ネットワークポートの設定
ONTAP 9

NetApp
December 20, 2024

目次

ネットワークポートの設定

物理ポートを組み合わせてインターフェイスグループを作成

インターフェイスグループはLink Aggregation Group（LAG；リンクアグリゲーショングループ）とも呼ばれ、同じノード上の複数の物理ポートを1つの論理ポートにまとめることで作成されます。論理ポートを使用すると、耐障害性と可用性が向上し、負荷も共有できます。

インターフェイス グループの種類

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

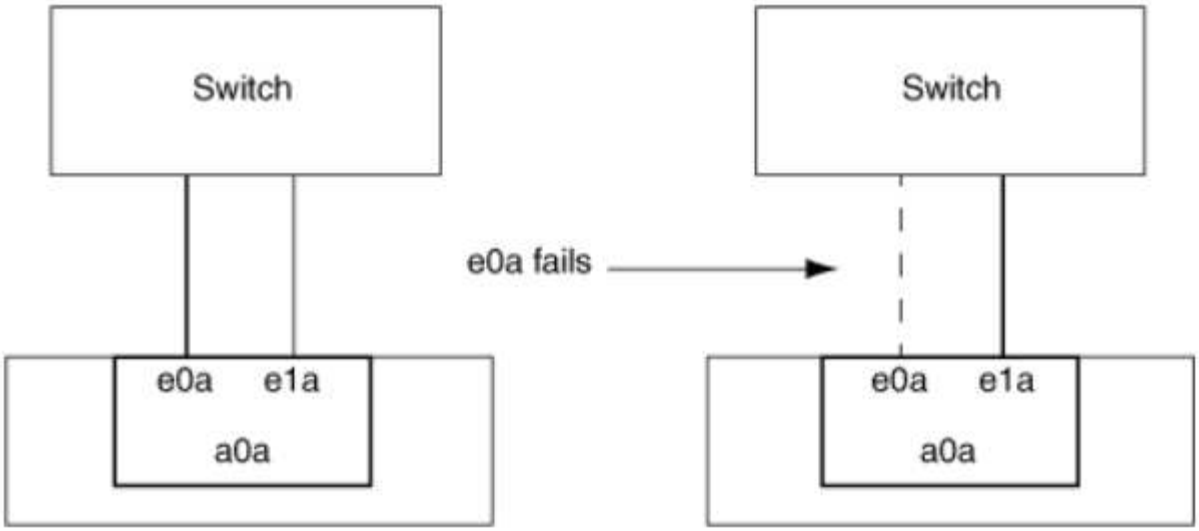
シングルモード インターフェイス グループの特性

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

シングルモード インターフェイス グループの特性は、次のとおりです。

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

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



シングルモード機能を実現するためには、フェイルオーバーグループを使用することを推奨します。フェイルオーバーグループを使用すると、2番目のポートを引き続き他のLIFに使用でき、未使用のままにする必要はありません。さらに、フェイルオーバーグループは3つ以上のポートにまたがることも、複数のノードのポートにまたがることもできます。

スタティックマルチモードインターフェイスグループの特性

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

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

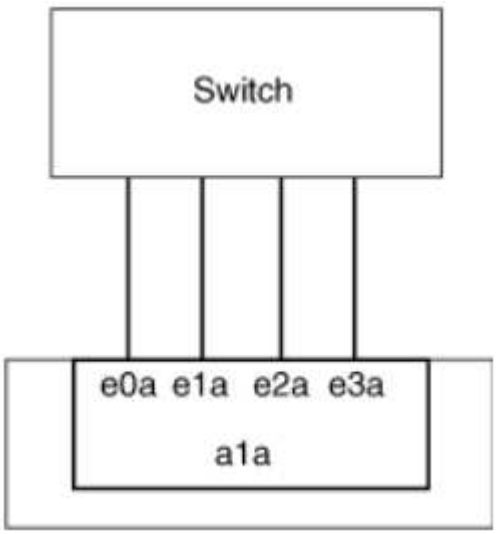
スタティックマルチモードインターフェイスグループの特性は次のとおりです。

- インターフェイスグループ内のすべてのインターフェイスがアクティブで、1つのMACアドレスを共有します。
  - 複数の接続が、インターフェイスグループ内のインターフェイスに分散されます。
  - 各接続またはセッションは、インターフェイスグループ内の1つのインターフェイスを使用します。シーケンシャルロードバランシング方式を使用すると、すべてのセッションがパケット単位で使用可能なリンクに分散され、インターフェイスグループの特定のインターフェイスにバインドされません。
- スタティックマルチモードインターフェイスグループは、最大で「n-1」個のインターフェイスの障害から回復できます。nは、インターフェイスグループを構成するインターフェイスの総数です。
- ポートに障害が発生した場合、またはポートが接続されていない場合、障害が発生したリンクを通過していたトラフィックは、残りのインターフェイスの1つに自動的に再配布されます。
- スタティックマルチモードインターフェイスグループではリンクの喪失は検出できますが、クライアントへの接続の喪失や、接続とパフォーマンスに影響する可能性のあるスイッチの設定ミスは検出できません。
- スタティックマルチモードインターフェイスグループには、複数のスイッチポートでのリンクアグリゲーションをサポートするスイッチが必要です。スイッチは、インターフェイスグループのリンクの接続先ポートがすべて1つの論理ポートを構成するように設定されています。一部のスイッチでは、ジャンボフレ

