論理インターフェイス（LIF）

ONTAP 9

NetApp
December 20, 2024

目次

論理インターフェイス（LIF）

LIFの概要

LIFの設定の概要

LIF（論理インターフェイス）は、クラスタ内のノードへのネットワークアクセスポイントを表します。LIFは、クラスタでネットワーク経由の通信の送受信に使用するポートに設定できます。

クラスタ管理者は、LIFを作成、表示、変更、移行、リバート、削除できます。SVM管理者は、SVMに関連付けられているLIFだけを表示できます。

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

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

LIFは次のポートでホストできます。

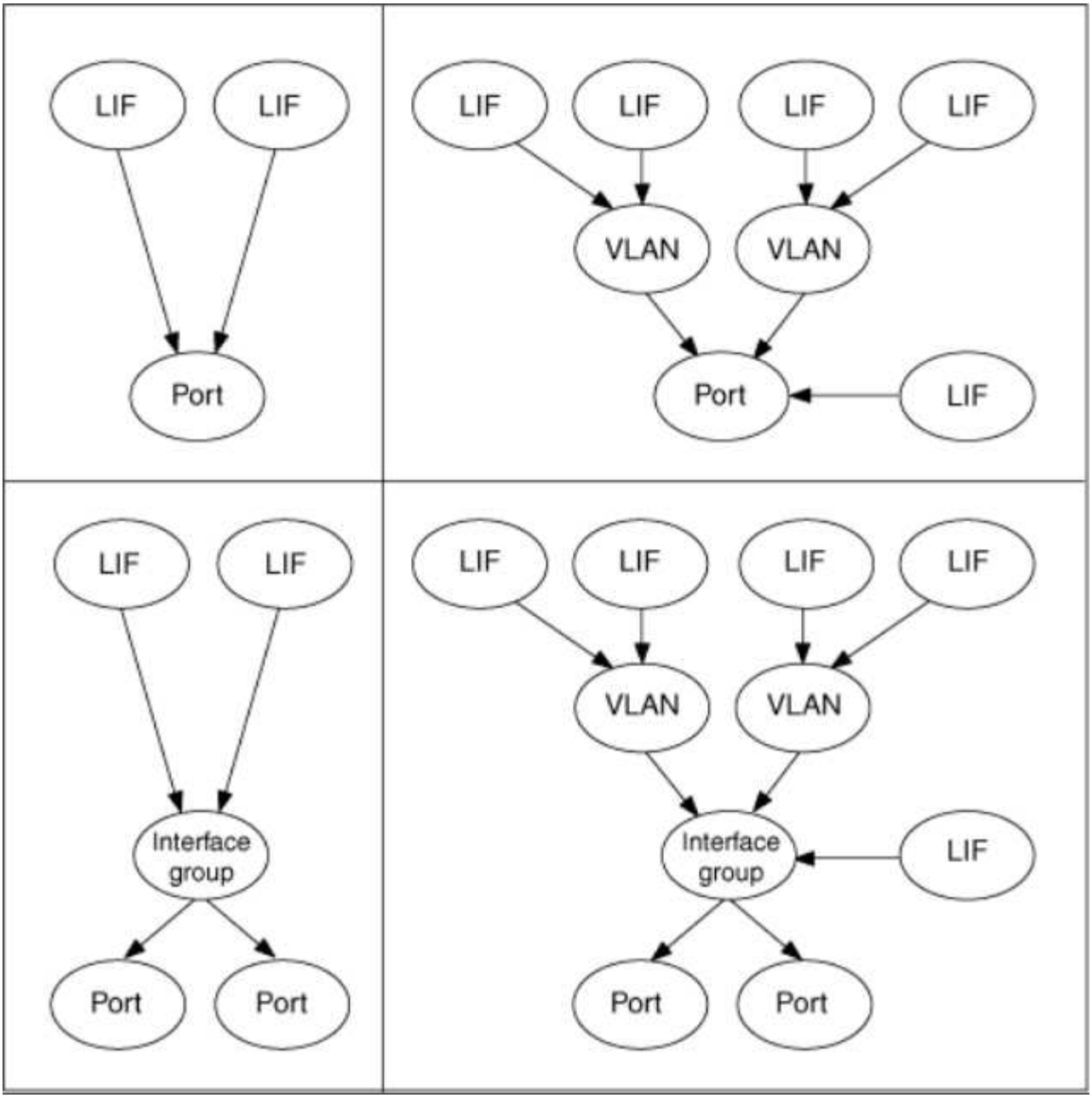
- インターフェイスグループに属していない物理ポート
- インターフェイスグループ
- VLAN
- VLANをホストする物理ポートまたはインターフェイスグループ
- 仮想IP（VIP）ポート

  ONTAP 9 5以降では、VIP LIFがサポートされ、VIPポートでホストされます。

LIFでFCなどのSANプロトコルを設定する際には、WWPNに関連付けられます。

"SAN管理"

次の図に、ONTAPシステムのポート階層を示します。



LIFのフェイルオーバーとギブバック

LIFのフェイルオーバーが発生すると、LIFがホーム ノードまたはポートからHAパートナー ノードまたはポートに移動します。LIFのフェイルオーバーは、物理イーサネット リンクが停止した場合や、ノードがレプリケートされたデータベース（RDB）クォーラムのメンバーでなくなった場合などの特定のイベント時に、ONTAPで自動的にトリガーすることも、クラスタ管理者が手動で開始することもできます。LIFのフェイルオーバーが発生した場合、フェイルオーバーの原因が解決されるまで、ONTAPはパートナー ノードで通常の動作を継続します。ホーム ノードまたはポートの健全性が回復すると、LIFはHAパートナーからホーム ノードまたはポートにリバートされます。このリバートはギブバックと呼ばれます。

LIFのフェイルオーバーとギブバックのためには、各ノードのポートが同じブロードキャスト ドメインに属している必要があります。各ノードの関連するポートが同じブロードキャスト ドメインに属していることを確認するには、以下を参照してください。

- ONTAP 9 .8以降："ポートの到達可能性を修復"

