます。

> インターフェイスグループのMACアドレスは、基盤となるポートの順序、およびこれらのポートがブート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更されることはありません。

ステップ

コマンドを使用し `network port ifgrp create`て、インターフェイスグループを作成します。

インターフェイスグループの名前には、という構文を使用する必要があります `a<number><letter>`。たとえば、a0a、a0b、a1c、a2aは有効なインターフェイスグループ名です。

このコマンドの詳細については、を参照して "ONTAPコマンド リファレンス"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または**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または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、使用するインターフェイス（System ManagerまたはCLI）によって異なります。

System Manager

- System Managerを使用して、LAGにポートを追加します。*

手順

1. [*Network]>[Ethernet port]>[LAG]を選択して、LAGを編集します。
2. LAGに追加する同じノードの追加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します。*

ステップ

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
```

このコマンドの詳細については、を参照して "ONTAPコマンド リファレンス"ください。

次の例は、a0aという名前の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イスグループに追加されてから約1分後に、適切なブロードキャストドメインにインターフェイスグループが自動的に配置されます。ONTAPでこの処理を行わず、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、パラメータをコマンドの一部として `ifgrp add-port`指定します `-skip-broadcast-domain-placement`。

インターフェイスグループまたは**LAG**からポートを削除する

LIFをホストするインターフェイスグループからは、その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かぎり、ポートを削除できます。最後のポートがインターフェイスグループから削除されないことを考慮して、インターフェイスグループがLIFをホストしていない、またはインターフェイスグループがLIFのホームポートで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を移行または移動する必要があります。

タスクの内容

インターフェイスグループまたはLAGから最大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、使用するインターフェイス（System ManagerまたはCLI）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. [*Network]>[Ethernet port]>[LAG]を選択して、LAGを編集します。
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します。*

ステップ

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
```

次の例は、a0aという名前の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または**LAG**を削除する

基盤となる物理ポートに直接LIFを設定する場合や、インターフェイスグループや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やLAGを削除できます。

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またはLAGは使用できません。
- インターフェイスグループまたはLAGをLIFのホームポートまたはフェイルオーバーターゲットにすることはできません。

実行する手順は、使用するインターフェイス（System ManagerまたはCLI）によって異なります。

System Manager

- LAGを削除するには、System Managerを使用します。*

手順

1. [*Network]>[Ethernet port]>[LAG]を選択して、LAGを削除します。
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イスグループ*を削除してください

ステップ

インターフェイスグループを削除するには、コマンドを使用し `network port ifgrp delete`ます。

このコマンドの詳細については、を参照して "ONTAPコマンド リファレンス"ください。

次の例は、a0bという名前のインターフェイスグループを削除する方法を示しています。

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

物理ポート経由の**VLAN**の設定

ONTAPでVLANを使用すると、分離されたブロードキャストドメインを作成してネットワークを論理的にセグメント化できます。ブロードキャストドメインは、物理的な境界に定義された従来のブロードキャストドメインとは異なり、スイッチポート単位で定義されます。

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。VLANに属するエンドステーションは、機能またはアプリケーションによって関連付けられます。

たとえば、VLAN内のエンドステーションは、エンジニアリングや経理などの部門ごと、またはリリース1やリリース2などのプロジェクトごとにグループ化できます。VLANではエンドステーションが物理的に近接していることは重要ではないため、エンドステーションを地理的に分散させても、スイッチド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 .13.1および9.14.1では、任意の論理インターフェイス（LIF）で使用されておらず、接続されているスイッチでネイティブ接続が確立されていないタグなしポートは、デグレードとマークされます。これは使用されていないポートを特定するためのもので、停止を示すものではありません。ネイティブVLANでは、ONTAP CFMブロードキャストなどのタグなしトラフィックをifgrpベースポートで許可します。タグなしトラフィックをブロックしないように、スイッチにネイティブVLANを設定します。

VLANの管理では、VLANに関する情報を作成、削除、または表示できます。

> 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上にある場合、そのインターフェイスにVLAN e0b-10を作成しないでください。

VLANを作成します。

同じネットワークドメイン内の分離されたブロードキャストドメインを管理するためのVLANを作成するには、System Managerまたはコマンドを使用し `network port vlan create`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。

タスクの内容

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

ポート上でVLANを初めて設定すると、ポートがダウンし、ネットワーク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を追加しても、ポートの状態には影響しません。

> 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上にある場合、そのインターフェイスにVLAN e0b-10を作成しないでください。

実行する手順は、使用するインターフェイス（System ManagerまたはCLI）によって異なります。

System Manager

- System Managerを使用してVLANを作成します。*

ONTAP 9 .12.0以降では、ブロードキャストドメインを自動的に選択することも、リストから手動で[オン]を選択することもできます。これまでは、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的に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、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ことを示す警告が表示されます。

手順

1. Network > Ethernet port >+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 to * automatically select broadcast domain（推奨）*。
   b. をクリックして、リストからブロードキャストドメインを手動で選択します。
4. VLANを形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を作成してください*

特定の状況において、ハードウェアの問題やソフトウェアの設定ミスを修正せずにデグレード状態のポートにVLANポートを作成する場合は、コマンドのパラメータ `network port modify`をに `true` 設定できます `-ignore-health-status`。

手順

1. コマンドを使用し `network port vlan create`てVLANを作成します。
2. VLANを作成するときは、または `port`オプションと `vlan-id`オプションのいずれかを指定する必要があります `vlan-name`。VLAN名は、ポート（またはインターフェイスグループ）の名前とネットワークスイッチのVLAN IDをハイフンでつないだものです。たとえば `e0c-24`、と `e1c-80`は有効なVLAN名です。

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

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

vlan.8以降では、ONTAP 9が作成されてから約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。この処理をONTAPで行わず、VLANをブロードキャストドメインに手動で配置する場合は、コマンドでパラメータを `vlan create`指定します `-skip-broadcast-domain-placement`。

このコマンドの詳細については、を参照して "ONTAPコマンド リファレンス"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を使用してVLANを編集する

ONTAP 9 .12.0以降では、ブロードキャストドメインを自動的に選択することも、リストから手動で[オン]を選択することもできます。これまでの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的に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、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ことを示す警告が表示されます。

手順

1. Network > Ethernet port > 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。

タスクの内容

ポートから最後のVLANを削除すると、そのポートからネットワーク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、使用するインターフェイス（System ManagerまたはCLI）によって異なります。

System Manager

- VLANを削除するには、System Managerを使用します。*

手順

1. Network > Ethernet port > VLAN *を選択します。
2. 削除するVLANを選択します。
3. [削除（ Delete ）] をクリックします。

CLI

- CLIを使用してVLAN *を削除します

ステップ

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

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

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

ネットワークポートの属性を変更します。

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。

タスクの内容

- 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を変更することは推奨されません。

  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る二重モードと速度）と異なる場合があります。

- 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を変更することは推奨されません。

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

- ノードのすべてのポート、またはノードで動作している最後のクラスタLIFをホストしているポートの管理設定をfalseに設定することは推奨されませ `-up-admin`ん。
- 管理ポートのMTUサイズを変更することは推奨されません `e0M`。
- ブロードキャストドメイン内のポートのMTUサイズは、ブロードキャストドメインに設定されているMTU値から変更することはできません。
- VLANのMTUサイズは、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. フィールドをtrueに設定する `-ignore-health-status`と、指定し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ようになります。

   ネットワークポートのヘルスステータスは「デグレード」から「正常」に自動的に変更され、このポートを使用してLIFをホストできるようになります。クラスタポートのフロー制御はに設定する必要があります `none`。デフォルトでは、フロー制御はに設定されて `full`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
```

10GbE接続用に**40GbE NIC**ポートを複数の**10GbE**ポートに変換

X1144A-R6およびX91440A-R6の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つの10GbEポートをサポートすることができます。

どちらかの NIC 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 を変換して必要な 10GbE 接続を提供する必要があります。

開始する前に

サポートされているブレークアウトケーブルを使用する必要があります。

タスクの内容

NICをサポートするプラットフォームの一覧については、を参照してください "Hardware Universe"。

X1144A-R6 NIC では、 4 つの 10GbE 接続をサポートするために変換できるのはポート A だけです。ポート A が変換されると、ポート e は使用できなくなります。

手順

1. メンテナンスモードに切り替えます。
2. NIC を 40GbE のサポートから 10GbE のサポートに変換します。

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

3. convertコマンドの使用が完了したら、ノードを停止します。
4. ケーブルを取り付けるか、交換します。
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システム用のUTA X1143A-R6ポートの設定

X1143A-R6ユニファイドターゲットアダプタのポートは、デフォルトではFCターゲットモードで構成されますが、10GbイーサネットポートおよびFCoEポート（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構成することができます。これには、 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10-GBEポート上でNICおよびFCoE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ターゲットモードまたはFCイニシエータモード用に個別に設定できます。つまり、1つのX1143A-R6アダプタで、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に接続されたポートペアは、同じモードで設定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デバイスと同様に動作し、最大速度は16Gbpsです。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できます。CNAモードでは、FCoE機能でFCターゲットモードのみがサポートされます。

ユニファイド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 個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. ポート設定を表示します。

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

2. 必要に応じて、Fibre Channel（FC；ファイバチャネル）またはConverged Network Adapter（CNA；統合ネットワークアダプタ）に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 10Gb イーサネットに適したケーブルを接続します。
4. 適切な SFP+ が取り付けら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イーサネット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 を使用します。

ONTAPでのUTA2ポートの変換

UTA2ポートは、Converged Network Adapter（CNA；統合ネットワークアダプタ）モードからFibre Channel（FC；ファイバチャネル）モードに、またはその逆に変換できます。

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イニシエータとターゲットをサポートする場合は、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モトカラ**FC**モトへ

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. 状況に応じて、管理者にポートの削除を依頼するか、 VIF マネージャでポートを削除します。
   - 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は、管理者は次の作業を行う必要があります。
     - LIF を移動するか、 ifgrp からポートを削除する、または VLAN をそれぞれ削除します。
     - コマンドを実行して、ポートを手動で削除し `network port delete`ます。コマンドが失敗した場合は `network port delete`、エラーに対処してからもう一度コマンドを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いない場合、 ifgrp のメンバーでない場合、および VLAN をホストしていない場合は、リブート時に VIF マネージャのレコードからポートが削除されます。VIFマネージャでポートが削除されない場合は、管理者がリブート後にコマンドを使用して手動で削除する必要があります `network port delete`。
5. 適切な SFP+ が取り付けら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イーサネットSFPを使用する必要があります。FC の場合は、ノードで構成を変更する前に、 8Gb SFP または 16Gb SFP を使用します。

FCモオトカラ**CNA**モオトへ

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+が取り付けら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。

ONTAPシステム用の**CNA / UTA2**光モジュールの変換

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ように、ユニファイドターゲットアダプタ（CNA / UTA2）の光モジュールを変更する必要があります。

手順

1. カードで使用されている現在の SFP+ を確認します。次に、現在の SFP+ を、優先して使用するパーソナリティ（ FC または CNA ）に適した SFP+ に差し替えます。
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. 使用するパーソナリティモード（FCまたはCNA）光ファイバに適したモジュールを挿入します。
4. 適切な SFP+ が取り付けられていることを確認します。

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

   サポートされるSFP+モジュールおよびCiscoブランドの銅線（Twinax）ケーブルについては、を参照し"NetApp Hardware Universe"てください。

ノードからの**NIC**の取り外し（**ONTAP 9.8**以降）

このトピックはONTAP 9.8以降が対象です。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。

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
```

ポートはすべてのインターフェイス グループから自動的に削除されます。ポートがインターフェイス グループの唯一のメンバーであった場合、そのインターフェイス グループは削除されます。

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`の各コマンドは一意であり、で始まる完全修飾コマンド名は必要ありません `cluster controller-replacement network`。

6. これらのVLANは削除されますが、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が設定されている場合は、同じブロードキャストドメイン内の別のポートの新しいホームポートがONTAPによって自動的に選択されます。同じFilerに適切なホーム・ポートが見つからない場合、それらのLIFは削除されたとみなされます。削除された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を追加すると、LIFのホームポートは自動的にリストアされます。または、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 `network interface modify -home-port -home-node or use the displaced- interface restore`。

ノードからの**NIC**の取り外し（**ONTAP 9.7**以前）

このトピックはONTAP 9.7以前が対象です。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。

開始する前に

- NICポートでホストされているすべてのLIFを移行または削除しておく必要があります。
- NICポートがLIFのホームポートになっているポートはありません。
- NICからポートを削除するには、高度なPrivilegesが必要です。

手順

1. NICからポートを削除します。

   ```
   network port delete
   ```

2. ポートが削除されたことを確認します。

   ```
   network port show
   ```

3. network port showコマンドの出力に削除したポートが表示される場合は、手順1を繰り返します。

ネットワークポートの監視

ネットワークポートの健全性の監視

ネットワークポートの ONTAP 管理では、健常性の自動監視機能と一連のヘルスモニタを使用して、 LIF のホストに適さない可能性のあるネットワークポートを特定できます。

タスクの内容

ヘルスモニタで健全でないと判断されたネットワークポートは、 EMS メッセージで管理者に警告が送信されるか、またはデグレードとマークされます。ONTAPは、デグレード状態のネットワークポートで別の正常なフェイルオーバーターゲットがある場合、そのLIFでのLIFのホストを回避します。ポートは、リンクフラッピング（リンクがアップとダウンを高速で繰り返す状態）やネットワークパーティショニングなどの軽度な障害イベントが原因でデグレード状態になります。

- 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。
- クラスタ以外の 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にデグレードとマークされます。

デグレード状態のポートの以下の動作に注意してください。

- デグレード状態のポートを VLAN または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、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正常な状態のポートに自動的に移行されます。
- フェイルオーバー時には、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。正常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 LIF を作成、移行、リバートすることはできません。

  ネットワークポートの設定はに `true`変更できます `ignore-health-status`。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で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 でデフォルトで有効になっていて使用可能なヘルスモニタは次のとおりです。

- リンクフラッピングヘルスモニタ：リンクフラッピングを監視します

  5 分以内に複数回のリンクフラッピングが発生しているポートは、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：同じブロードキャストドメインに設定されたすべてのポートで相互のポートに対するレイヤ 2 到達可能性が確保されてい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 におけるレイヤ 2 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：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。

3. コマンドを使用して、IPspaceのヘルスモニタを必要に応じて有効または無効にします `network options port-health-monitor modify`。
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、設定、およびポートがデグレードとマークされた理由のリストが表示され `ignore health status`ます。

ポートのヘルスステータスは `healthy`、または `degraded`です。

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

設定がの `false`場合、 `ignore health status`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判断されます。

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）

到達可能性の監視は、ONTAP 9 .8以降に組み込まれています。この監視機能を使用して、物理ネットワークトポロジがONTAPの設定と一致しない場合を特定します。場合に

よっては、ONTAPによってポートの到達可能性が修復されることがあります。それ以外の場合は、追加の手順が必要です。

タスクの内容

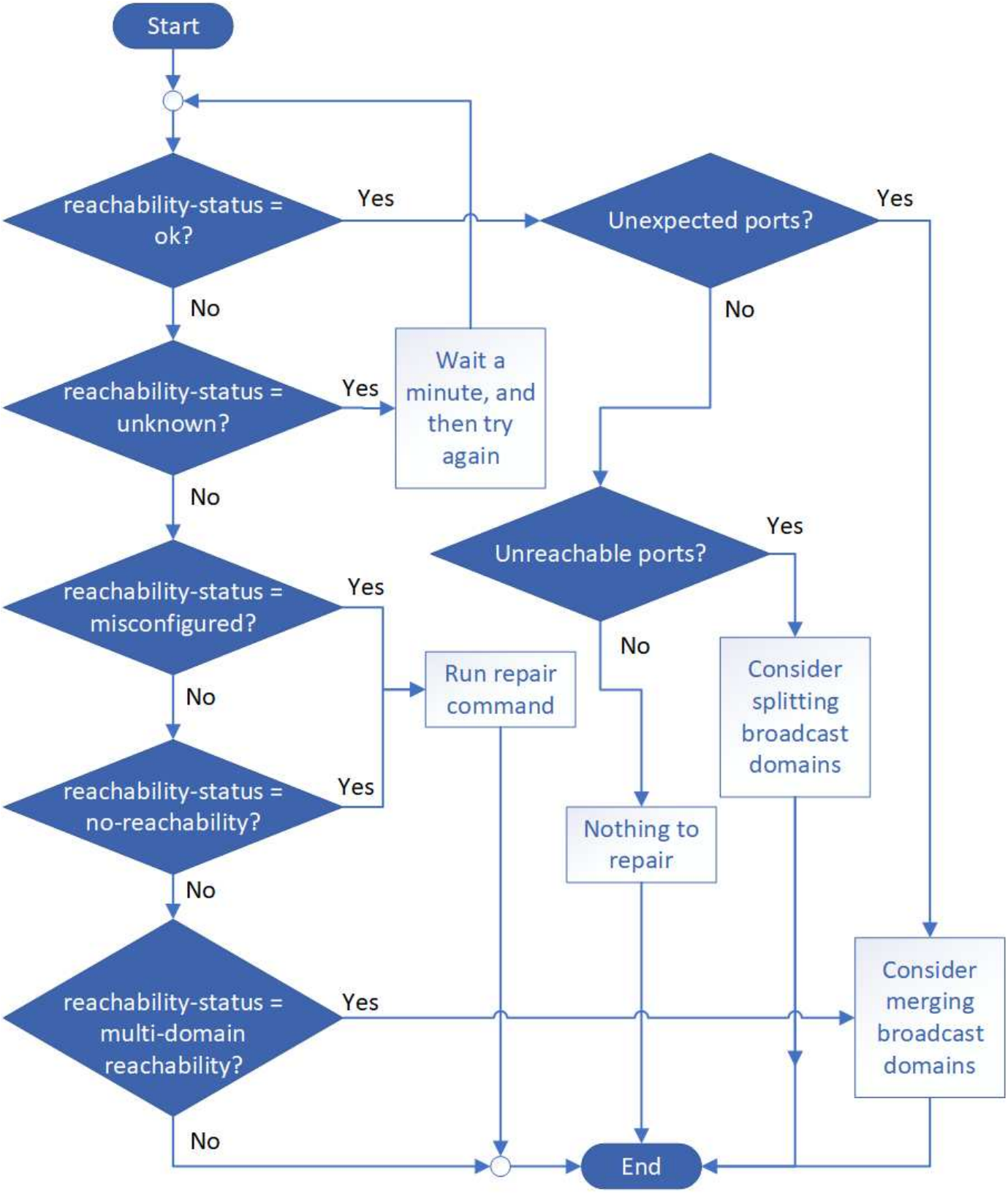
これらのコマンドを使用して、ONTAPの設定が物理的なケーブル配線またはネットワークスイッチの設定と一致しないことに起因するネットワークの設定ミスを検証、診断、および修復します。

ステップ

1. ポートの到達可能性を表示します。

```
network port reachability show
```

2. 次のDecision Treeと表を使用して、次の手順を決定します（該当する場合）。



プレゼンスステータス	説明

OK	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にレイヤ 2 の到達可能性があります。到達可能性ステータスが「ok」で、「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マージすることを検討してください。詳細については、次の _unexpected ports_row を参照してください。 到達可能性ステータスが「ok」で、到達不能な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スプリットすることを検討してください。詳細については、次の _Unreachable Ports_row を参照してください。 到達可能性ステータスが「ok」で、予期しないポートや到達不能なポートがない場合、設定は正しいです。
予期しないポートです	ポートには、割り当てられたブロードキャストドメインにレイヤ 2 に到達できることがありますが、少なくとも 1 つの他のブロードキャストドメインにレイヤ 2 に到達できることもあります。 物理接続とスイッチの設定を調べて、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にマージする必要がないかどうかを確認します。 詳細については、を参照してください "ブロードキャストドメインのマージ"。
到達不能ポート	1 つ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パーティショニングされている場合は、ブロードキャストドメインをスプリットして 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、到達不能なポートのリストには、物理的な設定とスイッチの設定に間違いがないことを確認したあとに、これらのポートを別のブロードキャストドメインに分割する必要があります。 詳細については、を参照してください "ブロードキャストドメインのスプリット"。
誤設定 - 到達可能性	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にレイヤ 2 に到達できるかどうかは関係ありませんが、ポートは別のブロードキャストドメインにレイヤ 2 に到達できるかどうかは関係ありません。 ポートの到達可能性を修復できます。次のコマンドを実行すると、到達可能な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、を参照してください"ポートの到達可能性を修復"。
到達不能	既存のどのブロードキャストドメインにもレイヤ 2 で接続できません。 ポートの到達可能性を修復できます。次のコマンドを実行すると、自動的にデフォルトIPspace内に作成された新しい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、を参照してください"ポートの到達可能性を修復"。

multi-domain-reachable	ポートには、割り当てられたブロードキャストドメインにレイヤ 2 に到達できることがありますが、少なくとも 1 つの他のブロードキャストドメインにレイヤ 2 に到達できることもあります。 物理接続とスイッチの設定を調べて、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にマージする必要がないかどうかを確認します。 詳細については、またはを参照してください"ブロードキャストドメインのマージ""ポートの到達可能性を修復"。
不明	reachable-status が「 unknown 」の場合は、数分待ってからもう一度コマンドを実行してください。

ポートを修理したら、削除されたLIFとVLANを確認して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の状況についても理解しておく必要があります。詳細については、を参照してください "ポートの到達可能性を修復"。

ONTAPポートの概要

多くのwell-knownポートは、特定のサービスとのONTAP通信用に予約されています。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。

次の表に、ONTAPで使用されるTCPポートとUDPポートを示します。

サービス	ポート / プロトコル	説明
SSH	22/tcp のようになります	Secure ShellログインSecure Shellログイン
Telnet	23/tcp のようになります	リモートログイン
DNS	53/tcp のようになります	ロードバランシングDNS
HTTP	80 / TCP	ハイパーテキスト転送プロトコル
rpcbind	111/tcp のようになります	リモートプロシージャコール
rpcbind	111/UDP	リモートプロシージャコール
NTP	123 / UDP	ネットワークタイムプロトコル
希望小売価格	135 / UDP	MSRPC
NetBIOS-SSN	139/tcp のようになります	NetBIOSサービスセッション
SNMP	161 / UDP	簡易ネットワーク管理プロトコル
HTTPS	443/tcp のようになります	HTTP over TLS
Microsoft-DS	445/tcp のようになります	Microsoft-DS
マウントする	635/tcp のようになります	NFSマウント
マウントする	635/UDP	NFSマウント
名前付き	953 / UDP	名前デーモン

NFS	2049/UDP	NFSサーバデーモン
NFS	2049 / TCP	NFSサーバデーモン
NRV	2050/tcp のようになります	NetAppリモートボリュームプロトコル
iSCSI	3260/tcp のようになります	iSCSIターゲットポート
ロックド	4045/tcp のようになります	NFSロックデーモン
ロックド	4045 / UDP	NFSロックデーモン
NSM	4046/tcp のようになります	ネットワークステータスモニタ
NSM	4046 / UDP	ネットワークステータスモニタ
rquotad	4049/UDP	NFS rquotadプロトコル
krb524	4444 / UDP	Kerberos 524
mDNS	5353 / UDP	マルチキャストDNS
HTTPS	5986/UDP	HTTPSポートリスニングバイナリプロトコル
HTTPS	8443/tcp のようになります	7MTT GUIツール（https経由）
NDMP	10000/tcp のようになります	ネットワークデータ管理プロトコル
クラスタピアリング	11104/tcp のようになります	クラスタピアリング、双方向
クラスタピアリング、双方向	11105/tcp のようになります	クラスタピアリング
NDMP	18600～18699/TCP	NDMP
NDMP	30000/tcp のようになります	セキュアソケットを介した制御接続の受け入れ
CIFS監視ポート	40001/tcp のようになります	CIFS監視ポート
TLS	50000/tcp のようになります	トランスポートレイヤセキュリティ
iSCSI	65200/tcp のようになります	iSCSIポート