ーム用に構成されたポートのリンクアグリゲーションがサポートされない場合があります詳細については、スイッチベンダーのマニュアルを参照してください。

- スタティックマルチモードインターフェイスグループのインターフェイス間でトラフィックを分散するために、いくつかのロードバランシングオプションを使用できます。

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



単一の集約リンク内のトラフィックを複数の物理スイッチに分散できるようにするテクノロジーがいくつか存在します。この機能を有効にするために使用されるテクノロジは、ネットワーク製品によって異なります。ONTAPのスタティックマルチモードインターフェイスグループは、IEEE 802.3規格に準拠しています。特定のマルチスイッチリンクアグリゲーションテクノロジがIEEE 802.3規格と相互運用または準拠していると言われている場合は、ONTAPと連携して動作する必要があります。

IEEE 802.3規格では、集約リンク内の送信デバイスが送信用の物理インターフェイスを決定すると規定されています。したがって、ONTAPは発信トラフィックの配信のみを担当し、着信フレームの着信方法を制御することはできません。集約リンク上の着信トラフィックの送信を管理または制御する場合は、直接接続されたネットワークデバイスでその送信を変更する必要があります。

ダイナミックマルチモードインターフェイスグループ

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

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

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

ONTAPは設定不可のアクティブモードでLACPを実装します。これは、アクティブモードまたはパッシブモードに設定されたスイッチと連動します。ONTAPは、IEEE 802.3 AD（802.1AX）で規定されているように、longおよびshortのLACPタイマーを実装します（3秒および90秒の設定不可の値で使用します）。

ONTAPロードバランシングアルゴリズムは、発信トラフィックの送信に使用されるメンバーポートを決定し

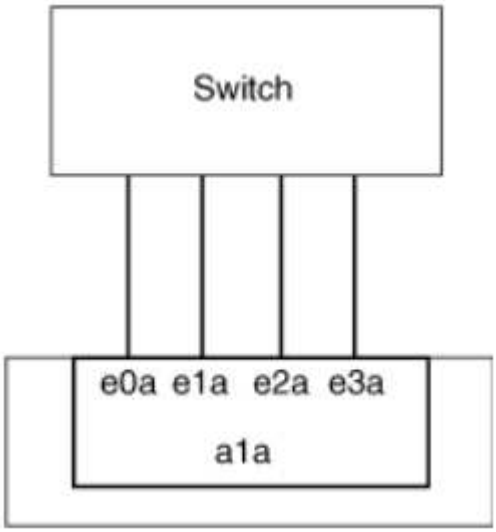
ますが、着信フレームの受信方法は制御しません。スイッチは、スイッチのポートチャネルグループに設定されたロードバランシングアルゴリズムに基づいて、送信に使用されるポートチャネルグループのメンバー（個々 の物理ポート）を決定します。したがって、スイッチの設定によって、トラフィックを受信するストレージシステムのメンバーポート（個 々 の物理ポート）が決まります。スイッチの設定の詳細については、スイッチベンダーのマニュアルを参照してください。

あるインターフェイスが連続するLACPプロトコルパケットの受信に失敗すると、そのインターフェイスは「ifgrp status」コマンドの出力で「lag_inactive」と表示されます。既存のトラフィックは、残りのアクティブインターフェイスに自動的に再ルーティングされます。

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

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

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



マルチモードインターフェイスグループでのロードバランシング

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

マルチモードインターフェイスグループのロードバランシング方式は、インターフェイスグループの作成時にのみ指定できます。

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

ポートベースのロードバランシング

ポートベースのロードバランシングが推奨されます。

ポートベースのロードバランシング方式を使用すると、マルチモードインターフェイスグループのトラフィックをトランスポートレイヤ（TCP / UDP）ポートに基づいて均等に分散できます。

ポートベースのロードバランシング方式では、トランスポートレイヤのポート番号に加えて、ソースとデスティネーションのIPアドレスに対して高速ハッシュアルゴリズムを使用します。