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

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

- データサービスポリシーを使用するLIFでは、フェイルオーバーポリシーの制限を確認できます。
  - ONTAP 9 .6以降："ONTAP 9 .6以降のLIFとサービスポリシー"
  - ONTAP 9 .5以前："ONTAP 9 .5以前のLIFのロール"
- LIFの自動リバートは、自動リバートがに設定されていて、LIFのホームポートが正常に機能していてLIFをホストできる場合に実行され `true`ます。
- 計画的または計画外のノードのテイクオーバーでは、テイクオーバーされたノードのLIFがHAパートナーにフェイルオーバーされます。LIFのフェイルオーバー先のポートは、VIF Managerによって決まります。
- フェイルオーバーが完了すると、LIFは正常に動作します。
- 自動リバートがに設定されている場合、ギブバックが開始されると、LIFはホームノードとホームポートにリバート `true`されます。
- 1つ以上のLIFをホストしているポートでイーサネットリンクが停止すると、VIF ManagerはLIFを停止しているポートから同じブロードキャストドメイン内の別のポートに移行します。新しいポートは、同じノードまたはそのHAパートナーに配置できます。リンクがリストアされたあとにauto-revertがに設定されている場合、 `true`VIF ManagerはLIFをそれぞれのホームノードとホームポートにリバートします。
- ノードがレプリケートされたデータベース（RDB）クォーラムのメンバーでなくなると、VIF ManagerはLIFをクォーラムのノードからHAパートナーに移行します。ノードがクォーラムに復帰し、自動リバートがに設定されている場合は `true`、VIF ManagerによってLIFがホームノードとホームポートにリバートされます。

ポートタイプトノ**LIF**ノゴカンセイ

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

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

LIF	説明
Data LIF	Storage Virtual Machine（SVM）に関連付けられたLIFで、クライアントとの通信に使用します。1つのポートに複数のデータLIFを設定できます。これらのインターフェイスは、クラスタ全体で移行またはフェイルオーバーできます。ファイアウォールポリシーをmgmtに変更すると、データLIFをSVM管理LIFとして使用できます。データLIFは、NIS、LDAP、Active Directory、WINS、およびDNSの各サーバに対するセッションで使用されます。

クラスタLIF	クラスタ内のノード間のトラフィックに使用されるLIFです。クラスタLIFは、常にクラスタポートに作成する必要があります。クラスタLIFは、同じノードのクラスタポート間でフェイルオーバーできますが、リモートノードに移行またはフェイルオーバーすることはできません。新しいノードがクラスタに追加されると、IPアドレスが自動的に生成されます。ただし、クラスタLIFにIPアドレスを手動で割り当てる場合は、新しいIPアドレスが既存のクラスタLIFと同じサブネット範囲にあることを確認する必要があります。
クラスタ管理LIF	クラスタ全体に対する単一の管理インターフェイスを提供するLIFです。クラスタ管理LIFは、クラスタ内の任意のノードにフェイルオーバーできます。クラスタポートまたはクラスタ間ポートにはフェイルオーバーできない
クラスタ間LIF	クラスタ間の通信、バックアップ、およびレプリケーションに使用されるLIFです。クラスタピア関係を確立する前に、クラスタ内の各ノードにクラスタ間LIFを作成する必要があります。これらのLIFは、同じノード内のポートにのみフェイルオーバーできます。クラスタ内の別のノードに移行またはフェイルオーバーすることはできません。
ノード管理LIF	クラスタ内の特定のノードを管理するために専用のIPアドレスを提供するLIFです。クラスタの作成時またはクラスタへのノードの追加時に作成されます。これらのLIFは、クラスタからノードにアクセスできなくなった場合など、システムのメンテナンスに使用されます。
VIP LIF	VIP LIFは、VIPポート上に作成された任意のデータLIFです。詳細については、を参照してください"仮想IP（VIP）LIFの設定"。

ONTAPでサポートされるトラフィックを管理します。

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

- ONTAP 9 .5以前のリリースでは、LIFのロールとファイアウォールサービスが使用されます。
- ONTAP 9 .6以降のリリースでは、LIFのサービスポリシーを使用します。
  - ONTAP 9 .5リリースで、LIFサービスポリシーが導入されました。
  - ONTAP 9 .6は、LIFのロールをLIFのサービスポリシーに置き換えました。
  - ファイアウォールサービスをONTAP 9のサービスポリシーに置き換えました。

設定する方法は、使用するONTAPのリリースによって異なります。

詳細については、以下を参照してください。

- ファイアウォールポリシーについては、を参照してください"コマンド：firewall-policy-show"。
- LIFのロールについては、を参照し"LIFのロール（ONTAP 9.5以前）"てください。
- LIFサービスポリシーについては、を参照し"LIFとサービスポリシー（ONTAP 9 .6以降）"てください。

LIFとサービスポリシー（ONTAP 9 .6以降）

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

クの種類を決定するサービスポリシーをLIFに割り当てることができます。サービスポリシーは、LIFでサポートされる一連のネットワークサービスを定義します。ONTAPには、LIFに関連付けることができる一連の組み込みのサービスポリシーが用意されています。

サービスポリシーとその詳細を表示するには、次のコマンドを使用します。

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

特定のサービスにバインドされていない機能では、システム定義の動作を使用してアウトバウンド接続用のLIFが選択されます。

サービスポリシーが空のLIF上のアプリケーションが予期せず動作することがあります。

システム**SVM**のサービスポリシー

管理SVMとシステムSVMには、管理LIFやクラスタ間LIFなど、そのSVMのLIFに使用できるサービスポリシーが含まれています。これらのポリシーは、IPspaceの作成時にシステムによって自動的に作成されます。

次の表に、ONTAP 9時点でのシステムSVMのLIFの組み込みのポリシーを示します。それ以外のリリースの場合は、次のコマンドを使用してサービスポリシーとその詳細を表示します。

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

ポリシー	付属サービス	同等のロール	説明
デフォルト - intercluster	インタークラスタコア、管理 - https ： //	クラスタ間	クラスタ間トラフィックを処理する LIF で使用されます。注：サービス intercluster-core は、 net-intercluster サービスポリシーという名前で ONTAP 9.5 から提供されています。
default-route-announce	management-bgp	-	BGP ピア接続を処理する LIF で使用されます。注： ONTAP 9.5 では net-route-announce サービスポリシーという名前で提供されています。

default-management	management-core 、management-https、management-http、management-ssh、management-autosupport、management-ems 、management-dns-client、management-ad-client, management-ldap-client, management-nis-client, management-ntp-client, management-log-forwarding	ノード管理、またはクラスタ管理	システムを対象としたこの管理ポリシーを使用して、システムSVMが所有するノードとクラスタを対象とした管理LIFを作成します。これらのLIFは、DNS、AD 、LDAP、またはNISサーバへのアウトバウンド接続に使用できるだけでなく、システム全体の代わりに実行されるアプリケーションをサポートするための追加の接続にも使用できます。ONTAP 9 12.1以降では、サービスを使用して、監査ログをリモートsyslogサーバに転送するために使用するLIFを制御でき `management-log-forwarding`ます。

