

# NSX トラブルシューティング ガイド

Update 8

更新日：2020 年 2 月 21 日

VMware NSX Data Center for vSphere 6.3



vmware®

最新の技術ドキュメントは、VMware の Web サイト (<https://docs.vmware.com/jp/>) でご確認ください。このドキュメントに関するご意見および感想は、[docfeedback@vmware.com](mailto:docfeedback@vmware.com) までお送りください。

**VMware, Inc.**  
3401 Hillview Ave.  
Palo Alto, CA 94304  
[www.vmware.com](http://www.vmware.com)

**ヴィエムウェア株式会社**  
105-0013 東京都港区浜松町 1-30-5  
浜松町スクエア 13F  
[www.vmware.com/jp](http://www.vmware.com/jp)

Copyright © 2010 - 2020 VMware, Inc. All rights reserved. [著作権および商標情報](#)。

# 目次

## 1 NSX トラブルシューティング ガイド 6

トラブルシューティングの一般的なガイドライン 6

NSX ダッシュボードの使用 7

NSX コマンド ライン クイック リファレンス 10

NSX ホストの健全性チェック 20

## 2 NSX インフラストラクチャのトラブルシューティング 22

ホストの準備 22

ホストの準備のアーキテクチャについて 27

ホストの準備のサービス デプロイ ワークフロー 31

サード パーティ サービスのサービス デプロイ ワークフロー 33

通信チャネルの健全性の確認 35

インストール ステータスに「準備ができていません」と表示される 37

サービスが応答しない 37

「OVF/VIB not accessible」エラーでサービスのデプロイが失敗する 39

[解決] オプションを使用して解決できない問題 40

vSphere ESX Agent Manager (EAM) について 41

NSX Manager の問題のトラブルシューティング 41

NSX Manager と vCenter Server の接続 44

セカンダリ NSX Manager が移行モードで止まる 46

NSX SSO Lookup Service の設定の失敗 47

論理ネットワークの準備 : VXLAN 転送 50

VXLAN VMkernel NIC が同期されない 52

VXLAN チーミング ポリシーと MTU 設定の変更 53

論理スイッチのポート グループが同期されない問題 55

## 3 NSX のルーティングのトラブルシューティング 57

分散論理ルーターの理解 58

上位レベルの分散論理ルーター パケット フロー 59

分散論理ルーター ARP の解決プロセス 60

Edge Services Gateway によって提供されるルーティングの理解 62

ECMP パケット フロー 62

NSX のルーティングの前提条件と考慮事項 64

分散論理ルーター (DLR) と Edge Services Gateway (ESG) のユーザー インターフェイス 67

NSX のルーティング用ユーザー インターフェイス 67

NSX Edge ユーザー インターフェイス 68

新しい NSX Edge (分散論理ルーター) 69

Edge Service Gateway (ESG) と分散論理ルーターの相違点 73

## 一般的な ESG および分散論理ルーター ユーザー インターフェイスの操作 73

Syslog 設定 74

スタティック ルート 75

ルート再配分 76

## NSX のルーティングのトラブルシューティング 77

NSX のルーティング CLI 77

ルーティングの概要 80

サンプル ルート トポロジを使用した分散論理ルーター状態の確認 81

分散論理ルーター (DLR) と関連するホスト コンポーネントの図解 88

分散ルーティング サブシステムのアーキテクチャ 91

NSX のルーティング サブシステム コンポーネント 95

NSX のルーティング制御プレーン CLI 97

NSX のルーティング サブシステムの障害の状況と影響 100

ルーティングに関連する NSX ログ 103

一般的な障害のシナリオと解決方法 105

トラブルシューティング データの収集 106

## 4 NSX Edge のトラブルシューティング 110

Edge ファイアウォールでパケットがドロップする問題 114

Edge ルーティング接続の問題 118

NSX Manager と Edge の通信の問題 120

メッセージ バスのデバッグ 121

Edge の診断とリカバリ 123

## 5 ファイアウォールのトラブルシューティング 126

分散ファイアウォールについて 126

分散ファイアウォールの CLI コマンド 127

分散ファイアウォールのトラブルシューティング 130

Identity Firewall 136

## 6 ロード バランシングのトラブルシューティング 139

シナリオ: ワンアーム ロード バランサの設定 139

ロード バランサのトラブルシューティングに関するフローチャート 145

ロード バランサ設定の確認とユーザー インターフェイスを使用したトラブルシューティング 146

CLI を使用したロード バランサのトラブルシューティング 157

一般的なロード バランサの問題 168

## 7 Virtual Private Network (VPN) のトラブルシューティング 173

L2 VPN 173

L2 VPN の一般的な設定の問題 173

ルーピングを軽減するための L2VPN のオプション 176

CLI を使用したトラブルシューティング	178
SSL VPN	180
SSL VPN Web ポータルを開くことができない	180
SSL VPN-Plus : インストールの失敗	181
SSL VPN-Plus : 通信の問題	184
SSL VPN-Plus : 認証の問題	187
SSL VPN-Plus クライアントが応答しない	188
基本的なログ分析	188
IPsec VPN	189
成功するネゴシエーション (フェーズ 1 とフェーズ 2 共)	189
フェーズ 1 ポリシーがマッチしない	190
フェーズ 2 がマッチしない	191
PFS 不一致	192
PSK が一致しない	194
成功するネゴシエーションのためのパケットのキャプチャ	194

## 8 NSX Controller のトラブルシューティング 201

コントローラ クラスター アーキテクチャについて	201
NSX Controller のデプロイに関する問題	204
ディスク遅延のトラブルシューティング	208
ディスク遅延アラートの表示	208
ディスク遅延の問題	210
NSX Controller クラスターの障害	211
方法 1 : 破損したコントローラを削除して新しいコントローラを再展開する	213
方法 2 : NSX Controller クラスターを再展開する	216
ファントム コントローラ	216
NSX Controller が切断された	218
制御プレーン エージェント (netcpa) の問題	219

## 9 ゲスト イントロスペクションのトラブルシューティング 223

ゲスト イントロスペクションのアーキテクチャ	223
ゲスト イントロスペクションのログ	224
ESX ゲスト イントロスペクション モジュール (MUX) のログ	225
ゲスト イントロスペクション シン エージェントのログ	228
ゲスト イントロスペクション EPSecLib とサービス仮想マシンのログ	230
ゲスト イントロスペクション環境とワークロードの詳細情報の収集	232
Linux または Windows でのシン エージェントのトラブルシューティング	233
ESX ゲスト イントロスペクション モジュール (MUX) のトラブルシューティング	236
EPSecLib のトラブルシューティング	238

# NSX トラブルシューティング ガイド

# 1

『NSX トラブルシューティング ガイド』では、NSX Manager のユーザー インターフェイス、vSphere Web Client、他の NSX コンポーネントを使用して、VMware NSX<sup>®</sup> for vSphere<sup>®</sup> システムの監視とトラブルシューティングを行う方法について説明します。

## 対象読者

本書は、VMware vCenter Server 環境で NSX のトラブルシューティングを行うユーザーを対象としています。本書に記載されている情報は、システム管理者としての経験があり、仮想マシン テクノロジーおよび仮想データセンターの操作に詳しい方を対象としています。本書は、VMware ESXi、vCenter Server、vSphere Web Client を含む VMware vSphere についての知識があることを前提としています。

## VMware の技術ドキュメントの用語集

VMware は、新しい用語を集めた用語集を提供しています。当社の技術ドキュメントで使用されている用語の定義については、<http://www.vmware.com/support/pubs> をご覧ください。

この章には、次のトピックが含まれています。

- [トラブルシューティングの一般的なガイドライン](#)

## トラブルシューティングの一般的なガイドライン

このトピックでは、一般的なガイドラインに従って NSX for vSphere で問題を解決する方法について説明します。

- 1 [NSX ダッシュボードの使用](#)に移動し、コンポーネントにエラーや警告が発生しているかどうか確認します。
- 2 プライマリ NSX Manager の [監視 (Monitor)] タブに移動し、システム イベントがトリガされているかどうか確認します。システム イベントとアラームの詳細については、『NSX のログ作成とシステム イベント』を参照してください。
- 3 GET `api/2.0/services/systemalarms` API を使用して、NSX オブジェクトのアラームを確認します。API の詳細については、『NSX API ガイド』を参照してください。
- 4 NSX トラブルシューティング ガイド の説明に従って、問題を解決します。
- 5 問題が解決しない場合は、テクニカル サポート ログをダウンロードし、VMware サポートにお問い合わせください。「[How to file a Support Request in My VMware](#)」を参照してください。ログのダウンロード方法の詳細については、『NSX のログ作成とシステム イベント』を参照してください。

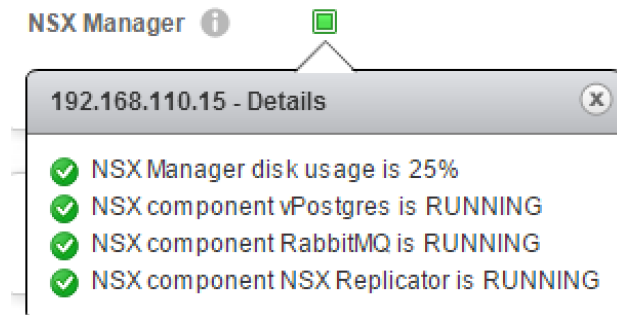
## NSX ダッシュボードの使用

NSX ダッシュボードでは、NSX コンポーネントの全体的な健全性をまとめて表示できます。NSX ダッシュボードを使用すると、NSX Manager、コントローラ、論理スイッチ、ホストの準備、サービスのデプロイ、バックアップ、Edge 通知など、異なる NSX コンポーネントのステータスを表示し、トラブルシューティングを容易に行うことができます。

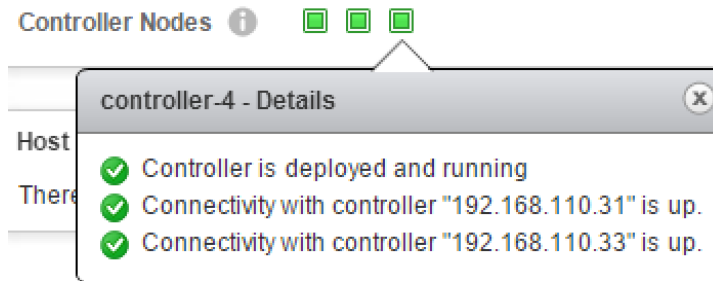
- 1 vSphere Web Client にログインします。
- 2 [Networking and Security (Networking & Security)] をクリックし、[ダッシュボード (Dashboard)] をクリックします。[ダッシュボード] ページが表示されます。
- 3 Cross-vCenter NSX 環境で、NSX Manager とプライマリ ロールまたはセカンダリ ロールを選択します。

ダッシュボードには、次の情報が表示されます。

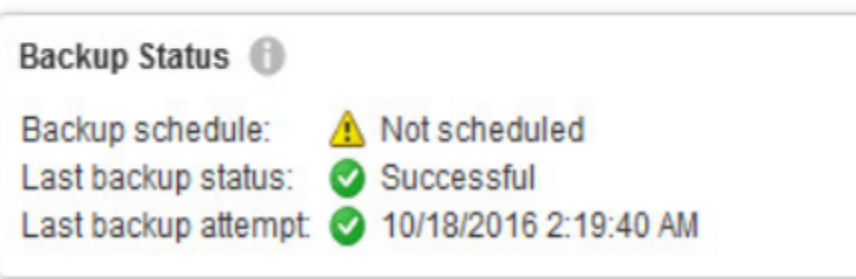
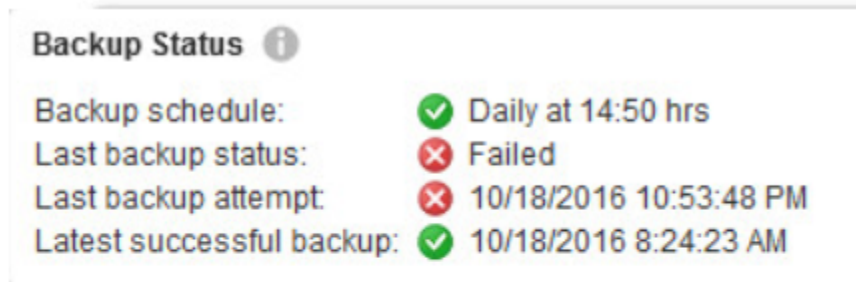
- NSX インフラストラクチャ： 次のサービスの NSX Manager コンポーネントのステータスを監視します。
  - データベース サービス (vPostgres)
  - メッセージ バス サービス (RabbitMQ)
  - レプリケータ サービス： Cross-vCenter NSX が有効な場合、レプリケーション エラーも監視します。
  - NSX Manager のディスク使用率：
    - 黄色は、ディスクの使用率が 80% 以上であることを示します。
    - 赤は、ディスクの使用率が 90% 以上であることを示します。



- NSX インフラストラクチャ： NSX Controller のステータス
  - コントローラ ノードのステータス（稼動/停止/実行中/デプロイ中/削除中/失敗/不明）
  - コントローラ ピアの接続ステータスが表示されます。コントローラが停止し、赤色で表示されている場合、ピア コントローラは黄色で表示されます。
  - コントローラ仮想マシンのステータス（パワーオフ/削除済み）
  - コントローラのディスク遅延アラート



- NSX Manager のバックアップ ステータス :
  - バックアップ スケジュール
  - 最新のバックアップ ステータス (失敗/成功/日時指定のスケジュールなし)
  - 実行した最新のバックアップ (日時と詳細付き)
  - 成功した最新のバックアップ (日時と詳細付き)



- NSX インフラストラクチャ : 次のサービスのホストのステータスを監視します。
  - デプロイ関連
    - インストールに失敗した状態のクラスタ数
    - アップグレードが必要なクラスタ数
    - インストールが進行中のクラスタ数
    - 準備未完了のクラスタ数
  - ファイアウォール
    - ファイアウォールが無効のクラスタ数



- ファイアウォールのステータスが黄色/赤色のクラスタ数：
  - 黄色は、いずれかのクラスタで分散ファイアウォールが無効になっていることを示します。
  - 赤色は、分散ファイアウォールが、いずれかのホストまたはクラスタにインストールできなかったことを示します。
- VXLAN
  - VXLAN が設定されていないクラスタ数
  - VXLAN のステータスが緑色/黄色/赤色のクラスタ数：
    - 緑色は、機能が正しく設定されていることを示します。
    - 黄色は、VXLAN 設定中にビジー状態であることを示します。
    - 赤色（エラー）は、VTEP の作成が失敗したとき、VTEP で IP アドレスが見つからなかったとき、VTEP に *LinkLocal* IP アドレスが割り当てられたときなどの状態を示します。
- NSX インフラストラクチャ：サービスのデプロイ ステータス
  - デプロイの失敗：失敗したデプロイのインストール ステータス
  - サービスのステータス：失敗したすべてのサービス
- NSX インフラストラクチャ：NSX Edge の通知

Edge 通知ダッシュボードは、特定のサービスについてのアクティブなアラームを示します。これは、次にリストする重要イベントを監視し、問題が解決されるまでそれらを追跡します。アラームは、リカバリー イベントが報告されたとき、または Edge が強制同期、再デプロイ、アップグレードされたときに自動的に解決されます。

  - ロード バランサ（Edge ロード バランサ サーバのステータス）
    - Edge ロード バランサのバックエンド サーバが停止
    - Edge ロード バランサのバックエンド サーバの警告ステータス
  - VPN（IPSec トンネル/IPSec チャネルのステータス）
    - Edge IPSec チャネルが停止
    - Edge IPSec トンネルが停止
  - アプライアンス（Edge 仮想マシン、Edge ゲートウェイ、Edge ファイル システム、NSX Manager、Edge サービス ゲートウェイのレポート ステータス）：
    - Edge Services Gateway に健全性チェックのパルスがない
    - Edge 仮想マシンがパワーオフされた
    - Edge 仮想マシンに健全性チェックのパルスがない
    - NSX Edge から不良状態がレポートされている
    - NSX Manager から Edge サービス ゲートウェイが不良状態であることがレポートされている
    - Edge 仮想マシンが vCenter Server のインベントリにない

- 高可用性 (HA) のスプリット ブレインが検出された

**注：** ロード バランサと VPN のアラームは、設定を更新しても自動的にクリアされません。問題が解決された場合は、API で `alarm-id` コマンドを使用し、手動でアラームをクリアする必要があります。次に、アラームをクリアする際に使用できる API の例を示します。詳細については、『NSX API ガイド』を参照してください。

```
GET https://<<NSX-IP>>/api/2.0/services/alarms/{source-Id}
POST https://<<NSX-IP>>/api/2.0/services/alarms?action=resolve

GET https://<<NSX-IP>>/api/2.0/services/systemalarms/<alarmId>
POST https://<<NSX-IP>>/api/2.0/services/systemalarms/<alarmId>?action=resolve
```

- NSX Services：ファイアウォールの発行ステータス：
  - ファイアウォールの発行ステータスが失敗になっているホスト数。発行した分散ファイアウォール設定の適用に失敗したホストがある場合、ステータスは赤色になります。
- NSX Services：論理ネットワークのステータス：
  - ステータスがエラーまたは警告の論理スイッチ数
  - バッキングされている分散仮想ポート グループが vCenter Server から削除された場合のフラグ

## NSX コマンド ライン クイック リファレンス

問題のトラブルシューティングに NSX コマンド ライン インターフェイス (CLI) を使用できます。

**表 1-1. ESXi ホストでの NSX インストール環境の確認：NSX Manager で実行するコマンド**

説明	NSX Manager のコマンド	メモ
すべてのクラスタを表示してクラスタ ID を取得します	<code>show cluster all</code>	すべてのクラスタ情報を表示します
クラスタにあるすべてのホストを表示して、ホスト ID を取得します	<code>show cluster clusterID</code>	クラスタにあるホストのリスト、ホスト ID、ホストの準備のインストールの状態を表示します
ホストにあるすべての仮想マシンを表示します	<code>show host hostID</code>	特定のホスト情報、仮想マシン、仮想マシン ID、および電源ステータスを表示します

表 1-2. ホストにインストールされている、コマンドで使用する VIB とモジュールの名前

NSX バージョン	ESXi バージョン	VIB	モジュール
すべての 6.3.x	5.5	esx-vxlan、esx-vsip	vdl2、vdrb、vsip、dvfilter-switch-security、bfd、traceflow
6.3.2 以前	6.0 以降	esx-vxlan、esx-vsip	vdl2、vdrb、vsip、dvfilter-switch-security、bfd、traceflow
6.3.3 以降	6.0 以降	esx-nsxv	nsx-vdl2、nsx-vdrb、nsx-vsip、nsx-dvfilter-switch-security、nsx-core、nsx-bfd、nsx-traceflow

表 1-3. ESXi ホストでの NSX インストール環境の確認 — ホストから実行するコマンド

説明	ホストのコマンド	メモ
インストールされている VIB は、NSX と ESXi のバージョンによって異なります。 ご利用の環境で確認するモジュールの詳細については、ホストにインストールされている VIB とモジュールの名前を参照してください。	<code>esxcli software vib get -- vibname &lt;name&gt;</code>	インストールされたバージョン/日付を確認します  <code>esxcli software vib list</code> は、システムにあるすべての VIB のリストを表示します
システムで現在ロードされているすべてのシステム モジュールを表示します	<code>esxcli system module list</code>	同じ機能の古いコマンド: <code>vmkload_mod -l   grep -E vdl2 vdrb vsip dvfilter-switch-security</code>
インストールされているモジュールは、NSX と ESXi のバージョンによって異なります。 ご利用の環境で確認するモジュールの詳細については、ホストにインストールされている VIB とモジュールの名前を参照してください。	<code>esxcli system module get -m &lt;name&gt;</code>	各モジュールでこのコマンドを実行します
2 つのユーザー ワールド エージェント (UWA): 制御プレーン エージェント、ファイアウォール エージェント	<code>/etc/init.d/vShield-Stateful-Firewall status</code> <code>/etc/init.d/netcpad status</code>	
UWA の接続 (コントローラへのポート 1234、NSX Manager へのポート 5671) を確認します	<code>esxcli network ip connection list   grep 1234</code> <code>esxcli network ip connection list   grep 5671</code>	コントローラの TCP 接続 メッセージ バスの TCP 接続
EAM のステータスを確認します	vSphere Web Client で、[管理 (Administration)] > [vSphere ESX Agent Manager (vSphere ESX Agent Manager)] の順に移動します	

表 1-4. ESXi ホストでの NSX インストール環境の確認: ホストのネットワーク コマンド

説明	ホストのネットワーク コマンド	メモ
物理 NIC/vmnic を表示します	<code>esxcli network nic list</code>	NIC のタイプ、ドライバのタイプ、リンクのステータス、MTU を確認します
物理 NIC の詳細	<code>esxcli network nic get -n vmnic#</code>	ドライバとファームウェアのバージョンを、その他の詳細情報とともに確認します

表 1-4. ESXi ホストでの NSX インストール環境の確認：ホストのネットワーク コマンド（続き）

説明	ホストのネットワーク コマンド	メモ
vmk NIC の IP アドレス/MAC/MTU などの情報を表示します	esxcli network ip interface ipv4 get	VTEP が正しくインスタンス化されていることを確認します
vSphere Distributed Switch 情報を含む、各 vmk NIC の詳細	esxcli network ip interface list	VTEP が正しくインスタンス化されていることを確認します
VXLAN vmk の vSphere distributed switch 情報を含む、各 vmk NIC の詳細	esxcli network ip interface list --netstack=vxlan	VTEP が正しくインスタンス化されていることを確認します
このホストの VTEP に関連付けられている分散仮想スイッチ名を特定します	esxcli network vswitch dvs vmware vxlan list	VTEP が正しくインスタンス化されていることを確認します
VXLAN 専用 TCP/IP スタックから Ping します	ping ++netstack=vxlan -I vmk1 x.x.x.x	VTEP 通信をトラブルシューティングするには、オプション -d -s 1572 を追加して、トランスポート ネットワークの MTU が VXLAN で正しいことを確認します
VXLAN 専用 TCP/IP スタックのルーティングテーブルを表示します。	esxcli network ip route ipv4 list -N vxlan	VTEP 通信の問題のトラブルシューティング
VXLAN 専用 TCP/IP スタックの ARP テーブルを表示します	esxcli network ip neighbor list -N vxlan	VTEP 通信の問題のトラブルシューティング

表 1-5. ESXi ホストでの NSX インストール環境の確認：ホストのログ ファイル

説明	ログ ファイル	メモ
NSX Manager から	show manager log follow	NSX Manager ログを追跡します ライブ トラブルシューティング向け
ホストのインストール環境に関するログ	/var/log/esxupdate.log	
ホストに関連する問題	/var/log/vmkernel.log	
VMkernel 警告、メッセージ、アラート、および可用性のレポート	/var/log/vmksummary.log /var/log/vmkwarning.log	
モジュールのロード エラーがキャプチャされません	/var/log/syslog	IXGBE ドライバ エラー NSX モジュールの依存関係のエラーが主要なインジケータです
vCenter Server 上で、ESX Agent Manager が更新を行います。	vCenter Server ログの eam.log	

表 1-6. 論理スイッチの確認：NSX Manager で実行するコマンド

説明	NSX Manager のコマンド	メモ
すべての論理スイッチを表示します	show logical-switch list all	すべての論理スイッチ、API で使用されるそれらの UUID、トランスポート ゾーン、および vdnscope を表示します

表 1-7. 論理スイッチ：NSX Controller から実行するコマンド

説明	コントローラのコマンド	メモ
VNI の所有者であるコントローラを特定します	<code>show control-cluster logical-switches vni 5000</code>	出力にあるコントローラの IP アドレスを特定して、そのアドレスに SSH 接続します
この VNI のこのコントローラに接続するすべてのホストを特定します	<code>show control-cluster logical-switch connection-table 5000</code>	出力にあるソース IP アドレスは、ホストの管理インターフェイスであり、ポート番号は TCP 接続のソース ポートです
この VNI をホストするために登録された VTEP を特定します	<code>show control-cluster logical-switches vtep-table 5002</code>	
この VNI の仮想マシンについて習得している MAC アドレスを表示します	<code>show control-cluster logical-switches mac-table 5002</code>	MAC アドレスがそのアドレスを報告している VTEP 上に実際に存在していることを確認します
仮想マシン IP の更新によって設定される ARP キャッシュを表示します	<code>show control-cluster logical-switches arp-table 5002</code>	ARP キャッシュは 180 秒で有効期限が切れます
特定のホスト/コントローラ ペアについて、どの VNI ホストが参加しているかを確認します	<code>show control-cluster logical-switches joined-vnis &lt;host_mgmt_ip&gt;</code>	

表 1-8. 論理スイッチ — ホストから実行するコマンド

説明	ホストのコマンド	メモ
ホスト VXLAN が同期しているかどうかを確認します	<code>esxcli network vswitch dvs vmware vxlan get</code>	同期の状態と、カプセル化に使用されるポートを表示します
接続している仮想マシンとデータバス キャプチャのためのローカル スイッチ ポート ID を表示します	<code>net-stats -l</code>	特定の仮想マシン用の仮想スイッチのポート番号を簡単に取得できる方法です
VXLAN カーネル モジュール vdl2 がロードされていることを確認します	<code>esxcli system module get -m vdl2</code>	特定のモジュールの詳細を表示します バージョンを確認します
正しい VXLAN VIB バージョンがインストールされていることを確認します ご利用の環境で確認する VIB の詳細については、ホストにインストールされている VIB とモジュールの名前を参照してください。	<code>esxcli software vib get --vibName esx-vxlan</code> または <code>esxcli software vib get --vibName esx-nsxv</code>	特定の VIB の詳細を表示します バージョンと日付を確認します
論理スイッチの他のホストをこのホストが認識しているか確認します	<code>esxcli network vswitch dvs vmware vxlan network vtep list --vxlan-id=5001 --vds-name=Compute_VDS</code>	vtep 5001 をホストしていることをこのホストが認識しているすべての VTEP のリストを表示します
制御プレーンが稼動しており、論理スイッチで有効であることを確認します	<code>esxcli network vswitch dvs vmware vxlan network list --vds-name Compute_VDS</code>	コントローラの接続が有効であり、ポート/MAC の数がこのホストの論理スイッチ上の仮想マシン数と一致していることを確認します
ホストがすべての仮想マシンの MAC アドレスを認識していることを確認します	<code>esxcli network vswitch dvs vmware vxlan network mac list --vds-name Compute_VDS --vxlan-id=5000</code>	これは、このホストの VNI 5000 仮想マシンのすべての MAC を表示します

表 1-8. 論理スイッチ — ホストから実行するコマンド（続き）

説明	ホストのコマンド	メモ
ホストにリモート仮想マシンについてローカルでキャッシュされた ARP エントリがあることを確認します	<code>esxcli network vswitch dvs vmware vxlan network arp list --vds-name Compute_VDS --vxlan-id=5000</code>	ホストにリモート仮想マシンについてローカルでキャッシュされた ARP エントリがあることを確認します
仮想マシンが論理スイッチに接続しており、ローカル VMKnic にマッピングされていることを確認します また、仮想マシン dvPort のマッピング先となる vmknic ID を表示します	<code>esxcli network vswitch dvs vmware vxlan network port list --vds-name Compute_VDS --vxlan-id=5000</code>	VNI がルーターに接続されている限り、vdrport は常に表示されます
vmknic ID とマッピングされているスイッチポート/アップリンクを表示します	<code>esxcli network vswitch dvs vmware vxlan vmknic list --vds-name=DSwitch-Res01</code>	

表 1-9. 論理スイッチの確認 — ログ ファイル

説明	ログ ファイル	メモ
ホストは、VNI をホストするコントローラに常に接続されます	<code>/etc/vmware/netcpa/config-by-vsm.xml</code>	このファイルには、表示されている環境にあるすべてのコントローラが常に含まれます。 <code>config-by-vsm.xml</code> ファイルは、 <code>netcpa</code> プロセスによって作成されます
<code>config-by-vsm.xml</code> ファイルは、 <code>vsfwd</code> を使用して NSX Manager によってプッシュされます <code>config-by-vsm.xml</code> ファイルが正しくない場合、 <code>vsfwd</code> ログを確認します	<code>/var/log/vsfwd.log</code>	このファイルを確認して、エラーを特定します プロセスを再開するには、 <code>/etc/init.d/vShield-Stateful-Firewall stop start</code> を実行します
コントローラへの接続には <code>netcpa</code> が使用されます	<code>/var/log/netcpa.log</code>	このファイルを確認して、エラーを特定します
論理スイッチ モジュールのログは、 <code>vmkernel.log</code> にあります	<code>/var/log/vmkernel.log</code>	<code>/var/log/vmkernel.log</code> で、論理スイッチ モジュールのログ「prefixed with VXLAN:」を確認します

表 1-10. 論理ルーティングの確認：NSX Manager から実行するコマンド

説明	NSX Manager のコマンド	メモ
ESG のコマンド	<code>show edge</code>	Edge Services Gateway (ESG) の CLI コマンドは、「show edge」から始まります
分散論理ルーター制御仮想マシンのコマンド	<code>show edge</code>	分散論理ルーター制御仮想マシンの CLI コマンドは、「show edge」から始まります
分散論理ルーターのコマンド	<code>show logical-router</code>	分散論理ルーターの CLI コマンドは、 <code>show logical-router</code> から始まります
すべての Edge を表示します	<code>show edge all</code>	集中管理 CLI をサポートするすべての Edge を表示します
Edge のすべてのサービスおよびデプロイ環境の詳細を表示します	<code>show edge edgeID</code>	Edge Services Gateway の情報を表示します

表 1-10. 論理ルーティングの確認：NSX Manager から実行するコマンド（続き）

説明	NSX Manager のコマンド	メモ
Edge のコマンド オプションを表示します	show edge edgeID ?	バージョン、ログ、NAT、ルーティング テーブル、ファイアウォール、設定、インターフェイス、およびサービスなどの詳細を表示します
ルーティングの詳細を表示します	show edge edgeID ip ?	ルーティング情報、BGP、OSPF および他の詳細を表示します
ルーティング テーブルを表示します	show edge edgeID ip route	Edge でのルーティング テーブルを表示します
ルーティング ネイバーを表示します	show edge edgeID ip ospf neighbor	ルーティング ネイバーの関係性を表示します
分散論理ルーターの接続情報を表示します	show logical-router host hostID connection	接続されている LIF の数が正しいこと、チーミング ポリシーが正しく、適切な vDS が使用されていることを確認します
ホストで実行されているすべての分散論理ルーター インスタンスを表示します	show logical-router host hostID dlr all	LIF とルートの数を確認します コントローラ IP は、分散論理ルーターのすべてのホストで同じである必要があります 「Control Plane Active」は「Yes」にする必要があります --brief を指定すると、簡潔な応答になります
ホストのルーティング テーブルを確認します	show logical-router host hostID dlr dlrID route	これはトランスポート ゾーンにあるすべてのホストに、コントローラからプッシュされるルーティング テーブルになります これは、すべてのホストで同じである必要があります いくつかのルートがいくつかのホストで見つからない場合、前述の同期コマンドをコントローラから実行します E フラグは、ルートが ECMP を介して習得されていることを示します
ホストの分散論理ルーターの LIF を確認します	show logical-router host hostID dlr dlrID interface (all   intName) verbose	LIF 情報は、コントローラからホストにプッシュされます このコマンドを使用して、必要なすべての LIF をホストが確実に認識できるようにします

表 1-11. 論理ルーティングの確認 — NSX Controller から実行するコマンド

説明	NSX Controller のコマンド	メモ
すべての分散論理ルーター インスタンスを特定します	show control-cluster logical-routers instance all	分散論理ルーター インスタンスと、分散論理ルーター インスタンスが関連付けられる必要があるトランスポート ゾーンのすべてのホストを表示します さらに、この分散論理ルーターを提供しているコントローラを表示します
各分散論理ルーターの詳細を表示します	show control-cluster logical-routers instance 0x570d4555	IP アドレス列は、この分散論理ルーターが存在するすべてのホストの vmk0 の IP アドレスを表示します

表 1-11. 論理ルーティングの確認 — NSX Controller から実行するコマンド（続き）

説明	NSX Controller のコマンド	メモ
分散論理ルーターに接続しているすべてのインターフェイスを表示します	<code>show control-cluster logical-routers interface-summary 0x570d4555</code>	IP アドレス列は、この分散論理ルーターが存在するすべてのホストの vmk0 の IP アドレスを表示します
この分散論理ルーターによって習得されたすべてのルートを表示します	<code>show control-cluster logical-routers routes 0x570d4555</code>	IP アドレス列は、この分散論理ルーターが存在するすべてのホストの vmk0 の IP アドレスを表示します
net stat の出力のように、確立されているすべてのネットワーク接続を表示します	<code>show network connections of-type tcp</code>	トラブルシューティングしているホストで、コントローラに netcpa 接続が確立されていることを確認します
コントローラとホストでインターフェイスを同期します	<code>sync control-cluster logical-routers interface-to-host &lt;logical-router-id&gt; &lt;host-ip&gt;</code>	新しいインターフェイスが分散論理ルーターに接続されたものの、すべてのホストと同期されていない場合に便利です
コントローラとホストでルート同期します	<code>sync control-cluster logical-routers route-to-host &lt;logical-router-id&gt; &lt;host-ip&gt;</code>	いくつかのルートがいくつかのホストで見つからないものの、ほとんどのホストで利用できる場合に便利です

表 1-12. 論理ルーティングの確認 — Edge から実行するコマンド

説明	Edge または分散論理ルーター制御仮想マシンのコマンド	メモ
設定を表示します	<code>show configuration &lt;global   bgp   ospf   ...&gt;</code>	
習得されたルートを表示します	<code>show ip route</code>	ルーティングとフォワーディング テーブルが同期されていることを確認します
フォワーディング テーブルを表示します	<code>show ip forwarding</code>	ルーティングとフォワーディング テーブルが同期されていることを確認します
分散論理ルーター インターフェイスを表示します	<code>show interface</code>	出力で最初に表示される NIC が分散論理ルーター インターフェイスになります 分散論理ルーター インターフェイスは、その仮想マシン上の実際の vNIC ではありません 分散論理ルーターに接続しているすべてのサブネットのタイプは、INTERNAL になります
その他のインターフェイス（管理）を表示します	<code>show interface</code>	管理/高可用性インターフェイスは、分散論理ルーター制御仮想マシン上の本当の vNIC です IP アドレスを指定せずに高可用性が有効にされた場合、169.254.x.x/ 30 が使用されます 管理インターフェイスに IP アドレスが指定されている場合、ここに表示されます
プロトコルのデバッグ	<code>debug ip ospf</code> <code>debug ip bgp</code>	設定に関する問題（一致しない OSPF 領域、タイマー、および不正な ASN など）を表示する場合に便利です 注：出力は Edge のコンソールでのみ表示されます（SSH セッションからは表示されません）



表 1-12. 論理ルーティングの確認 — Edge から実行するコマンド（続き）

説明	Edge または分散論理ルーター制御仮想マシンのコマンド	メモ
OSPF コマンド	<pre>show configuration ospf show ip ospf interface show ip ospf neighbor show ip route ospf show ip ospf database show tech-support (および「EXCEPTION」と「PROBLEM」の文字列で検索)</pre>	
BGP コマンド	<pre>show configuration bgp show ip bgp neighbor show ip bgp show ip route bgp show ip forwarding show tech-support (「EXCEPTION」と「PROBLEM」の文字列で検索)</pre>	

表 1-13. 論理ルーティング — ホストのログ ファイル

説明	ログ ファイル	メモ
分散論理ルーター インスタンスの情報は、vsfwd によってホストにプッシュされ、XML 形式で保存されます	/etc/vmware/netcpa/config-by-vsm.xml	分散論理ルーター インスタンスがホストで見つからない場合、まず、このファイルに該当のインスタンスが記載されているかどうかを確認します  表示されていない場合、vsfwd を再起動します また、このファイルを使用して、ホストにすべてのコントローラを確実に認識させます
上記のファイルは vsfwd を使用して NSX Manager にプッシュされます config-by-vsm.xml ファイルが正しくない場合、vsfwd ログを確認します	/var/log/vsfwd.log	このファイルを確認して、エラーを特定します プロセスを再開するには、/etc/init.d/vShield-Stateful-Firewall stop start を実行します
コントローラへの接続には netcpa が使用されます	/var/log/netcpa.log	このファイルを確認して、エラーを特定します
論理スイッチ モジュールのログは、vmkernel.log にあります	/var/log/vmkernel.log	/var/log/vmkernel.log で、論理スイッチ モジュールのログ「prefixed with vxlan:」を確認します

表 1-14. コントローラのデバッグ — NSX Manager から実行するコマンド

説明	コマンド (NSX Manager)	メモ
状態と一緒にすべてのコントローラを表示します	show controller list all	すべてのコントローラの一覧とその実行状態を表示します

表 1-15. コントローラのデバッグ — NSX Controller から実行するコマンド

説明	コマンド (コントローラ)	メモ
コントローラ クラスタのステータスを確認します	<code>show control-cluster status</code>	「Join complete」および「Connected to Cluster Majority」が常に表示されるはずです
フラッピング接続とメッセージの統計情報を確認します	<code>show control-cluster core stats</code>	ドロップされたカウンタは変更しません
クラスタに最初に参加したときや再起動後におけるノードのアクティビティを表示します	<code>show control-cluster history</code>	クラスタへの参加に関する問題をトラブルシューティングするときに便利です
クラスタにあるノードのリストを表示します	<code>show control-cluster startup-nodes</code>	有効なクラスタ ノードのみがリストに含まれるわけではありません このリストには、現在デプロイされているすべてのコントローラが含まれます このリストは、クラスタにある他のコントローラにアクセスするために、起動中のコントローラによって使用されます
<code>net stat</code> の出力のように、確立されているすべてのネットワーク接続を表示します	<code>show network connections of-type tcp</code>	トラブルシューティングしているホストで、コントローラに <code>netcpa</code> 接続が確立されていることを確認します
コントローラ プロセスを再起動します	<code>restart controller</code>	メイン コントローラのプロセスのみを再起動します。 クラスタの再接続を強制します
コントローラ ノードを再起動します	<code>restart system</code>	コントローラ仮想マシンを再起動します

表 1-16. コントローラのデバッグ — NSX Controller のデバッグ

説明	ログ ファイル	メモ
コントローラの履歴と最近の参加状況、再起動などを表示します	<code>show control-cluster history</code>	特にクラスタリングに関するコントローラの問題に対する有効なトラブルシューティング ツールとなります
低速なディスクを確認します	<code>show log cloudnet/cloudnet_java-zookeeper&lt;timestamp&gt;.log filtered-by fsync</code>	低速なディスクを確認する信頼性の高い方法は、 <code>cloudnet_java-zookeeper</code> ログで「fsync」メッセージを確認することです 同期に 1 秒以上かかった場合、ZooKeeper はこのメッセージを出力します。つまり、同じときにディスクが使用されていたことがわかります。
低速/機能不良ディスクを確認します	<code>show log syslog filtered-by collectd</code>	サンプル出力にある「collectd」のようなメッセージは、低速または機能不良のディスクに関連していることがあります
ディスク容量の使用率を確認します	<code>show log syslog filtered-by freespace:</code>	ディスク容量の使用率がしきい値に達した場合、ディスクから古いログや他のファイルを定期的クリーンアップする「freespace」と呼ばれるバックグラウンド ジョブがあります。ディスクが小さい場合や急速にディスク容量を減少させる場合などに、 <code>freespace</code> のメッセージが多数表示されます。これはディスク容量が少なくなっていることを示している場合があります

