# Network Management の略

ONTAP 9

NetApp
June 19, 2024

# 目次

# Network Management の略

## はじめに

### ネットワーク管理の概要

System ManagerまたはCLIを使用してストレージネットワークの基本的な管理を実行するには、次の情報を使用します。物理 / 仮想ネットワークポート（ VLAN およびインターフェイスグループ）の設定、 IPv4 と IPv6 を使用した LIF の作成、クラスタでのルーティングサービスとホスト解決サービスの管理、ロードバランシングを使用したネットワークトラフィックの最適化、 SNMP を使用したクラスタの監視が可能です。

特に記載がないかぎり、CLIの手順はONTAP 9のすべてのバージョンに適用されます。

各ONTAP 9リリースで使用できるネットワーク機能の影響については、を参照してください。 "ONTAP リリースノート"。

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できます。ONTAP 9.12以降では、ネットワークインターフェイスグリッドでLIFとサブネットの関連付けを表示できます。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"。

この新しいネットワーク可視化機能を使用すると、ホスト、ポート、 SVM 、ボリュームなど全体のネットワーク接続パスをグラフィカルインターフェイスに表示できます。

[ ネットワーク ]>[ 概要 *] を選択するか、またはを選択すると、グラフィックが表示されます → ダッシュボードの * ネットワーク * セクションから。

次のカテゴリのコンポーネントが図に示されています。

- 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 VMs
- データアクセスコンポーネント

各セクションには、ネットワーク管理タスクと設定タスクを実行するためにマウスを合わせるか、選択することができる詳細が表示されます。

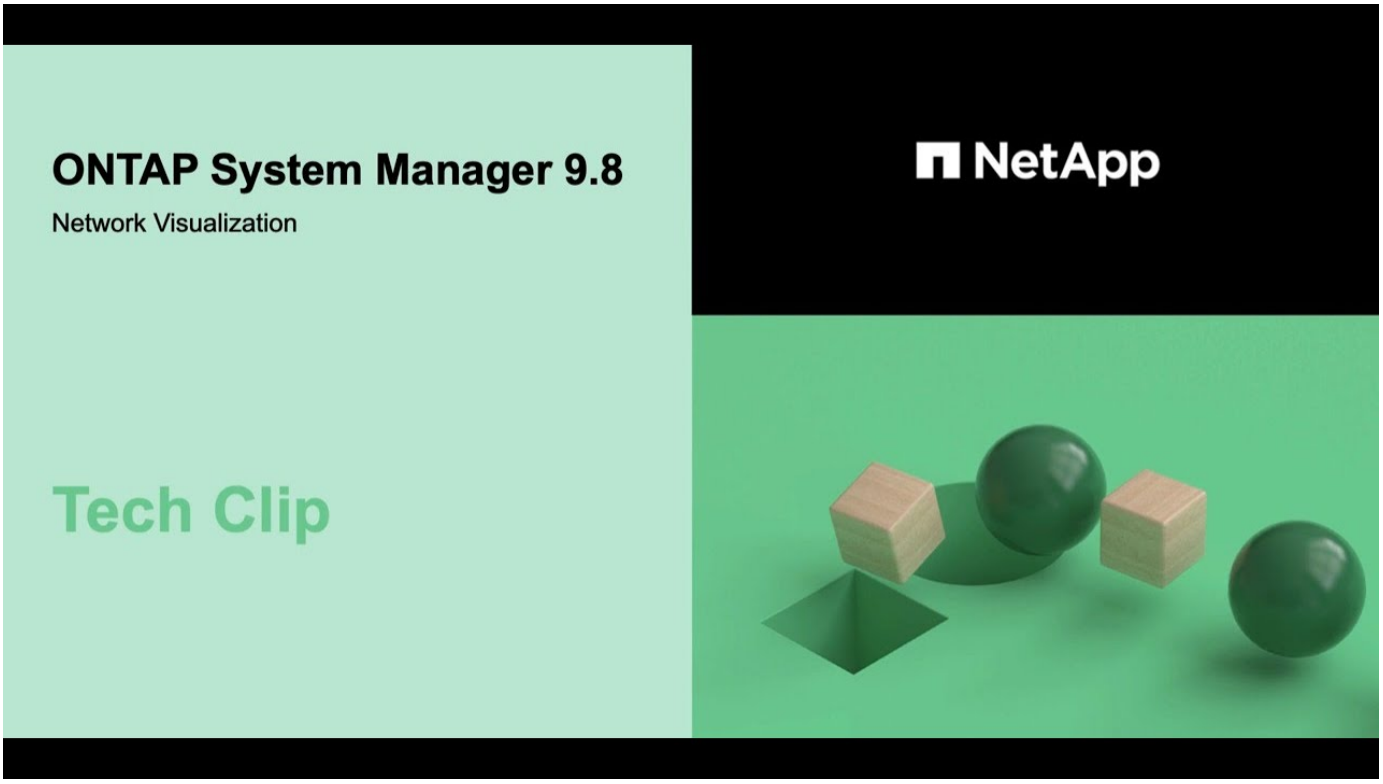
例

次の例は、グラフィックを操作して各コンポーネントの詳細を表示したり、ネットワークを管理するためのアクションを開始したりするさまざまな方法を示しています。

- ホストをクリックすると、ホストの設定（ポート、ネットワークインターフェイス、Storage VM、関連付けられてい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ると、ボリュームが選択されて詳細が表示されます。

- 過去 1 週間のパフォーマンスを表示するには、 iSCSI インターフェイスを選択してください。
- をクリックします ⋮ 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。
- 問題のあるコンポーネントの横に「 X 」と表示されている、ネットワークで問題が発生する可能性のある場所をすばやく特定します。

**System Manager** のネットワーク可視化に関するビデオ




## ONTAP 9.7x以前からのONTAPアップグレード後のネットワーク構成の確認

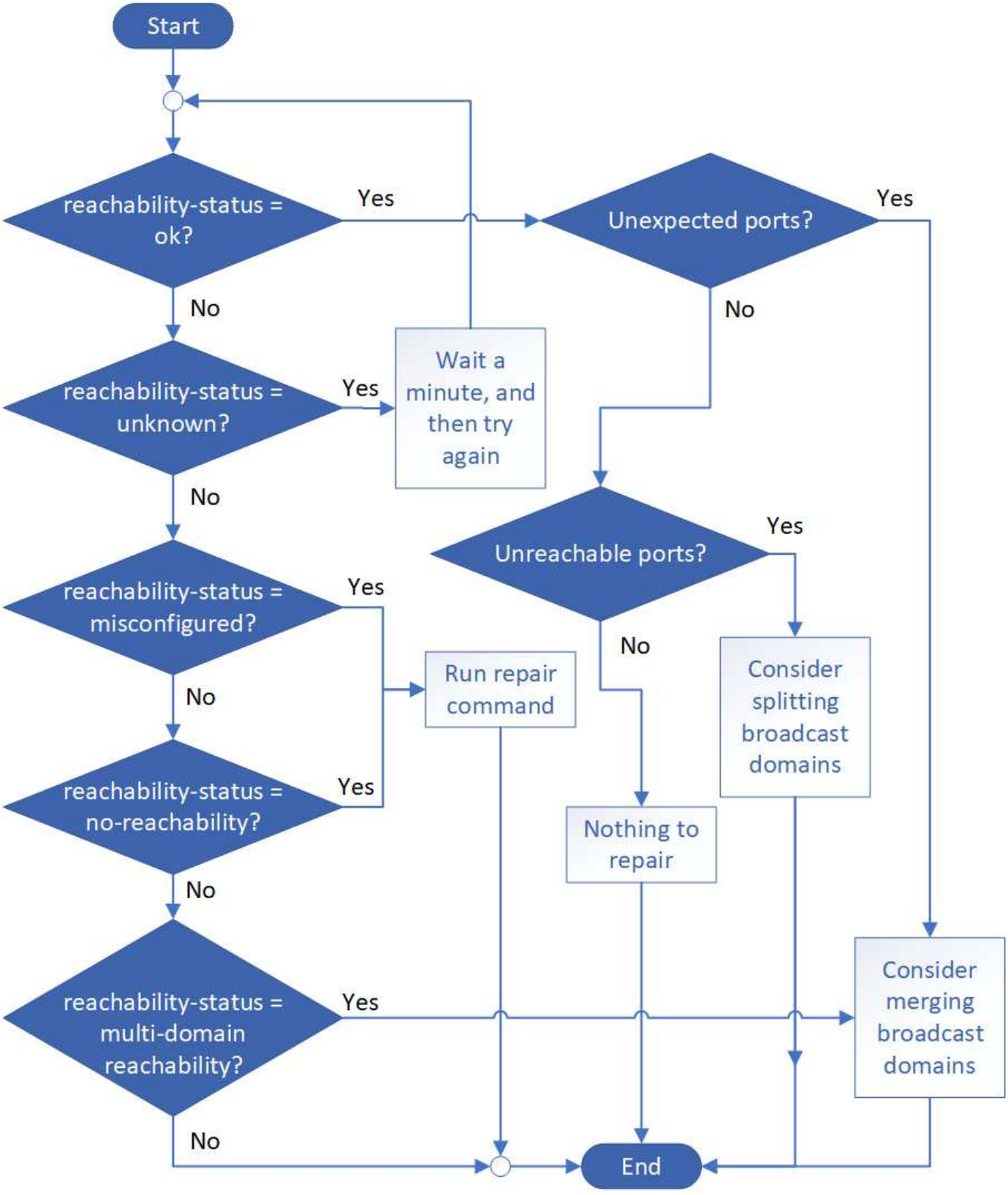
ONTAP 9.7x以前のバージョンからONTAP 9.8以降にアップグレードしたら、ネットワーク構成を確認する必要があります。アップグレード後、 ONTAP は自動的にレイヤ 2 の到達可能性を監視します。

ステップ

1. 各ポートに想定されるブロードキャストドメインへの到達可能性があることを確認します。

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

コマンド出力に到達可能性の結果が含まれています。次のデシジョンツリーとテーブルを使用して、到達可能性の結果（ reachable-status ）を理解し、次に何を実行するか（存在する場合）を決定します。




| プレゼンスステータス | 説明 |
| --- | --- |

| | |
|---|---|
| わかりました | 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。<br><br>reachable-status が「 OK 」であるのに、「予想外のポート」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、を参照してください "ブロードキャストドメインをマージします"。<br><br>reachable-status が「 OK 」であるが、「到達不能ポート」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、を参照してください "ブロードキャストドメインをスプリットします"。<br><br>reachable-status 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は、設定が正しいことを確認してください。 |
| 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。<br><br>ポートに到達できるかどうかを修復できます。次のコマンドを実行すると、ポートに到達できるブロードキャストドメインにポートが割り当てられます。<br><br>`network port reachability repair -node -port`<br><br>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します"。 |
| 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。<br><br>ポートに到達できるかどうかを修復できます。次のコマンドを実行すると、自動的に作成されたデフォルトの IPspace 内の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。<br><br>`network port reachability repair -node -port`<br><br>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します"。 |
| 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。<br><br>物理的な接続とスイッチの設定を調べて、正しくないか、またはポートに割り当てられているブロードキャストドメインを 1 つ以上のブロードキャストドメインにマージする必要があるかどうかを確認します。<br><br>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をマージします" または "ポートの到達可能性を修復します"。 |
| 不明です | 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。 |

ポートを修復したら、取り外された LIF や 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に何が起こったかを理解する必要もあります。 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します"。

# ネットワークコンポーネント

## 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設定することで、 ONTAP の持つ柔軟性とマルチテナンシー機能を活かせます。

クラスタのさまざまなネットワークコンポーネントを次に示します。

- 物理ポート

  Network Interface Card （ NIC ；ネットワークインターフェイスカード）と Host Bus Adapter （ HBA ；ホストバスアダプタ）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ファイバチャネル）を提供します。

  サイトの要件、スイッチの情報、ポートのケーブル接続の情報、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個別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のクライアントが、 IP アドレスの同じサブネット範囲内の重複した IP アドレスを使用してクラスタのデータにアクセスできるようになります。

- ブロードキャストドメイン

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

- サブネット

  サブネットはブロードキャストドメイン内に作成され、同じレイヤ 3 サブネットに属する IP アドレスのプールを含んでいます。この IP アドレスプールを使用すると、 LIF の作成時の IP アドレスの割り当てが簡単になります。

- 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 、クラスタを対象とした管理 LIF 、ノードを対象とした管理 LIF 、クラスタ間 LIF 、およびクラスタ 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、ノードを対象とした管理 LIF 、クラスタを対象とした管理 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

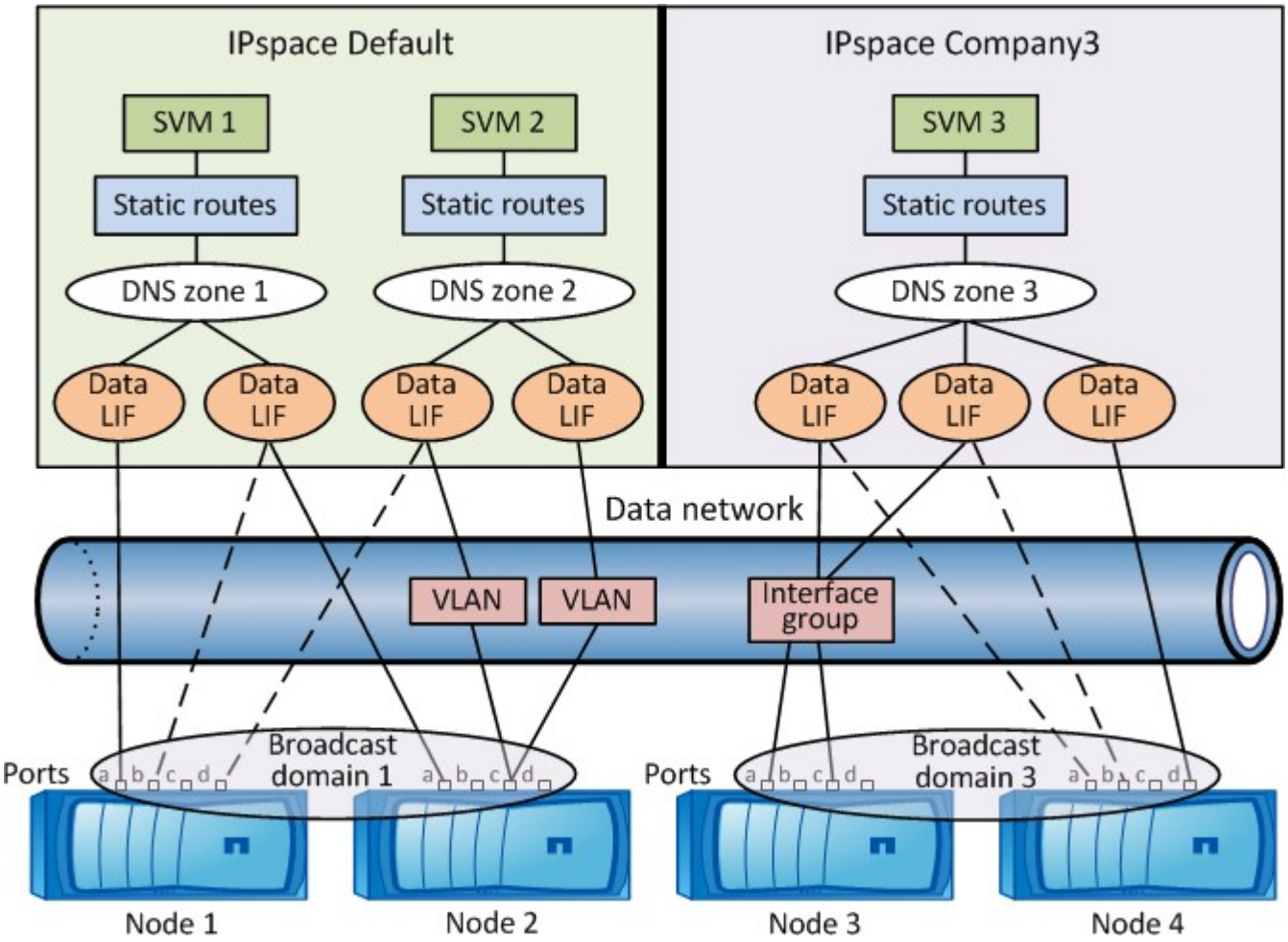
  DNS ゾーンは LIF の作成時に指定でき、クラスタの DNS サーバ経由でエクスポートされる LIF の名前を提供します。複数の LIF で同じ名前を共有できるため、 DNS ロードバランシング機能を使用し、その名前の IP アドレスを負荷に従って分散させることができます。

  SVM には、複数の DNS ゾーンを設定できます。

- ルーティング

  各 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。

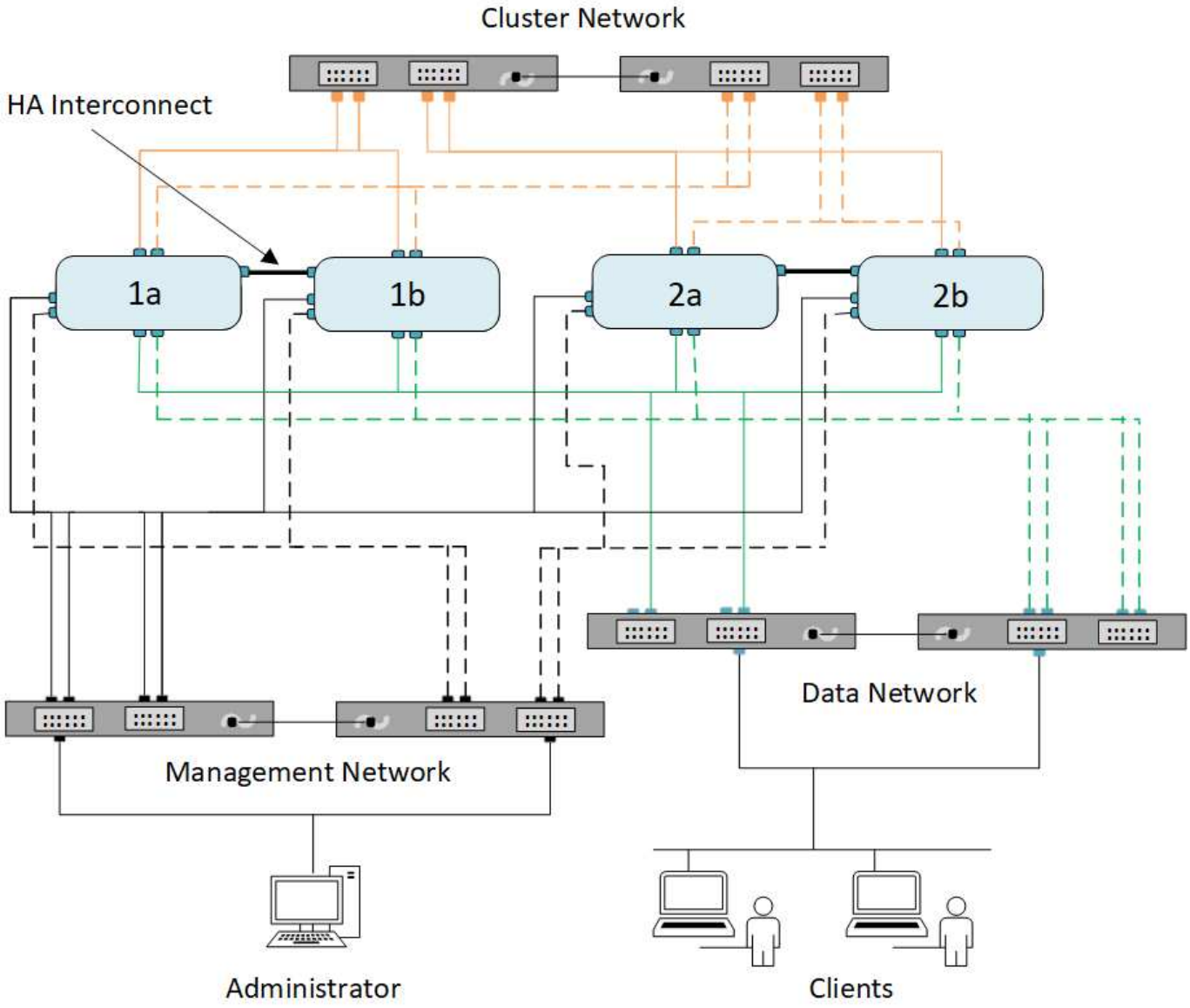


# ネットワークのケーブル配線のガイドライン

## ネットワークのケーブル配線のベストプラクティスでは、クラスタ、管理、データの各ネットワークにトラフィックを分離しています。

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。オプションですが、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から分離することを推奨します。分離されたネットワークを維持することで、パフォーマンスの向上、管理の容易さ、ノードへのセキュリティアクセスと管理アクセスの向上を実現できます。

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




ネットワークのケーブル配線を行うときは、次のガイドラインに従う必要があります。

- 各ノードは、 3 つの個別のネットワークに接続する必要があります。

  1 つは管理用、もう 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）トラフィックのフローを向上させるために、各ノードへのデータネットワーク接続を複数確立することができます。
- クラスタを作成する際、データネットワーク接続はなくてもかまいませんが、クラスタインターコネクト接続は必ず必要です。
- 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配線の詳細については、を参照してください "AFF および FAS システムドキュメントセンター" および "Hardware Universe"。

## ブロードキャストドメイン、フェイルオーバーグループ、フェイルオーバーポリシー間の関係

### 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に障害が発生した場合にテイクオーバーするポートを決定します。

ブロードキャストドメインには、同じレイヤ 2 イーサネットネットワークで到達できるすべてのポートがリストされます。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が、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。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された場合でも、元のポートから到達可能なすべてのローカルホストおよびリモートホストに到達できる可能性があるため、ブロードキャストドメインの一般的な到達可能性特性は LIF にとって重要です。

フェイルオーバーグループは、ブロードキャストドメイン内のポートを定義し、それぞれのポートが LIF のフェイルオーバー対象となります。各ブロードキャストドメインには、ポートをすべて含むフェイルオーバーグループが 1 つあります。このフェイルオーバーグループにはブロードキャストドメインのすべてのポートが含まれており、 LIF に対して推奨される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に同じリンク速度のポートのフェイルオーバーグループなど、定義したサブセットを減らして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場合に、 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。フェイルオーバーポリシーは、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みなされます。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、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その LIF のフェイルオーバーポリシーを適用することによって決まります。

LIF のフェイルオーバーターゲットを表示するには、次の CLI コマンドを使用します。

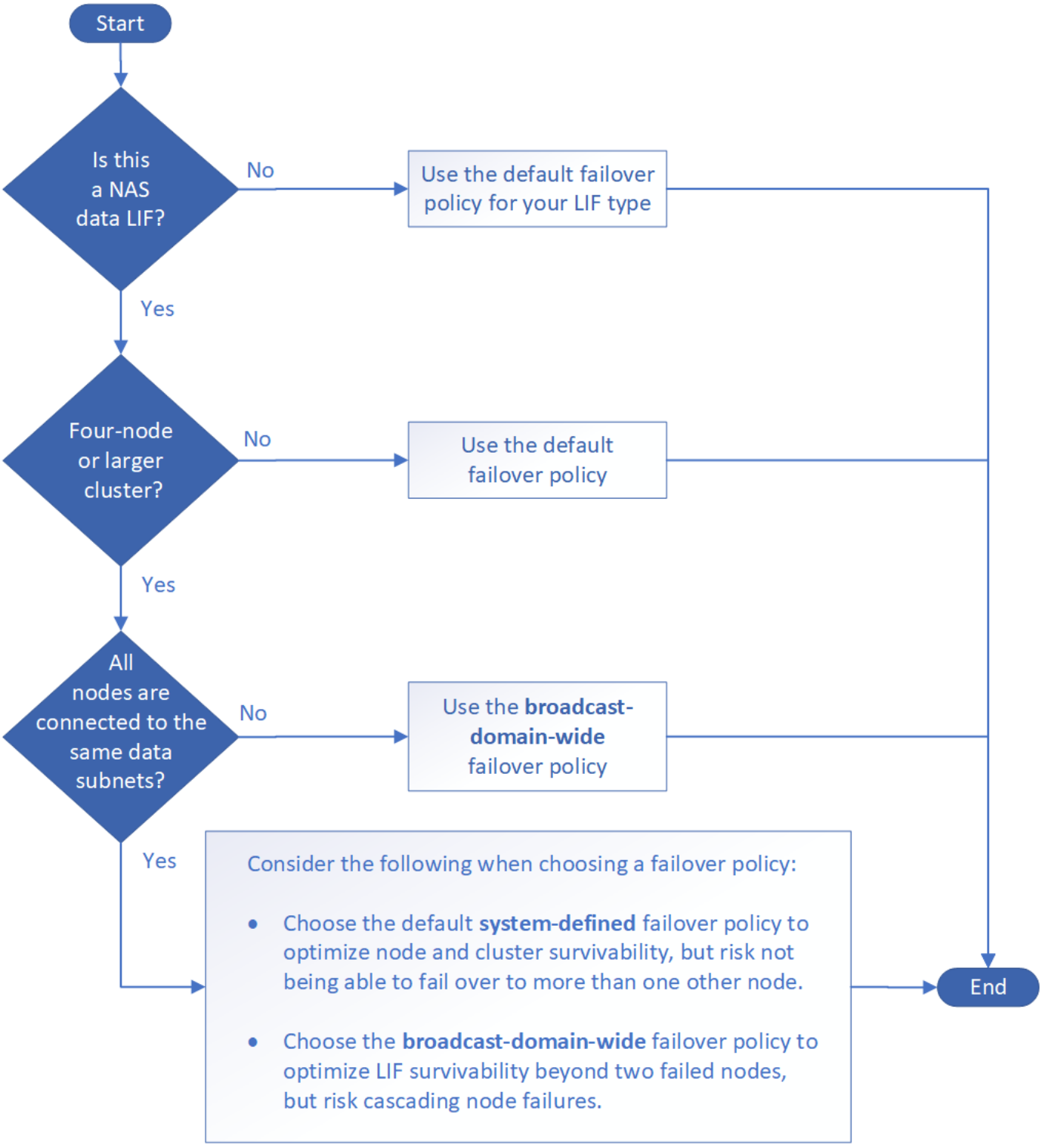
```
network interface show -failover
```