ONTAP内部ポート

次の表に、ONTAPで内部的に使用されるTCPポートとUDPポートを示します。これらのポートは、クラスタ内LIFの通信の確立に使用されます。

ポート / プロトコル	説明
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
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
982	NetAppクラスタRPC
983	NetAppクラスタRPC
5125	ディスクの代替制御ポート
5133	ディスクの代替制御ポート
5144	ディスクの代替制御ポート
65502	ノードスコープSSH
65503	LIF共有
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
8023	ノードスコープTelnet
8514	ノードスコープRSH
9877	KMIPクライアントポート（内部ローカルホストのみ）

IPspace

IPspaceの設定の概要

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。

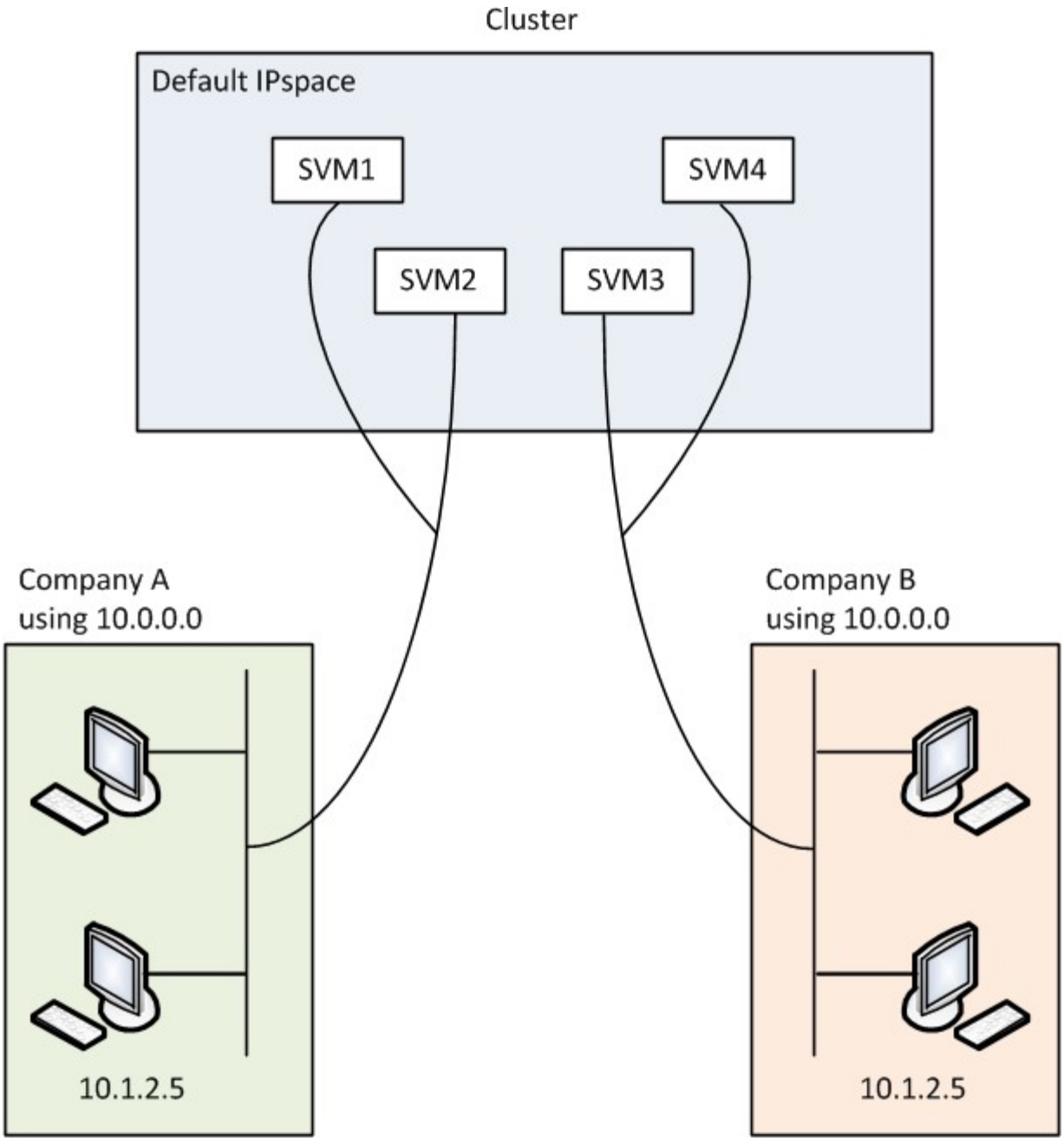
単一の組織のストレージを管理する場合は、IPspaceを設定する必要はありません。単一のONTAPクラスタで複数企業のストレージを管理していて、ユーザ間のネットワーク設定がないことが確実な場合も、IPspaceを使用する必要はありません。多くの場合、Storage Virtual Machine （SVM）を専用のIPルーティング テーブルと一緒に使用することで、IPspaceを使用しなくても固有のネットワーク設定を分離できます。

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。

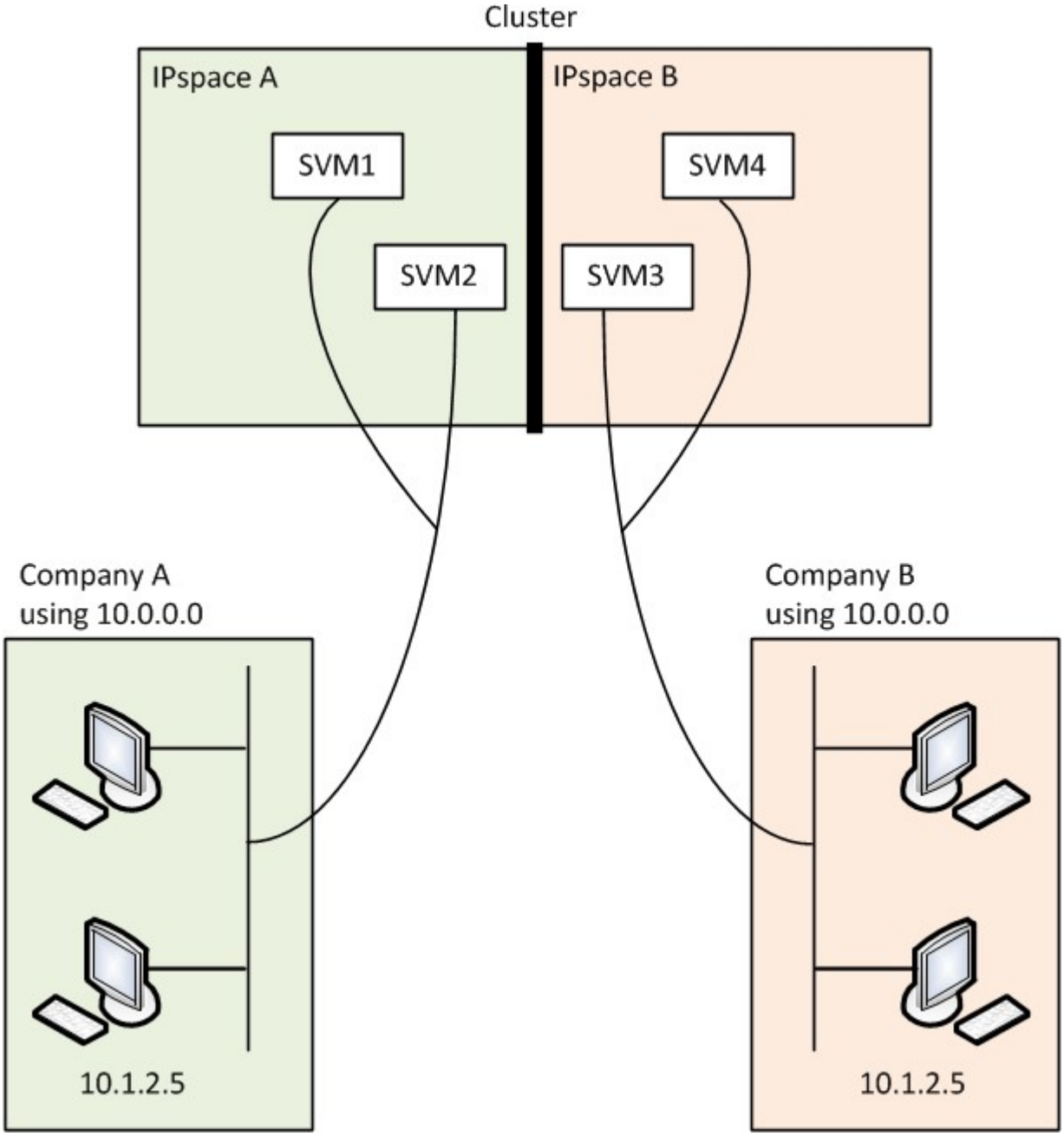
次の図に、この導入形態を示します。これは、両社で非プライベートIPアドレスの範囲を使用する場合に機能します。しかし、図に示すように両社が同じプライベートIPアドレスの範囲を使用すると問題が発生します。



両社がプライベートIPアドレスサブネット10.0.0.0を使用しているため、次の問題が発生します。

- 両社がそれぞれのSVMに同じIPアドレスを使用する場合、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に異なるIPアドレスを使用することに合意した場合でも、問題が生じる可能性があります。
- たとえば、Aのネットワーク内のいずれかのクライアントがBのネットワーク内のクライアントと同じIPアドレスを持っている場合、Aのアドレス空間内のクライアント宛てのパケットはBのアドレス空間内のクライアントにルーティングされ、その逆も同様です。
- 両社が相互に排他的なアドレススペースを使用する場合（たとえば、Aが10.0.0.0、ネットワークマスクが255.128.0.0、Bが10.128.0.0、ネットワークマスクが255.128.0.0など）、SSPはクラスタに静的ルートを設定して、トラフィックをAとBのネットワークに適切にルーティングする必要があります。
- このソリューションは、拡張性（静的ルートが原因）もセキュア（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）もありません。これらの問題を解決するために、SSPはクラスタに2つのIPspace（会社ごとに1つずつ）を定義します。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ため、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いても、次の図に示すように、それぞれの会社のデータがそれぞれのネットワークにセキュアにルーティングされます。



また、さまざまな構成ファイル（ファイル、ファイル、 `/etc/hosts.equiv` `the /etc/rc`ファイルなど）で参照されるIPアドレス `/etc/ hosts`は、そのIPspaceに対して相対的です。そのため、IPspaceを使用すると、SSPが複数のSVMの設定と認証データに同じIPアドレスを設定しても競合することはありません。

IPspaceの標準プロパティ

クラスタの最初の作成時に特別な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。

クラスタの初期化時に2つのIPspaceが自動的に作成されます。

- 「デフォルト」のIPspace

  このIPspaceは、ポート、サブネット、およびデータ提供用SVMのコンテナです。クライアントごとに個別のIPspaceを作成する必要がない設定の場合は、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ています。

- 「クラスタ」IPspace

  このIPspaceには、クラスタ内のすべてのノードのすべてのクラスタポートが含まれます。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。

IPspaceの作成

IPspaceは、Storage Virtual Machine（SVM）が配置される個別のIPアドレススペースです。SVMにセキュアなストレージ、管理、およびルーティングが必要な場合は、IPspaceを作成できます。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に属するクライアントは、同じIPアドレスサブネット範囲の重複するIPアドレスを使用してクラスタデータにアクセスできます。

タスクの内容

IPspaceの数はクラスタ全体で512個に制限されています。6GBのRAMを搭載したノードを含むクラスタのIPspaceは、クラスタ全体で256個までに制限されます。ご使用のプラットフォームに適用されるその他の制限については、Hardware Universeを参照してください。

"NetApp Hardware Universe"

「all」はシステムで予約されている名前であるため、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。

ステップ

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、クラスタにipspace1というIPspaceを作成します。

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

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

MetroCluster構成のクラスタに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「デフォルト」のIPspace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
```

IPspaceを表示します。

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。

ステップ

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 IPspace 、 SVM 、およびブロードキャストドメインをすべて表示します。

```
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
```

IPspaceを削除します。

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、または SVM がないようにします。

システム定義の「デフォルト」IPspaceと「クラスタ」IPspaceは削除できません。

ステップ

IPspaceを削除します。

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

次のコマンドは、クラスタから ipspace1 という IPspace を削除します。

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

ブロードキャストドメイン

ブロードキャストドメイン（**ONTAP 9 .8**以降）

ブロードキャストドメインの概要（**ONTAP 9 .8**以降）

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ネットワークポートをグループ化するためのものです。グループ化したポートは、データトラフィックまたは管理トラフィック用のStorage Virtual Machine（SVM）で使用できます。

ブロードキャストドメインはIPspace内にあります。クラスタの初期化では、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内の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

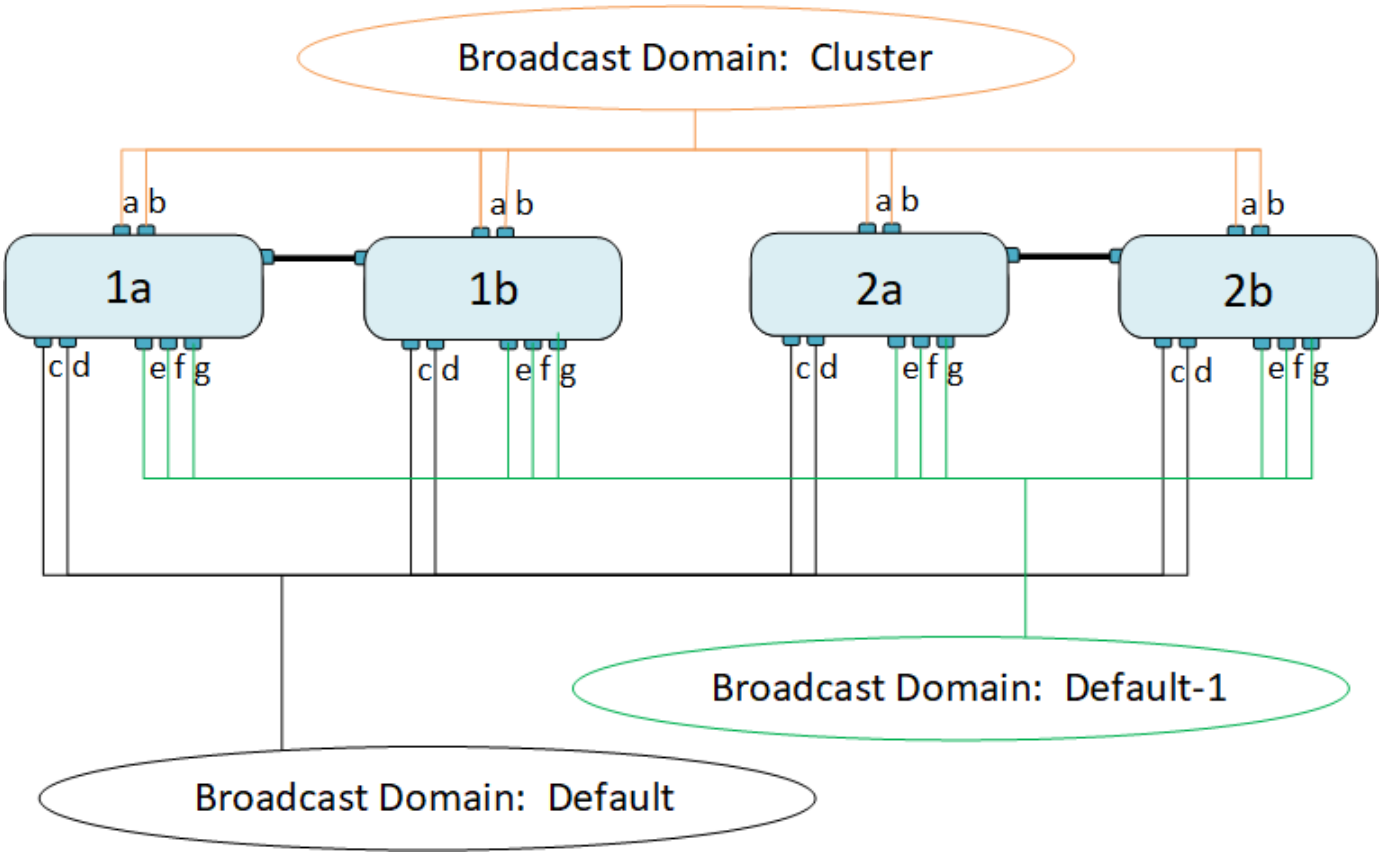
ブロードキャスト ドメインは、同じIPspace内にあり、相互にレイヤ2の到達可能性があるネットワーク ポートの集まりです。一般にクラスタ内の複数のノードのポートが含まれます。

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、クラスタの初期化時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時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。
- クラスタの初期化時に、レイヤ2ネットワークの到達可能性に基づいて追加のブロードキャストドメインが自動的に作成されます。これらの追加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。



各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または削除されると、そのフェイルオーバーグループのポートも自動的に追加または削除されます。

ブロードキャストドメインを追加する

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内のネットワークポートをグループ化します。作成したポートはSVMで使用できます。

ONTAP 9 .8以降では、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。System.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に加えて、ONTAP 9 Managerでブロードキャストドメインを手動で追加できます。

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、別のブロードキャストドメインに属していないポートである必要があります。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れらのポートを削除します。

タスクの内容

- ブロードキャストドメイン名はすべてIPspace内で一意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が、使用されていない場合は、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されたポートのMaximum Transmission Unit（MTU；最大伝送ユニット）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。

システムの設定を簡単にするために、同じポートを含む同じ名前の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. をクリックし ＋ Add
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 .7以前では、ブロードキャストドメインを手動で作成できます。

ONTAP 9 .8以降を使用している場合は、レイヤ2の到達可能性に基づいてブロードキャストドメインが自動的に作成されます。詳細については、を参照してください "ポートの到達可能性を修復"。

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
   ```

   大量のポートが表示される場合は、コマンドを使用し `network port show -broadcast-domain`て未割り当てのポートだけを表示します。

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。通常は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適用されます。

   c. `ipspace_name`は、このブロードキャストドメインを追加するIPspaceの名前です。

      このパラメータの値を指定しないかぎり、「Default」IPspaceが使用されます。

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

      ポートは、などの形式で追加され `node_name:port_number` `node1:e0c`ます。

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
   ```

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
```

終了後

この時点で、サブネットを作成してブロードキャストドメインで使用可能になるIPアドレスのプールを定義するか、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。詳細については、を参照してください "クラスタとSVMのピアリング"。

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、コマンドを使用し `network port broadcast-domain rename`ます。

ブロードキャストドメイン（**ONTAP 9 .8**以降）のポートを追加または削除します。

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。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または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別のブロードキャストドメインに属している場合は、次のトピックを参照してください。

"ポートの到達可能性を修復"

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間でイーサネットポートを再割り当てできます。すべてのイーサネットポートを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、ブロードキャストドメインからイーサネットポートの割り当てを解除した場合は、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、 * Edit * 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. 選択解除された各ポートについて、* Reassign Ethernet Port 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または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別のブロードキャストドメインに属している場合は、次のトピックを参照してください。

"ポートの到達可能性を修復"

または、コマンドまたは `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対してポートを手動で追加または削除することもできます `network port broadcast-domain add-ports`。

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、別のブロードキャストドメインに属していないポートにする必要があります。
- 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。

タスクの内容

ネットワークポートの追加と削除には、次のルールが適用されます。

ポートの追加	ポートの削除
ネットワークポート、VLAN、インターフェイスグループ（ifgrp）のいずれかです。	N/A
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がブロードキャストドメインのIPspaceの値に更新されます。	ポートはブロードキャストドメイン属性のない「Default」IPspaceに移動されます。

インターフェイスグループの最後のメンバーポートをコマンドを使用して削除する`network port ifgrp remove-port`と、そのインターフェイ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。これは、ブロードキャストドメインに空のインターフェイスグループポートが存在できないためです。

手順

1. 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 `network port show`。
2. ブロードキャストドメインにネットワークポートを追加または削除します。

状況	使用方法
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. ポートがブロードキャストドメインに対して追加または削除されたことを確認します。

```
network port show
```

これらのコマンドの詳細については、を参照してください。 "ONTAPコマンド リファレンス"