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

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

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

データ**SVM**のサービス ポリシー

すべてのデータSVMに、そのSVMのLIFで使用できるサービス ポリシーが含まれています。

次の表は、ONTAP 9.11.1以降のデータSVMでLIFが使用可能な組み込みのポリシーの一覧です。その他のリリースのサービス ポリシーとその詳細を表示するには、次のコマンドを使用します。

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

ポリシー	付属サービス	同等のデータプロトコル	説明
default-management	management-https、management-http、management-ssh、management-dns-client, management-ad-client, management-ldap-client 、management-nis-client	なし	このSVMを対象とした管理ポリシーを使用して、データSVMが所有するSVM管理LIFを作成します。これらのLIFを使用して、SVM管理者にSSHまたはHTTPSアクセスを提供できます。必要に応じて、これらのLIFを外部DNS、AD、LDAP、またはNISサーバへのアウトバウンド接続に使用できます。
default-data-blocks（デフォルトデータブロック）	データコア、データ- iSCSI	iSCSI	ブロックベースのSANデータトラフィックを処理するLIFで使用されます。ONTAP 9.10.1以降、「default-data-blocks」ポリシーは廃止されました。代わりに「default-data-iscsi」サービス ポリシーを使用してください。

default-data-files の形式で指定します	data-filc-client, data-dns-server , data-fflexcache , data-cifs , data-nfs , management-dns-client、management-ad-client, management-ldap-client, management-nis-client	NFS 、 CIFS 、 fcache	default-data-filesポリシーを使用して、ファイルベースのデータプロトコルをサポートするNAS LIFを作成します。SVM内にLIFが1つしかない場合もあるため、このポリシーでは、LIFを外部のDNS、AD、LDAP、またはNISサーバへのアウトバウンド接続に使用できるようにします。これらの接続で管理LIFのみを使用する場合は、これらのサービスをこのポリシーから削除できます。
default-data-iscsi	データコア、データ - iSCSI	iSCSI	iSCSIデータトラフィックを処理するLIFで使用されます。
default-data-nvme-tcpです	データコア、データNVMe - TCP	nvme-tcpが表示されます	NVMe/FCデータトラフィックを処理するLIFで使用します。

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

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

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

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

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

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

- データプロトコルのリストを指定してLIFを作成すると、指定したデータプロトコルに相当するサービスポリシーがLIFに割り当てられます。
- 同等のサービスポリシーが存在しない場合は、カスタムサービスポリシーが作成されます。
- サービスポリシーやデータプロトコルのリストを指定せずにLIFを作成した場合、デフォルトでdefault-data-filesサービスポリシーがLIFに割り当てられます。

data-coreサービス

data-coreサービスを使用すると、LIFのロール（ONTAP 9で廃止）ではなくサービスポリシーを使用してLIFを管理するようにアップグレードされたクラスタで、以前にdataロールのLIFを使用していたコンポーネントが想定どおりに動作するようになります。

data-coreをサービスとして指定してもファイアウォールのポートは開かれませんが、データSVMのすべてのサービスポリシーにこのサービスを含める必要があります。たとえば、default-data-filesサービスポリシーには、デフォルトで次のサービスが含まれています。

- データコア
- データ- NFS
- データ- CIFS
- Data FlexCache

data-coreサービスは、LIFを使用するすべてのアプリケーションが想定どおりに動作するようにポリシーに含

める必要がありますが、残りの3つのサービスは必要に応じて削除できます。

クライアント側の**LIF**サービス

ONTAP 9 .10.1以降では、ONTAPは複数のアプリケーションに対してクライアント側のLIFサービスを提供します。これらのサービスは、各アプリケーションの代わりにアウトバウンド接続に使用するLIFを制御します。

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

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

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

LIFのロール（**ONTAP 9.5**以前）

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

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

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

LIFのセキュリティ

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

LIFフェイルオーバー

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

LIFのルーティング

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

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

LIFのリバランシング

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

LIFのプライマリトラフィックタイプ

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

LIFの管理

LIFのサービスポリシーを設定する

LIFのサービスポリシーを設定して、LIFを使用する単一のサービスまたは一連のサービスを指定できます。

LIFのサービスポリシーを作成します。

LIFのサービスポリシーを作成できます。1つ以上のLIFにサービスポリシーを割り当てることで、1つまたは一連のサービスのトラフィックをLIFで伝送できるようにすることができます。

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

タスクの内容

データSVMとシステムSVMの両方のデータトラフィックと管理トラフィックの管理に組み込みのサービスとサービスポリシーを使用できます。ほとんどのユースケースでは、カスタムサービスポリシーを作成するのではなく、組み込みのサービスポリシーを使用して問題を解決できます。

これらの組み込みのサービスポリシーは、必要に応じて変更できます。

手順

1. クラスタで使用可能なサービスを表示します。

```
network interface service show
```

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

次の追加データサービスと管理サービスを使用できます。

```
cluster1::> network interface service show

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

2. クラスタ内のサービスポリシーを表示します。

```
cluster1::> network interface service-policy show

Vserver   Policy                       Service: Allowed Addresses
--------- --------------------------
----------------------------------------
cluster1
          default-intercluster         intercluster-core: 0.0.0.0/0
                                       management-https: 0.0.0.0/0

          default-management           management-core: 0.0.0.0/0
                                       management-autosupport: 0.0.0.0/0
                                       management-ssh: 0.0.0.0/0
                                       management-https: 0.0.0.0/0

          default-route-announce       management-bgp: 0.0.0.0/0

Cluster
          default-cluster              cluster-core: 0.0.0.0/0

vs0
          default-data-blocks          data-core: 0.0.0.0/0
                                       data-iscsi: 0.0.0.0/0

          default-data-files           data-core: 0.0.0.0/0
                                       data-nfs: 0.0.0.0/0
                                       data-cifs: 0.0.0.0/0
                                       data-flexcache: 0.0.0.0/0

          default-management           data-core: 0.0.0.0/0
                                       management-ssh: 0.0.0.0/0
                                       management-https: 0.0.0.0/0