IPアドレスおよび**MAC**アドレスによるロードバランシング

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

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

> ルータに直接接続するシステムでインターフェイスグループを作成する場合は、MACアドレスによるロードバランシング方式を選択しないでください。このような設定では、すべての発信IPフレームの宛先MACアドレスがルータのMACアドレスになります。そのため、インターフェイスグループの1つのインターフェイスだけが使用されます。

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

シーケンシャルロードバランシング

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

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

インターフェイスグループまたは**LAG**の作成

インターフェイスグループまたはLAG（シングルモード、スタティックマルチモード、またはダイナミックマルチモード（LACP））を作成すると、集約されたネットワークポートの機能を組み合わせて単一のインターフェイスとしてクライアントに提供できます。

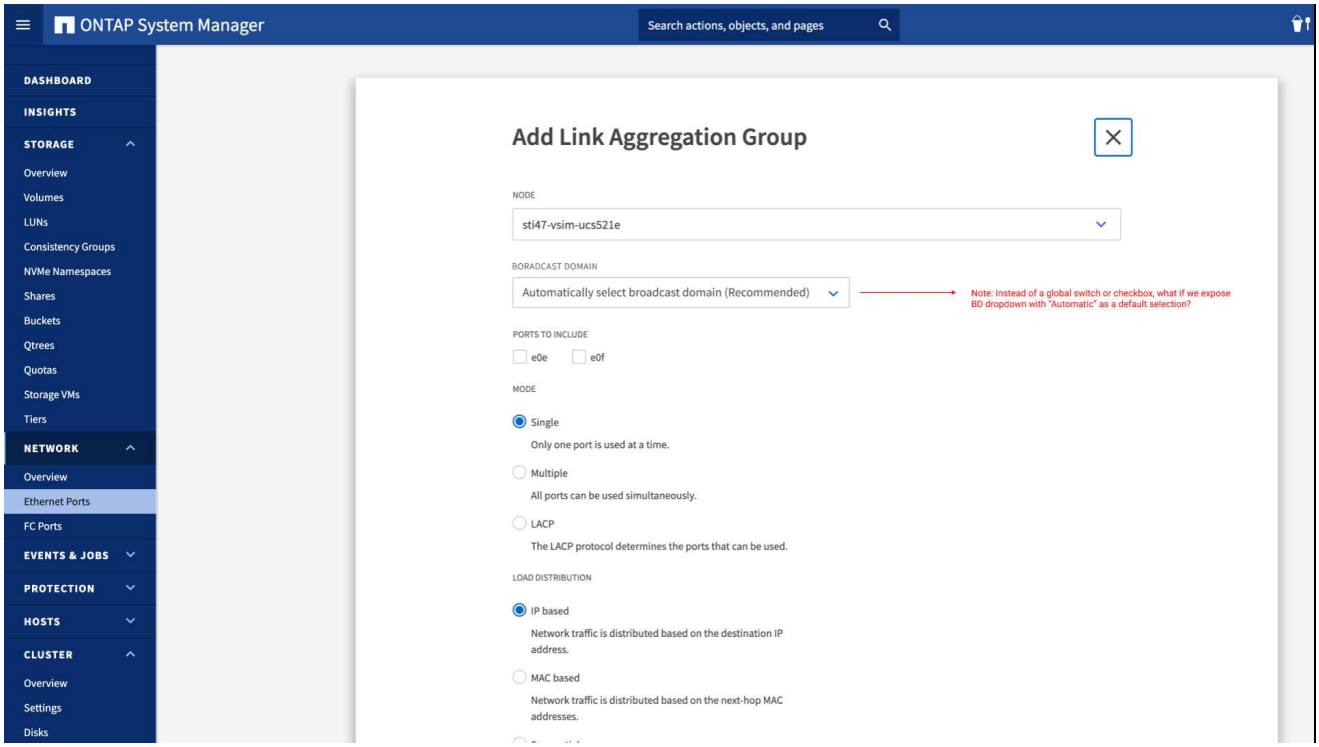
実行する手順は、使用するインターフェイス（System ManagerまたはCLI）によって異なります。

System Manager

- System Managerを使用してLAGを作成します。*

手順

1. [*Network]>[Ethernet port]>[+ Link Aggregation Group]を選択して、LAGを作成します。
2. ドロップダウンリストからノードを選択します。
3. 次のいずれかを選択します。
   a. ONTAP to * automatically select broadcast domain（推奨）*。
   b. ブロードキャストドメインを手動で選択するには、をクリックします。
4. LAGを構成するポートを選択します。
5. モードを選択します。
   a. Single：一度に1つのポートのみが使用されます。
   b. 複数：すべてのポートを同時に使用できます。
   c. LACP：LACPプロトコルによって、使用できるポートが決まります。
6. ロードバランシングを選択します。
   a. IPベース
   b. MACベース
   c. ポート
   d. シーケンシャル
7. 変更を保存します。



