# ネットワーク ポート

## ONTAP 9

NetApp
February 12, 2026

# 目次


ネットワーク ポート . . . 1
- ONTAPネットワークポート構成について学ぶ . . . 1
- ネットワーク ポートの設定 . . . 1
  - 物理ポートを組み合わせてONTAPインターフェースグループを作成する . . . 2
  - 物理ポート経由でONTAP VLANを設定する . . . 11
  - ONTAPネットワークポート属性を変更する . . . 15
  - 40GbE NICポートを変換してONTAPネットワーク用の10GbEポートを作成する . . . 16
  - ONTAPネットワーク用にUTA X1143A-R6ポートを設定する . . . 17
  - UTA2ポートをONTAPネットワークで使用するために変換する . . . 18
  - CNA/UTA2光モジュールをONTAPネットワーク用に変換する . . . 20
  - ONTAPクラスタノードからNICを削除する . . . 20
  - ネットワーク ポートの監視 . . . 22

# ネットワーク ポート

## ONTAPネットワークポート構成について学ぶ

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

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

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

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

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

ポートの命名規則は *enumberletter* です：

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

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

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

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

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

# ネットワーク ポートの設定

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

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

## インターフェイス グループの種類

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

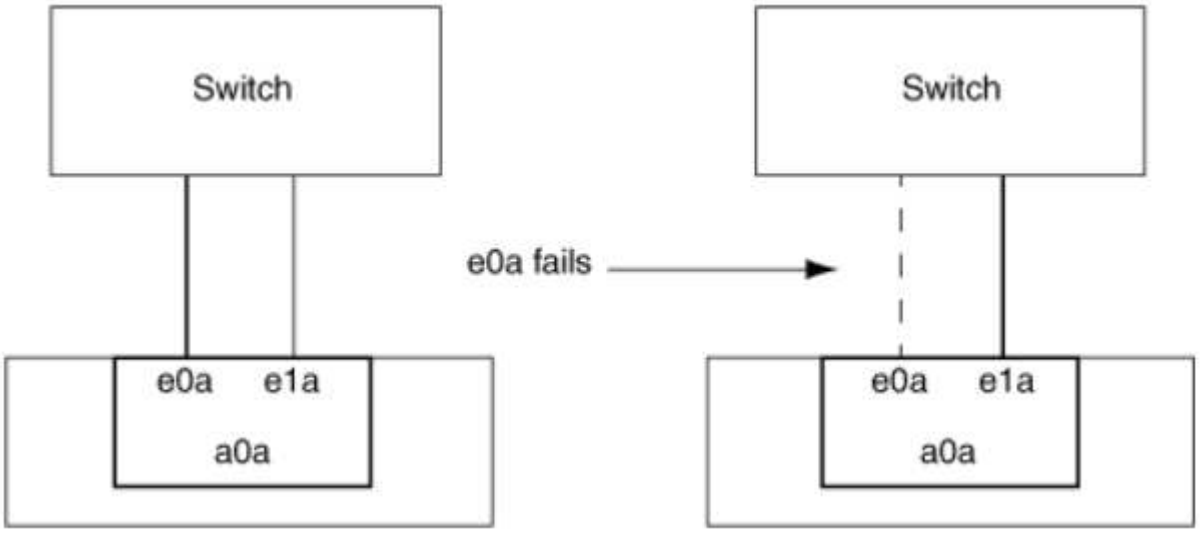
### シングルモード インターフェイス グループの特性

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

シングルモード インターフェイス グループの特性は、次のとおりです。

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

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



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

スタティック マルチモード インターフェイス グループの特性

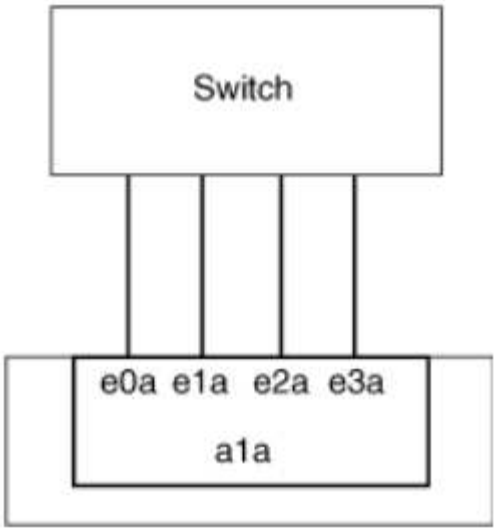