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
```

ブロードキャストドメインが自動的に作成されます。ただし、ポートを再接続した場合やスイッチの設定を変更した場合は、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（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、解決策を提案します。

の配線が正しくないと、ブロードキャストドメインポートが予期せず割り当てられる可能性があります。ONTAP 9 .10.1以降では、クラスタのセットアップ後や新しいノードが既存のクラスタに追加されたときに、クラスタでポートに到達できるかどうかを確認することで、ネットワーク配線の問題がないかどうかを自動的にチェックします。

System Manager

ポートの到達可能性の問題が検出された場合、System Managerでは修復処理を実行して問題を解決することを推奨します。

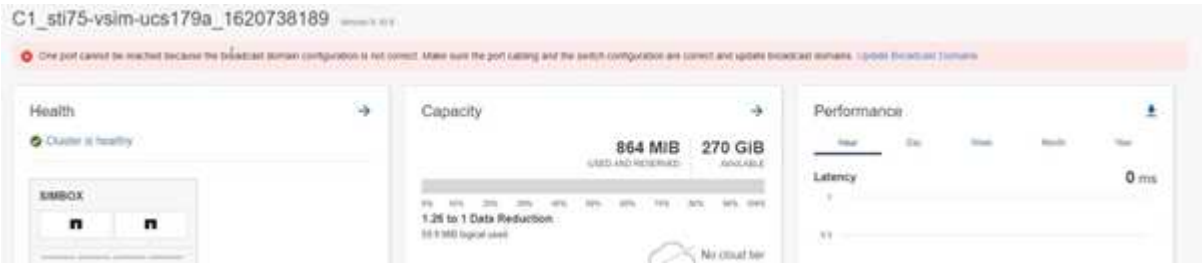
クラスタのセットアップが完了すると、ネットワーク配線の問題がダッシュボードに報告されます。

新しいノードをクラスタに追加すると、[Nodes]ページにネットワーク配線の問題が表示されます。

ネットワーク配線の健全性は、ネットワークダイアグラムで確認することもできます。ポートの到達可能性の問題は、ネットワークダイアグラムに赤いエラーアイコンで示されます。

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。



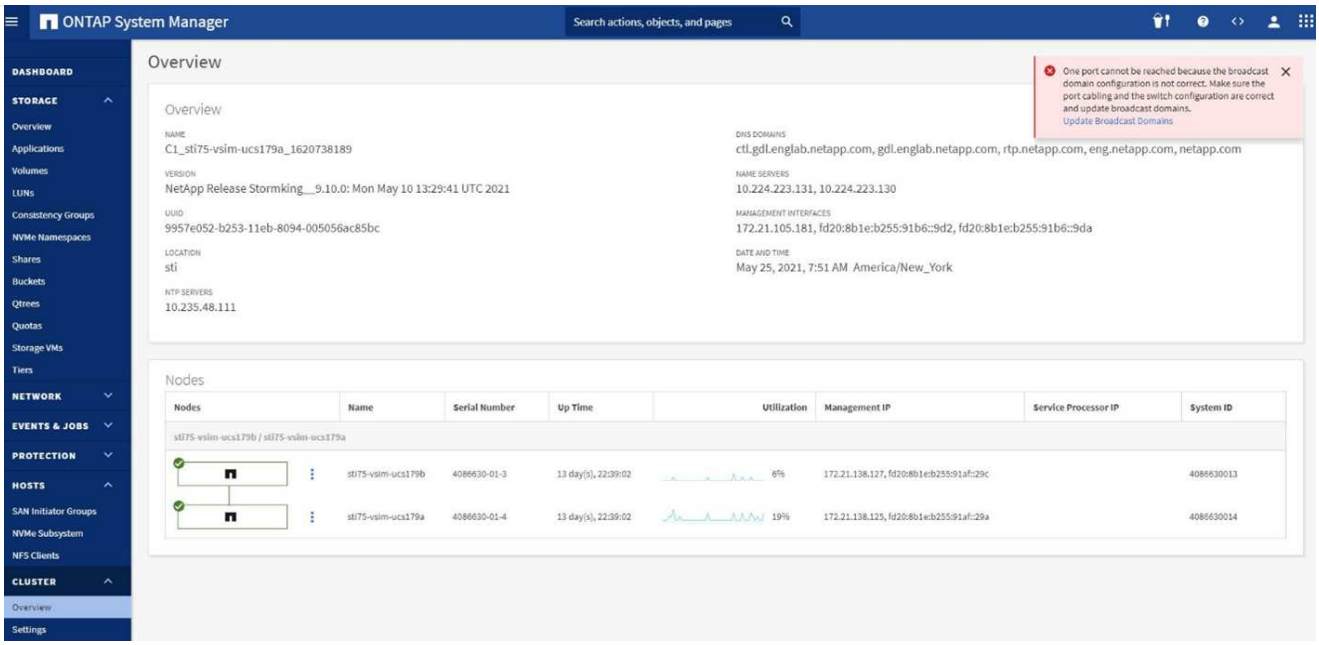
手順

1. メッセージに記載されているように配線を修正します。
2. リンクをクリックして[Update Broadcast Domains]ダイアログを起動します。[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. ポートに関する情報（ノード、問題、現在のブロードキャストドメイン、想定されるブロードキャストドメインなど）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。ポートは現在のブロードキャストドメインから想定されるブロードキャストドメインに移動されます。

ノードの追加後

新しいノードをクラスタに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. メッセージに記載されているように配線を修正します。
2. リンクをクリックして[Update Broadcast Domains]ダイアログを起動します。[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. ポートに関する情報（ノード、問題、現在のブロードキャストドメイン、想定されるブロードキャストドメインなど）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。ポートは現在のブロードキャストドメインから想定されるブロードキャストドメインに移動されます。

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。

タスクの内容

ONTAPで検出されたレイヤ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を使用できます。

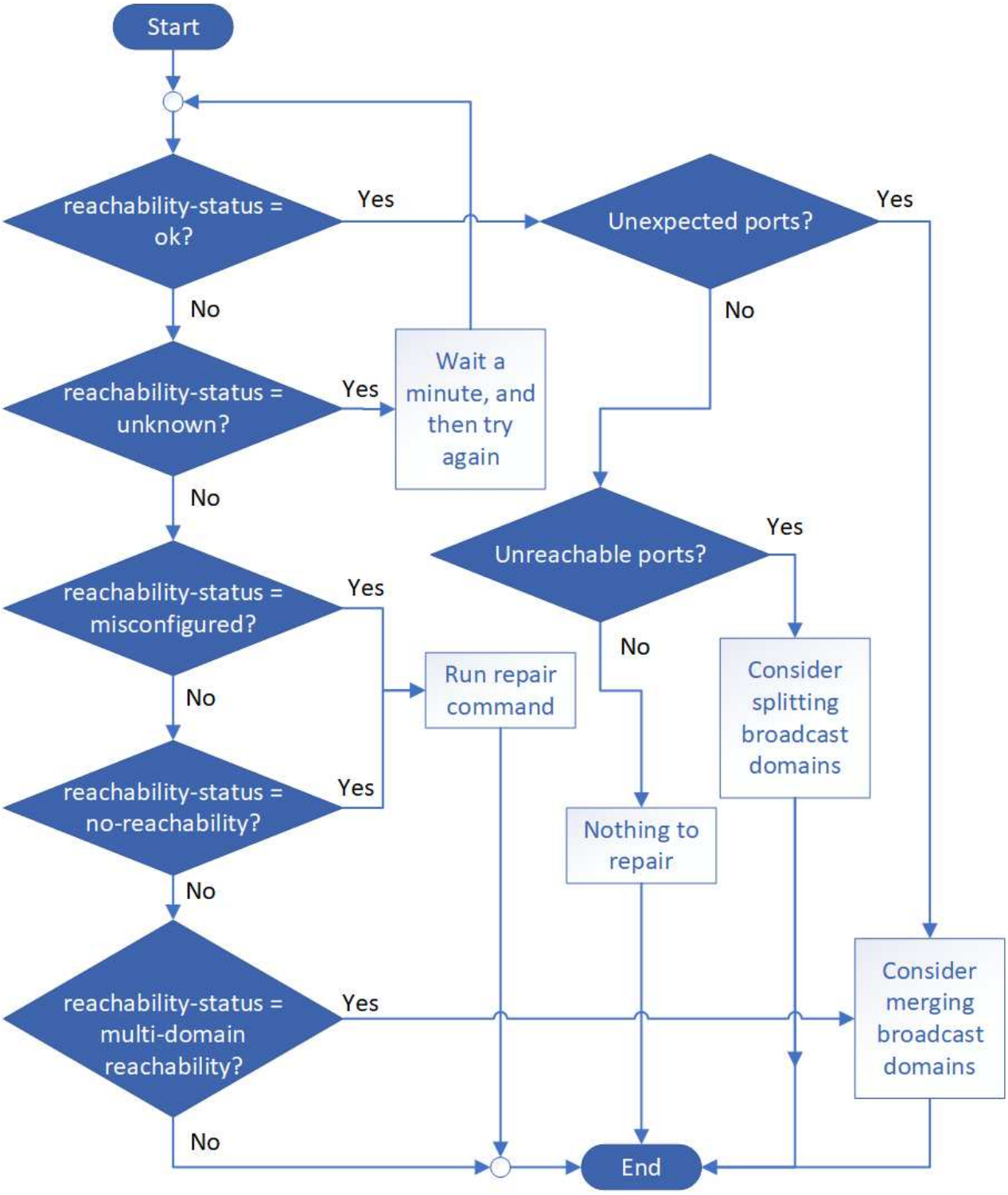
手順

1. スイッチの構成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。

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。



プレゼンスステータス	説明
OK	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にレイヤ 2 の到達可能性があります。到達可能性ステータスが「ok」で、「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マージすることを検討してください。詳細については、次の _unexpected ports_row を参照してください。 到達可能性ステータスが「ok」で、到達不能な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スプリットすることを検討してください。詳細については、次の _Unreachable Ports_row を参照してください。 到達可能性ステータスが「ok」で、予期しないポートや到達不能なポートがない場合、設定は正しいです。
予期しないポートです	ポートには、割り当てられたブロードキャストドメインにレイヤ 2 に到達できることがありますが、少なくとも 1 つの他のブロードキャストドメインにレイヤ 2 に到達できることもあります。 物理接続とスイッチの設定を調べて、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にマージする必要がないかどうかを確認します。 詳細については、を参照してください "ブロードキャストドメインのマージ"。
到達不能ポート	1 つ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パーティショニングされている場合は、ブロードキャストドメインをスプリットして 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、到達不能なポートのリストには、物理的な設定とスイッチの設定に間違いがないことを確認したあとに、これらのポートを別のブロードキャストドメインに分割する必要があります。 詳細については、を参照してください "ブロードキャストドメインのスプリット"。
誤設定 - 到達可能性	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にレイヤ 2 に到達できるかどうかは関係ありませんが、ポートは別のブロードキャストドメインにレイヤ 2 に到達できるかどうかは関係ありません。 ポートの到達可能性を修復できます。次のコマンドを実行すると、到達可能な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	既存のどのブロードキャストドメインにもレイヤ 2 で接続できません。 ポートの到達可能性を修復できます。次のコマンドを実行すると、自動的にデフォルトIPspace内に作成された新しい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` *注：*すべてのインターフェイスグループ（ifgrp）メンバーポートがレポートされた場合、 `no-reachability`メンバーポートごとにコマンドを実行する `network port reachability repair`と、各ポートが`ifgrp`から削除されて新しいブロードキャストドメインに配置され、`ifgrp`自体が削除されます。コマンドを実行する前に `network port reachability repair`、物理ネットワークトポロジに基づいて、ポートに到達可能なブロードキャストドメインが想定どおりであることを確認してください。
multi-domain-reachable	ポートには、割り当てられたブロードキャストドメインにレイヤ 2 に到達できることがありますが、少なくとも 1 つの他のブロードキャストドメインにレイヤ 2 に到達できることもあります。 物理接続とスイッチの設定を調べて、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にマージする必要がないかどうかを確認します。 詳細については、を参照してください "ブロードキャストドメインのマージ"。
不明	reachable-status が「 unknown 」の場合は、数分待ってからもう一度コマンドを実行してください。

ポートを修理したら、削除されたLIFとVLANがないか確認します。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の状況についても理解しておく必要があります。

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
```

- 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が設定されていた場合、それらのVLANは自動的に削除されますが、「削除」されたことも記録されます。削除されたVLANは次のとおりです。

```
displaced-vlans show
```

削除されたVLANがある場合は、次のいずれかを実行する必要があります。

- VLANを別のポートにリストアします。

```
displaced-vlans restore
```

- 「displaced-VLANs」テーブルからエントリを削除します。

```
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。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。

関連トピック

"Verify your network configuration after upgrading"

"ネットワーク ポートの到達可能性の監視"

ブロードキャストドメインを**IPspace**に移動（**ONTAP 9 .8**以降）

レイヤ2の到達可能性に基づいてシステムで作成したブロードキャストドメインを、作成したIPspaceに移動します。

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に到達できるかどうかを確認する必要があります。

ポートの自動スキャンでは、相互にアクセスできる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できますが、このスキャンでは適切なIPspaceを特定できません。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、クラスタの作成時および追加時に自動的に設定されます。ONTAPでは、「default」ブロードキャストドメインとは、クラスタに最初に作成されたノード上の管理インターフェイスのホームポートへレイヤ2で接続されている一連のポートを指します。他のブロードキャストドメインも必要に応じて作成され、「 * 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。

タスクの内容

- クラスタLIFが設定されたポートは、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ONTAPによって自動的に作成されます。
- VLANとインターフェイスグループを追加すると、作成してから約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に到達できるかどうかを確認します。ONTAPはレイヤ2の到達可能性を自動的に監視します。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
   ```

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、次の手順を実行します。

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

ブロードキャストドメインのスプリット（**ONTAP 9 .8**以降）

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つのグループに分割された場合は、ブロードキャストドメインをスプリットしてONTAP設定を物理的なネットワークトポロジと同期できます。

ネットワークポートのブロードキャストドメインが到達可能性の複数のセットに分割されているかどうかを確認するには、コマンドを使用し `network port reachability show -details`て、相互に接続されていないポート（「Unreachable ports」）に注意してください。一般に、到達不能ポートのリストでは、物理ポートとスイッチの設定が正確であることを確認したあとに、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るポートを定義します。

ステップ

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配置されているIPspaceの名前です。
- -`broadcast-domain`は、スプリットするブロードキャストドメインの名前です。
- -`new-broadcast-domain`は、作成す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の名前とポートです。

ブロードキャストドメインのマージ（**ONTAP 9 .8**以降）

物理的なネットワーク接続または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がすべて到達可能性を共有するようになった場合は、2つのブロードキャストドメインをマージしてONTAP設定を物理的なネットワークトポロジに同期できます。

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」コマンドを使用して、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（「予期しないポート」）に注意してください。通常、想定外のポートのリストに定義されるポートは、物理的な設定とスイッチの設定に間違いがないことを確認したあとにブロードキャストドメインにマージする必要があります。

ステップ

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のあるIPspaceの名前です。
- `-broadcast-domain`は、マージするブロードキャストドメインの名前です。
- `-into-broadcast-domain`は、追加のポートを受け取るブロードキャストドメインの名前です。

ブロードキャストドメイン（**ONTAP 9 .8**以降）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値を変更して、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。これは、ネットワークで行われたトポロジの変更をサポートするために実行できます。

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。

タスクの内容

MTU値を変更すると、影響を受けるポートを経由するトラフィックが一時的に中断されます。プロンプトが表示され、MTUを変更するには「y」と入力する必要があります。

ステップ

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>]
```

- `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。通常は1500と9000です。
- `ipspace`は、このブロードキャストドメインが配置されているIPspaceの名前です。このオプションの値を指定しないかぎり、「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>
```

ブロードキャストドメインを表示します（**ONTAP 9 .8**以降）。

クラスタ内の各IPspace内の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、各ブロードキャストドメインのポートとMTU値のリストも表示されます。

ステップ

クラスタのブロードキャストドメインと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、クラスタ内のすべてのブロードキャストドメインと関連付けられているポートを表示します。

```
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（ポートを適切に更新できなかった）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
```

詳細については、を参照して "ONTAPコマンド リファレンス"ください。

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。これにより、指定したブロードキャストドメインに関連付けられているポートが「デフォルト」のIPspaceに移動されます。

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、ま

たはSVMがないようにします。

タスクの内容

- システムで作成された「Cluster」ブロードキャストドメインは削除できません。
- ブロードキャストドメインを削除すると、そのブロードキャストドメインに関連するフェイルオーバーグループがすべて削除されます。

実行する手順は、使用するインターフェイス（System ManagerまたはCLI）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、またはブロードキャストドメインがサブネットに関連付けられている場合は、delete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. 削除するブロードキャストドメインの横にある*> Delete *を選択します ⋮ 。

CLI

*ブロードキャストドメイン*を削除するには、CLIを使用してください

ステップ

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
```

ブロードキャストドメイン（ONTAP 9 .7以前）

ブロードキャストドメインの概要（**ONTAP 9 .7**以前）

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ネットワークポートをグループ化するためのものです。グループ化したポートは、データトラフィックまたは管理トラフィック用のStorage Virtual Machine（SVM）で使用できます。

ブロードキャストドメインはIPspace内にあります。クラスタの初期化では、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。

- デフォルトのブロードキャストドメインには、デフォルトの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。

クライアント トラフィックを分離するために独自のIPspaceを作成した場合は、作成した各IPspace内にブロードキャスト ドメインを作成する必要があります。

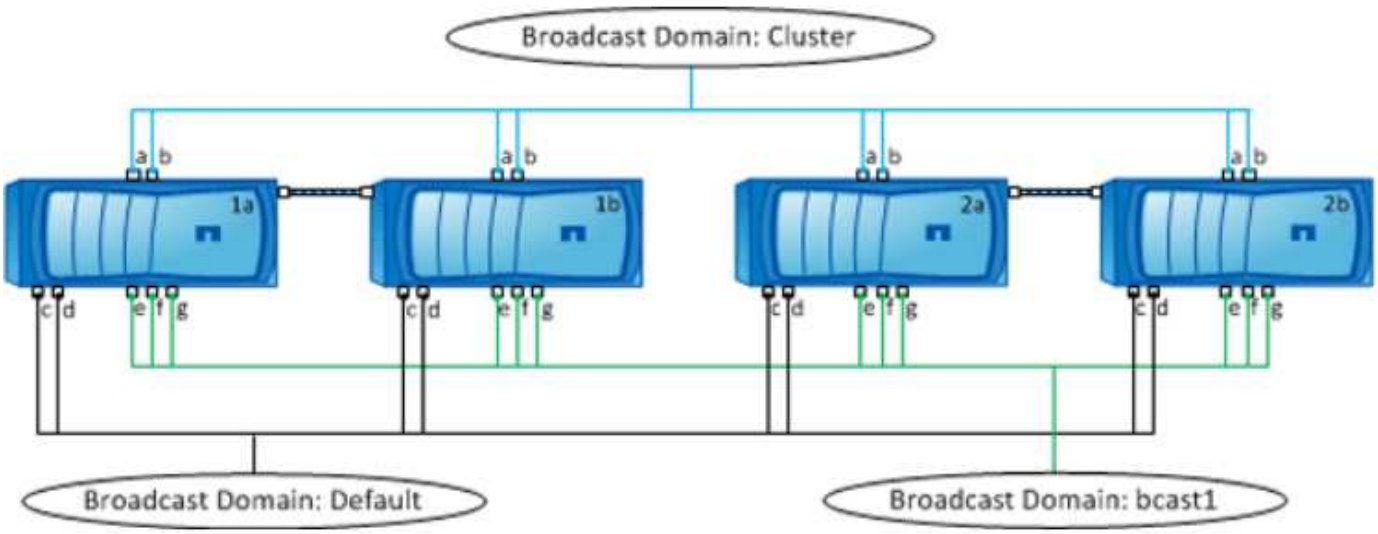
ブロードキャスト ドメインを作成して、同じレイヤ2ネットワークに属するクラスタのネットワーク ポートをグループ化します。これらのポートは、SVMで使用されます。

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。
- bcast1というブロードキャスト ドメインは手動で作成されたドメインで、クラスタ内の各ノードのポートe、f、gが含まれます。このブロードキャスト ドメインは、新しいクライアントが新しいSVMを介してデータにアクセスできるよう、システム管理者が作成したものです。



各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または削除されると、そのフェイルオーバーグループのポートも自動的に追加または削除されます。

ブロードキャストドメインに使用できるポートの確認（**ONTAP 9 .7**以前）

新しいIPspaceに追加するブロードキャストドメインを設定する前に、ブロードキャストドメインに使用できるポートを確認する必要があります。

このタスクは、ONTAP 9 8ではなくONTAP 9 .0 ~ 9.7に関連しています。

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。

タスクの内容

- ポートには、物理ポート、VLAN、インターフェイスグループ（ifgroup）を指定できます。
- 新しいブロードキャストドメインに追加するポートを既存のブロードキャストドメインに割り当てることはできません。
- ブロードキャストドメインに追加するポートがすでに別のブロードキャストドメイン（デフォルトIPspaceのデフォルトブロードキャストドメインなど）にある場合は、そのブロードキャストドメインからポートを削除してから新しいブロードキャストドメインに割り当てる必要があります。
- LIFが割り当てられているポートは、ブロードキャストドメインから削除できません。
- クラスタ管理LIFとノード管理LIFはデフォルトIPspace内のデフォルトブロードキャストドメインに割り当てられているため、これらのLIFに割り当てられているポートをデフォルトブロードキャストドメインから削除することはできません。

手順

1. 現在のポートの割り当てを確認します。

   ```
   network port show
   ```

   ```
   Node   Port IPspace  Broadcast Domain Link   MTU  Admin/Oper
   ------ ---- -------  ---------------- ----- ----  ------------
   node1
          e0a  Cluster  Cluster          up    9000  auto/1000
          e0b  Cluster  Cluster          up    9000  auto/1000
          e0c  Default  Default          up    1500  auto/1000
          e0d  Default  Default          up    1500  auto/1000
          e0e  Default  Default          up    1500  auto/1000
          e0f  Default  Default          up    1500  auto/1000
          e0g  Default  Default          up    1500  auto/1000
   node2
          e0a  Cluster  Cluster          up    9000  auto/1000
          e0b  Cluster  Cluster          up    9000  auto/1000
          e0c  Default  Default          up    1500  auto/1000
          e0d  Default  Default          up    1500  auto/1000
          e0e  Default  Default          up    1500  auto/1000
          e0f  Default  Default          up    1500  auto/1000
          e0g  Default  Default          up    1500  auto/1000
   ```

   この例では、コマンドの出力から次の情報が得られます。

   - 各ノードのポート `e0c`、 `e0d`、 `e0e`、、 `e0f`が `e0g`デフォルトブロードキャストドメインに割り当てられています。

- これらのポートは、作成するIPspaceのブロードキャストドメインで使用できる可能性があります。

2. デフォルトブロードキャストドメイン内の、LIFインターフェイスに割り当てられている、したがって新しいブロードキャストドメインに移動できないポートを確認します。

   `network interface show`

```
          Logical      Status     Network          Current   Current Is
Vserver   Interface    Admin/Oper Address/Mask     Node      Port    Home
-------   ----------   ---------- ------------   --------- -------  ----
Cluster
          node1_clus1  up/up       10.0.2.40/24   node1     e0a     true
          node1_clus2  up/up       10.0.2.41/24   node1     e0b     true
          node2_clus1  up/up       10.0.2.42/24   node2     e0a     true
          node2_clus2  up/up       10.0.2.43/24   node2     e0b     true

cluster1
          cluster_mgmt up/up       10.0.1.41/24   node1     e0c     true
          node1_mgmt   up/up       10.0.1.42/24   node1     e0c     true
          node2_mgmt   up/up       10.0.1.43/24   node2     e0c     true
```

   次の例では、コマンドの出力から次の情報が得られます。

   - ノードポートは各ノードのポートに割り当てられ `e0c`、クラスタ管理LIFのホームノードはに `node1`` なります `e0c`。
   - 各ノードのポート `e0d`、 `e0e`、 `e0f`、および`e0g`LIFをホストしていないため、デフォルトのブロードキャストドメインから削除して、新しいIPspaceの新しいブロードキャストドメインに追加できます。

ブロードキャストドメインの作成（**ONTAP 9 .7**以前）

ONTAP 9 .7以前では、ブロードキャストドメインを作成して、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ます。作成したポートはSVMで使用できます。カスタムIPspaceのブロードキャストドメインを作成する必要があります。IPspaceに作成されたSVMは、ブロードキャストドメイン内のポートを使用します。

このタスクは、ONTAP 9 8ではなくONTAP 9 .0 ~ 9.7に関連しています。

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。

ONTAP 9 .8以降では、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。ONTAP 9 .8以降を実行している場合は、これらの手順は必要ありません。

ONTAP 9 .7以前では、別のブロードキャストドメインに属しているポートは追加できません。

タスクの内容

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。ブロードキャストドメインを作成すると、同じ名前のフェイルオーバーグループがONTAPによって自動的に作成されます。フェイルオーバーグループには、ブロードキャストドメインに割り当てられているすべてのポートが含まれます。

- ブロードキャストドメイン名はすべてIPspace内で一意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できるポートは、物理ネットワークポート、VLAN、インターフェイスグループ（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が、使用されていない場合は、コマンドを使用し `network port broadcast-domain remove-ports`て既存のブロードキャストドメインからポートを削除します。
- ブロードキャストドメインに追加したポートの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。
- 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。

システムの設定を簡単にするために、同じポートを含む同じ名前のフェイルオーバーグループが自動的に作成されます。

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
   ```

   大量のポートが表示される場合は、コマンドを使用し `network port show -broadcast-domain`て未割り当てのポートだけを表示します。

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]
   ```

   - `*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。
   - `*mtu_value*`はIPパケットのMTUサイズです。通常は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適用されます。

   - `*ipspace_name*`は、このブロードキャストドメインを追加するIPspaceの名前です。

     このパラメータの値を指定しないかぎり、「Default」IPspaceが使用されます。

   - `*ports_list*`は、ブロードキャストドメインに追加するポートのリストです。

     ポートは、などの形式で追加され *node_name:port_number* `node1:e0c`ます。

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*`

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
```

終了後

この時点で、サブネットを作成してブロードキャストドメインで使用可能になるIPアドレスのプールを定義するか、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。詳細については、を参照してください "クラスタとSVMのピアリング"。

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、コマンドを使用し `network port broadcast-domain rename`ます。

ブロードキャストドメイン（**ONTAP 9 .7**以前）のポートを追加または削除します。

ブロードキャストドメインの作成時にネットワークポートを追加したり、既存のブロードキャストドメインに対してポートを追加したり削除したりできます。これにより、クラスタ内のすべてのポートを効率的に使用できます。

新しいブロードキャストドメインに追加するポートがすでに別のブロードキャストドメインにある場合は、新しいブロードキャストドメインに割り当てる前にそのブロードキャストドメインからポートを削除する必要があります。

このタスクは、ONTAP 9 8ではなくONTAP 9 .0 ~ 9.7に関連しています。

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、別のブロードキャストドメインに属していないポートにする必要があります。
- 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。

タスクの内容

ネットワークポートの追加と削除には、次のルールが適用されます。

ポートの追加	ポートの削除
ネットワークポート、VLAN、インターフェイスグループ（ifgrp）のいずれかです。	N/A
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がブロードキャストドメインのIPspaceの値に更新されます。	ポートはブロードキャストドメイン属性のない「Default」IPspaceに移動されます。

インターフェイスグループの最後のメンバーポートをコマンドを使用して削除する `network port ifgrp remove-port`と、そのインターフェイ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。これは、ブロードキャストドメインに空のインターフェイスグループポートが存在できないためです。

手順

1. 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 `network port show`。
2. ブロードキャストドメインにネットワークポートを追加または削除します。

状況	使用方法
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. ポートがブロードキャストドメインに対して追加または削除されたことを確認します。

```
network port show
```