CLI

- CLIを使用してインターフェイスグループを作成*

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

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

- `port`：ネットワークトラフィックは、トランスポートレイヤ（TCP / UDP）ポートに基づいて分散されます。これが推奨されるロードバランシング方式です。
- `mac`：ネットワークトラフィックはMACアドレスに基づいて分散されます。
- `ip`：ネットワークトラフィックはIPアドレスに基づいて分散されます。
- `sequential`：ネットワークトラフィックは受信したとおりに分散されます。

> インターフェイスグループのMACアドレスは、基盤となるポートの順序、およびこれらのポートがブート時にどのように初期化されるかによって決まります。そのため、ifgrpのMACアドレスがリブート後やONTAPのアップグレード後に変更されることはありません。

ステップ

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

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

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

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

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

インターフェイスグループまたはLAGへのポートの追加

すべてのポート速度のインターフェイスグループまたはLAGに最大16個の物理ポートを追加できます。

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

System Manager

- System Managerを使用して、LAGにポートを追加します。*

手順

1. [*Network]>[Ethernet port]>[LAG]を選択して、LAGを編集します。
2. LAGに追加する同じノードの追加ポートを選択します。
3. 変更を保存します。

CLI

- CLIを使用して、インターフェイス・グループにポートを追加します。*

ステップ

インターフェイスグループにネットワークポートを追加します。

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

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

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

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

ONTAP 9 8以降では、最初の物理ポートがインターフェイスグループに追加されてから約1分後に、適切なブロードキャストドメインにインターフェイスグループが自動的に配置されます。ONTAPでこの処理を行わず、ifgrpを手動でブロードキャストドメインに配置する場合は、パラメータをコマンドの一部として `ifgrp add-port`指定します `-skip-broadcast-domain-placement`。

インターフェイスグループまたは**LAG**からポートを削除する

LIFをホストするインターフェイスグループからは、そのポートがインターフェイスグループ内の最後のポートでないかぎり、ポートを削除できます。最後のポートがインターフェイスグループから削除されないことを考慮して、インターフェイスグループがLIFをホストしていない、またはインターフェイスグループがLIFのホームポートでないという要件はありません。ただし、最後のポートを削除する場合は、先にインターフェイスグループからLIFを移行または移動する必要があります。

タスクの内容

インターフェイスグループまたはLAGから最大16個のポート（物理インターフェイス）を削除できます。

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

System Manager

- System Managerを使用して、LAGからポートを削除します。*

手順

1. [*Network]>[Ethernet port]>[LAG]を選択して、LAGを編集します。
2. LAGから削除するポートを選択します。
3. 変更を保存します。

CLI

- CLIを使用して、インターフェイスグループからポートを削除します。*

ステップ

インターフェイスグループからネットワークポートを削除します。

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

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

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

インターフェイスグループまたは**LAG**を削除する

基盤となる物理ポートに直接LIFを設定する場合や、インターフェイスグループやLAGのモードや分散機能を変更する場合は、インターフェイスグループやLAGを削除できます。

開始する前に

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

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

System Manager

- LAGを削除するには、System Managerを使用します。*

手順

1. [*Network]>[Ethernet port]>[LAG]を選択して、LAGを削除します。
2. 削除するLAGを選択します。
3. LAGを削除します。

CLI

- CLIを使用してインターフェイスグループ*を削除してください

ステップ

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

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

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

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

物理ポート経由のVLANの設定

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

VLANは複数の物理ネットワークセグメントにまたがることができます。VLANに属するエンドステーションは、機能またはアプリケーションによって関連付けられます。

たとえば、VLAN内のエンドステーションは、エンジニアリングや経理などの部門ごと、またはリリース1やリリース2などのプロジェクトごとにグループ化できます。VLANではエンドステーションが物理的に近接していることは重要ではないため、エンドステーションを地理的に分散させても、スイッチドネットワークにブロードキャストドメインを含めることができます。

ONTAP 9 .13.1および9.14.1では、任意の論理インターフェイス（LIF）で使用されておらず、接続されているスイッチでネイティブ接続が確立されていないタグなしポートは、デグレードとマークされます。これは使用されていないポートを特定するためのもので、停止を示すものではありません。ネイティブVLANでは、ONTAP CFMブロードキャストなどのタグなしトラフィックをifgrpベースポートで許可します。タグなしトラフィックをブロックしないように、スイッチにネイティブVLANを設定します。

VLANの管理では、VLANに関する情報を作成、削除、または表示できます。

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

VLANを作成します。

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

開始する前に

次の要件を満たしていることを確認します。

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

タスクの内容

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

ポート上でVLANを初めて設定すると、ポートがダウンし、ネットワークが一時的に切断されることがあります。その後同じポートにVLANを追加しても、ポートの状態には影響しません。