表 1-16. コントローラのデバッグ — NSX Controller のデバッグ（続き）

説明	ログ ファイル	メモ
現在有効なクラスタ メンバーを検索します	show log syslog filtered-by Active cluster members	現在有効なクラスタ メンバーの node-id を表示します。このメッセージは常に出力されるわけではないため、古い Syslog の調査が必要になる場合があります。
コア コントローラのログを表示します	show log cloudnet/cloudnet_java- zookeeper.20150703-165223.3702.l og	複数の zookeeper ログが存在する場合、タイムスタンプが最新のファイルを確認します このファイルには、コントローラ クラスタ マスターの選択や、コントローラの分散状況に関するその他の情報が含まれます
コア コントローラのログを表示します	show log cloudnet/cloudnet.nsx- controller.root.log.INFO.2015070 3-165223.3668	LIF の作成、1234 での接続リスナー、シャードリングなど、メイン コントローラの動作に関するログ

表 1-17. 分散ファイアウォールの確認 : NSX Manager で実行するコマンド

説明	NSX Manager のコマンド	メモ
仮想マシンの情報を表示します	show vm vmID	データセンター、クラスタ、ホスト、仮想マシン名、vNIC、インストールされている dvfilter などの詳細を表示します
特定の仮想 NIC の情報を表示します	show vnic icID	vNIC 名、MAC アドレス、pg、適用されているフィルタなどの詳細
すべてのクラスタ情報を表示します	show dfw cluster all	クラスタ名、クラスタ ID、データセンター名、ファイアウォールのステータス
特定のクラスタの情報を表示します	show dfw cluster clusterID	ホスト名、ホスト ID、インストールの状態
分散ファイアウォールに関連するホスト情報を表示します	show dfw host hostID	仮想マシン、仮想マシン ID、電源のステータス
dvfilter 内の詳細を表示します	show dfw host hostID filter filterID <option>	各 vNIC のルール、統計情報、アドレス セットなどを表示します
仮想マシンの分散ファイアウォール情報を表示します	show dfw vm vmID	仮想マシンの名前、vNIC ID、フィルタなどを表示します
vNIC の詳細を表示します	show dfw vnic vnicID	vNIC 名、ID、MAC アドレス、ポート グループ、フィルタを表示します
各 vNIC にインストールされているフィルタを表示します	show dfw host hostID summarize- dvfilter	ターゲットの仮想マシン/vNIC を特定して、次のコマンドでフィルタとして使用する名前フィールドを取得します
特定のフィルタ/vNIC のルールを表示します	show dfw host hostID filter filterID rules show dfw vnic nicID	
アドレス セットの詳細を表示します	show dfw host hostID filter filterID addrsets	このルールは、アドレス セットのみを表示し、このコマンドはアドレス セットの一部を拡張するために使用できます
各 vNIC の spoofguard の詳細	show dfw host hostID filter filterID spoofguard	SpoofGuard が有効であるか、また現在の IP/MAC アドレスを確認します

表 1-17. 分散ファイアウォールの確認：NSX Manager で実行するコマンド（続き）

説明	NSX Manager のコマンド	メモ
フロー レコードの詳細を表示します	<code>show dfw host hostID filter filterID flows</code>	フロー モニタリングが有効な場合、ホストはフロー情報を定期的に NSX Manager に送信します  このコマンドを使用して、vNIC ごとのフローを表示します
vNIC の各ルールの統計情報を表示します	<code>show dfw host hostID filter filterID stats</code>	これは、ルールに問題があるかどうかを確認する場合に便利です。

表 1-18. 分散ファイアウォールの確認：ホストから実行するコマンド

説明	ホストのコマンド	注記
ホストにダウンロードされた VIB を表示します。 ご利用の環境で確認する VIB の詳細については、ホストにインストールされている VIB とモジュールの名前を参照してください。	<code>esxcli software vib list   grep esx-vmip</code>  または <code>esxcli software vib list   grep esx-nsxv</code>	正しい VIB バージョンが確実にダウンロードされていることを確認します
現在ロードされているシステム モジュールの詳細 ご利用の環境で確認するモジュールの詳細については、ホストにインストールされている VIB とモジュールの名前を参照してください。	<code>esxcli system module get -m vmip</code>  または <code>esxcli system module get -m nsx-vmip</code>	モジュールが確実にインストール/ロードされていることを確認します
プロセス リスト	<code>ps   grep vsfwd</code>	vsfwd プロセスがいくつかのスレッドで実行しているかどうかを確認します
デーモン コマンド	<code>/etc/init.d/vShield-Stateful-Firewall {start stop status restart}</code>	デーモンが実行されていることを確認し、必要に応じて再起動します
ネットワーク接続を確認します	<code>esxcli network ip connection list   grep 5671</code>	ホストが NSX Manager に TCP で接続しているか確認します

表 1-19. 分散ファイアウォールの確認：ホストのログ ファイル

説明	ログ	メモ
プロセス ログ	<code>/var/log/vsfwd.log</code>	vsfwd デーモン ログ、vsfwd プロセス、NSX Manager 接続、および RabbitMQ のトラブルシューティングに役立ちます
パケット ログ専用ファイル	<code>/var/log/dfwpktlogs.log</code>	パケット ログ専用のログ ファイル
dvfilter でのパケット キャプチャ	<code>pktcap-uw --dvfilter nic-1413082-eth0-vmware-sfw.2 --outfile test.pcap</code>	

## NSX ホストの健全性チェック

NSX Manager の集中管理 CLI から、各 ESXi ホストの健全性ステータスを確認できます。

健全性ステータスは、critical（重大）、unhealthy（不健全）、または healthy（健全）として報告されます。

次はその例です。

```
nsxmgr> show host host-30 health-status
status: HEALTHY

nsxmgr> show host host-29 health-status
UNHEALTHY, Standard Switch vSwitch1 has no uplinks.
UNHEALTHY, Storage volume datastore1 has no enough free spaces: 19.% free.
status: UNHEALTHY

nsxmgr> show host host-28 health-status
CRITICAL, VXLAN VDS vds-site-a VNI 200000 multicast addr is not synchronized with VSM: 0.0.0.0.
CRITICAL, VXLAN VDS vds-site-a VNI 200003 multicast addr is not synchronized with VSM: 0.0.0.0.
CRITICAL, VXLAN VDS vds-site-a VNI 5000 multicast addr is not synchronized with VSM: 0.0.0.0.
Status: CRITICAL
```

host-check コマンドは、NSX Manager API から実行できます。

# NSX インフラストラクチャのトラブルシューティング

## 2

NSX の準備では 4 つの手順を実行します。

- 1 NSX Manager を vCenter Server に接続します。NSX Manager と vCenter Server は 1 対 1 の関係です。
  - a vCenter Server に登録します。
- 2 NSX Controller をデプロイします。これは、論理スイッチ、分散ルーティング、またはユニキャスト/ハイブリッドモードの VXLAN にのみ必要です。分散ファイアウォール (DFW) を使用するだけであれば、コントローラは必要ありません。
- 3 ホストの準備：クラスタ内のすべてのホストで、VXLAN、分散ファイアウォール、および分散論理ルーター用に VIB をインストールします。Rabbit MQ ベースのメッセージングインフラストラクチャを設定します。ファイアウォールを有効にします。NSX 用にホストの準備が整っていることをコントローラに通知します。
- 4 IP アドレスプールの設定と VXLAN の設定：クラスタ内のすべてのホストで、VTEP ポートグループと VMKNIC を作成します。この手順の操作中に、トランスポート VLAN ID、チーミングポリシー、および MTU を設定できます。

各手順のインストールと設定の詳細については、『NSX インストールガイド』と『NSX 管理ガイド』を参照してください。

この章には、次のトピックが含まれています。

- [ホストの準備](#)
- [NSX Manager の問題のトラブルシューティング](#)
- [論理ネットワークの準備：VXLAN 転送](#)
- [論理スイッチのポートグループが同期されない問題](#)

## ホストの準備

vSphere ESX Agent Manager は、ESXi ホストに vSphere インストールバンドル (VIB) をデプロイします。

ホストにデプロイするには、ホスト、vCenter Server、および NSX Manager で DNS を設定する必要があります。デプロイには、ESXi ホストの再起動は必要はありませんが、VIB を更新または削除するときには、ESXi ホストを再起動する必要があります。

VIB は、NSX Manager でホストされ、zip ファイルで提供されます。

このファイルは、<https://<NSX-Manager-IP>/bin/vdn/nwfabric.properties> から入手できます。ダウンロードする zip ファイルは、NSX と ESXi のバージョンによって異なります。たとえば NSX 6.3.0 の場合、vSphere 6.0 ホストでは、<https://<NSX-Manager-IP>/bin/vdn/vibs-6.3.0/6.0-buildNumber/vxlan.zip> ファイルが使用されます。

```
# 5.5 VDN EAM Info
VDN_VIB_PATH.1=/bin/vdn/vibs-6.3.0/5.5-4744075/vxlan.zip
VDN_VIB_VERSION.1=4744075
VDN_HOST_PRODUCT_LINE.1=embeddedEsx
VDN_HOST_VERSION.1=5.5.*

# 6.0 VDN EAM Info
VDN_VIB_PATH.2=/bin/vdn/vibs-6.3.0/6.0-4744062/vxlan.zip
VDN_VIB_VERSION.2=4744062
VDN_HOST_PRODUCT_LINE.2=embeddedEsx
VDN_HOST_VERSION.2=6.0.*

# 6.5 VDN EAM Info
VDN_VIB_PATH.3=/bin/vdn/vibs-6.3.0/6.5-4744074/vxlan.zip
VDN_VIB_VERSION.3=4744074
VDN_HOST_PRODUCT_LINE.3=embeddedEsx
VDN_HOST_VERSION.3=6.5.*

# Single Version associated with all the VIBs pointed by above VDN_VIB_PATH(s)
VDN_VIB_VERSION=6.3.0.4744320

# Legacy vib location. Used by code to discover available legacy vibs.
LEGACY_VDN_VIB_PATH_FS=/common/em/components/vdn/vibs/legacy/
LEGACY_VDN_VIB_PATH_WEB_ROOT=/bin/vdn/vibs/legacy/
```

ホストにインストールされている VIB は、NSX と ESXi のバージョンによって異なります。

ESXi バージョン	NSX バージョン	インストールされている VIB
5.5	すべての 6.3.x	<ul style="list-style-type: none"> <li>■ esx-vsip</li> <li>■ esx-vxlan</li> </ul>
6.0 以降	6.3.2 以前	<ul style="list-style-type: none"> <li>■ esx-vsip</li> <li>■ esx-vxlan</li> </ul>
6.0 以降	6.3.3 以降	<ul style="list-style-type: none"> <li>■ esx-nsxv</li> </ul>

esxcli software vib list コマンドを使用すると、インストールされている VIB を表示できます。

```
[root@esx-01a:~] esxcli software vib list | grep -e vsip -e vxlan
esx-vsip                6.0.0-0.0.XXXXXXX      VMware  VMwareCertified
2016-04-20
esx-vxlan                6.0.0-0.0.XXXXXXX      VMware  VMwareCertified
2016-04-20
```

or

```
esxcli software vib list | grep nsxv
esx-nsxv                6.0.0-0.0.XXXXXXX      VMware  VMwareCertified
2017-08-11
```

## ホストを準備するときの一般的な問題

ホストを準備するときには発生する問題には、次のものがあります。

- ESX Agent Manager (EAM) が VIB のデプロイに失敗する。
  - ホストの DNS が正しく設定されていない可能性があります。
  - ESXi、NSX Manager、および vCenter Server 間で必要なポートがファイアウォールによってブロックされている可能性があります。

[解決 (Resolve)] オプションをクリックすると、ほとんどの問題が解決されます。[インストール ステータスに「準備ができていません」と表示される](#) を参照してください。

- 古いバージョンの VIB がすでにインストールされている。この場合には、ユーザーがホストを再起動する必要があります。
- NSX Manager と vCenter Server で通信の問題が発生します。Networking and Security プラグインの [ホストの準備 (Host Preparation)] タブに、すべてのホストが適切に表示されません。
  - vCenter Server がすべてのホストとクラスタを認識できることを確認します。

[解決 (Resolve)] オプションで問題が解決しない場合は、[\[解決\] オプションを使用して解決できない問題](#) を参照してください。

## ホスト準備 (VIB) のトラブルシューティング

- ホストの通信チャネルの健全性を確認します。[通信チャネルの健全性の確認](#) を参照してください。
- vSphere ESX Agent Manager にエラーがないか確認します。

[vCenter Server ホーム (vCenter home)] > [管理 (Administration)] > [vCenter Server 拡張機能 (vCenter Server Extensions)] > [vSphere ESX Agent Manager]

vSphere ESX Agent Manager で、「VCNS160」というプリフィックスのエージェントのステータスを確認します。ステータスが健全ではないエージェントを選択してその問題を確認します。



Agency	State	Status	Optimized Deployment
_VCNS_160_Management & Edge CI...	Enabled	✓ Normal	✓
_VCNS_160_Compute Cluster A_VMwa...	Enabled	⚠ Alert	✓

Issues for the selected agencies

Trigger Time	Agency	Issue	Host	Agent VM
Thu Apr 28 12:03:12 GMT-0...	_VCNS_160_Compute Clu...	Agent VIB module is not installed	esx-01a.corp.local	

- 問題があるホストで、`tail /var/log/esxupdate.log` コマンドを実行します。

```

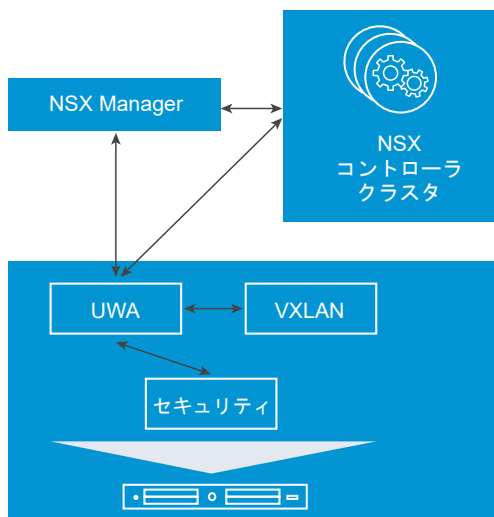
2016-04-28T19:02:52Z esxupdate: downloader: DEBUG: Downloading https://vcsa-01a.corp.local/tmp/tmpKT0wjN...
2016-04-28T19:03:12Z esxupdate: esxupdate: ERROR: An esxupdate error exception occurred
2016-04-28T19:03:12Z esxupdate: esxupdate: ERROR: Traceback (most recent call last):
2016-04-28T19:03:12Z esxupdate: esxupdate: ERROR:   File "/usr/sbin/esxupdate.py", line 106, in <module>
2016-04-28T19:03:12Z esxupdate: esxupdate: ERROR:     cmd.Run()
2016-04-28T19:03:12Z esxupdate: esxupdate: ERROR:   File "/build/mts/release/mtsite-packages/vmware/esx5update/Cmdline.py", line 106, in Run
2016-04-28T19:03:12Z esxupdate: esxupdate: ERROR:   File "/build/mts/release/mtsite-packages/vmware/esximage/Transaction.py", line 73, in DownloadMetadata
2016-04-28T19:03:12Z esxupdate: esxupdate: ERROR: MetadataDownloadError: ('https://vcsa-01a.corp.local:443/eam/vib?id=facdb160-2160-4000-8000-000000000000', None, "('https://vcsa-01a.corp.local:443/eam/vib?id=facdb160-2160-4000-8000-000000000000', None, 'Temporary failure in name resolution')")
2016-04-28T19:03:12Z esxupdate: esxupdate: DEBUG: <<<

```

## ホスト準備 (UWA) のトラブルシューティング

NSX Manager は、2 つのユーザー ワールド エージェントをクラスタ内のすべてのホスト上に設定します。

- メッセージング バス UWA (vsfwd)
- 制御プレーン UWA (netcpa)



まれに、VIB のインストールには成功するものの、何らかの理由によって、一方または両方のユーザー ワールド エージェントが正しく機能しない場合があります。以下のような問題が発生している場合があります。

- ファイアウォールのステータスが健全ではない。

Cluster & Hosts	Installation Status	Firewall
Cluster 1	6.0 Uninstall	Error

- ハイパーバイザーとコントローラ間の制御プレーンがダウンしている。NSX Manager システム イベントを確認します。『NSX のログ作成とシステム イベント』を参照してください。

Getting Started Summary Monitor Manage				
Audit Logs System Events Tasks				
Timestamp	Severity	Event Source	Code	Event Message
2/26/2014 10:56:38 AM	Critical	Host messaging infrastructure	391002	Messaging infrastructure down on host.
2/26/2014 10:51:56 AM	Critical	host-22	301502	Spoofguard configuration update number 139340752032...
2/26/2014 10:51:56 AM	Critical	host-20	301502	Spoofguard configuration update number 139340752032...

1 台以上の ESXi ホストが影響を受けている場合、Web ユーザー インターフェイスで NSX Manager アプライアンスにアクセスし、[サマリ (Summary)] タブで、メッセージ バス サービスのステータスを確認します。RabbitMQ が停止している場合には、再起動します。

**NSX Manager Virtual Appliance**

DNS Name: nsxmgr-l-01a  
 IP Address: 192.168.110.42  
 Version: 6.0.2 Build 2944561  
 Uptime: 7 days, 3 hours, 16 minutes  
 Current Time: Monday, 24 February 2014 01:29:52 PM UTC

Name	Version	Status	
vPostgres		Running	Stop
RabbitMQ		Running	Stop

NSX Manager でメッセージ バス サービスが有効な場合：

- ESXi ホストで `/etc/init.d/vShield-Stateful-Firewall status` コマンドを実行して、ホスト上のメッセージ バス エージェントとユーザー ワールド エージェントの状態を確認します。

```
[root@esx-01a:~] /etc/init.d/vShield-Stateful-Firewall status
vShield-Stateful-Firewall is running
```

- `/var/log/vsfdw.log` で、ホストのメッセージ バスとユーザー ワールドのログを確認します。

- `esxcfg-advcfg -l | grep Rmq` コマンドを ESXi ホストで実行して、すべての Rmq 変数を表示します。16 個の Rmq 変数が表示されます。

```
[root@esx-01a:~] esxcfg-advcfg -l | grep Rmq
/UserVars/RmqIpAddress [String] : Connection info for RMQ Broker
/UserVars/RmqUsername [String] : RMQ Broker Username
/UserVars/RmqPassword [String] : RMQ Broker Password
/UserVars/RmqVHost [String] : RMQ Broker VHost
/UserVars/RmqVsmRequestQueue [String] : RMQ Broker VSM Request Queue
/UserVars/RmqPort [String] : RMQ Broker Port
/UserVars/RmqVsmExchange [String] : RMQ Broker VSM Exchange
/UserVars/RmqClientPeerName [String] : RMQ Broker Client Peer Name
/UserVars/RmqHostId [String] : RMQ Broker Client HostId
/UserVars/RmqHostVer [String] : RMQ Broker Client HostVer
/UserVars/RmqClientId [String] : RMQ Broker Client Id
/UserVars/RmqClientToken [String] : RMQ Broker Client Token
/UserVars/RmqClientRequestQueue [String] : RMQ Broker Client Request Queue
/UserVars/RmqClientResponseQueue [String] : RMQ Broker Client Response Queue
/UserVars/RmqClientExchange [String] : RMQ Broker Client Exchange
/UserVars/RmqSslCertSha1ThumbprintBase64 [String] : RMQ Broker Server Certificate base64 Encoded Sha1 Hash
```

- `esxcfg-advcfg -g /UserVars/RmqIpAddress` コマンドを ESXi ホストで実行します。NSX Manager の IP アドレスが表示されます。

```
[root@esx-01a:~] esxcfg-advcfg -g /UserVars/RmqIpAddress
Value of RmqIpAddress is 192.168.110.15
```

- `esxcli network ip connection list | grep 5671` コマンドを ESXi ホストで実行して、有効なメッセージ バス接続を確認します。

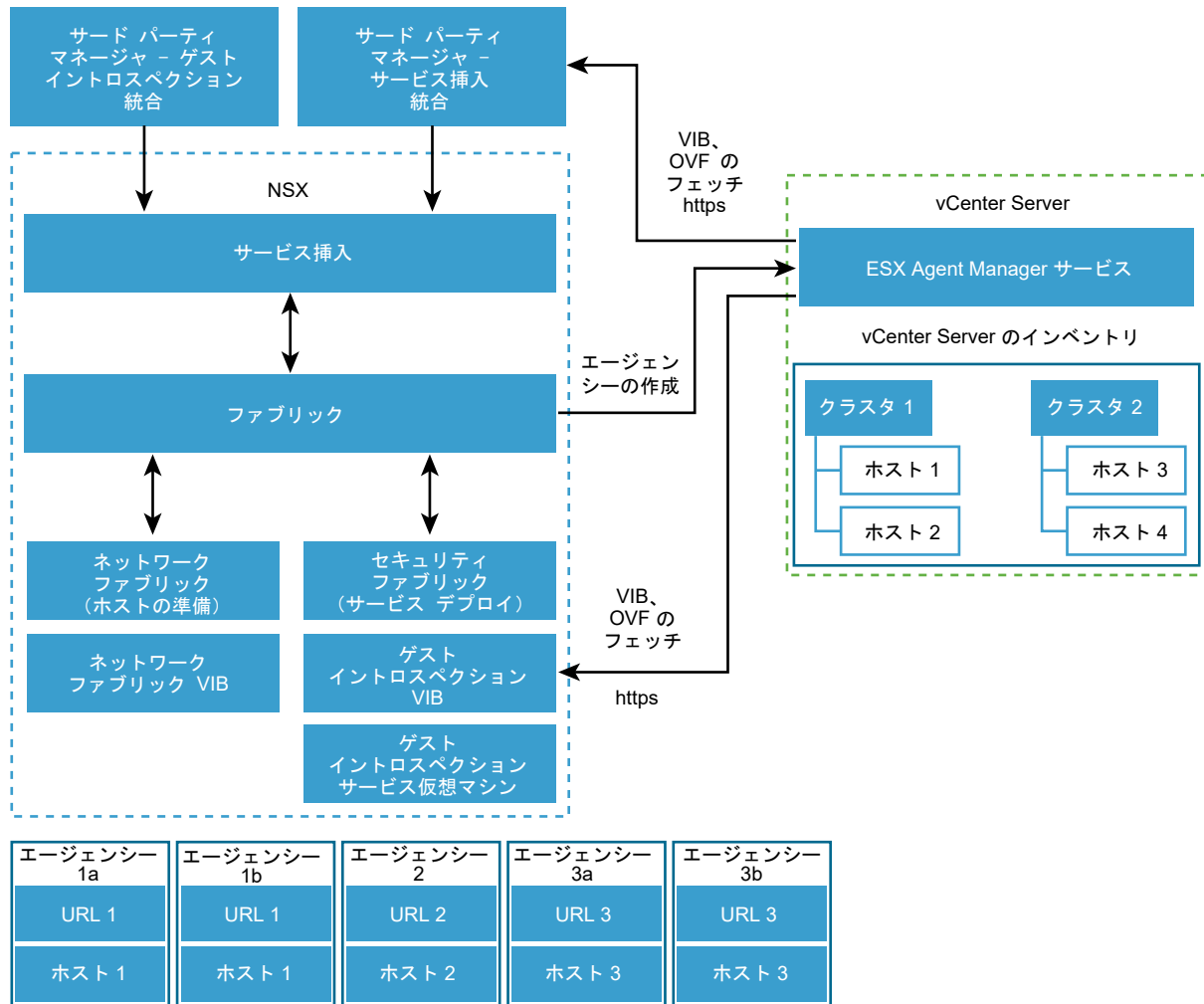
```
[root@esx-01a:~] esxcli network ip connection list | grep 5671
tcp          0      0 192.168.110.51:29969      192.168.110.15:5671      ESTABLISHED
35505 newreno vsfwd
tcp          0      0 192.168.110.51:29968      192.168.110.15:5671      ESTABLISHED
35505 newreno vsfwd
```

制御プレーン エージェントに関連する問題については、[制御プレーン エージェント \(netcpa\) の問題](#)を参照してください。

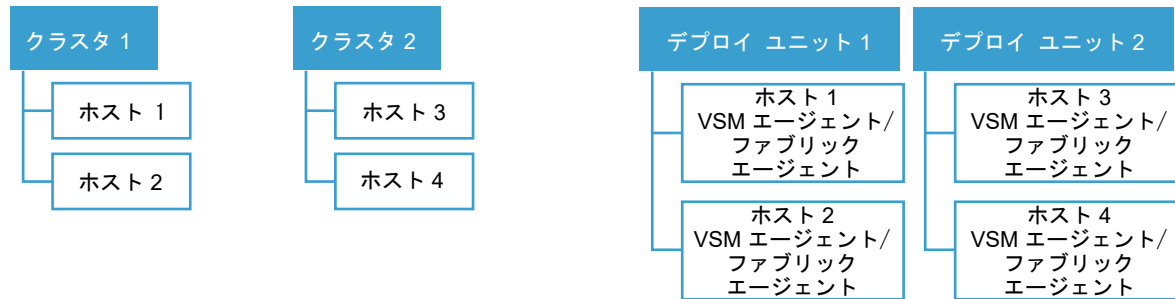
## ホストの準備のアーキテクチャについて

このトピックでは、基本的なホストの準備のアーキテクチャについて説明します。

- ネットワーク ファブリックをデプロイするには、[ホストの準備 (Host Preparation)] タブに移動します。
- セキュリティ ファブリックをデプロイするには、[サービス デプロイ (Service Deployment)] タブに移動します。

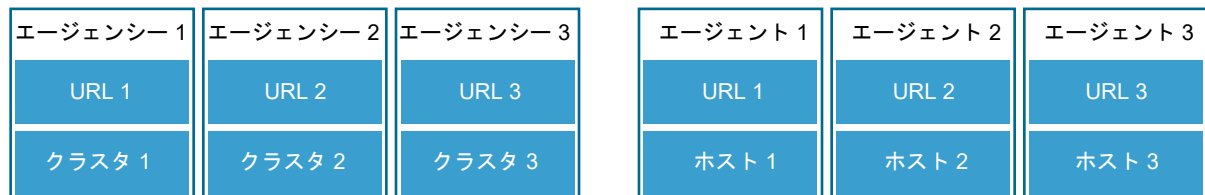
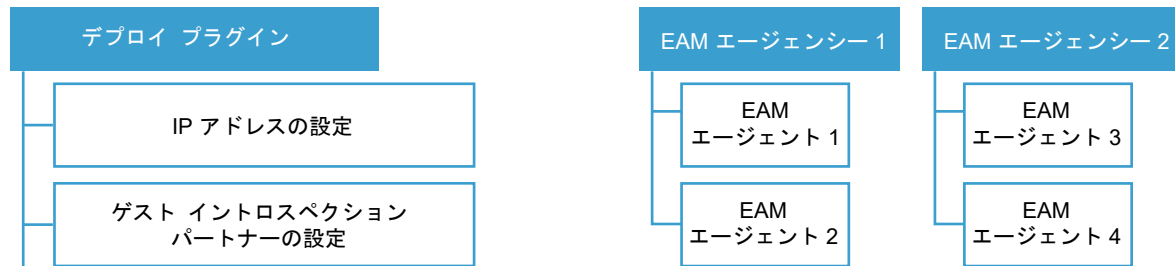


## NSX オブジェクト



ファブリック エージェント == VSM エージェント

## vSphere ESXi Agent Manager (EAM) オブジェクト



次の用語は、ホストの準備のアーキテクチャを理解する際に役立ちます。

<b>ファブリック</b>	ファブリックは NSX Manager のソフトウェア レイヤーで、ESX Agent Manager と相互に通信し、ネットワークおよびセキュリティ ファブリック サービスをホストにインストールします。
<b>ネットワーク ファブリック</b>	ネットワーク ファブリック サービスはクラスタにデプロイされます。ネットワーク ファブリック サービスには、ホストの準備、VXLAN、分散ルーティング、分散ファイアウォール、メッセージ バスが含まれます。
<b>セキュリティ ファブリック</b>	セキュリティ ファブリック サービスはクラスタにデプロイされます。セキュリティ ファブリック サービスには、ゲスト イントロスペクションとパートナーのセキュリティ ソリューションが含まれます。
<b>ファブリック エージェント</b>	<p>ファブリック エージェントは、NSX Manager データベース内のファブリック サービスとホストの組み合わせです。ネットワークまたはセキュリティ ファブリック サービスがデプロイされているクラスタのホスト 1 台につき、1 つのファブリック エージェントが作成されます。</p> <p>別名： VSM エージェント</p>
<b>デプロイ ユニット</b>	NSX Manager データベースでのファブリック サービスとクラスタの組み合わせ。ネットワークおよびセキュリティ サービスをインストールするには、デプロイ ユニットの作成する必要があります。
<b>ESX Agent Manager エージェント</b>	ESX Agent Manager エージェントは、vCenter Server データベース内のサービス仕様とホストの組み合わせです。ESX Agent Manager エージェントは、NSX ファブリック エージェントにマッピングされます。
<b>ESX Agent Manager エージェント</b>	<p>ESX Agent Manager エージェントは、vCenter Server データベース内の仕様とクラスタの組み合わせです。この仕様には、ESX Agent Manager エージェントと VIB、OVF、管理している構成（データストアやネットワークの設定など）が記述されています。</p> <p>NSX Manager は、準備中のクラスタに ESX Agent Manager エージェントを作成します。</p> <p>ESX Agent Manager エージェントは、NSX デプロイ ユニットのマッピングされます。デプロイ ユニットの NSX Manager データベースと ESX Agent Manager エージェントの vCenter Server ESX Agent Manager データベースは、同期する必要があります。まれに、2 つのデータベースが同期していない場合があります。その場合、NSX がイベントをトリガし、この状態をユーザーに通知します。NSX Manager は、データベースに各 ESX Agent Manager エージェントのデプロイ ユニットの作成します。</p>

NSX Manager は、準備するクラスタごとに、ESX Agent Manager エージェントを作成します。NSX Manager は、各 ESX Agent Manager エージェントのデータベースにデプロイ ユニットを作成します。1 つの ESX Agent Manager エージェントに 1 つのデプロイ ユニットが作成されます。

エージェントは、次の方法で確認できます。

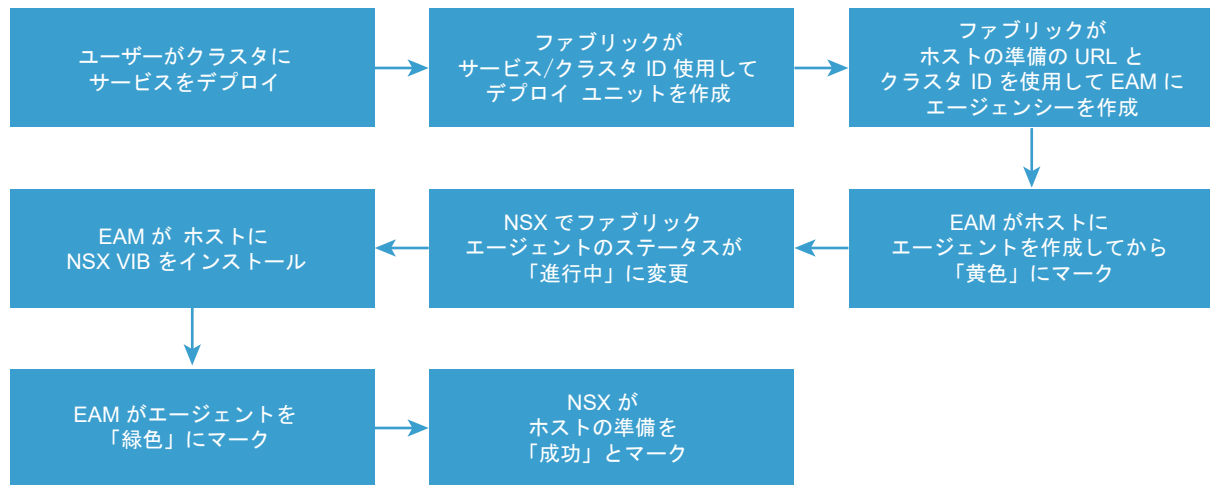
- EAM MOB から : <https://<VC-hostname/IP>/eam/mob/>
- vSphere Web Client から :
  - [vCenter Solutions Manager] - [vSphere ESX Agent Manager] - [管理 (Manage)] の順に移動します。
  - [ESX エージェント (ESX Agencies)] にエージェントが表示されます。ホストに準備されたクラスタごとに 1 つのエージェントが表示されます。

デプロイ ユニットのライフサイクルは、エージェントのライフサイクルに関連付けられています。ESX Agent Manager からエージェントを削除すると、NSX から対応するデプロイ ユニットが削除されます。

## ホストの準備のサービス デプロイ ワークフロー

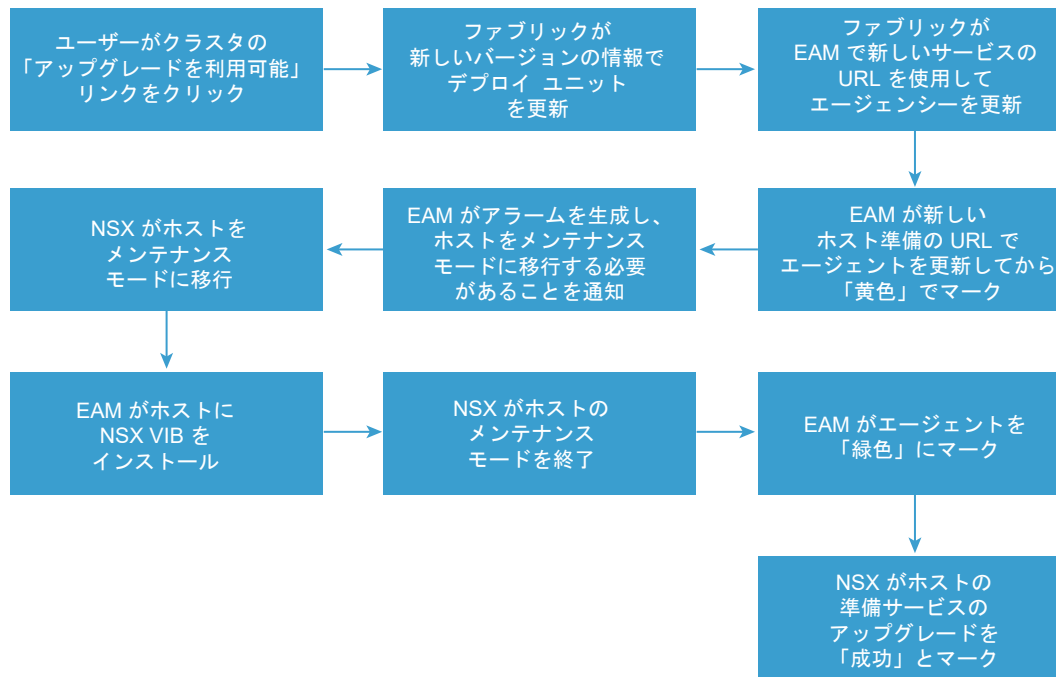
このトピックでは、ホストの準備のサービス デプロイ ワークフロー（インストールとアップグレード）を説明します。