ONTAPに実装されているスタティック マルチモード インターフェイス グループは、IEEE 802.3ad（static）に準拠しています。スタティック マルチモード インターフェイス グループでは、アグリゲーションはサポートするがアグリゲーション設定のための制御パケット交換は行わないスイッチを使用できます。

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

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

- インターフェイス グループ内のすべてのインターフェイスがアクティブで、単一のMACアドレスを共有します。
  - 複数の接続が、インターフェイス グループ内のインターフェイスに分散されます。
  - 各接続またはセッションが、インターフェイス グループ内の1つのインターフェイスを使用します。シーケンシャル ロード バランシング方式を使用する場合、すべてのセッションはパケット ベースで使用可能なリンク全体で分散され、インターフェイス グループの特定のインターフェイスにバインドされません。
- スタティック マルチモード インターフェイス グループは、最大「n-1」個のインターフェイスの障害から回復することができます。この「n」は、インターフェイス グループを構成しているインターフェイスの合計数です。
- あるポートで障害が発生した場合や切断された場合は、そのリンクを経由していたトラフィックが残りのインターフェイスの1つに自動的に再分散されます。
- スタティック マルチモード インターフェイス グループではリンクの喪失は検出できますが、クライアントへの接続の切断や、接続性とパフォーマンスに影響を及ぼす可能性があるスイッチの設定ミスは検出できません。
- スタティック マルチモード インターフェイス グループには、複数のスイッチ ポートでのリンク アグリゲーションをサポートするスイッチが必要です。インターフェイス グループの各リンクの接続先ポートがすべて1つの論理ポートを構成するよう、そのスイッチを設定します。一部のスイッチは、ジャンボ フレーム用に構成されたポートのリンク アグリゲーションをサポートしていない場合があります。詳細については、スイッチ ベンダーのマニュアルを参照してください。
- スタティック マルチモード インターフェイス グループのインターフェイス間でのトラフィック分散には、いくつかのロード バランシング オプションを使用できます。

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




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

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

### ダイナミック マルチモード インターフェイス グループ

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

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

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

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

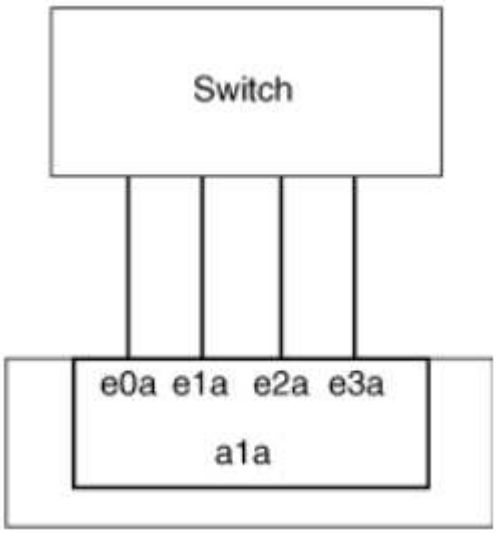
ONTAPのロード バランシング アルゴリズムは、発信トラフィックの転送に使用されるメンバー ポートを決定しますが、着信フレームの受信方法は制御しません。スイッチは、そのポート チャネル グループに設定されたロード バランシング アルゴリズムに基づいて、転送に使用されるポート チャネル グループのメンバー（個々の物理ポート）を決定します。したがって、スイッチの設定により、トラフィックを受信するストレージ システムのメンバー ポート（個々の物理ポート）が決まります。スイッチ設定の詳細については、スイッチ ベンダーのマニュアルを参照してください。