> スイッチのネイティブVLANと同じ識別子のVLANをネットワークインターフェイス上に作成しないでください。たとえば、ネットワークインターフェイスe0bがネイティブVLAN 10上にある場合、そのインターフェイスにVLAN e0b-10を作成しないでください。

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

System Manager

- System Managerを使用してVLANを作成します。*

ONTAP 9 .12.0以降では、ブロードキャストドメインを自動的に選択することも、リストから手動で[オン]を選択することもできます。これまでは、ブロードキャストドメインはレイヤ2の接続に基づいて常に自動的に選択されていました。ブロードキャストドメインを手動で選択すると、ブロードキャストドメインを手動で選択すると接続が失われる可能性があることを示す警告が表示されます。

手順

1. Network > Ethernet port >+VLAN *を選択します。
2. ドロップダウンリストからノードを選択します。
3. 次のいずれかを選択します。
   a. ONTAP to * automatically select broadcast domain（推奨）*。
   b. をクリックして、リストからブロードキャストドメインを手動で選択します。
4. VLANを形成するポートを選択します。
5. VLAN IDを指定します。
6. 変更を保存します。

CLI

- CLIを使用してVLANを作成してください*

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

手順

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

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

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

vlan.8以降では、ONTAP 9が作成されてから約1分後に適切なブロードキャストドメインに自動的に配置されます。この処理をONTAPで行わず、VLANをブロードキャストドメインに手動で配置する場合は、コマンドでパラメータを `vlan create`指定します `-skip-broadcast-domain-placement`。

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

VLANの編集

ブロードキャストドメインを変更したり、VLANを無効にしたりできます。

System Managerを使用してVLANを編集する

ONTAP 9 .12.0以降では、ブロードキャストドメインを自動的に選択することも、リストから手動で[オン]を選択することもできます。これまでのブロードキャストドメインは、レイヤ2の接続に基づいて常に自動的に選択されていました。ブロードキャストドメインを手動で選択すると、ブロードキャストドメインを手動で選択すると接続が失われる可能性があることを示す警告が表示されます。

手順

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

VLANの削除

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

開始する前に

VLANに関連付けられているLIFがないことを確認します。

タスクの内容

ポートから最後のVLANを削除すると、そのポートからネットワークが一時的に切断される可能性があります。

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

System Manager

- VLANを削除するには、System Managerを使用します。*

手順

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

CLI

- CLIを使用してVLAN *を削除します

ステップ

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

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

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

ネットワークポートの属性を変更します。

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

開始する前に

LIFをホストしているポートは変更できません。

タスクの内容

- 100GbE、40GbE、10GbE、または1GbEのネットワークインターフェイスの管理設定を変更することは推奨されません。

  二重モードおよびポート速度の設定値のことを管理設定と呼びます。ネットワークの制限によっては、管理設定が運用設定（ポートで実際に使用される二重モードと速度）と異なる場合があります。

- インターフェイスグループの基盤となる物理ポートの管理設定を変更することは推奨されません。

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

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

- VLANのMTUサイズは、ベースポートのMTUサイズの値を超えることはできません。

手順

1. ネットワークポートの属性を変更します。

   ```
   network port modify
   ```

2. フィールドをtrueに設定する `-ignore-health-status`と、指定したポートのネットワークポートのヘルスステータスを無視できるようになります。

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

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

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

10GbE接続用に40GbE NICポートを複数の10GbEポートに変換

X1144A-R6およびX91440A-R6の40GbEネットワークインターフェイスカード（NIC）を変換して、4つの10GbEポートをサポートすることができます。

どちらかの NIC をサポートするハードウェアプラットフォームを、 10GbE のクラスタインターコネクトと顧客データ接続をサポートするクラスタに接続する場合は、 NIC を変換して必要な 10GbE 接続を提供する必要があります。

開始する前に

サポートされているブレークアウトケーブルを使用する必要があります。

タスクの内容

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

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

手順

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

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

3. convertコマンドの使用が完了したら、ノードを停止します。
4. ケーブルを取り付けるか、交換します。

5. ハードウェアモデルに応じて、SP（サービスプロセッサ）またはBMC（ベースボード管理コントローラ）を使用してノードの電源を再投入し、変換を有効にします。

ONTAPシステム用のUTA X1143A-R6ポートの設定

X1143A-R6ユニファイドターゲットアダプタのポートは、デフォルトではFCターゲットモードで構成されますが、10GbイーサネットポートおよびFCoEポート（CNAポート）または16Gb FCイニシエータポートまたはターゲットポートとして構成することができます。これには、 SFP+ アダプタが必要です。