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

#### 使用する **LIF** フェイルオーバーポリシーを決定します

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です | 説明 |
|---|---|---|
| BGP LIF | 無効 | LIF は別のポートにフェイルオーバーしません。 |

| | | |
|---|---|---|
| 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 | LIF は、クラスタ内のすべてのノード上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 LIFs | 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 | LIF は、 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 LIFs | 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 | LIF は別のポートにフェイルオーバーしません。 |

「sfo-partner-only」フェイルオーバーポリシーはデフォルトではありませんが、LIFをホームノードまたはSFOパートナー上のポート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、ネットワーク設定を簡易化するワークフローで使用する。
- System Manager ではなく、 CLI を使用する。
- ONTAP 9.8 以降を実行している新しいシステムでネットワークを設定する場合。

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 から 9.7 の NAS パスフェイルオーバー手順を使用してください。

- "ONTAP 9.1-9.7 NAS パスのフェイルオーバーワークフロー"

ネットワーク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 9.8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。パスのフェイルオーバーは、 ONTAP のデフォルトを利用して管理できます。


リンク障害の発生後に手動で移動しないかぎり、 SAN LIF は移行されません。代わりに、ホストのマルチパステクノロジによって、別の LIF にトラフィックが転送されます。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 **"IPspaces** を作成します"

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を **IPspace** に移動します"

ブロードキャストドメインをIPspaceに移動します。

4 **"SVMs** を作成します"

クライアントにデータを提供するSVMを作成します。

5 **"LIFs** を作成します"

データへのアクセスに使用するポートにLIFを作成します。

6 **"SVM**用の**DNS**サービスの設定"

NFSサーバまたはSMBサーバを作成する前に、SVM用のDNSサービスを設定してください。

## 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記入しておく必要があります。

### IPspace の設定

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

| 情報 | 必須 | 値を入力します |
| --- | --- | --- |

| | | |
|---|---|---|
| IPspace 名<br>IPspaceの一意の識別子。 | はい。 | |

ブロードキャストドメイン設定

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

ブロードキャストドメインは IPspace に割り当てられます。1 つの IPspace に複数のブロードキャストドメインを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、同じ名前のフェイルオーバーグループが作成され、ブロードキャストドメインのすべてのポートが追加されます。

| 情報 | 必須 | 値を入力します |
|---|---|---|
| IPspace 名<br>ブロードキャストドメインを割り当てる IPspace を指定します。<br><br>既存の IPspace を指定する必要があります。 | はい。 | |
| ブロードキャストドメイン名<br>ブロードキャストドメインの名前を指定します。<br><br>この名前は IPspace 内で一意である必要があります。 | はい。 | |
| MTU<br>ブロードキャストドメインの最大伝送ユニットの値。一般に、* 1500 または 9000 *のいずれかに設定されます。<br><br>MTU 値は、ブロードキャストドメイン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。<br><br>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。e0Mポートの処理管理とサービスプロセッサのトラフィックでは、MTUを1500バイト以下に設定する必要があります。 | はい。 | |

| | | |
|---|---|---|
| ポート<br>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、を実行して到達可能性を確認します `network port reachability show` コマンドを実行します<br><br>追加できるポートは、物理ポート、 VLAN 、インターフェイスグループです。 | はい。 | |

サブネット構成

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

- SVM 上で LIF を作成する際には、 IP アドレスとサブネットを指定する代わりにサブネット名を指定できます。
- サブネットはデフォルトゲートウェイと一緒に設定できるため、 SVM を作成する際に別途デフォルトゲートウェイを作成する必要はありません。
- ブロードキャストドメインには、 1 つ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と関連付けることによって、別のサブネット上にある SVM LIF を設定できます。
- 各サブネットには、同じ IPspace 内の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 | 値を入力します |
|---|---|---|
| IPspace 名<br>サブネットを割り当てる IPspace 。<br><br>既存の IPspace を指定する必要があります。 | はい。 | |
| サブネット名<br>サブネットの名前。<br><br>この名前は IPspace 内で一意である必要があります。 | はい。 | |
| ブロードキャストドメイン名<br>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。<br><br>このブロードキャストドメインは、指定した IPspace 内に存在する必要があります。 | はい。 | |

| | | |
|---|---|---|
| サブネット名とマスク<br>IP アドレスが存在するサブネットとマスクです。 | はい。 | |
| ゲートウェイ<br>サブネットのデフォルトゲートウェイを指定できます。<br><br>ゲートウェイはサブネットを作成するときに割り当てなくても、あとから割り当てることができます。 | いいえ | |
| IP アドレスの範囲<br>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。<br><br>たとえば、次のような範囲を指定できます。<br><br>`192.168.1.1-192.168.1.100, 192.168.1.112, 192.168.1.145`<br><br>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<br>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。<br><br>デフォルトでは、サービスプロセッサインターフェイスやネットワークインターフェイスが指定した範囲の 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。<br><br>このパラメータを使用すると、手動でアドレスを指定したすべてのインターフェイスがサブネットに関連付けられ、コマンドは問題なく実行されます。 | いいえ | |

**SVM**設定

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、デフォルトデータ SVM を作成するために使用します。MetroCluster ソース SVM を作成する場合は、を参照してください "Fabric-attached MetroCluster Installation and Configuration Guide" または "ストレッチ MetroCluster インストールおよび設定ガイド"。

| 情報 | 必須 | 値を入力します |
|---|---|---|

| | | |
|---|---|---|
| SVM 名<br>SVMの完全修飾ドメイン名（FQDN）。<br><br>この名前はクラスタリーグ全体で一意である必要があります。 | はい。 | |
| ルートボリューム名<br>SVM ルートボリュームの名前。 | はい。 | |
| アグリゲート名<br>SVM ルートボリュームを保持するアグリゲートの名前。<br><br>既存のアグリゲートを指定する必要があります | はい。 | |
| セキュリティ形式<br>SVM ルートボリュームのセキュリティ形式。<br><br>指定できる値は、 * ntfs * 、 * unix * 、および * mixed * です。 | はい。 | |
| IPspace 名<br>SVM を割り当てる IPspace 。<br><br>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<br>SVM とそのボリュームで使用されるデフォルトの言語。<br><br>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。<br><br>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定されます。<br><br>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 ）を通じてクライアントとホストにデータを提供します。

| 情報 | 必須 | 値を入力します |
|---|---|---|
| SVM 名<br>LIF の SVM の名前。 | はい。 | |

| | | |
|---|---|---|
| LIF 名<br>LIFの名前。<br><br>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 を割り当てたりできます。<br><br>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。<br><br>* 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。 | はい。 | |
| サービスポリシー<br>LIFのサービスポリシー。<br><br>サービスポリシーは、 LIF を使用できるネットワークサービスを定義します。データ SVM とシステム SVM の両方でデータトラフィックと管理トラフィックの管理に使用できる組み込みのサービスとサービスポリシーを用意しています。 | はい。 | |
| 許可するプロトコル<br>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。<br><br>ファイバチャネルポートで SAN LIF に許可するプロトコルを指定します。これらのプロトコルで LIF を使用できます。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<br>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。<br><br>各データ LIF のホームノードを記録する必要があります。 | はい。 | |

| | | |
|---|---|---|
| ホームポートまたはブロードキャストドメイン<br>次のいずれかを選択します。<br><br>* 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。これは、 IPspace のサブネットにある最初の LIF に対してのみ実行されます。 LIF がないと必須ではありません。<br><br>* 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。 | はい。 | |
| サブネット名<br>SVM に割り当てるサブネット。<br><br>アプリケーションサーバへの継続的な可用性が確保された 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**設定

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

| 情報 | 必須 | 値を入力します |
|---|---|---|
| SVM 名<br>NFS または SMB サーバを作成する SVM の名前を指定します。 | はい。 | |
| DNS ドメイン名<br>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。<br><br>ローカルドメインを最初にリストし、そのあとに DNS クエリが最も頻繁に実行されるドメイン名を指定します。 | はい。 | |

| | | |
|---|---|---|
| DNSサーバのIPアドレス<br>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。<br><br>これらのDNSサーバには、Active Directory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。<br><br>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 ONTAP の作成に失敗します。<br><br>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 を統合した DNS サーバを SVM の DNS サーバとして構成することです。<br><br>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。<br><br>Active Directory 統合 SRV レコードの詳細については、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"。 | はい。 | |

動的 **DNS** 設定

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

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

| 情報 | 必須 | 値を入力します |
|---|---|---|
| SVM 名<br>NFS または SMB サーバを作成する SVM 。 | はい。 | |

| | | |
|---|---|---|
| DDNS を使用するかどうか<br>DDNS を使用するかどうかを指定します。<br><br>SVM 上で設定されている 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。 | はい。 | |
| セキュアな DDNS を使用するかどうか<br>Secure DDNS は、 Active Directory 統合 DNS でのみサポートされています。<br><br>Active Directory 統合 DNS で Secure DDNS 更新のみを許可する場合、このパラメータの値を true に設定する必要があります。<br><br>デフォルトでは、 Secure DDNS は無効になっています。<br><br>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することができます。 | いいえ | |
| DNS ドメインの FQDN<br>DNS ドメインの FQDN 。<br><br>SVM 上の DNS ネームサービスに設定されているドメイン名と同じ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 9.1-9.7 の NAS パス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、ネットワーク構成を簡易化したい。
- System Manager ではなく、 CLI を使用する。
- ONTAP 9.0 から 9.7 を実行している新しいシステムでネットワークを設定する。

9.7 よりも前のリリースの ONTAP を実行している場合は、 ONTAP 9.8 以降で NAS パス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

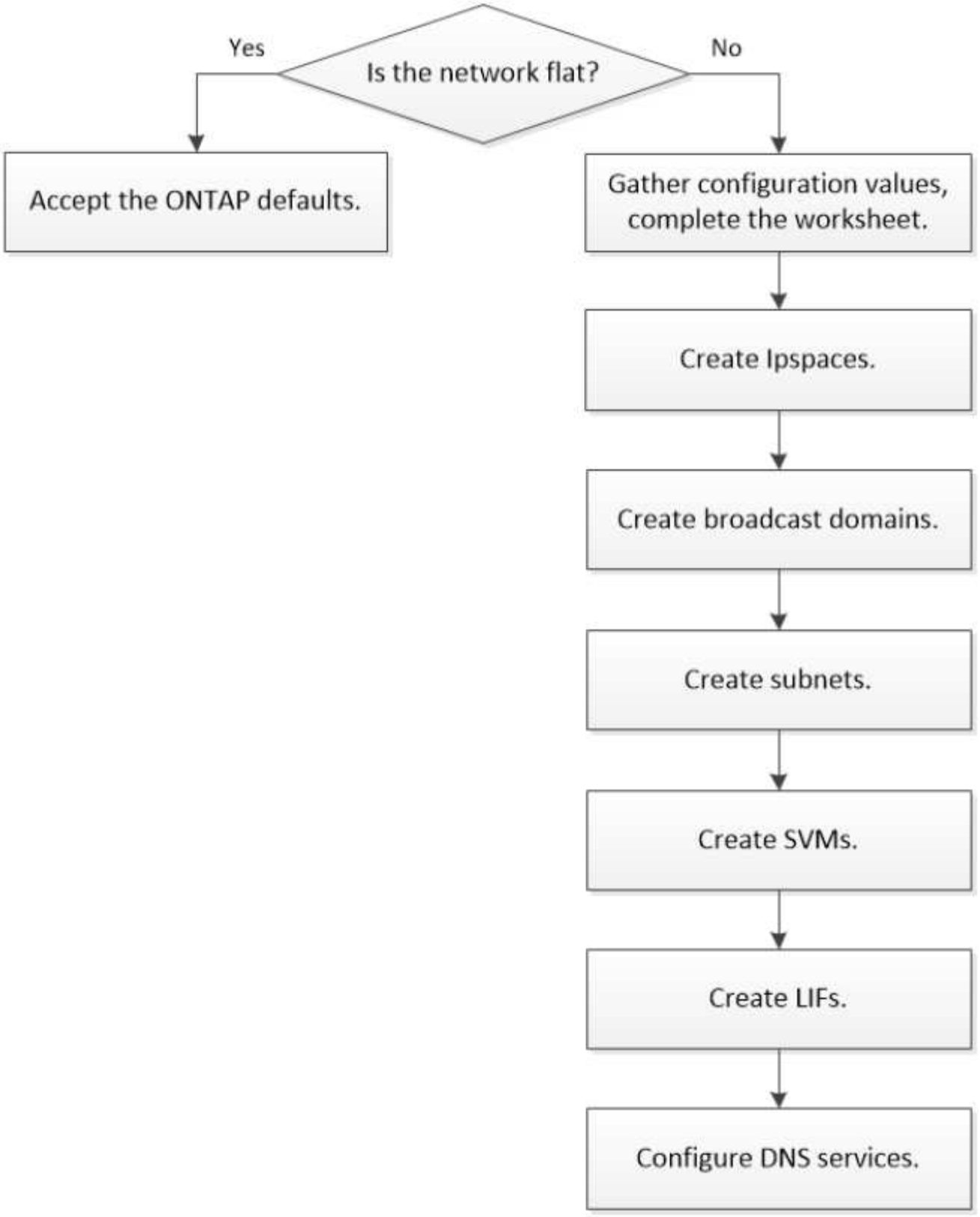
ネットワークコンポーネントと管理の詳細については、ネットワーク管理リファレンスを参照してください。

- 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構成であれば、 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。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。




リンク障害の発生後に手動で移動しないかぎり、 SAN LIF は移行されません。代わりに、ホストのマルチパステクノロジによって、別の LIF にトラフィックが転送されます。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 "IPspaces を作成します"

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を作成する"

ブロードキャストドメインを作成する

4 "サブネットを作成する"

サブネットを作成する。

5 "SVMs を作成します"

クライアントにデータを提供するSVMを作成します。

6 "LIFs を作成します"

データへのアクセスに使用するポートにLIFを作成します。

7 "SVM用のDNSサービスの設定"

NFSサーバまたはSMBサーバを作成する前に、SVM用のDNSサービスを設定してください。

## 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記入しておく必要があります。

### IPspace の設定

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

| 情報 | 必須 | 値を入力します |
| --- | --- | --- |

| | | |
|---|---|---|
| IPspace 名<br>• IPspace の名前。<br>• この名前はクラスタ内で一意である必要があります。 | はい。 | |

ブロードキャストドメイン設定

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

ブロードキャストドメインは IPspace に割り当てられます。1 つの IPspace に複数のブロードキャストドメインを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、 ONTAP によって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。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たすべてのポートが含まれます。

| 情報 | 必須 | 値を入力します |
|---|---|---|
| IPspace 名<br>• ブロードキャストドメインを割り当てる IPspace を指定します。<br>• 既存の IPspace を指定する必要があります。 | はい。 | |
| ブロードキャストドメイン名<br>• ブロードキャストドメインの名前を指定します。<br>• この名前は IPspace 内で一意である必要があります。 | はい。 | |

| | | |
|---|---|---|
| MTU<br>• ブロードキャストドメインの MTU を指定します。<br>• 一般的には* 1500 または 9000 *に設定されます。<br>• MTU 値は、ブロードキャストドメイン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。<br>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。e0Mポートの処理管理とサービスプロセッサのトラフィックでは、MTUを1500バイト以下に設定する必要があります。 | はい。 | |
| ポート<br>• 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。<br>• 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。<br>• ポートが別のブロードキャストドメイン内にある場合は、そのドメインから削除してからブロードキャストドメインに追加する必要があります。<br>• 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。たとえば node1 ： e0d とします。 | はい。 | |

サブネット構成

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

- SVM 上で LIF を作成する際には、 IP アドレスとサブネットを指定する代わりにサブネット名を指定できます。
- サブネットはデフォルトゲートウェイと一緒に設定できるため、 SVM を作成する際に別途デフォルトゲートウェイを作成する必要はありません。
- ブロードキャストドメインには、 1 つ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と関連付けることによって、別のサブネット上にある SVM LIF を設定できます。
- 各サブネットには、同じ IPspace 内の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 | 値を入力します |
| --- | --- | --- |
| IPspace 名<br>• サブネットを割り当てる IPspace 。<br>• 既存の IPspace を指定する必要があります。 | はい。 | |
| サブネット名<br>• サブネットの名前。<br>• 名前は IPspace 内で一意である必要があります。 | はい。 | |
| ブロードキャストドメイン名<br>• 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。<br>• ブロードキャストドメインは、指定された IPspace 内に存在する必要があります。 | はい。 | |
| サブネット名とマスク<br>• IP アドレスが存在するサブネットとマスクです。 | はい。 | |

| | | |
|---|---|---|
| ゲートウェイ<br>• サブネットのデフォルトゲートウェイを指定できます。<br>• ゲートウェイはサブネットを作成するときに割り当てなくても、いつでも割り当てることができます。 | いいえ | |
| IP アドレスの範囲<br>• 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。<br>たとえば、次のような範囲を指定できます。<br>`192.168.1.1-192.168.1.100,192.168.1.112,192.168.1.145`<br>• 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<br>• 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。<br>• デフォルトでは、サービスプロセッサインターフェイスやネットワークインターフェイスが指定した範囲の 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。<br>• このパラメータを使用すると、手動でアドレスを指定したすべてのインターフェイスがサブネットに関連付けられ、コマンドは問題なく実行されます。 | いいえ | |

**SVM**設定

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、デフォルトデータ SVM を作成するために使用します。MetroCluster ソース SVM を作成する

場合は、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" または "ストレッチMetroCluster をインストールします"。

| 情報 | 必須 | 値を入力します |
| --- | --- | --- |
| SVM 名<br>• SVM の名前。<br>• 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。 | はい。 | |
| ルートボリューム名<br>• SVM ルートボリュームの名前。 | はい。 | |
| アグリゲート名<br>• SVM ルートボリュームを保持するアグリゲートの名前。<br>• 既存のアグリゲートを指定する必要があります | はい。 | |
| セキュリティ形式<br>• SVM ルートボリュームのセキュリティ形式。<br>• 指定できる値は、 * ntfs * 、 * unix * 、および * mixed * です。 | はい。 | |
| IPspace 名<br>• SVM を割り当てる IPspace 。<br>• 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<br>• SVM とそのボリュームで使用されるデフォルトの言語。<br>• 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。<br>• 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定されます。<br>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 ）を通じてクライアントとホストにデータを提供します。

| 情報 | 必須 | 値を入力します |
|---|---|---|
| SVM 名<br>• LIF の SVM の名前。 | はい。 | |

| | | |
|---|---|---|
| LIF 名<br><br>• LIFの名前。<br>• 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 を割り当てたりできます。<br>• 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。<br>• 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。 | はい。 | |
| LIF のロール<br><br>• LIF のロール。<br>• データ LIF にはデータロールが割り当てられます。 | はい。<br>ONTAP 9.6から廃止 | データ |
| サービスポリシー<br>LIFのサービスポリシー。<br><br>サービスポリシーは、 LIF を使用できるネットワークサービスを定義します。データ SVM とシステム SVM の両方でデータトラフィックと管理トラフィックの管理に使用できる組み込みのサービスとサービスポリシーを用意しています。 | はい。<br>ONTAP 9.6以降 | |

| | | |
|---|---|---|
| 許可するプロトコル<br><br>• LIF を使用できるプロトコル。<br>• デフォルトでは、SMB、NFS、およびFlexCacheが許可されています。<br>FlexCache プロトコルを使用すると、 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としてボリュームを使用できます。<br><br>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<br><br>• 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。<br>• 各データ LIF のホームノードを記録する必要があります。 | はい。 | |
| ホームポートまたはブロードキャストドメイン<br><br>• 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。<br>• 各データ LIF のホームポートを記録する必要があります。 | はい。 | |
| サブネット名<br><br>• SVM に割り当てるサブネット。<br>• アプリケーションサーバへの継続的な可用性が確保された 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**設定

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

| 情報 | 必須 | 値を入力します |
| --- | --- | --- |
| SVM 名<br>• NFS または SMB サーバを作成する SVM の名前を指定します。 | はい。 | |
| DNS ドメイン名<br>• 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。<br>• ローカルドメインを最初にリストし、そのあとに DNS クエリが最も頻繁に実行されるドメイン名を指定します。 | はい。 | |

| | | |
|---|---|---|
| DNSサーバのIPアドレス<br><br>• 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。<br>• 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。<br>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 ONTAP の作成に失敗します。<br>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 を統合した DNS サーバを SVM の DNS サーバとして構成することです。<br>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。<br>• Active Directory 統合 SRV レコードの詳細については、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"。 | はい。 | |

動的 **DNS** 設定

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

SVM 上にあるすべてのデータ LIF について DNS レコードが作成されます。SVM 上に複数のデータ LIF を作成することによって、割り当てられたデータ IP アドレスへのクライアント接続の負荷を分散することができ

ます。DNS は、そのホスト名を使用して、割り当てられた IP アドレスへの接続をラウンドロビン方式で確立することで、接続の負荷を分散します。

| 情報 | 必須 | 値を入力します |
| --- | --- | --- |
| SVM 名<br>• NFS または SMB サーバを作成する SVM 。 | はい。 | |
| DDNS を使用するかどうか<br>• DDNS を使用するかどうかを指定します。<br>• SVM 上で設定されている 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。 | はい。 | |
| セキュアな DDNS を使用するかどうか<br>• Secure DDNS は、 Active Directory 統合 DNS でのみサポートされています。<br>• Active Directory 統合 DNS で Secure DDNS 更新のみを許可する場合、このパラメータの値を true に設定する必要があります。<br>• デフォルトでは、 Secure DDNS は無効になっています。<br>• 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することができます。 | いいえ | |
| DNS ドメインの FQDN<br>• DNS ドメインの FQDN 。<br>• SVM 上の DNS ネームサービスに設定されているドメイン名と同じ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 ）と仮想ポート（インターフェイスグループや VLAN など）に分類されます。

仮想ポートは仮想ローカルエリアネットワーク（ VLAN ）とインターフェイスグループで構成されます。インターフェイスグループは複数の物理ポートを 1 つのポートとして扱い、 VLAN は 1 つの物理ポートを複数の個別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。基になる物理ポートまたはインターフェイスグループポートは VLAN トランクポートとみなされるため、接続するスイッチポートは VLAN ID をトランクするように構成する必要があります。

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

- 仮想 IP （ VIP ）ポート： VIP LIF のホームポートとして使用される論理ポート。VIP ポートはシステムによって自動的に作成され、サポートされる操作は限られています。VIP ポートは ONTAP 9.5 以降でサポートされています。

ポートの命名規則は *enumberletter* ：

- 最初の文字は、ポートの種類を示します。
  「 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 文字目は複数ポートアダプタ上のポートの位置を示します。
  「 a 」は最初のポート、「 b 」は 2 番目のポート、というように続きます。

例： `e0b` イーサネットポートは、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ます `port_name-vlan-id`。

`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。例： `e1c-80` は有効なVLAN名です。

## ネットワークポートを設定

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する

## 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。

### インターフェイスグループのタイプ

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。インターフェイスグループごとに、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。

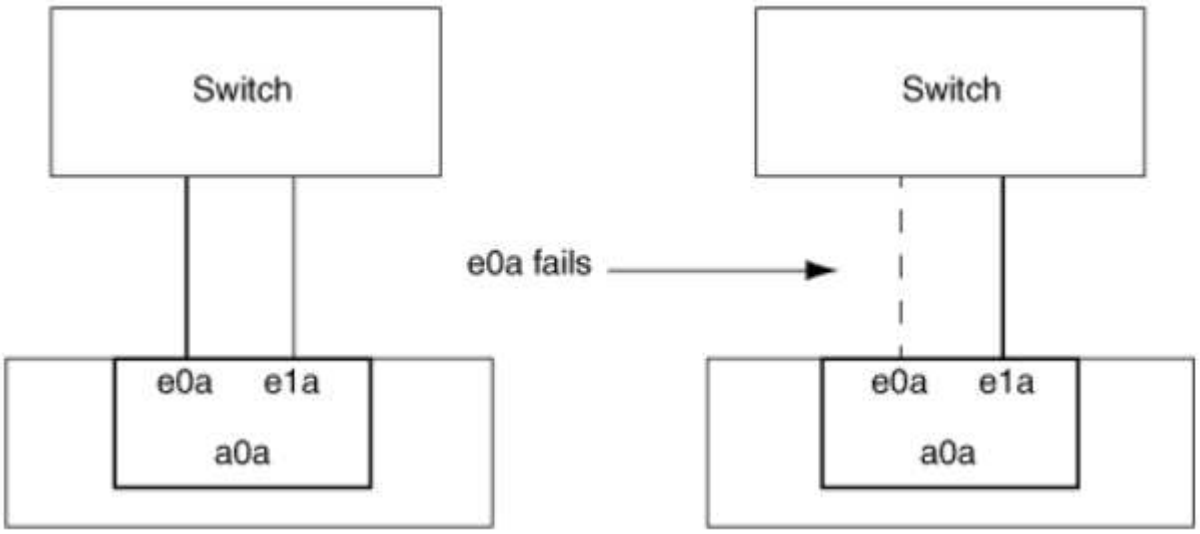
### シングルモードインターフェイスグループの特性

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ため、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の場合は、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。
- 送信元アドレスが 0.0.0.0 であるリンクモニタリング ARP パケットは、ポートを介して送信され、ポートが同じブロードキャストドメイン内にあることが確認されます。