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

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

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

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




マルチモード インターフェイス グループでのロード バランシング

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

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

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

ポートベースのロード バランシング

ポートベースのロード バランシングは推奨される方式です。

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

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

### IPアドレスおよびMACアドレスによるロード バランシング

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

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

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

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

### シーケンシャル ロード バランシング

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

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

### インターフェイス グループ（別名LAG）の作成

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

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

**System Manager**

**System Manager** を使用して **LAG** を作成します

手順

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

**CLI**

**CLI** を使用してインターフェース グループを作成する

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

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

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

手順

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

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

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

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

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

インターフェイス グループ（別名**LAG**）へのポートの追加

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

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

**System Manager**

**System Manager**を使用してポートを**LAG**に追加します

手順

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

**CLI**

**CLI** を使用してインターフェイス グループにポートを追加する

手順

インターフェイス グループにネットワーク ポートを追加します。

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

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

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

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

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

インターフェイス グループ（別名**LAG**）からのポートの削除

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

タスク概要

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

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

**System Manager**

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

手順

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

**CLI**

**CLI** を使用してインターフェイス グループからポートを削除する

手順

インターフェイス グループからネットワーク ポートを削除します。

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

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

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

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

インターフェイス グループ（別名**LAG**）の削除

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

開始する前に

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

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

**System Manager**

**System Manager**を使用して**LAG**を削除します

手順

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

**CLI**

**CLI** を使用してインターフェース グループを削除する

手順

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

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

次に、a0bという名前のインターフェイス グループを削除する例を示します。

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

## 物理ポート経由で**ONTAP VLAN**を設定する

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

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

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

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

管理者は、VLANを作成または削除したり、その情報を表示したりできます。

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

**VLAN**の作成

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

開始する前に

次の要件を満たしていることを確認します。

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

タスク概要

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

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

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

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

**System Manager**

**System Manager**を使用して**VLAN**を作成する

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

手順

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

**CLI**

**CLI** を使用して **VLAN** を作成する

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

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

手順

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

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

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

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

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

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

### VLANの編集

ブロードキャスト ドメインを変更したり、VLANを無効にしたりできます。

#### System Managerを使用したVLANの編集

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

手順

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

### VLANの削除

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

開始する前に

VLANに関連付けられているLIFがないことを確認します。

タスク概要

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

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

**System Manager**

**System Manager**を使用して**VLAN**を削除する

手順

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

**CLI**

**CLI** を使用して **VLAN** を削除する

手順

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

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

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

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

## ONTAPネットワークポート属性を変更する

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

開始する前に

LIFをホストしているポートは変更できません。

タスク概要

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

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

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

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

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

手順

1. ネットワーク ポートの属性を変更します。

   ```
   network port modify
   ```

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

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

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

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

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

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

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

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

開始する前に

サポート対象のブレークアウト ケーブルを使用している必要があります。

タスク概要

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

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

手順

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

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

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

## ONTAPネットワーク用にUTA X1143A-R6ポートを設定する

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

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

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

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

手順

1. ポート構成を表示します：

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

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

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

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

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

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

## UTA2ポートをONTAPネットワークで使用するために変換する

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

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

**CNA**モードから**FC**モードへ

手順

1. アダプタをオフラインにします。

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

2. ポートのモードを変更します。

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

3. ノードをリブートし、アダプタをオンラインにします。

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

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

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

5. 正しい SFP+ がインストールされていることを確認します：

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

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

**FC**モードから**CNA**モードへ

手順

1. アダプタをオフラインにします。

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

2. ポートのモードを変更します。

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

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

   CNAの場合は、10GbイーサネットSFPを使用する必要があります。

## CNA/UTA2光モジュールをONTAPネットワーク用に変換する

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

手順

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

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

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

## ONTAPクラスタノードからNICを削除する

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

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

手順

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

```
network port show
```

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

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

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

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

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

```
displaced-vlans restore
```

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

```
displaced-interface show
```