これらのコマンドの詳細については、を参照して "ONTAPコマンド リファレンス"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
```

ブロードキャストドメインのスプリット（**ONTAP 9 .7**以前）

既存のブロードキャストドメインを2つにスプリットして、それぞれのブロードキャストドメインに元のブロードキャストドメインに割り当てられていたポートの一部を含めることができます。

タスクの内容

- ポートがフェイルオーバーグループに含まれている場合は、フェイルオーバーグループ内のすべてのポートをスプリットする必要があります。
- ポートにLIFが関連付けられている場合、LIFをサブネットの範囲に含めることはできません。

ステップ

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のあるIPspaceの名前です。
- `-broadcast-domain`は、スプリットするブロードキャストドメインの名前です。
- `-new-broadcast-domain`は、作成す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の名前とポートです。

ブロードキャストドメインのマージ（**ONTAP 9 .7**以前）

mergeコマンドを使用して、1つのブロードキャストドメインのすべてのポートを既存のブロードキャストドメインに移動できます。

この方法を使用すると、ブロードキャストドメインのすべてのポートを削除してから既存のブロードキャストドメインに追加するだけで済みます。

ステップ

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のあるIPspaceの名前です。
- `-broadcast-domain`は、マージするブロードキャストドメインの名前です。
- `-into-broadcast-domain`は、追加のポートを受け取るブロードキャストドメインの名前です。

例

次の例では、bd-data1というブロードキャストドメインをbd-data2というブロードキャストドメインにマージしています。

```
network port -ipspace Default broadcast-domain bd-data1 into-broadcast-domain bd-
data2
```

ブロードキャストドメイン（**ONTAP 9 .7**以前）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値を変更して、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。これは、ネットワークで行われたトポロジの変更をサポートするために実行できます。

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。

タスクの内容

MTU値を変更すると、影響を受けるポートを経由するトラフィックが一時的に中断されます。プロンプトが表示され、MTUを変更するには「y」と入力する必要があります。

ステップ

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>]
```

- `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。通常は1500と9000です。
- `ipspace`は、このブロードキャストドメインが配置されているIPspaceの名前です。このオプションの値を指定しないかぎり、「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>
```

ブロードキャストドメインを表示する（**ONTAP 9 .7**以前）

クラスタ内の各IPspace内の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、各ブロードキャストドメインのポートとMTU値のリストも表示されます。

ステップ

クラスタのブロードキャストドメインと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、クラスタ内のすべてのブロードキャストドメインと関連付けられているポートを表示します。

```
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
        bcast1       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、bcast1ブロードキャストドメイン内のポートのうち、更新ステータスがerrorになっている（ポートを適切に更新できなかった）ポートを表示します。

```
network port broadcast-domain show -broadcast-domain bcast1 -port-update
-status error

IPspace Broadcast                                 Update
Name    Domain Name  MTU   Port List              Status Details
------- ----------- -----  --------------------- --------------
Default bcast1       1500
                           cluster-1-02:e0g       error
```

詳細については、を参照して "ONTAPコマンド リファレンス"ください。

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。これにより、指定したブロードキャストドメインに関連付けられているポートが「デフォルト」のIPspaceに移動されます。

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、ま

たはSVMがないようにします。

タスクの内容

- システムで作成された「Cluster」ブロードキャストドメインは削除できません。
- ブロードキャストドメインを削除すると、そのブロードキャストドメインに関連するフェイルオーバーグループがすべて削除されます。

実行する手順は、使用するインターフェイス（System ManagerまたはCLI）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、またはブロードキャストドメインがサブネットに関連付けられている場合は、delete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. 削除するブロードキャストドメインの横にある*> Delete *を選択します ⋮ 。

CLI

*ブロードキャストドメイン*を削除するには、CLIを使用してください

ステップ

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
```

フェイルオーバーグループとポリシー

LIFフェイルオーバーの概要

LIFのフェイルオーバーとは、LIFの現在のポートでリンク障害が発生した場合に、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コンポーネントです。LIFフェイルオーバーを設定するには、フェイルオーバーグループを作成し、フェイルオーバーグループを使用するようにLIFを変更して、フェイルオーバーポリシーを指定します。

フェイルオーバーグループには、クラスタ内の1つ以上のノードの一連のネットワークポート（物理ポート、VLAN、およびインターフェイスグループ）が含まれます。フェイルオーバーグループに含まれ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定義されます。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に有効なフェイルオーバーターゲットが設定されていないと、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します。フェイルオーバーの設定を確認するには、「network interface show -failover」コマンドを使用します。

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む同じ名前の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または削除されると、そのフェイルオーバーグループのポートも自動的に追加または削除されます。これは、管理者が自分でフェイルオーバーグループを管理する必要がない場合に効率的に機能するためです。

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場合に、 LIF が別のポートに自動的に移行できるようにします。これにより、システムのネットワークトラフィックがクラスタ内の使用可能な他のポートに再ルーティングされます。

タスクの内容

グループを作成し、そのグループにポートを追加するには、コマンドを使用し `network interface failover-groups create`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ポートは、すべて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に含めることができます。
- 異なる VLAN またはブロードキャストドメインに LIF がある場合は、 VLAN または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。

ステップ

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するポートのリストです。node_name > ： < port_number > という形式でポートを指定してください。たとえば、 node1 ： e0c のようになります。

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

- フェイルオーバーグループを作成したら、 LIF にフェイルオーバーグループを適用する必要があります。
- 有効なフェイルオーバーターゲットのないフェイルオーバーグループを LIF に設定すると、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。

LIFのフェイルオーバーを設定する

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に適用することで、ネットワークポートの特定のグループにLIFを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。

タスクの内容

- LIFを作成すると、LIFの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は、LIFのタイプとサービスポリシーに基づいた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さらに制限するように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はシステムによって自動的に更新されます。

- LIFのフェイルオーバーの動作を変更するには、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します。
- LIFを変更すると、LIFに有効なフェイルオーバーターゲットがなくなるため、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。

- All-Flash SAN Array（ASA）プラットフォームでは、Storage.11.1以降で、新規に作成したONTAP 9 VMに新しく作成したiSCSI LIFでiSCSI LIFのフェイルオーバーが自動的に有効になります。

  また、"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を指定することもできます。

- 次に、-failover-policyの設定が、フェイルオーバーグループから選択されるターゲットポートに与える影響を示します。

  > iSCSI LIFのフェイルオーバーの場合は、フェイルオーバーポリシー `sfo-partner-only`と`disabled`のみが `local-only`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のホームノードおよびクラスタ内の他の1つのノード（通常はSFOパートナー以外のノード（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`LIFにフェイルオーバーが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
```

フェイルオーバーグループとポリシーの管理用コマンド

フェイルオーバーグループを管理するには、コマンドを使用し`network interface failover-groups`ます。LIFに適用され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するには、コマンドを使用し`network interface modify`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します。	`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します	`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て、クラスタ内のどのLIFにも有効なフェイルオーバーターゲットが設定されないようにすると、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。

詳細については、コマンドと `network interface modify`コマンドのマニュアルページを参照して `network interface failover-groups`ください。

サブネット（クラスタ管理者のみ）

サブネットの概要

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。

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、あとでSVMのLIFを作成するときに使用することができます。

これにより、LIFごとにIPアドレスやネットワークマスク値を指定する代わりにサブネット名を指定することで、LIFを簡単に作成できます。

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。

サブネットを追加するブロードキャストドメインとIPspaceがすでに存在している必要があります。

タスクの内容

- サブネット名はすべて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追加する場合は、異なるサブネットまたはホストが同じIPアドレスを使用しないように、ネットワーク内でIPアドレスが重複しないようにする必要があります。
- 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は、そのサブネットを使用してLIFを作成するときに、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や、サブネットを定義するときにゲートウェイを指定しない場合は、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 `route create`あります。
- NetAppでは、データSVM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構成で重要です。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を使用してONTAPがデスティネーションクラスタのフェイルオーバーターゲットを決定できます。

手順

実行する手順は、使用するインターフェイス（System ManagerまたはCLI）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作成できます。

手順

1. [ネットワーク]>[概要]>[サブネット*]を選択します。
2. をクリックし + Add てサブネットを作成します。
3. サブネットに名前を付けます。
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てください。

```
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3サブネットの名前です。

  名前には、「Mgmt」のようなテキスト文字列を使用することも、192.0.2.0/24のような特定のサブネットIP値を使用することもできます。

- `broadcast_domain_name`は、サブネットが配置され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属するIPspaceの名前です。

  このオプションの値を指定しないかぎり、「Default」IPspaceが使用されます。

- `subnet_address`は、サブネットのIPアドレスとマスクです。たとえば、192.0.2.0/24のように指定します。
- `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。たとえば、192.0.2.1のように指定します。
- `ip_address_list`は、サブネットに割り当てるIPアドレスのリストまたは範囲です。

個 々 のアドレス、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。

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

  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、このコマンドは失敗します。この値をtrueに設定すると、手動でアドレスを指定し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、Default IPspaceのブロードキャストドメインdefault-1にサブネットsub1を作成します。IPv4サブネットのIPアドレスとマスク、ゲートウェイ、およびIPアドレスの範囲を追加します。

```
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にサブネットsub2を作成します。IPv6アドレスの範囲を追加します。

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

終了後

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、コマンドを使用し `network subnet rename`ます。

サブネットの**IP**アドレスを追加または削除する

最初に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。これにより、SVMに必要なIPアドレスだけを割り当てることができます。

実行する手順は、使用するインターフェイス（System ManagerまたはCLI）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*に対してIPアドレスを追加または削除できます

手順

1. [ネットワーク]>[概要]>[サブネット*]を選択します。
2. 変更するサブネットの横にある*>[編集]*を選択します ⋮ 。
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、IPアドレスをサブネットに追加したり、サブネットから削除したりします。*

タスクの内容

IPアドレスを追加するときに、追加する範囲の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とエラーが表示されます。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、このオプションをに `true`設定し `-force-update-lif-associations`ます。

IPアドレスを削除するときに、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とエラーが表示されます。サブネットから削除したIPアドレスをインターフェイスで引き続き使用するには、オプションをに `true`設定し `-force-update-lif-associations`ます。

ステップ

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	network subnet add-ranges
サブネットから IP アドレスを削除します	network subnet remove-ranges

これらのコマンドの詳細については、マニュアルページを参照してください。

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>
```

現在の範囲が1～10および20～40で、11～19および41～50（基本的には1～50）を追加する場合は、次のコマンドを使用して既存のアドレス範囲と重複することができます。このコマンドは新しいアドレスのみを追加し、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>
```

サブネットのプロパティの変更

既存のサブネットのサブネットアドレスとマスク値、ゲートウェイアドレス、またはIPアドレスの範囲を変更できます。

タスクの内容

- IPアドレスを変更する場合は、異なるサブネットまたはホストが同じIPアドレスを使用しないように、ネットワーク内でIPアドレスが重複しないようにする必要があります。
- ゲートウェイのIPアドレスを追加または変更した場合、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に適用されます。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しなければならないことがあります。

実行する手順は、使用するインターフェイス（System ManagerまたはCLI）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. [ネットワーク]>[概要]>[サブネット*]を選択します。
2. 変更する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します。*

ステップ

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、サブネットのあるIPspaceの名前です。
- `subnet`は、サブネットの新しいアドレスとマスクです（該当する場合）。たとえば、192.0.2.0/24のように指定します。
- `gateway`は、サブネットの新しいゲートウェイです（該当する場合）。たとえば、192.0.2.1のように指定します。「 * 」と入力すると、ゲートウェイのエントリが削除されます。
- `ip_ranges`は、サブネットに割り当てる新しいIPアドレスのリストまたは範囲です（該当する場合）。IPアドレスには、個 々 のアドレス、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。ここで指定した範囲を使用すると、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場合、このオプションの値を * true * に設定できます。指定した範囲の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、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、サブネットsub3のゲートウェイIPアドレスを変更します。

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

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できます。この出力には、各サブネットで使用可能なIPアドレスの総数、および現在使用されているアドレスの数も表示されます。

実行する手順は、使用するインターフェイス（System ManagerまたはCLI）によって異なります。

System Manager

- ONTAP 9.12.0以降では、System Managerでサブネットを表示できます*

手順

1. [ネットワーク]>[概要]>[サブネット*]を選択します。
2. サブネットのリストを表示します。

CLI

- CLIを使用してサブネット*を表示します

ステップ

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アドレス範囲を表示します。

```
network subnet show
```

次のコマンドは、サブネットとサブネット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
```

サブネットを削除します。

サブネットが不要になり、そのサブネットに割り当てられていたIPアドレスの割り当てを解除するには、サブネットを削除します。

実行する手順は、使用するインターフェイス（System ManagerまたはCLI）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. [ネットワーク]>[概要]>[サブネット*]を選択します。
2. 削除するサブネットの横にある*> Delete *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*を削除してください

タスクの内容

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と、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、サブネットとLIFの関連付けを解除します。

ステップ

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
```

SVMの作成

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ルートボリュームに設定するセキュリティ形式を確認し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場合は、ルートボリュームにNTFSセキュリティ形式を使用する必要があります。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に設定すると、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しないようになります。

- ONTAP 9.13.1以降では、Storage VMに最大容量を設定できます。また、SVMの容量レベルがしきい値に近づいたときにアラートを設定することもできます。詳細については、を参照してください SVM容量の管理。

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. をクリック + Add してStorage VMを作成します。
3. Storage VMに名前を付けます。
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の有効化*を選択した場合は、次の設定を行います。

フィールドまたはチェックボックス	説明
管理者名	SMB / CIFS Storage VMの管理者ユーザ名を指定してください。
パスワード	SMB / CIFS Storage VMの管理者パスワードを指定してください。
サーバ名	SMB / CIFS Storage VMのサーバ名を指定してください。
Active Directoryドメイン	SMB / CIFS Storage VMにユーザ認証を提供するActive Directoryドメインを指定してください。
組織単位	SMB / CIFSサーバに関連付けられたActive Directoryドメイン内の組織単位を指定します。デフォルト値は「CN=Computers」で、変更できます。
Storage VM内の共有へのアクセス時にデータを暗号化する	SMB 3.0を使用してデータを暗号化し、SMB / CIFS Storage VM内の共有に対する不正なファイルアクセスを防止するには、このチェックボックスを選択します。
ドメイン	SMB / CIFS Storage VMに対して表示されているドメインを追加、削除、または順序変更する。
ネームサーバ	SMB / CIFS Storage VMのネームサーバの追加、削除、または順序変更

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	Storage VMに設定するネットワークインターフェイスごとに、既存のサブネットを選択するか（少なくとも1つ存在する場合）、または「サブネットなし」と指定し、「 IPアドレス*」フィールドと「サブネットマスク」フィールドを入力します。使用する場合は、* 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ます。システムで自動的にホームポートを選択することも、使用するホームポートをリストから手動で選択することもできます。
管理者アカウントを管理する	Storage 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選択します。選択した場合、ユーザ名とパスワードを指定し、確認のためにもう一度パスワードを入力し、Storage 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（FCの有効化）を選択した場合は、次の設定を行います。

フィールドまたはチェックボックス	説明
Allow NFS client accessチェックボックス	NFS Storage VMに作成されたすべてのボリュームで、ルートボリュームパス「/」を使用してマウントとトラバースを行う必要がある場合は、このチェックボックスを選択します。中断のないマウントトラバーサルを許可するには、エクスポートポリシー「default」にルールを追加してください。

ルール	をクリックし + Add 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。 • Access Protocols：次のオプションを組み合わせて選択します。 ◦ SMB / CIFS ◦ FlexCache ◦ NFS ▪ NFSv3 ▪ NFSv4 • アクセスの詳細：各タイプのユーザについて、読み取り専用、読み取り/書き込み、または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。ユーザタイプは次のとおりです。 ◦ すべて ◦ all（匿名ユーザとして） ◦ 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	Storage VMに設定するネットワークインターフェイスごとに、既存のサブネットを選択するか（少なくとも1つ存在する場合）、または「サブネットなし」と指定し、「 IPアドレス*」フィールドと「サブネットマスク」フィールドを入力します。使用する場合は、* 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ます。システムで自動的にホームポートを選択することも、使用するホームポートをリストから手動で選択することもできます。

管理者アカウントを管理する	Storage 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選択します。選択した場合、ユーザ名とパスワードを指定し、確認のためにもう一度パスワードを入力し、Storage 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 iSCSI*]を選択した場合は、次の設定を行います。

フィールドまたはチェックボックス	説明
ネットワークインターフェイス	Storage VMに設定するネットワークインターフェイスごとに、既存のサブネットを選択するか（少なくとも1つ存在する場合）、または「サブネットなし」と指定し、「 IPアドレス*」フィールドと「サブネットマスク」フィールドを入力します。使用する場合は、* 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ます。システムで自動的にホームポートを選択することも、使用するホームポートをリストから手動で選択することもできます。
管理者アカウントを管理する	Storage 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選択します。選択した場合、ユーザ名とパスワードを指定し、確認のためにもう一度パスワードを入力し、Storage 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 FC（FCの有効化）を選択した場合は、次の設定を行います。

フィールドまたはチェックボックス	説明
FCポートを設定	Storage VMに含めるノードのネットワークインターフェイスを選択してください。ノードごとに2つのネットワークインターフェイスを推奨します。
管理者アカウントを管理する	Storage 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選択します。選択した場合、ユーザ名とパスワードを指定し、確認のためにもう一度パスワードを入力し、Storage 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、次の設定を行います。

フィールドまたはチェックボックス	説明

FCポートを設定	Storage VMに含めるノードのネットワークインターフェイスを選択してください。ノードごとに2つのネットワークインターフェイスを推奨します。
管理者アカウントを管理する	Storage 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選択します。選択した場合、ユーザ名とパスワードを指定し、確認のためにもう一度パスワードを入力し、Storage 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、次の設定を行います。

フィールドまたはチェックボックス	説明
ネットワークインターフェイス	Storage VMに設定するネットワークインターフェイスごとに、既存のサブネットを選択するか（少なくとも1つ存在する場合）、または「サブネットなし」と指定し、「 IPアドレス*」フィールドと「サブネットマスク」フィールドを入力します。使用する場合は、* 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ます。システムで自動的にホームポートを選択することも、使用するホームポートをリストから手動で選択することもできます。
管理者アカウントを管理する	Storage 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選択します。選択した場合、ユーザ名とパスワードを指定し、確認のためにもう一度パスワードを入力し、Storage 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

サブネットを作成するには、ONTAP CLIを使用してください。

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1GB以上の空きスペースが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直後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を作成するときにSnapshot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Snapshotポリシーの名前を確認して、その名前を控えます。

   ```
   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、コマンドはIPspace「ipspace1」に「vs1」という名前のSVMを作成します。ルートボリュームは「vs1_root」という名前で、NTFSセキュリティ形式で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の制限を適用できます。このポリシーはSVMの作成後にのみ適用できます。このプロセスの詳細については、を参照してくださいアダプティブポリシーグループテンプレートの設定。

論理インターフェイス（LIF）

LIFの概要

LIFの設定の概要

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するポートに設定できます。

クラスタ管理者は、LIFを作成、表示、変更、移行、リバート、削除できます。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するポートに設定できます。

ONTAP 9 10.1以降では、ファイアウォールポリシーが廃止され、LIFのサービスポリシーに全面的に置き換えられました。詳細については、を参照してください "LIFのファイアウォールポリシーを設定する"。

LIFは次のポートでホストできます。

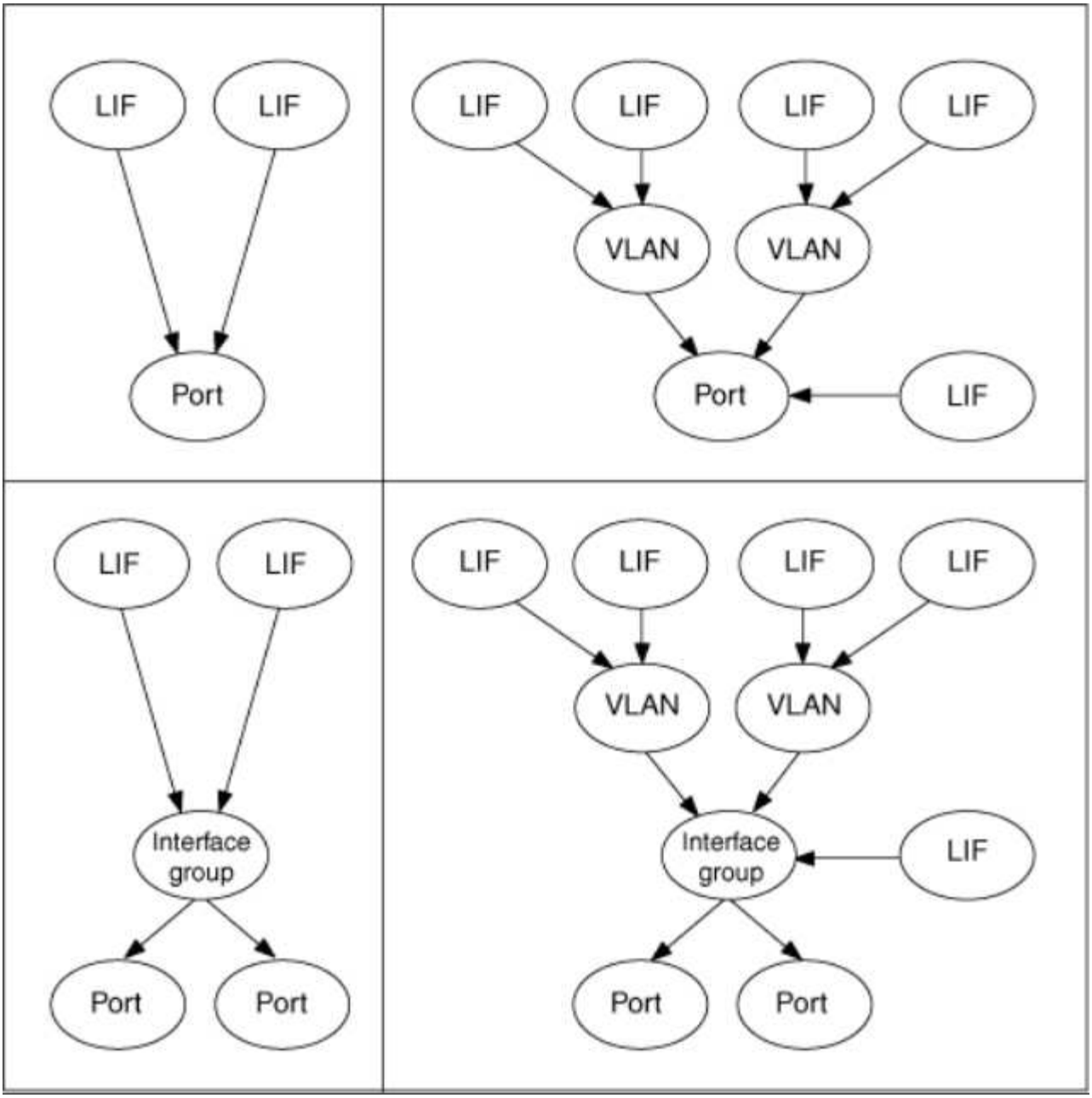
- インターフェイスグループに属していない物理ポート
- インターフェイスグループ
- VLAN
- VLANをホストする物理ポートまたはインターフェイスグループ
- 仮想IP（VIP）ポート

  ONTAP 9 5以降では、VIP LIFがサポートされ、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際には、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を修復"

- ONTAP 9 .7以前："ブロードキャストドメインのポートを追加または削除します。"

LIFのフェイルオーバーが（自動または手動で）有効になっているLIFの場合は、次の点に注意してください。

- データサービスポリシーを使用するLIFでは、フェイルオーバーポリシーの制限を確認できます。
  - ONTAP 9 .6以降："ONTAP 9 .6以降のLIFとサービスポリシー"
  - ONTAP 9 .5以前："ONTAP 9 .5以前のLIFのロール"
- LIFの自動リバートは、自動リバートがに設定されていて、LIFのホームポートが正常に機能していてLIFをホストできる場合に実行され `true`ます。
- 計画的または計画外のノードの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のポートは、VIF Managerによって決まります。
- フェイルオーバーが完了すると、LIFは正常に動作します。
- 自動リバートがに設定されている場合、ギブバックが開始されると、LIFはホームノードとホームポートにリバート `true`されます。
- 1つ以上のLIFをホストしているポートでイーサネットリンクが停止すると、VIF ManagerはLIFを停止している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移行します。新しいポートは、同じノードまたはそのHAパートナーに配置できます。リンクがリストアされたあとにauto-revertがに設定されている場合、 `true`VIF ManagerはLIFをそれぞれのホームノードとホームポートにリバートします。
- 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ると、VIF ManagerはLIFをクォーラムのノードから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、自動リバートがに設定されている場合は `true`、VIF ManagerによってLIFがホームノードとホームポートにリバートされます。

ポートタイプトノ**LIF**ノゴカンセイ

LIFにはさまざまな特性を持たせて、さまざまなポートタイプをサポートできます。

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のファイアウォールによってブロックされ、AutoSupport接続とNTP接続が失敗することがあります。コマンドを実行してクラスタ間LIFを切り替えることで、システムをリカバリでき `network interface modify -vserver *vserver name* -lif *intercluster LIF* -status-admin up|down`ます。ただし、この問題を回避するには、インタークラスタLIFと管理LIFを別 々 のサブネットに設定する必要があります。

LIF	説明
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できます。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のトラフィックに使用されるLIFです。クラスタLIFは、常に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アドレスが自動的に生成されます。ただし、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あることを確認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ない
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前に、クラスタ内の各ノードにクラスタ間LIFを作成する必要があります。これらのLIFは、同じノード内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。これらの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は、VIPポート上に作成された任意のデータLIFです。詳細については、を参照してください"仮想IP（VIP）LIFの設定"。

ONTAPでサポートされるトラフィックを管理します。

時間の経過とともに、LIFでサポートされるトラフィックのタイプのONTAPによる管理方法が変わりました。

- 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が使用されます。
- 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サービスポリシーが導入されました。
  - ONTAP 9 .6は、LIFのロールをLIFのサービスポリシーに置き換えました。
  - ファイアウォールサービスをONTAP 9のサービスポリシーに置き換えました。

設定する方法は、使用するONTAPのリリース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、を参照してください"コマンド：firewall-policy-show"。
- LIFのロールについては、を参照し"LIFのロール（ONTAP 9.5以前）"てください。
- LIFサービスポリシーについては、を参照し"LIFとサービスポリシー（ONTAP 9 .6以降）"てください。

LIFとサービスポリシー（**ONTAP 9 .6**以降）

LIFのロールやファイアウォールポリシーの代わりに、LIFでサポートされるトラフィッ

クの種類を決定するサービスポリシーをLIFに割り当てることができます。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。

サービスポリシーとその詳細を表示するには、次のコマンドを使用します。

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

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が選択されます。

サービスポリシーが空のLIF上のアプリケーションが予期せず動作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、管理LIFやクラスタ間LIFなど、そのSVMのLIF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。

次の表に、ONTAP 9時点でのシステムSVMのLIFの組み込みのポリシーを示します。それ以外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	同等のロール	説明
デフォルト - intercluster	インタークラスタコア、管理 - https ： //	クラスタ間	クラスタ間トラフィックを処理する LIF で使用されます。注：サービス intercluster-core は、 net-intercluster サービスポリシーという名前で ONTAP 9.5 から提供されています。
default-route-announce	management-bgp	-	BGP ピア接続を処理する LIF で使用されます。注： ONTAP 9.5 では net-route-announce サービスポリシーという名前で提供されています。

default-management	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	ノード管理、またはクラスタ管理	システムを対象としたこの管理ポリシーを使用して、システムSVMが所有するノードとクラスタを対象とした管理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使用できるだけでなく、システム全体の代わりに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の接続にも使用できます。ONTAP 9 12.1以降では、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 `management-log-forwarding`ます。

次の表に、ONTAP 9 .11.1以降でシステムSVMでLIFが使用できるサービスを示します。

サービス	フェイルオーバーの制限	説明
intercluster-core	home-node-only	中核となるクラスタ間サービス
管理コア	-	中核となる管理サービス
management-ssh	-	SSH管理アクセス用のサービス
Management - 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 ペイロードの送信に関連するサービス
management-bgp	home-port - Only （ホームポートのみ）	BGP ピアのやり取りに関連するサービス
backup-ndmp-control の実行	-	NDMP バックアップ制御のためのサービス
管理 - EMS	-	管理メッセージアクセス用のサービス
management-ntp-client	-	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。
management-ntp-server	-	ONTAP 9.10.1で導入されました。NTPサーバ管理アクセス用のサービス

管理 - portmap	-	portmap 管理用のサービス
management-srsh -server です	-	rsh サーバ管理のためのサービス
management-snmp-server	-	SNMP サーバ管理用のサービス
management-telnet-server	-	Telnet サーバ管理用のサービス
管理-ログ転送	-	ONTAP 9.12.1で導入されました。監査ログ転送用のサービス

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でLIFが使用可能な組み込みのポリシーの一覧です。その他のリリースのサービス ポリシーとその詳細を表示するには、次のコマンドを使用します。