7 entries were displayed.
```

3. サービスポリシーを作成します。

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support.
Do you wish to continue? (y or n): y

cluster1::> network interface service-policy create -vserver <svm_name>
-policy <service_policy_name> -services <service_name> -allowed
-addresses <IP_address/mask,...>
```

- 「service_name」には、ポリシーに含めるサービスのリストを指定します。
- 「ip_address/mask」には、サービスポリシー内のサービスへのアクセスを許可するアドレスのサブネットマスクのリストを指定します。デフォルトでは、指定されたすべてのサービスが、すべてのサブネットからのトラフィックを許可するデフォルトの許可アドレスリスト0.0.0.0/0で追加されます。デフォルト以外の許可アドレスリストを指定すると、ポリシーを使用するLIFは、指定したマスクのいずれにも一致しないソースアドレスからの要求をすべてブロックするように設定されます。

  次の例は、_nfs_or_SMB_servicesを含むSVM用のデータサービスポリシーsvm1_data_policy__を作成する方法を示しています。

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support.
Do you wish to continue? (y or n): y

cluster1::> network interface service-policy create -vserver svm1
-policy svm1_data_policy -services data-nfs,data-cifs,data-core
```

次の例は、クラスタ間サービスポリシーを作成する方法を示しています。

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support.
Do you wish to continue? (y or n): y

cluster1::> network interface service-policy create -vserver cluster1
-policy intercluster1 -services intercluster-core
```

4. サービスポリシーが作成されたことを確認します。

```
cluster1::> network interface service-policy show
```

次の出力は、使用可能なサービスポリシーを示しています。

```
cluster1::> network interface service-policy show

Vserver   Policy                       Service: Allowed Addresses
--------- --------------------------
--------------------------------------
cluster1
          default-intercluster         intercluster-core: 0.0.0.0/0
                                       management-https: 0.0.0.0/0

          intercluster1                intercluster-core: 0.0.0.0/0

          default-management           management-core: 0.0.0.0/0
                                       management-autosupport: 0.0.0.0/0
                                       management-ssh: 0.0.0.0/0
                                       management-https: 0.0.0.0/0

          default-route-announce       management-bgp: 0.0.0.0/0

Cluster
          default-cluster              cluster-core: 0.0.0.0/0

vs0
          default-data-blocks          data-core: 0.0.0.0/0
                                       data-iscsi: 0.0.0.0/0

          default-data-files           data-core: 0.0.0.0/0
                                       data-nfs: 0.0.0.0/0
                                       data-cifs: 0.0.0.0/0
                                       data-flexcache: 0.0.0.0/0

          default-management           data-core: 0.0.0.0/0
                                       management-ssh: 0.0.0.0/0
                                       management-https: 0.0.0.0/0

          svm1_data_policy             data-core: 0.0.0.0/0
                                       data-nfs: 0.0.0.0/0
                                       data-cifs: 0.0.0.0/0

9 entries were displayed.
```

終了後

LIFの作成時または既存のLIFの変更時に、サービスポリシーを割り当てます。

LIFへのサービスポリシーの割り当て

LIFへのサービスポリシーの割り当ては、LIFの作成時または変更時に実行できます。サービスポリシーは、LIFで使用できる一連のサービスを定義します。

タスクの内容

管理SVMとデータSVMのLIFにサービスポリシーを割り当てることができます。

ステップ

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

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

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

サービスポリシーは、サービスポリシーの作成時に指定したものと同じSVM内のLIFでのみ使用できます。

例

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

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

LIFのサービスポリシーの管理用コマンド

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

開始する前に

アクティブなSnapMirror関係にあるLIFのサービスポリシーを変更すると、レプリケーションスケジュールが中断されます。LIFをクラスタ間から非クラスタ間（またはその逆）に変換した場合、変更はピアクラスタにレプリケートされません。LIFサービスポリシーの変更後にピアクラスタを更新するには、最初にこの処理を実行し `snapmirror abort`てレプリケーション関係を再同期するください。

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

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

LIFを作成する（ネットワークインターフェイス）

SVMは、1つ以上のネットワーク論理インターフェイス（LIF）を介してクライアントにデータを提供します。データへのアクセスに使用するポートにLIFを作成する必要があります。LIF（ネットワークインターフェイス）は、物理ポートまたは論理ポートに関連付けられたIPアドレスです。コンポーネントに障害が発生しても、LIFは別の物理ポートにフェイルオーバーまたは移行できるため、引き続きネットワークと通信できます。

ベストプラクティス

ONTAPに接続されたスイッチポートは、LIFの移行時の遅延を軽減するために、スパニングツリーエッジポートとして設定する必要があります。

開始する前に

- このタスクを実行するには、クラスタ管理者である必要があります。
- 基盤となる物理または論理ネットワークポートの管理ステータスがupに設定されている必要があります。
- サブネット名を使用してLIFのIPアドレスとネットワークマスク値を割り当てる場合は、そのサブネットがすでに存在している必要があります。

  サブネットには、同じレイヤ3サブネットに属するIPアドレスのプールが含まれています。作成するには、System Managerまたはコマンドを使用し `network subnet create`ます。

- LIFで処理されるトラフィックのタイプを指定するメカニズムが変更されました。ONTAP 9 .5以前では、LIFで処理するトラフィックのタイプをロールで指定していました。ONTAP 9 .6以降では、LIFで処理するトラフィックのタイプをサービスポリシーを使用して指定します。