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



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

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

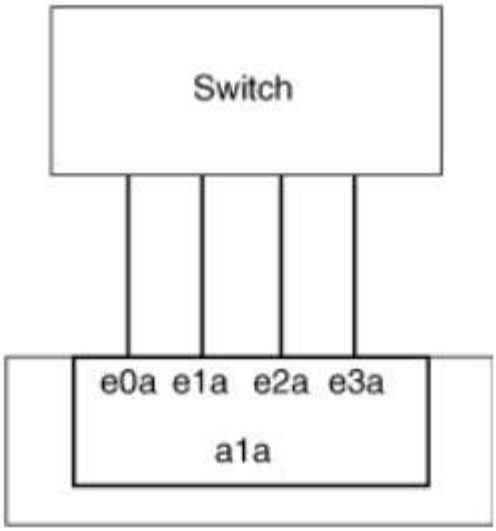
ONTAP に実装されているスタティックマルチモードインターフェイスグループは、 IEEE 802.3ad （ static ）に準拠しています。スタティックマルチモードインターフェイスグループでは、アグリゲーションはサポートするがアグリゲーション設定のための制御パケット交換は行わないスイッチを使用できます。

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

スタティックマルチモードインターフェイスグループの特性は、次のとおりです。

- インターフェイスグループ内のすべてのインターフェイスがアクティブで、 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場合、すべてのセッションはパケット単位で使用可能なリンク全体に分散され、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「 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しているインターフェイスの合計数です。
- あるポートで障害が発生した場合や切断された場合は、そのリンクを経由していたトラフィックが残りのインターフェイスの 1 つに自動的に再分散されます。
- スタティックマルチモードインターフェイスグループではリンクの喪失は検出できますが、クライアントへの接続の切断や、接続性とパフォーマンスに影響を及ぼす可能性があるスイッチの設定ミスは検出できません。
- スタティックマルチモードインターフェイスグループには、複数のスイッチポートでのリンクアグリゲーションをサポートするスイッチが必要です。
  インターフェイスグループの各リンクの接続先ポートがすべて 1 つの論理ポートを構成するよう、そのスイッチを設定します。一部のスイッチは、ジャンボフレーム用に構成されたポートのリンクアグリゲーションをサポートしていない場合があります。詳細については、スイッチベンダーのマニュアルを参照してください。
- スタティックマルチモードインターフェイスグループのインターフェイス間でのトラフィック分散には、いくつかのロードバランシングオプションを使用できます。

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




1 つの集約リンク内のトラフィックを複数の物理スイッチに分散でき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。IEEE 802.3 規格に対応または準拠すると言われている複数スイッチリンクアグリゲーションテクノロジであれば、 ONTAP と一緒に使用できます。

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

ダイナミックマルチモードインターフェイスグループ

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

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

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

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

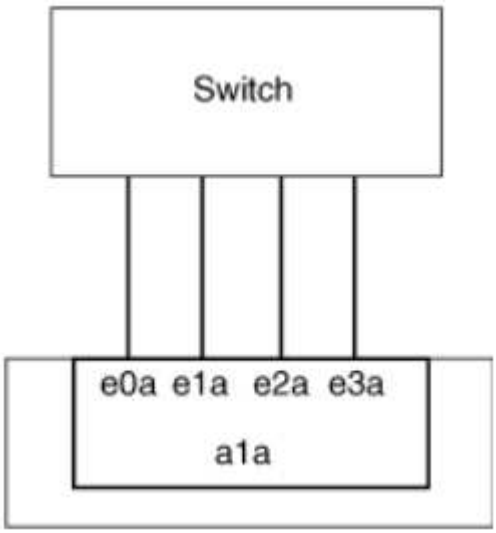
ONTAP ロードバランシングアルゴリズムは、発信トラフィックの転送に使用されるメンバーポートを決定しますが、着信フレームの受信方法は制御しません。スイッチは、スイッチのポートチャネルグループに設定されたロードバランシングアルゴリズムに基づいて、転送に使用されるポートチャネルグループのメンバー（個々の物理ポート）を決定します。したがって、スイッチの設定により、トラフィックを受信するストレージシステムのメンバーポート（個々の物理ポート）が決まります。スイッチ設定の詳細については、スイッチベンダーのマニュアルを参照してください。

あるインターフェイスが、連続する 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に対して、「 ifgrp status 」コマンドで「 lag_inactive 」と出力されます。既存のトラフィックは、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、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て、 1 つの MAC アドレスを共有する必要があります。

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




マルチモードインターフェイスグループでのロードバランシング

IP アドレスベース、 MAC アドレスベース、シーケンシャル、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させることにより、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を指定できるのは、インターフェイスグループの作成時だけです。

- ベストプラクティス * ：可能な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場合にのみ使用してください。

ポートベースのロードバランシング

推奨される方法はポートベースのロードバランシングです。

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

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

### IP アドレスおよび MAC アドレスによるロードバランシング

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

これらのロードバランシング方式では、送信元アドレスと送信先アドレス（ 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を使用します。ハッシュアルゴリズムの結果がリンク状態が UP でないインターフェイスに一致した場合は、次のアクティブなインターフェイスが使用されます。

> ルータ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。このような構成では、すべての発信 IP フレームの宛先 MAC アドレスはルータの MAC アドレスです。そのため、使用されるインターフェイスグループのインターフェイスは 1 つだけです。

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

### シーケンシャルロードバランシング

シーケンシャルロードバランシングでは、ラウンドロビンアルゴリズムを使用して複数のリンク間でパケットを均等に分散できます。シーケンシャルオプションを使用すると、 1 つの接続のトラフィックを複数のリンクに分散させて、単一の接続のスループットを向上させることができます。

ただし、シーケンシャルロードバランシングによって原因のパケット配信順序が乱れることがあるため、パフォーマンスが大幅に低下する可能性があります。したがって、一般にシーケンシャルロードバランシングは推奨されません。

#### インターフェイスグループまたは**LAG**を作成します

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、クライアントに単一のインターフェイスを提供できます。

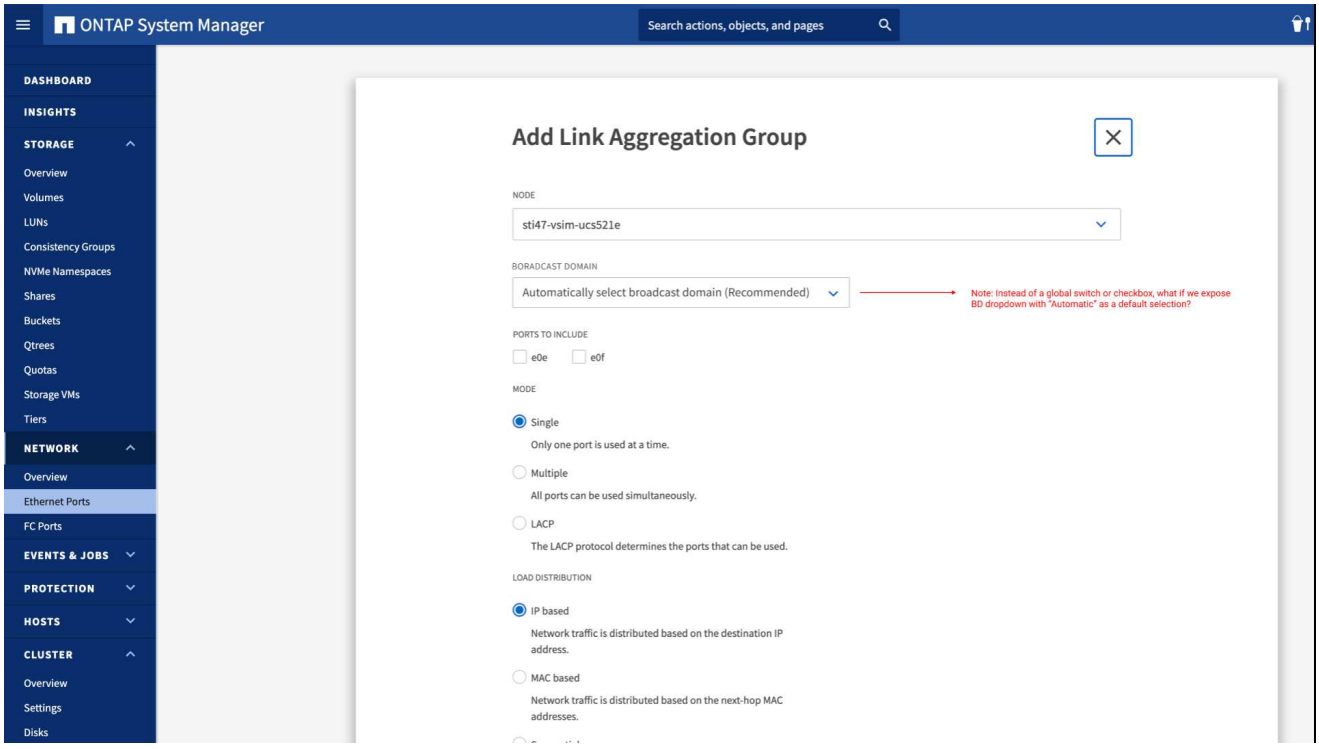
実行する手順 は、System ManagerまたはCLIを使用するインターフェイスによって異なります。

**System Manager** の略

- 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します。
4. LAGを形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** の使用

- 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、を参照してください `network port ifgrp add-port` のマニュアルページ。

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。これは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それらのポートがブートアップ時にどのように初期化されるかによって決まります。そのため、ifgrp の MAC アドレスがリブート後や ONTAP のアップグレード後に変わる可能性があることを想定しておいてください。

ステップ

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

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、を参照してください "ONTAP 9コマンドリファレンス"。

次の例は、ポートの分散機能を使用し、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**にポートを追加します

インターフェイスグループまたはLAGには、すべてのポート速度に対して最大16個の物理ポートを追加できます。

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

**System Manager** の略

- 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** の使用

- 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、を参照してください "ONTAP 9コマンドリファレンス"。

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

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

ONTAP 9.8 以降では、最初の物理ポートがインターフェイスグループに追加されてから約 1 分後に、インターフェイスグループが適切なブロードキャストドメインに自動的に配置されます。ONTAP でこの処理を行わず、ifgrpをブロードキャストドメインに手動で配置する場合は、を指定します `-skip -broadcast-domain-placement` パラメータをに指定します `ifgrp add-port` コマンドを実行します

インターフェイスグループまたは**LAG**からポートを削除します

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

このタスクについて

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、System ManagerまたはCLIを使用するインターフェイスによって異なります。

**System Manager** の略

- 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** の使用

- 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**を削除します

基盤となる物理ポートにLIFを直接設定したり、インターフェイスグループやLAGモード、または分散機能を変更したりする場合は、インターフェイスグループまたはLAGを削除できます。

作業を開始する前に

- インターフェイスグループまたはLAGがLIFをホストしていないことを確認する必要があります。
- インターフェイスグループまたはLAGは、LIFのホームポートでもフェイルオーバーターゲットでもない必要があります。

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

**System Manager** の略

- 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** の使用

- 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

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

このコマンドの詳細については、を参照してください "ONTAP 9コマンドリファレンス"。

次に、 a0b という名前のインターフェイスグループを削除する例を示します。

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

物理ポートを介して **VLAN** を設定します

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基づいて関連付けられます。

たとえば、エンジニアリングや財務などの部門単位、またはリリース 1 やリリース 2 などのプロジェクト単位で、 VLAN のエンドステーションをまとめることができます。VLAN ではエンドステーションが物理的に近接して配置されることは重要ではないので、エンドステーションを地理的に分散させても、スイッチ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VLAN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 を作成、削除、またはその情報を表示できます。

> 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 に割り当てられている場合、そのインターフェイス上に VLAN e0b-10 を作成しないでください。

### VLAN 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またはを使用します `network port vlan create` コマンドを実行します

#### 作業を開始する前に

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、またはベンダー固有の VLAN を実装している。
- 複数の VLAN をサポートするには、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必要があります。
- 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は作成されません。

#### このタスクについて

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

VLAN を初めてポートに設定したときに、ポートが停止してネットワーク接続が一時的に切断されることがあります。その後同じポートに VLAN を追加しても、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 に割り当てられている場合、そのインターフェイス上に VLAN e0b-10 を作成しないでください。

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

**System Manager** の略

- 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、リストから手動で選択することもできます。これまでは、レイヤ2接続に基づいて常にブロードキャストドメインが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した場合は、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. 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** の使用

- CLIを使用してVLAN *を作成します

特定の状況で、ハードウェア問題 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、を設定できます `-ignore-health-status` のパラメータ `network port modify` としてコマンドを実行します `true`。

手順

1. を使用します `network port vlan create` VLANを作成するコマンド。
2. どちらかを指定する必要があります `vlan-name` または `port` および `vlan-id` VLAN作成時のオプション。
   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 の識別子をハイフンでつないだ形式です。例： `e0c-24` および `e1c-80` は有効なVLAN名です。

次に、VLANを作成する例を示します `e1c-80` ネットワークポートに接続されています `e1c` をクリックします `cluster-1-01`：

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

ONTAP 9.8 以降では、作成後約 1 分後に、 VLAN が適切なブロードキャストドメインに自動的に配置されます。ONTAP でこの処理を行わず、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、を指定します `-skip-broadcast-domain-placement` パラメータをに指定します `vlan create` コマンドを実行します

このコマンドの詳細については、を参照してください "ONTAP 9コマンドリファレンス"。

### VLANを編集します

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、リストから手動で選択することもできます。以前は、レイヤ2接続に基づいて、常に自動的にブロードキャストドメインが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した場合は、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。
   - リストから別のブロードキャストドメインを選択して、ブロードキャストドメインを変更します。
   - [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 を削除します

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。

作業を開始する前に

VLAN に関連付けられている LIF がないことを確認します。

このタスクについて

ポートから最後の VLAN 原因を削除すると、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、System ManagerまたはCLIを使用するインターフェイスによって異なります。

**System Manager** の略

- System Managerを使用してVLANを削除します。*

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** の使用

- CLIを使用してVLAN *を削除します

ステップ

を使用します `network port vlan delete` VLANを削除するコマンド。

次に、VLANを削除する例を示します `e1c-80` ネットワークポートから `e1c` をクリックします `cluster-1-01`：

```
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。

作業を開始する前に

LIF をホストしているポートは変更できません。

このタスクについて

- 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ている二重モードおよび速度）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。

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

- を設定することは推奨されません `-up-admin` ノード上のすべてのポート、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にします。
- 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のポートの MTU サイズを、そのブロードキャストドメイン用に設定された MTU 値以外に変更することはできません。
- VLAN の MTU サイズがベースポートの MTU サイズの値を超えることはできません。

手順

1. ネットワークポートの属性を変更します。

   `network port modify`

2. を設定できます `-ignore-health-status` フィールドをtrueに設定すると、指定したポートのネットワークポート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健常性ステータスは「デグレード」から「正常」に自動的に変わり、このポートを使用して LIF をホストできるようになりました。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います `full`。

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** ポートに変換します

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

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。

作業を開始する前に

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。

このタスクについて

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 コマンドを使用した後、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。

このトピックは 環境 ONTAP 9.8以降です。障害の発生した NIC をスロットから取り外したり、メンテナンスのために 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. ノードの電源をオンにします。
4. ポートが削除されたことを確認します。

```
network port show
```

ONTAP は、すべてのインターフェイスグループからポートを自動的に削除します。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は、インターフェイスグループが削除されます。

5. ポートに VLAN が設定されている場合は、ポートが取り外されます。次のコマンドを使用すると、削除された VLAN を表示できます。

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

。 displaced-interface show、 displaced-vlans show`および `displaced-vlans restore コマンドは一意であり、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の別のポート上のそれらの LIF に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 上に適切なホーム・ポートが見つからない場合、これらの LIF は取り外されたと見なされます。削除した LIF を表示するには、次のコマンドを使用します。

```
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、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 コマンドを実行します

ノードからの**NIC**の取り外し（**ONTAP 9.7**以前）

## このトピックは環境 ONTAP 9.7 以前です。障害の発生した NIC をスロットから取り外したり、メンテナンスのために 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。

作業を開始する前に

- NIC ポートに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 のポートが LIF のホームポートでないことを確認します。
- NIC からポートを削除するには advanced 権限が必要です。

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ヘルスを監視する

## 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。

このタスクについて

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。LIF に対して別の正常なフェイルオーバーターゲットが用意されている場合、 ONTAP はデグレード状態のネットワークポートでの LIF のホストを回避します。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や、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 ）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。

  を変更できます `ignore-health-status` ネットワークポートをに設定します `true`。これで、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ヘルスの監視が有効になっているヘルスモニタを確認します。

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

   ポートのヘルスステータスは、ヘルスモニタの値によって決まります。

   ONTAP で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. 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` コマンドを実行します
4. ポートの詳細な健常性を表示します。

```
network port show -health
```

コマンド出力には、ポートのヘルスステータスが表示されます。 `ignore health status` 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。

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

状況に応じて `ignore health status` 設定はです `true`ポートのヘルスステータスがから変更されたことを示します `degraded` 終了： `healthy` 管理者によって作成されます。

状況に応じて `ignore health status` 設定はです `false`の場合、ポートのヘルスステータスはシステムによって自動的に判断されます。

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）

ONTAP 9.8 以降には、到達可能性の監視機能が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 構成と一致しない状況を特定します。場合によっては、 ONTAP がポートの到達可能性を修復できます。それ以外の場合は、追加の手順が必要になります。

このタスクについて

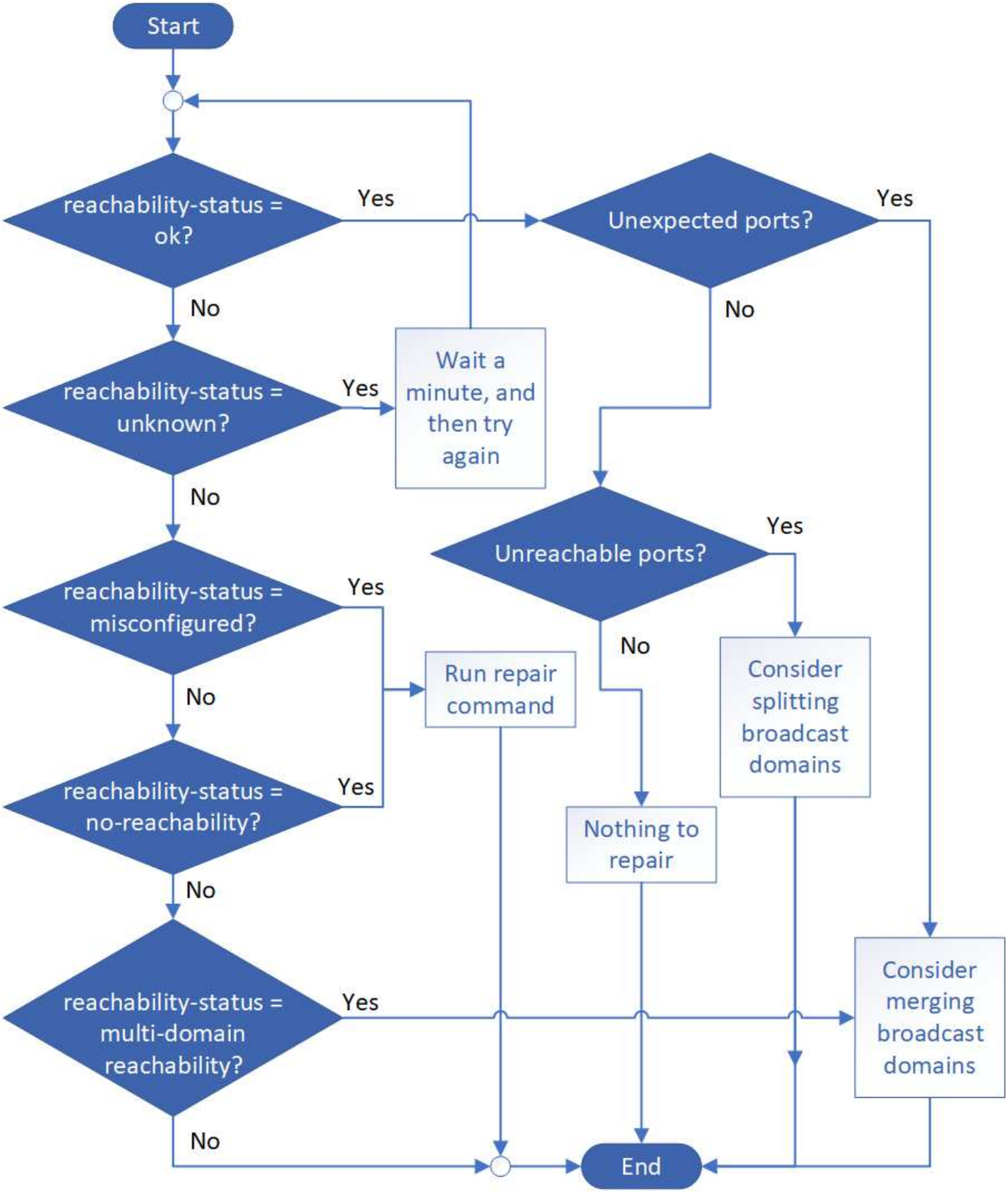
これらのコマンドを使用して、物理的なケーブル接続とネットワークスイッチの設定のどちらにも一致しない ONTAP 設定に起因するネットワークの設定ミスを検証、診断、および修復します。

ステップ

1. ポート到達可能性を表示します。

```
network port reachability show
```

2. 次のデシジョンツリーとテーブルを使用して、次のステップがあるかどうかを判断します。




| プレゼンスステータス | 説明 |
| --- | --- |

| | |
|---|---|
| わかりました | 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。<br>reachable-status が「 OK 」であるのに、「予想外のポート」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。<br><br>reachable-status が「 OK 」であるが、「到達不能ポート」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。<br><br>reachable-status 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は、設定が正しいことを確認してください。 |
| 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。<br><br>物理的な接続とスイッチの設定を調べて、正しくないか、またはポートに割り当てられているブロードキャストドメインを 1 つ以上のブロードキャストドメインにマージする必要があるかどうかを確認します。<br><br>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をマージします"。 |
| 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。<br><br>通常、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。<br><br>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をスプリットします"。 |
| 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。<br><br>ポートに到達できるかどうかを修復できます。次のコマンドを実行すると、ポートに到達できるブロードキャストドメインにポートが割り当てられます。<br><br>`network port reachability repair -node -port`<br>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します"。 |

| | |
|---|---|
| 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。<br><br>ポートに到達できるかどうかを修復できます。次のコマンドを実行すると、自動的に作成されたデフォルトの IPspace 内の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。<br><br>`network port reachability repair -node -port`<br>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します"。 |
| 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。<br><br>物理的な接続とスイッチの設定を調べて、正しくないか、またはポートに割り当てられているブロードキャストドメインを 1 つ以上のブロードキャストドメインにマージする必要があるかどうかを確認します。<br><br>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をマージします" または "ポートの到達可能性を修復します"。 |
| 不明です | 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。 |

ポートを修復したら、取り外された LIF や 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に何が起こったかを理解する必要もあります。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します"。

**ONTAP**ポートの概要

## 既知の多数のポートは、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におけるポート値が ONTAP ポートの値と同じである場合は、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 | Secure Shell ログイン |
| Telnet | 23 / TCP | リモートログイン |
| DNS | 53 / TCP | ロードバランシングされた DNS |
| HTTP | 80 / TCP | Hyper Text Transfer Protocol の略 |
| rpcbind | 111/TCP | リモート手順コール |
| rpcbind | 111/UDP | リモート手順コール |
| NTP | 123 / UDP | Network Time Protocol の略 |
| MSRPC | 135 / UDP | MSRPC |
| NetBios - SSN | 139 / TCP | 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 | HTTP over TLS |
| Microsoft - DS | 445 / TCP | Microsoft - DS |
| マウント | 635 / TCP | NFS マウント |
| マウント | 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 | NetApp リモートボリュームプロトコル |
| iSCSI | 3260 / TCP | iSCSI ターゲットポート |
| ロック | 4045 / TCP | NFS ロックデーモン |
| ロック | 4045 / UDP | NFS ロックデーモン |
| nsm の場合 | 4046 / TCP | Network Status Monitor サービスの略 |
| nsm の場合 | 4046 / UDP | Network Status Monitor サービスの略 |
| rquotad | 4049/UDP | NFS rquotad プロトコル |
| krb524 | 444/UDP | Kerberos 524 |
| mDNS | 533/UDP | マルチキャスト DNS |
| HTTPS | 5986/UDP | HTTPS ポートリスンバイナリプロトコル |
| HTTPS | 8443 / TCP | 7MTT GUI ツールから https ： // |
| NDMP | 10000 / TCP | Network Data Management Protocol の略 |
| クラスタピアリング | 11104 / TCP | 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 | クラスタピアリング |
| NDMP | 18600-18699/TCP | NDMP |
| NDMP | 30000 / TCP | 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 | トランスポートレイヤのセキュリティ |
| iSCSI | 65200/TCP | iSCSIポート |