## インストールのワークフロー





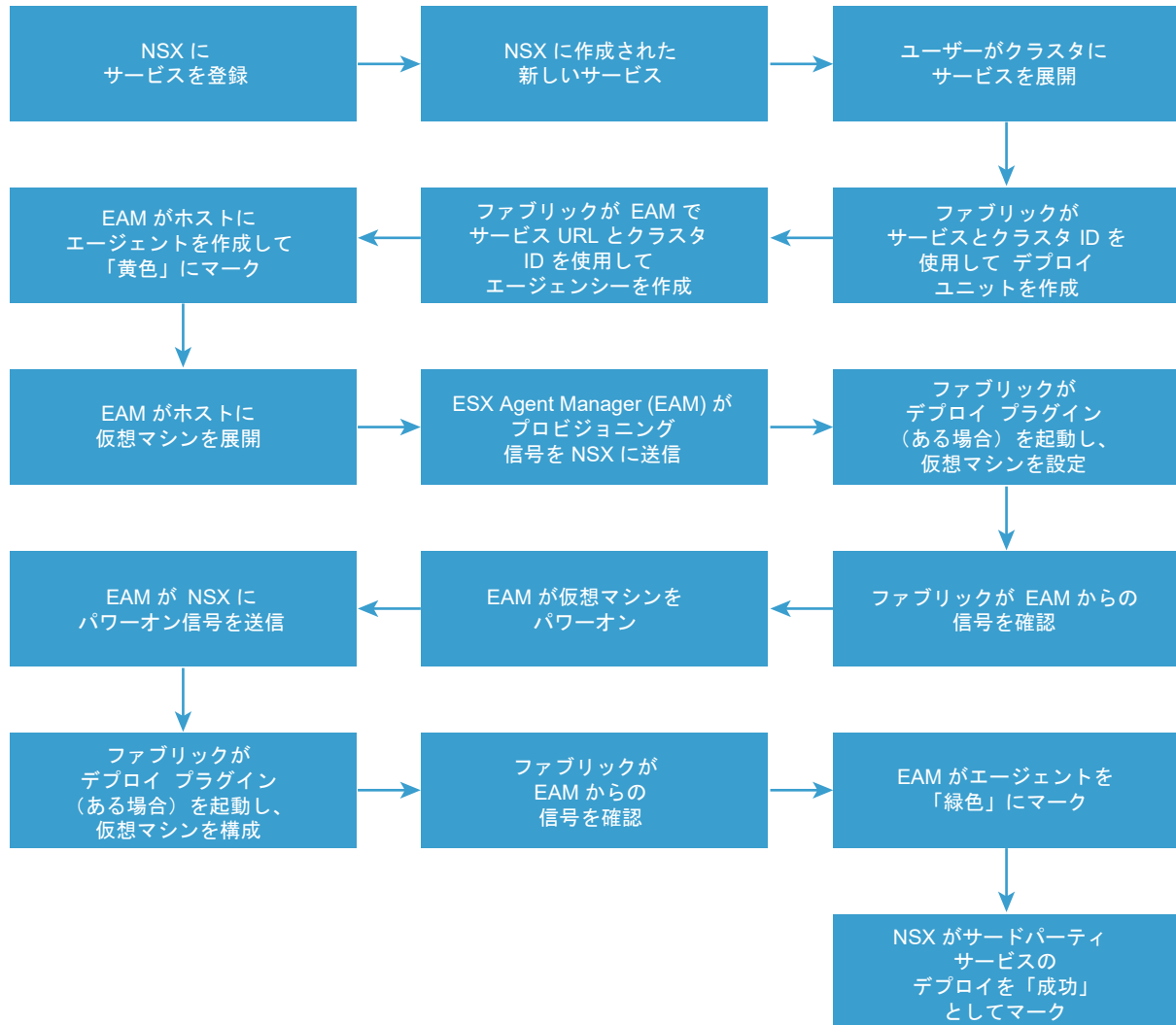
## アップグレードのワークフロー



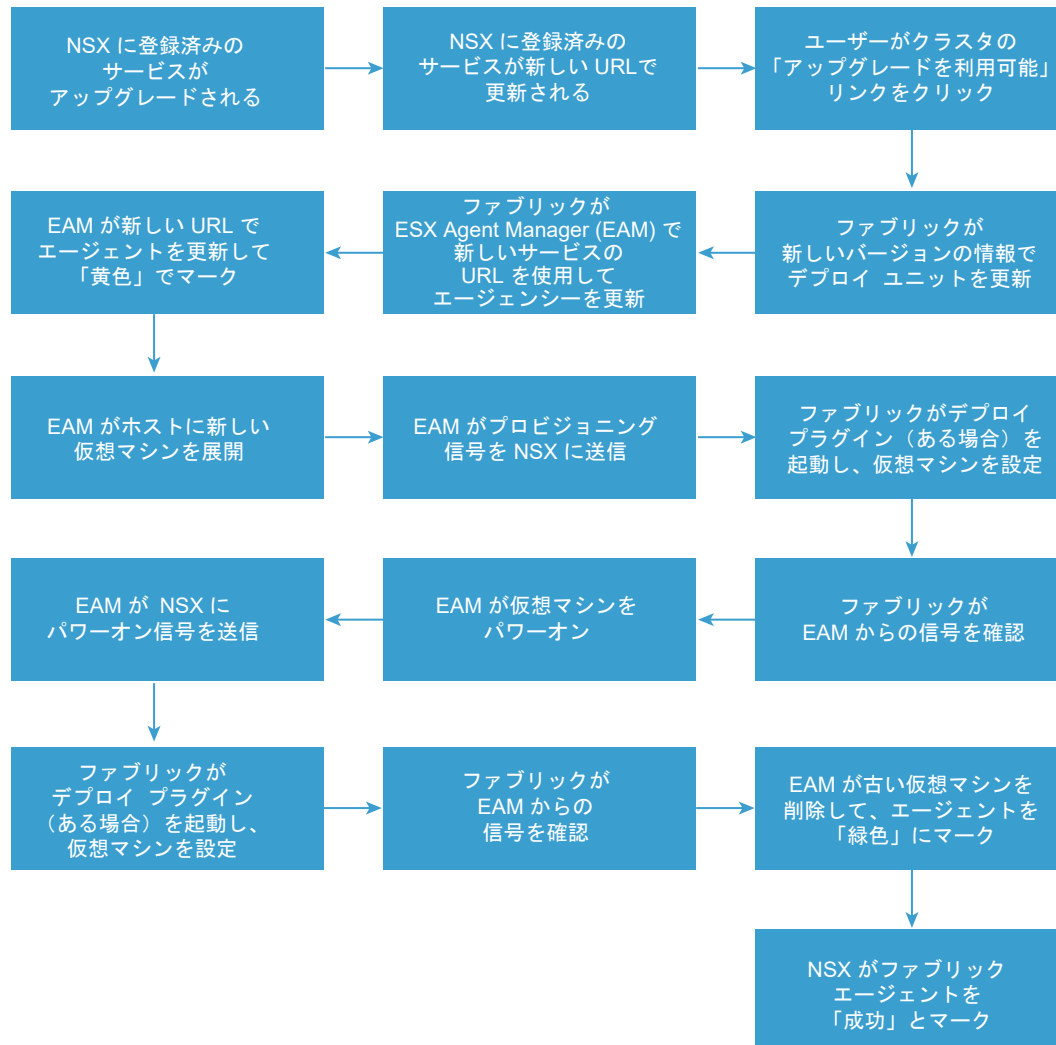
## サードパーティ サービスのサービス デプロイ ワークフロー

このトピックでは、サードパーティ サービスのサービス デプロイ ワークフロー（インストールとアップグレード）について説明します。

## インストールのワークフロー



## アップグレードのワークフロー



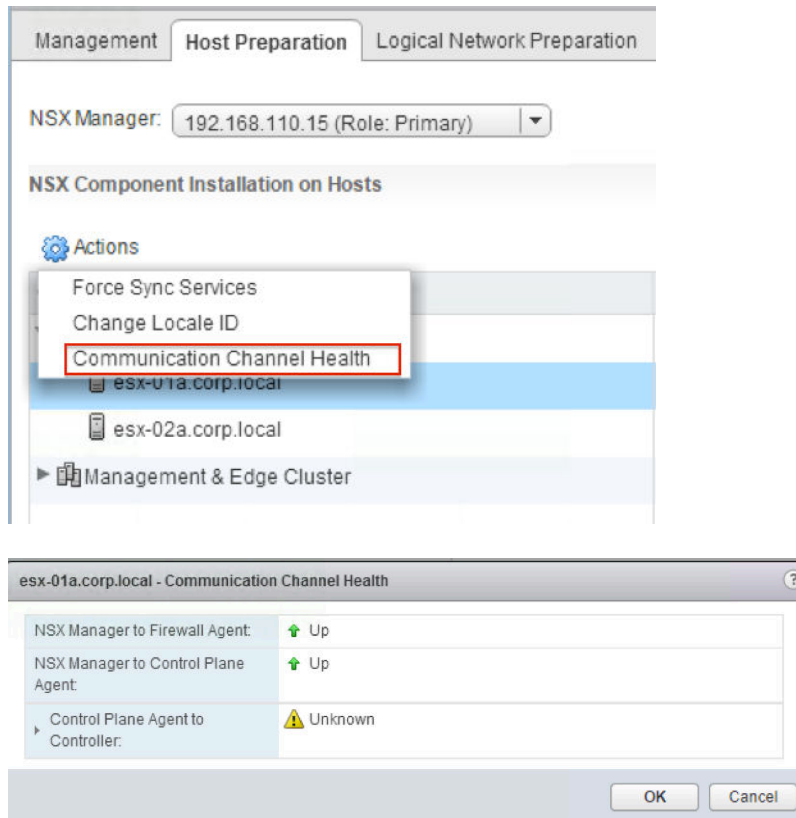
## 通信チャネルの健全性の確認

vSphere Web Client を使用すると、さまざまなコンポーネント間の通信の状態を確認できます。

NSX Manager とファイアウォール エージェント間、NSX Manager と制御プレーン エージェント間、および制御プレーン エージェントとコントローラ間の通信チャネルの健全性を確認するには、次の手順を実行します。

- 1 vSphere Web Client で、[Networking and Security (Networking & Security)] - [インストール手順 (Installation)] - [ホストの準備 (Host Preparation)] の順に移動します。
- 2 クラスタを選択するか、クラスタを展開して、ホストを選択します。[アクション (Actions)] (⚙️) をクリックし、[通信チャネルの健全性 (Communication Channel Health)] をクリックします。

通信チャネルの健全性情報が表示されます。



ホストの 3 つの接続のうちいずれかの状態が変更されると、NSX Manager ログにメッセージが書き込まれます。ログメッセージでは、接続状態は UP、DOWN、または NOT\_AVAILABLE (vSphere Web Client では [不明] と表示) のいずれかです。UP から DOWN または NOT\_AVAILABLE に状態が変更されると、警告メッセージが生成されます。次はその例です。

```
2016-05-23 23:36:34.736 GMT+00:00 WARN TaskFrameworkExecutor-25 VdnInventoryFacadeImpl
$HostStatusChangedEventHandler:200 - Host Connection Status Changed: Event Code: 1941, Host:
esx-04a.corp.local (ID: host-46), NSX Manager - Firewall Agent: UP, NSX Manager - Control Plane
Agent: UP, Control Plane Agent - Controllers: DOWN.
```

DOWN または NOT\_AVAILABLE から UP に状態が変更されると、警告メッセージに似た情報メッセージが生成されます。次はその例です。

```
2016-05-23 23:55:12.736 GMT+00:00 INFO TaskFrameworkExecutor-25 VdnInventoryFacadeImpl
$HostStatusChangedEventHandler:200 - Host Connection Status Changed: Event Code: 1938, Host:
esx-04a.corp.local (ID: host-46), NSX Manager - Firewall Agent: UP, NSX Manager - Control Plane
Agent: UP, Control Plane Agent - Controllers: UP.
```

制御プレーンのチャネルで通信障害が発生した場合、システム イベントが生成され、次の詳細な障害原因のうちの 1 つが示されます。

- 1255601 : 不完全なホスト証明書
- 1255602 : 不完全なコントローラ証明書
- 1255603 : SSL ハンドシェークに失敗しました

- 1255604 : 接続が拒否されました
- 1255605 : キープ アライブ タイムアウト
- 1255606 : SSL 例外
- 1255607 : 不正なメッセージ
- 1255620 : 不明なエラー

また、NSX Manager からホストへのハートビート メッセージが生成されます。NSX Manager と netcpa 間のハートビートが失われると、設定の完全同期がトリガされます。

アラートの表示方法の詳細については、『NSX 管理ガイド』を参照してください。

## インストール ステータスに「準備ができていません」と表示される

ホストの準備中に、クラスタのステータスに「準備ができていません」と表示される場合があります。

### 問題

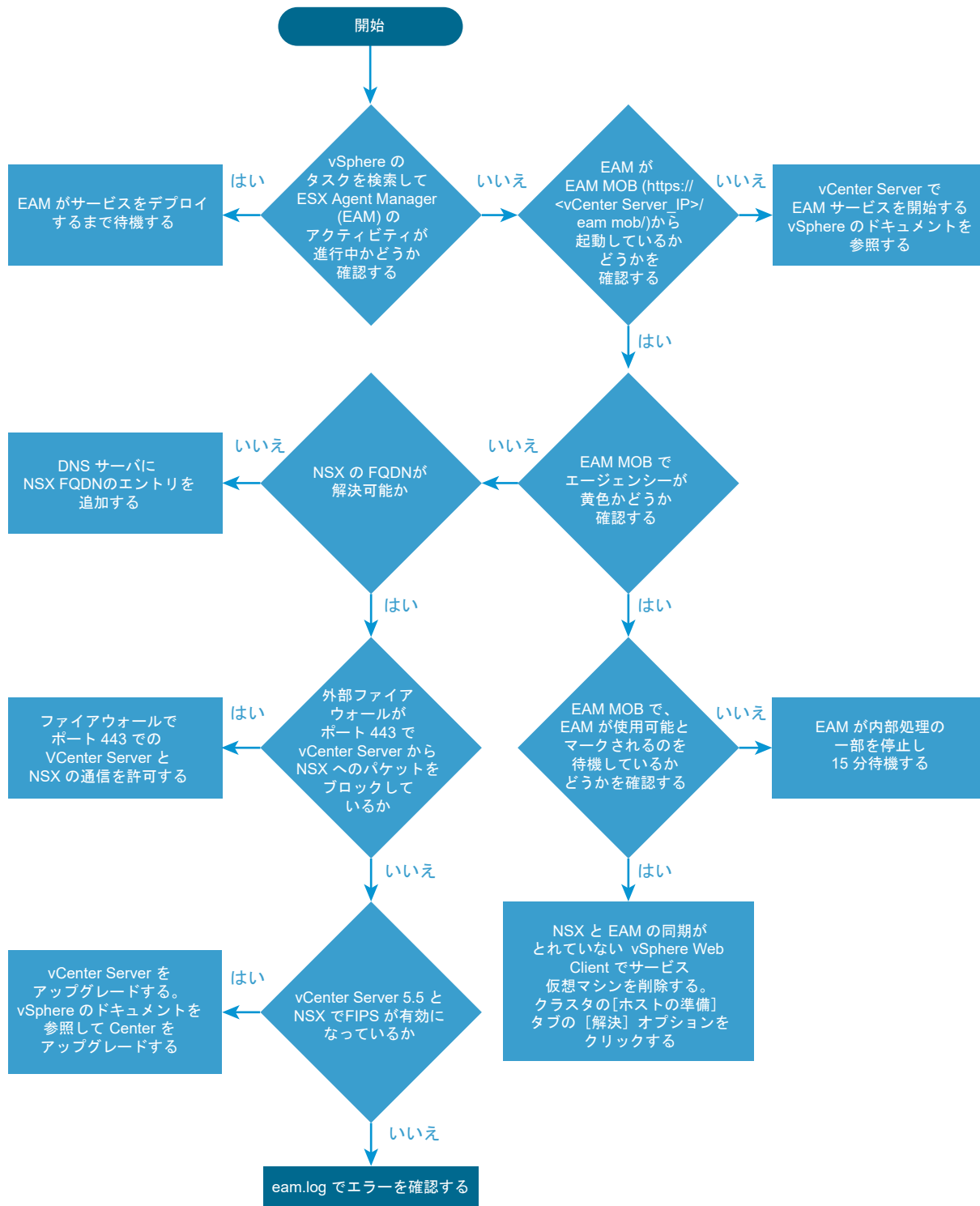
[ホストの準備 (Host Preparation)] タブまたは [サービス デプロイ (Service Deployment)] タブで、インストール ステータスに「準備ができていません」と表示されます。

### 解決方法

- 1 [Networking and Security (Networking & Security)] - [インストール手順 (Installation)] の順に移動し、[ホストの準備 (Host Preparation)] タブまたは [サービス デプロイ (Service Deployment)] タブを選択します。
- 2 クラスタとホストで、「準備ができていません」をクリックします。  
エラー メッセージが表示されます。
- 3 [解決 (Resolve)] オプションをクリックします。  
[解決 (Resolve)] オプションで解決される問題については、『NSX のログ作成とシステム イベント』を参照してください。
- 4 まだ「準備ができていません」が表示され、エラーが解決しない場合には、[\[解決\] オプションを使用して解決できない問題](#)を参照してください。

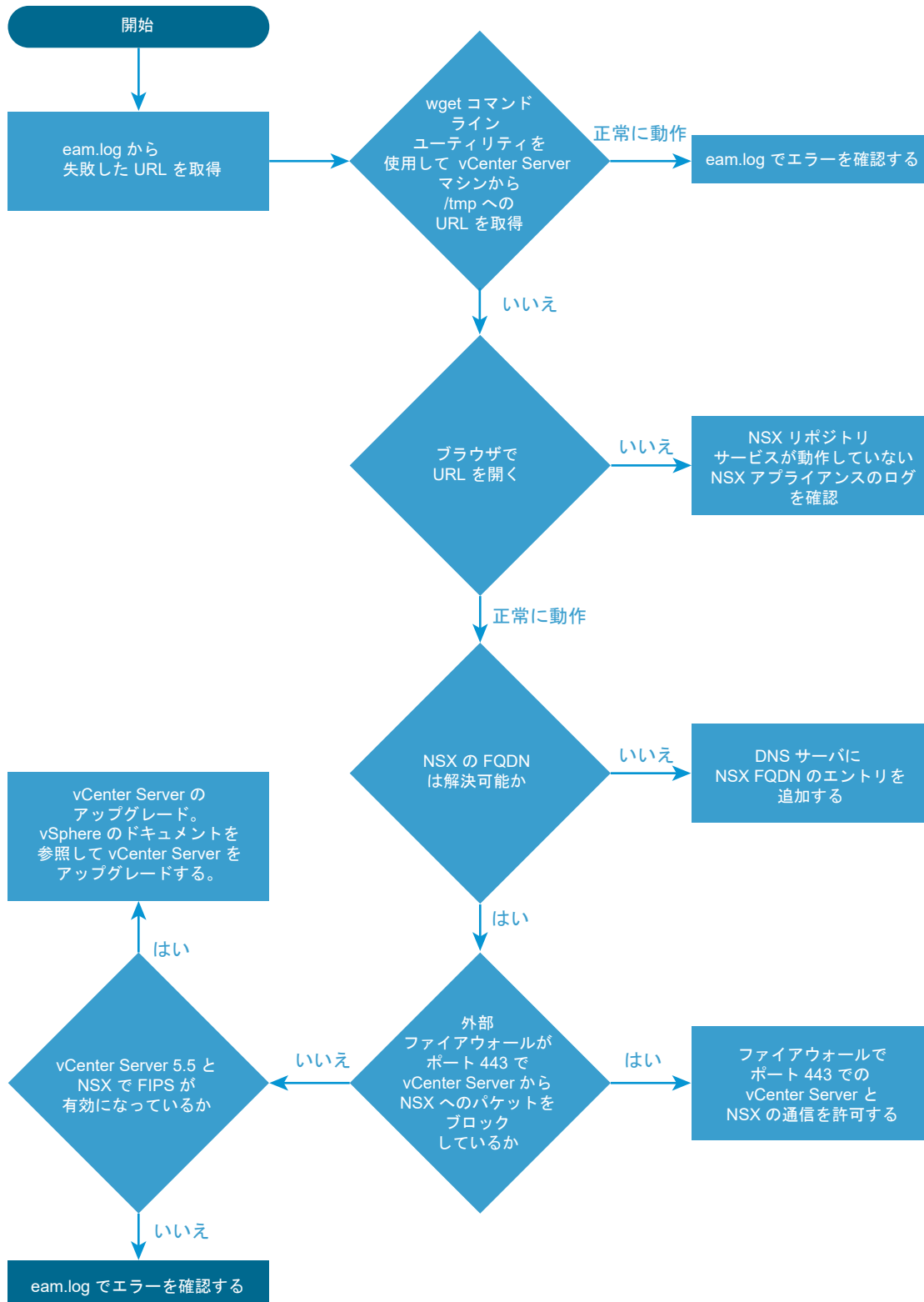
## サービスが応答しない

次のフローチャートは、NSX ホストの準備プロセスの概要を示したものです。サービスが長時間応答しない場合、あるいはアイコンが回転したまま長時間表示されている場合の対処方法についても説明しています。



## 「OVF/VIB not accessible」エラーでサービスのデプロイが失敗する

次のフローチャートは、サービスのデプロイが OVF/VIB not accessible エラーで失敗した場合の対処方法を示したものです。



## [解決] オプションを使用して解決できない問題

[Networking and Security (Networking & Security)] - [インストール手順 (Installation)] の順に移動して [ホストの準備 (Host Preparation)] タブまたは [サービス デプロイ (Service Deployment)] タブを表示すると、クラスタとホストのインストール ステータスに「準備ができていません」と表示されます。[解決 (Resolve)] オプションをクリックしても、この問題は解決されません。

### 問題

- 「準備ができていません」リンクをクリックすると、「エージェントの VIB モジュールがホストにインストールされていません」というエラーが表示されます。
- ESXi ホストで、vCenter Server から VIB へのアクセスに失敗しています。
- vShield Endpoint から NSX Manager への変更中に、失敗というステータスが表示される場合があります。

### 解決方法

- 1 vCenter Server、ESXi ホスト、および NSX Manager で DNS が正しく設定されていることを確認します。vCenter Server、ESXi、ホスト、NSX Manager、および vSphere Update Manager からの正引きと逆引きの DNS 解決が機能していることを確認します。
- 2 DNS 関連の問題かどうか判断するには、**esxupdate** ログを確認し、**esxupdate.log** ファイルで “esxupdate: ERROR: MetadataDownloadError:IOError: <urlopen error [Errno -2] Name= or service not known” というメッセージを検索します。

このメッセージは、ESXi ホストが vCenter Server の完全修飾ドメイン名 (FQDN) にアクセスできないことを意味します。詳細については、[Verifying the VMware vCenter Server Managed IP Address \(1008030\)](#)を参照してください。

- 3 NTP (Network Time Protocol) が正しく設定されていることを確認します。NTP を設定することをお勧めします。NTP の非同期状態が環境に影響を及ぼしているかどうかを判断するには、NSX 6.2.4 以降のバージョンの NSX Manager サポート バンドルで **/etc/ntp.drift** ファイルを確認します。
- 4 NSX for vSphere 6.x に必要なすべてのポートがファイアウォールでブロックされていないことを確認します。詳細については、次を参照してください。
  - [Network Port Requirements for VMware NSX for vSphere \(2079386\)](#)
  - [TCP and UDP Ports required to access VMware vCenter Server, VMware ESXi and ESX hosts, and other network components \(1012382\)](#)

---

**注：** VMware vSphere 6.x は、ポート 80 ではなくポート 443 での VIB のダウンロードをサポートしています。このポートの開閉は動的に行われます。ESXi ホストと vCenter Server 間の中間デバイスは、このポートを使用するトラフィックを許可する必要があります。

---

- 5 vCenter Server が管理する IP アドレスが正しく設定されていることを確認します。詳細については、[Verifying the VMware vCenter Server Managed IP Address \(1008030\)](#)を参照してください。



- 6 vSphere Update Manager が正常に動作していることを確認します。vCenter Server 6.0U3 以降では、NSX のインストールとアップグレード手順で、ESX Agent Manager と共に vSphere Update Manager を利用しません。vCenter Server 6.0U3 以降を実行することをお勧めします。アップグレードできない場合は、vSphere Update Manager サービスが実行されていることを確認します。 [KB 2053782](#) の説明に従って、vSphere Update Manager バイパス オプションを設定できます。
- 7 vCenter Server のデプロイでデフォルト以外のポートを指定する場合は、これらのポートが ESXi ホストのファイアウォールでブロックされていないことを確認します。
- 8 vCenter Server `vpzd` プロセスが TCP ポート 8089 で待機していることを確認します。NSX Manager は、デフォルトのポート 8089 のみをサポートしています。

## vSphere ESX Agent Manager (EAM) について

vSphere ESX Agent Manager は、ESXi ホストの機能を拡張して vSphere ソリューションに必要な追加サービスを提供しながら、NSX ネットワークおよびセキュリティ サービスのデプロイと管理プロセスを自動化します。

### ESX Agent Manager のログとサービス

ESX Agent Manager のログは、vCenter Server のログ バンドルの一部に含まれています。

- Windows : C:\ProgramData\VMware\vCenterServer\logs\eam\eam.log
- VCSA : /var/log/vmware/vpx/eam.log
- ESXi : /var/log/esxupdate.log

### ESX Agent Manager のモニタリング

**重要：** NSX のインストールを開始する前に、必ず `bypassVumEnabled` フラグを **True** に変更し、インストール後は **False** に戻してください。 <https://kb.vmware.com/kb/2053782> を参照してください。

ESX Agent Manager のステータスを確認するには：

- 1 vSphere Web Client に移動します。
- 2 [管理 (Administration)] > [vCenter Server の拡張機能 (vCenter Server Extensions)] の順にクリックし、vSphere ESX Agent Manager をクリックします。
  - a [管理 (Manage)] タブをクリックします。
 

[管理 (Manage)] タブに、実行中のエージェンシーに関する情報と、親なしの状態のすべての ESX エージェントが表示され、ESX Agent Manager が管理する ESX エージェントに関する情報が記録されます。

エージェントとエージェンシーの詳細については、vSphere のドキュメントを参照してください。
  - b [監視 (Monitor)] タブをクリックします。
 

[イベント (Events)] - [監視 (Monitor)] タブの順に移動すると、ESX Agent Manager に関連するイベントの情報が表示されます。

## NSX Manager の問題のトラブルシューティング

お使いの環境で、各トラブルシューティングの手順が当てはまるかどうかを確認します。これらの手順を実行することで、可能性のある原因を排除し、必要に応じて適切なアクションを実行できます。ここでは、問題を切り分けて適切な解決策を特定するために最適な手順を記載しています。どの手順も省略しないでください。

## 問題

- VMware NSX Manager のインストールに失敗する。
- VMware NSX Manager のアップグレードに失敗する。
- VMware NSX Manager へのログインに失敗する。
- VMware NSX Manager へのアクセスに失敗する。

## 解決方法

- 1 問題に関するバグが最新のリリースで修正されているかどうかは、『NSX リリース ノート』で確認できます。
- 2 VMware NSX Manager をインストールする場合、最小システム要件を満たしていることを確認します。  
『NSX インストール ガイド』を参照してください。
- 3 NSX Manager で必要なすべてのポートが開いていることを確認します。  
『NSX インストール ガイド』を参照してください。
- 4 インストールの問題：
  - Lookup Service または vCenter Server の設定に失敗する場合、NSX Manager および Lookup Service アプライアンスの時刻が同期されていることを確認します。NSX Manager と Lookup Service の両方で同じ NTP サーバ設定を使用するようにします。DNS が正しく設定されていることも確認します。
  - OVA ファイルが正しくインストールされていることを確認します。NSX OVA ファイルをインストールできない場合、vSphere Client のエラー ウィンドウに、失敗が発生した場所が表示されます。また、ダウンロードした OVA/OVF ファイルの MD5 チェックサムも検証してください。
  - ESXi ホストの時刻が NSX Manager と同期していることを確認します。
  - NSX Manager のインストール後すぐに NSX Manager データのバックアップをスケジュール設定することをお勧めします。
- 5 アップグレードの問題：
  - アップグレードする前に、「製品の相互運用性マトリクス」のページで最新の相互運用性の情報を参照します。
  - アップグレード前に、現在の設定をバックアップし、テクニカル サポート ログをダウンロードすることをお勧めします。
  - NSX Manager のアップグレード後に vCenter Server との強制的な再同期する必要がある場合があります。これを行うには、NSX Manager Web インターフェイスの GUI にログインします。次に、[[vCenter Server 登録の管理 (Manage vCenter Registration)] > [NSX 管理サービス (NSX Management Service)] > [編集] (Edit)] の順に移動し、管理者ユーザーのパスワードを再入力します。
- 6 パフォーマンスの問題：
  - vCPU の最小要件が満たされていることを確認します。

- ルート (/) パーティションに十分な容量があることを確認します。これを確認するには、ESXi ホストにログインして `df -h` コマンドを入力します。

次はその例です。

```
[root@esx-01a:~] df -h
Filesystem      Size  Used Available Use% Mounted on
NFS             111.4G  80.8G    30.5G   73% /vmfs/volumes/ds-site-a-nfs01
vfat            249.7M  172.2M    77.5M   69% /vmfs/volumes/68cb5875-d887b9c6-a805-65901f83f3d4
vfat            249.7M  167.7M    82.0M   67% /vmfs/volumes/fe84b77a-b2a8860f-38cf-168d5dfe66a5
vfat            285.8M  206.3M    79.6M   72% /vmfs/volumes/54de790f-05f8a633-2ad8-00505603302a
```

- CPU およびメモリを大量に消費しているプロセスを確認するには、`esxtop` コマンドを使用します。
- NSX Manager のメモリ不足のエラーがログに記録されていた場合、`/common/dumps/java.hprof` ファイルが存在するかどうかを確認します。ファイルが存在する場合、ファイルのコピーを作成し、NSX テクニカル サポートのログ バンドルに含めます。
- 環境でストレージ遅延の問題が発生していないことを確認します。
- NSX Manager を別の ESXi ホストに移行します。

## 7 接続の問題：

- NSX Manager と vCenter Server または ESXi ホストとの間で接続の問題が発生している場合、NSX Manager の CLI コンソールにログインし、`debug connection IP_of_ESXi_or_VC` コマンドを実行して出力を確認します。
- Virtual Center Web 管理サービスが起動しており、ブラウザがエラーの状態でないことを確認します。
- NSX Manager Web ユーザー インターフェイス (UI) が更新されていない場合、Web サービスを無効にしてから再度有効にすると、この問題を解決できる場合があります。<https://kb.vmware.com/kb/2126701> を参照してください。
- NSX Manager が使用しているポート グループとアップリンク NIC を確認するには、ESXi ホストで `esxtop` コマンドを使用します。詳細については、<https://kb.vmware.com/kb/1003893> を参照してください。
- NSX Manager を別の ESXi ホストに移行します。
- vSphere Web Client で [監視 (Monitor)] タブの下にある [タスクとイベント (Tasks and Events)] タブを選択すると、NSX Manager 仮想マシンのアプライアンスを確認できます。
- NSX Manager と vCenter Server との間に接続の問題が発生している場合、vCenter Server の仮想マシンを実行している ESXi ホストに NSX Manager を移行できるかどうか試行して、基盤の物理ネットワークに問題がないことを確認します。

これは、両方の仮想マシンが同じ VLAN およびポート グループで実行されている場合にのみ有効です。

## NSX Manager と vCenter Server の接続

NSX Manager と vCenter Server を接続することで、NSX Manager は vSphere API を使用して、サービス仮想マシンのデプロイ、ホストの準備、論理スイッチ ポート グループの作成などの機能を実行できます。この接続プロセスでは、Web Client Server に NSX 用 Web クライアント プラグインがインストールされます。

接続には、NSX Manager、vCenter Server、および ESXi ホストに DNS と NTP が設定されている必要があります。vSphere インベントリに ESXi をホスト名で追加している場合は、NSX Manager で DNS サーバが構成されており、名前解決が機能していることを確認してください。機能していないと、NSX Manager は IP アドレスを解決できません。SSO サーバと NSX Manager の時間が同期するよう、NTP サーバを指定する必要があります。NSX Manager では、/etc/ntp.drift のドリフト ファイルは NSX Manager 用テクニカル サポート バンドルに含まれています。

NSX Manager を vCenter Server に接続するために使用するユーザー アカウントには、vCenter Server の「Administrator」ロールが割り当てられている必要があります。「Administrator」ロールが割り当てられることで、NSX Manager が Security Token Service サーバに登録できるようになります。特定のユーザー アカウントを使用して NSX Manager を vCenter Server に接続する場合、そのユーザーの Enterprise Administrator ロールが NSX Manager 上に作成されます。

### NSX Manager と vCenter Server の接続に関する一般的な問題

- NSX Manager、vCenter Server、または ESXi ホストで DNS が誤って設定されている。
- NSX Manager、vCenter Server、または ESXi ホストで NTP が誤って設定されている。
- NSX Manager を vCenter Server に接続するために、vCenter Server の Administrator ロールを持たないユーザー アカウントが使用されている。
- NSX Manager と vCenter Server 間のネットワーク接続の問題。
- NSX Manager のロールを持たないユーザー アカウントを使用して、vCenter Server にログインしている。

まず、NSX Manager と vCenter Server との接続に使用したユーザー アカウントを使用して、vCenter Server へログインする必要があります。その後、[ホーム (Home)] > [Networking and Security (Networking & Security)] > [NSX Manager] > [NSX Manager の IP (IP of NSX Manager)] > [管理 (Manage)] > [ユーザー (Users)] の順に移動して、NSX Manager でロールが付与された追加のユーザーを作成できます。

初回ログインでは、vCenter Server が NSX ユーザー インターフェイス バンドルを読み込んでデプロイするまでに、4 分ほどかかる場合があります。

### NSX Manager から vCenter Server への接続の検証

- NSX Manager CLI コンソールにログインします。
- 接続を検証するには、ARP とルーティング テーブルを確認します。

```
nsxmgr# show arp
```

IP address	HW type	Flags	HW address	Mask	Device
192.168.110.31	0x1	0x2	00:50:56:ae:ab:01	*	mgmt
192.168.110.2	0x1	0x2	00:50:56:01:20:a5	*	mgmt
192.168.110.1	0x1	0x2	00:50:56:01:20:a5	*	mgmt
192.168.110.33	0x1	0x2	00:50:56:ae:4f:7c	*	mgmt

192.168.110.32	0x1	0x2	00:50:56:ae:50:bf	*	mgmt
192.168.110.10	0x1	0x2	00:50:56:03:19:4e	*	mgmt
192.168.110.51	0x1	0x2	00:50:56:03:30:2a	*	mgmt
192.168.110.22	0x1	0x2	00:50:56:01:21:f9	*	mgmt
192.168.110.55	0x1	0x2	00:50:56:01:23:21	*	mgmt
192.168.110.26	0x1	0x2	00:50:56:01:21:ef	*	mgmt
192.168.110.54	0x1	0x2	00:50:56:01:22:ef	*	mgmt
192.168.110.52	0x1	0x2	00:50:56:03:30:16	*	mgmt

```
nsxmgr# show ip route
Codes: K - kernel route, C - connected, S - static,
       > - selected route, * - FIB route

S>* 0.0.0.0/0 [1/0] via 192.168.110.1, mgmt
C>* 192.168.110.0/24 is directly connected, mgmt
```

- NSX Manager ログで、vCenter Server に接続できない理由を示すエラーを探します。ログを表示するためのコマンドは `show log manager follow` です。

```
2014-02-26 12:53:23.815 GMT INFO VcEventsReaderThread DefaultRequestDirector:491 - I/O exception (org.apache.http.NoHttpResponseException: The target server failed to respond)
2014-02-26 12:53:23.815 GMT INFO VcEventsReaderThread DefaultRequestDirector:498 - Retrying request
2014-02-26 12:53:23.815 GMT WARN VmInventoryThread VmInventory:1482 - We received error from VC, probably lost connection
2014-02-26 12:53:23.817 GMT INFO VcEventsReaderThread VcEventsReader$VcEventsReaderThread:347 - Caught exception:com.vmware.vim.client.exception.ConnectionException: org.apache.http.conn.HttpHostConnectException: Connection to https://vc-1-01a.corp.local refused
2014-02-26 12:53:23.821 GMT DEBUG VcEventsReaderThread VcEventsReader$VcEventsReaderThread:348 - Caught exception during p
com.vmware.vim.vimoml.client.exception.ConnectionException: org.apache.http.conn.HttpHostConnectException: Connection to ht
```

- `debug connection IP_of_ESXi_or_VC` コマンドを実行して、出力を確認します。

## NSX Manager でのパケット キャプチャによる接続の表示

パケットのデバッグ用コマンド `debug packet [capture|display] interface interface filter` を実行します。

NSX Manager のインターフェイス名は `mgmt` です。

フィルタの構文は、「`port_80_or_port_443`」の形式に従います。

コマンドは、権限モードでのみ実行します。権限モードを使用するには、`enable` コマンドを実行して管理者パスワードを入力します。

パケット キャプチャの例：

```
nsxmgr# en
nsxmgr# debug packet display interface mgmt port_80_or_port_443
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on mgmt, link-type EN10MB (Ethernet), capture size 262144 bytes
23:40:25.321085 IP 192.168.210.15.54688 > 192.168.210.22.443: Flags [P.], seq 2645022162:2645022199,
ack 2668322748, win 244, options [nop,nop,TS val 1447550948 ecr 365097421], length 37
...
```

## NSX Manager でのネットワーク設定の検証

show running-config コマンドは、管理インターフェイス、NTP、およびデフォルトのルート設定の基本設定を表示します。

```
nsxmgr# show running-config
Building configuration...

Current configuration:
!
ntp server 192.168.110.1
!
ip name server 192.168.110.10
!
hostname nsxmgr
!
interface mgmt
 ip address 192.168.110.15/24
!
ip route 0.0.0.0/0 192.168.110.1
!
web-manager
```

## NSX Manager の証明書

NSX Manager では、次の 2 つの方法で証明書を生成できます。

- NSX Manager が生成する証明書署名要求：Basic CSR による機能制限あり
- PKCS#12：本番環境に推奨

証明書管理サービス (CMS) がエラー通知もなく、API 呼び出しに失敗する既知の問題があります。

この問題は、信頼されないルート認証局、または自己署名された証明書の場合、呼び出し側にとって証明書発行者が不明となるために発生します。この問題を解決するには、ブラウザから IP アドレスまたはホスト名を使用して NSX Manager にアクセスし、証明書を受け入れます。

## セカンダリ NSX Manager が移行モードで止まる

以下の問題で説明するように、セカンダリ NSX Manager が移行モードで止まる場合は、その後に示す解決策を使用してください。この問題は、セカンダリ NSX Manager が移行モードのときに、プライマリ NSX Manager でバックアップをリストアした場合に発生します。

### 問題

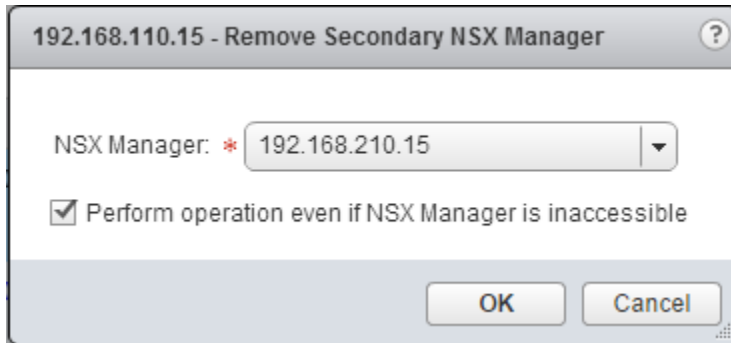
- 1 プライマリとセカンダリの NSX Manager を設定済みである。
- 2 プライマリ NSX Manager のバックアップを作成する。
- 3 その後、セカンダリ NSX Manager を削除する。セカンダリ NSX Manager が移行モードになる。
- 4 何らかの目的で、プライマリ NSX Manager でバックアップをリストアする。
- 5 データベースで、移行 NSX Manager が [セカンダリ (Secondary)] として更新されますが、ユーザー インターフェイスでは [移行 (Transit)] と表示され、同期に失敗する。

- 6 セカンダリ NSX Manager を削除できない、またはセカンダリとして再度昇格できない場合がある。
- 7 移行 NSX Manager を昇格中に、「IP アドレス/ホスト名を持つ NSX Manager ノードがすでに存在します」というエラー メッセージが表示される。
- 8 移行 NSX Manager を削除中に、「ユーザー名またはパスワードが正しくありません」というエラー メッセージが表示される。

#### 解決方法

- 1 vSphere Web Client を使用して、プライマリ NSX Manager にリンクされた vCenter Server にログインします。
- 2 [ホーム (Home)] - [Networking and Security (Networking & Security)]> [インストール手順 (Installation)] の順に移動し、[管理 (Management)] タブを選択します。
- 3 削除するセカンダリ NSX Manager を選択して [アクション (Actions)] をクリックし、[セカンダリ NSX Manager の削除 (Remove Secondary NSX Manager)] をクリックします。

確認のダイアログ ボックスが表示されます。



- 4 [NSX Manager にアクセスできない場合でも操作を実行 (Perform operation even if NSX Manager is inaccessible)] チェック ボックスを選択します。
- 5 [OK] をクリックします。  
セカンダリ NSX Manager がプライマリ データベースから削除されます。
- 6 セカンダリ NSX Manager を再度追加します。

#### 次のステップ

セカンダリ NSX Manager の追加に関する詳細については、『NSX インストール ガイド』を参照してください。

## NSX SSO Lookup Service の設定の失敗

#### 問題

- vCenter Server への NSX Manager の登録に失敗する
- SSO Lookup Service の設定に失敗する
- 次のエラーが表示される場合がある

```
nested exception is java.net.UnknownHostException: vc.local( vc.corp.local )
```

```
NSX Management Service operation failed.( Initialization of Admin Registration Service
Provider failed. Root Cause: Error occurred while registration of lookup service,
com.vmware.vim.sso.admin.exception.InternalError: General failure.
```

```
com.vmware.vshield.vsm.security.service.impl.SamlTokenSSOAuthenticator : SSO is not
configured or initialized properly so cannot authenticate user.
```

## 解決方法

### 1 接続の問題：

- NSX Manager と vCenter Server または ESXi ホストとの間で接続の問題が発生している場合、NSX Manager の CLI コンソールにログインし、`debug connection IP_of_ESXi_or_VC` コマンドを実行して出力を確認します。
- IP アドレスと 完全修飾ドメイン名 (FQDN) を使用して NSX Manager から vCenter Server に ping を送信し、ルーティングを確認します。あるいは、次のコマンドを使用して、スタティック ルートまたは動的 ルートを確認します。

```
nsxmgr-l-01a# show ip route
```

コード：

K – カーネル ルート

C – 接続

S – スタティック

> – 選択されたルート

\* – FIB ルート

```
S>* 0.0.0.0/0 [1/0] via 192.168.110.2, mgmt
```

```
C>* 192.168.110.0/24 is directly connected, mgmt
```

### 2 DNS の問題

FQDN を使用して次のコマンドを実行し、NSX Manager から vCenter Server に ping を送信します。

```
nsx-mgr> ping vc-l-01a.corp.local
```

次の例のような出力が表示されます。

```
nsx-mgr> ping vc-l-01a.corp.local
PING vc-l-01a.corp.local (192.168.110.51): 56 data bytes
64 bytes from 192.168.110.51: icmp_seq=0 ttl=64 time=1.749 ms
64 bytes from 192.168.110.51: icmp_seq=1 ttl=64 time=2.111 ms
64 bytes from 192.168.110.51: icmp_seq=2 ttl=64 time=8.082 ms
64 bytes from 192.168.110.51: icmp_seq=3 ttl=64 time=2.010 ms
64 bytes from 192.168.110.51: icmp_seq=4 ttl=64 time=0.857 ms
```