タスクの内容

- NASプロトコルとSANプロトコルを同じLIFに割り当てることはできません。

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

  - SMBトラフィックを伝送するLIFを、ホームノードに自動的にリバートするように設定しないでください。この推奨事項は、Hyper-V over SMBまたはSQL Server over SMBでノンストップオペレーションを実現するソリューションをSMBサーバでホストする場合に必須です。
- 同じネットワークポートにIPv4とIPv6の両方のLIFを作成できます。
- SVMで使用するすべてのネームマッピングサービスとホスト名解決サービス（DNS、NIS、LDAP、Active Directoryなど）が、SVMのデータトラフィックを処理する少なくとも1つのLIFから到達可能でなければなりません。
- クラスタ内のノード間トラフィックを処理するLIFは、管理トラフィックを処理するLIFまたはデータトラフィックを処理するLIFと同じサブネット上には配置できません。
- 有効なフェイルオーバーターゲットのないLIFを作成すると、警告メッセージが表示されます。
- クラスタに多数のLIFがある場合は、クラスタでサポートされるLIFの容量を確認できます。
  - System Manager：ONTAP 9.12.0以降では、ネットワークインターフェイスグリッドのスループットを表示します。
  - CLI：コマンドを使用し、各ノードでサポートされるLIFの容量を `network interface capacity details show`コマンド（advanced権限レベル）で確認し `network interface capacity show`ます。
- ONTAP 9 .7以降では、同じサブネットにSVM用の他のLIFがすでに存在する場合は、LIFのホームポートを指定する必要はありません。ONTAPは、同じサブネットにすでに設定されている他のLIFと同じブロードキャストドメイン内の指定したホームノード上の任意のポートを自動的に選択します。

  ONTAP 9 .4以降では、FC-NVMeがサポートされます。FC-NVMe LIFを作成する場合は、次の点に注意してください。

  - LIFを作成するFCアダプタでNVMeプロトコルがサポートされている必要があります。
  - データLIFで使用できるデータプロトコルはFC-NVMeのみです。
- SANをサポートするStorage Virtual Machine（SVM）ごとに、管理トラフィックを処理するLIFを1つ設定する必要があります。
- NVMe LIFとネームスペースは同じノードでホストされている必要があります。
- データトラフィックを処理するNVMe LIFは、SVMごとに1つだけ設定できます。
- サブネットを使用してネットワークインターフェイスを作成すると、選択したサブネットから使用可能なIPアドレスがONTAPによって自動的に選択され、ネットワークインターフェイスに割り当てられます。サブネットが複数ある場合はサブネットを変更できますが、IPアドレスは変更できません。
- ネットワークインターフェイス用にSVMを作成（追加）するときに、既存のサブネットと同じ範囲のIPアドレスを指定することはできません。サブネットの競合エラーが表示されます。この問題は、SVM設定やクラスタ設定でクラスタ間ネットワーク インターフェイスを作成または変更する場合など、ネットワーク

インターフェイスの他のワークフローでも発生します。

- .10.1以降では、CLIコマンドにONTAP 9 `network interface` over RDMA構成のパラメータが含まれて`-rdma-protocols`います。ONTAP 9 12.1以降では、NFS over RDMA構成用のネットワークインターフェイスの作成がSystem Managerでサポートされています。詳細については、を参照してください NFS over RDMA用にLIFを設定します。
- ONTAP 9 .11.1以降では、オールフラッシュSANアレイ（ASA）プラットフォームでiSCSI LIFの自動フェイルオーバーを使用できます。

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

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

  "ASAプラットフォームでのiSCSI LIFフェイルオーバー"

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

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

System Manager

- System Managerを使用して、ネットワークインターフェイスを追加*

手順

1. Network > Overview > Network Interfaces *を選択します。
2. を選択します + Add 。
3. 次のいずれかのインターフェイスロールを選択します。
   a. データ
   b. Intercluster
   c. SVM Management
4. プロトコルを選択します。
   a. SMB/CIFS and NFS
   b. iSCSI
   c. FC
   d. NVMe/FC
   e. NVMe / TCP
5. LIFに名前を付けるか、前の選択で生成した名前をそのまま使用します。
6. ホームノードをそのまま使用するか、ドロップダウンを使用して選択します。
7. 選択したSVMのIPspaceで少なくとも1つのサブネットが設定されている場合は、サブネットのドロップダウンが表示されます。
   a. サブネットを選択した場合は、ドロップダウンからサブネットを選択します。
   b. サブネットなしで続行すると、ブロードキャストドメインのドロップダウンが表示されます。
      i. IPアドレスを指定します。IPアドレスが使用中の場合は、警告メッセージが表示されます。
      ii. サブネット マスクを指定します。
8. ホーム ポートをブロードキャスト ドメインから自動で選択するか（推奨）、ドロップダウン メニューから選択します。ホーム ポートのオプションは、ブロードキャスト ドメインとサブネットの選択に基づいて表示されます。
9. ネットワーク インターフェイスを保存します。

CLI

- CLIを使用してLIFを作成してください*

手順

1. LIFに使用するブロードキャストドメインポートを決定します。

```
network port broadcast-domain show -ipspace ipspace1
```

```
IPspace     Broadcast                         Update
Name        Domain name   MTU   Port List     Status Details
ipspace1
            default       1500
                                node1:e0d     complete
                                node1:e0e     complete
                                node2:e0d     complete
                                node2:e0e     complete
```

2. LIFに使用するサブネットに未使用のIPアドレスが十分にあることを確認します。

   `network subnet show -ipspace ipspace1`

3. データへのアクセスに使用するポートに1つ以上のLIFを作成します。

   NetAppでは、データSVMのすべてのLIFに対してサブネットオブジェクトを作成することを推奨しています。これは特にMetroCluster構成で重要です。各サブネットオブジェクトにはブロードキャストドメインが関連付けられているため、サブネットオブジェクトを使用してONTAPがデスティネーションクラスタのフェイルオーバーターゲットを決定できます。手順については、を参照してください"サブネットを作成する"。

```
network interface create -vserver _SVM_name_ -lif _lif_name_
-service-policy _service_policy_name_ -home-node _node_name_ -home
-port port_name {-address _IP_address_ - netmask _Netmask_value_ |
-subnet-name _subnet_name_} -firewall- policy _policy_ -auto-revert
{true|false}
```

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

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

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

- `-auto-revert`起動時、管理データベースのステータスが変わったとき、ネットワーク接続が確立されたときなどの状況で、データLIFがホームノードに自動的にリバートされるかどうかを指定できます。デフォルトの設定はです `false`が、環境内のネットワーク管理ポリシーに応じてに設定できます `true`。
- `-service-policy`ONTAP 9 5以降では、オプションを使用してLIFのサービスポリシーを割り当てることができます `-service-policy`。LIFにサービスポリシーを指定すると、そのポリシーを使用してLIFのデフォルトロール、フェイルオーバーポリシー、およびデータプロトコルのリストが作成されます。.5では、クラスタ間およびONTAP 9ピアサービスでのみサービスポリシーがサポートされます。ONTAP 9 .6では、複数のデータサービスおよび管理サービスのサービスポリシーを作成できます。
- `-data-protocol`FCPまたはNVMe/FCプロトコルをサポートするLIFを作成できます。IP LIFを作成する場合、このオプションは必要ありません。