**ONTAP** の内部ポート

次の表に、 ONTAP によって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 の通信を確立するために使用されます。

| ポート / プロトコル | 説明 |
|---|---|
| 514 | syslog |

| | |
|---|---|
| 900 | ネットアップクラスタ RPC |
| 902 | ネットアップクラスタ RPC |
| 904 | ネットアップクラスタ RPC |
| 905 | ネットアップクラスタ RPC |
| 910 | ネットアップクラスタ RPC |
| 911 | ネットアップクラスタ RPC |
| 913 | ネットアップクラスタ RPC |
| 914 | ネットアップクラスタ RPC |
| 915 | ネットアップクラスタ RPC |
| 918 | ネットアップクラスタ RPC |
| 920 | ネットアップクラスタ RPC |
| 921 | ネットアップクラスタ RPC |
| 924 | ネットアップクラスタ RPC |
| 925 | ネットアップクラスタ RPC |
| 927 | ネットアップクラスタ RPC |
| 928 | ネットアップクラスタ RPC |
| 929 | ネットアップクラスタ RPC |
| 931 | ネットアップクラスタ RPC |
| 932 | ネットアップクラスタ RPC |
| 933 | ネットアップクラスタ RPC |
| 934 | ネットアップクラスタ RPC |
| 935 | ネットアップクラスタ RPC |
| 936 | ネットアップクラスタ RPC |
| 937 | ネットアップクラスタ RPC |
| 939 | ネットアップクラスタ RPC |
| 940 | ネットアップクラスタ RPC |
| 951 | ネットアップクラスタ RPC |
| 954 | ネットアップクラスタ RPC |
| 九五五 | ネットアップクラスタ RPC |
| 956 | ネットアップクラスタ RPC |
| 958 | ネットアップクラスタ RPC |
| 961 | ネットアップクラスタ RPC |
| 九六三 | ネットアップクラスタ RPC |
| 九六四 | ネットアップクラスタ RPC |

| | |
|---|---|
| 九六六 | ネットアップクラスタ RPC |
| 967 | ネットアップクラスタ RPC |
| 982 | ネットアップクラスタ RPC |
| 983 | ネットアップクラスタ RPC |
| 五一五 | 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 | ネットアップクラスタ RPC |
| 7811 | ネットアップクラスタ RPC |
| 7812 | ネットアップクラスタ RPC |
| 7813 | ネットアップクラスタ RPC |
| 7814 | ネットアップクラスタ RPC |
| 7815 | ネットアップクラスタ RPC |
| 7816 | ネットアップクラスタ RPC |
| 7817 | ネットアップクラスタ RPC |
| 7818 | ネットアップクラスタ RPC |
| 7819 | ネットアップクラスタ RPC |
| 7820 | ネットアップクラスタ RPC |
| 7821 | ネットアップクラスタ RPC |
| 7822 | ネットアップクラスタ RPC |
| 7823 | ネットアップクラスタ RPC |
| 7824 | ネットアップクラスタ RPC |
| 8023 | ノードスコープ Telnet |
| 8514 | ノードスコープ RSH |
| 977 | 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 内でのみ適用されます。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 の両方のアドレスがサポートされます。

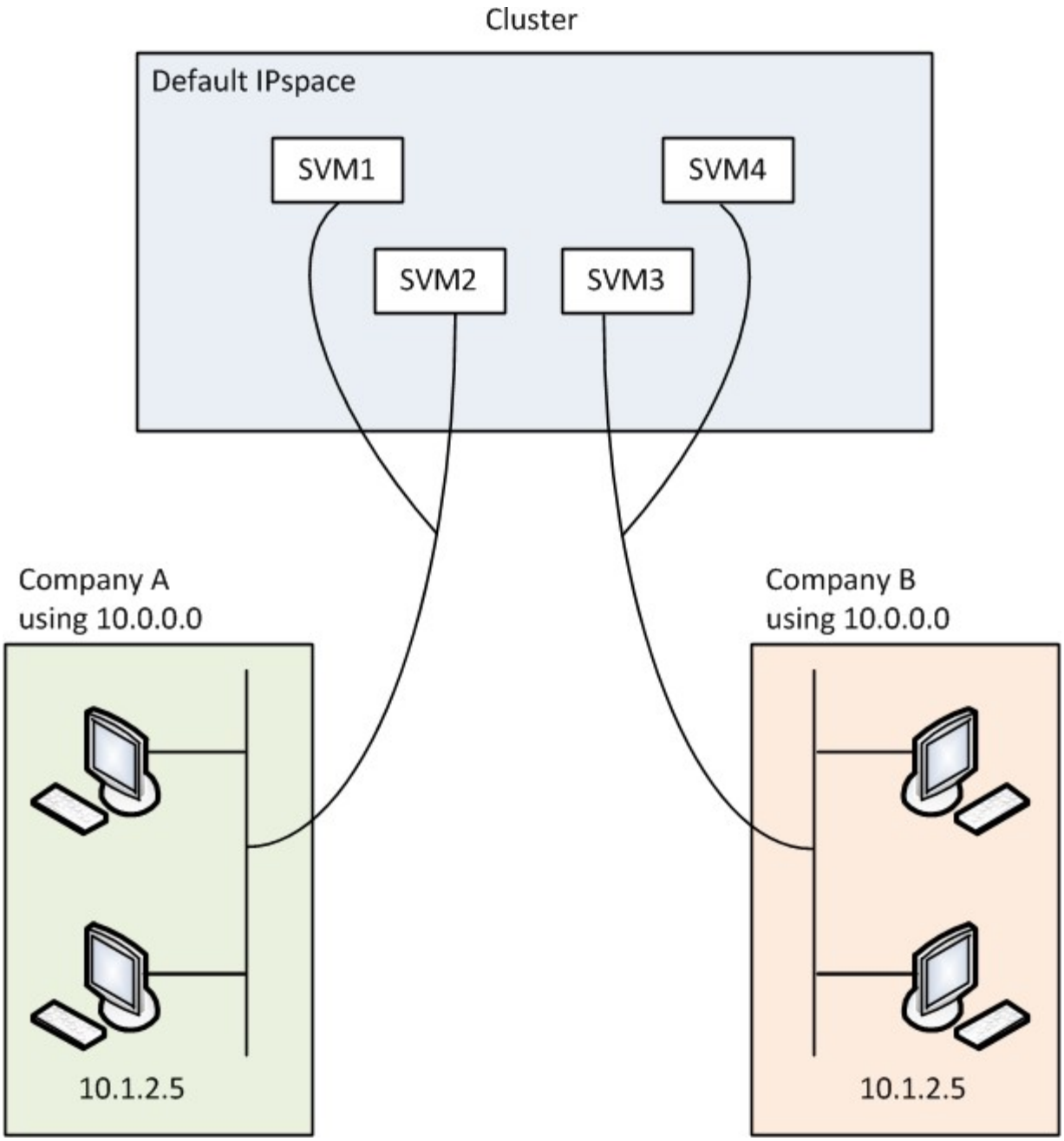
単一の組織のストレージを管理する場合は、 IPspace を設定する必要はありません。単一の ONTAP クラスタで複数企業のストレージを管理していて、ユーザ間のネットワーク設定がないことが確実な場合も、 IPspace を使用する必要はありません。多くの場合、 Storage Virtual Machine （ SVM ）を専用の IP ルーティングテーブルと一緒に使用することで、 IPspace を使用しなくても固有のネットワーク設定を分離できます。

**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 クラスタに接続させる必要があり、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、顧客ごとにクラスタに 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。

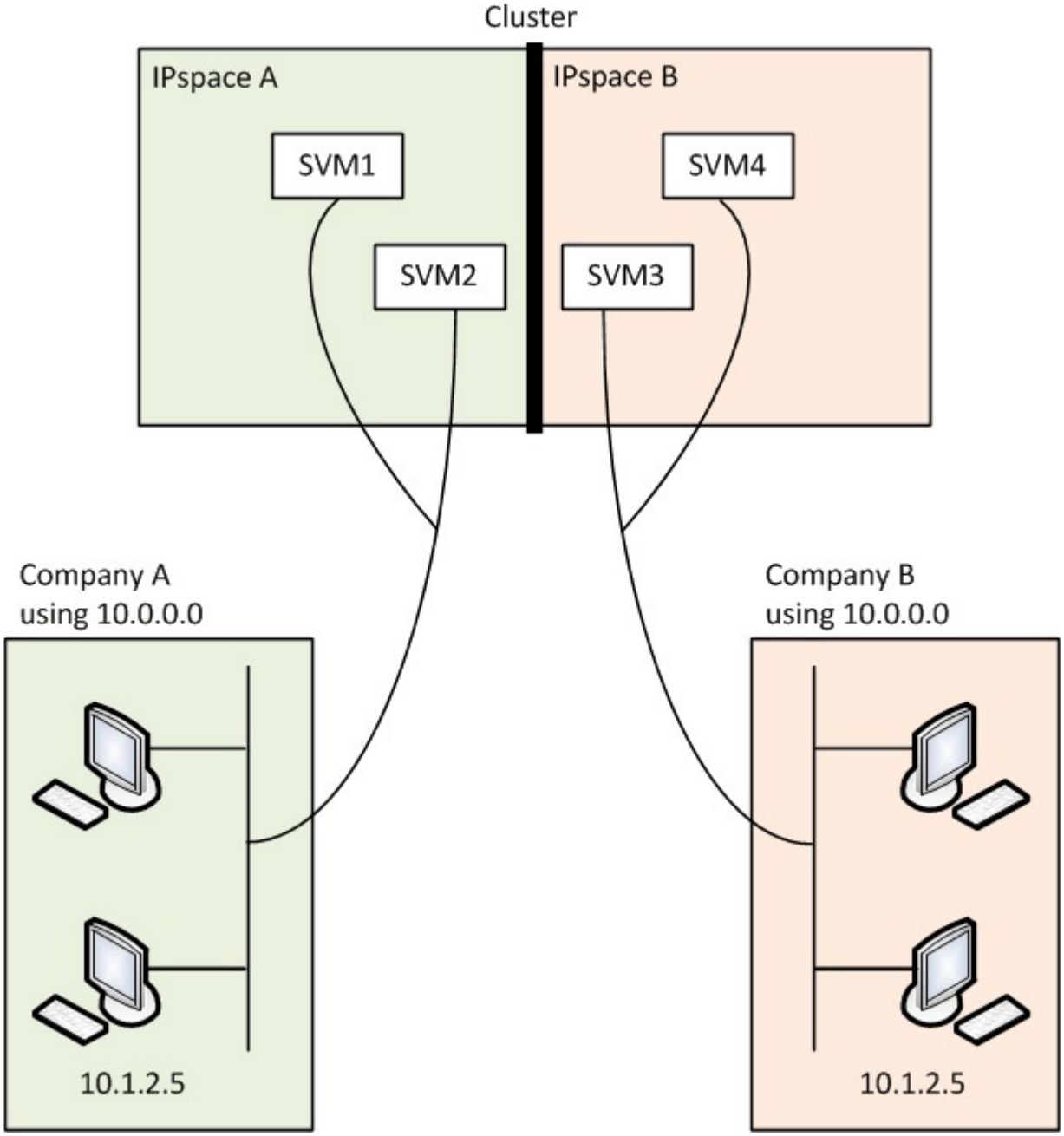
次の図に、このタイプの導入を示します。両社で非プライベート IP アドレスの範囲を使用する場合に機能します。ただし、図では、両方の企業が同じプライベート IP アドレス範囲を使用しているために問題が発生しています。




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

- 両社がそれぞれの SVM に同じ IP アドレスを使用した場合は、 SSP にあるクラスタ内の SVM で IP アドレスの競合が発生します。
- 両社がそれぞれの SVM に別々の IP アドレスを使用することにした場合でも、まだ問題は残ります。
- たとえば、 A のネットワーク内のクライアントの IP アドレスが B のネットワーク内のクライアントと同じ場合、 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 がアドレス 10.0.0.0 とネットワークマスク 255.128.0.0 を、 B がアドレス 10.128.0.0 とネットワークマスク 255.128.0.0 を使用する場合）は、次のように入力します。 SSP は、トラフィックを A および B のネットワークに適切にルーティングするように、クラスタ上のスタティックルートを設定する必要があります。
- この解決策は拡張性に優れておらず（静的ルートであるため）、セキュアではありません（ブロードキャ

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




また、などの各種構成ファイルで参照されるIPアドレス `/etc/ hosts` ファイル、 `/etc/hosts.equiv` ファイル、および `the /etc/rc` ファイルは、そのIPspaceを基準とした相対パスです。そのため、 IPspace を正しく使用すれば、 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

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

クラスタの初期化時に 2 つの IPspace が自動的に作成されます。

- 「 Default 」 IPspace

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

- 「 Cluster 」 IPspace に追加されました

  この IPspace には、クラスタ内のすべてのノード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、クラスタとノードの管理トラフィックをクラスタ間で伝送します。

  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、この 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 には、クライアントの SVM が 1 つ以上存在できます。各クライアント SVM は固有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。

## IPspaces を作成します

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

このタスクについて

IPspace の数はクラスタ全体で 512 個に制限されます。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。お使いのプラットフォームに適用されるその他の制限を確認するには、 Hardware Universe を参照してください。

"NetApp Hardware Universe の略"

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

作業を開始する前に

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。

完了後

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

ブロードキャストドメインは「 default 」 IPspace 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、次のコマンドを使用して、ブロードキャストドメインを「 default 」から「 ips1 」に移動します。

```
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。

作業を開始する前に

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。

システムで定義された「 default 」 IPspace と「 Cluster 」 IPspace は削除できません。

ステップ

IPspace を削除：

```
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の目的は、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ことです。グループ化したポートは、データまたは管理トラフィック用の Storage Virtual Machine （ SVM ）で使用できます。

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

- 「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。

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

  これらのポートはクラスタ通信に使用され、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。

  必要に応じて、追加のブロードキャストドメインがデフォルト IPspace に作成されます。「 default 」ブロードキャストドメインには、管理 LIF のホームポートに加え、そのポートにレイヤ 2 に到達できるその他のポートが含まれます。追加のブロードキャストドメインには、「 default-1 」、「 default-2 」などの名前が付けられます。

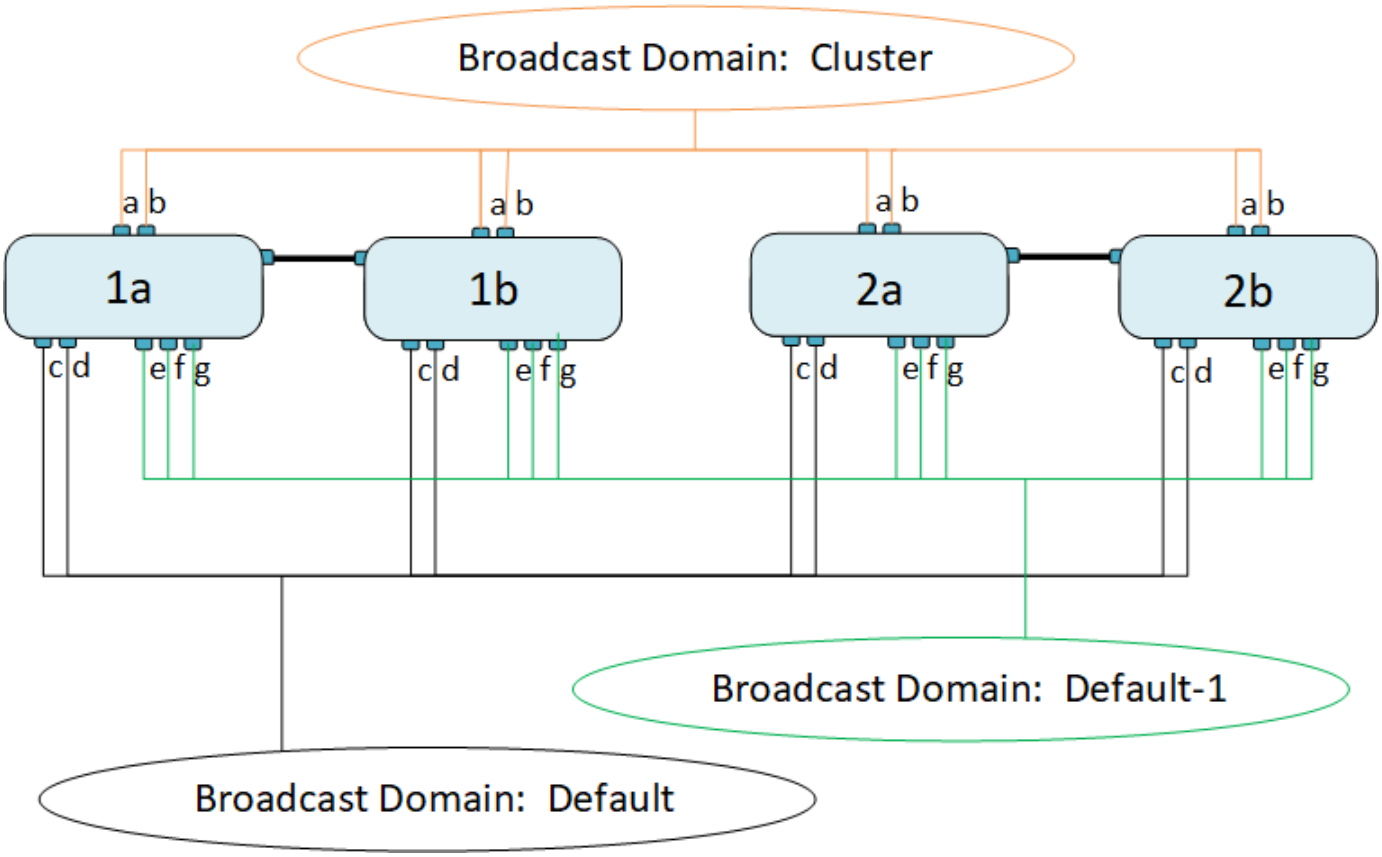
#### ブロードキャストドメインの使用例

ブロードキャストドメインは、同じ IPspace 内の一連のネットワークポートで、一般にクラスタ内の多数のノードのポートを含む、相互にレイヤ 2 に到達できるかどうかを示します。

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ていま

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 を含んでいます。
- 「 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 を含んでいます。
- レイヤ 2 ネットワークの到達可能性に基づいて、クラスタの初期化時に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。追加されるブロードキャストドメインには、 default-1 、 default-2 などの名前が付けられます。




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、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します

## 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たものです。これらのポートは、 SVM で使用されます。

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処理または参加処理中に自動的に作成されます。ONTAP 9.12.0以降では、自動的に作成されるブロードキャストドメインに加え、System Managerでブロードキャストドメインを手動で追加できます。

作業を開始する前に

ブロードキャストドメインに追加するポートは、他のブロードキャストドメインに属していないポートでなけ

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

このタスクについて

- すべてのブロードキャストドメイン名が 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、または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したポートの最大伝送ユニット（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。
- 管理トラフィックを処理する e0M ポートを除く、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の MTU 値が一致している必要があります。
- 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** の略

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. をクリックします ＋ 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** の使用

ONTAP 9.7以前では、手動でブロードキャストドメインを作成できます。

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します"。

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
   ```

   ディスプレイが大きい場合は、を使用します `network port show -broadcast-domain` 未割り当てのポートのみを表示するコマンド。

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。

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

   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。

      ポートはという形式で追加されます `node_name:port_number`例えば、 `node1:e0c`。

3. 必要に応じて、ブロードキャストドメインが作成されたことを確認します。

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

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
```

完了後

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、を使用します `network port broadcast-domain rename` コマンドを実行します

ブロードキャストドメインのポートの追加と削除（**ONTAP 9.8**以降）

## ブロードキャストドメインは、クラスタの作成または追加の処理中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。

ネットワークポートの到達可能性が、物理ネットワーク接続またはスイッチの設定を通じて変更され、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します"

**System Manager** の略

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、 をクリックします。
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** の使用

ネットワークポートの到達可能性が、物理ネットワーク接続またはスイッチの設定を通じて変更され、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します"

または、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` または `network port broadcast-domain remove-ports` コマンドを実行します

作業を開始する前に

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

このタスクについて

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 |
| --- | --- |
| 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。 | 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 は、ブロードキャストドメインの IPspace 値に更新されます。 | ポートは「 Default 」 IPspace に移動し、ブロードキャストドメイン属性はない。 |

を使用してインターフェイスグループの最後のメンバーポートを削除した場合 `network port ifgrp remove-port` このコマンドを実行すると、ブロードキャストドメインからインターフェイスグループポートが削除されます。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許可されていないためです。

手順

1. 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` コマンドを実行します
2. ブロードキャストドメインにポートを追加するか、ブロードキャストドメインからポートを削除します。

| 状況 | 使用 |
|---|---|
| ブロードキャストドメインにポートを追加します | `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します | `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 9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、到達可能なポートを特定して同じブロードキャストドメインに配置できますが、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。

作業を開始する前に

ブロードキャストドメインは、クラスタの作成処理および追加処理の一環として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を定義します。このドメインは、クラスタに最初に作成したノードの管理インターフェイスのホームポートにレイヤ 2 で接続されるポートのセットです。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。

ノードが既存のクラスタに参加すると、そのノード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自動的に既存のブロードキャストドメインに追加されます。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。

このタスクについて

- 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、クラスタの作成または追加処理の一環として、 ONTAP によって自動的に作成されます。
- VLAN やインターフェイスグループを追加すると、作成後約 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、「 OK 」の到達可能性があ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、次のようになります。

   ```
   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、到達可能なポートを特定して同じブロードキャストドメインに配置できますが、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。

作業を開始する前に

ブロードキャストドメインは、クラスタの作成処理および追加処理の一環として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を定義します。このドメインは、クラスタに最初に作成したノードの管理インターフェイスのホームポートにレイヤ 2 で接続されるポートのセットです。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。

ノードが既存のクラスタに参加すると、そのノード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自動的に既存のブロードキャストドメインに追加されます。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。

このタスクについて

- 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、クラスタの作成または追加処理の一環として、 ONTAP によって自動的に作成されます。
- VLAN やインターフェイスグループを追加すると、作成後約 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、「 OK 」の到達可能性があ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、次のようになります。

   ```
   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）

## ネットワークポートの到達可能性が、物理ネットワーク接続またはスイッチの設定によって変更された場合は、次の手順を実行します。 また、単一のブロードキャストドメインに設定していたネットワークポートのグループが、 2 つの到達可能性セットにパーティショニングされます。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複数の到達可能性セットに分割されているかどうかを確認するには、を使用します `network port reachability show -details` コマンドを実行し、どのポートが相互に接続されていないかに注意してください（「Unreachable ports」）。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うえで、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。

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更され、複数のブロードキャストドメインで設定されていた 2 つのネットワークポートグループがすべて到達可能性を共有するようになった場合、 2 つのブロードキャストドメインをマージすることで、 ONTAP 設定と物理ネットワークトポロジを同期できます。

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（「想定外のポート」）を調べます。通常、一連の予期しない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、ブロードキャストドメインにマージする必要がある一連のポートが定義されています。

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のポートの**MTU**値の変更（**ONTAP 9.8**以降）

あるブロードキャストドメインの MTU 値を変更することにより、そのブロードキャストドメインのすべてのポートの MTU 値を変更できます。これは、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。

作業を開始する前に

管理トラフィックを処理する e0M ポートを除く、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の MTU 値が一致している必要があります。

このタスクについて

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、回答の MTU 値を変更するために「 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。「 default 」IPspace は、このオプションの値を指定しないかぎり使用されます。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 9.8**以降）

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

ステップ

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

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

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

```
network port broadcast-domain show
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内のポートの更新ステータスがエラーであることを示し、ポートを正しく更新できなかったことを示しています。

```
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、を参照してください "ONTAP 9コマンドリファレンス"。

ブロードキャストドメインを削除する

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

作業を開始する前に

削除するブロードキャストドメインに、関連付けられているサブネット、ネットワークインターフェイス、SVM がないようにします。

このタスクについて

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

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

**System Manager** の略

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

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

手順

1. [ネットワーク]>[概要]>[ブロードキャストドメイン*]を選択します。
2. 選択するオプション ⋮ 削除するブロードキャストドメインの横にある削除*をクリックします。

**CLI** の使用

*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の目的は、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ことです。グループ化したポートは、データまたは管理トラフィック用の Storage Virtual Machine （ SVM ）で使用できます。

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

- 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。
- クラスタのブロードキャストドメインには、クラスタの IPspace 内にあるポートが含まれています。これらのポートはクラスタ通信に使用され、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、作成する個々の 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。