```
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	説明
default-management	management-https、management-http、management-ssh、management-dns-client, management-ad-client, management-ldap-client 、management-nis-client	なし	このSVMを対象とした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を使用して、SVM管理者にSSHまたはHTTPSアクセスを提供できます。必要に応じて、これらの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。
default-data-blocks（デフォルトデータブロック）	データコア、データ- iSCSI	iSCSI	ブロックベースのSANデータトラフィックを処理するLIFで使用されます。ONTAP 9.10.1以降、「default-data-blocks」ポリシーは廃止されました。代わりに「default-data-iscsi」サービス ポリシーを使用してください。

default-data-files の形式で指定します	data-filc-client, data-dns-server , data-fflexcache , data-cifs , data-nfs , management-dns-client、management-ad-client, management-ldap-client, management-nis-client	NFS 、 CIFS 、 fcache	default-data-filesポリシーを使用して、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を作成します。SVM内にLIFが1つしかない場合もあるため、このポリシーでは、LIFを外部の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るようにします。これらの接続で管理LIFのみを使用する場合は、これらのサービスをこのポリシーから削除できます。
default-data-iscsi	データコア、データ - iSCSI	iSCSI	iSCSIデータトラフィックを処理するLIFで使用されます。
default-data-nvme-tcpです	データコア、データNVMe - TCP	nvme-tcpが表示されます	NVMe/FCデータトラフィックを処理するLIFで使用します。

次の表に、データSVMで使用できる各サービスを、ONTAP 9 11.1以降のLIFのフェイルオーバーポリシーに適用される制限とともに示します。

サービス	フェイルオーバーの制限	説明
management-ssh	-	SSH管理アクセス用のサービス
Management - http ： //	-	ONTAP 9.10.1 Services for HTTP管理アクセスで導入されました
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
management-snmp-server	-	SNMPサーバ管理アクセス用のONTAP 9.10.1サービスで導入されました
データコア	-	コアデータサービス
データ- NFS	-	NFSデータサービス
データ- 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の場合はホームポートのみ、ASAの場合はSFOパートナーのみ	iSCSI データサービス

backup-ndmp-control の実行	-	ONTAP 9.10.1 Backup NDMPでデータサービスの制御が導入されました
data-dns-server	-	ONTAP 9.10.1で導入されたDNSサーバデータサービス
data-fpolicy-client	-	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 を選択します	home-port - Only （ホームポートのみ）	ONTAP 9.10.1でNVMe TCPデータサービスが導入されました
data-s3-server のように指定します	-	Simple Storage Service （ S3 ）サーバデータサービス

データSVM内のLIFへのサービスポリシーの割り当てについて理解しておく必要があります。

- データサービスのリストを指定してデータSVMを作成すると、指定したサービスを使用して、そのSVMに組み込みの「default-data-files」および「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を作成すると、そのSVMに組み込みの「default-data-files」サービスポリシーと「default-data-blocks」サービスポリシーが、デフォルトのデータサービスのリストを使用して作成されます。

  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ています。

- データプロトコルのリストを指定してLIFを作成すると、指定したデータプロトコルに相当する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。
- サービスポリシーや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サービスを使用すると、LIFのロール（ONTAP 9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、以前に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動作するようになります。

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かれませんが、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ています。

- データコア
- データ- NFS
- データ- 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動作するようにポリシーに含

める必要がありますが、残りの3つのサービスは必要に応じて削除できます。

クライアント側の**LIF**サービス

ONTAP 9 .10.1以降では、ONTAP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サービスを提供します。これらのサービスは、各アプリケーションの代わりにアウトバウンド接続に使用するLIFを制御します。

次の新しいサービスを使用すると、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を管理者が制御できます。

サービス	SVM の制限事項	説明
management-ad-client	-	ONTAP 9.11.1以降では、ONTAP は外部ADサーバへのアウトバウンド接続に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以降では、ONTAPは外部のDNSサーバへのアウトバウンド接続用にDNSクライアントサービスを提供しています。
管理-LDAPクライアント	-	ONTAP 9.11.1以降では、ONTAPは外部のLDAPサーバへのアウトバウンド接続用にLDAPクライアントサービスを提供しています。
management-nis-client	-	ONTAP 9.11.1以降では、ONTAPは外部のNISサーバへのアウトバウンド接続用にNISクライアントサービスを提供しています。
management-ntp-client	システムのみ	ONTAP 9.10.1以降では、ONTAPは外部のNTPサーバへのアウトバウンド接続用にNTPクライアントサービスを提供しています。
data-fpolicy-client	データ専用	ONTAP 9.8 以降では、 ONTAP はアウトバウンド FPolicy 接続のクライアントサービスを提供します。

新しいサービスはそれぞれ自動的に組み込みのサービスポリシーの一部に含まれますが、管理者はそれらのサービスを組み込みのポリシーから削除したり、カスタムポリシーに追加して、各アプリケーションの代わりにアウトバウンド接続に使用するLIFを制御したりすることができます。

LIFのロール（**ONTAP 9.5**以前）

LIFの特性はロールごとに異なります。LIFのロールによって、インターフェイスでサポートされるトラフィックの種類、およびLIFに適用されるフェイルオーバー ルールとファイアウォールの制限、セキュリティ、ロード バランシング、ルーティングの方法が決まります。LIFのロールは、クラスタ、クラスタ管理、データ、クラスタ間、ノード管理、undef（未定義）のいずれかになります。undefロールはBGP LIFに使用されます。

ONTAP 9.6以降では、LIFのロールは廃止されています。ロールの代わりに、LIFのサービス ポリシーを指定

する必要があります。サービス ポリシーを使用してLIFを作成する場合、LIFのロールを指定する必要はありません。

LIFのセキュリティ

	Data LIF	クラスタLIF	ノード管理LIF	クラスタ管理LIF	クラスタ間LIF
プライベートIPサブネットが必要かどうか	いいえ	○	いいえ	いいえ	いいえ
セキュアなネットワークが必要	いいえ	○	いいえ	いいえ	○
デフォルトのファイアウォールポリシー	非常に厳しい	完全にオープン	中	中	非常に厳しい
ファイアウォールをカスタマイズ可能	○	いいえ	○	○	○

LIFフェイルオーバー

	Data LIF	クラスタLIF	ノード管理LIF	クラスタ管理LIF	クラスタ間LIF
デフォルトの動作	LIFのホームノードとSFO以外のパートナーノードと同じフェイルオーバーグループのポート	LIFのホームノードと同じフェイルオーバーグループ内のポートのみ	LIFのホームノードと同じフェイルオーバーグループ内のポートのみ	同じフェイルオーバーグループ内の任意のポート	LIFのホームノードと同じフェイルオーバーグループ内のポートのみ
カスタマイズ可能	○	いいえ	○	○	○

LIFのルーティング

	Data LIF	クラスタLIF	ノード管理LIF	クラスタ管理LIF	クラスタ間LIF
デフォルトルートが必要になる状況	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	しない	プライマリトラフィックタイプのいずれかが別のIPサブネットへのアクセスを必要とする場合	管理者が別のIPサブネットから接続している場合	他のクラスタ間LIFが別のIPサブネットにある場合
特定のIPサブネットへの静的ルートが必要になる状況	ほとんどなし	しない	ほとんどなし	ほとんどなし	別のクラスタのノードのクラスタ間LIFが別 々のIPサブネットにある場合

特定のサーバへの静的ホストルートが必要になる状況	ノード管理LIFの下に表示されているトラフィックタイプのいずれかを、ノード管理LIFではなくデータLIFを経由させる場合。これには、対応するファイアウォールの変更が必要です。	しない	ほとんどなし	ほとんどなし	ほとんどなし

LIFのリバランシング

	Data LIF	クラスタLIF	ノード管理LIF	クラスタ管理LIF	クラスタ間LIF
DNS：DNSサーバとして使用しますか？	○	いいえ	いいえ	いいえ	いいえ
DNS：ゾーンとしてエクスポートしますか？	○	いいえ	いいえ	いいえ	いいえ

LIFのプライマリトラフィックタイプ

	Data LIF	クラスタLIF	ノード管理LIF	クラスタ管理LIF	クラスタ間LIF
主なトラフィックタイプ	NFSサーバ、CIFSサーバ、NISクライアント、Active Directory、LDAP、WINS、DNSクライアントおよびサーバ、iSCSIおよびFCサーバ	クラスタ内	SSHサーバ、HTTPSサーバ、NTPクライアント、SNMP、AutoSupportクライアント、DNSクライアント、ソフトウェア更新のロード	SSHサーバ、HTTPSサーバ	クラスタ間レプリケーション

LIFの管理

LIFのサービスポリシーを設定する

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できます。

LIFのサービスポリシーを作成します。

LIFのサービスポリシーを作成できます。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をLIFで伝送できるようにすることができます。

このコマンドを実行するには、高度なPrivilegesが必要です `network interface service-policy create`。

タスクの内容

データSVMとシステムSVMの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と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問題を解決できます。

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. クラスタで使用可能なサービスを表示します。

```
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と、クラスタが提供するアプリケーションのことです。各サービスには、アプリケーションがリスンしているTCPおよびUDPポートが0個以上含まれています。

次の追加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. クラスタ内のサービスポリシーを表示します。

```
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のサブネットマスクのリストを指定します。デフォルトでは、指定されたすべてのサービスが、すべてのサブネットからのトラフィックを許可するデフォルトの許可アドレスリスト0.0.0.0/0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すると、ポリシーを使用するLIFは、指定したマスクのいずれにも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_or_SMB_servicesを含むSVM用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

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へのサービスポリシーの割り当ては、LIFの作成時または変更時に実行できます。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。

タスクの内容

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。

ステップ

サービスポリシーをいつLIFに割り当てるかに応じて、次のいずれかの操作を実行します。

状況	サービスポリシーを割り当てています ...
LIFの作成	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場合、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を作成することもできます。

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ものと同じSVM内の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の管理用コマンド

LIFのサービスポリシーを管理するには、コマンドを使用し `network interface service-policy`ます。

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をクラスタ間から非クラスタ間（またはその逆）に変換した場合、変更はピアクラスタにレプリケートされません。LIFサービスポリシーの変更後にピアクラスタを更新するには、最初にこの処理を実行し `snapmirror abort`てレプリケーション関係を再同期するください。

状況	使用するコマンド
サービスポリシーを作成する（advanced権限が必要）	`network interface service-policy create`

状況	使用するコマンド
既存のサービスポリシーにサービスエントリを追加する（advanced権限が必要）	`network interface service-policy add-service`
既存のサービスポリシーのクローンを作成する（advanced権限が必要）	`network interface service-policy clone`
既存のサービスポリシーのサービスエントリを変更する（advanced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する（advanced権限が必要）	`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（advanced権限が必要）	`network interface service-policy rename`
既存のサービスポリシーを削除する（advanced権限が必要）	`network interface service-policy delete`
組み込みのサービスポリシーを元の状態にリストアする（advanced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`

LIFを作成する（ネットワークインターフェイス）

SVMは、1つ以上のネットワーク論理インターフェイス（LIF）を介し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ため、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、そのサブネットがすでに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ています。作成するには、System Managerまたはコマンドを使用し `network subnet create`ます。

- LIFで処理され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、LIFで処理するトラフィックのタイプをロールで指定していました。ONTAP 9 .6以降では、LIFで処理するトラフィックのタイプをサービスポリシーを使用して指定します。

タスクの内容

- NASプロトコルとSANプロトコルを同じLIFに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および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、同じ物理ポート上に存在できます。

  - 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。この推奨事項は、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に必須です。
- 同じネットワークポートに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配置できません。
- 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。
- クラスタに多数のLIFがある場合は、クラスタでサポートされるLIFの容量を確認できます。
  - 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のスループットを表示します。
  - CLI：コマンドを使用し、各ノードでサポートされるLIFの容量を `network interface capacity details show`コマンド（advanced権限レベル）で確認し `network interface capacity show`ます。
- ONTAP 9 .7以降では、同じサブネットにSVM用の他のLIFがすでに存在する場合は、LIFのホームポートを指定する必要はありません。ONTAPは、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内の指定したホームノード上の任意のポートを自動的に選択します。

  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 LIFとネームスペースは同じノードでホストされている必要があります。
- データトラフィックを処理するNVMe LIFは、SVMごとに1つだけ設定できます。
- 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、選択したサブネットから使用可能なIPアドレスがONTAPによって自動的に選択され、ネットワークインターフェイスに割り当てられます。サブネットが複数ある場合はサブネットを変更できますが、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にSVMを作成（追加）するときに、既存のサブネットと同じ範囲の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。

- .10.1以降では、CLIコマンドにONTAP 9 `network interface` over RDMA構成のパラメータが含まれて`-rdma-protocols`います。ONTAP 9 12.1以降では、NFS over RDMA構成用のネットワークインターフェイスの作成がSystem Managerでサポートされています。詳細については、を参照してください NFS over RDMA用にLIFを設定します。
- 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iSCSI LIFの自動フェイルオーバーを使用できます。

  指定したSVMにiSCSI LIFがない場合、または指定したSVMの既存のすべてのiSCSI LIFですでにiSCSI LIFのフェイルオーバーが有効になっている場合は、新しく作成したiSCSI LIFでiSCSI LIFの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に設定され、auto-revertの値がに `true`設定`sfo-partner-only`されます）。

  ONTAP 9 .11.1以降にアップグレードしたあとに、iSCSI LIFのフェイルオーバー機能が有効になっていないSVMに既存の(`disabled`iSCSI LIFがある場合に、同じSVMに新しいiSCSI LIFを作成すると、SVM内の既存のiSCSI LIFのフェイルオーバーポリシーが新しいiSCSI LIFで同じとみなされます）。

  "ASAプラットフォームでのiSCSI LIFフェイルオーバー"

ONTAP 9 .7以降では、ONTAPの同じサブネットにすでにLIFが1つでも存在していれば、LIFのホームポートが自動的に選択されます。ONTAPは、そのサブネット内の他のLIFと同じブロードキャストドメイン内のホームポートを選択します。ホームポートは指定できますが、指定したIPspaceの該当するサブネットにLIFがない場合は必須ではありません。

ONTAP 9 .12.0以降では、使用するインターフェイス（System ManagerまたはCLI）によって実行する手順が異なります。

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*

手順

1. Network > Overview > Network Interfaces *を選択します。
2. を選択します ＋ Add 。
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. Intercluster
   c. SVM Management
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に名前を付けるか、前の選択で生成し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で少なくとも1つのサブネットが設定されている場合は、サブネットのドロップダウンが表示されます。
   a. サブネットを選択した場合は、ドロップダウンからサブネットを選択します。
   b. サブネットなしで続行すると、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を作成してください*

手順

1. LIFに使用するブロードキャストドメインポートを決定します。

```
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
```

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`

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構成で重要です。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を使用してONTAPがデスティネーションクラスタのフェイルオーバーターゲットを決定できます。手順については、を参照してください"サブネットを作成する"。

```
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、LIFに対してコマンドを実行したときにLIFが戻るノードです `network interface revert`。

     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。

   - `-home-port`は、LIFに対してコマンドを実行したときにLIFが戻る物理ポートまたは論理ポートです `network interface revert`。
   - オプションと `-netmask`オプションでIPアドレスを指定することも、オプションでサブネットからの割り当てを有効にすることも `-subnet_name`できます `-address`。
   - 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（サブネットを使用せずに）割り当てる場合、クライアントまたはドメインコントローラが別のIPサブネットにあるときに、ゲートウェイへのデフォルトルートの設定が必要になることがあります。`network route create`のマニュアルページには、SVM内での静的ルートの作成に関する情報が記載されています。

- `-auto-revert`起動時、管理データベースのステータスが変わったとき、ネットワーク接続が確立されたときなどの状況で、データLIFがホームノードに自動的にリバートされるかどうかを指定できます。デフォルトの設定はです `false`が、環境内のネットワーク管理ポリシーに応じてに設定できます `true`。
- `-service-policy`ONTAP 9 5以降では、オプションを使用してLIFのサービスポリシーを割り当てることができます `-service-policy`。LIFにサービスポリシーを指定すると、そのポリシーを使用して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のリストが作成されます。.5では、クラスタ間およびONTAP 9ピアサービスで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の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イスで学習されたRAプレフィックスのリストを表示します。

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

   b. 形式を使用し `prefix::id`て、IPv6アドレスを手動で作成します。

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

   を生成するには `id`、ランダムな64ビット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
   ```

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	使用方法
IPv4アドレス	ネットワークping
IPv6アドレス	network ping6

例

次のコマンドは、LIFを作成し、パラメータと `-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値を指定し `-address`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
```

次のコマンドでは、NVMe/FC LIFを作成してデータプロトコルを指定し `nvme-fc`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
```

LIFを変更する

LIFの属性は変更できます。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あります。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。

タスクの内容

- LIFの管理ステータスをdownに変更すると、そのLIFの管理ステータスがupに戻るまで、未処理のNFSv4ロックが維持されます。

  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、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で使用されるデータプロトコルは変更できません。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を変更したり、IP LIFに割り当てられているサービスポリシーを変更したりすることはできます。

  FC LIFで使用されるデータプロトコルを変更するには、LIFを削除して再作成する必要があります。IP LIFのサービスポリシーを変更するために、更新中に短時間の停止が発生します。

- ノードを対象とした管理LIFのホームノードと現在のノードは変更できません。
- サブネットを使用してLIFのIPアドレスとネットワークマスク値を変更すると、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の以前のIPアドレスが別のサブネットから割り当てられている場合は、そのIPアドレスがそのサブネットに返されます。
- LIFのアドレスファミリーをIPv4からIPv6に変更するには、IPv6アドレスのコロン表記を使用し、パラメータに新しい値を追加する必要があります `-netmask-length`。
- 自動設定されたリンクローカルIPv6アドレスは変更できません。
- LIFを変更すると、LIFに有効なフェイルオーバーターゲットがなくなるため、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 .11.1以降では、All-Flash SAN Array（ASA）プラットフォームでiSCSI LIFの自動フェイルオーバーを使用できます。

  既存のiSCSI LIF（9.11.1以降へのアップグレード前に作成されたLIF）については、フェイルオーバーポリシーをに変更できます"iSCSI LIFの自動フェイルオーバーを有効にする"。

実行する手順は、使用するインターフェイス（System ManagerまたはCLI）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. Network > Overview > Network Interfaces *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*>[編集]*を選択します ⋮ 。
3. 1つ以上のネットワークインターフェイス設定を変更します。詳細については、を参照してください "LIFの作成"。
4. 変更を保存します。

CLI

- LIFの変更にはCLIを使用してください*

手順

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

   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を使用して変更する方法を示しています。

   ```
   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
   ```

2. IPアドレスに到達できることを確認します。

使用する機能	使用する方法
IPv4アドレス	`network ping`
IPv6アドレス	`network ping6`

LIFを移行する

ポートで障害が発生した場合やメンテナンスが必要な場合は、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が、LIFの移行は手動操作です。一方、LIFのフェイルオーバーは、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場合にLIFを