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

   a. network ndp prefix showコマンドを使用して、さまざまなインターフェイスで学習されたRAプレフィックスのリストを表示します。

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

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

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

   を生成するには `id`、ランダムな64ビット16進数を選択します。

5. LIFインターフェイスの設定が正しいことを確認します。

   ```
   network interface show -vserver vs1
   ```

   ```
             Logical    Status     Network          Current   Current Is
   Vserver   Interface  Admin/Oper Address/Mask     Node      Port
   Home
   --------- ---------- ---------- ---------------- --------- -------
   ----
   vs1
              lif1       up/up      10.0.0.128/24   node1     e0d
   true
   ```

6. フェイルオーバーグループの設定が適切であることを確認します。

   ```
   network interface show -failover -vserver vs1
   ```

```
          Logical    Home       Failover        Failover
Vserver   interface  Node:Port  Policy          Group
--------- ---------- ---------  ---------       --------
vs1
          lif1       node1:e0d  system-defined  ipspace1
Failover Targets: node1:e0d, node1:e0e, node2:e0d, node2:e0e
```

7. 設定したIPアドレスに到達できることを確認します。

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

例

次のコマンドは、LIFを作成し、パラメータと `-netmask`パラメータを使用してIPアドレスとネットワークマスク値を指定し `-address`ます。

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

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

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

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

```
network interface create -vserver vs1.example.com -lif datalif1 -data
-protocol nvme-fc -home-node node-4 -home-port 1c -address 192.0.2.145
-netmask 255.255.255.0 -auto-revert true
```

LIFを変更する

LIFの属性は変更できます。これには、ホームノードや現在のノード、管理ステータス、IPアドレス、ネットマスク、フェイルオーバーポリシー、ファイアウォールポリシー、サービスポリシーなどがあります。LIFのアドレスファミリーをIPv4からIPv6に変更することもできます。

タスクの内容

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

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

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

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

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

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

- ONTAP 9 5以降では、LIFに関連付けられているサービスポリシーを変更できます。
- ONTAP 9 .11.1以降では、All-Flash SAN Array（ASA）プラットフォームでiSCSI LIFの自動フェイルオーバーを使用できます。

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

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

System Manager

- ONTAP 9.12.0以降では、System Managerを使用してネットワークインターフェイス*を編集できます

手順

1. Network > Overview > Network Interfaces *を選択します。
2. 変更するネットワークインターフェイスの横にある*>[編集]*を選択します ⋮ 。
3. 1つ以上のネットワークインターフェイス設定を変更します。詳細については、を参照してください "LIFの作成"。
4. 変更を保存します。

CLI

- LIFの変更にはCLIを使用してください*

手順

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

   次の例は、datalif2というLIFのIPアドレスとネットワークマスクを、サブネットclient1_subのIPアドレスとネットワークマスク値を使用して変更する方法を示しています。

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

   次の例は、LIFのサービスポリシーを変更する方法を示しています。

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

2. IPアドレスに到達できることを確認します。

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

LIFを移行する

ポートで障害が発生した場合やメンテナンスが必要な場合は、同じノードの別のポートやクラスタ内の別のノードにLIFを移行しなければならないことがあります。LIFの移行はLIFのフェイルオーバーと似ていますが、LIFの移行は手動操作です。一方、LIFのフェイルオーバーは、LIFの現在のネットワークポートでリンク障害が発生した場合にLIFを

自動的に移行する処理です。

開始する前に

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

タスクの内容

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

  この問題を回避するには、遅延が発生しないNFSv4.1を使用します。

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

  iSCSI LIFの移行は、ホームノードまたはHAパートナーのポートに限定されます。

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

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

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

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

System Manager

- System Managerを使用して、ネットワーク・インターフェイス*を移行します

手順

1. Network > Overview > Network Interfaces *を選択します。
2. 変更するネットワークインターフェイスの横にある*> Migrate *を選択します ⋮ 。

   iSCSI LIFの場合、*[インターフェイスの移行]*ダイアログボックスで、HAパートナーのデスティネーションノードとポートを選択します。

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

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

CLI

- LIFの移行にはCLIを使用してください*

ステップ

特定のLIFを移行するかすべてのLIFを移行するかに応じて、該当する処理を実行します。

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

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

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

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

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

LIFをホームポートにリバートします。

別のポートにフェイルオーバーまたは移行されたLIFを、手動または自動でホームポートにリバートできます。特定のLIFのホームポートを使用できない場合、LIFは現在のポートに残り、リバートされません。

タスクの内容

- 自動リバートオプションを設定する前にLIFのホームポートをup状態にした場合、LIFはホームポートに戻りません。
- 「auto-revert」オプションの値をtrueに設定しないかぎり、LIFは自動的にリバートされません。
- LIFをホームポートにリバートするには、「auto-revert」オプションを有効にする必要があります。

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

System Manager

- System Managerを使用して、ネットワークインターフェイスをホームポートに戻します。*

手順

1. Network > Overview > Network Interfaces *を選択します。
2. 変更するネットワークインターフェイスの横にある*> Revert *を選択します ⋮ 。
3. ネットワークインターフェイスをホームポートに戻すには、* Revert *を選択します。

CLI

- CLIを使用してLIFをホームポート*にリバートします

ステップ

LIFをホームポートに手動または自動でリバートします。

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

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

クラスタネットワークがスイッチにケーブル接続されているが、Cluster IPspaceに設定されているすべてのポートがCluster IPspaceに設定されている他のポートに到達できない場合、クラスタを作成できません。

タスクの内容

スイッチクラスタで、クラスタネットワークインターフェイス（LIF）が間違ったポートに設定されている場合、またはクラスタポートが間違ったネットワークに接続されている場合、 `cluster create`コマンドが次のエ

ラーで失敗することがあります。

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

コマンドの結果では `network port show`、クラスタLIFが設定されたポートに接続されているために、複数のポートがクラスタIPspaceに追加されたと表示されることがあります。ただし、コマンドの結果から、`network port `reachability show -detail`相互に接続されていないポートが特定されます。