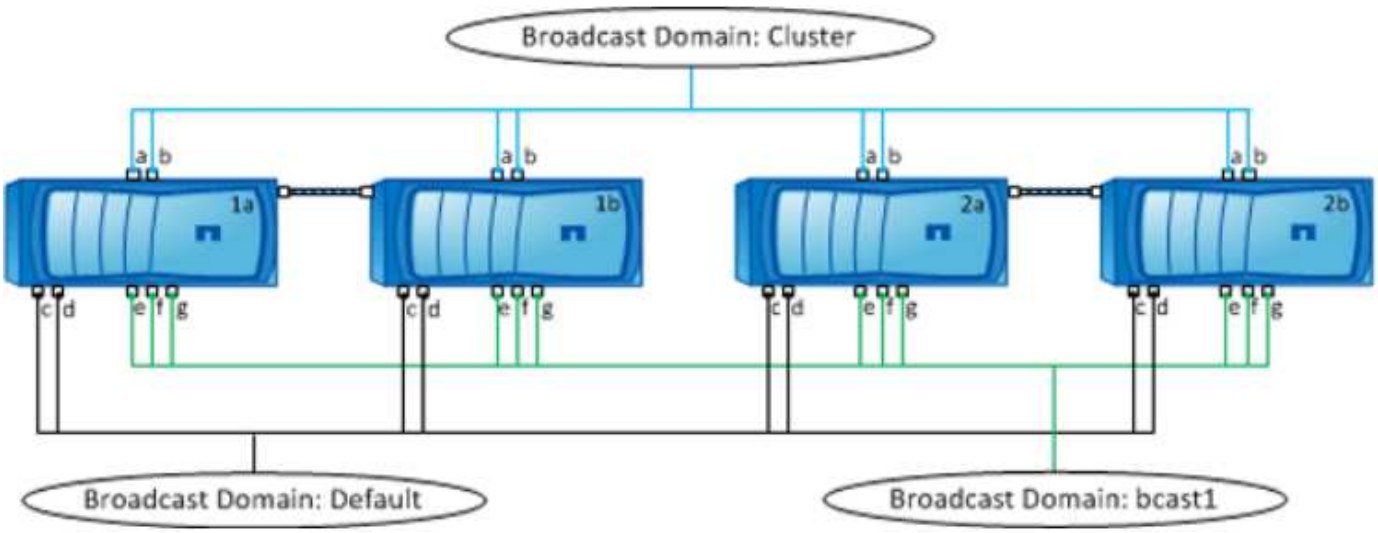
ブロードキャストドメインを作成して、同じレイヤ 2 ネットワークに属するクラスタのネットワークポートをグループ化します。これらのポートは、 SVM で使用されます。

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 内の一連のネットワークポートで、一般にクラスタ内の多数のノードのポートを含む、相互にレイヤ 2 に到達できるかどうかを示します。

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ています。

- 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 を含んでいます。
- 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 を含んでいます。
- 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す。クラスタ内の各ノードのポート e 、 f 、 g を含んでいます。
  このブロードキャストドメインは、新しい SVM を介してデータにアクセスする新しいクライアント専用に、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、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 9.1-9.7 に関連しています。

作業を開始する前に

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。

このタスクについて

- 使用できるポートは、物理ポート、 VLAN 、インターフェイスグループ（ ifgroup ）です。

- 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（たとえば、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を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。
- 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るため、これらの LIF に割り当てられているポートはデフォルトブロードキャストドメインから削除できません。

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。

   - ポート `e0c`、 `e0d`、 `e0e`、 `e0f`および `e0g` 各ノードにはデフォルトのブロードキャストドメインが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。

- ノードポートがポートに割り当てられます `e0c` 各ノードで、クラスタ管理LIFのホームノードがオンになっている `e0c` オン `node1`。
- ポート `e0d`、 `e0e`、 `e0f`および `e0g` 各ノードが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、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するブロードキャストドメインを作成します。これらのポートは、 SVM で使用されます。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 に作成した SVM では、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 9.1-9.7 に関連しています。

作業を開始する前に

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処理または参加処理中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、ブロードキャストドメインに追加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ない必要がありました。

このタスクについて

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、 ONTAP によって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。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たすべてのポートが含まれます。

- すべてのブロードキャストドメイン名が 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、を使用します `network port broadcast-domain remove-ports` 既存のブロードキャストドメインからポートを削除するコマンド。
- 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。
- 管理トラフィックを処理する e0M ポートを除く、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の MTU 値が一致している必要があります。
- 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
   ```

   ディスプレイが大きい場合は、を使用します `network port show -broadcast-domain` 未割り当てのポートのみを表示するコマンド。

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。

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

   - *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。

     ポートはという形式で追加されます *node_name:port_number*`例えば、 `node1:e0c。

3. 必要に応じて、ブロードキャストドメインが作成されたことを確認します。
   `network port show -instance -broadcast-domain new_domain`

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*

完了後

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、を使用します `network port broadcast-domain rename` コマンドを実行します

ブロードキャストドメインのポートを追加または削除する（**ONTAP 9.7**以前）

ブロードキャストドメインの最初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または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、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。

このタスクは、 ONTAP 9.8 ではなく、 ONTAP 9.1-9.7 に関連しています。

作業を開始する前に

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

このタスクについて

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 |
| --- | --- |
| 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。 | 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 は、ブロードキャストドメインの IPspace 値に更新されます。 | ポートは「 Default 」 IPspace に移動し、ブロードキャストドメイン属性はない。 |

を使用してインターフェイスグループの最後のメンバーポートを削除した場合 `network port ifgrp remove-port` このコマンドを実行すると、ブロードキャストドメインからインターフェイスグループポートが削除されます。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許可されていないためです。

手順

1. 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` コマンドを実行します
2. ブロードキャストドメインにポートを追加するか、ブロードキャストドメインからポートを削除します。

| 状況 | 使用 |
| --- | --- |
| ブロードキャストドメインにポートを追加します | `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します | `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 9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のスプリット（**ONTPA 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いくつかを含めることができます。

このタスクについて

- 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、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は、 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することができます。

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という手順を踏まなくて済みます。

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 値を変更することにより、そのブロードキャス

トドメインのすべてのポートの MTU 値を変更できます。これは、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。

作業を開始する前に

管理トラフィックを処理する e0M ポートを除く、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の MTU 値が一致している必要があります。

このタスクについて

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、回答の MTU 値を変更するために「 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。「 default 」IPspace は、このオプションの値を指定しないかぎり使用されます。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）

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

ステップ

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

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

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

```
network port broadcast-domain show
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 というブロードキャストドメインにある、更新ステータスがエラーのポートを表示します。このポートは、ポートを正しく更新できなかったことを示します。

```
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、を参照してください "ONTAP 9コマンドリファレンス"。

ブロードキャストドメインを削除する

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

作業を開始する前に

削除するブロードキャストドメインに、関連付けられているサブネット、ネットワークインターフェイス、 SVM がないようにします。

このタスクについて

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

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

**System Manager** の略

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

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

手順

1. [ネットワーク]>[概要]>[ブロードキャストドメイン*]を選択します。
2. 選択するオプション ⋮ 削除するブロードキャストドメインの横にある削除*をクリックします。

**CLI** の使用

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

LIF に有効なフェイルオーバーターゲットを設定していないと、 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、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。この機能により、管理者が自分のフェイルオーバーグループを管理する手間を省くことができます。

## フェイルオーバーグループを作成します

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。

### このタスクについて

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

- フェイルオーバーグループに追加できるポートは、ネットワークポート、 VLAN 、インターフェイスグループ（ ifgrp ）です。
- フェイルオーバーグループに追加するポートは、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
```

完了後

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

このタスクについて

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

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

  > フェイルオーバーをさらに制限する方法で LIF のサービスポリシーを変更すると、 LIF のフェイルオーバーポリシーが自動的に更新されます。

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

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

- ONTAP 9.11.1以降のオールフラッシュSANアレイ（ASA）プラットフォームでは、新規に作成したStorage VM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、を使用することもできます "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を意味します。

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

  > iSCSI LIF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のみ `local-only`、 `sfo-partner-only` および `disabled` がサポートされます。

- `broadcast-domain-wide` フェイルオーバーグループ内のすべてのノードのすべてのポートを環境 にします。
- `system-defined` 環境 は、LIFのホームノードとクラスタ内の他の1つのノード（存在する場合は通常はSFO以外のパートナー）にあるポートのみを対象とします。
- `local-only` 環境 を実行するのは、LIFのホームノードのポートだけです。
- `sfo-partner-only` 環境 を実行するのは、LIFのホームノードとそのSFOパートナーのポートだけです。
- `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。

ステップ

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を管理するためのコマンドです

を使用できます `network interface failover-groups` フェイルオーバーグループを管理するためのコマンド。を使用します `network interface modify` コマンドを使用して、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します。

| 状況 | 使用するコマンド |
| --- | --- |

| | |
|---|---|
| フェイルオーバーグループにネットワークポートを追加します | `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します | `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します | `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します | `network interface failover-groups delete` |

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

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

# 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。そのため、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して、LIFを簡単に作成できます。

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推奨します。また、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

## 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できます。

そのため、各 LIF の 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して簡単に LIF を作成できます。

### 作業を開始する前に

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。

### このタスクについて

- すべてのサブネット名が IPspace 内で一意である必要があります。
- サブネットに IP アドレスの範囲を追加するときは、別々のサブネットまたはホストで同じ IP アドレスが使用されないように、ネットワーク内で IP アドレスの範囲が重複しないことを確認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、または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、を使用する必要があります `route create` コマンドを使用してSVMにルートを手動で追加します。

### 手順

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

**System Manager** の略

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. をクリックします + Add をクリックしてください。
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. サブネットが属してい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** の使用

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。

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

- `broadcast_domain_name` は、サブネットが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。

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

- `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。

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

- 値 `true` に設定できます `-force-update-lif-associations` オプション

  指定した範囲の IP アドレスを現在使用しているサービスプロセッサまたはネットワークインターフェイスがある場合は、このコマンドが失敗します。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、 Default IPspace のブロードキャストドメイン default-1 に sub1 というサブネットを作成します。IPv4 のサブネット IP アドレスとマスク、ゲートウェイ、 IP アドレスの範囲を指定しています。

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

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

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

完了後

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、を使用します `network subnet rename` コマンドを実行します

## サブネットの **IP** アドレスを追加または削除します

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

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

**System Manager** の略

- 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. 選択するオプション ⋮ *>変更するサブネットの横にあるEdit *をクリックします。
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** の使用

- 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。*

このタスクについて

IP アドレスを追加するときに、追加しようとしている範囲の 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、を設定できます `-force-update-lif-associations` オプションをに設定します `true`。

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、を設定します `-force-update-lif-associations` オプションをに設定します `true`。

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 と 20~40 で、追加するアドレスが 11~19 と 41~50 （つまり、 1~50 を範囲にする）の場合は、次のコマンドを使用して既存のアドレス範囲と重複させることができます。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を変更します

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

このタスクについて

- IP アドレスを変更するときは、別々のサブネットまたはホストで同じ IP アドレスが使用されることのないように、ネットワーク内で IP アドレスの範囲が重複しない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は、 LIF を作成するときに、変更したゲートウェイがサブネットを使用して新しい SVM に適用されます。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する必要があります。

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

**System Manager** の略

- 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. 選択するオプション *>変更するサブネットの横にあるEdit *をクリックします。
3. 変更を加えます。
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** の使用

- 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）。個別の IP アドレス、 IP アドレスの範囲、またはその組み合わせをカンマで区切って指定できます。ここで指定した範囲によって、既存の IP アドレスが置き換えられます。
- `force-update-lif-associations` は、IPアドレス範囲を変更する場合に必要です。IP アドレスの範囲を変更する場合、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は、このコマンドが失敗します。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、 sub3 というサブネットのゲートウェイの IP アドレスを変更します。

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

## サブネットを表示します

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

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

**System Manager** の略

- 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** の使用

- 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 アドレスの範囲を表示します。

```
network subnet show
```

次のコマンドは、サブネットおよび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、そのサブネットの IP アドレスの割り当てを解除したい場合は、サブネットを削除します。

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

**System Manager** の略

- 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. 選択するオプション ⋮ 削除するサブネットの横にある削除*をクリックします。
3. 変更を保存します。

**CLI** の使用

- CLIを使用してサブネット*を削除してください

このタスクについて

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

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
```

# SVMs を作成します

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。

作業を開始する前に

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

  この SVM に Hyper-V over SMB または SQL Server over SMB 解決策を実装する予定がある場合は、ルートボリュームに NTFS セキュリティ形式を使用してください。Hyper-V ファイルまたは SQL データベースファイルを格納するボリュームは、作成時に NTFS セキュリティ形式に設定する必要があります。ルートボリュームのセキュリティ形式を NTFS に設定しておくと、 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することがありません。

- 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** の略

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. をクリックします ＋ Add Storage VMを作成してください。
3. Storage VMの名前を指定
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 |
| --- | --- |
| 管理者の名前 | 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。 |
| サーバー名 | 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。「CN=Computers」はデフォルト値であり、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。 |
| Network Interface の略 | 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。<br>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。<br>ホームポートを自動的に選択することも、リストから使用するポートを手動で選択することもできます。 |
| 管理者アカウントを管理する | 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。選択すると、ユーザ名とパスワードを指定し、確認のためにパスワードをもう一度入力し、Storage VM管理用に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. NFS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。エクスポートポリシー「default」にルールを追加して、マウントを中断なくトラバースできるようにします。 |

| | |
|---|---|
| ルール | をクリックします + Add ルールを作成します。<br><br>• 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。<br>• Access Protocols：次のオプションを組み合わせて選択します。<br>◦ SMB/CIFS<br>◦ FlexCache<br>◦ NFS<br>▪ NFSv3<br>▪ NFSv4<br>• 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。<br>◦ すべて<br>◦ すべて（匿名ユーザとして）<br>◦ 「 UNIX 」<br>◦ Kerberos 5.<br>◦ Kerberos 5i<br>◦ Kerberos 5p<br>◦ NTLM<br><br>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。 |
| Network Interface の略 | 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。<br>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。<br>ホームポートを自動的に選択することも、リストから使用するポートを手動で選択することもできます。 |

| | |
|---|---|
| 管理者アカウントを管理する | 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。選択すると、ユーザ名とパスワードを指定し、確認のためにパスワードをもう一度入力し、Storage VM管理用に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 |
|---|---|
| Network Interface の略 | 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。<br>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。<br>ホームポートを自動的に選択することも、リストから使用するポートを手動で選択することもできます。 |
| 管理者アカウントを管理する | 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。選択すると、ユーザ名とパスワードを指定し、確認のためにパスワードをもう一度入力し、Storage VM管理用に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。選択すると、ユーザ名とパスワードを指定し、確認のためにパスワードをもう一度入力し、Storage VM管理用に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 NVMe/FC *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。選択すると、ユーザ名とパスワードを指定し、確認のためにパスワードをもう一度入力し、Storage VM管理用に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 |
|---|---|
| Network Interface の略 | 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。<br>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。<br>ホームポートを自動的に選択することも、リストから使用するポートを手動で選択することもできます。 |
| 管理者アカウントを管理する | 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。選択すると、ユーザ名とパスワードを指定し、確認のためにパスワードをもう一度入力し、Storage VM管理用に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** の使用

ONTAP CLIを使用してサブネットを作成してください。

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

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

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

   ```
   vserver create -language ?
   ```

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

ONTAP 9.13.1以降では、アダプティブQoSポリシーグループテンプレートを設定して、SVM内のボリュームにスループットの下限と上限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を設定します。

# 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されるポートに設定できます。

クラスタ管理者は、次のものを作成、表示、変更、移行、リバートできます。 または LIF を削除します。SVM 管理者は、 SVM に関連付けられている LIF だけを表示できます。

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

ONTAP 9.10.1以降では、ファイアウォールポリシーは廃止され、完全にLIFのサービスポリシー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します"。

LIF をホストできるポートは次のとおりです。

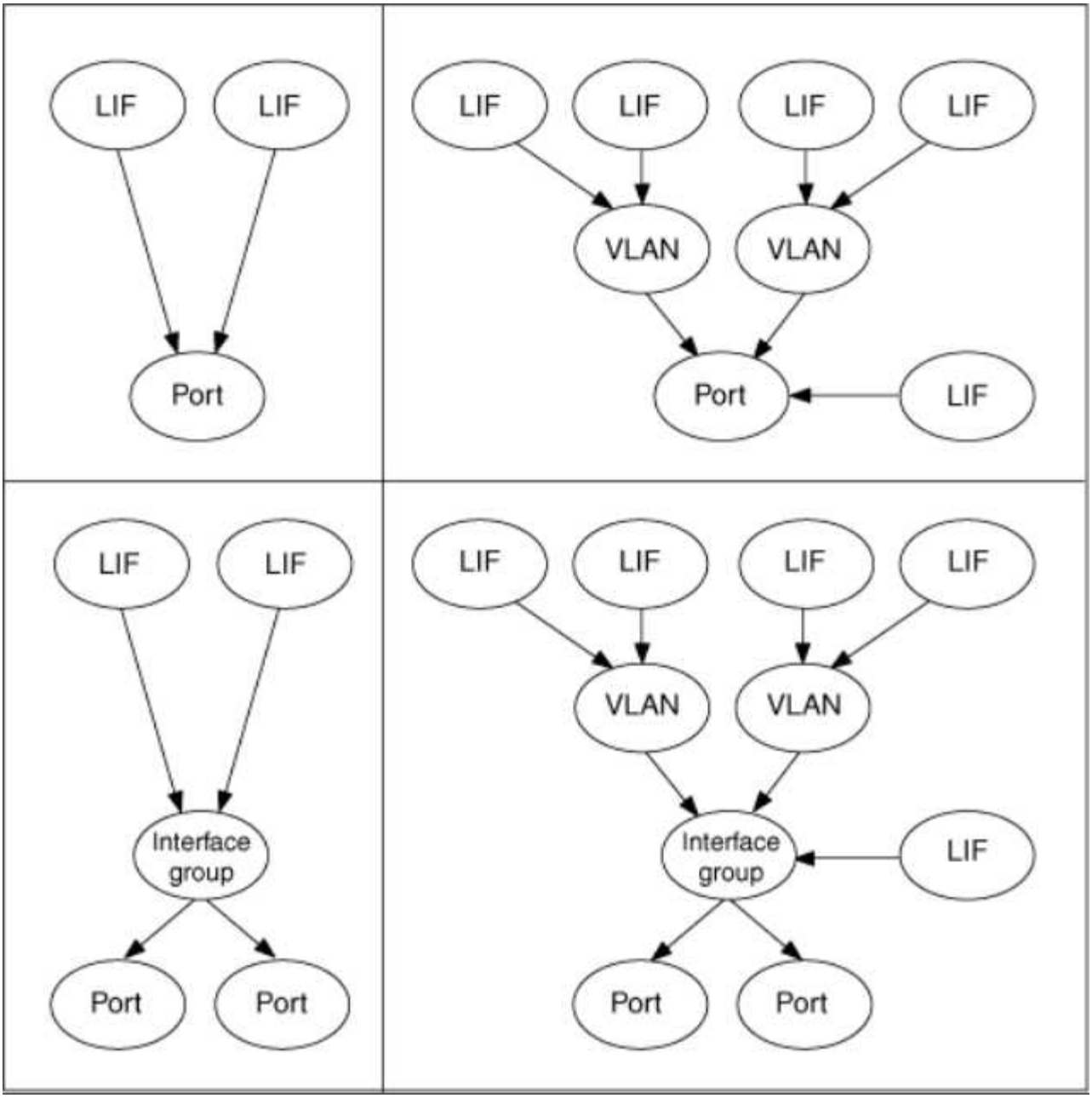
- インターフェイスグループに属していない物理ポート
- インターフェイスグループ
- VLAN
- VLAN をホストする物理ポートまたはインターフェイスグループ
- 仮想 IP （ VIP ）ポート

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

LIF で FC などの SAN プロトコルを設定する場合は、 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は、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たときに発生します。LIFのフェイルオーバーは、ONTAPによって自動的にトリガーされることも、クラスタ管理者が手動でトリガーして、物理イーサネットリンクの停止やノードのReplicated Database（RDB；レプリケートされたデータベース）クォーラムのメンバーでないノードなどのイベントが発生したときにトリガーされます。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理由が解決されるまで、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ホームポートの健常性が回復すると、LIFはHAパートナーからホームノードまたはホーム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を実行するには、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、次の手順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します"

- 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、自動リバートをに設定した場合に実行されます `true` LIFのホームポートが正常に機能しており、LIFをホストできる場合。
- 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で決定されます。
- フェイルオーバーが完了すると、LIFは正常に動作します。
- auto-revert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されます。 `true`。
- 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、auto-revertがに設定されている場合 `true`を選択すると、LIFがそれぞれのホームノードおよびホームポートにリバートされます。
- 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戻ったあと、およびauto-revertがに設定されている場合 `true`を選択すると、LIFがそれぞれのホームノードおよびホームポートにリバートされます。

ポートのタイプと **LIF** の互換性があります

## LIF には、さまざまなポートタイプをサポートするための特性があります。

クラスタ間 LIF と管理 LIF が同じサブネットに設定されていると、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 接続が失敗する可能性があります。システムをリカバリするには、を実行します `network interface modify -vserver` *`vserver name`* `-lif` *`intercluster LIF`* `-status-admin up|down` コマンドを入力してクラスタ間LIFを切り替えます。ただし、この問題を回避するには、クラスタ間 LIF と管理 LIF を別々のサブネットに設定する必要があります。

| LIF | 説明 |
| --- | --- |
| データ 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。<br>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。<br><br>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クラスタ内トラフィックに使用される LIF です。クラスタ LIF は、必ずクラスタポート上に作成する必要があります。<br><br>クラスタ LIF は、同じノードのクラスタポート間でフェイルオーバーできますが、リモートノードに移行またはフェイルオーバーすることはできません。新しいノードがクラスタに追加されると、 IP アドレスは自動的に生成されます。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含まれるようにする必要があります。 |
| クラスタ管理 LIF | クラスタ全体に対する単一の管理インターフェイスを提供する LIF です。<br><br>クラスタ管理 LIF は、クラスタ内の任意のノードにフェイルオーバーできます。クラスタポートまたはクラスタ間ポートにはフェイルオーバーできません |
| クラスタ間 LIF | クラスタ間の通信、バックアップ、およびレプリケーションに使用される LIF です。クラスタピア関係を確立する前に、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。<br><br>これらの LIF は、同じノードのポートにのみフェイルオーバーできます。クラスタ内の別のノードに移行またはフェイルオーバーすることはできません。 |
| ノード管理 LIF | クラスタ内の特定のノードを管理するために専用の IP アドレスを提供する LIF です。クラスタの作成時またはクラスタへのノードの追加時に作成されます。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 ポートで作成される任意のデータ LIF です。詳細については、を参照してください "仮想 IP （ VIP ） LIF を設定する"。 |

**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。

システム **SVM** のサービスポリシー

管理 SVM とすべてのシステム SVM には、管理 LIF とクラスタ間 LIF を含む、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 9.12.1以降のシステムSVMのLIFの組み込みのポリシーを示します。その他のリリースでは、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 | 含まれるサービス | 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。<br>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。<br>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や、システム全体に代わって実行されるアプリケーションをサポートするための追加の接続に使用できます。<br>ONTAP 9.12.1以降では、を使用できます `management-log-forwarding` 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を制御するサービス。 |

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

| サービス | フェイルオーバーの制限 | 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。<br>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。<br>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。<br>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。

次の表に、ONTAP 9.11.1以降の、データSVMのLIFの組み込みのポリシーを示します。その他のリリースでは、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 | 含まれるサービス | 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。これらのLIFは、必要に応じて、外部DNSサーバ、ADサーバ、LDAPサーバ、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ます。 |
| 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にLIFが1つしかないことがあるため、このポリシーでは、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LIFを使用することができます。これらの接続で管理LIFのみを使用する場合は、このポリシーからこれらのサービスを削除できます。 |
| 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以降で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で導入<br>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 |
| 管理 - portmap | - | portmap 管理アクセス用のサービス |

| | | |
|---|---|---|
| management-snmp-server | - | ONTAP 9.10.1で導入<br>SNMPサーバ管理アクセス用のサービス |
| 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 |
| データ 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で導入<br>Backup NDMP はデータサービスを制御します |
| data-dns-server | - | ONTAP 9.10.1で導入<br>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で導入<br>NVMe TCP データサービス |
| 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 の LIF に対するサービスポリシーの割り当てについて、次の点に注意してください。

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

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

- データプロトコルのリストを指定して LIF を作成した場合、指定したデータプロトコルと同等のサービスポリシーが LIF に割り当てられます。
- 同等のサービスポリシーが存在しない場合は、カスタムサービスポリシーが作成されます。
- サービスポリシー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。

データコアサービス

コアサービスでは、データロールが割り当てられた LIF を使用していたコンポーネントを、 LIF のロール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想定どおりに機能させることができます（ ONTAP 9.6 では廃止）。

コアをサービスとして指定してもファイアウォール内のポートは開かれませんが、データ SVM のサービスポリシーには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
- データ FlexCache

LIF を使用するすべてのアプリケーションが想定どおりに機能するように、コアサービスをポリシーに含めます。ただし、必要に応じて、他の 3 つのサービスは削除できます。

クライアント側の **LIF** サービス

ONTAP 9.10.1 以降の ONTAP は、複数のアプリケーションにクライアント側の 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。

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

| サービス | SVM の制限事項 | 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DNSサーバへのアウトバウンド接続にDNSクライアントサービスを提供します。 |
| management-ldap-clientの場合 | - | ONTAP 9.11.1以降では、ONTAPが外部LDAPサーバへのアウトバウンド接続に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 以降の ONTAP は、外部 NTP サーバへのアウトバウンド接続に NTP クライアントサービスを提供します。 |

| | | |
|---|---|---|
| data-fpolicy-client | データのみ | 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一部の組み込みのサービスポリシーに自動的に含まれますが、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するか、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 のロールにより、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のほか、適用されるフェイルオーバールール、適用される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 のロールには、 cluster 、 cluster management 、 data 、 intercluster 、 node management 、 undef （未定義）です。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** セキュリティ

| | データ 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 | はい。 | 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 | はい。 | いいえ | いいえ | はい。 |
| 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 | はい。 | いいえ | はい。 | はい。 | はい。 |

**LIF** フェイルオーバー

| | データ 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 |
|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| デフォルトの動作です | LIF のホームノードおよび 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内のポートにフェイルオーバーします | 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にフェイルオーバーします | 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にフェイルオーバーします | 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にフェイルオーバーします |
| カスタマイズ可能 | はい。 | いいえ | はい。 | はい。 | はい。 |

**LIF** のルーティング

| | データ 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別の IP サブネットにある場合 | なし | いずれかのプライマリトラフィックタイプで、別の IP サブネットへのアクセスが必要な場合 | 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 | まれです | なし | まれです | まれです | 別のクラスタのノードのクラスタ間 LIF が異なる 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 の欄に記載されたいずれかのトラフィックタイプを使用するには、ノード管理 LIF ではなく、データ LIF を経由します。これには、対応するファイアウォールの変更が必要です。 | なし | まれです | まれです | まれです |

**LIF** のリバランシング

| | データ 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 | はい。 | 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 | はい。 | 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

| | データ 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、ソフトウェアアップデートのロード | 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

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

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

を実行するにはadvanced権限が必要です `network interface service-policy create` コマンドを実行します

このタスクについて

データ SVM とシステム SVM の両方でデータトラフィックと管理トラフィックの管理に使用できる組み込みのサービスとサービスポリシーを用意しています。ほとんどのユースケースでは、カスタムサービスポリシーを作成するのではなく、組み込みのサービスポリシーを使用して対応できます。

これらの組み込みのサービスポリシーは必要に応じて変更できます。

手順

1. クラスタで使用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、およびクラスタで提供されるアプリケーションです。各サービスには、アプリケーションがリスンしている TCP ポートと UDP ポートが 0 個以上含まれます。

次のデータサービスと管理サービスも利用できます。