問題が解決しない場合には、NSX Manager で [管理(Manage)] > [ネットワーク(Network)] > [DNS サーバ (DNS Servers)] の順に移動し、DNS が正しく設定されていることを確認します。

### 3 ファイアウォールの問題

NSX Manager と vCenter Server 間にファイアウォールがある場合には、TCP/443 で SSL が有効になっていることを確認します。あるいは、ping を送信して接続を確認します。

### 4 NSX Manager で必要な次のポートが開いていることを確認します。

表 2-1. NSX Manager で開いているポート

ポート	目的
443/TCP	ESXi ホストへの OVA ファイルのダウンロード (デプロイ) REST API の使用 NSX Manager ユーザー インターフェイスの使用
80/TCP	vSphere SDK との接続の開始 NSX Manager と NSX ホスト モジュール間のメッセージング
1234/TCP	NSX Controller と NSX Manager 間の通信
5671	Rabbit MQ (メッセージング バス テクノロジー)
22/TCP	CLI へのコンソール アクセス (SSH) 注：デフォルトでは、このポートは閉じられています。

### 5 NTP の問題

vCenter Server と NSX Manager 間で時刻が同期されていることを確認します。同期するには、NSX Manager と vCenter Server で同じ NTP サーバの設定を使用します。

NSX Manager の時刻を確認するには、CLI から次のコマンドを実行します。

```
nsxmgr-l-01a# show clock
Tue Nov 18 06:51:34 UTC 2014
```

vCenter Server の時刻を確認するには、CLI で次のコマンドを実行します。

```
vc-l-01a:~ # date
```

次のような出力が表示されます。

```
Tue Nov 18 06:51:31 UTC 2014
```

注：時刻の設定後、アプライアンスを再起動します。

### 6 ユーザー権限の問題

ユーザーに **admin** 権限があることを確認します。

vCenter Server または SSO Lookup Service に登録するには、管理者権限が必要です。

デフォルトのアカウントは administrator user: administrator@vsphere.local です。

### 7 認証情報を入力して SSO に再接続します。

## 論理ネットワークの準備：VXLAN 転送

NSX は、VTEP VMkernel NIC 用の分散仮想ポート グループを作成することにより、VXLAN 用に選択された vSphere Distributed Switch を準備します。

VXLAN の設定で、VTEP のチーミング ポリシー、ロード バランシングの方法、MTU、VLAN ID が選択されます。チーミングとロード バランシングの方法は、VXLAN 用に選択された分散仮想スイッチの設定と一致する必要があります。

MTU は、少なくとも 1600 に設定する必要があります。分散仮想スイッチで設定されている値より低くしないでください。

作成される VTEP の数は、選択されたチーミング ポリシーと分散仮想スイッチの設定によって異なります。

### VXLAN の準備に関する一般的な問題

VXLAN の準備に失敗する場合、いくつかの理由が考えられます。

- VXLAN に選択されたチーミングの方法が、分散仮想スイッチがサポートする方法と一致しない。サポートされている方法については、<https://communities.vmware.com/docs/DOC-27683> で VMware NSX for vSphere Network Virtualization Design Guide を参照してください。
- VTEP に不正な VLAN ID が選択されている。
- VTEP の IP アドレスを割り当てるために DHCP が選択されているものの、DHCP サーバが利用できない。
- VMkernel NIC が見つからない。 [VXLAN VMkernel NIC が同期されない](#)の説明に従って、エラーを解決してください。
- VMkernel NIC の IP アドレスが不正である。<https://kb.vmware.com/kb/2137025> の説明に従って、エラーを解決してください。
- VTEP の MTU 設定が正しくない。このトピックの説明に従って、MTU の不一致があるかどうか確認する必要があります。
- 正しい VXLAN ゲートウェイが選択されていない。このトピックの説明に従って、VXLAN ゲートウェイの設定でエラーが発生していないかどうか確認する必要があります。

### 重要なポート番号

VXLAN UDP ポートは、UDP カプセル化で使用されます。NSX 6.2.3 より前のバージョンでは、デフォルトの VXLAN ポート番号は 8472 でした。NSX 6.2.3 では、新しいインストール環境でのデフォルトの VXLAN ポート番号が 4789 に変更されました。ハードウェア VTEP が使用される NSX 6.2 以降のインストール環境では、VXLAN ポート番号 4789 を使用する必要があります。VXLAN ポート設定の変更に関する詳細については、『NSX 管理ガイド』の「VXLAN ポートの変更」を参照してください。

### コントローラに接続するアクティブな仮想マシンがホストに含まれていない場合、制御プレーンのステータスが **disabled** と表示される

show logical-switch コマンドを使用して、ホストの VXLAN の詳細を確認します。詳細については、『NSX コマンドライン インターフェイス リファレンス』を参照してください。

コントローラ クラスタへ接続してテーブル情報を転送する必要がある仮想マシンがホストに配置されていない場合、`show logical-switch host hostID verbose` コマンドを使用すると、制御プレーンのステータスが *disabled* と表示されます。

```
Network count: 18
VXLAN network: 32003
Multicast IP: 0.0.0.0
Control plane: Disabled <<=====
MAC entry count: 0
ARP entry count: 0
Port count: 1
```

## VXLAN ゲートウェイの設定エラー

[Networking and Security (Networking & Security)] > [インストール手順 (Installation)] > [ホストの準備 (Host Preparation)] > [VXLAN の設定 (Configure VXLAN)] の順にクリックし、固定 IP アドレス プールを使用して VXLAN を設定する際、VTEP 上に IP アドレス プール ゲートウェイを設定できないと、ホスト クラスタの VXLAN 設定ステータスがエラー (赤) 状態になります。エラー メッセージは「ホスト上で VXLAN ゲートウェイを設定できません」、エラー ステータスは「VXLAN\_GATEWAY\_SETUP\_FAILURE」です。

REST API 呼び出し GET `https://<nsxmgr-ip>/api/2.0/nwfabric/status?resource=<cluster-moid>` では、VXLAN のステータスは次のようになります。

```
<nwFabricFeatureStatus>
<featureId>com.vmware.vshield.nsxmgr.vxlan</featureId>
  <featureVersion>5.5</featureVersion>
  <updateAvailable>false</updateAvailable>
  <status>RED</status>
  <message>VXLAN Gateway cannot be set on host</message>
  <installed>true</installed>
  <enabled>true</enabled>
  <errorStatus>VXLAN_GATEWAY_SETUP_FAILURE</errorStatus>
</nwFabricFeatureStatus>
```

回避策：このエラーの修正方法は次の 2 つがあります。

- Option 1：ホスト クラスタの VXLAN 設定を削除します。ゲートウェイが適切に設定されてアクセスできることを確認し、IP アドレス プール内で基盤となるゲートウェイのセットアップを修正した後、ホスト クラスタの VXLAN を再設定します。
- Option 2：次の手順を実行してください。
  - a IP アドレス プール内で使用されているゲートウェイを適切に設定し、ゲートウェイに確実にアクセスできるようにします。
  - b ホストをメンテナンス モードにして、ホスト上でアクティブになっている仮想マシン トラフィックがないことを確認します。
  - c VXLAN VTEP をホストから削除します。

- d ホストのメンテナンス モードを終了します。ホストのメンテナンス モードを終了すると、NSX Manager で VXLAN VTEP の作成プロセスがトリガされます。NSX Manager は、ホスト上で必要な VTEP の再作成を試みます。

## MTU の不一致の調査

- MTU が 1600 以上に設定されていることを確認するには、次のコマンドを実行します。

```
ping ++netstack=vxlan -d -s 1572 -I <vmkx hostname_or_IP>
```

*vmkx* は VMkernel ポートの ID、*hostname\_or\_IP* は VMkernel ポートの IP アドレスまたはホスト名です。

これにより、すべてのアップリンクが有効かどうか確認できます。マルチ VTEP 環境ですべてのアップリンクを検証するには、それぞれの VTEP VMkernel 送信元/宛先インターフェイスから ping コマンドを実行し、すべてのパスを検証します。

- 物理インフラストラクチャを確認します。多くの場合、物理インフラストラクチャ構成を変更することで問題を解決できます。
- この問題が 1 台の論理スイッチに限定されているのか、他の論理スイッチにも影響しているのかを確認します。この問題がすべての論理スイッチに影響しているかどうかを確認します。

MTU チェックの詳細については、NSX アップグレード ガイドの「NSX の動作状態の確認」を参照してください。

## VXLAN VMkernel NIC が同期されない

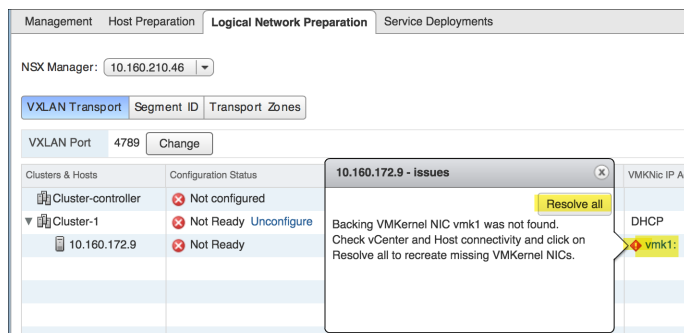
ホスト上の VMkernel NIC が削除されたにも関わらず、NSX に VMkernel NIC 情報が残っている場合、NSX Manager は削除された VMkernel NIC を [エラー (Error)] アイコンで示します。

### 前提条件

ホストで VMkernel NIC が削除されます。

### 手順

- 1 vSphere Web Client で、[Networking and Security (Networking & Security)] - [インストール手順 (Installation)] > [論理ネットワークの準備 (Logical Network Preparation)] の順に移動します。
- 2 [VXLAN 転送 (VXLAN Transport)] タブで、[ホストおよびクラスタ] を展開します。



- 3 [エラー (Error)] アイコンをクリックして、ホスト上で削除された VMkernel NIC の情報を表示します。
- 4 [すべてを解決 (Resolve All)] ボタンをクリックして、削除された VMkernel NIC を再作成します。

## 結果

削除された VMkernel NIC がホスト上で再作成されます。

## VXLAN チーミング ポリシーと MTU 設定の変更

VXLAN チーミング ポリシーと MTU 設定は、VXLAN が準備されたホストとクラスタ上で変更できますが、これらの変更は、VXLAN 用に新しいホストとクラスタを準備するときのみ適用されます。VTEP VMkernel の既存の仮想ポート グループを変更するには、ホストとクラスタを手動で再度準備する必要があります。チーミング ポリシーと MTU 設定は、API を使用して変更できます。

## 問題

VTEP の MTU 設定が正しくない。

## 解決方法

- 1 GET `https://<NSX-Manager-IP-Address>/api/2.0/vdn/switches` API を使用して、VXLAN で使用するすべてのスイッチに関する情報を取得します。

API の出力で、変更を加えるスイッチを探し、名前をメモします。例：*dvs-35*

- 2 名前をメモした vSphere Distributed Switch で、クエリを実行します。

例：GET `https://<NSX-Manager-IP-Address>/api/2.0/vdn/switches/dvs-35` API

次の例のような出力が表示されます。

```
<vdsContext>
<switch>
  <objectId>dvs-35</objectId>
  <objectTypeName>VmwareDistributedVirtualSwitch</objectTypeName>
  <vsmUuid>423A993F-BEE6-1285-58F1-54E48D508D90</vsmUuid>
  <nodeId>916287b3-761d-430b-8ab2-83878dfe3e7f</nodeId>
  <revision>6</revision>
  <type>
    <typeName>VmwareDistributedVirtualSwitch</typeName>
  </type>
  < name>vds-site-a</name>
  <scope>
    <id>datacenter-21</id>
    <objectTypeName>Datacenter</objectTypeName>
    < name>Datacenter Site A</name>
  </scope>
  <clientHandle/>
  <extendedAttributes/>
  <isUniversal>false</isUniversal>
  <universalRevision>0</universalRevision>
</switch>
<mtu>1600</mtu>
```

```
<teaming>FAILOVER_ORDER</teaming>
<uplinkPortName>Uplink 4</uplinkPortName>
<promiscuousMode>>false</promiscuousMode>
</vdsContext>
```

- 3 API 呼び出しを使用して、vSphere Distributed Switch でチーミング ポリシーや MTU などのパラメータを変更できます。次の例では、*dvs-35* のチーミング ポリシーを *FAILOVER\_ORDER* から *LOADBALANCE\_SRCMAC* に変更し、MTU を *1600* から *9000* に変更します。

■ NSX : PUT <https://<NSX-Manager-IP-Address>/api/2.0/vdn/switches>

次の例のような出力が表示されます。

```
<vdsContext>
<switch>
  <objectId>dvs-35</objectId>
  <objectTypeName>VmwareDistributedVirtualSwitch</objectTypeName>
  <vsmUuid>423A993F-BEE6-1285-58F1-54E48D508D90</vsmUuid>
  <nodeId>916287b3-761d-430b-8ab2-83878dfe3e7f</nodeId>
  <revision>6</revision>
  <type>
    <typeName>VmwareDistributedVirtualSwitch</typeName>
  </type>
  <name>vds-site-a</name>
  <scope>
    <id>datacenter-21</id>
    <objectTypeName>Datacenter</objectTypeName>
    <name>Datacenter Site A</name>
  </scope>
  <clientHandle/>
  <extendedAttributes/>
  <isUniversal>>false</isUniversal>
  <universalRevision>0</universalRevision>
</switch>
<mtu>9000</mtu>
```

```
<teaming>LOADBALANCE_SRCMAC</teaming>
<uplinkPortName>Uplink 4</uplinkPortName>
<promiscuousMode>>false</promiscuousMode>
</vdsContext>
```

**注：** <teaming> パラメータに有効なチーミング ポリシーのエントリは次のとおりです。

- FAILOVER\_ORDER
- ETHER\_CHANNEL
- LACP\_ACTIVE
- LACP\_PASSIVE
- LOADBALANCE\_LOADBASED
- LOADBALANCE\_SRCID
- LOADBALANCE\_SRCMAC LACP\_V2

- 4 GET コマンドを使用して、使用している構文が正しく、処理中の vSphere Distributed Switch で変更がアクティブになっていることを確認します。例：GET https://<NSX-Manager-IP-Address>/api/2.0/vdn/switches/dvs-35
- 5 vSphere Web Client を開き、設定の変更が反映されていることを確認します。

## 論理スイッチのポート グループが同期されない問題

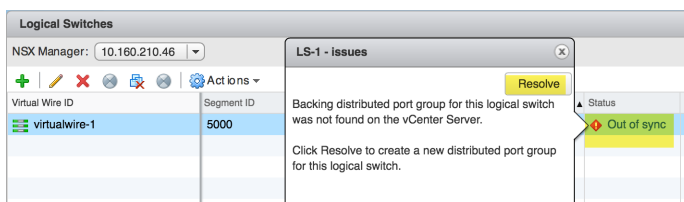
論理スイッチのバックアップ分散仮想ポート グループ (DVPG) が vCenter Server で削除されると、[論理スイッチ (Logical Switches)] ページの [ステータス] 列が [同期なし (Out of sync)] ステータスになります。

### 前提条件

vCenter Server で論理スイッチの DVPG が削除されています。

### 手順

- 1 vSphere Web Client で、[ホーム (Home)] - [ネットワークとセキュリティ (Networking & Security)] > [論理スイッチ (Logical Switches)] の順に移動します。



- 2 [ステータス] 列で、[同期なし (Out of sync)] リンクをクリックして、この非同期状態の詳しい原因を確認します。
- 3 [解決 (Resolve)] ボタンをクリックして、問題を解決します。

## 結果

これにより、バックアップ DVPG を再作成する API が呼び出されます。



# NSX のルーティングのトラブルシューティング

## 3

NSX には 2 つのルーティング サブシステムが含まれ、2 つのキーのニーズ合うよう最適化されています。

NSX のルーティング サブシステムは、次のとおりです。

- 論理空間内のルーティング。「内部」のルーティングとも呼ばれ、分散論理ルーターにより提供されます。
- 物理空間と論理空間の間でのルーティング。「アップリンク」のルーティングとも呼ばれ、Edge Services Gateway (ESG) により提供されます。

どちらも、水平方向の拡張オプションを提供します。

内部の分散ルーティングは、分散論理ルーターを介して拡張できます。

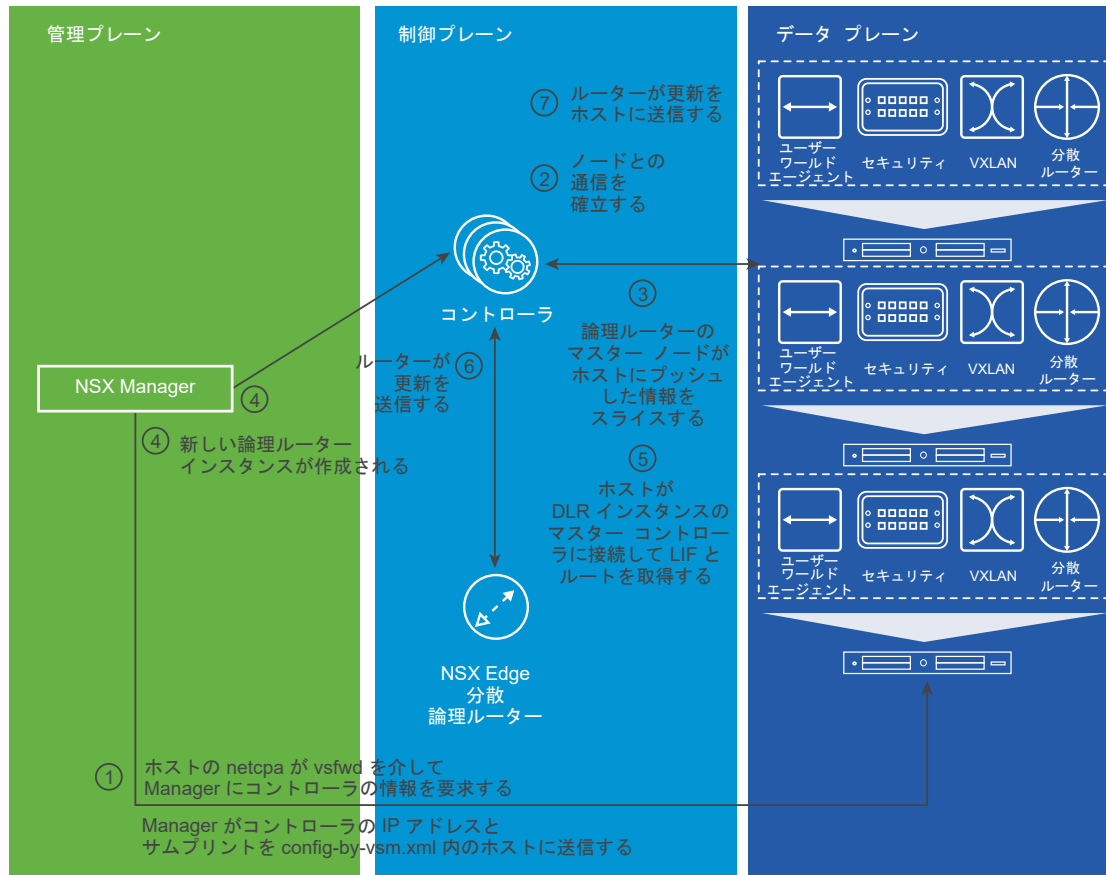
分散論理ルーターで一度に実行できるのは 1 つの動的ルーティング プロトコル (OSPF または BGP) ですが、ESG では両方のプロトコルを同時に実行できます。これは、分散論理ルーターが 1 つの出力パスを使用する「スタブ」ルーターとして機能するように設計され、より高度なルーティング設定が通常は必要とされないためです。

分散論理ルーターと ESG は両方とも、固定および動的ルートの組み合わせの使用をサポートします。

分散論理ルーターと ESG は両方とも、ECMP ルートをサポートします。

両方とも L3 ドメインの分離を提供し、分散論理ルーターまたは Edge Services Gateway の各インスタンスは L3VPN VRF に類似する独自の L3 設定を使用します。

図 3-1. 分散論理ルーターの作成



この章には、次のトピックが含まれています。

- 分散論理ルーターの理解
- Edge Services Gateway によって提供されるルーティングの理解
- ECMP パケット フロー
- NSX のルーティングの前提条件と考慮事項
- 分散論理ルーター (DLR) と Edge Services Gateway (ESG) のユーザー インターフェイス
- 新しい NSX Edge (分散論理ルーター)
- 一般的な ESG および分散論理ルーター ユーザー インターフェイスの操作
- NSX のルーティングのトラブルシューティング

## 分散論理ルーターの理解

分散論理ルーターは、VXLAN または VLAN でバックアップされるポートグループ上の仮想マシン間の論理領域での転送のために最適化されています。

分散論理ルーターには、次のプロパティがあります。

- 高パフォーマンス、低オーバーヘッドのファーストホップ ルーティング：

- ホスト数に合わせて直線的に拡張
- アップリンクで 8 ウェイ ECMP をサポート
- ホストあたり最大 1,000 の分散論理ルーター インスタンス
- 各分散論理ルーターで最大 999 の論理インターフェイス (LIF) (8 x アップリンク + 991 の内部) + 管理 x 1
- ホストあたり 10,000 の LIF をすべての分散論理ルーター インスタンスで分散 (NSX Manager によって強制されません)

次の点に注意してください。

- いずれの VLAN や VXLAN にも 複数の分散論理ルーターを接続できません。
- 各分散論理ルーターでは複数のルーティング プロトコルを実行できません。
- OSPF が使用されている場合、複数の分散論理ルーター アップリンクで OSPF を実行できません。
- VXLAN と VLAN 間をルーティングするには、トランスポート ゾーンが 1 つの分散仮想スイッチにかかっている必要があります。

上位レベルでの分散論理ルーターの設計は、次の点で、モジュール化されたルーター筐体に似ています。

- ESXi ホストは、ライン カードと同じように動作します。
  - ポートを実装し、エンド ステーション (仮想マシン) に接続します。
  - ここで転送に関する決定を行います。
- 分散論理ルーター制御仮想マシンは、ルータ プロセッサ エンジンのように動作します。
  - 動的ルーティング プロトコルを実行し、ルーティング情報をネットワークの他の部分と交換します。
  - インターフェイスの設定、スタティック ルート、動的ルーティング情報を基準として「ライン カード」のフォワーディング テーブルを計算します。
  - これらのフォワーディング テーブルを「ライン カード」にプログラミングします (拡張性と復元性を向上するために、コントローラ クラスタを介して)。
- ESXi ホストを相互に接続する物理ネットワークは、バックプレーンのように動作します。
  - VLAN または VXLAN でカプセル化されたデータを「ライン カード」間で運搬します。

## 上位レベルの分散論理ルーター パケット フロー

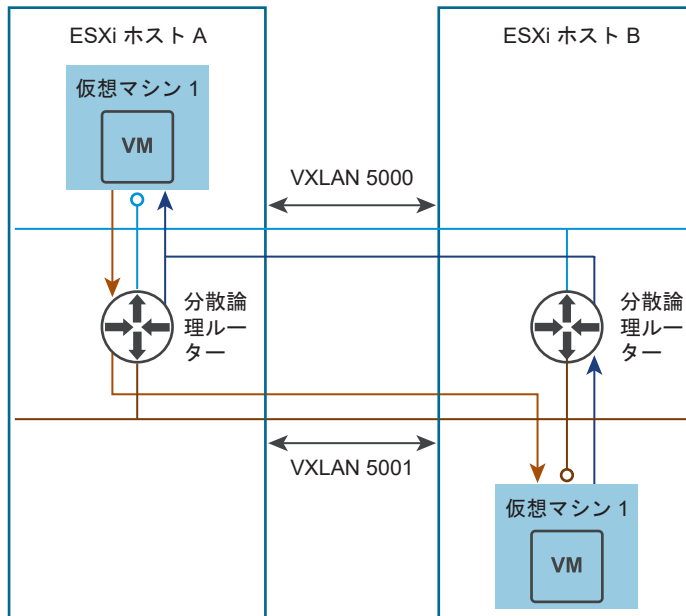
ESXi ホストには、設定済みの各分散論理ルーター インスタンスのコピーがそれぞれ関連付けられます。各分散論理ルーター インスタンスは、パケットを転送するために必要な情報を含む独自のテーブル セットが関連付けられます。この情報は、この分散論理ルーター インスタンスが存在するすべてのホスト間で同期されます。異なるホスト間の個々の分散論理ルーターのインスタンスに、正確に同じ情報が関連付けられます。

ルーティングは、ソース仮想マシンが実行されている同じホストにある分散論理ルーター インスタンスによって常に処理されます。つまり、送信元と宛先仮想マシンが異なるホストにある場合、これらの仮想マシン間でルーティングを実行する分散論理ルーター インスタンスは、送信元仮想マシンから宛先仮想マシンに送信されるパケットのみを見ることができます。宛先仮想マシンのホストにある同じ分散論理ルーターの一致するインスタンスだけが、リターントラフィックを見ることができます。

分散論理ルーターがルーティングを完了した後で、送信元と宛先仮想マシンが異なるホストにある場合には、最終的なターゲットへの配信は、L2 – VXLAN または VLAN を介して分散仮想スイッチによって実行され、これらが同じホストにある場合には分散仮想スイッチによってローカルで実行されます。

図 3-2. 上位レベルの分散論理ルーター パケット フロー は、異なるホスト上で実行され、異なる 2 つの論理スイッチ VXLAN 5000 と VXLAN 5001 に接続する VM1 と VM2 の 2 台の仮想マシン間のデータ フローを示します。

図 3-2. 上位レベルの分散論理ルーター パケット フロー



パケット フロー (ARP 解決は省略) :

- 1 VM1 が VM2 にパケットを送信します。このとき、VM2 のサブネット (またはデフォルト) 用に VM1 が使用するゲートウェイが宛先となります。このゲートウェイは、分散論理ルーターの VXLAN 5000 LIF です。
- 2 ESXi ホスト A の分散仮想スイッチは、このホストの分散論理ルーターにパケットを送信し、ここでルックアップが実行され、出力方向の LIF が決定されます (この場合は、VXLAN 5001 LIF)。
- 3 次に、パケットはターゲット LIF から送信されます。この場合、基本的にはパケットは分散仮想スイッチに戻されますが、異なる論理スイッチ (5001) が使用されます。
- 4 次に、分散仮想スイッチは L2 を介してターゲット ホスト (ESXi ホスト B) にパケットを配信します。ここでは、分散仮想スイッチが VM2 にパケットを転送します。

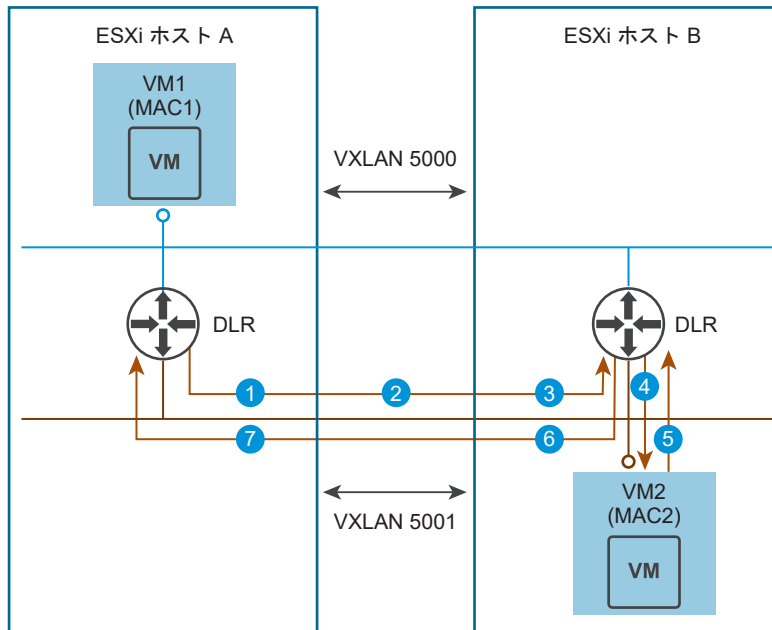
リターン トラフィックも同じ順序で処理され、VM2 からのトラフィックは ESXi ホスト B の分散論理ルーター インスタンスに転送され、VXLAN 5000 の L2 を介して配信されます。

## 分散論理ルーター ARP の解決プロセス

VM1 のトラフィックが VM2 に到着する前に、分散論理ルーターは VM2 の MAC アドレスを特定しておく必要があります。VM2 の MAC アドレスを特定したら、分散論理ルーターは送信パケットの正しい L2 ヘッダーを作成できます。

図 3-3. 分散論理ルーター ARP プロセス は、分散論理ルーターの ARP 解決のプロセスを示しています。

図 3-3. 分散論理ルーター ARP プロセス



MAC アドレスを特定するために、分散論理ルーターは次のように動作します。

- 1 ホスト A の分散論理ルーター インスタンスが、SRC MAC = vMAC および DST MAC = Broadcast の ARP 要求パケットを生成します。ホスト A の VXLAN モジュールは、出力方向の VXLAN 5001 ですべての VTEP を検出し、そのブロードキャスト フレームのコピーをそれぞれに送信します。
- 2 VXLAN カプセル化プロセスでフレームがホストから送信されると、SRC MAC が vMAC から pMAC A に変更されるため、リターン トラフィックはホスト A の送信元分散論理ルーター インスタンスを見つけることができます。この時フレームは、SRC MAC = pMAC A および DST MAC = Broadcast になります。
- 3 フレームはホスト B で受信され、カプセル化が解除されますが、このときの検証で、VXLAN 5001 のローカル分散論理ルーター インスタンスの LIF と一致する IP アドレスが送信元であると認識されます。これにより、フレームに `abrequest` のフラグが設定され、プロキシ ARP 機能が実行されます。DST MAC が Broadcast から vMAC に変更され、フレームはローカル分散論理ルーター インスタンスに到達できるようになります。
- 4 ホスト B のローカル分散論理ルーター インスタンスは、SRC MAC = pMAC A、DST MAC = vMAC の ARP 要求フレームを受信し、これを要求する自分の LIF IP アドレスを確認します。このインスタンスは、SRC MAC を保存し、SRC MAC = vMAC、DST MAC = Broadcast の新しい ARP 要求パケットを生成します。このフレームは、dvUplink を介してフラッドされないように「DVS Local」とタグ付けされます。分散仮想スイッチ (DVS) は、フレームを VM2 に配信します。
- 5 VM2 は、SRC MAC = MAC2、DST MAC = vMAC の ARP リプライを送信します。分散仮想スイッチは、これをローカル分散論理ルーター インスタンスに配信します。
- 6 ホスト B の分散論理ルーター インスタンスは、DST MAC を手順 4 で保存された pMAC A と置き換え、分散仮想スイッチにパケットを返送して、ホスト A に再配信します。
- 7 ARP リプライがホスト A に到着した後は、DST MAC は vMAC に変更され、SRC MAC = MAC2 と DST MAC = vMAC の ARP リプライ フレームは、ホスト A の分散論理ルーター インスタンスに到着します。

ARP 解決プロセスは完了し、ホスト A の分散論理ルーターは、VM2 へのトラフィックの送信を開始できます。

## 分散論理ルーターの ARP 抑制

アドレス解決プロトコル (ARP) 抑制とは、同じ論理スイッチに接続されている仮想マシン間の個々の VXLAN セグメント内で、ARP ブロードキャスト フラッドの量を低減するための手法です。

VM1 が VM2 の MAC アドレスを確認するときに、ARP 要求を送信します。この ARP 要求が論理スイッチによって傍受されます。論理スイッチに宛先の ARP エントリがある場合、仮想マシンに ARP 応答が送信されます。

エントリがない場合は、NSX Controller に ARP クエリを送信します。コントローラが仮想マシンの IP アドレスと MAC アドレスのバインディングを認識している場合、コントローラがバインディング情報を返し、論理スイッチが ARP 応答を送信します。コントローラに ARP エントリがない場合、論理スイッチで ARP 要求が再度ブロードキャストされます。NSX Controller は、ARP 要求/DHCP パケットをスヌーピングするスイッチ セキュリティ モジュールから MAC アドレスを取得します。

ARP 抑制が拡張され、分散論理ルーター (DLR) でも機能するようになりました。

- 分散論理ルーターからの ARP 要求は、他の仮想マシンからの ARP 要求と同様に処理され、抑制の対象となります。分散論理ルーターが宛先 IP アドレスの ARP 要求を解決するときに、コントローラが IP アドレスと MAC アドレスのバインディングを認識している場合、論理スイッチが ARP 要求を抑制し、フラッドを抑制します。
- LIF が作成されると、分散論理ルーターが論理スイッチに LIF IP アドレスの ARP エントリを追加します。これにより、論理スイッチが LIF IP アドレスの ARP 要求も抑制します。

## Edge Services Gateway によって提供されるルーティングの理解

NSX ルーティングのセカンドサブシステムは、Edge Services Gateway によって提供されます

ESG は基本的に仮想マシン内のルーターです。アプライアンスのように 4 つのサイズのフォームファクタを利用でき、NSX Manager によってライフサイクル全体が管理されます。ESG は主に、境界ルーターとして使用され、複数の分散論理ルーター間および物理的な環境と仮想ネットワーク間にデプロイされます。

ESG には、次のプロパティがあります。

- 各 ESG には最大で 10 個の vNIC インターフェイスまたは 200 個のトランク サブインターフェイスを関連付けることができます。
- 各 ESG は、バスの冗長化と拡張性のために、8 ウェイ ECMP をサポートします。

## ECMP パケット フロー

物理環境で 2 ウェイ ECMP アップリンクを使用して分散論理ルーター インスタンスを提供するために 2 つの ESG がデプロイされているとしましょう。

**図 3-4. ECMP が使用される場合の上位レベルの ESG と分散論理ルーター パケット フロー** は、ECMP (等コスト マルチパス) ルーティングが ESG と物理インフラストラクチャ間で有効である場合の、ESG と分散論理ルーター パケット フローを示しています。

このように、VM1 は単一の ESG のデプロイ環境と比較して、2 倍の双方向のスループットでアクセスできます。

VM1 は、VNI 5000 によって論理スイッチに接続されます。

分散論理ルーターには VNI 5000 の内部および VNI 5001 のアップリンクの 2 つの LIF があります。

分散論理ルーターでは ECMP が有効になっており、動的ルーティング プロトコル (BGP または OSPF) を介して ESG のペア (ESG A および ESG B) から VLAN 20 の IP アドレス サブネットへ等コスト ルートを受信します。

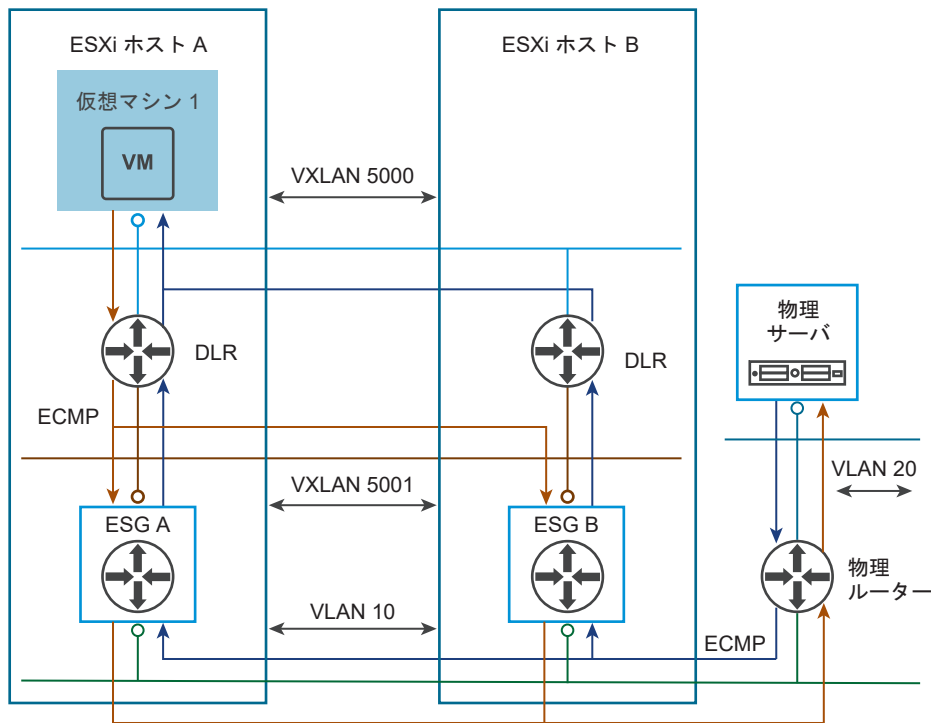
2 つの ESG は、VLAN 10 に関連付けられている VLAN でバックアップされる dvPortgroup に接続されます。

VLAN 10 では、VLAN 20 に接続する物理ルーターも接続されます。

ESG は、物理ルーターの動的ルーティング プロトコルを介して、VLAN 20 の外部ルートを受信します。

代わって、物理ルーターは両方の ESG の VXLAN 5000 に関連付けられている IP サブネットを取得し、そのサブネットにある仮想マシンへのトラフィックについて ECMP ロード バランスを実行します。

図 3-4. ECMP が使用される場合の上位レベルの ESG と分散論理ルーター パケット フロー



分散論理ルーターは、最大で 8 つの等コスト ルートを受信して、ルート間でトラフィックをバランシングすることが可能です。図の ESG A と ESG B は、2 つの等コスト ルートを提供します。

ESG は、物理ネットワークに対して ECMP ルーティングを実行できます (複数の物理ルータが存在していると仮定)。図を簡潔にするため、ここでは 1 台の物理ルーターを表示しています。

すべての分散論理ルーター LIF は、ESG が存在する同じホストで「ローカル」となっているため、分散論理ルーターに対して ESG で ECMP を設定する必要はありません。分散論理ルーターで複数のアップリンク インターフェイスを設定しても、さらにメリットを得ることはできません。

内部の帯域幅を増やす必要がある場合は、複数の ESG を異なる ESXi ホストに配置し、8 つの ESG を使用して 80 Gbps まで拡張できます。

**ECMP パケット フロー (ARP 解決を含まない) :**

- 1 VM1 は、物理サーバにパケットを送信します。パケットは、ESXi ホスト A にある VM1 の IP アドレス ゲートウェイ (分散論理ルーターの LIF) に送信されます。
- 2 分散論理ルーターは、物理サーバの IP アドレスについてルートを検索し、直接接続されていないことを確認しますが、ESG A と ESG B から受信した 2 つの ECMP ルートを一致させます。
- 3 分散論理ルーターは、ECMP ハッシュを計算し、ネクスト ホップ (ESG A または ESG B のいずれか) を決定し、パケットを VXLAN 5001 LIF から送信します。
- 4 分散仮想スイッチは、選択された ESG にパケットを送信します。
- 5 ESG は、ルーティングを検索し、ESG のインターフェイスのいずれかに直接接続する VLAN 10 にある物理ルーターの IP アドレスから物理サーバのサブネットにアクセスできることを確認します。
- 6 パケットは、分散仮想スイッチを介して送信されます。VLAN ID 10 の正しい 801.Q タグを関連付けた後に、物理ネットワークにパケットが渡されます。
- 7 パケットは、物理的なスイッチ インフラストラクチャを通過して、物理ルーターに到着します。物理ルーターはルックアップを実行し、物理サーバが VLAN 20 にインターフェイスに直接接続しているかを確認します。
- 8 物理ルーターは、パケットを物理サーバに送信します。