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

関連情報

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

# ネットワーク ポートの監視

**ONTAP**ネットワークポートの健全性を監視する

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

タスク概要

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

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

デグレード状態のポートについては、以下の動作に注意する必要があります。

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

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

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

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

手順

1. advanced権限モードにログインします。

```
set -privilege advanced
```

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

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

ポートのヘルス ステータスは、ヘルスモニタの値によって決まります。

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

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

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

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

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

- CRCモニター：ポートのCRC統計を監視します

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

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

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

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

4. ポートの詳細な健全性を表示します。

   ```
   network port show -health
   ```

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

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

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

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

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

**ONTAP**ネットワークポートの到達可能性を監視する

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

タスク概要

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

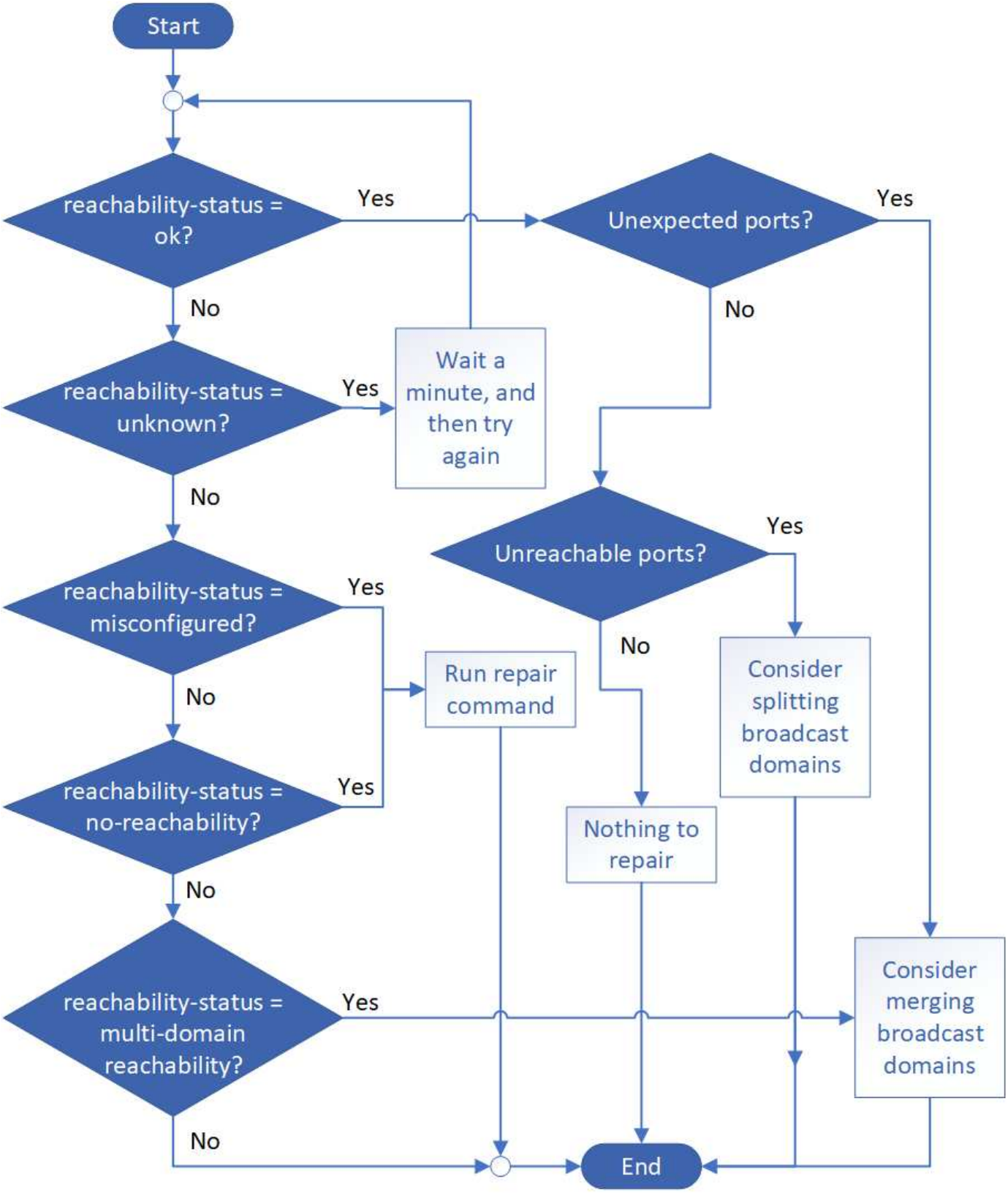
手順

1. ポートの到達可能性を表示します。

```
network port reachability show
```

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

2. 次のデシジョン ツリーと表を参照して、次に実行する手順を確認します。




| 到達可能性ステータス | 概要 |
| --- | --- |

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

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

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

**ONTAP**ネットワークでのポートの使用について学ぶ

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

インバウンド トラフィック

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

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