クラスタLIFが設定されている他のポートに到達できないポートに設定されたクラスタLIFをリカバリするには、次の手順を実行します。

手順

1. クラスタLIFのホームポートを正しいポートにリセットします。

```
network port modify -home-port
```

2. クラスタLIFが設定されていないポートをクラスタブロードキャストドメインから削除します。

```
network port broadcast-domain remove-ports
```

3. クラスタを作成します。

```
cluster create
```

結果

クラスタの作成が完了すると、正しい設定が検出され、正しいブロードキャストドメインにポートが配置されます。

LIFを削除する

不要になったネットワークインターフェイス（LIF）は削除できます。

開始する前に

使用中のLIFは削除できません。

手順

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

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

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

削除の対象	入力するコマンド
特定の LIF	`network interface delete -vserver vserver_name -lif lif_name`
すべての LIFs	`network interface delete -vserver vserver_name -lif *`

次のコマンドは、mgmtlif2というLIFを削除します。

```
network interface delete -vserver vs1 -lif mgmtlif2
```

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

ONTAP仮想IP（VIP）LIFの設定

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

タスクの内容

VIPデータLIFは、どのサブネットにも属さず、同じIPspace内のBGP LIFをホストするすべてのポートから到達可能なLIFです。VIPデータLIFを使用すると、ホストは個 々 のネットワークインターフェイスに依存しなくなります。複数の物理アダプタがデータトラフィックを伝送するため、すべての負荷が単一のアダプタおよび関連するサブネットに集中することはありません。VIPデータLIFの存在は、ルーティングプロトコルであるBorder Gateway Protocol（BGP）を使用してピアルータにアドバタイズされます。

VIPデータLIFには次の利点があります。

- ブロードキャストドメインやサブネットをまたいで LIF を移動できます。各 VIP データ LIF の現在の場所が BGP を通じてルータに通知されるため、 VIP データ LIF をネットワークのどのサブネットにもフェイルオーバーできます。
- アグリゲートスループット： VIP データ LIF は、同時に複数のサブネットまたはポートに対してデータを送受信できるため、個々のポートの帯域幅を超えるアグリゲートスループットをサポートできます。

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

VIP LIFを作成する前に、BGPを設定する必要があります。BGPは、VIP LIFの存在をピアルータに通知するためのルーティングプロトコルです。

ONTAP 9 .9.1以降では、BGPピアグループを使用したデフォルトルート自動化がオプションで提供され、設定が簡素化されます。

ONTAPには、BGPピアが同じサブネット上にある場合に、BGPピアをネクストホップルータとして使用して

デフォルトルートを学習する簡単な方法があります。この機能を使用するには、属性をに `true`設定し `-use-peer-as-next-hop`ます。デフォルトでは、この属性はです `false`。

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

開始する前に

設定されたAutonomous System Number（ASN；自律システム番号）のBGP接続をBGP LIFから受け入れるようにピアルータを設定する必要があります。

> ONTAPはルータからの着信ルートアナウンスを処理しません。したがって、クラスタにルートアップデートを送信しないようにピアルータを設定する必要があります。これにより、ピアとの通信が完全に機能するようになるまでの時間が短縮され、ONTAP内の内部メモリ使用量が削減されます。

タスクの内容

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

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

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

コマンドと `network bgp peer-group modify`コマンドに次のフィールドが追加されまし `network bgp peer-group create`た。

- `-md5-enabled <true/false>`
- `-md5-secret <md5 secret in string or hex format>`

これらのパラメータを使用すると、セキュリティを強化するためにMD5シグニチャを使用してBGPピアグループを設定できます。MD5認証の使用には、次の要件が適用されます。

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

ONTAP 9 .9.1以降では、次のフィールドが追加されました。

- `-asn`OR `-peer-asn` (4バイトの値)属性自体は新しいものではありませんが、現在は4バイトの整数を使用しています。
- `-med`

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

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

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

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

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

ONTAPは上記のBGP属性をサポートしていますが、ルータはこれらの属性を尊重する必要はありません。NetAppでは、ルータでサポートされているアトリビュートを確認し、それに応じてBGPピアグループを設定することを強く推奨します。詳細については、ルータが提供するBGPのマニュアルを参照してください。

手順

1. advanced権限レベルにログインします。

   ```
   set -privilege advanced
   ```

2. オプション：次のいずれかの操作を実行して、クラスタの BGP 設定を作成するか、デフォルトの BGP 設定を変更します。

   a. BGP設定を作成します。

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

   - `-routerid`パラメータは、ASドメイン内で一意である必要があるドット付き10進32ビット値を受け入れます。NetAppでは、一意性が保証されるノード管理IP（v4）アドレスを使用することを推奨しています `<router_id>`。
   - ONTAP BGPは32ビットASN番号をサポートしますが、サポートされるのは標準10進表記のみです。プライベートASNでは4259840001ではなく65000.1などのドット付きASN表記はサポートされません。

   2バイトASNのサンプル：

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

4バイトASNのサンプル：

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

a. デフォルトのBGP設定を変更します。

```
network bgp defaults modify -asn <asn_number> -holdtime <hold_time>
network bgp defaults modify -asn 65502 -holdtime 60
```

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

> ONTAPでサポートされるグローバル、 `<hold_time>`、、およびは `<router_id>`1つだけです。これは、 `<asn_number>`複数のIPspaceに対してBGPを設定する場合でも同様です。BGPとすべてのIPルーティング情報は、1つのIPspace内で完全に分離されます。IPspaceは、Virtual Routing and Forwarding（VRF；仮想ルーティング/転送）インスタンスに相当します。

3. システムSVM用のBGP LIFを作成します。

デフォルトIPspaceの場合、SVM名はクラスタ名です。追加のIPspaceの場合、SVM名はIPspace名と同じになります。

```
network interface create -vserver <system_svm> -lif <lif_name> -service
-policy default-route-announce -home-node <home_node> -home-port
<home_port> -address <ip_address> -netmask <netmask>
```

BGP LIFのサービスポリシー、または「management-bgp」サービスを含む任意のカスタムサービスポリシーを使用できます `default-route-announce`。

```
network interface create -vserver cluster1 -lif bgp1 -service-policy
default-route-announce -home-node cluster1-01 -home-port e0c -address
10.10.10.100 -netmask 255.255.255.0
```