**反対方向のパケット フロー :**

- 1 物理サーバが、パケットを VM1 に送信します。このとき、物理ルーターがネクスト ホップになります。
- 2 物理ルーターが、VM1 のサブネットのルックアップを実行し、ネクスト ホップがあるサブネットへの 2 つの等コストパスである、ESG A と ESG B の VLAN 10 インターフェイスをそれぞれ確認します。
- 3 物理ルーターは、いずれかのパスを選択して、一致する ESG に対してパケットを送信します。
- 4 物理ネットワークは、ESG が存在する ESXi ホストにパケットを送信し、分散仮想スイッチに送信します。分散仮想スイッチはパケットのカプセル化を解除して、VLAN 10 が関連付けられている dvPortgroup で ESG に転送します。
- 5 ESG は、ルーティング ルックアップを実行し、分散論理ルーターのアップリンク インターフェイスの IP アドレスとなっているネクスト ホップがある VXLAN 5001 に関連付けられているインターフェイスを介して、VM1 のサブネットにアクセスできることを確認します。
- 6 ESG は、ESG と同じホストにある分散論理ルーター インスタンスにパケットを送信します。
- 7 分散論理ルーターは、ルーティング ルックアップを実行し、VM1 がその VXLAN 5000 LIF を介してアクセスできることを確認します。
- 8 分散論理ルーターは、VXLAN 5000 LIF から分散仮想スイッチにパケットを送信し、分散論理ルーターが最終的にパケットを配信します。

**NSX のルーティングの前提条件と考慮事項**

分散論理ルーターと ESG は分散仮想スイッチを使用して、dvPortgroup (VXLAN ベースおよび VLAN ベースの両方) の L2 フォワーディング サービスを提供し、End-to-End の接続を可能にします。

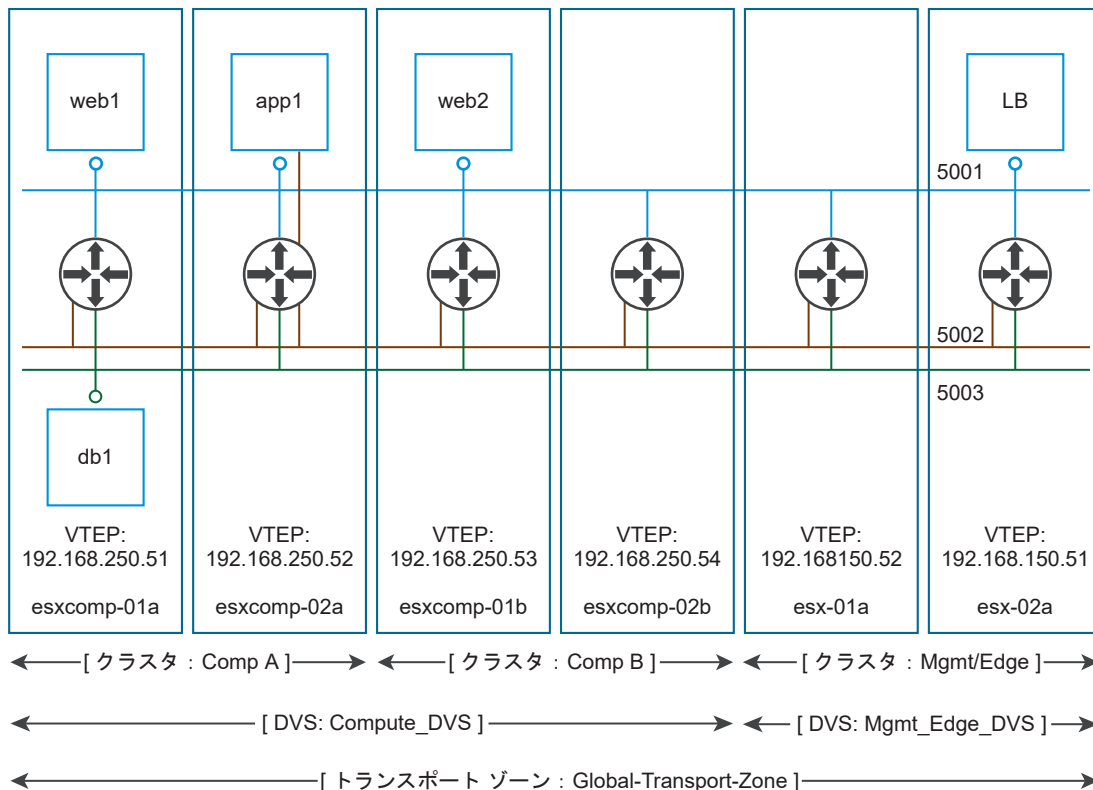


つまり、分散論理ルーターまたは ESG に接続される L2 フォワーディング サービスが設定され、動作している必要があります。NSX のインストール プロセスでは、これらのサービスは [ホストの準備] および [論理ネットワークの準備] を使用して提供されます。

マルチクラスタ分散仮想スイッチ設定でトランスポート ゾーンを作成する場合、選択した分散仮想スイッチ内のすべてのクラスタがトランスポート ゾーンに含まれていることを確認します。これにより、分散仮想スイッチの dvPortgroup が使用可能なすべてのクラスタで、分散論理ルーターを使用できるようになります。

すべてのトランスポート ゾーンが分散仮想スイッチの境界に一致していれば、分散論理ルーター インスタンスが正しく作成されます。

図 3-5. トランスポート ゾーンと分散仮想スイッチの境界が一致する場合



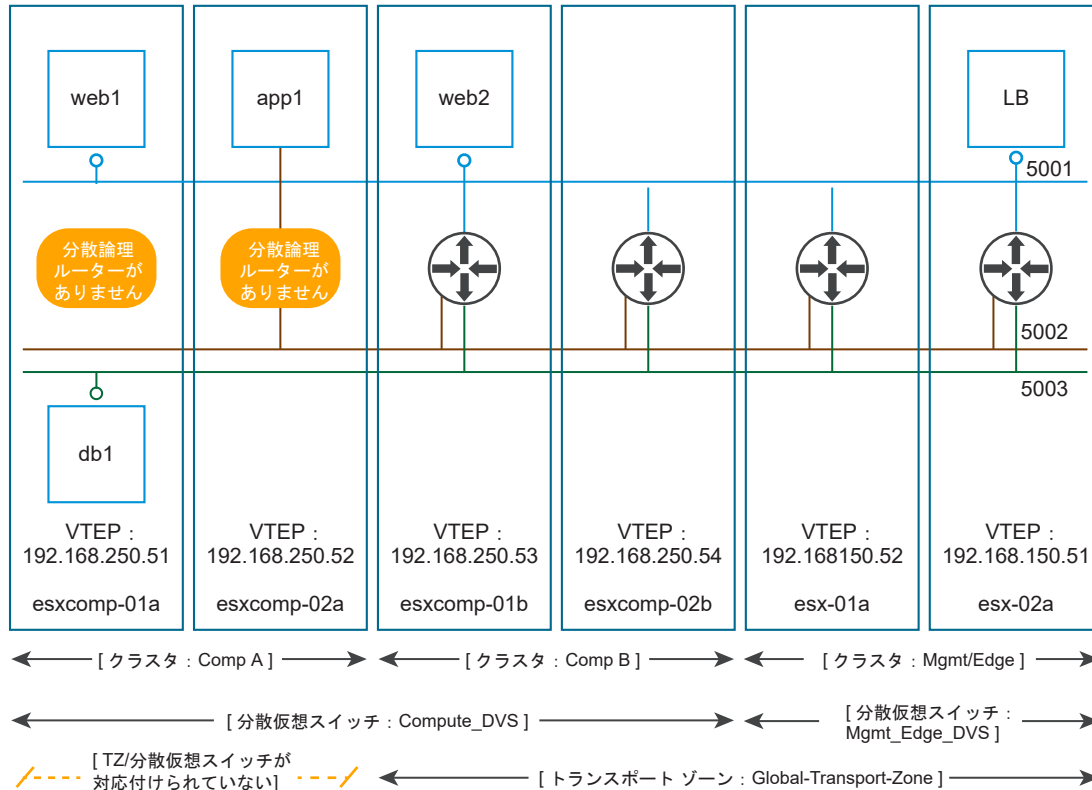
トランスポート ゾーンが分散仮想スイッチの境界と一致していないと、論理スイッチ (5001、5002、5003) とそれらの論理スイッチが接続される分散論理ルーター インスタンスの範囲の結合が解除されて、クラスタ Comp A 内の仮想マシンが分散論理ルーターの LIF にアクセスできなくなります。

上記の図では、Compute\_DVS という分散仮想スイッチの範囲に Comp A と Comp B の 2 つのクラスタが含まれます。Global-Transport-Zone には、Comp A と Comp B の両方が含まれます。

したがって、論理スイッチ (5001、5002、5003) と、これらの論理スイッチが存在するすべてのクラスタのすべてのホストで作成された分散論理ルーター インスタンスの範囲が正しく一致します。

次の例では、トランスポート ゾーンの設定にクラスタ Comp A が含まれていません。

図 3-6. トランスポート ゾーンと分散仮想スイッチの境界が一致しない場合



この例では、クラスター Comp A で実行される仮想マシンには、すべての論理スイッチへの完全なアクセス権限があります。これは、論理スイッチがホストの dvPortgroup により示され、dvPortgroup が分散仮想スイッチ全体で構築されているためです。サンプルの環境では、Compute\_DVS の範囲には Comp A と Comp B の両方が含まれます。

しかし、分散論理ルーター インスタンスはトランスポート ゾーンの範囲に厳密に一致するように作成されています。つまり、分散論理ルーター インスタンスは Comp A のホストでは作成されません。

このため、仮想マシン web1 は、同じ論理スイッチ上の仮想マシン web2 と仮想マシン LB にアクセスできますが、仮想マシン app1 と仮想マシン db1 は通信できません。

ESG と異なり、分散論理ルーターはコントローラ クラスタを使用することによって機能します。分散論理ルーター設定を作成または変更する前に、コントローラ クラスタが稼動していて、使用可能であることを確認します。

分散論理ルーターを VLAN dvPortgroup に接続する場合は、分散論理ルーター VLAN ベースの ARP プロキシが機能するよう、分散論理ルーターが設定されている ESXi ホストが UDP/6999 で相互にアクセスできるようにします。

考慮事項：

- 分散論理ルーター インスタンスは、異なるトランスポート ゾーンにある論理スイッチには接続できません。これは、すべての論理スイッチと分散論理ルーター インスタンスを確実に一致させるためです。
- 分散論理ルーターが複数の分散仮想スイッチにわたる論理スイッチに接続されている場合、VLAN がバックグランドのポートグループにその分散論理ルーターを接続することはできません。これはホスト全体で、論理スイッチと dvPortgroup に分散論理ルーター インスタンスを正確に一致させるためです。

- 分散論理ルーター制御仮想マシンの配置場所を選択する際、アップストリーム ESG が同じクラスタに存在する場合は、DRS の非アフィニティ ルールを使用して、1 つ以上のアップストリーム ESG と同じホストに配置しないようにします。これによって、ホストの分散論理ルーター フォワーディングで障害が発生した場合の影響を低減できます。
- OSPF を有効にできるアップリンクは 1 つだけです（ただし、複数の隣接関係はサポートされます）。逆に、BGP は必要に応じて複数のアップリンク インターフェイスで有効にすることができます。

## 分散論理ルーター (DLR) と Edge Services Gateway (ESG) のユーザー インターフェイス

分散論理ルーターと ESG のユーザー インターフェイスでは、システムの稼動状況のインジケータが提供されています。

### NSX のルーティング用ユーザー インターフェイス

vSphere Web Client ユーザー インターフェイスは、NSX のルーティングに関連して主に 2 つのセクションを提供します。

これらのセクションには、L2 および制御プレーン インフラストラクチャの依存関係や、ルーティング サブシステムの設定が含まれます。

NSX の分散ルーティングでは、コントローラ クラスタにより提供される機能が必要とされます。次のスクリーンショットは、健全な状態のコントローラ クラスタを示しています。

NSX Controller nodes

Name	Controller Node	NSX Manager	Managed By	DNS Name	Status	Peers	Software Version
	192.168.110.31 controller-1	192.168.110.15	192.168.110.15		✓ Connected		6.2.46893
	192.168.110.32 controller-2	192.168.110.15	192.168.110.15		✓ Connected		6.2.46893
	192.168.110.33 controller-3	192.168.110.15	192.168.110.15		✓ Connected		6.2.46893

注：

- 3 台のコントローラがデプロイされています。
- すべてのコントローラの [ステータス] は [接続済み] です。
- すべてのコントローラのソフトウェア バージョンは同一です。
- 各コントローラ ノードは 2 つのピアを持ちます。

分散ルーティングのホスト カーネル モジュールは、ホストの VXLAN 設定の一部としてインストールおよび構成されます。つまり、分散ルーティングのためには、ESXi ホストが準備され、ESXi ホストで VXLAN が設定されている必要があります。

Clusters & Hosts	Installation Status	Firewall	VXLAN
▶ Compute Cluster A	✓ 6.2.3.3771501	✓ Enabled	✓ Configured
▶ Management & Edge Cluster	✓ 6.2.3.3771501	✓ Enabled	✓ Configured

注：

- [インストールの状態] は緑色で表示されています。
- [VXLAN] は [構成済み] です。

VXLAN の転送コンポーネントが設定されていることを確認します。

VXLAN Transport		Segment ID	Transport Zones				
Clusters & Hosts	Configuration Status	Switch	VLAN	MTU	VMKNic IP Addressing	Teaming Policy	VTEP
▼ Compute Cluster A	✓ Unconfigure	vds-site-a	0	1600	IP Pool	Fail Over	1
esx-02a.corp.local	✓ Ready				vmk3: 192.168.130.51		
esx-01a.corp.local	✓ Ready				vmk3: 192.168.130.52		
▼ Management & Edge	✓ Unconfigure	vds-mgt-edge	0	1600	IP Pool	Fail Over	1
esxmgmt-02a.corp.l	✓ Ready				vmk3: 192.168.120.52		
esxmgmt-01a.corp.l	✓ Ready				vmk3: 192.168.120.51		

注：

- VTEP の転送 VLAN 用として VLAN ID が正しくなければなりません。上記のスクリーンショットでは、「0」となっています。実際の環境では、このようには表示されません。
- MTU の設定は 1600 以上になります。仮想マシンの MTU も 9000 に設定されることを期待して、この MTU を 9000 にしないでください。分散仮想スイッチの最大 MTU 数は 9000 であり、仮想マシンでも 9000 に設定されていると、VXLAN ヘッダー用の容量がありません。
- VMKNic のアドレスは正確でなければなりません。このアドレスが 169.254.x.x に設定されていないことを確認してください。このように設定されていると、ノードは DHCP からのアドレスの取得に失敗します。
- 同一分散仮想スイッチのすべてのクラスターメンバーで、一貫するチームングポリシーを使用する必要があります。
- VTEP の数は、dvUplink の数と同じである必要があります。予想どおりの有効な IP アドレスが表示されていることを確認します。

一部のクラスターで分散論理ルーターが検出されないという状況が起きないように、トランスポートゾーンが分散仮想スイッチの境界に一致している必要があります。

Name	NSX vSwitch	Status
Compute Cluster A	vds-site-a	✓ Normal
Management & Edge ...	vds-mgt-edge	✓ Normal

## NSX Edge ユーザー インターフェイス

NSX のルーティングサブシステムの設定と管理は、ユーザーインターフェイスの [NSX Edge] セクションで操作します。

ユーザーインターフェイスのこの部分を選択すると、次のように表示されます。

Home		NSX Manager: 192.168.110.15 (Role: Primary)						
Networking & Security		0 Installing 0 Failed						
NSX Home		Id	Name	Type	Version	Status	Tenant	Interfaces
Dashboard		edge-2	Local-Distributed-Router	Logical Router	6.2.3	Deployed	Default	4
Installation		edge-3	Perimeter-Gateway-01	NSX Edge	6.2.3	Deployed	Default	2
Logical Switches		edge-4	OneArm-LoadBalancer-01	NSX Edge	6.2.3	Deployed	Default	1
NSX Edges		edge-5	Perimeter-Gateway-02	NSX Edge	6.2.3	Deployed	Default	2
Firewall		edge-6	OneArm-LoadBalancer-02	NSX Edge	6.2.3	Deployed	Default	1
SpoolGuard		edge-9178...	Universal-Distributed-Router	Universal Distributed Router	6.2.3	Deployed	Default	4
								Size
								Compact
								Compact
								Compact
								Compact
								Compact
								Compact

現在デプロイされているすべての分散論理ルーターと Edge Security Gateway (ESG) が表示され、それぞれに次の情報が示されます。

- [ID] には ESG または分散論理ルーター Edge アプライアンスの ID が表示されます。ID は、その ESG または分散論理ルーターに関する API 呼び出しに使用できます。
- [テナント] + [ID] で、分散論理ルーターのインスタンス名になります。この名前は、NSX CLI で表示および使用されます。
- [サイズ] は、分散論理ルーターについては常に [Compact] になります。また、これは ESG のオペレータによって選択されたものです。

テーブルに表示される情報の他に、ボタンまたは [アクション] を使用してアクセス可能なコンテキスト メニューがあります。

表 3-1. NSX Edge のコンテキスト メニュー

アイコン	アクション
	[強制同期] の操作を使用すると、ESG または分散論理ルーター制御仮想マシンに対して、設定の消去、再起動、および設定の再プッシュを実行できます。
	[再デプロイ] を使用すると、ESG または分散論理ルーターを破棄し、同じ設定を使用して新しい ESG または分散論理ルーターを作成できます。既存の ID は保持されます。
	[自動ルール設定の変更] は、ESG に組み込まれたファイアウォール ルールに適用されます。ファイアウォール ルールは、ESG でサービスを有効にすると作成されます（たとえば、TCP/179 を必要とする BGP など）。
	[テクニカル サポート ログのダウンロード] を使用すると、ESG または分散論理ルーター制御仮想マシンからログ バンドルを作成できます。 分散論理ルーターの場合、ホストのログはテクニカル サポート バンドルに含まれず、個別に収集する必要があります。
	[アプライアンス サイズの変更] は、ESG のみが操作対象となります。この操作は、新しいアプライアンスを使用して「再デプロイ」を実行します（vNIC MAC アドレスは変更されます）。
	[CLI 認証情報の変更] を使用すると、オペレータは CLI 認証情報を強制更新できます。 ESG または分散論理ルーター制御仮想マシンでログインが 5 回失敗した後に CLI がロックアウトされた場合、この操作を使用してもロックアウトは解除されません。5 分間待つか、または ESG/分散論理ルーターを再デプロイして、正しい資格情報で改めてログインする必要があります。
	[ログ レベルの変更] を使用すると、ESG/分散論理ルーターの Syslog に送信される詳細のレベルを変更できます。
	[詳細デバッグの設定] を使用すると、コア ダンプを有効にし、コア ダンプ ファイルの保存用として追加の仮想ディスクを接続して、ESG または分散論理ルーターを再デプロイできます。
	[デプロイ] を使用すると、ESG が作成され、デプロイされていないときに使用できます。 このオプションは、単にデプロイ手順（OVF のデプロイ、インターフェイスの設定、作成されたアプライアンスへの設定のプッシュ）を実行します。
	ESG/分散論理ルーターのバージョンが NSX Manager よりも古い場合は、[アップグレード バージョン] オプションを使用できます。
	[フィルタ] を使用すると、ESG/分散論理ルーターを [名前] で検索できます。

## 新しい NSX Edge（分散論理ルーター）

オペレータが分散論理ルーターを新規作成するときには、次のウィザードを使用して必要な情報を収集します。

**New NSX Edge**

**1 Name and description**

**Name and description**

Install Type: ☐ Edge Services Gateway  
Provides common gateway services such as DHCP, Firewall, VPN, NAT, Routing and Load Balancing.

☒ Logical (Distributed) Router  
Provides Distributed Routing and Bridging capabilities.

☐ Universal Logical (Distributed) Router  
Provides Distributed Routing capabilities for Universal Logical Switches.

Name: \* DLR-01

Hostname: dlr-01

Description:

Tenant: Tenant01

☒ Deploy Edge Appliance  
Deploys NSX Edge Appliance to support Firewall and Dynamic routing.

☐ Enable High Availability  
Enable HA, for enabling and configuring High Availability.

[名前および説明] 画面で、次の情報を収集します。

- [名前] は、NSX Edge のユーザー インターフェイスに表示されます。
- [ホスト名] は、ESG または分散論理ルーター制御仮想マシンの DNS 名を設定するために使用され、SSH/コンソール セッション、Syslog メッセージ、および ESG/分散論理ルーター仮想マシンの vCenter Server の [サマリ] ページの [DNS 名] に表示されます。
- ユーザー インターフェイスの [説明] は、NSX Edge のリストを表示します。
- [テナント] は、NSX CLI によって使用される分散論理ルーター インスタンス名を生成するために使用されます。また、外部のクラウド管理プラットフォームによって使用される場合があります。

[設定] 画面：

**New NSX Edge**

**2 Settings**

**Settings**

CLI credentials will be set on the NSX Edge appliance(s). These credentials can be used to login to the read only command line interface of the appliance.

User Name: \* admin

Password: \*

Confirm password: \*

☒ Enable SSH access

Edge Control Level Logging EMERGENCY

Set the Edge Control Level Logging

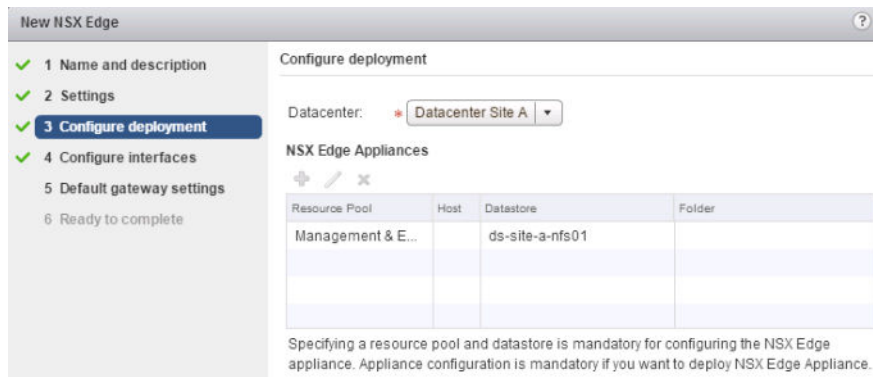
- [ユーザー名] と [パスワード] は、分散論理ルーター制御仮想マシンにアクセスするための CLI/仮想マシンの認証情報を設定します。NSX は、ESG または分散論理ルーター制御仮想マシンで AAA をサポートしません。このアカウントには、ESG/分散論理ルーター制御仮想マシンへの完全なアクセス権限がありますが、CLI/仮想マシン コンソールからは ESG/分散論理ルーターの設定は変更できません。

- [SSH アクセスの有効化] によって、分散論理ルーター制御仮想マシンで SSH デーモンを起動できるようになります。
- SSH ネットワーク アクセスを許可するには、制御仮想マシンのファイアウォール ルールを調整する必要があります。
- オペレータは、制御仮想マシンの管理インターフェイスのサブネット上のホストから、またはプロトコル アドレスが設定されている場合は、このような制限なく、OSPF/BGP の「プロトコル アドレス」上のホストから分散論理ルーター制御仮想マシンに接続できます。

**注：** 分散論理ルーター制御仮想マシンと分散論理ルーターの「内部」インターフェイスのいずれかで設定されているサブネットに分類される IP アドレス間でネットワーク接続することはできません。これは、分散論理ルーター制御仮想マシンのこれらのサブネットの出力方向のインターフェイスは、データ プレーンに接続しない疑似インターフェイス「分散論理ルーター」を指定するためです。

- [高可用性の有効化] によって、アクティブ/スタンバイの高可用性ペアとして制御仮想マシンがデプロイされます。
- [Edge の制御レベル ログ] は、Edge アプライアンスの Syslog レベルを設定します。

[デプロイの] 画面：



Resource Pool	Host	Datastore	Folder
Management & E...		ds-site-a-nfs01	

- [データセンター] では、制御仮想マシンをデプロイする vCenter Server データセンターを選択します。
- [NSX Edge アプライアンス] は、分散論理ルーター制御仮想マシンを示し、1 つのみを定義できます（以下を参照）。
  - [高可用性] が有効な場合、スタンバイ Edge は、同じクラスタ、ホスト、データストアにデプロイされます。DRS の「仮想マシンを分割」ルールが、アクティブおよびスタンバイ分散論理ルーター制御仮想マシンで作成されます。

[インターフェイスの設定] 画面：



Name	IP Address	Subnet Prefix Length	Connected To
LS A-Uplink	192.168.10.5*	29	vds-mgt_Uplink Network

#### ■ 「高可用性インターフェイス」

- は、ルーティング可能な分散論理ルーター論理インターフェイスとしては作成されません。これは、制御仮想マシン上の単なる vNIC です。
- NSX は VMCI から分散論理ルーターの設定を管理するため、このインターフェイスは IP アドレスを必要としません。
- [名前と説明] 画面で分散論理ルーターの [高可用性の有効化] がチェックされている場合、このインターフェイスは高可用性のハートビートに使用されます。
- [この NSX Edge のインターフェイスを設定します] は、分散論理ルーター論理インターフェイス (LIF) を指します。
  - 分散論理ルーターは、[接続先] の dvPortgroup 上の仮想マシンまたは一致するサブネットの IP アドレスが関連付けられている論理スイッチに L3 ゲートウェイ サービスを提供します。
  - 「アップリンク」タイプの LIF は、制御仮想マシンで vNIC として作成されるため、最大で 8 つがサポートされます。利用可能な最後の 2 つの vNIC は、高可用性インターフェイスと予約されている vNIC に割り当てられます。
  - 「アップリンク」タイプの LIF は、分散論理ルーターで動的ルーティングが動作させるために必要です。
  - 「内部」タイプの LIF は、制御仮想マシンで疑似 vNIC として作成され、最大で 991 個作成できます。

[デフォルト ゲートウェイ設定] 画面：

- [デフォルト ゲートウェイの設定] が選択されている場合、分散論理ルーターでデフォルトのスタティック ルートが作成されます。前の画面で「アップリンク」タイプの LIF が作成すると、このオプションを利用できます。



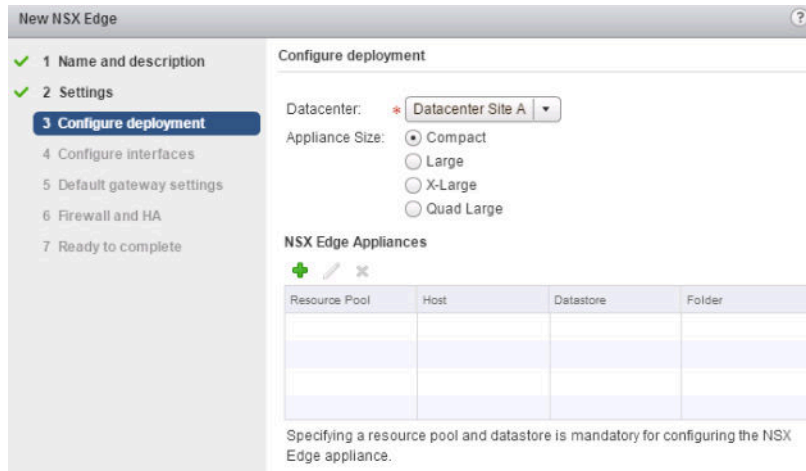
- ECMP がアップリンクで使用されている場合、ネクスト ホップで障害が発生したときに、データプレーンの動作が中断しないようにこのオプションを無効することをお勧めします。

**注：** 右上隅にある二重の右矢印を使用すると、進行中のウィザードを中断して、後で再開できます。

## Edge Service Gateway (ESG) と分散論理ルーターの相違点

ESG のデプロイに使用するウィザード画面は、分散論理ルーターと比較していくつかの相違点があります。

1 つめは、[デプロイの] 画面です。



Resource Pool	Host	Datastore	Folder

ESG の [デプロイの] 画面では、Edge のサイズを選択できます。ESG がルーティングのみに使用されている場合、[Large] が一般的なサイズとなり、ほとんどのシナリオで最適となります。さらに大きなサイズを選択しても、CPU リソースが ESG のルーティング プロセスに提供されず、スループットが増加するわけではありません。

ESG をデプロイせずに作成することも可能ですが、その場合でも、Edge アプライアンスを設定する必要があります。

「デプロイされない」Edge は、API 呼び出しまたはユーザー インターフェイスからデプロイ操作を実行して、後でデプロイできます。

Edge 高可用性が選択されている場合、少なくとも 1 つの「内部」インターフェイスを作成する必要があります。これを行わないと、高可用性が失敗しても通知されず、「スプリットブレイン」の状態になります。

オペレータは NSX のユーザー インターフェイスと API を使用して、最後の「内部」インターフェイスを削除できます。このために、高可用性が失敗しても通知されません。

## 一般的な ESG および分散論理ルーター ユーザー インターフェイスの操作

最初にデプロイした後、一般的に行われる設定がいくつかあります。

一般的に次の設定を行います。

- Syslog 設定
- スタティック ルートの管理

## ■ ルーティング プロトコルとルート再配分の設定

### Syslog 設定

リモート Syslog サーバにログ エントリを送信するように ESG や分散論理ルーター制御仮想マシンを設定します。

The screenshot shows the NSX Manager interface for a device named DLR-01. The 'Manage' tab is selected, and the 'Settings' sub-tab is active. The left sidebar shows 'Configuration' > 'Interfaces'. The main panel displays the 'Details' of the Syslog configuration. The configuration includes a 'Size' of 'Compact', 'Auto generate rules' set to 'Enabled', and a 'Syslog servers' section with a 'Change' link. Below this, 'Server 1' is set to '192.168.110.79' and 'Server 2' is empty.

注：

- ESG/分散論理ルーター制御仮想マシンは DNS リゾルバが設定されていないため、Syslog サーバは IP アドレスとして設定する必要があります。
  - ESG の場合は、[DNS サービスの有効化] (DNS プロキシ) を選択でき、ESG 自体が DNS 名を解決するために DNS を使用できますが、一般的に、IP アドレスとして Syslog サーバを指定する方法が、依存関係が少なく信頼性がより高い方法となります。
- ユーザー インターフェイスで Syslog ポートを指定することはできませんが (常に 514)、プロトコル (UDP/TCP) は指定できます。
- Syslog メッセージは、Edge のフォワーディング テーブルによって Syslog サーバの IP の出力方向として選択された Edge のインターフェイスの IP アドレスから送信されます。
  - 分散論理ルーターの場合は、Syslog サーバには、分散論理ルーター「内部」のインターフェイスで設定されたサブネットにある IP アドレスは指定できません。これは、分散論理ルーター制御仮想マシンのこれらのサブネットの出力方向のインターフェイスは、データ プレーンに接続しない pseudo-interface「分散論理ルーター」を指定するためです。

デフォルトでは、ESG/分散論理ルーター ルーティング エンジンのログは無効になっています。必要な場合には、ユーザー インターフェイスで [動的ルーティング] で [編集] をクリックして有効にします。

DLR-01 Actions ▾

Summary **Manage**

Settings Firewall **Routing** Bridging DHCP Relay

Global Configuration  
Static Routes  
OSPF  
BGP  
Route Redistribution

Routing Configuration : Reset

ECMP : Disabled Enable

Default Gateway : Edit Delete

Interface :  
Gateway IP :  
MTU :  
Description :

Dynamic Routing Configuration : Edit

Router ID :  
OSPF : Disabled  
BGP : Disabled  
Logging : Disabled  
Log Level :

ルーター ID も設定する必要があります。この ID は通常、アップリンク インターフェイスの IP アドレスになります。

## スタティック ルート

スタティック ルートには、分散論理ルーター LIF または ESG インターフェイスのいずれかに関連付けられているサブネット上の IP アドレスに設定されたネクスト ホップが必要です。そうでない場合、設定に失敗します。

「インターフェイス」が選択されていない場合、ネクスト ホップが直接接続しているサブネットの 1 つに一致させることで、自動的に設定されます。

**Add Static Route** ?

Network: \*

10.10.10.0/24

*Network should be entered in CIDR format  
e.g. 192.169.1.0/24*

Next Hop: \*

192.168.10.1

Interface:

▼

i

MTU:

1500

Description:

OK

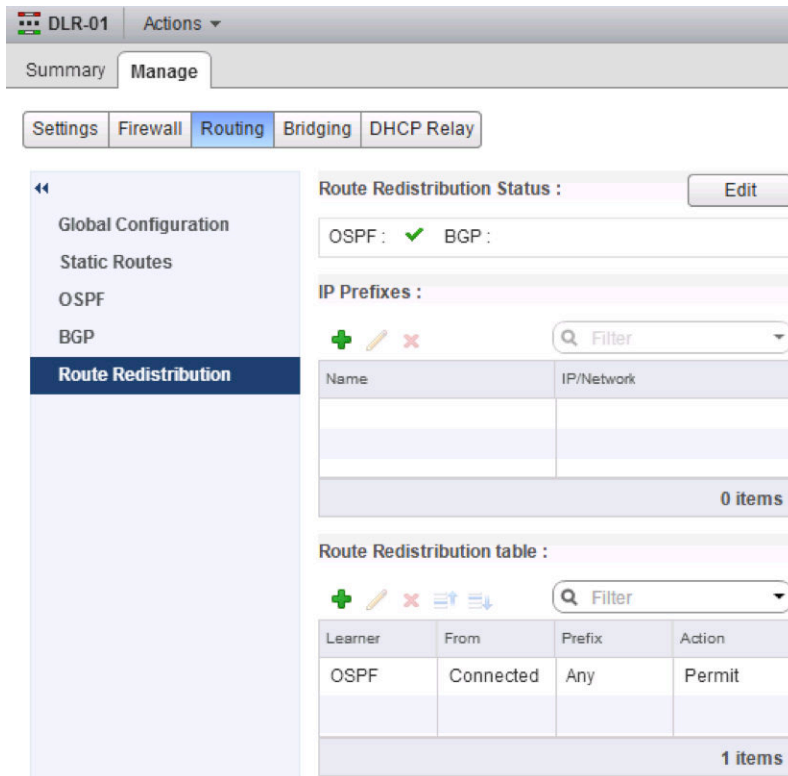
Cancel

## ルート再配分

[ルート再配分テーブル] にエントリを追加しても、選択した [ラーナー プロトコル] で再配分が自動的に有効になりません。これは、[ルート再配分ステータス] の [編集] から明示的に実行する必要があります。

分散論理ルーターは、デフォルトで OSPF への接続ルートの再配分によって構成されますが、ESG は構成されません。

[ルート再配分テーブル] は、上から下に順番に処理され、最初に一致したときに処理は停止します。再配分からいくつかのプリフィックスを除外するには、テーブルの上部に特定のエントリをさらに追加します。



## NSX のルーティングのトラブルシューティング

NSX は、ルーティングが動作していることを確認するためのいくつかのツールを提供しています。

### NSX のルーティング CLI

CLI コマンドの集合を使用して、オペレータは NSX のルーティング サブシステムのさまざまな部分の実行状態を確認できます。

NSX のルーティング サブシステムは分散型であるため、多数の CLI を使用して、NSX の多様なコンポーネントでアクセスできます。NSX バージョン 6.2 以降、NSX は集中管理 CLI も提供します。これは、分散するさまざまなコンポーネントへのアクセスおよびログインに必要な「移動時間」を短縮する上で役立ちます。この CLI により、NSX Manager シェル上の 1 つの場所からほとんどの情報にアクセスできます。

### 前提条件の確認

各 ESXi ホストについて、主に 2 つの前提条件を満たす必要があります。

- 分散論理ルーターに接続されているすべての論理スイッチが健全であること。
- VXLAN 用に ESXi ホストの準備が正常に完了していること。

## 論理スイッチの健全性チェック

NSX のルーティングは、NSX の論理スイッチに連動します。分散論理ルーターに接続された論理スイッチが健全であることを確認するには、次の手順を実行します。

- 対象となる分散論理ルーターに接続する各論理スイッチのセグメント ID (VXLAN VNI) を検索します（たとえば、5004..5007）。

Logical Switches						
NSX Manager: 192.168.110.42						
Actions						
Name	1	Status	Transport Zone	Segment ID	Control Plane Mode	Description
LS A		✓ Normal	Global-Transport-Zone	5004	Unicast	
LS B		✓ Normal	Global-Transport-Zone	5005	Unicast	
LS C		✓ Normal	Global-Transport-Zone	5006	Unicast	
LS D		✓ Normal	Global-Transport-Zone	5007	Unicast	

- この分散論理ルーターの処理対象となる仮想マシンが実行される ESXi ホストで、この分散論理ルーターに接続する論理スイッチの VXLAN 制御プレーンの状態を確認します。

```
# esxcli network vswitch dvs vmware vxlan network list --vds-name=Compute_VDS
```

VXLAN ID	Multicast IP	Control Plane	Controller Connection	Port
Count	MAC Entry Count	ARP Entry Count		
-----	-----	-----	-----	-----
5004	N/A (headend replication)	Enabled (multicast proxy, ARP proxy)	192.168.110.201	
(up)	2	2	0	
5005	N/A (headend replication)	Enabled (multicast proxy, ARP proxy)	192.168.110.202	
(up)	1	0	0	
5006	N/A (headend replication)	Enabled (multicast proxy, ARP proxy)	192.168.110.203	
(up)	1	1	0	
5007	N/A (headend replication)	Enabled (multicast proxy, ARP proxy)	192.168.110.202	
(up)	1	0	0	

関連する各 VXLAN について、次の状態を確認します。

- ハイブリッド モードまたはユニキャスト モードの論理スイッチの場合：
  - 制御プレーンが「Enabled」になっていること。
  - 「multicast proxy」と「ARP proxy」が表示され、IP アドレス検出を無効にしている場合でも「ARP proxy」が表示されること。
  - コントローラのリストに有効なコントローラ IP アドレスが表示され、接続の状態が「up」であること。
- ポート数が正しく示されること。対象の論理スイッチに接続するホストに仮想マシンがない場合でも、少なくとも 1 が表示されます。この 1 つのポートは vdrPort で、ESXi ホストの分散論理ルーター カーネル モジュールに接続されている特殊な dvPort です。

- vdrPort が関連する各 VXLAN に接続されていること。これは、次のコマンドを実行して確認します。

```
~ # esxcli network vswitch dvs vmware vxlan network port list --vds-name=Compute_VDS --vxlan-id=5004
Switch Port ID   VDS Port ID   VMKNIC ID
-----
50331656   53             0
50331650   vdrPort        0

~ # esxcli network vswitch dvs vmware vxlan network port list --vds-name=Compute_VDS --vxlan-id=5005
Switch Port ID   VDS Port ID   VMKNIC ID
-----
50331650   vdrPort        0
```

- 上記の例では、VXLAN 5004 には 1 台の仮想マシンと 1 つの分散論理ルーター接続があり、VXLAN 5005 には 1 つの分散論理ルーター接続だけがあります。
- 仮想マシンが対応する VXLAN に適切に接続されているかどうか確認します (たとえば、VXLAN 5004 の web-sv-01a)。

```
~ # esxcli network vswitch -l
DVS Name      Num Ports   Used Ports   Configured Ports   MTU      Uplinks
Compute_VDS   1536        10           512                1600     vmnic0

DVPort ID      In Use      Client
[. .skipped..]
53             1           web-sv-01a.eth0
```

## VXLAN の準備の確認

ESXi ホストの VXLAN を設定する一貫として、分散論理ルーター カーネル モジュールもインストールおよび設定され、VXLAN 用に準備された分散仮想スイッチの dvPort に接続されます。