```
cluster1::> network interface service show

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

2. クラスタに存在するサービスポリシーを表示します。

```
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 」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、すべてのサブネットからのトラフィックが許可されます。デフォルト以外の許可アドレスリストを指定した場合、そのポリシーを使用する LIF は、指定したマスクと一致しないソースアドレスを使用するすべての要求を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.
```

完了後

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 にサービスポリシーを割り当てます

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

このタスクについて

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

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

| 実行する作業 | サービスポリシーを割り当てています ... |
| --- | --- |
| LIF を作成する | network interface create -vserver SVM_name -lif <LIF_name> -home-node <node_name > -home-port <port_name> ｛ （ -address <IP_address> -netmask <IP_address> ） -subnet-name <subnet_name> ｝ -service-policy <service_policy_name> |
| LIF の変更 | network interface modify -vserver <svm_name> -lif <lif_name> -service -policy <service_policy_name> |

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

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同じ SVM に含まれる LIF でのみ使用できます。

例

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

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

### LIF のサービスポリシーを管理するためのコマンド

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

作業を開始する前に

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、まず `snapmirror abort` 操作Then レプリケーション関係を再同期する。

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

作業を開始する前に

- 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またはを使用します `network subnet create` コマンドを実行します

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

このタスクについて

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

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

  - SMBトラフィックを伝送するLIFを、ホームノードに自動的にリバートするように設定しないでください。Hyper-V over SMB または SQL Server over SMB でノンストップオペレーションを実現する解決策を SMB サーバでホストする場合、これは必須です。

- 同じネットワークポート上に IPv4 と IPv6 の両方の LIF を作成できます。
- DNS 、 NIS 、 LDAP 、 Active Directory など、 SVM で使用され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 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 から到達可能である必要があります。
- ノード間のクラスタ内トラフィックを処理する LIF は、管理トラフィックを処理する LIF またはデータトラフィックを処理する LIF と同じサブネット上には存在しないようにしてください。
- 有効なフェイルオーバーターゲットのない LIF を作成すると、警告メッセージが表示されます。
- クラスタ内のLIFの数が多い場合は、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：を使用します `network interface capacity show` コマンドとを使用して、各ノードでサポートされるLIFの容量を確認します `network interface capacity details show` コマンド（advanced権限レベル）。
- ONTAP 9.7 以降では、同じサブネット内に SVM 用の他の LIF がすでに存在する場合、 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にある指定したホームノード上のランダムな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 の LIF とネームスペースは、同じノードでホストする必要があります。
- 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。複数のサブネットがある場合はサブネットを変更できますが、IPアドレスを変更することはできません。

- ネットワークインターフェイスに対してSVMを作成（追加）するときに、既存のサブネットの範囲内の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設定または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実行します。
- ONTAP 9.10.1以降の `network interface` CLIコマンドにはが含まれています `-rdma-protocols` NFS over RDMA構成用のパラメータ。ONTAP 9.12.1以降では、System ManagerでRDMA構成を使用するNFS用ネットワークインターフェイスの作成が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。

  iSCSI LIFのフェイルオーバーは自動的に有効になります（フェイルオーバーポリシーはに設定されます） `sfo-partner-only` auto-revertの値はに設定されています `true`）。指定したSVMにiSCSI LIFが存在しない場合、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。

  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iSCSI LIFがある場合に、同じSVMに新しいiSCSI LIFを作成すると、新しいiSCSI LIFでも同じフェイルオーバーポリシーが適用されます (`disabled`）を作成します。

  "ASA プラットフォームのiSCSI LIFのフェイルオーバー"

ONTAP 9.7 以降では、少なくとも 1 つの LIF が同じサブネットにすでに存在するかぎり、 ONTAP によって 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 のサブネットにまだ LIF がない場合を除き、指定する必要はありません。

ONTAP 9.12.0以降では、使用するインターフェイスに応じて次の手順 が使用されます。System ManagerまたはCLI：

**System Manager** の略

- 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. 選択するオプション + 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. クラスタ間
   c. SVM管理
4. プロトコルを選択します。
   a. SMB / CIFSとNFS
   b. iSCSI
   c. FC
   d. NVMe/FC
   e. NVMe/FC
5. LIFに名前を付けるか、以前の選択内容から生成された名前をそのまま使用します。
6. ホームノードを受け入れるか、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に少なくとも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選択します。
   b. サブネットを指定せずに続行すると、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. ブロードキャストドメインからホームポートを自動的に選択するか（推奨）、ドロップダウンメニューからホームポートを選択します。ホームポート制御は、ブロードキャストドメインまたは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** の使用

- 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の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。

```
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、の実行時にLIFが戻るノードです `network interface revert` LIFに対してコマンドを実行します。

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

   - `-home-port` は、の実行時にLIFが戻る物理ポートまたは論理ポートです `network interface revert` LIFに対してコマンドを実行します。
   - でIPアドレスを指定できます `-address` および `-netmask` オプションを使用するか、サブネットからの割り当てを有効にするには、 `-subnet_name` オプション
   - 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。
   - サブネットを使用せずに手動で IP アドレスを割り当てると、クライアントまたはドメインコントローラが別の IP サブネットにある場合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。デフォルト設定はです `false`に設定することもできます `true` 環境内のネットワーク管理ポリシーによって異なります。
   - `-service-policy` ONTAP 9.5以降では、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` オプション
     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、データプロトコルのリストが作成されます。ONTAP 9.5 では、クラスタ間および BGP ピアのサービスについてのみサービスポリシーがサポートされます。ONTAP 9.6 では、複数のデータサービスおよび管理サービスに対してサービスポリシーを作成できます。

- `-data-protocol` FCPまたはNVMe/FCプロトコルをサポートするLIFを作成できます。IP LIFを作成する場合、このオプションは必要ありません。

4. オプション：-addressオプションでIPv6アドレスを割り当てます。

   a. network ndp prefix show コマンドを使用し、各種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。

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

   b. の形式を使用します `prefix::id` 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。

   を導出するため `id`で、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 |
| --- | --- |

| | |
|---|---|
| IPv4 アドレス | ネットワーク ping |
| IPv6アドレス | ネットワーク ping6 |

例

次のコマンドでは、を使用して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ます `-address` および `-netmask` パラメータ：

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

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

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

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

```
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 の属性は変更することができます。これには、ホームノードや現在のノード、管理ステータス、 IP アドレス、ネットマスク、フェイルオーバーポリシー、 ファイアウォールポリシー、およびサービスポリシー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。

このタスクについて

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

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

- FC LIF で使用され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 を削除して作成し直す必要があります。IP

LIF にサービスポリシーを変更するには、更新が短時間停止します。

- ノードを対象とした管理 LIF のホームノードや現在のノードを変更することはできません。
- LIF の IP アドレスとネットワークマスク値を変更するためにサブネットを使用すると、指定したサブネットから IP アドレスが割り当てられます。 LIF の以前の IP アドレスが別のサブネットから割り当てられた場合は、そのサブネットに IP アドレスが返されます。
- 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て、に新しい値を追加する必要があります `-netmask-length` パラメータ
- 自動構成されたリンクローカル IPv6 アドレスは変更できません。
- LIF の変更によって、 LIF に有効なフェイルオーバーターゲットがなくなる場合は警告メッセージが表示されます。

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

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

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

- ONTAP 9.11.1以降では、オールフラッシュSANアレイ（ASA）プラットフォームで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）の場合は、フェイルオーバーポリシーを "iSCSI LIFの自動フェイルオーバーを有効にする"。

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

**System Manager** の略

- 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. 選択するオプション ⋮ *>変更するネットワークインターフェイスの横にある[Edit]をクリックします。
3. ネットワークインターフェイスの設定を変更します。詳細については、を参照してください "LIF を作成"。
4. 変更を保存します。

**CLI** の使用

- LIFの変更にはCLIを使用してください*

手順

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

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

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

   次の例は、 LIF のサービスポリシーを変更する方法を示しています。

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

2. IP アドレスに到達できることを確認します。

| 使用するポート | 使用する方法 |
| --- | --- |
| IPv4 アドレス | `network ping` |
| IPv6アドレス | `network ping6` |

**LIF** を移行

ポートで障害が発生した場合やメンテナンスを行う場合など、同じノードの別のポートやクラスタ内の別のノードに LIF を移行しなければならないことがあります。LIF の移行は LIF のフェイルオーバーと似ていますが、 LIF の移行は手動で行います。 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のリンク障害に対応して LIF を自動的に移行する機能です。

作業を開始する前に

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

このタスクについて

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

  この問題を回避するには、 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。

  この問題を回避するには、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 "iSCSI LIFを作成しています"。

- NFS over RDMA用の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。ONTAP 9.10.1以降を実行してCLIでLIFを移行するか、ONTAP 9.12.1を実行してSystem Managerで移行する必要があります。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。の詳細を確認してください "NFS over RDMA用のLIFを設定しています"。
- VMware VAAI のコピーオフロード処理は、ソース LIF またはデスティネーション LIF を移行すると失敗します。コピーオフロードについては、以下を参照してください。
  - "NFS環境"
  - "SAN 環境"

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

**System Manager** の略

- 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. 選択するオプション ⋮ *>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が完全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** の使用

- 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、該当する操作を実行します。

| 移行する項目 | 入力するコマンド |
| --- | --- |
| 特定の LIF | `network interface migrate` |
| ノードのすべてのデータ 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、という名前のLIFを移行する方法を示しています `datalif1` 指定します `vs0` をポートに追加します `e0d` オン `node0b`：

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

次の例は、現在（ローカル）のノードからすべてのデータ 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する

## 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、その LIF は現在のポートにとどまり、リバートされません。

このタスクについて

- 自動リバートオプションを設定する前に LIF のホームポートの状態を up にすると、 LIF はホームポートにリバートされません。
- 「 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ることはありません。
- LIF がホームポートにリバートされるように、「 auto-revert 」オプションを有効にしてください。

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

**System Manager** の略

- 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. 選択するオプション ⋮ >変更するネットワークインターフェイスの横にある復帰。
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** の使用

- 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 |
|---|---|
| 手動で実行する | `network interface revert -vserver vserver_name -lif lif_name` |
| 自動的に | `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、クラスタ IPspace に設定されたすべてのポートがクラスタ IPspace に設定された他のポートに到達できない場合は、クラスタを作成できません。

このタスクについて

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は、が表示されます `cluster create` 次のエラーが表示されてコマンドが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.
```

の結果 `network port show` コマンドでは、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、の結果 `network port reachability show -detail` コマンドは、相互に接続されていないポートを表示します。

クラスタ LIF が設定された他のポートに到達できないポート上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 ）を削除できます。

作業を開始する前に

削除する LIF が使用中でないことを確認します。

手順

1. 次のコマンドを使用して、削除する LIF を意図的に停止したものとしてマークします。

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

2. を使用します `network interface delete` 1つまたはすべてのLIFを削除するコマンド：

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

# 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することができます。その結果、 LIF とポートがバランスよく使用されるようになり、クラスタのパフォーマンスが向上します。

DNS ロードバランシングを使用すると、負荷が適切なデータ LIF を選んで、使用可能なデータポートすべて（物理、インターフェイスグループ、 VLAN ）にユーザネットワークのトラフィックを分散させることができます。

DNS ロードバランシングでは、 LIF が SVM のロードバランシングゾーンに関連付けられます。サイト規模の DNS サーバは、すべての DNS 要求を転送し、ネットワークトラフィックおよびポートのリソースの可用性（ CPU 使用率、スループット、開いている接続など）に基づいて負荷の最も少ない LIF を返すように設定されています。DNS ロードバランシングのメリットは次のとおりです。

- 新しいクライアント接続が、使用可能なリソース全体に分散されます。
- 特定の SVM をマウントするときに使用する LIF を手動で決める必要がありません。
- 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に対応しています。

## **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します

DNS ロードバランシングゾーンを作成すると、 LIF にマウントされているクライアントの数など、負荷に基づいて LIF を動的に選択できるようになります。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。

作業を開始する前に

サイト規模の DNS サーバ上に、設定した LIF にロードバランシングゾーンに対するすべての要求を転送する DNS フォワーダを設定しておく必要があります。

技術情報アーティクル "clustered Data ONTAP での DNS ロードバランシングの設定方法" NetApp Support Siteには、条件付き転送を使用する DNS ロードバランシングの設定に関する詳細が記載されています。

このタスクについて

- すべてのデータ LIF は、 DNS ロードバランシングゾーン名の DNS クエリに応答できます。
- DNS ロードバランシングゾーンの名前はクラスタ内で一意でなければなりません。ゾーン名の要件は次のとおりです。
  - 256 文字以内にする必要があります。
  - ピリオドが少なくとも 1 つ必要です。
  - 先頭と末尾の文字をピリオドなどの特殊文字にすることはできません。
  - 文字間にスペースを使用することはできません。
  - DNS 名の各ラベルの最大文字数は 63 文字です。

    ラベルは、ピリオドの前後のテキストです。たとえば、 storage.company.com という名前の DNS ゾーンは 3 つのラベルで構成されています。

ステップ

を使用します `network interface create` コマンドにを指定します `dns-zone` DNSロードバランシングゾーンを作成するオプション。

ロードバランシングゾーンがすでに存在する場合は、 LIF がそのロードバランシングゾーンに追加されます。コマンドの詳細については、を参照してください。 "ONTAP 9コマンドリファレンス"。

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ます `lif1`：

```
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して **LIF** を追加または削除する

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。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。

作業を開始する前に

- 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。
- 各 LIF は 1 つの DNS ロードバランシングゾーンにのみ含めることができます。
- サブネットの異なる LIF がある場合は、サブネットごとのフェイルオーバーグループが設定されている必要があります。

このタスクについて

管理ステータスが down の LIF は一時的に DNS ロードバランシングゾーンから削除されます。LIF の管理ステータスが up に戻ると、自動的に DNS ロードバランシングゾーンに追加されます。

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`*<br>例<br>`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`<br>例<br>`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`<br>例<br>`network interface modify -vserver vs0 -lif * -dns-zone none`<br>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。

このタスクについて

Active Directory 統合 DNS サーバには、ドメイン LDAP およびドメインコントローラサーバのサービスロケーションレコード（ SRV ）が格納されます。SVM が Active Directory LDAP サーバおよびドメインコントローラを見つけられない場合は、 NFS または SMB サーバのセットアップに失敗します。

SVM は、ホストについての情報を検索する際に、 hosts ネームサービス ns-switch データベースを使用してどのネームサービスを使用するか、どの順番で使用するかを決定します。hosts データベースでサポートされている 2 つのネームサービスは、 files および dns です。

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

mgwd プロセスと SecD プロセスについて DNS ネームサービスの統計を表示するには、統計画面を使用します。

手順

1. hosts ネームサービスデータベースの現在の設定を確認します。この例では、 hosts ネームサービスデータベースはデフォルトの設定を使用しています。

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

   ```
   Vserver: vs1
   Name Service Switch Database: hosts
   Vserver: vs1 Name Service Switch Database: hosts
   Name Service Source Order: files, dns
   ```

2. 必要に応じて、次の操作を実行します。

   a. DNS ネームサービスを希望の順序で hosts ネームサービスデータベースに追加するか、ソースの順序を変更します。

      この例では、 DNS ファイルとローカルファイルを順に使用するように 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 サービスを設定する

   ```
   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 コマンドを使用すると、設定の自動検証が行われ、 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てください。

   ```
   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** に動的 **DNS** を設定します

Active Directory に統合された 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。

作業を開始する前に

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 DDNS を使用する場合は、 Active Directory 統合 DNS ネームサーバを使用して、 SVM 用の NFS または SMB サーバまたは Active Directory アカウントを作成しておく必要があります。

このタスクについて

完全修飾ドメイン名（ FQDN ）は一意にする必要があります。

完全修飾ドメイン名（ FQDN ）は一意にする必要があります。

- NFSの場合は、で指定した値です `-vserver-fqdn` の一部として `vserver services name-service dns dynamic-update` コマンドがLIFの登録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された値が、 LIF の登録済み FQDN になります。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 更新の RFC ルールに準拠していない SVM FQDN の設定エラーを回避するには、 RFC に準拠した FQDN 名を使用します。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。例： `*.netapp.com` が無効です。

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。

このタスクについて

Active Directory 統合 DNS サーバには、ドメイン LDAP およびドメインコントローラサーバのサービスロケーションレコード（ SRV ）が格納されます。SVM が Active Directory LDAP サーバおよびドメインコントローラを見つけられない場合は、 NFS または SMB サーバのセットアップに失敗します。

SVM は、ホストについての情報を検索する際に、 hosts ネームサービス ns-switch データベースを使用してどのネームサービスを使用するか、どの順番で使用するかを決定します。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です `files` および `dns`。

それを確認する必要があります `dns` は、SMBサーバを作成する前のソースの1つです。

mgwd プロセスと SecD プロセスについて DNS ネームサービスの統計を表示するには、統計画面を使用します。

手順

1. の現在の設定を確認します `hosts` ネームサービスデータベース

   この例では、 hosts ネームサービスデータベースはデフォルトの設定を使用しています。

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

   ```
                         Vserver: vs1
   Name Service Switch Database: hosts
      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序で hosts ネームサービスデータベースに追加するか、ソースの順序を変更します。

      この例では、 DNS ファイルとローカルファイルを順に使用するように 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 サービスを設定する

   ```
   vserver services name-service dns create -vserver vs1 -domains
   ```

*example.com,example2.com* -name-servers *10.0.0.50,10.0.0.51*

SVMサービス `name-service dns create` コマンドは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てください。

```
           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** に動的 **DNS** を設定します

Active Directory に統合された 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。

作業を開始する前に

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 DDNS を使用する場合は、 Active Directory 統合 DNS ネームサーバを使用して、 SVM 用の NFS または SMB サーバまたは Active Directory アカウントを作成しておく必要があります。

このタスクについて

完全修飾ドメイン名（ FQDN ）は一意にする必要があります。

- NFSの場合は、で指定した値です `-vserver-fqdn` の一部として `vserver services name-service dns dynamic-update` コマンドがLIFの登録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された値が、 LIF の登録済み FQDN になります。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 更新の RFC ルールに準拠していない SVM FQDN の設定エラーを回避するには、 RFC に準拠した FQDN 名を使用します。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。例： `*.netapp.com` が無効です。

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 サービスを設定する

Active Directory に統合された 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。

作業を開始する前に

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 DDNS を使用する場合は、 Active Directory 統合 DNS ネームサーバを使用して、 SVM 用の NFS または SMB サーバまたは Active Directory アカウントを作成しておく必要があります。

このタスクについて

一意の FQDN を指定する必要があります。

DDNS 更新の RFC ルールに準拠していない SVM FQDN の設定エラーを回避するには、 RFC に準拠した FQDN 名を使用します。

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。例： `*.netapp.com` が無効です。

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 では、クライアントにアクセスを提供したりサービスにアクセスしたりするために、ホスト名を数値の IP アドレスに変換できなければなりません。Storage Virtual Machine （ SVM ）でローカルまたは外部のネームサービスを使用してホスト情報を解決するように設定する必要があります。ONTAP では、ホスト名を解決するために外部 DNS サーバまたはローカルの hosts ファイルを使用するように設定できます。

外部 DNS サーバを使用する場合は、動的 DNS （ DDNS ）を設定できます。これにより、新規または変更された DNS 情報がストレージシステムから DNS サーバに自動的に送信されます。動的 DNS 更新を使用しない場合は、新しいシステムがオンラインになったときや既存の DNS 情報が変更されたときに、特定された DNS サーバに手動で DNS 情報（ DNS の名前と IP アドレス）を追加する必要があります。このプロセスは時間が

かかり、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で設定を行っていると、ダウンタイムが長くなる可能性があります。

## ホスト名解決に使用する **DNS** を設定します

ホスト情報を取得するには、 DNS を使用してローカルソースまたはリモートソースにアクセスします。これらのソースのいずれかまたは両方にアクセスするために DNS を設定する必要があります。

ONTAP がクライアントに適切なアクセスを許可するには、ホスト情報を検索できなければなりません。ネームサービスを設定して、 ONTAP がホスト情報を取得するためにローカルまたは外部の DNS サービスにアクセスできるようにします。

ONTAP では、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` UNIX システム上のファイル。

### 外部 **DNS** サーバを使用して、ホスト名解決のために **SVM** とデータ **LIF** を設定する

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

#### 作業を開始する前に

ホスト名を検索するために、サイト規模の DNS サーバが使用可能である必要があります。

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つだけの場合は警告が表示されます。

#### このタスクについて

を参照してください 動的 DNS サービスを設定する SVMでの動的DNSの設定に関する詳細については、を参照してください。

#### 手順

1. SVM で DNS を有効にします。

```
vserver services name-service dns create -vserver <vserver_name>
-domains <domain_name> -name-servers <ip_addresses> -state enabled
```

次のコマンドは、 SVM vs1 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
```

。 `vserver services name-service dns create` コマンドは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. を使用してネームサーバのステータスを検証します `vserver services name-service dns check` コマンドを実行します

```
vserver services name-service dns check -vserver vs1.example.com
                                        Name Server
Vserver             Name Server     Status       Status Details
-------------       --------------- ------------
--------------------------
vs1.example.com     10.0.0.50       up           Response time (msec): 2
vs1.example.com     10.0.0.51       up           Response time (msec): 2
```

DNSに関連するサービスポリシーの詳細については、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"。

ホスト名解決用のネームサービススイッチテーブルを設定します

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。

作業を開始する前に

環境内のホストのマッピングでどのネームサービスを使用するかを決めておく必要があります。

手順

1. ネームサービススイッチテーブルに必要なエントリを追加します。

```
vserver services name-service ns-switch modify -vserver <vserver_name>
-database <database_name> -source <source_names>
```

2. ネームサービススイッチテーブルに想定されるエントリが適切な順序で格納されていることを確認します。