自動的に移行する処理です。

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と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。

タスクの内容

- 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から実行する必要があります。
- ノードを対象としたLIF（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）はリモートノードに移行できません。
- NFSv4のLIFをノード間で移行した場合、そのLIFが新しいポートで使用できるようになるまでに最大45秒かかります。

  この問題を回避するには、遅延が発生しないNFSv4.1を使用します。

- iSCSI LIFは、ONTAP 9 .11.1以降を実行しているオールフラッシュSANアレイ（ASA）プラットフォームで移行できます。

  iSCSI LIFの移行は、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。

- ONTAPバージョン9.11.1以降を実行しているオールフラッシュSANアレイ（ASA）プラットフォームでないプラットフォームでは、ノード間でiSCSI LIFを移行することはできません。

  この制限を回避するには、デスティネーションノードにiSCSI LIFを作成する必要があります。詳細はこちらをご覧ください "iSCSI LIFを作成しています"。

- RDMA経由のNFSのLIF（ネットワークインターフェイス）を移行する場合は、デスティネーションポートがRoCEに対応していることを確認する必要があります。を使用してを移行するには、.10.1以降を実行している必要があります。ONTAP 9を使用して移行するには、ONTAP 9 .12.1を実行している必要があります。System ManagerでRoCE対応のデスティネーション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。詳細については、をご覧ください "NFS over RDMA用のLIFを設定しています"。
- ソースLIFまたはデスティネーションLIFを移行すると、VMware VAAIのコピーオフロード処理が失敗します。コピーオフロードの詳細：
  - "NFS環境"
  - "SAN環境"

実行する手順は、使用するインターフェイス（System ManagerまたはCLI）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*を移行します

手順

1. Network > Overview > Network Interfaces *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パートナーのデスティネーションノードとポートを選択します。

   iSCSI LIFを永続的に移行する場合は、チェックボックスを選択します。iSCSI LIFは完全に移行される前にオフラインにする必要があります。また、iSCSI LIFが永続的に移行されたあとは、元に戻すことはできません。リバートオプションはありません。

3. [* Migrate （移行）] をクリックします
4. 変更を保存します。

CLI

- LIFの移行にはCLIを使用してください*

ステップ

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、該当する処理を実行します。

移行する項目	入力するコマンド
特定の LIF	`network interface migrate`
ノードのすべてのデータ LIF とクラスタ管理 LIF	`network interface migrate-all`
ポートに接続していないすべての LIF です	`network interface migrate-all -node <node> -port <port>`

次の例は、SVM上の `vs0`というLIFをの `node0b`ポートに `e0d`移行する方法を示してい `datalif1`ます。

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

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

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

LIFをホームポートにリバートします。

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のホームポートを使用できない場合、LIFは現在のポートに残り、リバートされません。

タスクの内容

- 自動リバートオプションを設定する前にLIFのホームポートをup状態にした場合、LIFはホームポートに戻りません。
- 「auto-revert」オプションの値をtrueに設定しないかぎり、LIFは自動的にリバートされません。
- LIFをホームポートにリバートするには、「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、使用するインターフェイス（System ManagerまたはCLI）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します。*

手順

1. Network > Overview > Network Interfaces *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*> Revert *を選択します ⋮ 。
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、* Revert *を選択します。

CLI

- CLIを使用してLIFをホームポート*にリバートします

ステップ

LIFをホームポートに手動または自動でリバートします。

ホームポートへの LIF のリバートの方法	入力するコマンド
シユトウ	`network interface revert -vserver vserver_name -lif lif_name`
自動	`network interface modify -vserver vserver_name -lif lif_name -auto-revert true`

ONTAP 9.8 以降：正しく設定されていないクラスタ **LIF** からリカバリします

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るが、Cluster IPspaceに設定されているすべてのポートがCluster IPspaceに設定されている他のポートに到達できない場合、クラスタを作成できません。

タスクの内容

スイッチクラスタで、クラスタ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`コマンドが次のエ

ラーで失敗することがあります。

```
Not all local cluster ports have reachability to one another.
Use the "network port reachability show -detail" command for more details.
```

コマンドの結果では `network port show`、クラスタLIFが設定されたポートに接続されているために、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、コマンドの結果から、`network port `reachability show -detail`相互に接続されていないポートが特定されます。

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
```

2. クラスタLIFが設定されていないポートをクラスタ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
```

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。

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

使用中のLIFは削除できません。

手順

1. 次のコマンドを使用して、削除するLIFを「Administratively Down」にマークします。

```
network interface modify -vserver vserver_name -lif lif_name -status
-admin down
```

2. コマンドを使用し `network interface delete`て、1つまたはすべてのLIFを削除します。

削除の対象	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 LIFs	`network interface delete -vserver vserver_name -lif *`

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. コマンドを使用し `network interface show`て、LIFが削除されたことを確認します。

ONTAP仮想IP（VIP）LIFの設定

一部の次世代データセンターでは、サブネット間でLIFをフェイルオーバーする必要があるレイヤ3（IP）ネットワークメカニズムが使用されています。ONTAPは、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ために、仮想IP（VIP）データLIFと関連するルーティングプロトコルであるBorder Gateway Protocol（BGP）をサポートしています。

タスクの内容

VIPデータLIFは、どのサブネットにも属さず、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 々 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がデータトラフィックを伝送するため、すべての負荷が単一のアダプタおよび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）を使用してピアルータにアドバタイズされます。

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やサブネットをまたいで LIF を移動できます。各 VIP データ LIF の現在の場所が BGP を通じてルータに通知されるため、 VIP データ LIF をネットワークのどのサブネットにもフェイルオーバーできます。
- アグリゲートスループット： VIP データ LIF は、同時に複数のサブネットまたはポートに対して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アグリゲートスループットをサポートできます。

Border Gateway Protocol（BGP;ボーダーゲートウェイプロトコル）のセットアップ

VIP LIFを作成する前に、BGPを設定する必要があります。BGPは、VIP LIFの存在をピアルータ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、BGPピアグループを使用したデフォルトルート自動化がオプションで提供され、設定が簡素化されます。

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、属性をに `true`設定し `-use-peer-as-next-hop`ます。デフォルトでは、この属性はです `false`。

静的ルートが設定されている場合でも、自動化されたデフォルトルートよりも静的ルートが優先されます。

開始する前に

設定されたAutonomous System Number（ASN；自律システム番号）のBGP接続をBGP LIFから受け入れるようにピアルータを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を処理しません。したがって、クラスタにルートアップデートを送信しないようにピアルータを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ようになるまでの時間が短縮され、ONTAP内の内部メモリ使用量が削減されます。

タスクの内容

BGPをセットアップするには、必要に応じてBGP設定を作成し、BGP LIFを作成し、BGPピアグループを作成します。ONTAPは、最初のBGPピアグループが特定のノードに作成されると、デフォルト値を使用してデフォルトのBGP設定を自動的に作成します。

BGP LIFは、ピアルータとのBGP TCPセッションの確立に使用されます。ピアルータの場合、BGP LIFはVIP LIFに到達するためのネクストホップです。BGP LIFのフェイルオーバーは無効になっています。BGPピアグループは、そのピアグループが使用するIPspace内のすべてのSVMのVIPルートをアドバタイズします。ピアグループで使用されるIPspaceはBGP LIFから継承されます。

セッションを保護するために、ONTAP 9ピアグループでMD5認証がサポートされるようになりました。MD5がイネーブルの場合、BGPセッションは許可されたピア間でのみ確立および処理されるため、許可されていないアクターによるセッションの中断を防ぐことができます。

コマンドと `network bgp peer-group modify`コマンドに次のフィールドが追加されまし `network bgp peer-group create`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ると、セキュリティを強化するためにMD5シグニチャを使用してBGPピアグループを設定できます。MD5認証の使用には、次の要件が適用されます。

- パラメータを指定できるのは、パラメータがに設定されて `true`いる場合 `-md5-enabled`のみ `-md5-secret`です。
- MD5 BGP認証をイネーブルにする前に、IPSecをグローバルにイネーブルにする必要があります。BGP LIFにはアクティブなIPsec設定は必要ありません。を参照してください "IP Security（IPsec）のネットワーク上での暗号化の設定"。
- NetAppでは、ONTAPコントローラでMD5を設定する前に、ルータにMD5を設定することを推奨します。

ONTAP 9 .9.1以降では、次のフィールドが追加されました。

- `-asn`OR `-peer-asn` (4バイトの値)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ています。
- `-med`

- `-use-peer-as-next-hop`

パス優先順位付けのためのMulti-Exit Discriminator（MED）サポートを使用して、高度なルート選択を行うことができます。MEDは、トラフィックに最適なルートを選択するようにルータに指示するBGPアップデートメッセージのオプション属性です。MEDは符号なし32ビット整数（0～4294967295）です。小さい値が推奨されます。

ONTAP 9 .8以降では、次のフィールドがコマンドに追加されてい `network bgp peer-group`ます。

- `-asn-prepend-type`
- `-asn-prepend-count`
- `-community`

これらのBGP属性を使用すると、BGPピアグループのASパス属性およびコミュニティ属性を設定できます。

ONTAPは上記のBGP属性をサポートしていますが、ルータはこれらの属性を尊重する必要はありません。NetAppでは、ルータでサポートされているアトリビュートを確認し、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、ルータが提供するBGPのマニュアル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：次のいずれかの操作を実行して、クラスタの BGP 設定を作成するか、デフォルトの BGP 設定を変更します。

   a. BGP設定を作成します。

   ```
   network bgp config create -node {node_name | local} -asn <asn_number>
   -holdtime
   <hold_time> -routerid <router_id>
   ```

   - `-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付き10進32ビット値を受け入れます。NetAppでは、一意性が保証されるノード管理IP（v4）アドレスを使用することを推奨しています `<router_id>`。
   - ONTAP BGPは32ビットASN番号をサポートしますが、サポートされるのは標準10進表記のみです。プライベートASNでは4259840001ではなく65000.1などのドット付きASN表記はサポートされません。

   2バイトASNのサンプル：

   ```
   network bgp config create -node node1 -asn 65502 -holdtime 180
   -routerid 1.1.1.1
   ```

4バイトASNのサンプル：

```
network bgp config create -node node1 -asn 85502 -holdtime 180 -routerid
1.1.1.1
```

a. デフォルトのBGP設定を変更します。

```
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。.8以降では、ONTAP 9 for BGPは2バイトの非負整数をサポートしています。これは16ビットの数値です（使用可能な値は1～65534です）。.9.1以降では、ONTAP 9 for BGPは4バイトの非負整数（1～4294967295）をサポートしています。デフォルトのASNは65501です。ASN 23456は、4バイトのASN機能を通知しないピアとのONTAPセッション確立用に予約されています。
- `<hold_time>`保持時間を秒単位で指定します。デフォルト値は180sです。

> ONTAPでサポートされるグローバル、 `<hold_time>`、、およびは `<router_id>`1つだけです。これは、 `<asn_number>`複数のIPspaceに対してBGPを設定する場合でも同様です。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、Virtual Routing and Forwarding（VRF；仮想ルーティング/転送）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IPspaceの場合、SVM名はクラスタ名です。追加のIPspaceの場合、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>
```

BGP LIFのサービスポリシー、または「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 `default-route-announce`。

```
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する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。

例 1 ：自動デフォルトルートのないピアグループを作成する

この場合、管理者はBGPピアへのスタティック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
```

例 2 ：自動デフォルトルートを使用して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
```

例3：MD5を有効にして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をイネーブルにして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進キーを使用した例：

```
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
0x746573742073656372657400
```

文字列を使用した例：

```
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あと、コマンドを実行すると、仮想イーサネットポート（v0a..v0z、v1a…で始まるポート）が表示され `network port show`ます。このインターフェイスのMTUは常に1500で報告されます。トラフィックに実際に使用されるMTUは、トラフィックが送信されるタイミングで決定される物理ポート（BGP LIF）から取得されます。

仮想**IP**（**VIP**）データ**LIF**を作成する

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）を使用してピアルータにアドバタイズされます。

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の発信VIPトラフィック用に、BGPルータまたはBGP LIFのサブネット内のそ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。
- 発信VIPトラフィックが使用可能なすべてのルートを利用できるように、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がイネーブルになっていない場合、すべての発信VIPトラフィックは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
```

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 `network interface create`ます。

デフォルトでは、VIPデータLIFは、システムによってIPspaceごとに作成される「vip」という名前のブロードキャストドメインに属します。VIPブロードキャストドメインは変更できません。

VIPデータLIFは、IPspaceのBGP LIFをホストしているすべてのポートで同時に到達できます。ローカルノードにVIPのSVMに対するアクティブなBGPセッションがない場合、VIPデータLIFは、そのSVMに対してBGPセッションが確立されているノードの次の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セッションのステータスがup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
```

あるノードのSVMのBGPステータスがの場合、 `down`VIPデータLIFは、そのSVMのBGPステータスがupになってい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ステータスが設定されている場合は `down、VIPデータLIFをどこでもホストできず、LIFステータスがdownになります。

BGPの管理用コマンド

5以降では、コマンドを使用してONTAPでONTAP 9 `network bgp`セッションを管理します。

BGP設定を管理します。

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ピアグループを管理します。

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を使用した**BGP**ピアグループの管理

ONTAP 9 .16.1以降では、既存のピアグループでMD5認証をイネーブルまたはディセーブルにできます。

既存のBGPピアグループでMD5をイネーブルまたはディセーブルにすると、BGP接続が終了し、MD5設定の変更を適用するために再作成されます。

状況	使用するコマンド
既存のBGPピアグループでMD5をイネーブルにする	`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をディセーブルにする	`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"

ネットワーク負荷の分散

Balanceネットワークの概要

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できます。その結果、LIFとポートの利用率がバランスよくなるため、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を選択し、使用可能なすべてのポート（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は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要求を転送し、ネットワークトラフィックとポートリソースの可用性（CPU使用率、スループット、開いている接続など）に基づいて最も負荷の低い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には次の利点があります。

- 新しいクライアント接続は、使用可能なリソース全体に分散されます。
- 特定のSVMをマウントするときに使用するLIFが手動操作なしで決定されます。
- DNSロードバランシングは、NFSv3、NFSv4、NFSv4.1、SMB 2.0、SMB 2.1、SMB 3.0、S3をサポートしています。

DNSロードバランシングの仕組み

クライアントは、 LIF に関連付けられた IP アドレス、または複数の IP アドレスに関連付けられたホスト名を指定することにより、 SVM をマウントします。デフォルトでは、すべての LIF のワークロードのバランスが取れるように、サイト規模の DNS サーバによってラウンドロビン方式で LIF が選択されます。

ラウンドロビン方式のロードバランシングでは、 LIF のいくつかが過負荷になることがあります。そのため、 SVM でホスト名の解決を取り扱う DNS のロードバランシングゾーンを使用するオプションがあります。DNS ロードバランシングゾーンを使用すると、新しいクライアント接続が使用可能なリソース間でバランスよく配分されるため、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、クラスタ内の DNS サーバであり、すべての LIF の負荷を動的に評価して、負荷を適切に割り当てる LIF を返します。ロードバランシングゾーンでは、 DNS が負荷に基づいてそれぞれの LIF に重み（メトリック）を割り当てます。

すべての LIF に、ポートの負荷とホームノードの CPU 利用率に基づいて重みが割り当てられます。DNS クエリでは、負荷が低いポートの LIF から優先的に返されます。重みは手動で割り当てることもできます。

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数）に基づいてLIFを動的に選択できます。ロードバランシングゾーンはデータLIFの作成時に作成できます。

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フォワーダを設定する必要があります。

条件付き転送を使用するDNSロードバランシングの設定の詳細については、NetAppサポートサイトの技術情報アーティクルを参照してください"clustered Data ONTAP での DNS ロードバランシングの設定方法"。

タスクの内容

- どのデータLIF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ある必要があり、ゾーン名は次の要件を満たしている必要があります。
  - 最大文字数は256文字です。
  - ピリオドを少なくとも1つ含める必要があります。
  - 最初と最後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。

ステップ

`network interface create`コマンドでオプションを指定し `dns-zone`て、DNSロードバランシングゾーンを作成します。

ロードバランシングゾーンがすでに存在する場合は、LIFがロードバランシングゾーンに追加されます。コマンドの詳細については、を参照して "ONTAPコマンド リファレンス"ください。

次の例は、LIF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 `lif1`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に対するLIFの追加または削除

仮想マシン（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。また、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。
- 1つのLIFが属することができるDNSロードバランシングゾーンは1つだけです。
- LIFが別 々 のサブネットに属している場合は、各サブネット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。

タスクの内容

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、LIFは自動的にDNSロードバランシングゾーンに追加されます。

ステップ

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	入力するコマンド
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`
1 つの 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 を削除します	`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のすべてのLIFを削除することで、そのゾーンからSVMを削除できます。

DNSサービスの設定（ONTAP 9.8以降）

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。

タスクの内容

Active Directory統合DNSサーバには、ドメインLDAPサーバと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、ホストに関する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、使用するネームサービスとその順序を決定します。hostsデータベースでサポートされる2つのネームサービスは、filesと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プロセスおよびsecdプロセスのDNSネームサービスの統計を表示するには、統計UI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でデフォルトの設定が使用されています。

   `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DNSネームサービスが設定されている必要があります。セキュアなDDNSを使用する場合は、Active Directory統合DNSネームサーバを使用し、SVM用にNFSサーバまたはSMBサーバまたはActive Directoryアカウントを作成しておく必要があります。

タスクの内容

完全修飾ドメイン名（FQDN）は一意である必要があります。

完全修飾ドメイン名（FQDN）は一意である必要があります。

- NFSの場合、コマンドで `vserver services name-service dns dynamic-update`に指定した値 `-vserver-fqdn`がLIFに登録された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 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更新に関する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準拠のFQDN名を使用してください。詳細については、を参照してください "RFC 1123"。

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
   ```

   カスタマイズした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
   ```

DNSサービスの設定（ONTAP 9.7以前）

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。

タスクの内容

Active Directory統合DNSサーバには、ドメインLDAPサーバと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、ホストに関する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、使用するネームサービスとその順序を決定します。hostsデータベースでサポートされる2つのネームサービスは `files`、と `dns`です。

SMBサーバを作成する前に、がソースの1つであることを確認する必要があります `dns`。

mgwdプロセスおよびsecdプロセスのDNSネームサービスの統計を表示するには、統計UIを使用します。

手順

1. 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 `hosts`。

   この例では、hostsネームサービスデータベースでデフォルトの設定が使用されています。

   ```
   vserver services name-service ns-switch show -vserver vs1 -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
   ```

   a. 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
      ```

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コマンドは `name-service dns create`設定の自動検証を実行し、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。

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DNSネームサービスが設定されている必要があります。セキュアなDDNSを使用する場合は、Active Directory統合DNSネームサーバを使用し、SVM用にNFSサーバまたはSMBサーバまたはActive Directoryアカウントを作成しておく必要があります。

タスクの内容

完全修飾ドメイン名（FQDN）は一意である必要があります。

- NFSの場合、コマンドで `vserver services name-service dns dynamic-update`に指定した値 `-vserver-fqdn`がLIFに登録された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 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更新に関する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準拠のFQDN名を使用してください。詳細については、を参照してください "RFC 1123"。

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
   ```

   カスタマイズした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
```

動的DNSサービスの設定

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DNSネームサービスが設定されている必要があります。セキュアなDDNSを使用する場合は、Active Directory統合DNSネームサーバを使用し、SVM用にNFSサーバまたはSMBサーバまたはActive Directoryアカウントを作成しておく必要があります。

タスクの内容

一意の FQDN を指定する必要があります。

DDNS更新に関する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
   ```

   カスタマイズした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
   ```

ホストメイカイケツ

ホストメイカイケツノカイヨウ

ONTAP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ファイルを設定できます。

外部DNSサーバを使用する場合は、新規または変更されたDNS情報をストレージシステムからDNSサーバに自動的に送信する動的DNS（DDNS）を設定できます。動的DNS更新を使用しない場合、新しいシステムがオンラインになったとき、または既存のDNS情報が変更されたときに、識別されたDNSサーバにDNS情報（DNS名とIPアドレス）を手動で追加する必要があります。このプロセスには時間がかかり、エラーが発生し

やすくなります。ディザスタリカバリ時に手動設定を行うと、長時間のダウンタイムが発生する可能性があります。

ホスト名解決に使用するDNSの設定

ホスト情報を取得するには、DNSを使用してローカルまたはリモートのソースにアクセスします。これらのソースの一方または両方にアクセスするように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る必要があります。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する必要があります。

ONTAPでは、UNIXシステムのファイルに相当するテーブルにネームサービス設定情報が格納されます `/etc/nsswitch.conf`。

外部DNSサーバを使用してホスト名解決用にSVMとデータLIFを設定する

コマンドを使用して、SVMでDNSを有効にし、ホスト名解決にDNSを使用するように設定でき `vserver services name-service dns`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

ホスト名検索にサイト規模のDNSサーバが使用できる必要があります。

単一点障害を回避するには、複数のDNSサーバを設定する必要があります。 `vserver services name-service dns create`入力したDNSサーバ名が1つだけの場合は、コマンドによって警告が表示されます。

タスクの内容

SVMでの動的DNSの設定の詳細については、を参照してください動的DNSサービスの設定。

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
```

> コマンドは `vserver services name-service dns create`設定の自動検証を実行し、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. コマンドを使用して、ネームサーバのステータスを検証し `vserver services name-service dns check`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、を参照してください"ONTAP 9 .6以降のLIFとサービスポリシー"。

ホスト名解決のための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

環境内のホストマッピングに使用するネームサービス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内のエントリを、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変更します。

```
vserver services name-service ns-switch modify -vserver vs1 -database
hosts -sources files,dns
```

hostsテーブルの管理（クラスタ管理者のみ）

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、および表示できます。SVM管理者は、割り当てられたSVMのホスト名エントリのみを設定できます。

ローカルホスト名エントリの管理用コマンド

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 `vserver services name-service dns hosts`。

DNSホスト名エントリを作成または変更する場合は、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します	`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`

コマンドの詳細については `vserver services name-service dns hosts` 、を参照して "ONTAPコマンド リファレンス"ください。

ネットワークのセキュリティを確保

連邦情報処理標準（**FIPS**）を使用したネットワークセキュリティの設定

ONTAPは、すべてのSSL接続について、連邦情報処理標準（FIPS）140-2に準拠しています。ONTAPでは、SSL FIPSモードをオンまたはオフにしたり、SSLプロトコルをグローバルに設定したり、RC4などの弱い暗号を無効にしたりできます。

デフォルトでは、次のコマンドを使用して、ONTAPのSSLはFIPS準拠を無効にし、SSLプロトコルを有効にして設定されます。

- TLSv1.3（ONTAP 9 .11.1以降）
- TLSv1.2
- TLSv1.1
- TLSv1

SSL FIPSモードが有効な場合、ONTAPからONTAPの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通信では、SSL用のFIPS準拠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、ホストキーの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以降では、ホストキーアルゴリズムのサポートが変更されています。

ONTAP リリース	サポートされているキータイプ	サポートされていないキータイプです

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

FIPSを有効にする前に、サポートされているキーアルゴリズムがない既存のSSH公開鍵アカウントをサポートされているキータイプで再設定する必要があります。そうしないと、管理者認証が失敗します。

詳細については、を参照してください "SSH公開鍵アカウントの有効化"。

SSL FIPSモードの設定の詳細については、のマニュアルページを参照して `security config modify`ください。

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お勧めします。SSL FIPSモードが有効な場合、ONTAPからONTAPの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通信では、SSL用のFIPS準拠の暗号が使用されます。

FIPSが有効な場合、RSAキーの長さが4096の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 -interface SSL -is-fips-enabled true
   ```

3. 続行するかどうかを尋ねられたら、 `y`
4. 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つずつ手動でリブートします。ONTAP 9.9.1以降では、リブートは必要ありません。