- 1 show cluster all を実行して、クラスタ ID を取得します。
- 2 show cluster cluster-id を実行して、ホスト ID を取得します。
- 3 show logical-router host hostID connection を実行して、ステータス情報を取得します。

```
nsxmgr-01a# show logical-router host <hostID> connection

Connection Information:
-----

DvsName      VdrPort      NumLifs   VdrVmac
-----
Compute_VDS   vdrPort       4         02:50:56:56:44:52
Teaming Policy: Default Teaming
Uplink       : dvUplink1(50331650): 00:50:56:eb:41:d7(Team member)
```

Stats : Pkt Dropped	Pkt Replaced	Pkt Skipped
Input : 0	0	1968734458
Output : 303	7799	31891126

- VXLAN を使用して有効になっている分散仮想スイッチには、1 つの vdrPort が作成され、その ESXi ホスト上のすべての分散論理ルーター インスタンスにより共有されます。
- 「NumLifs」は、このホスト上に存在するすべての分散論理ルーター インスタンスからの LIF の合計数です。
- 「VdrVmac」は、すべてのインスタンスのすべての LIF で分散論理ルーターが使用する vMAC です。この MAC は、すべてのホストで同一です。これは、ESXi ホストの外部となる物理ネットワークで送信されるフレームに表示されません。
- VXLAN を使用して有効になっている分散仮想スイッチの各 dvUplink には、一致する VTEP があります。ただし、LACP/固定イーサチャネルのチーミング モードが使用される場合は、dvUplink の数に関係なく VTEP が 1 つだけ作成されます。
  - ホストから送信されるときに分散論理ルーター (SRC MAC = vMAC) によって作成されるトラフィックについては、SRC MAC が対応する dvUplink の pMAC に変更されます。
  - 元の仮想マシンのソース ポートまたはソース MAC は、dvUplink を特定するために使用されます (各パケットで、その分散仮想スイッチのメタデータに保持されます)。
  - ホストに VTEP が複数あり、いずれかの dvUplink に障害が発生した場合、問題の dvUplink に関連付けられている VTEP は、その VTEP に指定されているすべての仮想マシンとともに、残りのいずれかの dvUplink に移動されます。これによって、仮想マシンの別の VTEP への移動に伴って制御プレーンの変更が大量に発生する状況を回避します。
- 各「dvUplinkX」の横に表示される () 内の数字は、dvPort 番号です。これは、個々のアップリンクでパケットキャプチャを実行する場合に役立ちます。
- 各「dvUplinkX」に表示される MAC アドレスは、その dvUplink に関連付けられている「pMAC」です。この MAC アドレスは、分散論理ルーターによって生成された ARP クエリや、これらのパケットが ESXi から送信されるときに分散論理ルーターによりルーティングされたパケットなどの、分散論理ルーターからのトラフィックに使用されます。この MAC アドレスは、物理ネットワークで表示されます (分散論理ルーター LIF が VLAN タイプの場合は直接的に、または VXLAN LIF の VXLAN パケット内に)。
- 「Pkt Dropped」、「Pkt Replaced」、「Pkt Skipped」は、分散論理ルーターの内部的な実装の詳細に関連するカウンタであり、通常はトラブルシューティングや監視には使用されません。

## ルーティングの概要

ルーティングのトラブルシューティングを効率的に行うため、ルーティングの仕組みと関連情報のテーブルを確認することをお勧めします。

- 1 パケットを受信し、宛先 IP アドレスに送信します。
- 2 ルーティング テーブルで、ネクスト ホップの IP アドレスを確認します。
- 3 このアドレスに到達可能なネットワーク インターフェイスを確認します。
- 4 該当のネクスト ホップの MAC アドレスを取得します (ARP を介して)。



5 L2 フレームを構築します。

6 インターフェイスからフレームを送信します。

ルーティングには、次のテーブルが必要です。

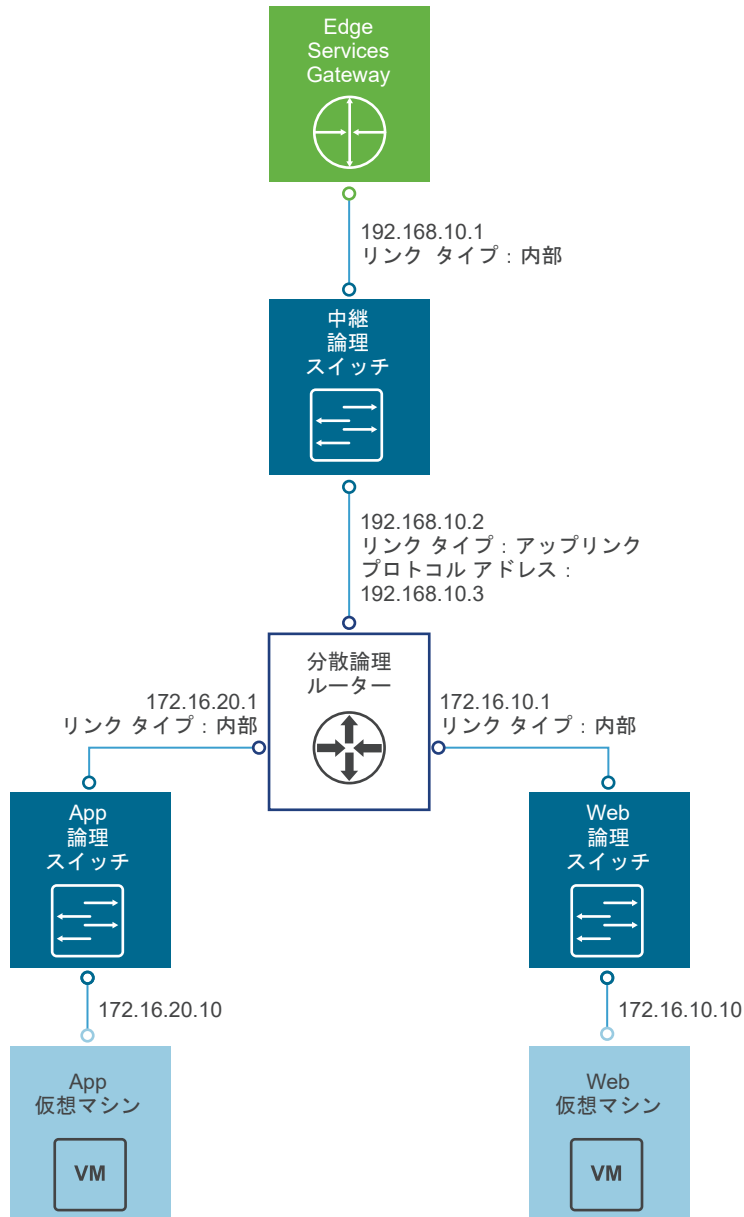
- インターフェイス テーブル（インターフェイスの IP アドレスおよびネットマスクを含む）
- ルーティング テーブル
- ARP テーブル

## サンプル ルート トポロジを使用した分散論理ルーター状態の確認

このセクションでは、分散論理ルーターがパケットをルーティングするために必要となる情報を確認する方法について説明します。

サンプル ルート トポロジを使用して、複数の論理スイッチと 1 つの分散論理ルーターのセットを NSX で作成します。

図 3-7. サンプル ルート トポロジ



図に表示されている要素：

- 論理スイッチ x 4、それぞれに自身のサブネットがあります。
- 仮想マシン x 3、論理スイッチ 1 つにつき 1 台接続されています。
  - それぞれに自身の IP アドレスと IP ゲートウェイがあります。
  - それぞれに MAC アドレスがあります（最後の 2 つのオクテットが表示されています）。
- 1 つの分散論理ルーターは 4 つの論理スイッチに接続し、1 つの論理スイッチは「アップリンク」用であり、残りの論理スイッチは内部用です。
- 分散論理ルーターのアップストリーム ゲートウェイとして動作する外部ゲートウェイ。ESG になる場合があります。

[設定内容の確認] ウィザードの画面が上記の分散論理ルーターに表示されます。

**New NSX Edge**

Ready to complete

**Name and description**  
 Name: DLR1  
 Install Type: Logical (Distributed) Router  
 Tenant:  
 HA: Disabled

**Management Interface Configuration**  
 Connected To: Mgmt\_Edge\_VDS - Mgmt

IP Address	Subnet Prefix Length

**NSX Edge Appliances**

Resource Pool	Host	Datastore	Folder
Management and Edge Cluster		ds-site-a-nfs01	

**Interfaces**

Name	IP Address	Subnet Prefix Length	Connected To
LS A	172.16.10.1*	24	LS A
LS B	172.16.20.1*	24	LS B
LS C	172.16.30.1*	24	LS C
LS D	192.168.10.2*	29	LS D

Back Next Finish Cancel

分散論理ルーターのデプロイが終了したら、ESXi CLI コマンドを使用して、参加しているホストにある対象の分散論理ルーターの分散状態を表示して確認できます。

## 分散論理ルーター インスタンスの確認

分散論理ルーター インスタンスが作成されているか、制御プレーンがアクティブであるかを最初に確認します。

- 1 NSX Manager のシェルで、`show cluster all` を実行して、クラスタ ID を取得します。
- 2 `show cluster cluster-id` を実行して、ホスト ID を取得します。
- 3 `show logical-router host hostID dlr all verbose` を実行して、ステータス情報を取得します。

```
nsxmgr# show logical-router host host-id dlr all verbose
```

VDR Instance Information :

```
-----
Vdr Name:          default+edge-1
Vdr Id:            1460487509
Number of Lifs:    4
Number of Routes:  5
State:             Enabled
Controller IP:     192.168.110.201
Control Plane Active: Yes
Control Plane IP:  192.168.210.51
Edge Active:       No
```

重要 :

- このコマンドは、指定された ESXi ホストにあるすべての分散論理ルーター インスタンスを表示します。

- 「Vdr Name」は、「テナント」+「Edge ID」で設定されます。この例では、「テナント」が指定されていないため、「default」という単語が使用されています。「Edge ID」は「edge-1」ですが、これは NSX のユーザー インターフェイスで確認できます。
  - ホストに多くの分散論理ルーター インスタンスがある場合に、ユーザー インターフェイスの [NSX Edge] に表示される「Edge ID」を検索することで、正しいインスタンスを探すことができます。
- 「Vdr Id」は、ログなどをさらに検索するときに使用します。
- 「Number of Lifs」は、個別の分散論理ルーター インスタンス上の LIF を表示します。
- ここでは「Number of Routes」が 5 になっています。この内訳は、直接接続している 4 つのルート（各 LIF に 1 つ）とデフォルトのルートです。
- 「State」は分散論理ルーター 制御プレーンの状態を示し、「Controller IP」に正しいコントローラの IP アドレスが表示され、「Control Plane Active」が「Yes」と表示されます。分散論理ルーターが動作するには、コントローラが稼動している必要があります。上記は、正常な分散論理ルーター インスタンスの出力です。
- 「Control Plane IP」は、ESXi ホストがコントローラとの通信に使用する IP アドレスを示します。これは、常に ESXi ホストの管理用 vmknic（通常は vmk0）に関連付けられる IP アドレスとなります。
- 「Edge Active」は、このホストで分散論理ルーター インスタンスの制御仮想マシンが実行されているかどうか、そして有効な状態であるかどうかを示します。
  - 有効な分散論理ルーター制御仮想マシンを配置し、NSX L2 ブリッジが有効な場合に、ブリッジを実行するために使用される ESXi ホストを決定します。
- また、このコマンドには、概要を即座に生成する「簡易版」があります。「Vdr Id」は、ここでは 16 進数の形式で表示されます。

```
nsxmgr# show logical-router host host-id dlr all brief
```

VDR Instance Information :

-----

State Legend: [A: Active], [D: Deleting], [X: Deleted], [I: Init]

State Legend: [SF-R: Soft Flush Route], [SF-L: Soft Flush LIF]

Vdr Name	Vdr Id	#Lifs	#Routes	State	Controller Ip	CP Ip
default+edge-1	0x570d4555	4	5	A	192.168.110.201	192.168.210.51

「Soft Flush」は、LIF ライフサイクルの短期的に発生した一時的な状態を示し、通常、正常な分散論理ルーターでは表示されません。

## 分散論理ルーターの論理インターフェイス

分散論理ルーターが作成されていることを確認したら、すべての分散論理ルーターの論理インターフェイスが存在し、正しく設定されていることを確認します。

- 1 NSX Manager のシェルで、show cluster all を実行して、クラスタ ID を取得します。
- 2 show cluster cluster-id を実行して、ホスト ID を取得します。
- 3 show logical-router host hostID dlr all brief を実行して、dlrID（Vdr 名）を取得します。

- 4 `show logical-router host hostID dlr dlrID interface all brief` を実行して、すべてのインターフェイスのステータス情報の概要を取得します。
- 5 `show logical-router host hostID dlr dlrID interface (all | intName) verbose` を実行して、すべてのインターフェイスまたは特定のインターフェイスのステータス情報を取得します。

```
nsxmgr# show logical-router host hostID dlr dlrID interface all verbose
```

```
VDR default+edge-1:1460487509 LIF Information :
```

```
Name:          570d45550000000a
Mode:          Routing, Distributed, Internal
Id:           Vxlan:5000
Ip(Mask):      172.16.10.1(255.255.255.0)
Connected Dvs: Compute_VDS
VXLAN Control Plane: Enabled
VXLAN Multicast IP: 0.0.0.1
State:         Enabled
Flags:         0x2388
DHCP Relay:    Not enabled
```

```
Name:          570d45550000000c
Mode:          Routing, Distributed, Internal
Id:           Vxlan:5002
Ip(Mask):      172.16.30.1(255.255.255.0)
Connected Dvs: Compute_VDS
VXLAN Control Plane: Enabled
VXLAN Multicast IP: 0.0.0.1
State:         Enabled
Flags:         0x2288
DHCP Relay:    Not enabled
```

```
Name:          570d45550000000b
Mode:          Routing, Distributed, Internal
Id:           Vxlan:5001
Ip(Mask):      172.16.20.1(255.255.255.0)
Connected Dvs: Compute_VDS
VXLAN Control Plane: Enabled
VXLAN Multicast IP: 0.0.0.1
State:         Enabled
Flags:         0x2388
DHCP Relay:    Not enabled
```

```
Name:          570d455500000002
Mode:          Routing, Distributed, Uplink
Id:           Vxlan:5003
Ip(Mask):      192.168.10.2(255.255.255.248)
Connected Dvs: Compute_VDS
VXLAN Control Plane: Enabled
VXLAN Multicast IP: 0.0.0.1
State:         Enabled
Flags:         0x2208
DHCP Relay:    Not enabled
```

**重要：**

- LIF の「Name」は、ホストのあるすべての分散論理ルーター インスタンス全体で一意となります。ホストと分散論理ルーターのマスター コントローラ ノードでは、同じ名前 (Name) になります。
- LIF の「Mode」は、LIF がルーティングかブリッジか、また内部リンクかアップリンクかを示します。
- 「Id」は、LIF タイプと対応するサービス ID (VXLAN と VNI、または VLAN と VID) を示します。
- 「Ip(Mask)」は、LIF が「ルーティング」の場合に表示されます。
- LIF がハイブリッドまたはユニキャスト モードで VXLAN に接続している場合、「VXLAN Control Plane」は「Enabled」になります。
- VXLAN LIF については、VXLAN がユニキャスト モードの場合、「VXLAN Multicast IP」は「0.0.0.1」となります。それ以外の場合には、実際のマルチキャスト IP アドレスが表示されます。
- ルーティング LIF の場合、「State」は、「Enabled」になります。ブリッジ LIF については、ブリッジを実行しているホストでは「Enabled」となり、その他のすべてのホストでは「Init」となります。
- 「Flags」は、LIF の状態の概要を示し、LIF の以下の情報を表示します。
  - ルーティングまたはブリッジ
  - VLAN LIF が代表インスタンスか
  - DHCP リレーが有効か
  - フラグ 0x0100 は、分散論理ルーターによって VXLAN VNI に参加したときに設定されます (その VXLAN に仮想マシンがあるホストとは対照的に)。
  - 「簡易」モードではフラグはさらに読みやすい形式で表示されます。

```
nsxmgr# show logical-router host hostID dlr dlrID interface all brief
```

```
VDR default+edge-1 LIF Information :
```

```
State Legend: [A:Active], [d:Deleting], [X:Deleted], [I:Init],[SF-L:Soft Flush LIF]
```

```
Modes Legend: [B:Bridging],[E: Empty], [R:Routing],[S:Sedimented],[D:Distributed]
```

```
Modes Legend: [In:Internal],[Up:Uplink]
```

Lif Name	Id	Mode	State	Ip(Mask)
570d45550000000a	Vxlan:5001	R,D,In	A	172.16.10.1(255.255.255.0)
570d45550000000c	Vxlan:5003	R,D,In	A	172.16.30.1(255.255.255.0)
570d45550000000b	Vxlan:5002	R,D,In	A	172.16.20.1(255.255.255.0)
570d455500000002	Vxlan:5000	R,D,Up	A	192.168.10.5(255.255.255.248)

**分散論理ルーター (DLR) のルート**

分散論理ルーターが正常な状態にあり、すべての LIF が関連付けられていることを確認したら、次にルーティング テーブルを確認します。

- 1 NSX Manager のシェルで、`show cluster all` を実行して、クラスタ ID を取得します。
- 2 `show cluster cluster-id` を実行して、ホスト ID を取得します。

- 3 `show logical-router host hostID dlr all brief` を実行して、dlrID (Vdr 名) を取得します。
- 4 `show logical-router host hostID dlr dlrID route` を実行して、すべてのインターフェイスのステータス情報を取得します。

```
nsxmgr# show logical-router host hostID dlr dlrID route
```

VDR default+edge-1:1460487509 Route Table

Legend: [U: Up], [G: Gateway], [C: Connected], [I: Interface]

Legend: [H: Host], [F: Soft Flush] [!: Reject] [E: ECMP]

Destination	GenMask	Gateway	Flags	Ref	Origin	UpTime	Interface
0.0.0.0	0.0.0.0	192.168.10.1	UG	1	AUTO	10068944	570d455500000002
172.16.10.0	255.255.255.0	0.0.0.0	UCI	1	MANUAL	10068944	570d45550000000a
172.16.20.0	255.255.255.0	0.0.0.0	UCI	1	MANUAL	10068944	570d45550000000b
172.16.30.0	255.255.255.0	0.0.0.0	UCI	1	MANUAL	10068944	570d45550000000c
192.168.10.0	255.255.255.248	0.0.0.0	UCI	1	MANUAL	10068944	570d455500000002

重要：

- 「Interface」は、出力方向の LIF を示します。これは、対応する「Destination」に選択されます。分散論理ルーターの LIF のいずれかの「Lif Name」に設定されます。
- ECMP ルートの場合は、「Destination」、「GenMask」、および「Interface」が同じで「Gateway」が異なる複数のルートがあります。また、ECMP ルートであることを示す「E」が「Flags」に追加されます。

## 分散論理ルーター (DLR) の ARP テーブル

分散論理ルーターがパケットを送信するには、分散論理ルーターがネクスト ホップの IP アドレスの ARP 要求を解決できる必要があります。この解決プロセスの結果は、個々のホストのローカル分散論理ルーター インスタンスに格納されます。

コントローラはこのプロセスには関与せず、解決された ARP エントリを他のホストに配信するためにも使用されません。

無効なキャッシュ エントリは、600 秒間保持された後に削除されます。DLR ARP の解決プロセスの詳細については、[分散論理ルーター ARP の解決プロセス](#)を参照してください。

- 1 NSX Manager のシェルで、`show cluster all` を実行して、クラスター ID を取得します。
- 2 `show cluster cluster-id` を実行して、ホスト ID を取得します。
- 3 `show logical-router host hostID dlr all brief` を実行して、dlrID (Vdr 名) を取得します。
- 4 `show logical-router host hostID dlr dlrID arp` を実行して、すべてのインターフェイスのステータス情報を取得します。

```
nsxmgr# show logical-router host hostID dlr dlrID arp
```

VDR default+edge-1:1460487509 ARP Information :

Legend: [S: Static], [V: Valid], [P: Proxy], [I: Interface]

Legend: [N: Nascent], [L: Local], [D: Deleted]

Network	Mac	Flags	Expiry	SrcPort	Interface	Refcnt
-----	---	-----	-----	-----	-----	-----
172.16.10.1	02:50:56:56:44:52	VI	permanent	0	570d45550000000a	1
172.16.10.11	00:50:56:a6:7a:a2	VL	147	50331657	570d45550000000a	2
172.16.30.1	02:50:56:56:44:52	VI	permanent	0	570d45550000000c	1
172.16.30.11	00:50:56:a6:ba:09	V	583	50331650	570d45550000000c	2
172.16.20.11	00:50:56:a6:84:52	VL	568	50331658	570d45550000000b	2
172.16.20.1	02:50:56:56:44:52	VI	permanent	0	570d45550000000b	1
192.168.10.2	02:50:56:56:44:52	VI	permanent	0	570d455500000002	1
192.168.10.1	00:50:56:8e:ee:ce	V	147	50331650	570d455500000002	1

注：

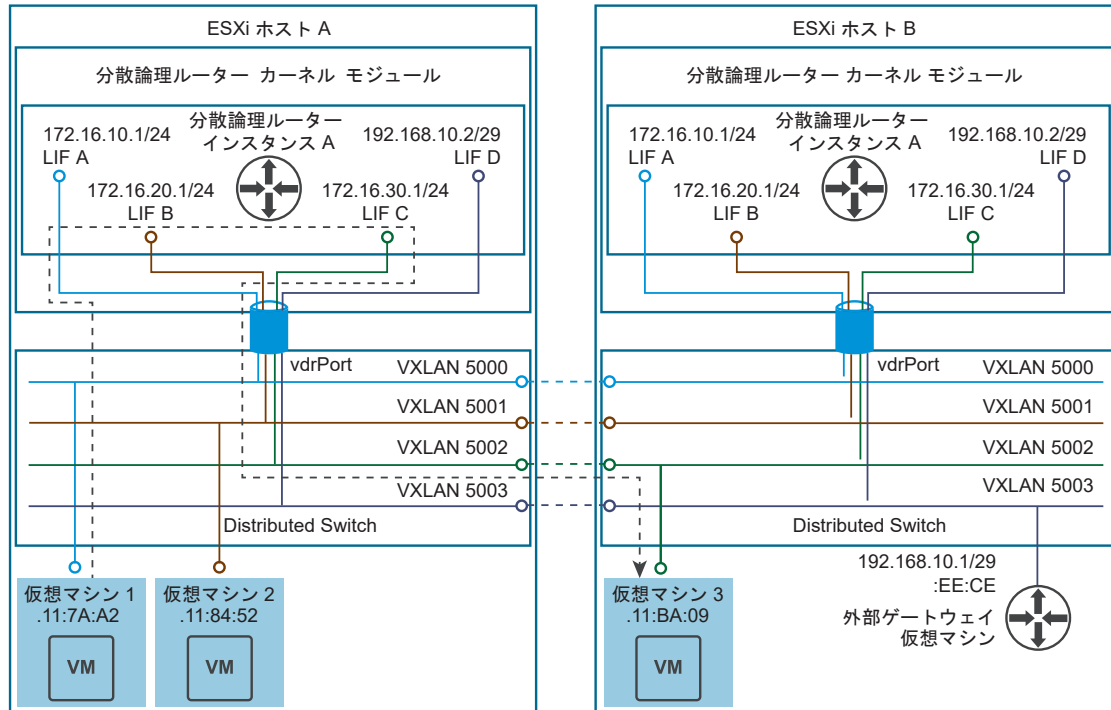
- 分散論理ルーター自身の LIF (「I」フラグ) のすべての ARP エントリは同じであり、[VXLAN の準備の確認](#)で説明したのと同じ vMAC を表示します。
- 「L」フラグが付いた ARP エントリは、CLI コマンドが実行されたホストで稼働している仮想マシンと一致します。
- 「SrcPort」は、ARP エントリの送信元の dvPort ID を表示します。ARP エントリの送信元が別のホストである場合には、dvUplink の dvPort ID が表示されます。この dvPort ID は、[VXLAN の準備の確認](#)で説明した dvUplink dvPort ID と相互参照される場合があります。
- 「Nascent」フラグは通常は表示されません。このフラグは、分散論理ルーターが ARP リプライの到着を待機中に設定されます。このフラグがついたエントリがある場合、ARP の解決に問題があることを示しています。

## 分散論理ルーター (DLR) と関連するホスト コンポーネントの図解

次の図は、ESXi ホスト A と ESXi ホスト B の 2 台のホストを示しています。この例では「分散論理ルーター インスタンス A」が設定され、4 個の VXLAN LIF に接続されています。



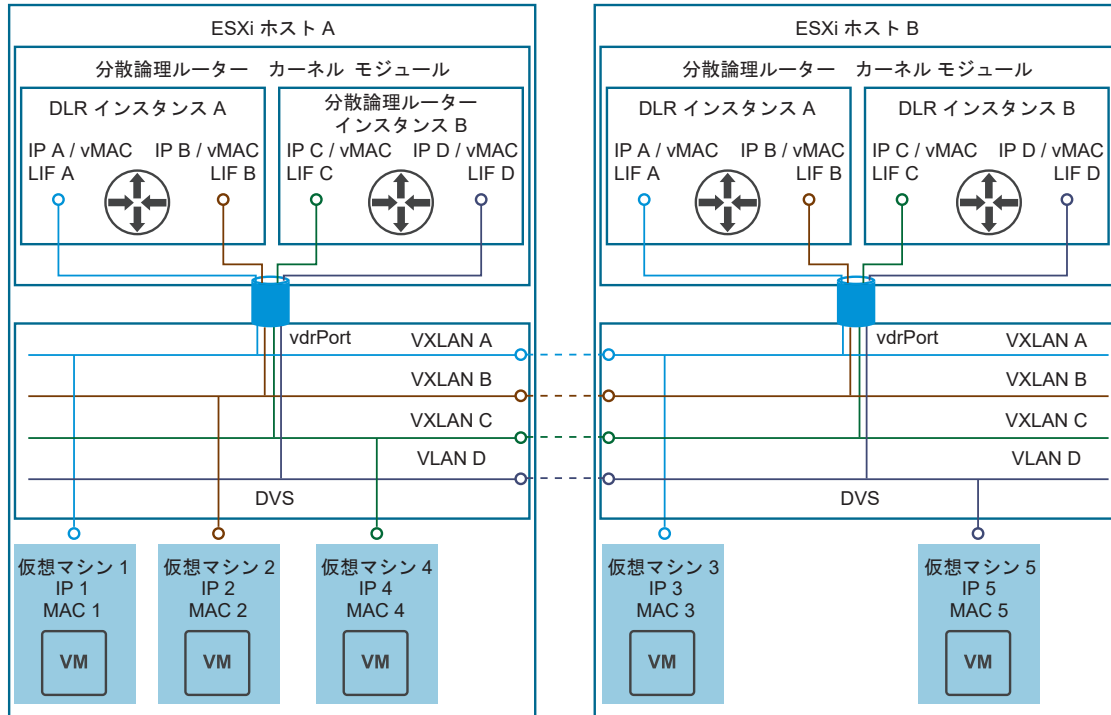
図 3-8. 2 台のホストと単一の分散論理ルーターインスタンス



- 各ホストには「L2 スイッチ」(分散仮想スイッチ (DVS)) が 1 台含まれ、「Router on a Stick」(分散論理ルーター カーネル モジュール) が「トランク」インターフェイス (vdrPort) からこの「スイッチ」に接続されます。
  - この「トランク」は、VLAN と VXLAN の両方のトラフィックを送受信できますが、vdrPort を経由するパケットには、801.Q や UDP/VXLAN ヘッダーは存在しません。代わりに、分散仮想スイッチは、内部のメタデータをタグ付けする方法で、分散論理ルーター カーネル モジュールとこの情報との通信を確立します。
- 分散仮想スイッチが Destination MAC = vMAC というフレームを確認すると、これが分散論理ルーターのフレームであると認識され、このフレームを vdrPort に転送します。
- vdrPort を介して分散論理ルーター カーネル モジュールにパケットが到着すると、メタデータが検証され、パケットが VXLAN VNI か VLAN ID のどちらかに属しているかが特定されます。次にこの情報は、どの分散論理ルーター インスタンスのどの LIF にパケットが属しているかを特定するために使用されます。
  - このシステムでは、1 つの分散論理ルーター インスタンスのみが、指定した VLAN や VXLAN に接続できることになります。

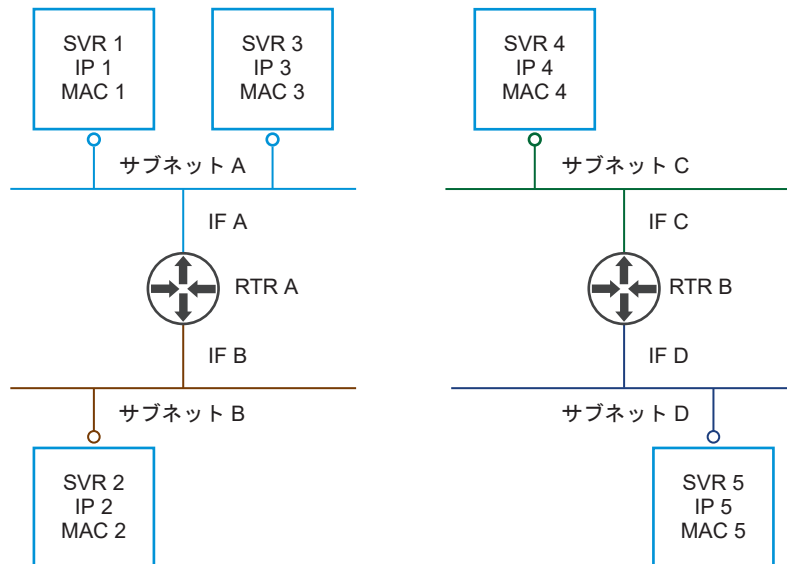
複数の分散論理ルーター インスタンスが存在する場合、次のような図になります。

図 3-9. 2 台のホストと 2 つの分散論理ルーター インスタンス



これは、IP アドレスが重複している可能性がある 2 つの独立したルーティング ドメインが完全に個別に稼動しているネットワーク トポロジに対応する場合があります。

図 3-10. 2 台のホストと 2 つの分散論理ルーター インスタンスに対応するネットワーク トポロジ



## 分散ルーティング サブシステムのアーキテクチャ

ESXi ホストの分散論理ルーター インスタンスは、L3 ルーティングを実行するために必要なすべての情報にアクセスできます。

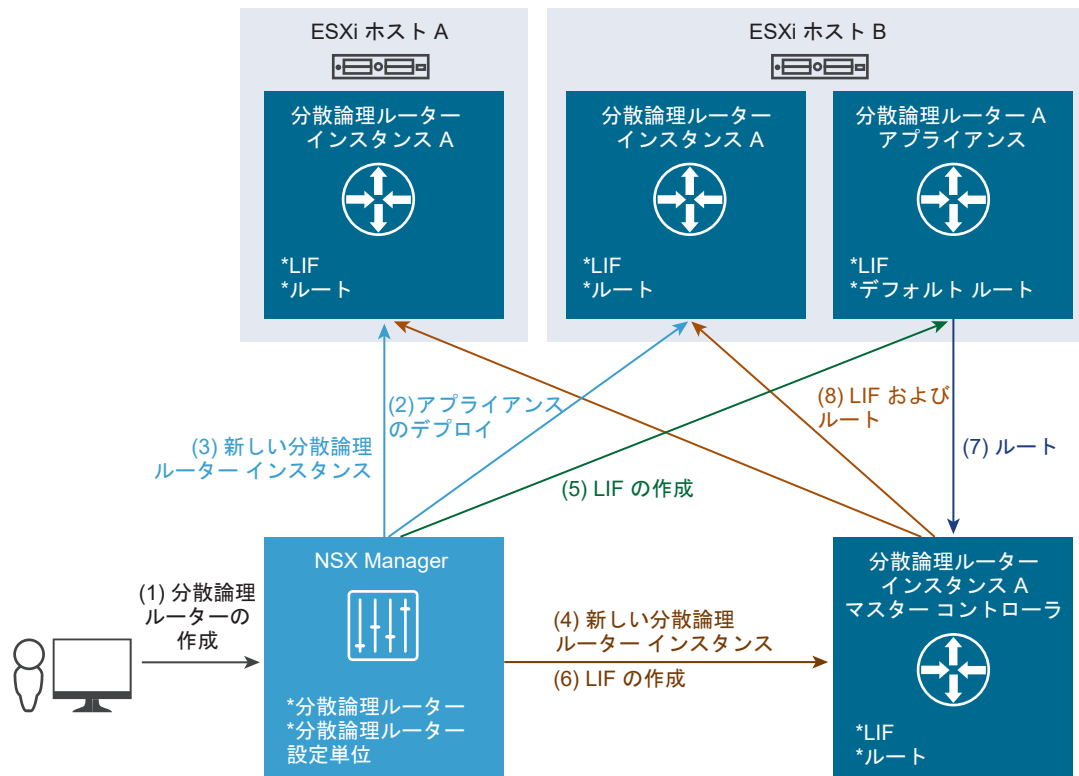
- ネットワークの直接接続（インターフェイス設定から判別）
- 各サブネットのネクスト ホップ（ルーティング テーブルで検索）
- ネクスト ホップ（ARP テーブル）に到達するため、出力方向のフレームに挿入する MAC アドレス

この情報は、複数の ESXi ホストのインスタンスにわたってに配信されます。

### 分散論理ルーター（DLR）の作成プロセス

次の図は、NSX が新しい分散論理ルーターを作成するときのプロセスの概要を示しています。

図 3-11. 分散論理ルーター（DLR）の作成プロセス



新しい分散論理ルーターをデプロイするため、ユーザー インターフェ이스のウィザードで [終了] ボタンを押すか、API 呼び出しが行われると、システムは次の手順で処理を実行します。

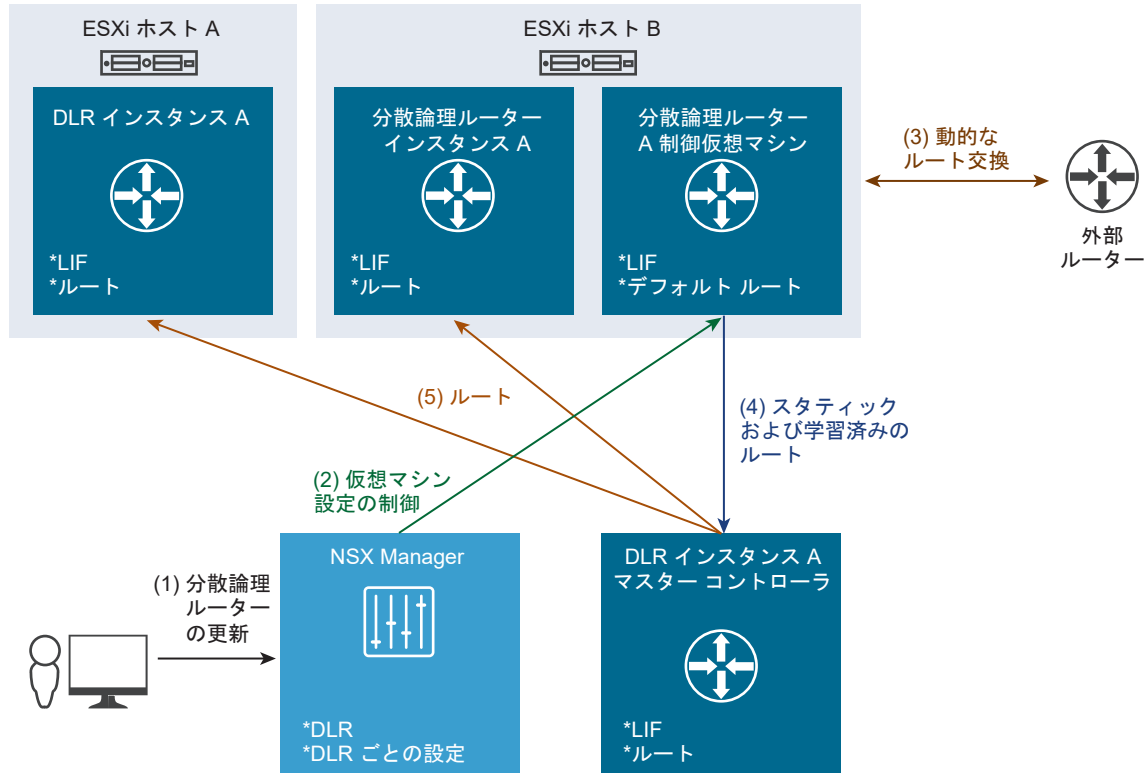
- 1 NSX Manager が、新しい分散論理ルーターをデプロイするための API 呼び出し（直接呼び出し、または vSphere Web Client ユーザー インターフェ이스のウィザードから呼び出し）を受信します。
- 2 NSX Manager は、リンクされている vCenter Server を呼び出し、分散論理ルーター制御仮想マシン 1 台（高可用性が要求されている場合は 2 台）をデプロイします。
  - a 設定を受信するには、分散論理ルーター制御仮想マシンをパワーオンし、NSX Manager に再接続します。

- b 高可用性を実現するため、分散論理ルーター制御仮想マシンを 2 台デプロイしている場合、NSX Manager は非アフィニティ ルールを設定し、2 台の分散論理ルーター制御仮想マシンが異なるホストで実行されるようにします。次に、DRS が 2 台を引き離すアクションを実行します。
- 3 NSX Manager は、ホスト上に分散論理ルーター インスタンスを作成します。
- a NSX Manager は、新しい分散論理ルーターに接続される論理スイッチを検出し、これらのスイッチが属するトランスポート ゾーンを決定します。
  - b 次に、このトランスポート ゾーンに設定されているクラスタ リストを検索し、これらのクラスタにある各ホストで新しい分散論理ルーターを作成します。
  - c この時点で、ホストは新しい分散論理ルーター ID のみを認識しており、その他の情報 (LIF またはルート) を持っていません。
- 4 NSX Manager は、コントローラ クラスタで新しい分散論理ルーター インスタンスを作成します。
- a コントローラ クラスタは、コントローラ ノードのうち 1 台をこの分散論理ルーター インスタンスのマスターとして割り当てます。
- 5 NSX Manager は、LIF を含む設定を分散論理ルーター制御仮想マシンに送信します。
- a ESXi ホスト (分散論理ルーター制御仮想マシンを実行しているホストを含む) は、コントローラ クラスタから一部の情報を受け取り、新しい分散論理ルーター インスタンスを担当するコントローラ ノードを決定して、既存の接続がない場合はそのコントローラ ノードに接続します。
- 6 分散論理ルーター制御仮想マシンで LIF が作成されたら、NSX Manager はコントローラ クラスタで新しい分散論理ルーターの LIF を作成します。
- 7 分散論理ルーター制御仮想マシンは、新しい分散論理ルーター インスタンスのコントローラ ノードに接続し、コントローラ ノードにルートを送信します。
- a 最初に分散論理ルーターは、LIF にプリフィックスを解決することによって、ルーティング テーブルをフォーワーディング テーブルに変換します。
  - b 次に、分散論理ルーターは、変換したテーブルをコントローラ ノードに送信します。
- 8 コントローラ ノードは、手順 5.a で確立した接続を介して、新しい分散論理ルーターが存在する他のホストに LIF とルートをプッシュします。

### 分散論理ルーター (DLR) への動的ルーティングの追加

vSphere Web Client ユーザー インターフェイスを使用するのではなく、直接的な API 呼び出しで分散論理ルーターを作成する場合は、動的ルーティング (1) を含む完全な構成で提供できます。