```
vserver services name-service ns-switch show -vserver <vserver_name>
```

例

次の例は、SVM vs1のネームサービススイッチテーブル内のエントリを、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、表示できます。SVM 管理者は、割り当てられた SVM に対してのみホスト名エントリを設定できます。

ローカルホスト名エントリを管理するコマンド

を使用できます `vserver services name-service dns hosts` DNSホストテーブルエントリを作成、変更、または削除するコマンド。

DNS ホスト名エントリを作成または変更するときは、複数のエイリアスアドレスをカンマで区切って指定できます。

| 状況 | 使用するコマンド |
| --- | --- |
| DNS ホスト名エントリを作成します | `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` |

詳細については、を参照してください `vserver services name-service dns hosts` コマンド、を参照 "ONTAP 9コマンドリファレンス"。

# ネットワークを保護します

## 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 接続に対する連邦情報処理標準（ FIPS ） 140-2 に準拠しています。ONTAP では、 SSL FIPS モードを有効または無効にしたり、 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、 ONTAP の SSL は、次のプロトコルを使用して FIPS 準拠が無効、 SSL プロトコルが有効な状態で設定されます。

- TLSv1（ONTAP 9.11.1以降）
- TLSv1.2
- TLSv1.1
- TLSv1

SSL FIPS モードがイネーブルの場合、 ONTAP から ONTAP 外部のクライアントまたはサーバコンポーネントへの SSL 通信には、 FIPS 準拠の SSL 用暗号が使用されます。

管理者アカウントが SSH 公開鍵を使用して SVM にアクセスできるようにする場合は、 SSL FIPS モードを有効にする前に、ホストキーアルゴリズムがサポートされていることを確認する必要があります。

*注：ONTAP 9.11.1以降では、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+<br>rsa-sha2-256+<br>SSH-ed25519以降<br>SSH-DSS+<br>SSH-RSA |
| 9.10.1以前 | ECDSA-sha2-nistp256+<br>SSH-ed25519 | SSH-DSS+<br>SSH-RSA |

FIPS を有効にする前に、サポートされるキーアルゴリズムを使用していない既存の SSH 公開鍵アカウントをサポート対象のキータイプで再設定する必要があります。再設定しないと、管理者認証は失敗します。

詳細については、を参照してください "SSH 公開鍵アカウントを有効にします"。

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

**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、すべてのセキュアユーザがセキュリティ設定を調整することを推奨します。SSL FIPS モードがイネーブルの場合、 ONTAP から ONTAP 外部のクライアントまたはサーバコンポーネントへの SSL 通信には、 FIPS 準拠の SSL 用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、と入力します `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** を無効にする

古いシステム構成を実行し続けている状況で、 ONTAP の設定で下位互換性を確保する場合は、 FIPS が無効な場合にのみ SSLv3 を有効にすることができます。

手順

1. advanced 権限レベルに切り替えます。

   ```
   set -privilege advanced
   ```

2. 次のように入力して FIPS を無効に

   ```
   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、と入力します `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** 準拠ステータスを表示します

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することができます。

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ていること、および FIPS のオン / オフモード、プロトコル、暗号に対する変更がすべて反映されていることを確認するには、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
```

## ワイヤ暗号化を介した **IP** セキュリティ（ **IPsec** ）を設定します

ONTAPは、転送モードでインターネットプロトコルセキュリティ(IPsec)を使用して、転送中もデータの安全性と暗号化を継続的に確保します。IPSec では、 NFS 、 iSCSI 、

## SMB の各プロトコルを含むすべての IP トラフィックを暗号化できます。

ONTAP 9.12.1以降では、フロントエンドホストプロトコルIPsecサポートは、MetroCluster IPおよびMetroCluster ファブリック接続構成で利用できます。
MetroCluster クラスタでのIPSecのサポートは、フロントエンドのホストトラフィックに限定され、MetroCluster のクラスタ間LIFではサポートされません。

ONTAP 9.10.1 以降では、 Pre-Shared Key （ PSK; 事前共有キー）または証明書のいずれかを使用して IPSec での認証を行うことができます。以前は、 IPsec でサポートされていたのは PSK だけでした。

ONTAP 9.9.1以降では、IPsecで使用される暗号化アルゴリズムがFIPS 140-2に準拠しています。アルゴリズムは、ONTAP のNetApp Cryptographic Moduleによって生成され、FIPS 140-2認定を継承しています。

ONTAP 9.8以降では、ONTAPでトランスポートモードのIPsecがサポートされます。

IPSec の設定後は、リプレイ攻撃や中間者（ MITM ）攻撃に対抗するための予防措置を講じて、クライアントと ONTAP 間のネットワークトラフィックを保護します。

NetApp SnapMirror およびクラスタピアリングトラフィックの暗号化では、クラスタピアリング暗号化（ CPE ）の場合でも、 IPSec 経由でセキュアな転送レイヤセキュリティ（ TLS ）を使用することを推奨します。これは、TLSの方がIPsecよりもパフォーマンスが優れているためです。

クラスタで IPSec 機能が有効になっている場合、ネットワークでトラフィックを処理するには、保護対象のトラフィックと一致する Security Policy Database （ SPD ）エントリ、および保護の詳細（暗号スイートや認証方式など）を指定する必要があります。各クライアントには、対応する SPD エントリも必要です。

### クラスタで **IPSec** を有効に設定します

クラスタの IPSec を有効にして、転送中もデータのセキュリティを継続的に確保し、暗号化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検出します。

   ```
   security ipsec config show
   ```

   結果にが含まれている場合 `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
   ```

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た `IPsec Enabled: true`。

### 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。

- エンドエンティティ（ONTAPまたはクライアント）の証明書を両側で検証できるように、ONTAPとクライアントの両方に相手のCA証明書をインストールする必要があります。
- ポリシーに含まれる ONTAP LIF の証明書がインストールされます

ONTAP LIF は証明書を共有できます。証明書と LIF の間に 1 対 1 のマッピングは必要ありません。

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、を使用して、ONTAP証明書管理CAをIPsecモジュールに追加します。 `security ipsec ca-certificate add` コマンドを実行します

   サンプルコマンド
   ```
   cluster::> security ipsec ca-certificate add -vserver svm_name -ca-certs
   my_ca_cert
   ```

3. ONTAP LIF で使用する証明書を作成してインストールします。この証明書の発行元 CA がすでに ONTAP にインストールされ、 IPSec に追加されている必要があります。

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

ONTAPの証明書の詳細については、ONTAP 9のドキュメントのsecurity certificateコマンドを参照してください。

セキュリティポリシーデータベース（ **SPD** ）の定義

IPSec では、トラフィックをネットワーク上に転送する前に 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している場合にも当てはまります。

手順

1. を使用します `security ipsec policy create` コマンドの宛先：
   a. ONTAP IP アドレスまたは IP アドレスのサブネットを選択して、 IPSec 転送に参加します。
   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、 Pre-Shared Key （ 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. 任意。上位層プロトコル（UDP、TCP、ICMPなど）など、きめ細かなトラフィックパラメータを選択します。）、ローカルポート番号、およびトラフィックを保護するリモートポート番号。対応するパラメータはです `protocols`、 `local-ports` および `remote-ports` それぞれ。

   ONTAP IP アドレスとクライアント IP アドレスの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。デフォルトでは、すべてのトラフィックを保護します。

d. の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` 必要な認証方式のパラメータ。

   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` および `remote-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、パラメータはオプションです。

   ii. PKIを入力する場合は、も入力する必要があります `cert-name`、 `local-identity`、 `remote-identity` パラメータ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、特殊なIDを入力します。 `ANYTHING`。

```
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。詳細については、クライアント側のIPsec設定を参照してください。

**IPsec ID** を使用する

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、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はオプションです。

PKI/ 証明書認証方式の場合、ローカル ID とリモート ID の両方が必須です。IDは、各側の証明書内で認証され、検証プロセスで使用されるIDを指定します。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を使用します `ANYTHING`。

このタスクについて

ONTAP では、 SPD エントリを変更するか、または SPD ポリシーを作成する際に、 ID を指定します。SPD には、 IP アドレスまたは文字列形式の ID 名を使用できます。

ステップ

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
```

コマンドの例を示します

```
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

多数のクライアントで IPSec を利用する必要がある場合、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で IPSec を利用する必要がある場合には、 IPSec の複数クライアント設定を使用することを推奨します。

このタスクについて

ONTAP では、 IPSec が有効な単一の SVM IP アドレスに、多数のネットワーク上にある複数のクライアントを接続できます。これを行うには、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、を指定する必要があります `remote-ip-subnets` サブネット形式。また、を指定する必要があります `remote-identity` フィールドに正しいクライアント側IDを入力します。

  > サブネット設定で 1 つ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 Pre-Shared Key （ PSK ；事前共有キー）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、各クライアントは独自の一意の証明書または共有証明書を使用して認証できます。ONTAP IPSec は、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、証明書の有効性をチェックします。ONTAP は、証明書失効リスト (CRL) チェックもサポートしています。

- * 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にSVMのIPsec対応IPアドレスへの接続を許可するには、を使用します `0.0.0.0/0` ワイルドカードヲシテイスルバアイ `remote-ip-subnets` フィールド。

  また、を指定する必要があります `remote-identity` フィールドに正しいクライアント側IDを入力します。証明書認証の場合は、と入力できます `ANYTHING`。

  また、ときに `0.0.0.0/0` ワイルドカードを使用する場合は、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。例： `NFS port 2049`。

  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
     ```

コマンドの例を示します

```
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
```

コマンドの例を示します

```
security ipsec policy create -vserver vs1 -name test35 -local-ip-subnets
IPsec_IP_address/32 -remote-ip-subnets 0.0.0.0/0 -local-ports 2049 -local
-identity ontap_side_identity -remote-identity client_side_identity
```

**IPSec** の統計情報

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を実行する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。

コマンドの例を示します

IKE SA サンプルコマンド：

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

IPSec SA サンプルコマンドおよび出力：

```
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 サンプルコマンドおよび出力：

```
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します

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を強化して、ストレージシステムへの不正アクセスを防止するのに役立ちます。デフォルトでは、オンボードファイアウォールは、データ LIF 、管理 LIF 、クラスタ間 LIF の特定の IP サービス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。これまでは、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。この機能は、LIF のサービスポリシーを使用して実行されるようになりました。
- すべてのファイアウォールポリシーが空であり、基盤となるファイアウォールのどのポートも開かない。代わりに、 LIF のサービスポリシーを使用してすべてのポートを開く必要があります。
- ファイアウォールポリシーからLIFサービスポリシーに移行するために9.10.1以降にアップグレードしたあとは必要な処理はありません。以前のONTAP リリースで使用されていたファイアウォールポリシーと整合性のあるLIFサービスポリシーが自動的に構築されます。カスタムファイアウォールポリシーを作成および管理するスクリプトやその他のツールを使用している場合は、カスタムサービスポリシーを作成するスクリプトのアップグレードが必要になることがあります。

詳細については、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 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。 NDMP 、 NDMPS 、 RSH 、 DNS 、または SNMP 。NFS や SMB などのデータプロトコル用にファイアウォールポリシーを設定することはできません。

ファイアウォールサービスとポリシーは、次の方法で管理できます。

- ファイアウォールサービスを有効または無効にします
- 現在のファイアウォールサービスの設定を表示しています
- 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してください
- ファイアウォールポリシーを論理インターフェイスに適用する
- 既存のファイアウォールポリシーとまったく同一の新しいポリシーを作成する

この機能は、同じ SVM 内でよく似たポリシーを作成するときや、別の SVM にポリシーをコピーするときに使用できます。

- ファイアウォールポリシーに関する情報を表示する
- ファイアウォールポリシーで使用する IP アドレスとネットマスクを変更する
- LIF で使用していないファイアウォールポリシーを削除する

ファイアウォールポリシーと **LIF**

LIF のファイアウォールポリシーは、各 LIF を介したクラスタへのアクセスを制限するために使用します。デフォルトのファイアウォールポリシーが、各タイプの LIF を介したシステムアクセスにどのように影響するか、および LIF のセキュリティを強化または低下させるためにファイアウォールポリシーをカスタマイズする方法について理解しておく必要があります。

を使用してLIFを設定する場合 `network interface create` または `network interface modify` コマンドを入力します。に指定した値です `-firewall-policy` パラメータは、LIFへのアクセスを許可するサービスプロトコルとIPアドレスを決定します。

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。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は、 SSH 、 HTTP 、 HTTPS 、 Telnet 、 NTP 、 NDMP 、 NDMPS 、 RSH 、 DNS 、および SNMP 。

すべてのクラスタLIFのファイアウォールポリシーのデフォルトはです `""` およびは変更できません。

次の表に、 LIF の作成時にそのロール（ ONTAP 9.5 以前）またはサービスポリシー（ ONTAP 9.6 以降）に応じて LIF に割り当てられるデフォルトのファイアウォールポリシーを示します。

| ファイアウォールポリシー | デフォルトのサービスプロトコル | デフォルトのアクセス権 | 割り当て先の 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 |
| Mgmt - NFS を管理します | 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 RPC サービスがリスンするポートにマッピングします。

ONTAP 9.3 以前では portmap サービスに常にアクセス可能で、 ONTAP 9.4 では ONTAP 9.6 で設定可能になっており、 ONTAP 9.7 以降では自動的に管理されます。

- ONTAP 9.3 までは、サードパーティのファイアウォールではなく組み込みの ONTAP ファイアウォールを使用するネットワーク構成では、ポート 111 で portmap サービス（ rpcbind ）へのアクセスが常に許可されていました。
- ONTAP 9.4 から ONTAP 9.6 までは、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が廃止されています。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 リリースから ONTAP 9.6 リリースまでの portmap ファイアウォールサービスの設定方法について説明します。

設定によっては、特定のタイプの LIF 、通常は管理 LIF とクラスタ間 LIF でのサービスへのアクセスを禁止できる場合があります。状況によっては、データ LIF からのアクセスも禁止できます。

想定される動作

ONTAP 9.4 から ONTAP 9.6 への動作は、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可能なサービスをLIFタイプ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。影響を受け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 から 9.6 にアップグレードした場合、 ONTAP は、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 サービスを追加します。
- 新しいクラスタ ONTAP 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
```

既存の LIF にファイアウォールポリシーを適用するには、 network interface modify コマンドを使用します。

コマンド構文全体については、を参照してください "ONTAP 9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 を作成するときに、デフォルトのファイアウォールポリシーが割り当てられます。多くの場合、ファイアウォールのデフォルト設定をそのまま使用でき、変更する必要はありません。LIF にアクセスできるネットワークサービスや IP アドレスを変更する場合は、カスタムファイアウォールポリシーを作成して LIF に割り当てることができます。

### このタスクについて

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

  これらの値は、システム定義のファイアウォールポリシー用に予約されています。

- クラスタ LIF のファイアウォールポリシーを設定したり変更したりすることはできません。

  クラスタ LIF のファイアウォールポリシーは、どのサービスタイプでも 0.0.0.0/0 に設定されます。

- ポリシーからサービスを削除する必要がある場合は、既存のファイアウォールポリシーを削除してから、新しいポリシーを作成する必要があります。
- クラスタで IPv6 が有効になっている場合は、 IPv6 アドレスを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には、許可されるアドレスのリストにIPv6ワイルドカード::/0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ときは、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、必ず、クラスタ間 LIF と会社所有のファイアウォールの両方で HTTPS サービスを許可してください。

  デフォルトでは、が表示されます `intercluster` ファイアウォールポリシーは、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や、クラスタ間 LIF の独自のファイアウォールポリシーを作成する場合は、許可されるアドレスのリストに各クラスタ間 LIF の IP アドレスを追加して、 HTTPS サービスを有効にする必要があります。

- ONTAP 9.6 以降では、 HTTPS および SSH のファイアウォールサービスはサポートされていません。

  ONTAP 9.6では、 `management-https` および `management-ssh` LIFサービスは、HTTPSとSSHの管理アクセスに使用できます。

### 手順

1. 特定の SVM の LIF で使用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
   ```

   ファイアウォールポリシーに追加するネットワークサービスごとに上記のコマンドを繰り返して、各サービスで許可される IP アドレスを指定できます。

2. 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` コマンドを実行します
3. ファイアウォールポリシーを LIF に適用します。

   `network interface modify -vserver` *`vserver_name`* `-lif` *`lif_name`* `-firewall-policy` *`policy_name`*

4. 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` コマンドを実行します

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およびポリシーを管理するためのコマンド

を使用できます `system services firewall` ファイアウォールサービスを管理するためのコマンド `system services firewall policy` ファイアウォールポリシーを管理するコマンド、および `network interface modify` LIFのファイアウォール設定を管理するコマンド。

| 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します | `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します | `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してください | `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た IP アドレスとネットマスクを変更する | `system services firewall policy modify` |
| ファイアウォールポリシーに関する情報を表示する | `system services firewall policy show` |
| 既存のファイアウォールポリシーとまったく同一の新しいポリシーを作成します | `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、のマニュアルページを参照してください `system services firewall`、 `system services firewall policy`および `network interface modify` のコマンド "ONTAP 9コマンドリファレンス"。

# 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 Quality of Service （ QoS ；サービス品質）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発信（出力） IP パケットトラフィックで Differentiated Services Code Point （ DSCP ）マーキングをイネーブルにできます。DSCP マーキングは、ネットワークトラフィックを分類および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。

特定のプロトコルに対して DSCP マーキングを有効にするときに 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。

作業を開始する前に

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

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

- 。 `-ipspace` パラメータは、QoSマーキングエントリを変更するIPspaceを指定します。
- 。 `-protocol` パラメータは、QoSマーキングエントリを変更するプロトコルを指定します。。 `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。
- 。 `-dscp` パラメータには、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。
- 。 `-is-enabled` パラメータを使用して、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します `-ipspace` パラメータ

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

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

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 の管理には、 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、特定のイベントが発生するたびにトラップ通知も生成します。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

MIB （管理情報ベース）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、 Object Identifier （ OID ；オブジェクト識別子）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 ファイルがあります。

- ネットアップのカスタムMIB (`netapp.mib`)

ONTAP は、 IPv6 （ RFC 2465 ）、 TCP （ RFC 4022 ）、 UDP （ RFC 4113 ）、および ICMP （ RFC 2466 ）の MIB をサポートします。これらの MIB では IPv4 と IPv6 の両方のデータが表示されます。

ONTAP では、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` ファイル。

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 機能の評価用に提供されています。

### SNMP トラップ

SNMP トラップは、 SNMP エージェントから SNMP マネージャに非同期通知として送信されたシステム監視情報をキャプチャします。

SNMP トラップには、標準、ビルトイン、およびユーザ定義の 3 種類があります。ユーザ定義トラップは、 ONTAP ではサポートされていません。

トラップを使用して、 MIB に定義された運用上のしきい値または障害を定期的にチェックすることができます。しきい値に到達するか、障害が検出されると、 SNMP エージェントは、イベントを警告するメッセージ（トラップ）をトラップホストに送信します。

ONTAP は、 SNMPv1 トラップ、および ONTAP 9.1 以降の SNMPv3 トラップをサポートしています。ONTAP は、 SNMPv2c トラップおよび INFORM をサポートしていません。

#### 標準 SNMP トラップ

これらのトラップは RFC 1215 で定義されています。ONTAP でサポートされている SNMP トラップは、 coldStart 、 warmStart 、 linkDown 、 linkUp 、および authenticationFailure の 5 つです。

authenticationFailure トラップは、デフォルトで無効になっています。を使用する必要があります `system snmp authtrap` トラップをイネーブルにするコマンド。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 9 のコマンド"

組み込みの **SNMP** トラップ

ビルトイントラップは ONTAP に事前定義されたトラップで、イベントの発生時にトラップホストリストのネットワーク管理ステーションに自動的に送信されます。diskFailedShutdown 、 cpuTooBusy 、 volumeNearlyFull など、これら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で識別されます。

## SNMP コミュニティを作成して LIF に割り当てます

### 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、などのコマンドを実行できます `snmpwalk` および `snmpget` （データLIF）。

このタスクについて

- 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 でサポートされるのは、読み取り専用のコミュニティです。
- デフォルトでは、データLIFに割り当てられている「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います `deny`。

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

  > ONTAP 9.10.1以降では、ファイアウォールポリシーは廃止され、完全にLIFのサービスポリシー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します"。

- 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でのクエリにはネットアップのルートOID（1.3.6.1.4.1.789）を含める必要があります。次に例を示します。 `snmpwalk -v 2c -c snmpNFS 10.238.19.14 1.3.6.1.4.1.789`。

手順

1. を使用してSNMPコミュニティを作成します `system snmp community add` コマンドを実行します次のコマンドは、管理 SVM cluster-1 に SNMP コミュニティを作成する方法を示しています。

   ```
   system snmp community add -type ro -community-name comty1 -vserver
   cluster-1
   ```

   次のコマンドは、データ SVM vs1 に SNMP コミュニティを作成する方法を示しています。

```
system snmp community add -type ro -community-name comty2 -vserver vs1
```

2. system snmp community show コマンドを使用して、コミュニティが作成されたことを確認します。

   次のコマンドは、 SNMPv1 および SNMPv2c 用に作成された 2 つのコミュニティを表示します。

```
system snmp community show
cluster-1
rocomty1
vs1
rocomty2
```

3. 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 コマンドを実行します

   次のコマンドは、デフォルトの「 data 」ファイアウォールポリシーでは SNMP サービスが許可されていないことを示しています（ SNMP サービスは「 mgmt 」ファイアウォールポリシー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. を使用したアクセスを許可する新しいファイアウォールポリシーを作成します `snmp` を使用してサービス

を提供します `system services firewall policy create` コマンドを実行します

次のコマンドは、「data1」という名前の新しいデータファイアウォールポリシーを作成して、を許可します `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
```

## クラスタに **SNMPv3** ユーザを設定します

SNMPv3 は、 SNMPv1 や SNMPv2c に比べて安全なプロトコルです。SNMPv3 を使用するには、 SNMP マネージャから SNMP ユーティリティを実行するための SNMPv3 ユーザを設定する必要があります。

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 ユーティリティのコマンドを実行できます。

**SNMPv3** セキュリティパラメータ

SNMPv3 には認証機能が備わっており、この機能を選択すると、コマンドの呼び出し時に、ユーザ名、認証プロトコル、認証キー、および必要なセキュリティレベルの入力が必要になります。

次の表に、 SNMPv3 セキュリティパラメータを示します。

| パラメータ | コマンドラインオプション | 説明 |
| --- | --- | --- |
| エンジン ID | -e engineID | SNMP エージェントのエンジン ID 。デフォルト値はローカルのエンジン ID （推奨）です。 |
| 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

次に、さまざまなセキュリティレベルで作成されたSNMPv3ユーザが、などのSNMPクライアント側コマンドを使用する例を示します `snmpwalk`をクリックして、クラスタオブジェクトを照会します。

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。

を使用する必要があります `snmpwalk` 認証プロトコルがSHAの場合は5.3.1以降。

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 -username 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** テストを実行します

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 -username snmpv3user1 -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** テストを実行します

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 -username snmpv3user2 -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** テストを実行します

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します

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。

作業を開始する前に

- クラスタで SNMP トラップと SNMP トラップが有効になっている必要があります。

  SNMP トラップと SNMP トラップはデフォルトで有効になっています。

- クラスタでトラップホスト名を解決するように DNS が設定されている必要があります。
- IPv6 アドレスを使用して SNMP トラップホストを設定するには、クラスタで IPv6 を有効にする必要があります。
- 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。

このタスクについて

クラスタをポーリングするには、次のようなサードパーティのコマンドを使用する必要があります。 `snmpwalk`。

手順

1. SNMP コマンドを送信して、別のクラスタからクラスタをポーリングします。

   SNMPv1を実行しているシステムの場合は、CLIコマンドを使用します。 `snmpwalk -v version -c community_stringip_address_or_host_name system` 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の場合は、CLIコマンドを使用します。 `snmpwalk -v version -c community_stringip_address_or_host_name system` 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の場合は、CLIコマンドを使用します。 `snmpwalk -v 3 -a MD5 or SHA -l authnopriv -u username -A passwordip_address_or_host_name system` 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 を管理するためのコマンド

を使用できます `system snmp` SNMP、トラップ、およびトラップホストを管理するコマンド。を使用できます `security` SVMごとにSNMPユーザを管理するコマンド。を使用できます `event` SNMPトラップに関連するイベントを管理するコマンド。

**SNMP** を設定するためのコマンド

| 状況 | 使用するコマンド |
| --- | --- |
| クラスタで SNMP を有効にします | `options -option-name snmp.enable -option-value on`<br><br>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 を無効にします | `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 ユーザを設定する | `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します | `security login modify` |

連絡先と場所の情報を提供するコマンド

| 状況 | 使用するコマンド |
|---|---|
| クラスタの連絡先の詳細を表示または変更する | `system snmp contact` |
| クラスタの場所の詳細を表示または変更する | `system snmp location` |

**SNMP** コミュニティを管理するコマンド

| 状況 | 使用するコマンド |
|---|---|
| 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でのクエリにはネットアップのルートOID（1.3.6.1.4.1.789）を含める必要があります。次に例を示します。 `snmpwalk -v 2c -c snmpNFS 10.238.19.14 1.3.6.1.4.1.789`。

**SNMP** オプションの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、トラップホストを送信するようにクラスタが設定されているかどうか、トラップホストのリスト、コミュニティとアクセス制御の種類のリストなど、すべての SNMP オプションの現在の値を表示します | `system snmp show` |

**SNMP** のトラップおよびトラップホストを管理するコマンド

| 状況 | 使用するコマンド |
|---|---|
| クラスタからの SNMP トラップの送信を有効にします | `system snmp init -init 1` |
| クラスタからの SNMP トラップの送信を無効にします | `system snmp init -init 0` |

| | |
|---|---|
| クラスタの特定のイベントに関する SNMP 通知を受信するトラップホストを追加します | `system snmp traphost add` |
| トラップホストを削除します | `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を管理するコマンド

| 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`<br><br>を使用します `-snmp-support true` SNMP関連のイベントのみを表示するためのパラメータ。<br><br>を使用します `instance -messagename <message>` パラメータを使用して、イベントが発生した理由と対処方法の詳細な概要 を表示します。<br><br>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` |

詳細については、を参照してください `system snmp`、 `security`および `event` コマンド、を参照 "ONTAP 9コマンドリファレンス"。

# 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。ルーティングテーブルがどのように機能するかを理解し、ネットワークの問題が発生する前に防止することが重要です。

ルーティングルールは次のとおりです。

- ONTAP は、使用可能な最も限定的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、 ONTAP は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）でトラフィックをルーティングします。

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、これは特に問題です。

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、より限定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取り扱うかを制御できます。

SVM に関連するルートエントリを作成すると、そのルートが、ゲートウェイと同じサブネットにあり、指定した SVM に所有されているすべての LIF で使用されます。