イーサネットおよびFCoE用に設定した場合、X1143A-R6アダプタは、同じ10-GBEポート上でNICおよびFCoEターゲットトラフィックを同時にサポートします。FC用に設定した場合、同じASICを共有する2ポートの各ペアをFCターゲットモードまたはFCイニシエータモード用に個別に設定できます。つまり、1つのX1143A-R6アダプタで、1つの2ポートペアでFCターゲットモードをサポートし、もう1つの2ポートペアでFCイニシエータモードをサポートできます。同じASICに接続されたポートペアは、同じモードで設定する必要があります。

X1143A-R6アダプタは、FCモードでは既存のFCデバイスと同様に動作し、最大速度は16Gbpsです。X1143A-R6アダプタをCNAモードで使用すると、同じ10GbEポートを共有するNICおよびFCoEのトラフィックを同時に処理できます。CNAモードでは、FCoE機能でFCターゲットモードのみがサポートされます。

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

手順

1. ポート設定を表示します。

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

2. 必要に応じて、Fibre Channel（FC；ファイバチャネル）またはConverged Network Adapter（CNA；統合ネットワークアダプタ）にポートを設定します。

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

3. FC または 10Gb イーサネットに適したケーブルを接続します。
4. 適切な SFP+ が取り付けられていることを確認します。

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

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

ONTAPでのUTA2ポートの変換

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

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

CNAモトカラ**FC**モトへ

手順

1. アダプタをオフラインにします。

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

2. ポートのモードを変更します。

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

3. ノードをリブートし、アダプタをオンラインにします。

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

4. 状況に応じて、管理者にポートの削除を依頼するか、 VIF マネージャでポートを削除します。
   - ポートが LIF のホームポートとして使用されている場合、インターフェイスグループ（ ifgrp ）のメンバーである場合、または VLAN をホストしている場合は、管理者は次の作業を行う必要があります。
     - LIF を移動するか、 ifgrp からポートを削除する、または VLAN をそれぞれ削除します。
     - コマンドを実行して、ポートを手動で削除し `network port delete`ます。コマンドが失敗した場合は `network port delete`、エラーに対処してからもう一度コマンドを実行する必要があります。
   - ポートが LIF のホームポートとして使用されていない場合、 ifgrp のメンバーでない場合、および VLAN をホストしていない場合は、リブート時に VIF マネージャのレコードからポートが削除されます。VIFマネージャでポートが削除されない場合は、管理者がリブート後にコマンドを使用して手動で削除する必要があります `network port delete`。
5. 適切な SFP+ が取り付けられていることを確認します。

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

CNAの場合は、10GbイーサネットSFPを使用する必要があります。FC の場合は、ノードで構成を変更する前に、 8Gb SFP または 16Gb SFP を使用します。

FCモオトカラ**CNA**モオトへ

手順

1. アダプタをオフラインにします。

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

2. ポートのモードを変更します。

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

3. ノードをリブートする
4. 正しいSFP+が取り付けられていることを確認します。

   CNAの場合は、10GbイーサネットSFPを使用する必要があります。

ONTAPシステム用のCNA / UTA2光モジュールの変換

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

手順

1. カードで使用されている現在の SFP+ を確認します。次に、現在の SFP+ を、優先して使用するパーソナリティ（ FC または CNA ）に適した SFP+ に差し替えます。
2. X1143A-R6アダプタから現在の光モジュールを取り外します。
3. 使用するパーソナリティモード（FCまたはCNA）光ファイバに適したモジュールを挿入します。
4. 適切な SFP+ が取り付けられていることを確認します。

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

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

ノードからのNICの取り外し（ONTAP 9.8以降）

このトピックはONTAP 9.8以降が対象です。障害の発生したNICをスロットから取り外したり、メンテナンス時にNICを別のスロットに移したりしなければならない場合があります。

手順

1. ノードの電源をオフにします。
2. NICをスロットから物理的に取り外します。

3. ノードの電源を投入します。
4. ポートが削除されたことを確認します。

```
network port show
```

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

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

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

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

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

```
displaced-vlans restore
```

7. ポートにLIFが設定されている場合は、同じブロードキャストドメイン内の別のポートの新しいホームポートがONTAPによって自動的に選択されます。同じFilerに適切なホーム・ポートが見つからない場合、それらのLIFは削除されたとみなされます。削除されたLIFは、次のコマンドを使用して確認できます。

```
displaced-interface show
```

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

ノードからのNICの取り外し（ONTAP 9.7以前）

このトピックはONTAP 9.7以前が対象です。障害の発生したNICをスロットから取り外したり、メンテナンス時にNICを別のスロットに移したりしなければならない場合があります。