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

送信トラフィック

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

基本的なアウトバウンドルール

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

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

高度なアウトバウンドルール

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

### Active Directory

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

### AutoSupport

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

### SNMP

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

**SnapMirror**

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

その他のサービス

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

**ONTAP**内部ポートについて学ぶ

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

このリストは網羅的なものではなく、環境によって異なる場合があります。

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

| | |
|---|---|
| 914 | NetAppクラスタRPC |
| 915 | NetAppクラスタRPC |
| 918 | NetAppクラスタRPC |
| 920 | NetAppクラスタRPC |
| 921 | NetAppクラスタRPC |
| 924 | NetAppクラスタRPC |
| 925 | NetAppクラスタRPC |
| 927 | NetAppクラスタRPC |
| 928 | NetAppクラスタRPC |
| 929 | NetAppクラスタRPC |
| 930 | カーネルサービスおよび管理機能（KSMF） |
| 931 | NetAppクラスタRPC |
| 932 | NetAppクラスタRPC |
| 933 | NetAppクラスタRPC |
| 934 | NetAppクラスタRPC |
| 935 | NetAppクラスタRPC |
| 936 | NetAppクラスタRPC |
| 937 | NetAppクラスタRPC |
| 939 | NetAppクラスタRPC |
| 940 | NetAppクラスタRPC |
| 951 | NetAppクラスタRPC |
| 954 | NetAppクラスタRPC |
| 955 | NetAppクラスタRPC |
| 956 | NetAppクラスタRPC |
| 958 | NetAppクラスタRPC |
| 961 | NetAppクラスタRPC |
| 963 | NetAppクラスタRPC |
| 964 | NetAppクラスタRPC |
| 966 | NetAppクラスタRPC |
| 967 | NetAppクラスタRPC |
| 975 | Key Management Interoperability Protocol（KMIP） |
| 982 | NetAppクラスタRPC |
| 983 | NetAppクラスタRPC |
| 5125 | ディスク用の代替制御ポート |

| | |
|---|---|
| 5133 | ディスク用の代替制御ポート |
| 5144 | ディスク用の代替制御ポート |
| 65502 | ノードを対象としたSSH |
| 65503 | LIFの共有 |
| 7700 | Cluster Session Manager（CSM） |
| 7810 | NetAppクラスタRPC |
| 7811 | NetAppクラスタRPC |
| 7812 | NetAppクラスタRPC |
| 7813 | NetAppクラスタRPC |
| 7814 | NetAppクラスタRPC |
| 7815 | NetAppクラスタRPC |
| 7816 | NetAppクラスタRPC |
| 7817 | NetAppクラスタRPC |
| 7818 | NetAppクラスタRPC |
| 7819 | NetAppクラスタRPC |
| 7820 | NetAppクラスタRPC |
| 7821 | NetAppクラスタRPC |
| 7822 | NetAppクラスタRPC |
| 7823 | NetAppクラスタRPC |
| 7824 | NetAppクラスタRPC |
| 7835-7839および7845-7849 | クラスタ内通信用のTCPポート |
| 8023 | ノードを対象としたTelnet |
| 8443 | Amazon FSx 用 ONTAP S3 NAS ポート |
| 8514 | ノードを対象としたRSH |
| 9877 | KMIPクライアント ポート（内部ローカル ホストのみ） |
| 10006 | HAインターコネクト通信用のTCPポート |

## 著作権に関する情報



## 商標に関する情報