例

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 -interface SSL -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
```

FIPSの無効化

古いシステム構成を実行していて、ONTAPを下位互換性のある方法で設定したい場合は、FIPSが無効になっている場合にのみSSLv3を有効にできます。

手順

1. advanced権限レベルに切り替えます。

   ```
   set -privilege advanced
   ```

2. FIPSを無効にするには、

   ```
   security config modify -interface SSL -is-fips-enabled false
   ```

3. 続行するかどうかを尋ねられたら、と入力し `y`ます。
4. 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リブートします。ONTAP 9.9.1以降では、リブートは必要ありません。

例

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 -interface SSL -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

クラスタ全体で現在のセキュリティ設定が実行されているかどうかを確認できます。

手順

1. クラスタ内の各ノードを1つずつリブートします。

   すべてのクラスタノードを同時にリブートしないでください。クラスタ内のすべてのアプリケーションで新しいセキュリティ設定が実行されるようにするには、リブートが必要です。また、FIPSのオン/オフモード、プロトコル、および暗号に対するすべての変更を行うには、リブートが必要です。

2. 現在の準拠ステータスを表示します。

   ```
   security config show
   ```

```
security config show

          Cluster                                                  Cluster
Security
Interface FIPS Mode  Supported Protocols     Supported Ciphers Config
Ready
--------- ---------- ---------------------- -----------------
----------------
SSL       false      TLSv1_2, TLSv1_1, TLSv1 ALL:!LOW:!aNULL:  yes
                                             !EXP:!eNULL
```

IPSec転送中暗号化の設定

IPセキュリティを使用する準備

ONTAP 9 .8以降では、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

を保護するオプションが用意されています。IPSecは、ONTAPで使用できる複数の転送中データ暗号化または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によって維持されているインターネット標準です。IPレベルでネットワークエンドポイント間を流れるトラフィックに対して、データの暗号化と整合性、および認証を提供します。

ONTAPでは、ONTAPとさまざまなクライアント（NFS、SMB、iSCSIプロトコルを含む）の間のすべてのIPトラフィックがIPsecによって保護されます。プライバシーとデータの整合性に加えて、ネットワークトラフィックはリプレイ攻撃や中間者攻撃などのいくつかの攻撃から保護されます。ONTAPでは、IPsecトランスポートモードの実装が使用されます。Internet Key Exchange（IKE;インターネットキーエクスチェンジ）プロトコルバージョン2を利用して、IPv4またはIPv6を使用してONTAPとクライアント間でキーマテリアルをネゴシエートします。

クラスタでIPSec機能を有効にすると、ネットワークでは、ONTAPセキュリティポリシーデータベース（SPD）にさまざまなトラフィック特性に一致するエントリが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、認証方式など）にマッピングされます。各クライアントには、対応するSPDエントリも必要です。

トラフィックの種類によっては、別の転送中データ暗号化オプションを使用することをお勧めします。たとえば、NetApp SnapMirrorおよびクラスタピアリングトラフィックの暗号化には、一般に、IPsecではなくTransport Layer Security（TLS）プロトコルが推奨されます。これは、ほとんどの状況でTLSの方がパフォーマンスが向上するためです。

関連情報

- "インターネット技術タスクフォース"
- "RFC 4301：『Security Architecture for the Internet Protocol』"

ONTAP IPsec実装の進化

IPsecは最初にONTAP 9で導入されました。8.実装は、次のように進化し、改善され続けています。

> ⓘ 特定のONTAPリリース以降に導入された機能は、特に記載がないかぎり、以降のリリースでもサポートされます。

ONTAP 9 .16.1

暗号化や整合性チェックなどの暗号化処理のいくつかは、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、を参照してください IPSecハードウェアオフロード機能 。

ONTAP 9 12.1

IPSecフロントエンド・ホスト・プロトコルは、MetroCluster IPおよびMetroClusterファブリック接続構成でサポートされます。MetroClusterクラスタで提供されるIPSecのサポートはフロントエンドホストトラフィックに限定され、MetroClusterクラスタ間LIFではサポートされません。

ONTAP 9 10.1

証明書は、事前共有キー（PSK）に加えて、IPsec認証にも使用できます。PSK .10.1より前のONTAP 9バージョンでは、PSKのみが認証でサポートされていました。

ONTAP 9 .9.1

IPsecで使用される暗号化アルゴリズムはFIPS 140-2に準拠しています。これらのアルゴリズムは、ONTAPのNetApp暗号モジュールによって処理され、FIPS 140-2の検証が行われます。

ONTAP 9.8

IPsecのサポートは、最初はトランスポートモードの実装に基づいて利用可能になります。

IPSec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は、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取り付けられたNetwork Interface Controller（NIC;ネットワークインターフェイスコントローラ）カードにオフロードすることができます。このハードウェアオフロードオプションを使用すると、IPsecで保護される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ハードウェアオフロード機能を使用する前に、いくつかの要件を考慮する必要があります。

サポートされるイーサネットカード

ストレージノードに取り付けて使用する必要があるのは、サポートされているイーサネットカードだけです。ONTAP 9 .16.1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イーサネットコントローラ CX7）
- X60243A（4p、10G/25Gイーサネットコントローラ CX7）

クラスタスコープ

IPSecハードウェアオフロード機能は、クラスタに対してグローバルに設定されます。たとえば、コマンドは`security ipsec config`クラスタ内のすべてのノードに適用されます。

一貫した構成

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、オフロードに対応したNICで一部のLIFが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。

アンチリプレイを無効にする

IPsecアンチリプレイ保護は、ONTAP（デフォルト設定）およびIPsecクライアントでディセーブルにする必要があります。ディセーブルにしない場合、フラグメンテーションおよびマルチパス（冗長ルート）はサポートされません。

制限事項

IPsecハードウェアオフロード機能を使用する前に、いくつかの制限事項を考慮する必要があります。

IPv6

IPバージョン6は、IPsec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。IPv6は、IPsecソフトウェア実装でのみサポートされます。

拡張シーケンス番号

IPSec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

IPSecハードウェアオフロード機能では、リンクアグリゲーションはサポートされません。そのため、ONTAP CLIのコマンドで管理するインターフェイ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 `network port ifgrp`。

ONTAP CLIでの設定のサポート

ONTAP 9 .16.1では、次に説明するように、3つの既存のCLIコマンドが更新され、IPSecハードウェアオフロード機能がサポートされています。詳細については、も参照してください"ONTAPでのIPセキュリティの設定"。

ONTAPコマンド	更新
`security ipsec config show`	ブーリアンパラメータは `Offload Enabled`、現在のNICオフロードステータスを示します。
`security ipsec config modify`	パラメータを `is-offload-enabled`使用して、NICオフロード機能を有効または無効にできます。
`security ipsec config show-ipsecsa`	インバウンドおよびアウトバウンドトラフィックをバイトおよびパケット単位で表示するために、4つの新しいカウンタが追加されました。

ONTAP REST APIでの設定のサポート

ONTAP 9 .16.1では、次に説明するように、2つの既存のREST APIエンドポイントが更新され、IPsecハードウェアオフロード機能がサポートされます。

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ました。

を含むONTAP REST APIの詳細については、ONTAP自動化に関するドキュメントを参照し "ONTAP REST APIの新機能"てください。の詳細については、ONTAP自動化に関するドキュメントも参照して "IPSecエンドポイント"ください。

ONTAPでのIPセキュリティの設定

ONTAPクラスタで転送中のIPSec暗号化を設定してアクティブにするには、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、を確認してください"IPセキュリティを使用する準備"。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IPSecを有効にする

クラスタでIPSecを有効にすると、転送中もデータが継続的に暗号化されてセキュアになるようにすることができます。

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
   ```

   結果にが含まれている場合は `IPsec Enabled: false`、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
   ```

   IPSecハードウェアオフロード機能は、ブーリアンパラメータを使用してイネーブルにできます `is-offload-enabled`。

3. 検出コマンドを再度実行します。

   ```
   security ipsec config show
   ```

   結果にが含まれるようになりまし `IPsec Enabled: true`た。

証明書認証を使用した**IPSec**ポリシーの作成の準備

認証に事前共有キー（PSK）のみを使用し、証明書認証を使用しない場合は、この手順を省略できます。

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. 相互認証で使用したすべてのCA証明書（ONTAP側CAとクライアント側CAの両方を含む）をONTAP証明書管理にインストールします（ONTAPの自己署名ルートCAの場合など）。

   サンプルコマンド
   ```
   cluster::> security certificate install -vserver svm_name -type server-ca
   -cert-name my_ca_cert
   ```

2. インストールされているCAが認証時にIPsec CA検索パス内にあることを確認するには、コマンドを使用して、IPsecモジュールにONTAP証明書管理CAを追加し `security ipsec ca-certificate add`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。この証明書の発行者CAが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. コマンドを使用し `security ipsec policy create`て次の処理を行います
   a. ONTAP転送に参加する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 IPアドレスに接続するクライアントIPアドレスを選択します。

      クライアントは、事前共有キー（PSK）を使用してInternet Key Exchangeバージョン2（IKEv2）をサポートしている必要があります。

   c. オプション。トラフィックを保護するために、上位レイヤプロトコル（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、きめ細か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`、それぞれ、 `local-ports`および `remote-ports`です。

      ONTAP IPアドレスとクライアントIPアドレス間のすべてのトラフィックを保護するには、この手順を省略します。すべてのトラフィックを保護することがデフォルトです。

   d. 目的の認証方式のパラメータにPSKまたは公開キーインフラストラクチャ（PKI）を入力します `auth-method`。
      i. PSKを入力する場合は、パラメータを指定し、<enter>キーを押して事前共有キーの入力と確認を求めるプロンプトを表示します。

         `local-identity`ホストとクライアントの両方で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、パラメータと `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、、 `local-identity`、 `remote-identity`パラメータも入力する必要があり`cert-name`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が予想される場合は、特別なIDを入力し `ANYTHING`ます。

```
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が一致するIPsecポリシーを設定し、認証クレデンシャル（PSKまたは証明書）が両側に配置されるまで、IPトラフィックはクライアントとサーバの間を流れません。

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 / 証明書を使用する認証方式では、ローカルとリモートの両方のIDが必須です。IDはONTAPとクライアントそれぞれの証明書でどのIDが認定されているかを示すもので、検証プロセスで使用されます。リモートIDが不明な場合、または多数の異なるIDである可能性がある場合は、特別なIDを使用し `ANYTHING`ます。

タスクの内容

ONTAP内では、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名を指定できます。

手順

1. 既存のSPD ID設定を変更するには、次のコマンドを使用します。

```
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を利用する必要があ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1つのSPDエントリを使用すれば十分です。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、NetApp IPsecの複数クライアント構成を使用することを推奨します。

タスクの内容

ONTAPでは、IPSecを有効にした状態で、1つの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。これには、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（192.168.134.0/24など）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、をサブネット形式で指定する必要があります `remote-ip-subnets`。また、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 `remote-identity`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設定を許可 *

  ソースIPアドレスに関係なくすべてのクライアントがSVMのIPsec対応IPアドレスに接続できるようにするには `0.0.0.0/0`、フィールドにワイルドカードを指定し `remote-ip-subnets`ます。

  また、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 `remote-identity`ます。証明書認証の場合は、と入力できます `ANYTHING`。

  また、ワイルドカードを使用する場合は `0.0.0.0/0`、使用する特定のローカルまたはリモートポート番号を設定する必要があります。たとえば、 `NFS port 2049`です。

  手順

  a. 複数のクライアントに対してIPsecを設定するには、次のいずれかのコマンドを使用します。

     i. サブネット設定*を使用して複数のIPsecクライアントをサポートする場合：

     ```
     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. [すべてのクライアントの設定を許可する]*を使用して複数のIPsecクライアントをサポートする場合は、次の手順を実行します。

     ```
     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統計を表示します。

ネゴシエーションを使用すると、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を確立できます。IPsec SAは、実際のデータ暗号化および復号化作業を行うために、両方のエンドポイントにインストールされます。statistics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、コマンドでいくつかの新しいカウンタが表示され `security ipsec config show-ipsecsa`ます。

コマンド例

IKE SAサンプルコマンド：

```
security ipsec show-ikesa -node hosting_node_name_for_svm_ip
```

ipsec saコマンドおよび出力例：

```
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コマンドおよび出力例：

```
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
```

LIFのファイアウォールポリシーを設定する

ファイアウォールを設定すると、クラスタのセキュリティが強化され、ストレージシステムへの不正アクセスを防止できます。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、およびクラスタ間LIFに対して特定のIPサービスセットへの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の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されていました。これには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、基盤となるファイアウォールのポートは開かれません。代わりに、LIF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も、ファイアウォールポリシーからLIFのサービスポリシーに移行するための対処は必要ありません。以前のONTAPリリースで使用していたファイアウォールポリシーと整合性のあるLIFのサービスポリシーが自動的に作成されます。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する場合は、それらのスクリプトをアップグレードしてカスタムサービスポリシーを作成する必要があります。

詳細については、を参照してください"ONTAP 9 .6以降のLIFとサービスポリシー"。

ファイアウォールポリシーを使用して、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できます。NFSやSMBなどのデータプロトコル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は次の方法で管理できます。

- ファイアウォールサービスの有効化と無効化
- 現在のファイアウォールサービス設定の表示
- 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
- 論理インターフェイスへのファイアウォールポリシーの適用
- 既存のポリシーとまったく同じ新しいファイアウォールポリシーを作成する

  この機能は、同じSVM内で同様の特性を持つポリシーを作成する場合や、別のSVMにポリシーをコピーする場合に使用できます。

- ファイアウォールポリシーに関する情報の表示
- ファイアウォールポリシーで使用されるIPアドレスとネットマスクの変更
- LIFで使用され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されます。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を介したシステムアクセスに与える影響と、ファイアウォールポリシーをカスタマイズしてLIFのセキュリティを増減する方法を理解しておく必要があります。

コマンドまたは `network interface modify`コマンドを使用してLIFを設定する場合、 `network interface create`パラメータに指定した値 `-firewall-policy`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。

多くの場合、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。また、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。使用可能な管理サービスプロトコルには、SSH、HTTP、HTTPS、Telnet、NTP、NDMP、NDMPS、RSH、DNS、およびSNMPがあります。

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設定さ `""`れており、変更することはできません。

次の表に、LIFの作成時にロール（ONTAP 9 .5以前）またはサービスポリシー（ONTAP 9 .6以降）に応じて各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	適用先のLIF
管理	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 LIF 、 SVM 管理 LIF 、ノード管理 LIF
管理- 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
クラスタ間	HTTPS、NDMP、ndmps	任意のアドレス（0.0.0.0/0 ）	すべてのクラスタ間LIF
データ	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サービスをリッスンするポートにマッピングします。

portmapサービスはONTAP 9 .3以前では常にアクセス可能であり、ONTAP 9 .4ではONTAP 9 .6を使用して設定可能になり、ONTAP 9 .7から自動的に管理されるようになりました。

- ONTAP 9 .3以前では、サードパーティ製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）に常にアクセスできました。
- ONTAP 9 .4~lif.6 ONTAP 9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ています。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きます。
- ポートマップサービスは、 ONTAP 9.4 ～ ONTAP 9.6* のファイアウォールで設定可能です

このトピックの残りの部分では、ONTAP 9 .4～ONTAP 9 .6リリースの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。

構成によっては、特定のタイプのLIF（通常は管理LIFとクラスタ間LIF）で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へのアクセスを禁止することもできます。

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。コマンド構文全体については、を参照してください "ONTAPコマンド リファレンス"。

ファイアウォールポリシーを作成して**LIF**に割り当てる

LIFの作成時に、デフォルトのファイアウォールポリシーが各LIFに割り当てられます。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。

タスクの内容

- `intercluster`、、 `cluster`、またはの `mgmt`名前 `data`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 `policy`。

  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または変更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、すべてのサービスタイプで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アドレスを使用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有効なアドレスのリストに::/0というIPv6ワイルドカードが含まれます。

- 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場合は、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サービスを許可する必要があります。

  デフォルトでは、ファイアウォールポリシーは `intercluster`すべてのIPアドレス（IPv6の場合は0.0.0.0/0、または：：：/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、またはインタークラスタ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、許可されるリストに各インタークラスタLIFのIPアドレスを追加し、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` `management-ssh`、HTTPSおよびSSH管理アクセスにLIFサービスとLIFサービスを使用できます。

手順

1. 特定のSVMのLIFで使用できる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`*

   このコマンドを複数回使用して、ファイアウォールポリシーに複数のネットワークサービスと各サービスで許可されるIPアドレスのリストを追加できます。

2. 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 `system services firewall policy show`。
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. 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 -fields firewall-policy`。

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の管理用コマンド

ファイアウォールサービスを管理するにはコマンド、ファイアウォールポリシーを管理する `network interface modify`にはコマンド、 `system services firewall policy`LIFのファイアウォール設定を管理するにはコマンドを使用し `system services firewall`ます。

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か、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`
ファイアウォールポリシーをLIFに適用する	`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ている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`
既存のポリシーとまったく同じ新しいファイアウォールポリシーを作成する	`system services firewall policy clone`
LIFで使用され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`

詳細については `system services firewall policy` `network interface modify`、の各コマンドのマニュアルページを参照して `system services firewall`"ONTAP 9コマンドリファレンス"ください。

QoSマーキング（クラスタ管理者のみ）

QoSの概要

ネットワーク サービス品質（QoS）マーキングを使用すると、ネットワークの状態に基づいて各トラフィック タイプに優先順位を付け、ネットワーク リソースを効率的に利用できます。各IPspaceでサポートされるトラフィック タイプについて、送信IPパケットのDifferentiated Services Code Point（DSCP）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 _ サービスマーキングの品質）は、 IPspace 、プロトコル、DSCP の値を指定することで有効になります。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マーキングをイネーブルにするときに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。

QoSマーキング値を変更します。

IPspace ごとに、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。

ステップ

コマンドを使用して、QoSマーキング値を変更します `network qos-marking modify`。

- パラメータは `-ipspace`、QoSマーキングエントリを変更するIPspaceを指定します。
- パラメータは `-protocol`、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。 `network qos-marking modify`のマニュアルページに、プロトコルの指定可能な値が記載されています。
- パラメータは `-dscp`、Differentiated Services Code Point（DSCP）値を指定します。指定できる値の範囲は、 0~63 です。
- パラメータは `-is-enabled`、パラメータで指定したIPspace内の指定したプロトコルのQoSマーキングを有効または無効にする場合に使用し `–ipspace`ます。

次のコマンドは、デフォルトの IPspace の NFS プロトコルに対して 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、デフォルトの IPspace の NFS プロトコルに対して DSCP 値を 20 に設定します。

```
network qos-marking modify -ipspace Default -protocol NFS -dscp 20
```

QoSマーキング値を表示します。

IPspace ごとに、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。

ステップ

コマンドを使用して、QoSマーキング値を表示します `network qos-marking show`。

次のコマンドは、デフォルトの IPspace 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.
```

SNMPの管理（クラスタ管理者のみ）

SNMPの概要

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、を参照してください "TR-4220 ：『 SNMP Support in Data ONTAP 』"。

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、IPv4とIPv6の両方のデータを表示するIPv6（RFC 2465）、TCP（RFC 4022）、UDP（RFC 4113）、およびICMP（RFC 2466）MIBをサポートしています。

ONTAPでは、ファイル内のオブジェクト識別子（OID）とオブジェクトの簡略名の簡単な相互参照も提供されています `traps.dat`。

> ONTAP の MIB および「 traps.dat 」ファイルの最新バージョンは、NetApp Support Siteから入手できます。ただし、サポートサイトにあるファイルのバージョンが、お使いのONTAPバージョンのSNMP機能に必ずしも対応しているとは限りません。これらのファイルは、最新バージョンのONTAPのSNMP機能を評価するのに役立ちます。

SNMPトラツフ

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、およびユーザ定義の3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で定義されている動作しきい値または障害を定期的にチェックできます。しきい値に達するか障害が検出されると、SNMPエージェントはトラップホストにイベントを警告するメッセージ（トラップ）を送信します。

> ONTAPはSNMPv1トラップをサポートしており、ONTAP 9 SNMP.1トラップを開始しています。ONTAPでは、SNMPv2cトラップおよびINFORMはサポートされていません。

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ディセーブルになっています。トラップを有効にするには、コマンドを使用する必要があり `system snmp authtrap` ます。詳細については、次のマニュアルページを参照してください。 "ONTAPコマンド リファレンス"

ビルトイン**SNMP**トラップ

ビルトイントラップはONTAPで事前定義されており、イベントが発生すると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。diskFailedShutdown、cpuTooBusy、volumeNearlyFullなどのトラップは、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によって識別されます。

SNMPコミュニティを作成してLIFに割り当てる

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ことで、データLIFでや `snmpget`などのコマンドを実行でき `snmpwalk`ます。

タスクの内容

- 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。

  SNMPv1とSNMPv2cは、SNMPコミュニティを作成すると有効になります。

- ONTAPでは、読み取り専用コミュニティがサポートされます。
- デフォルトでは、データLIFに割り当てられている「data」ファイアウォールポリシーでは、SNMPサービスがに設定されて `deny`います。

  データSVMのSNMPユーザを作成するときに、新しいファイアウォールポリシーを作成してSNMPサービスをに設定する必要があります `allow`。

  ONTAP 9 10.1以降では、ファイアウォールポリシーが廃止され、LIFのサービスポリシーに全面的に置き換えられました。詳細については、を参照してください "LIFのファイアウォールポリシーを設定する"。

- 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でのクエリにはNetAppのルート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. コマンドを使用して、SNMPコミュニティを作成し `system snmp community add`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. 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 `system services firewall policy` show。

   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でのみ許可されています）。

```
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. コマンドを使用して、サービス `system services firewall policy create`による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作成し `snmp`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. firewall-policy パラメータを指定して「 network interface modify 」コマンドを使用し、ファイアウォールポリシーをデータ LIF に適用します。

   次のコマンドは、新しい「data1」ファイアウォールポリシーをLIF「datalif1」に割り当てます。

```
network interface modify -vserver vs1 -lif datalif1 -firewall-policy
data1
```

クラスタでの**SNMPv3**ユーザの設定

SNMPv3は、SNMPv1やSNMPv2cに比べてセキュアなプロトコルです。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ようにSNMPv3ユーザを設定する必要があります。

ステップ

「security login createコマンド」を使用してSNMPv3ユーザを作成します。

次の情報を入力するように求められます。

- エンジン ID ：デフォルトで、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には認証機能が含まれています。この機能を選択すると、コマンドを呼び出すときに、ユーザの名前、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	説明
エンジン ID	-e engineID	SNMP エージェントのエンジン ID 。デフォルト値はlocal engineIDです（推奨）。
securityName の略	-u 名	ユーザ名は 32 文字以内にする必要があります。
authProtocol の略	• a ｛ none	md5
sha	SHA-256 ｝	認証タイプには、 none 、 md5 、 SHA 、または SHA-256 を指定できます。
authKey	• パスフレーズ	8 文字以上の長さのパスフレーズ
セキュリティレベル	-l ｛ authNoPriv	AuthPriv
noAuthNoPriv ｝	セキュリティレベルには、「 Authentication 、 No Privacy 」、「 Authentication 、 Privacy 」、「 No Authentication 、 No Authentication 」のいずれかを指定できます。 プライバシーなし。	privProtocol の略
-x ｛ none	des	aes128 ｝
プライバシープロトコルには、 none 、 des 、または aes128 を指定できます	プライベートパスワード	-X パスワード

さまざまなセキュリティレベルの例

次の例は、さまざまなセキュリティレベルで作成したSNMPv3ユーザが、SNMPクライアント側のコマンド（など）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てい `snmpwalk`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、5.3.1以降を使用する必要があります `snmpwalk`。

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 admin
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、authNoPriv SNMPv3ユーザをFIPSモードで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 admin
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"
```

SNMP通知を受信する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 ）を受信するトラップホスト（ 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または 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および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。
- ONTAP 9.1 以降のバージョンでは、トラップホストの作成時に、事前定義されているユーザベースのセキュリティモデル（ USM ）の認証とプライバシーのクレデンシャルを指定しておく必要があります。

ステップ

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、少なくとも 1 つの 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ときのみです。

次のコマンドは、 yyy.example.com という新しい SNMPv3 トラップホストを既知の USM ユーザとともに追加します。