図 3-12. 分散論理ルーター (DLR) での動的ルーティング



- 1 NSX Manager は、API 呼び出しを受け取り、既存の分散論理ルーター設定を変更します。ここでは、動的ルーティングの追加を行います。
- 2 NSX Manager は、新しい設定を分散論理ルーター制御仮想マシンに送信します。
- 3 分散論理ルーター制御仮想マシンは設定を適用し、ルーティングの隣接関係の確立や、ルーティング情報の交換などのプロセスを実行します。
- 4 ルーティング情報の交換後、分散論理ルーター制御仮想マシンはフォワーディング テーブルを計算して、これを分散論理ルーターのマスター コントローラ ノードに送信します。
- 5 続いて、分散論理ルーターのマスター コントローラ ノードは、更新されたルートを分散論理ルーター インスタンスが存在する ESXi ホストに配信します。

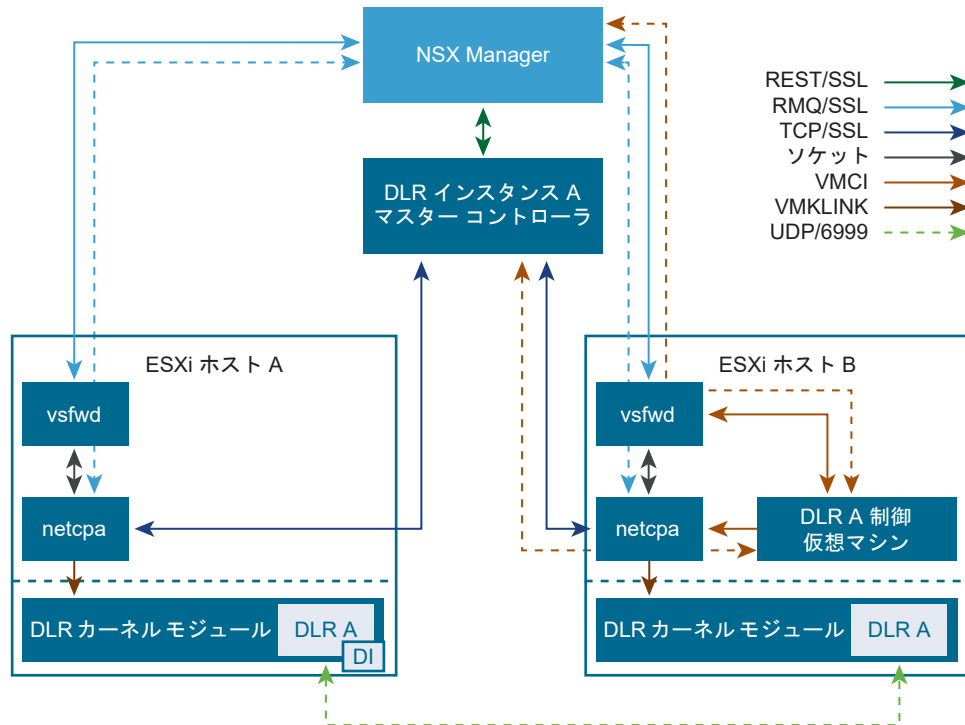
分散論理ルーター制御仮想マシンが実行している ESXi ホスト上の分散論理ルーター インスタンスは、分散論理ルーターのマスター コントローラ ノードのみから LIF とルートを受信し、分散論理ルーター制御仮想マシンや NSX Manager から直接受信することはありません。

### 分散論理ルーターの制御および管理プレーンのコンポーネントと通信

このセクションでは、分散論理ルーターの制御および管理プレーンのコンポーネントの概要について説明します。

この図は、コンポーネントおよび対応するコンポーネント間の通信チャネルを示しています。

図 3-13. 分散論理ルーターの制御および管理プレーンのコンポーネント



- NSX Manager :
  - コントローラ クラスタと直接通信します。
  - NSX が動作する各ホストで実行されているメッセージ バス クライアント (vsfwd) プロセスと、直接常時接続を保持します。
- 各分散論理ルーター インスタンスで、利用可能な 3 台のコントローラ ノードの中から 1 台がマスターとして選出されます。
  - 元のコントローラ ノードで障害が発生すると、マスター ノードの機能を別のコントローラ ノードに移動することができます。
- 各 ESXi ホストは、メッセージ バス クライアント (vsfwd) と制御プレーン エージェント (netcpa) の 2 つのユーザー ワールド エージェント (UWA) を実行します。
  - netcpa が動作するには NSX Manager からの情報が必要となります (たとえば、コントローラを検索する場所や認証方法など)。この情報には、vsfwd が提供するメッセージ バス接続を介してアクセスします。
  - netcpa は、分散論理ルーター カーネル モジュールと通信し、コントローラから受信した関連情報をこのモジュールに組み込みます。
- 各分散論理ルーター インスタンスには分散論理ルーター制御仮想マシンが 1 台存在し、ESXi ホストのいずれか 1 台で実行されます。分散論理ルーター制御仮想マシンには、次の 2 つの通信チャンネルがあります。
  - vsfwd を介して NSX Manager に接続する VMCi チャンネル。このチャンネルは、制御仮想マシンの設定に使用されます。

- netcpa を介して分散論理ルーター マスター コントローラに接続する VMCI チャネル。このチャネルは、コントローラに分散論理ルーター のルーティング テーブルを送信するために使用されます。
- 分散論理ルーターに VLAN LIF がある場合、参加している ESXi ホストの 1 台がコントローラによって代表インスタンスに選定されます。他の ESXi ホストの分散論理ルーター カーネル モジュールは、関連する VLAN 上で代表インスタンスがプロキシ ARP クエリを実行するように要求します。

## NSX のルーティング サブシステム コンポーネント

NSX のルーティング サブシステムは、複数のコンポーネントによって有効になります。

- NSX Manager
- コントローラのクラスタ
- ESXi ホスト モジュール（カーネルと UWA）
- 分散論理ルーター制御仮想マシン
- ESG

### NSX Manager

NSX Manager は、NSX のルーティングに関連して次の機能を提供します。

- 集中管理された管理プレーンとして、すべての NSX 管理操作の統合 API アクセス ポイント機能を提供する
- 分散ルーティング カーネル モジュールとユーザー ワールド エージェント (UWA) をホストにインストールして、NSX 機能用に準備する
- 分散論理ルーターおよび分散論理ルーターの LIF を作成/破壊する
- vCenter Server を介して、分散論理ルーター制御仮想マシンおよび ESG をデプロイ/削除する
- REST API を介してコントローラ クラスタを設定し、メッセージ バスを介してホストする
  - ホストの制御プレーン エージェントにコントローラの IP アドレスを提供する
  - 証明書を生成してホストとコントローラに配布し、制御プレーンの通信を保護する
- メッセージ バスを介して ESG および分散論理ルーター制御仮想マシンを設定する
  - ESG は準備されていないホストにデプロイでき、その場合はメッセージ バスの代わりに VIX が使用される

### コントローラのクラスタ

NSX の分散ルーティングで必要とされるコントローラは、拡張性と可用性を実現するためにクラスタ化され、次の機能を提供します。

- VXLAN および分散ルーティング制御プレーンをサポートする
- 統計およびランタイム状態用の CLI を提供する
- 各分散論理ルーター インスタンス用にマスター コントローラ ノードを選択する
  - マスター ノードは、分散論理ルーター制御仮想マシンからルーティング情報を受信し、これをホストに送信する

- LIF テーブルをホストに送信する
- 分散論理ルーター制御仮想マシンが存在するホストを追跡する
- VLAN LIF 用の代表インスタンス (DI) を選択してホストに通知し、制御プレーンのキープアライブを介して DI ホストを監視し（タイムアウトは 30 秒、検出時間は 20 ～ 40 秒）、選択した DI ホストを認識できない場合に更新情報をホストに送信する

## ESXi ホスト モジュール

NSX のルーティングは、2 つのユーザー ワールド エージェント (UWA) と 1 つのルーティング カーネル モジュールを直接使用し、さらに VXLAN 接続のために VXLAN カーネル モジュールを使用します。

これらのコンポーネントの機能の概要は次のとおりです。

- 制御プレーン エージェント (netcpa) は、制御プレーン プロトコルを使用してコントローラと通信する TCP (SSL) クライアントです。複数のコントローラに接続する場合があります。netcpa は、制御プレーンに関連する情報を NSX Manager から取得するために、メッセージ バス クライアント (vsfwd) と通信します。
- netcpa のパッケージ化とデプロイ：
  - エージェントは VXLAN VIB (vSphere インストール バンドル) にパッケージ化されている
  - ホストの準備中に、NSX Manager により EAM (ESX Agency Manager) を介してインストールされる
  - ESXi netcpa でサービス デモンとして実行する
  - 起動スクリプト /etc/init.d/netcpad を使用して起動、停止、およびクエリを実行できる
  - リモートから ネットワークとセキュリティ ユーザー インターフェイスで [インストール手順] > [ホストの準備] > [インストールの状態] を使用して、個別のホストまたはクラスタ全体で再起動できる
- 分散論理ルーター カーネル モジュール (vdrb) と分散仮想スイッチの統合により L3 フォワーディングを有効にする
  - netcpa により設定される
  - VXLAN VIB 環境の一部としてインストールされる
  - VLAN と VXLAN の両方をサポートする特殊トランクの「vdrPort」を介して分散仮想スイッチに接続する
  - 各分散論理ルーター インスタンスについて次の情報を保持する
    - LIF およびルート テーブル
    - ホストとローカルの ARP キャッシュ
- netcpa、ESG および分散論理ルーター制御仮想マシンは、NSX Manager との通信のためにメッセージ バス クライアント (vsfwd) を使用する
  - vsfwd は、vpxa/hosd を介して vCenter Server により設定される /UserVars/RmqIpAddress から NSX Manager の IP アドレスを取得し、他の /UserVars/Rmq\* 変数に格納されているホスト別の証明書を使用してメッセージ バス サーバにログインする



- ESXi ホストで実行される netcpa は、次の動作のために vsfwd を使用する
  - NSX Manager からホストの制御プレーン SSL プライベート キーおよび証明書を取得する。これらの情報は /etc/vmware/ssl/rui-for-netcpa.\* に格納される。
  - NSX Manager からコントローラの IP アドレスと SSL サンプリントを取得する。これらの情報は /etc/vmware/netcpa/config-by-vsm.xml に格納される。
  - NSX Manager からの指示により、自らのホスト上で分散論理ルーター インスタンスの作成および削除を実行する。
- パッケージ化とデプロイ
  - netcpa と同様に、VXLAN VIB の一部としてパッケージ化
  - ESXi vsfwd のサービス デーモンとして実行
  - 起動スクリプト /etc/init.d/vShield-Stateful-Firewall を使用して起動、停止、およびクエリを実行できる
- ESG および分散論理ルーター制御仮想マシンは、vsfwd への VMCI チャンネルを使用して NSX Manager から設定を受信する

## 分散論理ルーター制御仮想マシンおよび ESG

- 分散論理ルーター制御仮想マシンは、分散論理ルーター インスタンスの「ルート プロセッサ」として機能する
  - IP アドレスの設定とともに、各分散論理ルーター LIF の「プレースホルダー」または「現実の vNIC」のインターフェイスを使用する
  - 使用可能な 2 つの動的ルーティング プロトコル（BGP または OSPF）のいずれかを実行したり、スタティック ルートを使用したりできる
  - 少なくとも 1 つの「アップリンク」LIF が OSPF または BGP を実行できる必要がある
  - 直接接続された (LIF) サブネット、スタティック ルート、および動的ルートからフォワーディング テーブルを計算し、netcpa への VMCI リンクを介して分散論理ルーター インスタンスのマスター コントローラに送信する
  - アクティブおよびスタンバイの 2 台の仮想マシンを使用する構成によって、高可用性をサポートする
- ESG は、仮想マシン内の自己完結型ルーター
  - NSX 分散論理ルーター ルーティング サブシステムから完全に独立する（NSX 制御プレーンに統合されない）
  - 通常は、1 つ以上の分散論理ルーター のアップストリーム ゲートウェイとして使用される
  - 同時に実行される複数の動的ルーティング プロトコルをサポートする

## NSX のルーティング制御プレーン CLI

ホスト コンポーネントに加えて、NSX のルーティングではコントローラ クラスタおよび分散論理ルーター制御仮想マシンのサービスが使用されます。これらは、それぞれ分散論理ルーター制御プレーンの情報ソースとなり、固有の CLI により情報を確認します。

## 分散論理ルーター インスタンスのマスター コントローラ

各分散論理ルーター インスタンスは、いずれかのコントローラ ノードに属します。次の CLI コマンドを使用すると、分散論理ルーター インスタンスについてマスターであるコントローラ ノードが持つ情報を表示できます。

```
nsx-controller # show control-cluster logical-routers instance 1460487509
LR-Id      LR-Name      Hosts[]      Edge-Connection Service-Controller
1460487509 default+edge-1 192.168.210.57      192.168.110.201
              192.168.210.51
              192.168.210.52
              192.168.210.56
              192.168.110.51
              192.168.110.52

nsx-controller # show control-cluster logical-routers interface-summary 1460487509
Interface      Type  Id      IP[]
570d45550000002 vxlan 5003    192.168.10.2/29
570d4555000000b vxlan 5001    172.16.20.1/24
570d4555000000c vxlan 5002    172.16.30.1/24
570d4555000000a vxlan 5000    172.16.10.1/24

nsx-controller # show control-cluster logical-routers routes 1460487509
LR-Id      Destination      Next-Hop
1460487509 0.0.0.0/0        192.168.10.1
```

- `show control-cluster logical-routers` コマンドの `instance` サブコマンドを使用すると、この分散論理ルーター インスタンス用として、このコントローラに接続されているホストのリストが表示されます。正常に機能している環境では、このリストには分散論理ルーターが存在するすべてのクラスタからのすべてのホストが含まれます。
- `interface-summary` サブコマンドを使用すると、コントローラが NSX Manager から学習した LIF が表示されます。この情報はホストに送信されます。
- `routes` サブコマンドは、この分散論理ルーター制御仮想マシンによってコントローラに送信されたルーティング テーブルが表示されます。この情報は LIF 設定によって提供されるため、ESXi ホストの場合とは異なり、この テーブルには直接接続されているサブネットは含まれません。

## 分散論理ルーター制御仮想マシン

分散論理ルーター制御仮想マシンには、LIF およびルーティング/フォワーディング テーブルが含まれます。分散論理ルーター制御仮想マシンのライフサイクルからの主な出力は、分散論理ルーター ルーティング テーブルです。この テーブルには、インターフェイスとルートの情報が含まれます。

```
edge-1-0> show ip route

Codes: 0 - OSPF derived, i - IS-IS derived, B - BGP derived,
C - connected, S - static, L1 - IS-IS level-1, L2 - IS-IS level-2,
IA - OSPF inter area, E1 - OSPF external type 1, E2 - OSPF external type 2

Total number of routes: 5
```

```

S      0.0.0.0/0          [1/1]      via 192.168.10.1
C      172.16.10.0/24     [0/0]      via 172.16.10.1
C      172.16.20.0/24     [0/0]      via 172.16.20.1
C      172.16.30.0/24     [0/0]      via 172.16.30.1
C      192.168.10.0/29    [0/0]      via 192.168.10.2

```

```

edge-1-0> show ip forwarding
Codes: C - connected, R - remote,
       > - selected route, * - FIB route
R>* 0.0.0.0/0 via 192.168.10.1, vNic_2
C>* 172.16.10.0/24 is directly connected, VDR
C>* 172.16.20.0/24 is directly connected, VDR
C>* 172.16.30.0/24 is directly connected, VDR
C>* 192.168.10.0/29 is directly connected, vNic_2

```

- フォワーディング テーブルは、ターゲット サブネットの出力方向として選択された分散論理ルーター インターフェイスを示すためのものです。
  - 「分散論理ルーター」インターフェイスは、「Internal」タイプのすべての LIF について表示されます。「分散論理ルーター」インターフェイスは、対応する vNIC を持たない擬似インターフェイスです。

分散論理ルーター制御仮想マシンのインターフェイスは、次のように表示されます。

```

edge-1-0> show interface
Interface VDR is up, line protocol is up
  index 2 metric 1 mtu 1500 <UP,BROADCAST,RUNNING,NOARP>
  HWaddr: be:3d:a1:52:90:f4
  inet6 fe80::bc3d:a1ff:fe52:90f4/64
  inet 172.16.10.1/24
  inet 172.16.20.1/24
  inet 172.16.30.1/24
  proxy_arp: disabled
  Auto-duplex (Full), Auto-speed (2460Mb/s)
    input packets 0, bytes 0, dropped 0, multicast packets 0
    input errors 0, length 0, overrun 0, CRC 0, frame 0, fifo 0, missed 0
    output packets 0, bytes 0, dropped 0
    output errors 0, aborted 0, carrier 0, fifo 0, heartbeat 0, window 0
    collisions 0

Interface vNic_0 is up, line protocol is up
  index 3 metric 1 mtu 1500 <UP,BROADCAST,RUNNING,MULTICAST>
  HWaddr: 00:50:56:8e:1c:fb
  inet6 fe80::250:56ff:fe8e:1cfb/64
  inet 169.254.1.1/30
  inet 10.10.10.1/24
  proxy_arp: disabled
  Auto-duplex (Full), Auto-speed (2460Mb/s)
    input packets 582249, bytes 37339072, dropped 49, multicast packets 0
    input errors 0, length 0, overrun 0, CRC 0, frame 0, fifo 0, missed 0
    output packets 4726382, bytes 461202852, dropped 0
    output errors 0, aborted 0, carrier 0, fifo 0, heartbeat 0, window 0
    collisions 0

Interface vNic_2 is up, line protocol is up

```

```

index 9 metric 1 mtu 1500 <UP,BROADCAST,RUNNING,MULTICAST>
HWaddr: 00:50:56:8e:ae:08
inet 192.168.10.2/29
inet6 fe80::250:56ff:fe8e:ae08/64
proxy_arp: disabled
Auto-duplex (Full), Auto-speed (2460Mb/s)
  input packets 361446, bytes 30167226, dropped 0, multicast packets 361168
  input errors 0, length 0, overrun 0, CRC 0, frame 0, fifo 0, missed 0
  output packets 361413, bytes 30287912, dropped 0
  output errors 0, aborted 0, carrier 0, fifo 0, heartbeat 0, window 0
  collisions 0

```

注：

- インターフェイス「分散論理ルーター」には、仮想マシン NIC (vNIC) が関連付けられていません。これは単一の「疑似インターフェイス」であり、分散論理ルーターのすべての「Internal」LIF について、すべての IP アドレスが設定されています。
- この例のインターフェイス vNic\_0 は、高可用性インターフェイスです。
  - 上記の出力は、高可用性を有効にしてデプロイされた分散論理ルーターから取得されたものであり、高可用性インターフェイスには IP アドレスが指定されています。これは 2 つの IP アドレスとして表示されています。169.254.1.1/30 は高可用性用として自動的に指定されたアドレスであり、10.10.10.1/24 は高可用性インターフェイスに手動で指定されたアドレスです。
  - ESG では、オペレータはいずれかの vNIC を高可用性として手動で指定できます。または、デフォルトのままにしておくことで、使用可能な「Internal」インターフェイスから自動的に選択されます。「Internal」タイプを使用することは必須条件です。そうでない場合は、高可用性が失敗します。
- インターフェイス vNic\_2 は Uplink タイプです。したがって、これは「現実」の vNIC として示されています。
  - このインターフェイスで示されている IP アドレスは、分散論理ルーターの LIF と同じです。しかし、分散論理ルーター制御仮想マシンは LIF IP アドレス（この例では 192.168.10.2/29）の ARP クエリには応答しません。この vNIC の MAC アドレスには、そのための ARP フィルタが適用されています。
  - ただし、動的ルーティング プロトコルが分散論理ルーターで設定されると、IP アドレスが ARP フィルタと一緒に削除され、動的ルーティング プロトコルの設定中に指定された「プロトコル IP」アドレスに置き換えられます。
  - この vNIC は、分散論理ルーター制御仮想マシンで実行される動的ルーティング プロトコルによって使用され、ルートの通知と学習のために他のルーターとの通信が行われます。
- Edge が切断され、高可用性フェイルオーバーが実行された後、切断されている Edge インターフェイスの IP アドレスが、アクティブ Edge のルーティング情報ベース (RIB)/転送情報ベース (FIB) から削除されます。スタンバイ Edge の FIB テーブルまたは show ip forwarding コマンドには IP アドレスが表示され、FIB テーブルから削除されません。これは、想定どおりの動作です。

## NSX のルーティング サブシステムの障害の状況と影響

この章では、NSX のルーティング サブシステムのコンポーネントに影響を与える可能性のある典型的な障害のシナリオを確認し、これらの障害の影響について概要を説明します。

## NSX Manager

表 3-2. NSX Manager の障害の状況と影響

障害の状況	障害の影響
NSX Manager 仮想マシンとのネットワーク接続が失われる	<ul style="list-style-type: none"> <li>■ NSX Manager のすべての機能（NSX ルーティング/ブリッジ用 CRUD を含む）が完全に停止する</li> <li>■ データは失われない</li> <li>■ データや制御プレーンは停止しない</li> </ul>
NSX Manager および ESXi ホストの間のネットワーク接続が失われる、または RabbitMQ サーバの障害が発生する	<ul style="list-style-type: none"> <li>■ 影響を受けるホストで分散論理ルーター制御仮想マシンまたは ESG が実行している場合は、それらの CRUD 操作が失敗する</li> <li>■ 影響を受けるホストの分散論理ルーター インスタンスの作成や削除が失敗する</li> <li>■ データは失われない</li> <li>■ データや制御プレーンは停止しない</li> <li>■ 動的ルーティングの更新は引き続き動作する</li> </ul>
NSX Manager とコントローラの間のネットワーク接続が失われる	<ul style="list-style-type: none"> <li>■ NSX の分散ルーティングおよびブリッジの作成、更新、および削除操作が失敗する</li> <li>■ データは失われない</li> <li>■ データや制御プレーンは停止しない</li> </ul>
NSX Manager 仮想マシンが破壊される（データストアの障害）	<ul style="list-style-type: none"> <li>■ NSX Manager のすべての機能（NSX ルーティング/ブリッジ用 CRUD を含む）が完全に停止する</li> <li>■ NSX Manager が以前のにリストアされた場合に、ルーティング/ブリッジ インスタンスのサブセットが実体のない状態になるリスクが生じ、手動のクリーンアップと調整が必要となる</li> <li>■ データや制御プレーンは停止しない（調整が必要になる場合を除く）</li> </ul>

## コントローラ クラスタ

表 3-3. NSX Controller の状況と影響

障害の状況	障害の影響
コントローラ クラスタが ESXi ホストとのネットワーク接続を失う	<ul style="list-style-type: none"> <li>■ 分散論理ルーター制御プレーンの機能（動的ルートを含むルートの作成、更新、および削除）が完全に停止する</li> <li>■ 分散論理ルーター管理プレーンの機能（ホストでの LIF の作成、更新、および削除）が停止する</li> <li>■ VXLAN フォワーディングが影響を受け、そのためにエンド ツー エンド (L2 + L3) のフォワーディング プロセスも失敗することがある</li> <li>■ データ プレーンは、最後に把握された状態に基づいて引き続き動作する</li> </ul>
1 台以上のコントローラが ESXi ホストとの接続を失う	<ul style="list-style-type: none"> <li>■ 影響を受けるコントローラがクラスタ内の他のコントローラに引き続きアクセスできる場合、このコントローラをマスターとする分散論理ルーター インスタンスが上記と同じ影響を受ける。他のコントローラには自動的に引き継がれない</li> </ul>
1 台のコントローラが、他のコントローラとのネットワーク接続、または完全なネットワーク接続を失う	<ul style="list-style-type: none"> <li>■ 分離されたコントローラによって処理されていた VXLAN と分散論理ルーターの処理を、残る 2 台のコントローラが引き継ぐ</li> <li>■ 影響を受けるコントローラが読み取り専用モードになり、ホストに対してセッションをドロップし、新しいセッションを拒否する</li> </ul>

表 3-3. NSX Controller の状況と影響（続き）

障害の状況	障害の影響
コントローラが相互の接続を失う	<ul style="list-style-type: none"> <li>■ すべてのコントローラが読み取り専用モードになり、ホストへの接続を閉じ、新しい接続を拒否する</li> <li>■ すべての分散論理ルーターの LIF およびルート（動的ルートを含む）の作成、更新、および削除操作が失敗する</li> <li>■ NSX Manager とコントローラ クラスタの間で NSX のルーティング設定 (LIF) が同期されなくなり、手動での同期が必要となることがある</li> <li>■ ホストは、最後に把握された制御プレーンの状態に基づいて稼動し続ける</li> </ul>
1 台のコントローラ仮想マシンが失われる	<ul style="list-style-type: none"> <li>■ コントローラ クラスタの冗長性が損なわれる</li> <li>■ 管理/制御プレーンは通常どおりに稼動し続ける</li> </ul>
2 台のコントローラ仮想マシンが失われる	<ul style="list-style-type: none"> <li>■ 残りのコントローラは読み取り専用モードになり、コントローラが相互の接続を失う場合（上記）と同じ影響がある。クラスタのリカバリを手動で実行しなければならない可能性が高い</li> </ul>

## ホスト モジュール

netcpa は、コントローラとの間で保護された通信を確立するために、SSL キーおよび証明書に加えて SSL サムプリントを使用します。これらは、メッセージ バス（vsfwd から提供）を介して NSX Manager から取得します。

証明書の交換プロセスが失敗すると、netcpa はコントローラに正常に接続できなくなります。

注：カーネル モジュールの障害は影響は深刻 (PSOD) であり、まれにしか起こらないものであることから、このセクションでは扱いません。

表 3-4. ホスト モジュールの障害の状況と影響

障害の状況	障害の影響
vsfwd がメッセージ バス サーバにアクセスするために認証で使用するユーザー名/パスワードが期限切れになることがある	<ul style="list-style-type: none"> <li>■ 新規に準備された ESXi ホストの vsfwd が 2 時間以内に NSX Manager にアクセスできない場合、インストール中に提供された一時ログイン/パスワードの有効期限が切れ、このホストのメッセージバスを操作できなくなる</li> </ul>
メッセージ バス クライアント (vsfwd) の障害の影響は、障害が発生したタイミングによって異なる。	
NSX 制御プレーンの他の部分が安定して実行するようになる前に障害が発生した場合	<ul style="list-style-type: none"> <li>■ ホストがコントローラと通信できないため、ホストの分散ルーティングが機能しなくなる</li> <li>■ ホストが NSX Manager から分散論理ルーター インスタンスを学習しない</li> </ul>
ホストが安定して実行するようになった後に障害が発生した場合	<ul style="list-style-type: none"> <li>■ ホストの ESG および分散論理ルーター制御仮想マシンは設定の更新を受信できない</li> <li>■ ホストは新しい分散論理ルーター インスタンスを学習せず、既存の分散論理ルーターを削除できない</li> <li>■ ホストのデータバスは、障害発生時にホストが把握していた設定に基づいて動作し続ける</li> </ul>

表 3-5. netcpa の障害の状況と影響

障害の状況	障害の影響
制御プレーン エージェント (netcpa) の障害の影響は、障害が発生したタイミングによって異なる	
NSX データベースのカーネル モジュールが安定して実行するようになる前に障害が発生した場合	<ul style="list-style-type: none"> <li>■ ホストの分散ルーティングが機能しなくなる</li> </ul>
ホストが安定して実行するようになった後に障害が発生した場合	<ul style="list-style-type: none"> <li>■ ホストで実行される分散論理ルーター制御仮想マシンが、コントローラにフォワーディング テーブルの更新を送信できない</li> <li>■ 分散ルーティングのデータベースは、コントローラから LIF またはルートの更新を受信しなくなるが、障害発生時に把握していた設定に基づいて動作し続ける</li> </ul>

## 分散論理ルーター制御仮想マシン

表 3-6. 分散論理ルーター制御仮想マシンの障害の状況と影響

障害の状況	障害の影響
分散論理ルーター制御仮想マシンが失われる、またはパワーオフされる	<ul style="list-style-type: none"> <li>■ 分散論理ルーターの LIF およびルートの作成、更新、および削除操作が失敗する</li> <li>■ 動的ルートの更新（解除された隣接関係を介して受信していたブリフィックスの取り消しを含む）がホストに送信されない</li> </ul>
分散論理ルーター制御仮想マシンが、NSX Manager およびコントローラとの接続を失う	<ul style="list-style-type: none"> <li>■ 上記と同じ影響があるが、分散論理ルーター制御仮想マシンとそのルーティングの隣接関係が引き続き動作している場合は、以前に学習したブリフィックスとの間のトラフィックは影響を受けない</li> </ul>
分散論理ルーター制御仮想マシンが、NSX Manager との接続を失う	<ul style="list-style-type: none"> <li>■ NSX Manager での、この分散論理ルーターの LIF およびルートの作成、更新、および削除操作が失敗し、再試行されない</li> <li>■ 動的ルーティングの更新は引き続き送信される</li> </ul>
分散論理ルーター制御仮想マシンが、コントローラとの接続を失う	<ul style="list-style-type: none"> <li>■ この分散論理ルーターのルーティングの変更（固定または動的）は、ホストに送信されない</li> </ul>

## ルーティングに関連する NSX ログ

ベスト プラクティスとして、ログを中央のコレクタに送信するように NSX のすべてのコンポーネントを設定しすることをお勧めします。

必要に応じて、NSX コンポーネントのログ レベルを変更できます。詳細については、『NSX のログ作成とシステムイベント』で「NSX コンポーネントのログ レベルの設定」を参照してください。

### NSX Manager のログ

- NSX Manager CLI の show log コマンド
- テクニカル サポート ログ バンドル（NSX Manager ユーザー インターフェイスで収集されます）

## NSX Manager Virtual Appliance Management



NSX Manager のログには、管理プレーンに関連する情報が含まれます。この情報の対象範囲は、CRUD（作成、読み取り、更新、削除）の操作です。

## コントローラのログ

コントローラには複数のモジュールが含まれ、その多くでは独自のログ ファイルが使用されます。コントローラのログには、`show log <log file> [ filtered-by <string> ]` コマンドを使用してアクセスできます。ルーティングに関連するログ ファイルは、次のとおりです。

- `cloudnet/cloudnet_java-vnet-controller.<開始時のタイムスタンプ>.log`：このログは、設定と内部の API サーバを管理します。
- `cloudnet/cloudnet.nsx-controller.log`：コントローラのメイン プロセスのログです。
- `cloudnet/cloudnet_cpp.log.nsx-controller.log`：このログは、クラスタリングとブートストラップを管理します。
- `cloudnet/cloudnet_cpp.log.ERROR`：このファイルは、エラーが発生した場合に作成されます。

コントローラのログには詳細情報が含まれます。ほとんどの場合、VMware のエンジニアリング チームが困難な問題を解決するために必要となります。

CLI の `show log` コマンドに加えて、`watch log <logfile> [ filtered-by <string> ]` コマンドを使用することで個々のログ ファイルの更新状況をリアル タイムで確認できます。

ログは、コントローラ サポート バンドルに含まれます。このサポート バンドルを生成してダウンロードするには、NSX ユーザー インターフェイスでコントローラ ノードを選択して、[テクニカル サポート ログのダウンロード (Download tech support logs)] アイコンをクリックします。

## ESXi ホストのログ

ESXi ホストで実行される NSX コンポーネントによって、いくつかの種類のログ ファイルが作成されます。

- VMkernel のログ： `/var/log/vmkernel.log`
- 制御プレーン エージェントのログ： `/var/log/netcpa.log`
- メッセージ バス クライアントのログ： `/var/log/vsfwd.log`

vCenter Server から生成される仮想マシン サポート バンドルの一部として、ログを収集することも可能です。ログ ファイルにアクセスできるのは、`root` 権限を持つユーザーまたはユーザー グループだけです。



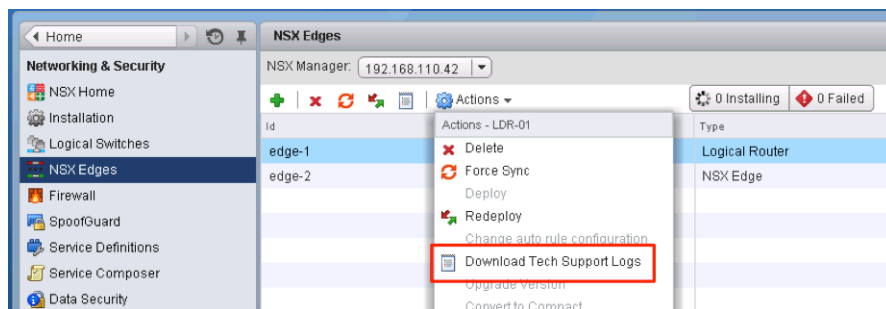
## ESG/分散論理ルーター制御仮想マシンのログ

ESG および分散論理ルーター制御仮想マシンのログ ファイルにアクセスする方法は 2 種類あります。CLI を使用して表示する方法と、CLI またはユーザー インターフェイスを使用してテクニカル サポート バンドルをダウンロードする方法です。

ログを表示するための CLI コマンドは、`show log [ follow | reverse ]` です。

テクニカル サポート バンドルをダウンロードするには、次の手順を実行します。

- CLI から、enable モードを使用して `export tech-support <[ scp | ftp ]> <URI>` コマンドを実行します。
- vSphere Web Client から、[アクション (Actions)] メニューの [テクニカル サポート ログのダウンロード (Download Tech Support Logs)] オプションを選択します。



## その他の役立つファイル、およびファイルの場所

正確にはログではありませんが、NSX のルーティングの理解とトラブルシューティングに役立つファイルが多数あります。

- 制御プレーン エージェント設定の `/etc/vmware/netcpa/config-by-vsm.xml` には、次のコンポーネントに関する情報が含まれます。
  - コントローラ、IP アドレス、TCP ポート、証明書のサムプリント、SSL の有効/無効
  - VXLAN を使用して有効にされた分散仮想スイッチの dvUplink (チーミング ポリシー、名前、UUID)
  - ホストが把握する分散論理ルーター インスタンス (DLR ID、名前)
- 制御プレーン エージェント設定の `/etc/vmware/netcpa/netcpa.xml` には、ログ レベル (デフォルトは [info]) など、netcpa の多様な設定オプションが含まれます。
- 制御プレーンの証明書ファイル: `/etc/vmware/ssl/rui-for-netcpa.*`
  - 2 つのファイル: ホスト証明書、ホストのプライベート キー
  - コントローラでホストの接続を認証するために使用

これらのファイルはすべて、vsfwd によるメッセージ バス接続を介して NSX Manager から受信する情報を使用して、制御プレーン エージェントによって作成されます。

## 一般的な障害のシナリオと解決方法

一般的な障害のシナリオは 2 つに分類されます。

一般的に、問題が発生するのは設定および制御プレーンです。管理プレーンで問題が発生する可能性もありますが、一般的ではありません。

## 設定の問題と解決方法

一般的な設定の問題と影響については、表 3-7. 一般的な構成の問題と影響に記載されています。

表 3-7. 一般的な構成の問題と影響

問題	影響
動的ルーティングでは、プロトコル IP アドレスとフォワーディング IP アドレスが逆になる	動的プロトコルの隣接関係が提示されない
トランスポート ゾーンが分散仮想スイッチの境界と一致していない	分散ルーティングがトランスポート ゾーンに含まれない ESXi ホストのサブセットで動作しない
動的ルーティング プロトコル設定の組み合わせが不適切（タイマー、MTU、BGP ASN、パスワード、インターフェイスから OSPF 領域へのマッピング）	動的プロトコルの隣接関係が提示されない
分散論理ルーター高可用性インターフェイスが IP アドレスに割り当てられ、接続ルートの再分散が有効になる	分散論理ルーター制御仮想マシンに高可用性インターフェイス サブネットのトラフィックが集中し、トラフィックがブラックホール状態になる

これらの問題を解決するには、設定を見直し、必要に応じて修正します。

必要な場合は、プロトコルの設定の問題を検出するために、CLI コマンドの `debug ip ospf` または `debug ip bgp` を使用して、分散論理ルーター制御仮想マシンまたは Edge サービス ゲートウェイ (ESG) コンソール (SSH セッションを経由しない) でログを確認します。

## 制御プレーンの問題と解決方法

制御プレーンの問題は、次の問題によって引き起こされる場合があります。

- ホスト制御プレーン エージェント (`netcpa`) が、`vsfwd` により提供されるメッセージ バス チャネルから NSX Manager に接続できない
  - コントローラ クラスタで、分散論理ルーター/VXLAN インスタンスのマスター ロールの処理に問題がある
- マスター ロールの処理に関連するコントローラ クラスタの問題は、NSX Controller のいずれかを再起動 (NSX Controller の CLI で `restart controller` を使用) することで解決できる場合があります。

制御プレーンに関する問題のトラブルシューティングについては、<http://kb.vmware.com/kb/2125767> を参照してください。

## トラブルシューティング データの収集

このセクションでは、NSX のルーティングをトラブルシューティングするときに一般的に使用される CLI コマンドの概要について説明します。

### NSX Manager

NSX ルーティングのトラブルシューティングを行うため、NSX Controller および他の NSX コンポーネントから実行されていたコマンドは、NSX 6.2 以降では、NSX Manager から直接実行されます。

- 分散論理ルーター インスタンスのリスト

- 各分散論理ルーター インスタンスの LIF のリスト
- 各分散論理ルーター インスタンスのルートへのリスト
- 分散論理ルーター ブリッジ インスタンスの MAC アドレスのリスト
- インターフェイス
- ルーティングとフォワーディング テーブル
- 動的ルーティング プロトコル (OSPF または BGP) の状態
- NSX Manager によって分散論理ルーター制御仮想マシンまたは Edge Service Gateway (ESG) に送信される設定

## 分散論理ルーター制御仮想マシンおよび ESG

分散論理ルーター制御仮想マシンおよび ESG は、インターフェイスでパケットをキャプチャする機能を提供します。パケット キャプチャは、ルーティング プロトコルの問題のトラブルシューティングに役立ちます。

- 1 `show interfaces` を実行して、インターフェイスの名を一覧表示します。
- 2 `debug packet [ display | capture ] interface <interface name>` を実行します。
  - キャプチャを使用している場合、パケットは .pcap ファイルに保存されます。
- 3 `debug show files` を実行して、保存されたキャプチャ ファイルを一覧表示します。
- 4 `debug copy [ scp | ftp ] ...` を実行して、オフライン分析のためにキャプチャをダウンロードします。

```
d1r-01-0> debug packet capture interface vNic_2
tcpdump: listening on vNic_2, link-type EN10MB (Ethernet), capture size 65535 bytes
43 packets captured
48 packets received by filter
0 packets dropped by kernel
```

```
d1r-01-0> debug show files
total 4.0K
-rw----- 1 3.6K Mar 30 23:49 tcpdump_vNic_2.0
```

```
d1r-01-0> debug copy
  scp  use scp to copy
  ftp  use ftp to copy
```

```
d1r-01-0> debug copy scp
URL  user@<remote-host>:<path-to>
```

`debug packet` コマンドは `tcpdump` をバックグラウンドで使用し、UNIX における `tcpdump` のフィルタリング修飾子のような形式で、フィルタリング修飾子を受け入れます。フィルタ式の空白文字はアンダースコア ( `_` ) で置換する必要があることにのみ注意してください。