4. リモートピアルータとのBGPセッションを確立するために使用するBGPピアグループを作成し、ピアルータにアドバタイズされるVIPルート情報を設定します。

例 1 ：自動デフォルトルートのないピアグループを作成する

この場合、管理者はBGPピアへのスタティックルートを作成する必要があります。

```
network bgp peer-group create -peer-group <group_name> -ipspace
<ipspace_name> -bgp-lif <bgp_lif> -peer-address <peer-router_ip_address>
-peer-asn <peer_asn_number> {-route-preference <integer>} {-asn-prepend-
type <ASN_prepend_type>} {-asn-prepend-count <integer>} {-med <integer>}
{-community BGP community list <0-65535>:<0-65535>}
```

```
network bgp peer-group create -peer-group group1 -ipspace Default -bgp
-lif bgp1 -peer-address 10.10.10.1 -peer-asn 65503 -route-preference 100
-asn-prepend-type local-asn -asn-prepend-count 2 -med 100 -community
9000:900,8000:800
```

例 2 ：自動デフォルトルートを使用してピアグループを作成する

```
network bgp peer-group create -peer-group <group_name> -ipspace
<ipspace_name> -bgp-lif <bgp_lif> -peer-address <peer-router_ip_address>
-peer-asn <peer_asn_number> {-use-peer-as-next-hop true} {-route-
preference <integer>} {-asn-prepend-type <ASN_prepend_type>} {-asn-
prepend-count <integer>} {-med <integer>} {-community BGP community list
<0-65535>:<0-65535>}
```

```
network bgp peer-group create -peer-group group1 -ipspace Default -bgp
-lif bgp1 -peer-address 10.10.10.1 -peer-asn 65503 -use-peer-as-next-hop
true -route-preference 100 -asn-prepend-type local-asn -asn-prepend
-count 2 -med 100 -community 9000:900,8000:800
```

例3：MD5を有効にしてピアグループを作成する

a. IPSecを有効にします。

   ```
   security ipsec config modify -is-enabled true
   ```

b. MD5をイネーブルにしてBGPピアグループを作成します。

   ```
   network bgp peer-group create -ipspace Default -peer-group
   <group_name> -bgp-lif bgp_lif -peer-address <peer_router_ip_address>
   {-md5-enabled true} {-md5-secret <md5 secret in string or hex format>}
   ```

   16進キーを使用した例：

```
network bgp peer-group create -ipspace Default -peer-group peer1 -bgp
-lif bgp_lif1 -peer-address 10.1.1.100 -md5-enabled true -md5-secret
0x7465737420736563726574
```

文字列を使用した例：

```
network bgp peer-group create -ipspace Default -peer-group peer1 -bgp
-lif bgp_lif1 -peer-address 10.1.1.100 -md5-enabled true -md5-secret "test
secret"
```

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

仮想IP（VIP）データLIFを作成する

VIPデータLIFの存在は、ルーティングプロトコルであるBorder Gateway Protocol（BGP）を使用してピアルータにアドバタイズされます。

開始する前に

- BGPピアグループをセットアップし、LIFを作成するSVMのBGPセッションをアクティブにしておく必要があります。
- SVMの発信VIPトラフィック用に、BGPルータまたはBGP LIFのサブネット内のその他のルータへの静的ルートを作成する必要があります。
- 発信VIPトラフィックが使用可能なすべてのルートを利用できるように、マルチパスルーティングをオンにする必要があります。

  マルチパスルーティングがイネーブルになっていない場合、すべての発信VIPトラフィックは1つのインターフェイスから送信されます。

手順

1. VIPデータLIFを作成します。

```
network interface create -vserver <svm_name> -lif <lif_name> -role data
-data-protocol
{nfs|cifs|iscsi|fcache|none|fc-nvme} -home-node <home_node> -address
<ip_address> -is-vip true -failover-policy broadcast-domain-wide
```

コマンドでホームポートを指定しない場合は、VIPポートが自動的に選択され `network interface create`ます。

デフォルトでは、VIPデータLIFは、システムによってIPspaceごとに作成される「vip」という名前のブロ

ードキャストドメインに属します。VIPブロードキャストドメインは変更できません。

VIPデータLIFは、IPspaceのBGP LIFをホストしているすべてのポートで同時に到達できます。ローカルノードにVIPのSVMに対するアクティブなBGPセッションがない場合、VIPデータLIFは、そのSVMに対してBGPセッションが確立されているノードの次のVIPポートにフェイルオーバーします。

2. VIPデータLIFのSVMに対してBGPセッションのステータスがupになっていることを確認します。

```
network bgp vserver-status show

Node        Vserver  bgp status
          ----------  -------- ---------
          node1       vs1      up
```

あるノードのSVMのBGPステータスがの場合、 `down`VIPデータLIFは、そのSVMのBGPステータスがupになっている別のノードにフェイルオーバーします。すべてのノードでBGPステータスが設定されている場合は `down`、VIPデータLIFをどこでもホストできず、LIFステータスがdownになります。

BGPの管理用コマンド

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

BGP設定を管理します。

状況	使用するコマンド
BGP設定を作成する	`network bgp config create`
BGP設定を変更する	`network bgp config modify`
BGP設定を削除する	`network bgp config delete`
BGP設定を表示する	`network bgp config show`
VIP LIFのSVMに対するBGPステータスを表示する	`network bgp vserver-status show`

BGPのデフォルト値の管理

状況	使用するコマンド
BGPのデフォルト値を変更する	`network bgp defaults modify`
BGPのデフォルト値を表示する	`network bgp defaults show`

BGPピアグループを管理します。

状況	使用するコマンド
BGPピアグループを作成する	`network bgp peer-group create`
BGPピアグループを変更する	`network bgp peer-group modify`

BGPピア グループを削除する	`network bgp peer-group delete`
BGPピア グループの情報を表示する	`network bgp peer-group show`
BGPピア グループの名前を変更する	`network bgp peer-group rename`

MD5を使用した**BGP**ピアグループの管理

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

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

状況	使用するコマンド
既存のBGPピアグループでMD5をイネーブルにする	`network bgp peer-group modify -ipspace Default -peer-group <group_name> -bgp -lif <bgp_lif> -peer-address <peer_router_ip_address> -md5-enabled true -md5-secret <md5 secret in string or hex format>`
既存のBGPピアグループでMD5をディセーブルにする	`network bgp peer-group modify -ipspace Default -peer-group <group_name> -bgp -lif <bgp_lif> -md5-enabled false`

関連情報

"ONTAPコマンド リファレンス"

著作権に関する情報

商標に関する情報