```
system snmp traphost add -peer-address yyy.example.com -usm-username
MyUsmUser
```

次のコマンドは、トラップホストの IPv6 アドレスを指定して、そのホストを追加します。

```
system snmp traphost add -peer-address 2001:0db8:1:1:209:6bff:feae:6d67
```

SNMP ポーリングのテスト

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。

タスクの内容

クラスタをポーリングするには、などのサードパーティのコマンドを使用する必要があり `snmpwalk`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では、CLIコマンドを使用し `snmpwalk -v version -c community_stringip_address_or_host_name system`てMIB（管理情報ベース）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。要求された 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コマンドを使用し `snmpwalk -v version -c community_stringip_address_or_host_name system`てMIB（管理情報ベース）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。要求された 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コマンドを使用し `snmpwalk -v 3 -a MD5 or SHA -l authnopriv -u username -A passwordip_address_or_host_name system`てMIB（管理情報ベース）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。要求された 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の管理用コマンド

SNMP、トラップ、およびトラップホストを管理するには、コマンドを使用し `system snmp`ます。SVMのSNMPユーザを管理するには、コマンドを使用し `security`ます。SNMPトラップに関連するイベントを管理するには、コマンドを使用し `event`ます。

SNMPの設定用コマンド

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`

SNMP v1、**v2c**、および**v3**ユーザを管理するコマンド

状況	使用するコマンド
SNMPユーザの設定	`security login create`
SNMP ユーザを表示します	`security snmpusers and security login show -application snmp`
SNMP ユーザを削除する	`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コミュニティの管理用コマンド

状況	使用するコマンド
1 つの SVM 、またはクラスタのすべての SVM に読み取り専用（ ro ）コミュニティを追加する	`system snmp community add`
1 つまたはすべてのコミュニティを削除します	`system snmp community delete`

すべてのコミュニティのリストを表示します。	`system snmp community show`

SVMはSNMP標準の一部ではないため、データLIFでのクエリにはNetAppのルートOID（1.3.6.1.4.1.789）を含める必要があります。たとえば、のように指定します。 `snmpwalk -v 2c -c snmpNFS 10.238.19.14 1.3.6.1.4.1.789`

SNMPオプション値を表示するコマンド

状況	使用するコマンド
クラスタの連絡先、連絡先の場所、クラスタがトラップを送信するように設定されているかどうか、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など、すべてのSNMPオプションの現在の値を表示する	`system snmp show`

SNMPトラップおよびトラップホストの管理用コマンド

状況	使用するコマンド
クラスタから送信されるSNMPトラップを有効にする	`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`
クラスタ内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します。	`system snmp traphost show`

SNMPトラップに関連するイベントの管理用コマンド

状況	使用するコマンド

SNMP トラップ（ビルトイン）が生成されたイベントを表示します	`event route show` SNMP関連のイベントのみを表示するには、パラメータを使用し `-snmp-support true`ます。 パラメータを使用して `instance -messagename <message>`、イベントが発生した理由と対処方法の詳細を表示します。 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 トラップ履歴レコードのリストを表示します。 SNMP トラップに送信されたイベント通知です	`event snmphistory show`
SNMP トラップ履歴レコードを削除します	`event snmphistory delete`

、、およびの各コマンドの詳細については `system snmp security event` 、を参照して "ONTAPコマンドリファレンス"ください。

SVMのルーティングを管理します。

SVMルーティングの概要

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つだけ設定することを推奨します。システム停止を回避するには、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デフォルトルートが到達できることを確認する必要があります。詳細については、技術情報アーティクルを参照してください。 "SU134 ： clustered ONTAP で誤ったルーティング設定が行われるとネットワークアクセスが中断される可能性があります"

静的ルートを作成します。

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使用するかを制御できます。

SVMに関連付けられた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。

ステップ

コマンドを使用し `network route create`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
```

マルチパスルーティングの有効化

複数のルートが1つの宛先に対して同じメトリックを持つ場合、発信トラフィック用に選択されるルートは1つだけです。これにより、発信トラフィックの送信に他のルートが使用されなくなります。マルチパスルーティングをイネーブルにすると、使用可能なすべてのルートをメトリックに応じてロードバランシングできます。ECMPルーティングでは、同じメトリックの使用可能なルート間でロードバランシングが行われます。

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
   ```

   クラスタ内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っている。

```
network options multipath-routing modify -is-enabled true
```

ONTAPで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。

ステップ

コマンドを使用し `network route delete`て、静的ルートを削除します。

リンクhttp://docs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。NetApp .com /us-en/ONTAP -CLI/ network-route-delete.html[`network route`^]コマンドを参照してください。

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、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
```

ルーティング情報を表示します。

クラスタの各 SVM のルーティング設定に関する情報を表示することができます。この情報は、クライアントアプリケーションまたはサービスとクラスタ内のノード上の LIF との接続に関連するルーティングの問題を診断するのに役立ちます。

手順

1. コマンドを使用し `network route show`て、1つ以上のSVM内のルートを表示します。次の例は、 vs0 という SVM に設定されているルートを表示しています。

```
network route show
  (network route show)
Vserver             Destination     Gateway         Metric
------------------- --------------- --------------- ------
vs0
                    0.0.0.0/0       172.17.178.1    20
```

2. コマンドを使用し `network route show-lifs`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。

   次の例は、 vs0 という SVM が所有しているルートと 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
```

3. コマンドを使用して `network route active-entry show`、1つ以上のノード、SVM、サブネットに設定されているルート、または指定したデスティネーションに一致するルートを表示します。

   次の例は、特定の SVM に設定されている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.
```

ルーティングテーブルからの動的ルートの削除

IPv4 と 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。デフォルトでは、ダイナミックルートは300秒後に削除されます。動的ルートを維持する時間を変更する場合は、タイムアウト値を変更できます。

タスクの内容

0~65 、 535 秒のタイムアウト値を設定できます。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、無効なルートの永続性が原因で接続が切断されるの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の場合：

     ```
     network tuning icmp show
     ```

   - IPv6の場合：

     ```
     network tuning icmp6 show
     ```

2. タイムアウト値を変更します。
   - IPv4の場合：

     ```
     network tuning icmp modify -node node_name -redirect-timeout
     timeout_value
     ```

   - IPv6の場合：

     ```
     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の場合：

     ```
     network tuning icmp show
     ```

   - IPv6の場合：

     ```
     network tuning icmp6 show
     ```

ネットワーク情報の表示

ネットワーク情報の概要を表示する

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できます。ONTAP 9 .8以降では、ネットワークについてSystem Managerに表示されるデータもダウンロードできます。

この情報は、ネットワーク設定の再設定時やクラスタのトラブルシューティング時に役立ちます。

クラスタ管理者は、ネットワーク情報をすべて表示できます。SVM管理者は、割り当てられているSVMに関する情報のみを表示できます。

System Managerの_リスト表示_に情報を表示するときに*[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。

- このリストは、カンマ区切り値（ 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。

ネットワークポート情報を表示します。

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。

タスクの内容

次の情報が表示されます。

- ノード名
- ポート名
- IPspaceメイ
- ブロードキャストドメイン名
- リンクステータス（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（1ギガビットまたは10ギガビット/秒）
- 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タグ情報（該当する場合）
- ポートのヘルスステータス（healthまたはdegraded）
- ポートがデグレードとマークされた理由

該当するデータがないフィールドの値はと表示されます（アクティブでないポートの二重モードの動作中や速度は表示されません）。 -

ステップ

コマンドを使用して、ネットワークポートの情報を表示します `network port show`。

各ポートの詳細情報を表示するには、パラメータを指定します。特定の情報を表示 `-instance`するには、パラメータを使用してフィールド名を指定し `-fields`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.
```

VLANに関する情報を表示する（クラスタ管理者のみ）

クラスタ内の特定の VLAN またはすべての VLAN の情報を表示できます。

タスクの内容

パラメータを指定すると、各VLANの詳細情報を表示できます `-instance`。特定の情報を表示するには、パラメータを使用してフィールド名を指定し `-fields`ます。

ステップ

コマンドを使用して、VLANに関する情報を表示します `network port vlan show`。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
```

インターフェイスグループ情報の表示（クラスタ管理者のみ）

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。

タスクの内容

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、またはシーケンシャル）
- インターフェイスグループの Media Access Control （ 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。集約されたポートがアクティブであるかどうか（すべてのポートがアクティブであるかどうか）、アクティブであるポートがないかどうか（一部のポートがアクティブであるかどうか）、アクティブでないかどうかを示します

ステップ

コマンドを使用して、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`。

各ノードの詳細情報を表示するには、パラメータを指定し `-instance`ます。特定の情報を表示するには、パラメータを使用してフィールド名を指定し `-fields`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の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: -
```

LIF情報を表示する

LIF に関する詳細情報を表示して、そ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。

タスクの内容

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 のステータスによって決まります。SVM が停止すると、 LIF の動作ステータスが 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

該当するデータがないフィールド（ステータスの詳しい情報がない場合など）については、と表示されます - 。

ステップ

network interface showコマンドを使用して、LIFの情報を表示します。

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
```

ルーティング情報を表示します。

SVM内のルートに関する情報を表示できます。

ステップ

表示するルーティング情報のタイプに応じて、該当するコマンドを入力します。

表示する情報	入力するコマンド
SVM の静的ルート	`network route show`
SVM の各ルートの LIF	`network route show-lifs`

パラメータを指定すると、各ルートの詳細情報を表示できます `-instance`。次のコマンドは、cluster-1のSVM内の静的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
```

DNSホストテーブルエントリを表示する（クラスタ管理者のみ）

DNS hosts テーブルエントリは、ホスト名と IP アドレスのマッピングです。クラスタ内のすべての SVM のホスト名およびエイリアス名と IP アドレスのマッピングを表示する

ことができます。

ステップ

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。

次の例は、ホストテーブルエントリを表示します。

```
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
```

コマンドを使用して、SVMでDNSを有効にし、ホスト名解決にDNSを使用するように設定でき `vserver services name-service dns`ます。ホスト名は外部DNSサーバを使用して解決されます。

DNSドメイン設定の表示

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。

ステップ

コマンドを使用して、DNSドメイン設定を表示します `vserver services name-service dns show`。

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
```

次のコマンドを実行すると、SVM vs1のDNS設定の詳細が表示されます。

```
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
```

フェイルオーバーグループに関する情報を表示する

フェイルオーバーグループに関する情報を表示することができます。これには、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が含まれます。

手順

1. 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 `network interface failover-groups show`。

   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に関する情報を表示します。

```
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
```

2. 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 `network interface failover-groups show`。

   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しい情報を表示します。

```
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. コマンドを使用して、すべてのLIFで使用されているフェイルオーバー設定を表示します `network interface show`。

   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
```

LIFのフェイルオーバーターゲットを表示します。

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かどうかを確認しなければならない場合があります。フェイルオーバールールを間違って設定しないように、 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。

タスクの内容

LIF のフェイルオーバーターゲットを表示すると、次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どうか
- 表示されたフェイルオーバーターゲットのポートが LIF に適しているかどうか
- 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 ）でないかどうか

ステップ

コマンドのオプションを `network interface show`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 `failover。

次のコマンドは、 2 ノードクラスタのすべての 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。行は `Failover Targets`、特定のLIFにおけるノードとポートの組み合わせの（優先順位の高い）リストを示しています。

```
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
```

ロードバランシングゾーンの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を表示することで、そのゾーンが正しく設定されているかどうかを確認できます。特定のLIFのロードバランシングゾーン、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。

ステップ

次のいずれかのコマンドを使用して、必要なLIFとロードバランシングの詳細を表示します。

表示する内容	入力するコマンド
特定のロードバランシングゾーンに属する 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とそれに対応するDNSゾーンのリストを表示します。

```
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
```

ONTAPのクラスタ接続を表示します。

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数を表示したりできます。クラスタ内のリスンしている接続をすべて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を表示する（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を表示して、特定のクライアントが使用し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。

タスクの内容

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。

ステップ

コマンドを使用して、ノードのアクティブな接続数をクライアント別に表示します `network connections active show-clients`。

リンクhttp://docs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。NetApp .com /us-en/ONTAP -CLI/ network-connections-active-show-clients.html[`network connections active show-clients`^]コマンドを参照してください。

```
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を表示する（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。

タスクの内容

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。

ステップ

コマンドを使用して、ノードのアクティブな接続数をプロトコル別に表示します `network connections active show-protocols`。

このコマンドの詳細については、マニュアルページを参照してください。

```
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を表示します（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。これは、クラスタ内のサービスの使用状況を比較するのに役立ちます。これは、ノードのプライマリワークロードを特定するのに役立ちます。

タスクの内容

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する。コマンドを使用して、ノードのアクティブな接続数をサービス別に表示します `network connections active show-services`。

このコマンドの詳細については、マニュアルページを参照してください。 "ONTAPコマンド リファレンス"

```
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**別にアクティブな接続を表示する

ノードおよびStorage Virtual Machine（SVM）別のLIF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。

タスクの内容

LIF別のアクティブな接続数は、次のような場合に役立ちます。

- 各LIFの接続数を比較して過負荷のLIFを特定する。
- 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。

ステップ

コマンドを使用して、SVMとノードのアクティブな接続数をLIF別に表示します `network connections active show-lifs`。

このコマンドの詳細については、マニュアルページを参照してください。 "ONTAPコマンド リファレンス"

```
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を表示します。

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、個 々 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。

タスクの内容

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。

ステップ

コマンドを使用して、クラスタ内のアクティブな接続数を表示します `network connections active show`。

このコマンドの詳細については、マニュアルページを参照してください"ONTAPコマンド リファレンス"。

次のコマンドは、ノードnode1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を表示する

クラスタ内のリスンしている接続に関する情報を表示して、特定のプロトコルおよびサービスの接続を受け入れているLIFとポートを確認できます。

タスクの内容

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。

ステップ

コマンドを使用して、ノードごとにリスンしている接続を表示します `network connections listening`

show。

```
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
```

ネツトワアクモンタイノシンタンヨウコマント

ネットワークの問題を診断するには、や `tcpdump`などのコマンドを使用し `ping, traceroute, ndp,`ます。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 `ping6`。

状況	入力するコマンド
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使用できます。
クラスタ内の各ノードおよびポートから検出された隣接デバイスに関する情報（リモートデバイスのタイプやデバイスプラットフォームなど）を表示する	`network device-discovery show`

ノードのCDP隣接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使用できます。
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使用できます。
クラスタ間ノードまたはクラスタ内ノード間のレイテンシとスループットを測定	`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、を参照して"パフォーマンス管理"ください。

これらのコマンドの詳細については、を参照して "ONTAPコマンド リファレンス"ください。

近接探索プロトコルによるネットワーク接続を表示します。

近接探索プロトコルによるネットワーク接続を表示します。

データセンターでは、近接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れらのネットワークインターフェイス間のネットワーク接続を表示できます。ONTAP では、 2 つの近接探索プロトコルとして、 Cisco Discovery Protocol （ CDP ）と Link Layer Discovery Protocol （ LLDP ）がサポートされます。

近接探索プロトコルを使用すると、ネットワーク内の直接接続されたプロトコル対応デバイスを自動的に検出し、その情報を表示できます。各デバイスは、ID、機能、および接続情報をアドバタイズします。この情報はイーサネットフレームでマルチキャストMACアドレスに送信され、隣接するすべてのプロトコル対応デバイスで受信されます。

2つのデバイスをネイバーにするには、各デバイスでプロトコルが有効になっており、正しく設定されている必要があります。検出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。ネイバーには、スイッチ、ルータ、ブリッジなどのプロトコル対応デバイスを含めることができます。ONTAPでは、2つの近接探索プロトコルがサポートされており、個別に使用することも一緒に使用することもできます

- シスコ検出プロトコル（ CDP ） *

CDPは、Cisco Systemsが開発した独自のリンク層プロトコルです。クラスタポートのONTAPでは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。

- リンク層検出プロトコル（ LLDP ） *

LLDPは、標準ドキュメントIEEE 802.1ABで指定されているベンダーに依存しないプロトコルです。すべてのポートに対して明示的にイネーブルにする必要があります。

CDPを使用したネットワーク接続の検出

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	説明
9.10.1以前	CDPは、クラスタスイッチヘルスモニタでも使用され、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的に検出します。
9.11.1以降	CDPは、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クラスタスイッチヘルスモニタでも使用されます。

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。そのため、ONTAPノードがCDPv1通知を送信すると、CDP対応の隣接デバイスがCDPv1通知を返します。

ノードでCDPを有効にする前に、次の点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通知を送受信するには、送信デバイスと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通知は一定の間隔で送信され、送信間隔を設定できます。
- 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パケットの最大サイズは1500バイトであるため、LIFが多数設定されたポートでは、隣接するスイッ

チで報告されるIPアドレスの一部しかありません。

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。

タスクの内容

オプションは `cdpd.enable`、ノードのポートでCDPを有効にするか無効にするかを制御します。

- ONTAP 9 .10.1以前の場合、onを指定すると、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を指定すると、クラスタ以外のポートとストレージ以外のポートでCDPが有効になります。
- ONTAP 9 .10.1以前の場合、offを指定すると非クラスタポートの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を指定すると、非クラスタポートとストレージポートでCDPが無効になります。クラスタポートでは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場合があります。

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。

CDP 設定を表示する対象	入力するコマンド
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	入力するコマンド
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

クラスタのノードのポートにCDP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。ネイバー情報を表示するには、コマンドを使用し `network device-discovery show -protocol cdp`ます。

タスクの内容

ONTAP 9 .10.1以前では、CDPはクラスタポートで常に有効になっているため、これらのポートのCDP隣接情報が常に表示されます。非クラスタポートの隣接情報を表示するには、非クラスタポートでCDPを有効にする必要があります。

ONTAP 9 .11.1以降では、クラスタポートとストレージポートのCDPは常に有効になっているため、それらのポートのCDP隣接情報が常に表示されます。非クラスタポートおよび非ストレージポートのネイバー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。

ステップ

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。

- このオプションの値は `cdpd.holdtime`、HAペアの両方のノードで同じに設定する必要があります。
- デフォルトの保持時間の値は180秒ですが、10~255秒の範囲の値を入力できます。
- 保持期限が切れる前にIPアドレスが削除された場合、CDP情報は保持期限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	入力するコマンド
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のすべてのポートでCDP保持時間を設定します。

保持時間を設定する対象	入力するコマンド
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通知の送信間隔を設定する

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節することができます。

- このオプションの値は `cdpd.interval`、HAペアの両方のノードで同じに設定する必要があります。
- デフォルトの間隔は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	入力するコマンド
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のすべてのポートについて、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	入力するコマンド
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。

タスクの内容

ONTAP 9 .10.1以前では、CDPはポートに対して常にイネーブルになっているため、これらのポートのトラフィックについては常にCDP統計情報が表示されます。ポートの統計情報を表示するには、CDPをポートでイネーブルにする必要があります。

ONTAP 9 .11.1以降では、クラスタポートとストレージポートのCDPは常に有効になっているため、これらのポートのトラフィックのCDP統計は常に表示されます。非クラスタポートまたは非ストレージポートの統計を表示するには、非クラスタポートまたは非ストレージポートでCDPを有効にする必要があります。

ステップ

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	入力するコマンド
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

一部のベンダースイッチではCDPがサポートされていません。 "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"詳細については、ナレッジベースの記事を参照してください。

この問題を解決するには、次の2つの方法があります。

- CDPを無効にし、LLDPを有効にします（サポートされている場合）。詳細については、を参照してください "LLDPを使用したネットワーク接続の検出" 。
- CDPアドバタイズメント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しま

す。

LLDPを使用したネットワーク接続の検出

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、隣接デバイスの表示、LLDPの設定値の調整（必要な場合）で構成されます。

ネイバーデバイスに関する情報を表示するには、スイッチおよびルータでもLLDPをイネーブルにする必要があります。

ONTAPは現在、次のType-Length-Value構造体（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以外のポートの場合：
  - シャーシIDは、ノード上のいずれかのポートの固定MACアドレスです。
  - port IDは、ノード上のそれぞれのポートのポート名です。
- CNAポートの場合：
  - シャーシIDとポートIDは、ノード上の各ポートのMACアドレスです。

ただし、これらのタイプのポートについては、クラスタで表示されるデータに一貫性があります。

LLDP仕様では、SNMP MIBを介した収集された情報へのアクセスが定義されています。ただし、ONTAPは現在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。

タスクの内容

LLDP .10.1以前の場合ONTAP 9は、 `lldp.enable`オプションでノードのポートでLLDPを有効にするか無効にするかを制御します。

- `on`すべてのポートでLLDPをイネーブルにします。
- `off`すべてのポートでLLDPをディセーブルにします。

LLDP.11.1以降の場合、ONTAP 9オプションは、 `lldp.enable`ノードの非クラスタポートおよび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ストレージポートでLLDPをイネーブルにします。
- `off`すべての非クラスタポートおよび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。
   - シングルノード： `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のすべてのポートでLLDPを有効または無効にします。

LLDPを有効または無効にする対象	入力するコマンド
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}`

   - シングルノード：

```
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。

ステップ

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準拠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の情報を表示します。出力には、指定したノードの各ポートに接続されているLLDP対応デバイスが表示されます。この `-protocol`オプションを省略すると、CDP対応デバイスも出力に表示されます。

```
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通知の送信間隔を調整する

LLDP通知は、一定の間隔でLLDPネイバーに送信されます。ネットワークトラフィックやネットワークトポロジの変化に応じて、LLDP通知の送信間隔を増減できます。

タスクの内容

IEEEが推奨するデフォルトの間隔は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通知の現在の間隔を表示します。
   - シングルノード：

     ```
     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のすべてのポートについて、LLDP通知の送信間隔を調整します。
   - シングルノード：

     ```
     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値を調整する

Time-To-Live（TTL）は、LLDP通知がLLDP準拠の隣接デバイスのキャッシュに格納される期間です。TTLは各LLDPパケットでアドバタイズされ、ノードがLLDPパケットを受信するたびに更新されます。TTLは発信LLDPフレームで変更できます。

タスクの内容

- TTLは計算された値(`lldp.xmit.interval`（送信間隔の積）と保持乗数(`lldp.xmit.hold`）に1を足したものです。
- デフォルトの保持乗数の値は4ですが、1～100の範囲の値を入力できます。
- したがって、IEEEが推奨するデフォルトのTTLは121秒ですが、送信間隔と保持乗数の値を調整することで、発信フレームの値を6秒から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を表示します。
   - シングルノード：

     ```
     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のすべてのポートで、保持の乗数を調整します。
   - シングルノード：

     ```
     run -node <node_name> options lldp.xmit.hold <hold_value>
     ```

   - すべてのノード：

     ```
     options lldp.xmit.hold <hold_value>
     ```

LLDP統計の表示またはクリア

各ノードのクラスタポートと非クラスタポートのLLDP統計を表示して、ネットワーク接続の潜在的な問題を検出できます。LLDP統計情報は、最後に消去された時点からの累積値です。

タスクの内容

LLDP.10.1以前の場合、ONTAP 9はクラスタポートで常に有効になっているため、これらのポートのトラフィックについては常にLLDP統計が表示されます。非クラスタポートの統計を表示するには、非クラスタポートでLLDPを有効にする必要があります。

LLDPはクラスタポートとストレージポートで常に有効になるため、LLDP統計はそれらのポートのトラフィックについて常に表示されますONTAP 9。非クラスタポートおよびストレージポートの統計情報を表示するには、非クラスタポートおよびストレージポートでLLDPを有効にする必要があります。

ステップ

ノードのすべてのポートの現在のLLDP統計を表示または消去します。

状況	入力するコマンド
LLDP統計を表示します	`run -node node_name lldp stats`
LLDP統計情報をクリアします	`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、クリア前のLLDP統計情報を表示します。出力には、統計情報が最後に消去されてから送受信されたパケットの合計数が表示されます。

```
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統計情報をクリアします。

```
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、次のLLDPアドバタイズメントが送信または受信されたあとに統計情報が蓄積され始めます。