ステップ

を使用します `network route create` ルートを作成するコマンド。

```
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を有効にします

複数のルートが同じメトリックを宛先に持つ場合、送信トラフィックには 1 つのルートのみが選択されます。これにより、他のルートが発信トラフィックの送信に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ります。

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

## 静的ルートを削除します

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

を使用します `network route delete` 静的ルートを削除するコマンド。

このコマンドの詳細については、を参照してください 。

次の例では、 SVM vs0 に関連付けられている、ゲートウェイ 10.63.0.1 とデスティネーション IP アドレス 0.0.0.0/0 の静的ルートを削除しています。

```
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. を使用します `network route show` コマンドを使用して、1つ以上のSVM内のルートを表示します。次の例は、 vs0 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. を使用します `network route show-lifs` コマンドを使用して、1つ以上のSVM内のルートとLIFの関連付けを表示します。

   次の例は、 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. を使用します `network route active-entry show` コマンドを使用して、1つ以上のノード、SVM、サブネット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ダイナミックルートを削除します

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、動的ルートは 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。

このタスクについて

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
```

# ネットワーク情報を表示します

## ネットワーク情報の概要を表示する

CLIを使用すると、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。ONTAP 9.8以降では、使用している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、ネットワークの再設定やクラスタのトラブルシューティングを行うときに役立ちます。

クラスタ管理者の場合は、使用可能な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 に関連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の情報を表示します

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。

このタスクについて

次の情報が表示されます。

- ノード名
- ポート名
- IPspace 名
- ブロードキャストドメイン名
- リンクステータス（ up または down ）
- MTU を設定します
- ポート速度の設定と動作ステータス（毎秒 1 ギガビットまたは 10 ギガビット）
- 自動ネゴシエーション設定（ true または false ）
- 二重モードと動作ステータス（ half または full ）
- ポートのインターフェイスグループ（該当する場合）
- ポートの VLAN タグ情報（該当する場合）
- ポートのヘルスステータス（「正常」または「デグレード」）
- ポートがデグレードとマークされた理由

該当するデータがないフィールドにはという値が表示されます。たとえば、アクティブでないポートの二重モードの動作ステータスや速度の情報はありません -。

ステップ

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` コマンドを実行します

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

```
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。

このタスクについて

を指定すると、各VLANの詳細情報を表示できます `-instance` パラメータでフィールド名を指定すると、特定の情報を表示できます `-fields` パラメータ

ステップ

を使用して、VLANに関する情報を表示します `network port vlan show` コマンドを実行します次のコマンドは、クラスタ内のすべての VLAN に関する情報を表示します。

```
network port vlan show
                  Network Network
Node   VLAN Name Port    VLAN ID  MAC Address
------ --------- ------- -------- -----------------
cluster-1-01
       a0a-10    a0a     10       02:a0:98:06:10:b2
       a0a-20    a0a     20       02:a0:98:06:10:b2
       a0a-30    a0a     30       02:a0:98:06:10:b2
       a0a-40    a0a     40       02:a0:98:06:10:b2
       a0a-50    a0a     50       02:a0:98:06:10:b2
cluster-1-02
       a0a-10    a0a     10       02:a0:98:06:10:ca
       a0a-20    a0a     20       02:a0:98:06:10:ca
       a0a-30    a0a     30       02:a0:98:06:10:ca
       a0a-40    a0a     40       02:a0:98:06:10:ca
       a0a-50    a0a     50       02:a0:98:06:10:ca
```

## 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。

このタスクについて

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

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` コマンドを実行します

各ノードの詳細情報を表示するには、を指定します `-instance` パラメータでフィールド名を指定すると、特定の情報を表示できます `-fields` パラメータ

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 情報を表示します

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。

このタスクについて

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` |

各ルートの詳細情報を表示するには、を指定します `-instance` パラメータ次のコマンドは、 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 hosts 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
```

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

## DNS ドメイン設定を表示します

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

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

次のコマンドは、クラスタ内のすべての SVM の DNS 設定を表示します。

```
vserver services name-service dns show
                                                  Name
Vserver         State     Domains                 Servers
--------------- --------- ----------------------- -------------
cluster-1        enabled   xyz.company.com         192.56.0.129,
                                                  192.56.0.130
vs1             enabled   xyz.company.com         192.56.0.129,
                                                  192.56.0.130
vs2             enabled   xyz.company.com         192.56.0.129,
                                                  192.56.0.130
vs3             enabled   xyz.company.com         192.56.0.129,
                                                  192.56.0.130
```

次のコマンドは、 SVM vs1 の DNS 設定の詳細を表示します。

```
vserver services name-service dns show -vserver vs1
               Vserver: vs1
               Domains: xyz.company.com
          Name Servers: 192.56.0.129, 192.56.0.130
    Enable/Disable DNS: enabled
        Timeout (secs): 2
      Maximum Attempts: 1
```

## フェイルオーバーグループに関する情報を表示します

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. 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` コマンドを実行します

   次のコマンドは、 2 ノードクラスタのすべてのフェイルオーバーグループ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. 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` コマンドを実行します

   次のコマンドは、 SVM vs4 の data12 というフェイルオーバーグループに関する詳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. 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` コマンドを実行します

   次のコマンドは、各 LIF で使用されているフェイルオーバーポリシーとフェイルオーバーグループを表示します。

```
network interface show -vserver * -lif * -fields failover-
group,failover-policy
vserver   lif                  failover-policy        failover-group
--------  -------------------  ---------------------  --------------
Cluster   cluster1-01_clus_1  local-only             Cluster
Cluster   cluster1-01_clus_2  local-only             Cluster
Cluster   cluster1-02_clus_1  local-only             Cluster
Cluster   cluster1-02_clus_2  local-only             Cluster
cluster1  cluster_mgmt        broadcast-domain-wide  Default
cluster1  cluster1-01_mgmt1   local-only             Default
cluster1  cluster1-02_mgmt1   local-only             Default
vs1       data1               disabled               Default
vs3       data2               system-defined         group2
```

## 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。

このタスクについて

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

を使用して、LIFのフェイルオーバーターゲットを表示します `failover` のオプション `network interface show` コマンドを実行します

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。。 `Failover Targets` 行には、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）リストが表示されます。

```
network interface show -failover
         Logical       Home                  Failover        Failover
Vserver  Interface     Node:Port             Policy          Group
-------- ------------ --------------------- --------------- ---------
Cluster
         node1_clus1   node1:e0a             local-only      Cluster
                       Failover Targets: node1:e0a,
                                         node1:e0b
         node1_clus2   node1:e0b             local-only      Cluster
                       Failover Targets: node1:e0b,
                                         node1:e0a
         node2_clus1   node2:e0a             local-only      Cluster
                       Failover Targets: node2:e0a,
                                         node2:e0b
         node2_clus2   node2:e0b             local-only      Cluster
                       Failover Targets: node2:e0b,
                                         node2:e0a
cluster1
         cluster_mgmt  node1:e0c             broadcast-domain-wide
                                                             Default
                       Failover Targets: node1:e0c,
                                         node1:e0d,
                                         node2:e0c,
                                         node2:e0d
         node1_mgmt1   node1:e0c             local-only      Default
                       Failover Targets: node1:e0c,
                                         node1:e0d
         node2_mgmt1   node2:e0c             local-only      Default
                       Failover Targets: node2:e0c,
                                         node2:e0d
vs1
         data1         node1:e0e             system-defined  bcast1
                       Failover Targets: node1:e0e,
                                         node1:e0f,
                                         node2:e0e,
                                         node2:e0f
```

## ロードバランシングゾーンの **LIF** を表示します

ロードバランシングゾーンに属するすべての LIF を表示して、そのゾーンが正しく設定されているかどうかを確認できます。特定の LIF 、またはすべての LIF のロードバランシングゾーンを表示することもできます。

ステップ

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

| 表示する内容 | 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`<br><br>`zone_name` ロードバランシングゾーンの名前を指定します。 |
| 特定の LIF のロードバランシングゾーン | `network interface show -lif lif_name -fields dns-zone` |
| すべての LIF のロードバランシングゾーン | `network interface show -fields dns-zone` |

**LIF** のロードバランシングゾーンを表示する例

次のコマンドは、 SVM vs0 の storage.company.com というロードバランシングゾーンに属するすべての LIF の詳細を表示します。

```
net int show -vserver vs0 -dns-zone storage.company.com

          Logical    Status     Network            Current   Current Is
Vserver   Interface  Admin/Oper Address/Mask       Node      Port    Home
--------- ---------- ---------- ------------------ --------- ------- ----
vs0
          lif3         up/up    10.98.226.225/20   ndeux-11  e0c     true
          lif4         up/up    10.98.224.23/20    ndeux-21  e0c     true
          lif5         up/up    10.98.239.65/20    ndeux-11  e0c     true
          lif6         up/up    10.98.239.66/20    ndeux-11  e0c     true
          lif7         up/up    10.98.239.63/20    ndeux-21  e0c     true
          lif8         up/up    10.98.239.64/20    ndeux-21  e0c     true
```

次のコマンドは、 data3 という LIF の DNS ゾーンの詳細を表示します。

```
network interface show -lif data3 -fields dns-zone
Vserver  lif    dns-zone
-------  -----  --------
vs0      data3  storage.company.com
```

次のコマンドは、クラスタ内のすべての LIF 、および対応する DNS ゾーンを表示します。

```
network interface show -fields dns-zone
Vserver   lif          dns-zone
-------   ------------ --------
cluster   cluster_mgmt none
ndeux-21  clus1        none
ndeux-21  clus2        none
ndeux-21  mgmt1        none
vs0       data1        storage.company.com
vs0       data2        storage.company.com
```

## クラスタの接続を表示します

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を表示したりできます。クラスタ内のリスンしているすべての接続を表示することもできます。

### クライアント別のアクティブな接続を表示する（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で使用されているノードを確認したり、ノードあたりのクライアント数に不均衡がないかどうかを確認したりできます。

#### このタスクについて

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特定する。
- 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。
- 接続数が予期せず多くなっているクライアントを特定する。
- 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

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` コマンドを実行します

このコマンドの詳細については、を参照してください "ONTAP 9コマンドリファレンス"。

```
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。

このタスクについて

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くと、 UDP クライアントが最初に破棄されます。

- 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

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` コマンドを実行します

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する（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際に役立ちます。これにより、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。

このタスクについて

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、および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。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` コマンドを実行します

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 9 のコマンド"

```
network connections active show-services
Node        Vserver Name    Service    Count
---------  --------------  ---------  ------
node0
            vs0             mount           3
            vs0             nfs            14
            vs0             nlm_v4          4
            vs0             cifs_srv        3
            vs0             port_map       18
            vs0             rclopcp        27
            Cluster         ctlopcp        60
node1
            vs0             cifs_srv        3
            vs0             rclopcp        16
            Cluster         ctlopcp        60
node2
            vs1             rclopcp        13
            Cluster         ctlopcp        60
node3
            vs1             cifs_srv        1
            vs1             rclopcp        17
            Cluster         ctlopcp        60
```

ノードおよび **SVM** の **LIF** 別のアクティブな接続の情報を表示します

ノードおよび Storage Virtual Machine （ SVM ）の LIF 別のアクティブな接続数を表示して、クラスタ内の LIF 間で接続数の不均衡がないかどうかを確認できます。

このタスクについて

LIF 別のアクティブな接続数の情報は、次のような場合に役立ちます。

- 各 LIF の接続数を比較することで、過負荷の LIF を探す。
- すべてのデータ LIF に対して DNS ロードバランシングが機能していることを確認する。
- さまざまな SVM への接続数を比較して、最もよく使用されている SVM を特定する。

ステップ

を使用して、SVMおよび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` コマンドを実行します

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 9 のコマンド"

```
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、それぞれの接続で使用されている LIF 、ポート、リモートホスト、サービス、 Storage Virtual Machine （ SVM ）、およびプロトコルを確認できます。

このタスクについて

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が正しいノードで正しいプロトコルと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ことができます。

ステップ

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

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 9 のコマンド"

次のコマンドは、 node1 というノードのアクティブな接続の情報を表示します。

```
network connections active show -node node1
Vserver  Interface           Remote
Name     Name:Local Port     Host:Port           Protocol/Service
-------  ------------------  ------------------  ---------------
Node: node1
Cluster  node1_clus_1:50297  192.0.2.253:7700    TCP/ctlopcp
Cluster  node1_clus_1:13387  192.0.2.253:7700    TCP/ctlopcp
Cluster  node1_clus_1:8340   192.0.2.252:7700    TCP/ctlopcp
Cluster  node1_clus_1:42766  192.0.2.252:7700    TCP/ctlopcp
Cluster  node1_clus_1:36119  192.0.2.250:7700    TCP/ctlopcp
vs1      data1:111           host1.aa.com:10741  UDP/port-map
vs3      data2:111           host1.aa.com:10741  UDP/port-map
vs1      data1:111           host1.aa.com:12017  UDP/port-map
vs3      data2:111           host1.aa.com:12017  UDP/port-map
```

次のコマンドは、 SVM vs1 のアクティブな接続の情報を表示します。

```
network connections active show -vserver vs1
Vserver  Interface           Remote
Name     Name:Local Port     Host:Port           Protocol/Service
-------  ------------------  ------------------  ---------------
Node: node1
vs1      data1:111           host1.aa.com:10741  UDP/port-map
vs1      data1:111           host1.aa.com:12017  UDP/port-map
```

クラスタ内のリスンしている接続を表示します

クラスタ内のリスンしている接続を表示して、特定のプロトコルとサービスの接続を受け入れている LIF とポートを確認することができます。

このタスクについて

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、それぞれのインタークラスタ 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

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` コ

マンドを実行します

```
network connections listening show
Vserver Name     Interface Name:Local Port        Protocol/Service
---------------- -------------------------------  ----------------
Node: node0
Cluster          node0_clus_1:7700                TCP/ctlopcp
vs1              data1:4049                       UDP/unknown
vs1              data1:111                        TCP/port-map
vs1              data1:111                        UDP/port-map
vs1              data1:4046                       TCP/sm
vs1              data1:4046                       UDP/sm
vs1              data1:4045                       TCP/nlm-v4
vs1              data1:4045                       UDP/nlm-v4
vs1              data1:2049                       TCP/nfs
vs1              data1:2049                       UDP/nfs
vs1              data1:635                        TCP/mount
vs1              data1:635                        UDP/mount
Cluster          node0_clus_2:7700                TCP/ctlopcp
```

## ネットワークの問題を診断するためのコマンドです

ネットワークの問題を診断するには、などのコマンドを使用します `ping`, `traceroute`, `ndp`, および `tcpdump`。などのコマンドを使用することもできます `ping6` および `traceroute6` IPv6の問題を診断する。

| 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します | `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します | `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` |
| 近接探索プロトコル（ 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`<br><br>注：このコマンドはノードシェルから使用できます。 |
| リモートデバイスタイプやデバイスプラットフォームなど、クラスタ内の各ノードとポートで検出されている隣接デバイスに関する情報を表示します | `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`<br><br>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します | `network tcpdump start -node node-name -port port_name`<br><br>注：このコマンドはノードシェルから使用できます。 |
| クラスタ間またはクラスタ内のノード間のレイテンシとスループットを測定します | `network test -path -source-node source_nodename local -destination -cluster destination_clustername -destination-node destination_nodename -session-type Default, AsyncMirrorLocal, AsyncMirrorRemote, SyncMirrorRemote, or RemoteDataTransfer`<br><br>詳細については、を参照してください "パフォーマンス管理"。 |

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 9コマンドリファレンス"。

## 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、物理または仮想システムのペアとそのネットワークインターフェ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ている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 アドレスへ送信され、近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 つのデバイスがネイバーになるには、各デバイスでプロトコルが有効になっていて、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。近接機器には、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が含まれます。ONTAP では、 2 つの近接探索プロトコルがサポートされます。これらは個別に使用することも一緒に使用することもでき

- シスコ検出プロトコル（ CDP ） *

CDP は、 Cisco Systems が開発したリンクレイヤプロトコルです。ONTAP では、クラスタポートに対してこのプロトコルがデフォルトで有効になりますが、データポートに対しては明示的に有効にする必要があります。

- リンク層検出プロトコル（ LLDP ） *

LLDP は、ベンダーに依存しないプロトコルであり、 IEEE 802.1AB 規格のドキュメントで指定されています。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 を使用してネットワーク接続を検出するには、導入時の考慮事項を確認し、データポートで CDP を有効にし、ネイバーデバイスを表示し、必要に応じて CDP 設定値を調整します。クラスタポートでは、 CDP はデフォルトで有効になります。

隣接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、クラスタと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。 |
| 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。したがって、 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、次の点を確認してください。

- 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 通知は一定間隔で送信され、送信間隔は設定可能です。
- LIF の IP アドレスが変更されると、ノードは更新された情報を次の CDP 通知で送信します。
- ONTAP 9.10.1以前：
  - CDP はクラスタポートで常に有効になります。
  - 非クラスタポートでは、 CDP はデフォルトで無効になります。
- ONTAP 9.11.1以降：
  - CDPは、クラスタポートとストレージポートで常に有効になります。
  - 非クラスタポートと非ストレージポートでは、CDPはデフォルトで無効になっています。

> 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パケットが1500バイト以下に制限されているため、ポート上
多数のLIFで構成されている場合、隣接するスイッチではこれらのIPアドレスの一部のみが報告されることがあります。

#### CDP を有効または無効にします

CDP 対応の隣接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以前のデフォルトでは、ノードのすべてのクラスタポートでCDPが有効になり、ノードのすべての非クラスタポートで無効になります。

ONTAP 9.11.1以降では、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CDPが有効になり、ノードの非クラスタポートと非ストレージポートで無効になっています。

このタスクについて

。 `cdpd.enable` オプションは、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、非クラスタポートと非ストレージポートでCDPが有効になります。
- ONTAP 9.10.1以前のバージョンでは、offを指定すると非クラスタポートでCDPが無効になります。クラスタポートのCDPを無効にすることはできません。
- ONTAP 9.11.1以降では、offを指定すると、非クラスタポートと非ストレージポートでCDPが無効になります。クラスタポートのCDPを無効にすることはできません。

CDP 対応デバイスに接続されているポートで CDP を無効にすると、ネットワークトラフィックが最適化されない可能性があります。

手順

1. クラスタ内の 1 つまたはすべてのノードの、現在の CDP 設定を表示します。

| 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 ネイバー情報を表示します

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、そのポートの隣接デバイスの情報を表示することができます。を使用できます `network device-discovery show -protocol cdp` ネイバー情報を表示するコマンド。

このタスクについて

ONTAP 9.10.1以前では、クラスタポートでCDPが常に有効になっているため、これらのポートのCDPネイバー情報は常に表示されます。非クラスタポートの隣接情報を表示するには、これらのポートで CDP を有効にする必要があります。

ONTAP 9.11.1以降では、クラスタポートとストレージポートでCDPが常に有効になっているため、これらのポートのCDP隣接情報は常に表示されます。非クラスタポートおよび非ストレージポートでCDPを有効にして、これらのポートのネイバー情報を表示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ネイバーを表示します。

```
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
```

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を設定します

保持時間とは、 CDP 通知が CDP 対応の隣接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。

- の値 `cdpd.holdtime` オプションの値は、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は 180 ですが、 10~255 秒の値を入力できます。
- 保持時間が切れる前に IP アドレスが削除された場合、 CDP 情報は保持時間が切れるまでキャッシュされます。

手順

1. クラスタ内の 1 つまたはすべてのノードの CDP メッセージの現在の保持時間を表示します。

| 保持時間を表示する対象 | 入力するコマンド |
| --- | --- |
| 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で、すべてのポートの CDP 通知の保持時間を設定します。

| 保持時間を設定する対象 | 入力するコマンド |
| --- | --- |
| 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します

CDP 通知は、一定の間隔で CDP 隣接機器に送信されます。ネットワークトラフィックの量やネットワークトポロジの変化に応じて、 CDP 通知の送信間隔を調整することができます。

- の値 `cdpd.interval` オプションの値は、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。
- デフォルトの送信間隔は 60 秒ですが、 5~900 秒の値を入力できます。

手順

1. クラスタ内の 1 つまたはすべてのノードについて、 CDP 通知の現在の送信間隔を表示します。

| 送信間隔を表示する対象 | 入力するコマンド |
| --- | --- |
| 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で、すべてのポートの CDP 通知の送信間隔を設定します。

| 送信間隔を設定する対象 | 入力するコマンド |
| --- | --- |
| 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 統計情報を表示または消去します

ネットワーク接続に潜在的な問題を検出するために、各ノードのクラスタポートと非クラスタポートの CDP 統計を表示することができます。CDP 統計は、値が前回消去されたときからの累積値です。

このタスクについて

ONTAP 9.10.1以前では、ポートでCDPが常にイネーブルになっているため、これらのポート上のトラフィックに関するCDP統計情報は常に表示されます。これらのポートの統計情報を表示するには、ポート上で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でCDPが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CDP統計情報が常に表示されます。非クラスタポートまたは非ストレージポートでCDP統計情報を表示するには、これらのポートでCDPを有効にする必要があります。

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 統計情報を表示します | `run -node node_name cdpd show-stats` |
| CDP 統計情報を消去します | `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 統計情報を表示します。出力には、前回統計情報が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。

```
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
```

統計を消去すると、次回 CDP 通知を送信または受信したあとに統計が累積され始めます。

#### CDPをサポートし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。 サポート技術情報の記事を参照してください "ONTAPデバイス検出でスイッチではなくノードが表示される" を参照してください。

この問題を解決するには、次の2つのオプションがあります。

- 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）。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" を参照してください。
- 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 を使用してネットワーク接続を検出するには、導入時の考慮事項を確認し、すべてのポートで LLDP を有効にし、隣接デバイスを表示し、必要に応じて LLDP の設定値を調整します。

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（ 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で異なる場合があります。

  CNAポートとCNA以外のポートについてスイッチで表示されるシャーシIDとポートIDのデータが異なる場合があります。

例：

- 非CNAポートの場合：
  - シャーシIDは、ノードのいずれかのポートの固定MACアドレスです
  - Port IDは、ノード上の対応する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、ノード上の対応するポートのMACアドレスです。

ただし、これらのポートタイプについては、クラスタで表示されるデータに整合性があることを示しています。

LLDP の仕様では、 SNMP MIB による収集情報へのアクセスを定義します。ただし、現時点では、 ONTAP は LLDP MIB をサポートしていません。

**LLDP**の有効化または無効化

LLDP対応の隣接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、 LLDP がノードのすべてのポートでデフォルトで有効になっています。

このタスクについて

ONTAP 9.10.1以前の場合は `lldp.enable` オプションは、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。

ONTAP 9.11.1以降の場合は `lldp.enable` オプションは、ノードの非クラスタポートと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：options `lldp.enable`

2. クラスタ内の 1 つまたはすべてのノードで、すべてのポートの LLDP を有効または無効に設定します。

| LLDPを有効または無効にする対象 | 入力するコマンド |
| --- | --- |
| 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ネイバー情報の表示

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、そのポートの隣接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、 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隣接デバイスの情報を表示します。この出力には、指定したノードの各ポートに接続されている LLDP 対応デバイスが一覧表示されます。状況に応じて `-protocol` オプションを省略すると、CDP対応デバイスも表示されます。

```
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します

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。

このタスクについて

IEEE が推奨するデフォルトの送信間隔は 30 秒ですが、 5~300 秒の値を入力できます。

手順

1. クラスタ内の1つまたはすべてのノードについて、LLDP通知の現在の間隔を表示します。
   - 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で、すべてのポートの 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 TTL 値を調整します

Time-To-Live （ TTL ）とは、 LLDP 通知が LLDP 対応の隣接デバイスのキャッシュに格納される時間です。TTL は各 LLDP パケットで通知され、ノードが LLDP パケットを受信するたびに更新されます。発信 LLDP フレームで TTL を変更できます。

このタスクについて

- TTLは計算された値であり、送信間隔の積です (`lldp.xmit.interval`）とホールド乗数 (`lldp.xmit.hold`）プラス1。
- デフォルトの保持の乗数値は 4 ですが、 1~100 の値を入力できます。
- IEEE が推奨するデフォルトの TTL は 121 秒ですが、送信間隔と保持の乗数の値を調整することにより、発信フレームの値を 6~30001 秒に指定できます。
- TTL が期限切れになる前に IP アドレスが削除された場合、 LLDP 情報は TTL が期限切れになるまでキャッシュされます。

手順

1. クラスタ内の 1 つまたはすべてのノードの現在の保持の乗数値を表示します。
   - 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で、すべてのポートの保持の乗数値を調整します。
   - 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統計情報を表示または消去します

ネットワーク接続に潜在的な問題を検出するために、各ノードのクラスタポートと非クラスタポートのLLDP統計を表示できます。LLDP統計は、前回消去されたときからの累積値です。

このタスクについて

ONTAP 9.10.1以前では、クラスタポートでLLDPが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。非クラスタポートでLLDP統計が表示されるようにするに

は、LLDP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でLLDPが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LLDP統計が常に表示されます。これらのポートに対して統計情報を表示するには、クラスタ以外のポートおよびストレージ以外のポートで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` |

統計の例を表示および消去します

次のコマンドは、LLDP統計をクリアする前に表示します。出力には、前回統計情報が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
```

統計を消去すると、LLDP通知が次回送信または受信されたあとに統計が累積され始めます。