開始する前に

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

手順

1. NICからポートを削除します。

   ```
   network port delete
   ```

2. ポートが削除されたことを確認します。

   ```
   network port show
   ```

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

ネットワークポートの監視

ネットワークポートの健全性の監視

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

タスクの内容

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

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

デグレード状態のポートの以下の動作に注意してください。

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

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

- LIFは、デグレード状態のポートから正常な状態のポートに自動的に移行されます。
- フェイルオーバー時には、デグレード状態のポートはフェイルオーバーターゲットとみなされません。正常なポートがない場合は、通常のフェイルオーバーポリシーに従ってデグレード状態のポートがLIFをホストします。
- デグレード状態のポートに LIF を作成、移行、リバートすることはできません。

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

手順

1. advanced権限モードにログインします。

```
set -privilege advanced
```

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

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

ポートのヘルスステータスは、ヘルスモニタの値によって決まります。

ONTAP でデフォルトで有効になっていて使用可能なヘルスモニタは次のとおりです。

- リンクフラッピングヘルスモニタ：リンクフラッピングを監視します

  5 分以内に複数回のリンクフラッピングが発生しているポートは、デグレードとマークされます。

- L2 到達可能性ヘルスモニタ：同じブロードキャストドメインに設定されたすべてのポートで相互のポートに対するレイヤ 2 到達可能性が確保されているかどうかを監視します

  このヘルスモニタは、すべての IPspace におけるレイヤ 2 到達可能性の問題を報告しますが、デグレードとマークされるのはクラスタ IPspace 内のポートのみです。

- CRC モニタ：ポートの CRC 統計を監視します

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

3. コマンドを使用して、IPspaceのヘルスモニタを必要に応じて有効または無効にします `network options port-health-monitor modify`。
4. ポートの詳細な健全性を表示します。

```
network port show -health
```

コマンド出力には、ポートのヘルスステータス、設定、およびポートがデグレードとマークされた理由のリストが表示され `ignore health status`ます。

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

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

設定がの `false`場合、 `ignore health status`ポートのヘルスステータスはシステムによって自動的に判断されます。

ネットワークポートの到達可能性を監視する（**ONTAP 9 .8**以降）

到達可能性の監視は、ONTAP 9 .8以降に組み込まれています。この監視機能を使用して、物理ネットワークトポロジがONTAPの設定と一致しない場合を特定します。場合によっては、ONTAPによってポートの到達可能性が修復されることがあります。それ以外の場合は、追加の手順が必要です。

タスクの内容

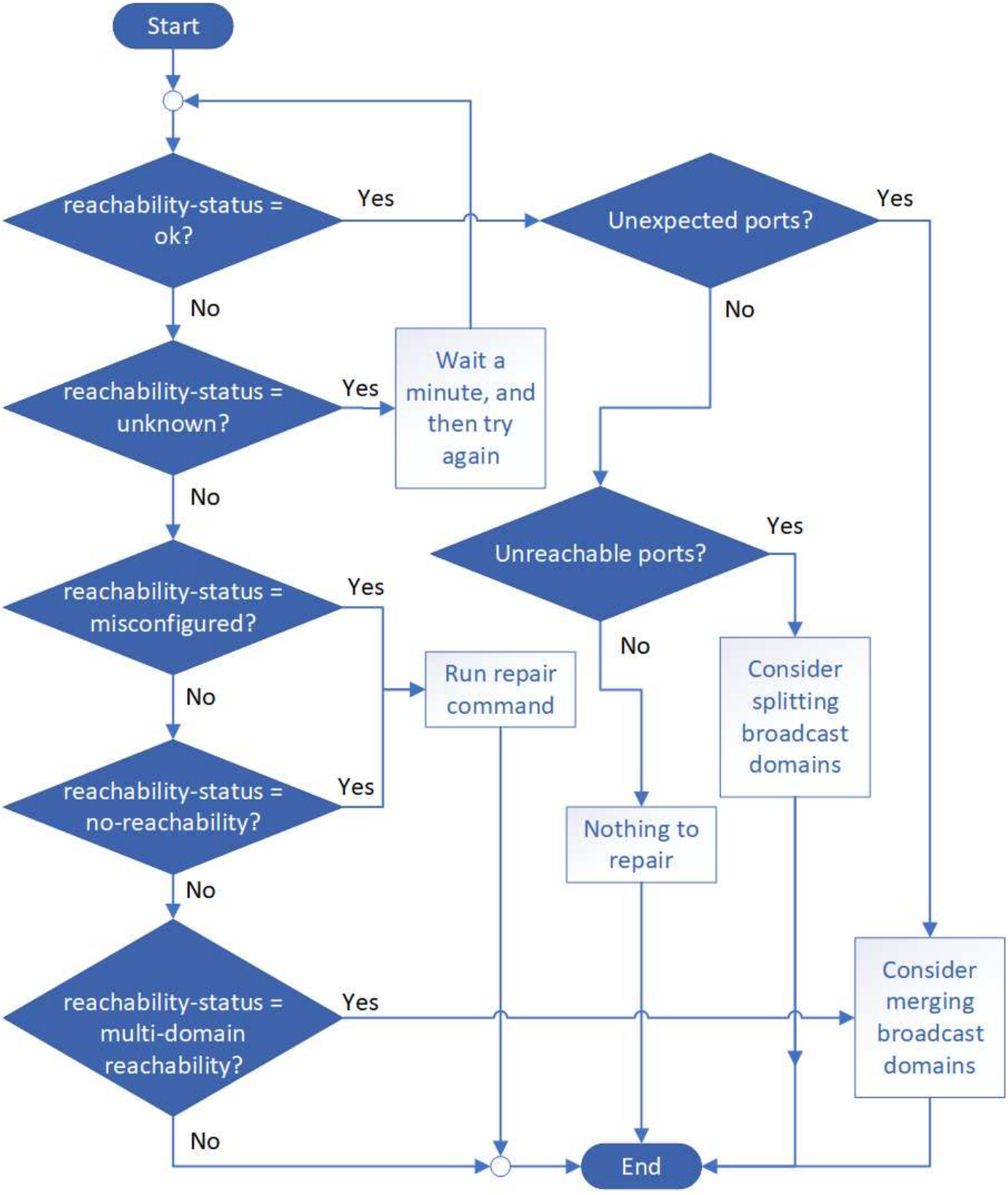
これらのコマンドを使用して、ONTAPの設定が物理的なケーブル配線またはネットワークスイッチの設定と一致しないことに起因するネットワークの設定ミスを検証、診断、および修復します。

