ネットワーク ポートの監視

ONTAP 9

NetApp
February 12, 2026

目次

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。

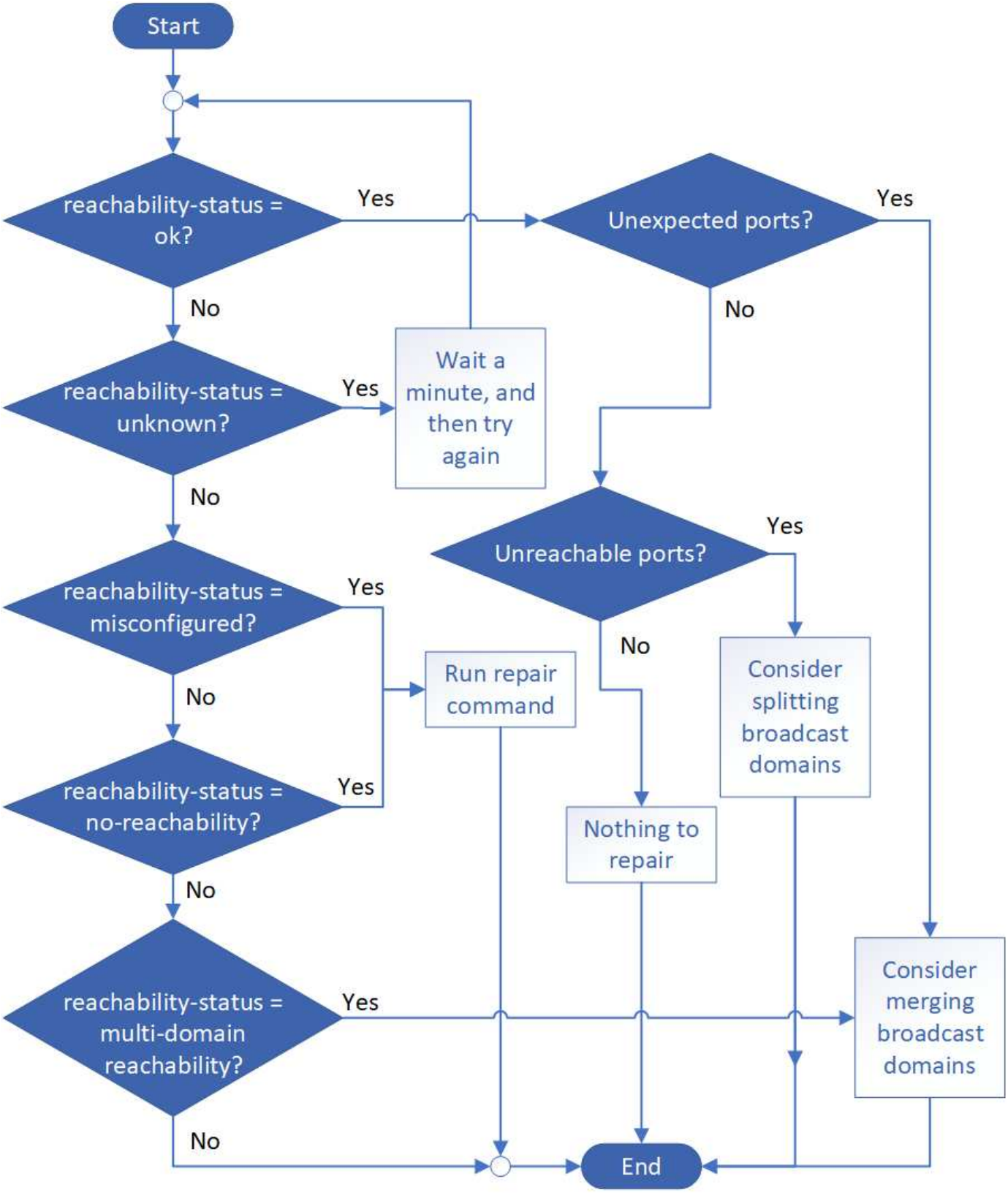
手順

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

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

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

ONTAPネットワークでのポートの使用について学ぶ

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

インバウンド トラフィック

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

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

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

送信トラフィック

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

基本的なアウトバウンドルール

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

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

高度なアウトバウンドルール

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

Active Directory

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

AutoSupport

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

SNMP

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

SnapMirror

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

その他のサービス

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

ONTAP内部ポートについて学ぶ

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

このリストは網羅的なものではなく、環境によって異なる場合があります。

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

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

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

著作権に関する情報

商標に関する情報