ステップ

1. ポートの到達可能性を表示します。

```
network port reachability show
```

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



プレゼンスステータス	説明

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

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

ポートを修理したら、削除されたLIFとVLANを確認して解決する必要があります。ポートがインターフェイスグループに属していた場合は、そのインターフェイスグループの状況についても理解しておく必要があります。詳細については、を参照してください "ポートの到達可能性を修復"。

ONTAPポートの概要

多くのwell-knownポートは、特定のサービスとのONTAP通信用に予約されています。ストレージネットワーク環境のポート値がONTAPポートの値と同じ場合、ポートの競合が発生します。

次の表に、ONTAPで使用されるTCPポートとUDPポートを示します。

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

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

ONTAP内部ポート

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

ポート / プロトコル	説明
514	syslog

900	NetAppクラスタRPC
902	NetAppクラスタRPC
904	NetAppクラスタRPC
905	NetAppクラスタRPC
910	NetAppクラスタRPC
911	NetAppクラスタRPC
913	NetAppクラスタRPC
914	NetAppクラスタRPC
915	NetAppクラスタRPC
918	NetAppクラスタRPC
920	NetAppクラスタRPC
921	NetAppクラスタRPC
924	NetAppクラスタRPC
925	NetAppクラスタRPC
927	NetAppクラスタRPC
928	NetAppクラスタRPC
929	NetAppクラスタRPC
931	NetAppクラスタRPC
932	NetAppクラスタRPC
933	NetAppクラスタRPC
934	NetAppクラスタRPC
935	NetAppクラスタRPC
936	NetAppクラスタRPC
937	NetAppクラスタRPC
939	NetAppクラスタRPC
940	NetAppクラスタRPC
951	NetAppクラスタRPC
954	NetAppクラスタRPC
955	NetAppクラスタRPC
956	NetAppクラスタRPC
958	NetAppクラスタRPC
961	NetAppクラスタRPC
963	NetAppクラスタRPC
964	NetAppクラスタRPC

966	NetAppクラスタRPC
967	NetAppクラスタRPC
982	NetAppクラスタRPC
983	NetAppクラスタRPC
5125	ディスクの代替制御ポート
5133	ディスクの代替制御ポート
5144	ディスクの代替制御ポート
65502	ノードスコープSSH
65503	LIF共有
7810	NetAppクラスタRPC
7811	NetAppクラスタRPC
7812	NetAppクラスタRPC
7813	NetAppクラスタRPC
7814	NetAppクラスタRPC
7815	NetAppクラスタRPC
7816	NetAppクラスタRPC
7817	NetAppクラスタRPC
7818	NetAppクラスタRPC
7819	NetAppクラスタRPC
7820	NetAppクラスタRPC
7821	NetAppクラスタRPC
7822	NetAppクラスタRPC
7823	NetAppクラスタRPC
7824	NetAppクラスタRPC
8023	ノードスコープTelnet
8514	ノードスコープRSH
9877	KMIPクライアントポート（内部ローカルホストのみ）

著作権に関する情報

商標に関する情報