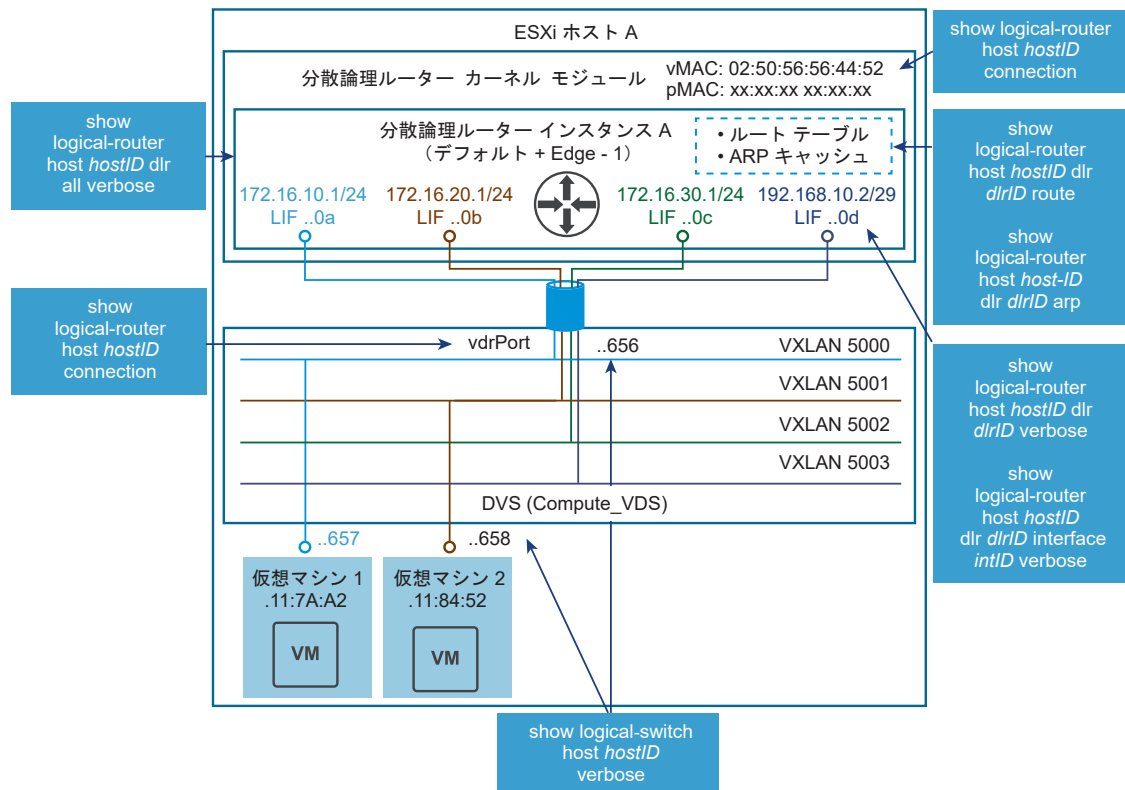
たとえば、次のコマンドは、SSH を除いて vNic\_0 を通過するすべてのトラフィックを表示し、インタラクティブセッション自体に属するトラフィックの検索は回避します。

```
plr-02-0> debug packet display interface vNic_0 port_not_22
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on vNic_0, link-type EN10MB (Ethernet), capture size 65535 bytes
04:10:48.197768 IP 192.168.101.3.179 > 192.168.101.2.25698: Flags [P.], seq 4191398894:4191398913,
ack 2824012766, win 913, length 19: BGP, length: 19
04:10:48.199230 IP 192.168.101.2.25698 > 192.168.101.3.179: Flags [.], ack 19, win 2623, length 0
04:10:48.299804 IP 192.168.101.2.25698 > 192.168.101.3.179: Flags [P.], seq 1:20, ack 19, win 2623,
length 19: BGP, length: 19
04:10:48.299849 IP 192.168.101.3.179 > 192.168.101.2.25698: Flags [.], ack 20, win 913, length 0
04:10:49.205347 IP 192.168.101.3.179 > 192.168.101.2.25698: Flags [P.], seq 19:38, ack 20, win 913,
length 19: BGP, length: 19
```

## ESXi ホスト

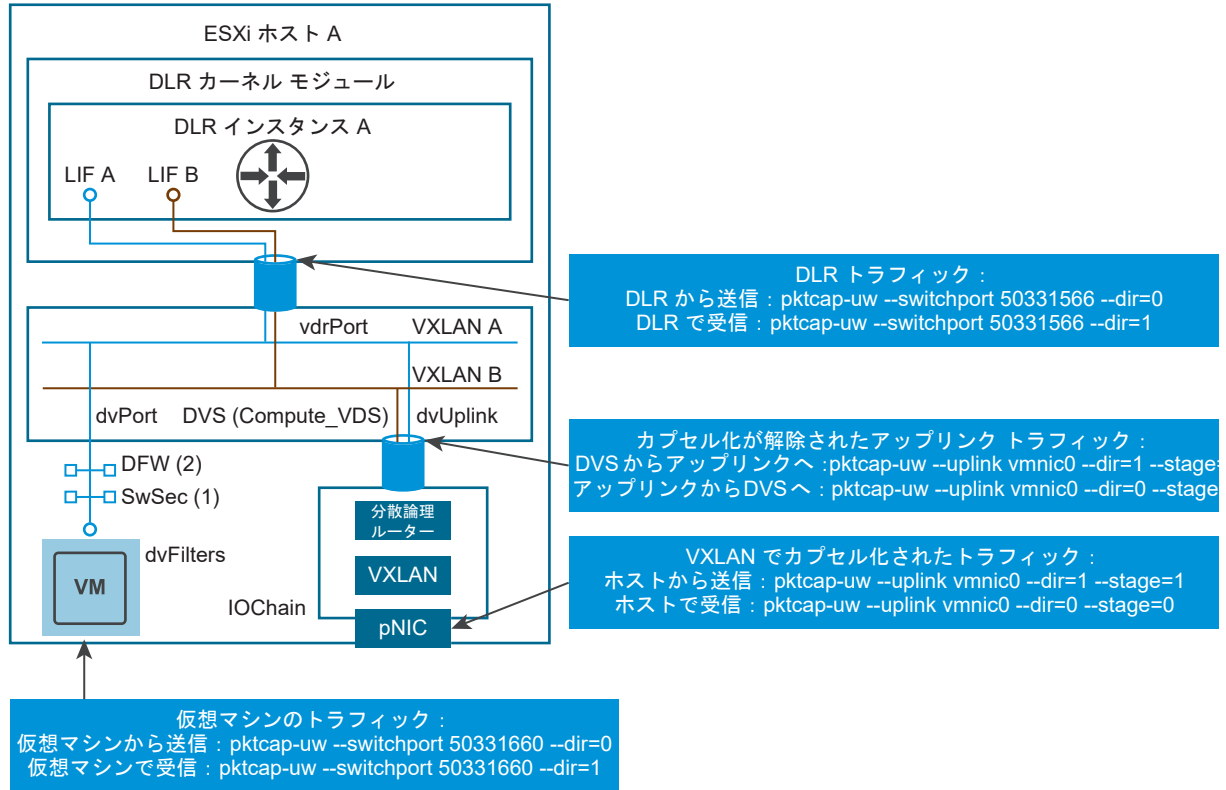
ホストは、NSX ルーティングと緊密に連携します。図 3-14. NSX ルーティングのトラブルシューティングに関するホスト コンポーネント は、ルーティング サブシステムに参加するコンポーネントとこれらの情報を表示するために使用される NSX Manager CLI コマンドを示しています。

図 3-14. NSX ルーティングのトラブルシューティングに関するホスト コンポーネント



データパスでキャプチャされたパケットは、パケット フォワーディングのさまざまな段階における問題の特定に役立つ場合があります。図 3-15. キャプチャ ポイントと関連する CLI コマンド は、主なキャプチャ ポイントと、各ポイントで使用する CLI コマンドを示しています。

図 3-15. キャプチャ ポイントと関連する CLI コマンド



# NSX Edge のトラブルシューティング

# 4

このトピックでは、VMware NSX Edge を理解してトラブルシューティングを行うための情報を提供します。

NSX Edge アプライアンスの問題をトラブルシューティングするには、次のトラブルシューティング手順が環境に当てはまるかどうかを確認します。各手順では、問題の原因を取り除き、必要に応じて修正アクションを実行するための方法とドキュメントへのリンクが提供されています。ここでは、問題を切り分けて適切な解決策を特定するために最適な手順を記載しています。どの手順も省略しないでください。

本リリースのリリース ノートで、この問題が解決されているかを確認します。

VMware NSX Edge をインストールする場合、最小システム要件を満たしていることを確認します。『NSX インストール ガイド』を参照してください。

## インストールとアップグレードの問題

- 発生している問題が「Would Block」の問題に関連していないことを確認します。詳細については、<https://kb.vmware.com/kb/2107951> を参照してください。
- アップグレードや再デプロイが成功するのに、Edge インターフェイスに接続できない場合は、バックエンドのレイヤー 2 スイッチの接続を確認してください。<https://kb.vmware.com/kb/2135285> を参照してください。
- Edge のデプロイやアップグレードで、次のエラーが表示され失敗する場合：

```
/sbin/ifconfig vNic_1 up failed : SIOCSIFFLAGS: Invalid argument
```

また

- デプロイやアップグレードが成功したにも関わらず、Edge インターフェイスに接続できない場合：
- `show interface` コマンドを実行すると、次のようなエントリが表示されます。これらのエントリは Edge のサポート ログにも表示されます。

```
vNic_0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc mq state DOWN qlen 1000
link/ether 00:50:56:32:05:03 brd ff:ff:ff:ff:ff:ff
inet 21.12.227.244/23 scope global vNic_0
inet6 fe80::250:56ff:fe32:503/64 scope link tentative dadfailed
valid_lft forever preferred_lft forever
```

いずれの場合も、ホスト スイッチの準備ができていないか、問題がいくつか発生しています。解決するには、ホスト スイッチを確認します。

## 設定の問題

- NSX Edge の診断情報を収集します。<https://kb.vmware.com/kb/2079380> を参照してください。

vse\_die の文字列で検索し、NSX Edge ログをフィルタします。この文字列の周辺のログに、設定エラーに関する情報が示されていることがあります。

## CPU 使用率が高い

NSX Edge の CPU 使用率が高くなっている場合には、esxtop コマンドを ESXi ホストで使用して、アプライアンスのパフォーマンスを確認します。次のナレッジベースの記事を確認します。

- <https://kb.vmware.com/kb/1008205>
- <https://kb.vmware.com/kb/1008014>
- <https://kb.vmware.com/kb/1010071>
- <https://kb.vmware.com/kb/2096171>

また、<https://communities.vmware.com/docs/DOC-9279> を参照してください。

ksoftirqd プロセスの値が高い場合、受信パケット レートが高いことを示します。ファイアウォール ルールのログなど、データ パスでログが有効になっていることを確認します。show log follow コマンドを実行して、該当するログが多数記録されているかどうかを判別します。

## パケット ドロップの統計の表示

NSX for vSphere 6.2.3 以降では、show packet drops コマンドを使用して、次のパケット ドロップの統計を表示できます。

- インターフェイス
- ドライバ
- L2
- L3
- ファイアウォール

コマンドを実行するには、NSX Edge の CLI にログインし、基本モードにします。詳細については、『NSX コマンド ライン インターフェイス リファレンス』を参照してください。次はその例です。

```
show packet drops
```

```
vShield Edge Packet Drop Stats:
```

```
Driver Errors
```

```
=====
```

	TX	TX	TX	RX	RX	RX
Interface	Dropped	Error	Ring	Full	Dropped	Error
vNic_0	0	0	0	0	0	0
vNic_1	0	0	0	0	0	0
vNic_2	0	0	0	0	0	2
vNic_3	0	0	0	0	0	0
vNic_4	0	0	0	0	0	0
vNic_5	0	0	0	0	0	0

## Interface Drops

=====

Interface RX Dropped TX Dropped

vNic_0	4	0
vNic_1	2710	0
vNic_2	0	0
vNic_3	2	0
vNic_4	2	0
vNic_5	2	0

## L2 RX Errors

=====

Interface length crc frame fifo missed

vNic_0	0	0	0	0	0
vNic_1	0	0	0	0	0
vNic_2	0	0	0	0	0
vNic_3	0	0	0	0	0
vNic_4	0	0	0	0	0
vNic_5	0	0	0	0	0

## L2 TX Errors

=====

Interface aborted fifo window heartbeat

vNic_0	0	0	0	0
vNic_1	0	0	0	0
vNic_2	0	0	0	0
vNic_3	0	0	0	0
vNic_4	0	0	0	0
vNic_5	0	0	0	0

## L3 Errors

=====

## IP:

ReasmFails : 0  
 InHdrErrors : 0  
 InDiscards : 0  
 FragFails : 0  
 InAddrErrors : 0  
 OutDiscards : 0  
 OutNoRoutes : 0  
 ReasmTimeout : 0

## ICMP:

InTimeExcds : 0  
 InErrors : 227  
 OutTimeExcds : 0  
 OutDestUnreachs : 152



```

OutParmProbs : 0
InSrcQuenchs : 0
InRedirects : 0
OutSrcQuenchs : 0
InDestUnreachs : 151
OutErrors : 0
InParmProbs : 0

Firewall Drop Counters
=====

Ipv4 Rules
=====
Chain - INPUT
rid pkts bytes target prot opt in out source destination
0 119 30517 DROP all -- * * 0.0.0.0/0 0.0.0.0/0 state INVALID
0 0 0 DROP all -- * * 0.0.0.0/0 0.0.0.0/0
Chain - POSTROUTING
rid pkts bytes target prot opt in out source destination
0 101 4040 DROP all -- * * 0.0.0.0/0 0.0.0.0/0 state INVALID
0 0 0 DROP all -- * * 0.0.0.0/0 0.0.0.0/0

Ipv6 Rules
=====
Chain - INPUT
rid pkts bytes target prot opt in out source destination
0 0 0 DROP all * * ::/0 ::/0 state INVALID
0 0 0 DROP all * * ::/0 ::/0
Chain - POSTROUTING
rid pkts bytes target prot opt in out source destination
0 0 0 DROP all * * ::/0 ::/0 state INVALID
0 0 0 DROP all * * ::/0 ::/0

```

## NSX Edge の管理において予期される動作

- vSphere Web Client で、ESX Edge に L2 VPN を設定し、[サイト構成の詳細 (Site Configuration Details)] を追加、削除、変更すると、既存の接続がすべて切断されてから再接続されます。これは通常の動作です。
- NSX Edge は仮想マシンで、ストレージ デバイスに格納された複数のファイルで構成されます。主要なファイルは、構成ファイル、仮想ディスク ファイル、NVRAM 設定ファイル、スワップ ファイル、ログ ファイルです。仮想マシンの構成ファイル、仮想ディスク ファイル、スワップ ファイルは、適用された仮想マシン ストレージ プロファイルや手動配置での設定に応じて、同じ場所または異なるデータストアの別々の場所に保存されます。仮想マシン ファイルが別々の場所に保存されている場合、NSX Manager は仮想マシンのデプロイで VMX ファイルのあるデータストアを表示し、使用します。再デプロイまたはアップグレードを行うときに、NSX Manager は、設定済みのデータストアまたは VMX ファイルを含むライブ データストアに NSX Edge 仮想マシンをデプロイします。データストア名とデータストア ID (仮想マシンの VMX ファイルがある場所) が、

Appliance パラメータの一部として返され、ユーザー インターフェイスに表示されたり、REST API の応答として提供されます。NSX Manager 仮想マシン ファイルとこれらのファイルが保存されるデータストアの正確なレイアウトについては、vCenter Server を参照してください。詳細については、次のドキュメントを参照してください。

- *vSphere* 仮想マシン管理者
- *vSphere* リソース管理
- *vCenter Server* およびホストの管理

この章には、次のトピックが含まれています。

- [Edge ファイアウォールでパケットがドロップする問題](#)
- [Edge ルーティング接続の問題](#)
- [NSX Manager と Edge の通信の問題](#)
- [メッセージ バスのデバッグ](#)
- [Edge の診断とリカバリ](#)

## Edge ファイアウォールでパケットがドロップする問題

### ファイアウォール パケット ドロップの統計表示

NSX for vSphere 6.2.3 以降では、show packet drops コマンドを使用して、ファイアウォール パケット ドロップの統計を表示できます。

コマンドを実行するには、NSX Edge の CLI にログインし、基本モードにします。詳細については、『NSX コマンド ライン インターフェイス リファレンス』を参照してください。次はその例です。

```
show packet drops

vShield Edge Packet Drop Stats:

Firewall Drop Counters
=====

Ipv4 Rules
=====
Chain - INPUT
rid pkts bytes target prot opt in out source destination
0 119 30517 DROP all -- * * 0.0.0.0/0 0.0.0.0/0 state INVALID
0 0 0 DROP all -- * * 0.0.0.0/0 0.0.0.0/0
Chain - POSTROUTING
rid pkts bytes target prot opt in out source destination
0 101 4040 DROP all -- * * 0.0.0.0/0 0.0.0.0/0 state INVALID
0 0 0 DROP all -- * * 0.0.0.0/0 0.0.0.0/0

Ipv6 Rules
=====
```

```
Chain - INPUT
rid pkts bytes target prot opt in out source destination
0 0 0 DROP all * * ::/0 ::/0 state INVALID
0 0 0 DROP all * * ::/0 ::/0
Chain - POSTROUTING
rid pkts bytes target prot opt in out source destination
0 0 0 DROP all * * ::/0 ::/0 state INVALID
0 0 0 DROP all * * ::/0 ::/0
```

## Edge パケット ファイアウォールの問題

コマンドを実行するには、NSX Edge の CLI にログインし、基本モードにします。詳細については、『NSX コマンド ライン インターフェイス リファレンス』を参照してください。

- 1 `show firewall` コマンドを使用して、ファイアウォール ルール テーブルを確認します。`usr_rules` テーブルに、設定されているルールが表示されます。

```
nsxedge> show firewall
Chain PREROUTING (policy ACCEPT 3146M packets, 4098G bytes)
rid  pkts bytes target  prot opt in      out      source      destination

Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
rid  pkts bytes target  prot opt in      out      source      destination
0    78903 16M ACCEPT  all -- lo      *      0.0.0.0/0  0.0.0.0/0
0      0 0 DROP    all -- *      *      0.0.0.0/0  0.0.0.0/0
state INVALID
0    140K 9558K block_in all -- *      *      0.0.0.0/0  0.0.0.0/0
0    23789 1184K ACCEPT  all -- *      *      0.0.0.0/0  0.0.0.0/0
state RELATED,ESTABLISHED
0    116K 8374K usr_rules all -- *      *      0.0.0.0/0  0.0.0.0/0
0      0 0 DROP    all -- *      *      0.0.0.0/0  0.0.0.0/0

Chain FORWARD (policy ACCEPT 3146M packets, 4098G bytes)
rid  pkts bytes target  prot opt in      out      source      destination

Chain OUTPUT (policy ACCEPT 173K packets, 22M bytes)
rid  pkts bytes target  prot opt in      out      source      destination

Chain POSTROUTING (policy ACCEPT 0 packets, 0 bytes)
rid  pkts bytes target  prot opt in      out      source      destination
0    78903 16M ACCEPT  all -- *      lo      0.0.0.0/0  0.0.0.0/0
0    679K 41M DROP    all -- *      *      0.0.0.0/0  0.0.0.0/0
state INVALID
0    3146M 4098G block_out all -- *      *      0.0.0.0/0  0.0.0.0/0
0      0 0 ACCEPT  all -- *      *      0.0.0.0/0  0.0.0.0/0
PHYSDEV match --physdev-in tap0 --physdev-out vNic_+
0      0 0 ACCEPT  all -- *      *      0.0.0.0/0  0.0.0.0/0
PHYSDEV match --physdev-in vNic_+ --physdev-out tap0
0      0 0 ACCEPT  all -- *      *      0.0.0.0/0  0.0.0.0/0
PHYSDEV match --physdev-in na+ --physdev-out vNic_+
0      0 0 ACCEPT  all -- *      *      0.0.0.0/0  0.0.0.0/0
PHYSDEV match --physdev-in vNic_+ --physdev-out na+
0    3145M 4098G ACCEPT  all -- *      *      0.0.0.0/0  0.0.0.0/0
state RELATED,ESTABLISHED
```

0	221K	13M	usr_rules	all	--	*	*	0.0.0.0/0	0.0.0.0/0
0	0	0	DROP	all	--	*	*	0.0.0.0/0	0.0.0.0/0
Chain block_in (1 references)									
rid	pkts	bytes	target	prot	opt	in	out	source	destination
Chain block_out (1 references)									
rid	pkts	bytes	target	prot	opt	in	out	source	destination
Chain usr_rules (2 references)									
rid	pkts	bytes	target	prot	opt	in	out	source	destination
131074	70104	5086K	ACCEPT	all	--	*	*	0.0.0.0/0	0.0.0.0/0
match-set 0_131074-os-v4-1 src									
131075	116K	8370K	ACCEPT	all	--	*	*	0.0.0.0/0	0.0.0.0/0
match-set 1_131075-ov-v4-1 dst									
131073	151K	7844K	ACCEPT	all	--	*	*	0.0.0.0/0	0.0.0.0/0

show firewall コマンドの POST\_ROUTING セクションにある DROP invalid ルールの増分値を確認します。一般的な原因は次のとおりです。

- 非対称ルーティングの問題
- TCP ベースのアプリケーションが 1 時間以上無効になっています。一定時間操作がないためにタイムアウトが発生し、アプリケーションが長時間アイドル状態になっている場合は、REST API を使用して inactivity-timeout の設定値を増やします。<https://kb.vmware.com/kb/2101275> を参照してください。

## 2 show ipset コマンドの出力を収集します。

```
nsxedge> show ipset
Name: 0_131074-os-v4-1
Type: bitmap:if (Interface Match)
Revision: 3
Header: range 0-64000
Size in memory: 8116
References: 1
Number of entries: 1
Members:
vse (vShield Edge Device)

Name: 0_131074-os-v6-1
Type: bitmap:if (Interface Match)
Revision: 3
Header: range 0-64000
Size in memory: 8116
References: 1
Number of entries: 1
Members:
vse (vShield Edge Device)

Name: 1_131075-ov-v4-1
Type: hash:oservice (Match un-translated Ports)
Revision: 2
Header: family inet hashsize 64 maxelem 65536
```

```

Size in memory: 704
References: 1
Number of entries: 2
Members:
Proto=6, DestPort=179, SrcPort=Any    (encoded: 0.6.0.179,0.6.0.0/16)
Proto=89, DestPort=Any, SrcPort=Any    (encoded: 0.89.0.0/16,0.89.0.0/16)

Name: 1_131075-ov-v6-1
Type: hash:oservice (Match un-translated Ports)
Revision: 2
Header: family inet hashsize 64 maxelem 65536
Size in memory: 704
References: 1
Number of entries: 2
Members:
Proto=89, DestPort=Any, SrcPort=Any    (encoded: 0.89.0.0/16,0.89.0.0/16)
Proto=6, DestPort=179, SrcPort=Any    (encoded: 0.6.0.179,0.6.0.0/16)

```

- 3 REST API や Edge ユーザー インターフェイスを使用して、特定のファイアウォール ルールのログを有効にし、`show log follow` コマンドを使用してこのログを監視します。

ログが表示されない場合、次の REST API を使用して、DROP Invalid ルールのログを有効にします。

```

URL : https://NSX_Manager_IP/api/4.0/edges/{edgeId}/firewall/config/global

PUT Method
Input representation
<globalConfig>    <!-- Optional -->
<tcpPickOngoingConnections>false</tcpPickOngoingConnections>    <!-- Optional. Defaults to false -->
<tcpAllowOutOfWindowPackets>false</tcpAllowOutOfWindowPackets>    <!-- Optional. Defaults to false -->
<tcpSendResetForClosedVsePorts>true</tcpSendResetForClosedVsePorts>    <!-- Optional. Defaults to true -->
<dropInvalidTraffic>true</dropInvalidTraffic>    <!-- Optional. Defaults to true -->
<logInvalidTraffic>true</logInvalidTraffic>    <!-- Optional. Defaults to false -->
<tcpTimeoutOpen>30</tcpTimeoutOpen>    <!-- Optional. Defaults to 30 -->
<tcpTimeoutEstablished>3600</tcpTimeoutEstablished>    <!-- Optional. Defaults to 3600 -->
<tcpTimeoutClose>30</tcpTimeoutClose>    <!-- Optional. Defaults to 30 -->
<udpTimeout>60</udpTimeout>    <!-- Optional. Defaults to 60 -->
<icmpTimeout>10</icmpTimeout>    <!-- Optional. Defaults to 10 -->
<icmp6Timeout>10</icmp6Timeout>    <!-- Optional. Defaults to 10 -->
<ipGenericTimeout>120</ipGenericTimeout>    <!-- Optional. Defaults to 120 -->
</globalConfig>
Output representation
No payload

```

show log follow コマンドを使用して、次のようなログを検索します。

```
2016-04-18T20:53:31+00:00 edge-0 kernel: nf_ct_tcp: invalid TCP flag combination IN= OUT=
SRC=172.16.1.4 DST=192.168.1.4 LEN=40 TOS=0x00 PREC=0x00 TTL=64 ID=43343 PROTO=TCP
SPT=5050 DPT=80 SEQ=0 ACK=1572141176 WINDOW=512 RES=0x00 URG PSH FIN URGP=0
2016-04-18T20:53:31+00:00 edge-0 kernel: INVALID IN= OUT=vNic_1 SRC=172.16.1.4
DST=192.168.1.4 LEN=40 TOS=0x00 PREC=0x00 TTL=63 ID=43343 PROTO=TCP SPT=5050 DPT=80
WINDOW=512 RES=0x00 URG PSH FIN URGP=0
```

- 4 show flowtable rule\_id コマンドを使用して、Edge ファイアウォールの状態テーブルで一致する接続を確認します。

```
nsxedge> show flowtable
1: tcp 6 21554 ESTABLISHED src=192.168.110.10 dst=192.168.5.3 sport=25981
dport=22 pkts=52 bytes=5432 src=192.168.5.3 dst=192.168.110.10 sport=22 dport=259
81 pkts=44 bytes=7201 [ASSURED] mark=0 rid=131073 use=1
2: tcp 6 21595 ESTABLISHED src=127.0.0.1 dst=127.0.0.1 sport=53194
dport=10 001 pkts=33334 bytes=11284650 src=127.0.0.1 dst=127.0.0.1 sport=10001 dport=5319
4 pkts=33324 bytes=1394146 [ASSURED] mark=0 rid=0 use=1
```

show flowstats コマンドを使用して、アクティブな接続数と許可される最大接続数を比較します。

```
nsxedge> show flowstats
Total Flow Capacity: 65536
Current Statistics :
cpu=0 searched=3280373 found=3034890571 new=52678 invalid=659946 ignore=77605
delete=52667 delete_list=49778 insert=49789 insert_failed=0 drop=0 early_drop=0
error=0 search_restart=0
```

- 5 show log follow コマンドを使用して Edge のログを確認して、ALG のドロップがないか確認します。tftp\_alg、msrpc\_alg、または oracle\_tns のような文字列を検索します。詳細については、以下を参照してください。

- <https://kb.vmware.com/kb/2126674>
- <https://kb.vmware.com/kb/2137751>

## Edge ルーティング接続の問題

- 1 ping <destination\_IP\_address> コマンドを使用して、クライアントから制御されたトラフィックを開始します。
- 2 両方のインターフェイスでトラフィックを同時にキャプチャして、出力をファイルに書き込み、SCP を使用してエクスポートします。

次はその例です。

次のコマンドを使用して入力側のインターフェイスでトラフィックをキャプチャします。

```
debug packet display interface vNic_0 -n_src_host_1.1.1.1
```

次のコマンドを使用して出力方向のインターフェイスでトラフィックをキャプチャします。

```
debug packet display interface vNic_1 -n_src_host_1.1.1.1
```

同時にパケットをキャプチャするには、ESXi のパケット キャプチャ ユーティリティ `pktcap-uw` ツールを ESXi で使用します。 <https://kb.vmware.com/kb/2051814> を参照してください。

パケットが常にドロップしている場合は、次に関連する設定エラーを確認します。

- IP アドレスとルート
  - ファイアウォール ルールまたは NAT ルール
  - 非対称ルーティング
  - RP フィルタ チェック
- a `show interface` コマンドを使用してインターフェイスの IP アドレス/サブネットを確認します。
  - b データ プレーンで欠落しているルートがある場合には、次のコマンドを実行します。
    - `show ip route`
    - `show ip route static`
    - `show ip route bgp`
    - `show ip route ospf`
  - c `show ip forwarding` コマンドを実行して、必要なルートのルーティング テーブルを確認します。
  - d 複数のパスがある場合、`show rpfilter` コマンドを実行します。

```
nsxedge> show rpfilter
net.ipv4.conf.VDR.rp_filter = 0
net.ipv4.conf.all.rp_filter = 0
net.ipv4.conf.br-sub.rp_filter = 1
net.ipv4.conf.default.rp_filter = 1
net.ipv4.conf.lo.rp_filter = 0
net.ipv4.conf.vNic_0.rp_filter = 1
net.ipv4.conf.vNic_1.rp_filter = 1
net.ipv4.conf.vNic_2.rp_filter = 1
net.ipv4.conf.vNic_3.rp_filter = 1
net.ipv4.conf.vNic_4.rp_filter = 1
net.ipv4.conf.vNic_5.rp_filter = 1
net.ipv4.conf.vNic_6.rp_filter = 1
net.ipv4.conf.vNic_7.rp_filter = 1
net.ipv4.conf.vNic_8.rp_filter = 1
net.ipv4.conf.vNic_9.rp_filter = 1
```

```
nsxedge> show rpfstats
RPF drop packet count: 484
```

RPF 統計情報を確認するには、`show rpfstats` コマンドを実行します。

```
nsxedge> show rpfstats
RPF drop packet count: 484
```

パケットが不規則にドロップする場合、次のリソースが不足していないかどうかを確認します。

a CPU やメモリの使用率については、次のコマンドを実行します。

- `show system cpu`
- `show system memory`
- `show system storage`
- `show process monitor`
- `top`

ESXi については、`esxtop n` コマンドを実行します。

```
PCPU USED(%): 2.5 5.0 3.7 77 AVG: 22
PCPU UTIL(%): 0.5 2.7 3.3 92 AVG: 24
```

ID	GID	NAME	NWLD	%USED	%RUN	%SYS	%WAIT
98255269	98255269	esxtop.11224149	1	67.04	69.86	0.00	6.26
2	2	system	139	3.03	4.61	0.00	12053.58
86329	86329	app-01a	6	0.69	0.57	0.00	466.09
78730	78730	db-01a	6	0.48	0.67	0.00	441.44
90486	90486	app-02a	6	0.38	0.32	0.00	463.42

%VMWAIT	%RDY	%IDLE	%OVRLP	%CSTP	%MLMTD	%SWPWT
11.01	-	0.39	0.00	0.09	0.00	0.00
600.00	53.81	0.10	93.13	0.00	0.00	0.00
13900.00	-	28.68	0.00	2.69	0.00	0.00
600.00	53.81	0.10	93.13	0.00	0.00	0.00
600.00	0.00	0.19	151.92	0.00	0.00	0.00

## NSX Manager と Edge の通信の問題

NSX Manager は、VIX やメッセージバスを介して NSX Edge と通信します。これは、Edge がデプロイされるときに NSX Manager によって選択され、変更されることはありません。

**注：** VIX は、NSX 6.3.0 以降でサポートされていません。



## VIX

- VIX は、ESXi ホストの準備が整っていない場合、NSX Edge によって使用されます。
- NSX Manager は、vCenter Server からホストの認証情報を取得して、最初に ESXi ホストに接続します。
- NSX Manager は、Edge の認証情報を使用して、Edge アプライアンスにログインします。
- Edge の vmtoolsd プロセスが、VIX との通信を処理します。

VIX の障害が発生する場合、以下の原因が考えられます。

- NSX Manager が vCenter Server と通信できない。
- NSX Manager が ESXi ホストと通信できない。
- NSX Manager の内部に問題がある。
- Edge の内部に問題がある。

## VIX のデバッグ

NSX Manager のログで VIX のエラー「VIX\_E\_<error>」を確認して、原因を絞り込みます。次のようなエラーを確認します。

```
Vix Command 1126400 failed, reason com.vmware.vshield.edge.exception.VixException: vShield
Edge:10013:Error code 'VIX_E_FILE_NOT_FOUND' was returned by VIX API.:null

Health check failed for edge edge-13 VM vm-5025 reason:
com.vmware.vshield.edge.exception.VixException: vShield Edge:10013:Error code
'VIX_E_VM_NOT_RUNNING' was returned by VIX API.:null
```

一般的に、多くの Edge で同時に同じエラーが発生している場合は、Edge 側の問題ではありません。

## メッセージ バスのデバッグ

メッセージ バスは、ESXi ホストが準備されているときに、NSX Edge の通信に使用されます。

問題が発生する場合、NSX Manager ログに次のようなエントリが含まれる場合があります。

```
GMT ERROR taskScheduler-6 PublishTask:963 - Failed to configure VSE-vm index 0, vm-id vm-117,
edge edge-5. Error: RPC request timed out
```

次のような場合に、この問題が発生します。

- Edge の状態が正しくない
- メッセージ バスに接続していない

Edge でこの問題を診断するには、次のように操作します。

- RMQ との接続を確認するには、次のコマンドを実行します。

```
nsxedge> show messagebus messages
-----
Message bus is enabled
cmd conn state : listening
init_req      : 1
init_resp     : 1
init_req_err   : 0
...
```

- VMCI との接続を確認するには、次のコマンドを実行します。

```
nsxedge> show messagebus forwarder
-----
Forwarder Command Channel
vmci_conn      : up
app_client_conn : up
vmci_rx        : 3649
vmci_tx        : 3648
vmci_rx_err    : 0
vmci_tx_err    : 0
vmci_closed_by_peer: 8
vmci_tx_no_socket : 0
app_rx         : 3648
app_tx         : 3649
app_rx_err     : 0
app_tx_err     : 0
app_conn_req   : 1
app_closed_by_peer : 0
app_tx_no_socket : 0
-----
Forwarder Event Channel
vmci_conn      : up
app_client_conn : up
vmci_rx        : 1143
vmci_tx        : 13924
vmci_rx_err    : 0
vmci_tx_err    : 0
vmci_closed_by_peer: 0
vmci_tx_no_socket : 0
app_rx         : 13924
app_tx         : 1143
app_rx_err     : 0
app_tx_err     : 0
app_conn_req   : 1
app_closed_by_peer : 0
app_tx_no_socket : 0
-----
```

```
cli_rx      : 1
cli_tx      : 1
cli_tx_err  : 0
counters_reset : 0
```

この例の `vmci_closed_by_peer: 8` という出力は、ホスト エージェントが終了した接続の回数を示しています。この数が増加しており、`vmci conn` がダウンしている場合、ホスト エージェントは RMQ ブローカに接続できません。`show log follow` を使用して、Edge ログで次のエラーが繰り返し発生していないか確認します。VmciProxy: [daemon.debug] VMCi Socket is closed by peer

ESXi ホストの問題を診断するには：

- ESXi ホストが RMQ ブローカに接続しているかどうかを確認するには、次のコマンドを実行します。

```
esxcli network ip connection list | grep 5671

tcp    0    0  10.32.43.4:43329  10.32.43.230:5671  ESTABLISHED    35854  newreno
vsfwd
tcp    0    0  10.32.43.4:52667  10.32.43.230:5671  ESTABLISHED    35854  newreno
vsfwd
tcp    0    0  10.32.43.4:20808  10.32.43.230:5671  ESTABLISHED    35847  newreno
vsfwd
tcp    0    0  10.32.43.4:12486  10.32.43.230:5671  ESTABLISHED    35847  newreno vsfwd
```

## Edge の診断とリカバリ

### Edge の診断

- 次のコマンドを使用して、`vmtoolsd` が実行されていることを確認します。

```
nsxedge> show process list
Perimeter-Gateway-01-0> show process list
%CPU %MEM    VSZ   RSZ STAT  STARTED    TIME COMMAND
 0.0  0.1   4244   720 Ss     May 16 00:00:15 init [3]
...
 0.0  0.1   4240   640 S      May 16 00:00:00 logger -p daemon debug -t vserrdd
 0.2  0.9  57192  4668 S      May 16 00:23:07 /usr/local/bin/vmtoolsd --plugin-pa
 0.0  0.4   4304  2260 SLs    May 16 00:01:54 /usr/sbin/watchdog
...
```

- 次のコマンドを実行して、Edge が健全な状態であることを確認します。

```
nsxedge> show eventmgr
-----
messagebus      : enabled
debug           : 0
profiling       : 0
cfg_rx          : 1
cfg_rx_msgbus   : 0
...
```

show eventmgr コマンドを使用して、クエリ コマンドを受信して処理していることを確認します。

```

nsxedge> show eventmgr
-----
messagebus      : enabled
debug           : 0
profiling       : 0
cfg_rx          : 1
cfg_rx_msgbus   : 0
cfg_rx_err      : 0
cfg_exec_err    : 0
cfg_resp        : 0
cfg_resp_err    : 0
cfg_resp_ln_err : 0
fastquery_rx    : 0 fastquery_err : 0
clearcmd_rx     : 0
clearcmd_err    : 0
ha_rx           : 0
ha_rx_err       : 0
ha_exec_err     : 0
status_rx       : 16
status_rx_err   : 0
status_svr      : 10
status_evt      : 0
status_evt_push : 0
status_ha       : 0
status_ver      : 1
status_sys      : 5
status_cmd      : 0
status_svr_err  : 0
status_evt_err  : 0
status_sys_err  : 0
status_ha_err   : 0
status_ver_err  : 0
status_cmd_err  : 0
evt_report      : 1
evt_report_err  : 0
hc_report       : 10962
hc_report_err   : 0
cli_rx          : 2
cli_resp        : 1
cli_resp_err    : 0
counter_reset   : 0
----- Health Status -----
system status   : good
ha state        : active
cfg version     : 7
generation      : 0
server status   : 1
syslog-ng       : 1
haproxy         : 0
ipsec           : 0
sslvpn          : 0
l2vpn           : 0

```

```

dns          : 0
dhcp         : 0
heartbeat    : 0
monitor      : 0
gslb         : 0
----- System Events -----

```

## Edge のリカバリ

vmtoolsd が実行されていない、あるいは、NSX Edge が健全な状態でない場合、Edge を再起動します。

クラッシュからリカバリするには、再起動で十分です。再デプロイの必要はありません。

---

**注：** 再デプロイを行った場合には、古い Edge のログ情報をすべて記録してください。

---

カーネル クラッシュをデバッグするには、次のものがが必要です。

- クラッシュ状態の Edge 仮想マシンの vmss（仮想マシンのサスペンド）または vmsn（仮想マシンのスナップショット）ファイルのいずれか。vmem ファイルがある場合、これも必要です。VMware サポートが分析するカーネル コア ダンプ ファイルの抽出に使用できます。
- クラッシュした Edge の再起動直後に生成された Edge サポート ログ（再デプロイ後のログではありません）。また、Edge のログも確認できます。<https://kb.vmware.com/kb/2079380> を参照してください。
- Edge コンソールのスクリーン ショットも役立ちますが、通常、完全なクラッシュ レポートには含まれていません。

# ファイアウォールのトラブルシューティング

# 5

このセクションでは、ファイアウォールの問題のトラブルシューティングに関する情報を提供します。

この章には、次のトピックが含まれています。

- [分散ファイアウォールについて](#)
- [Identity Firewall](#)

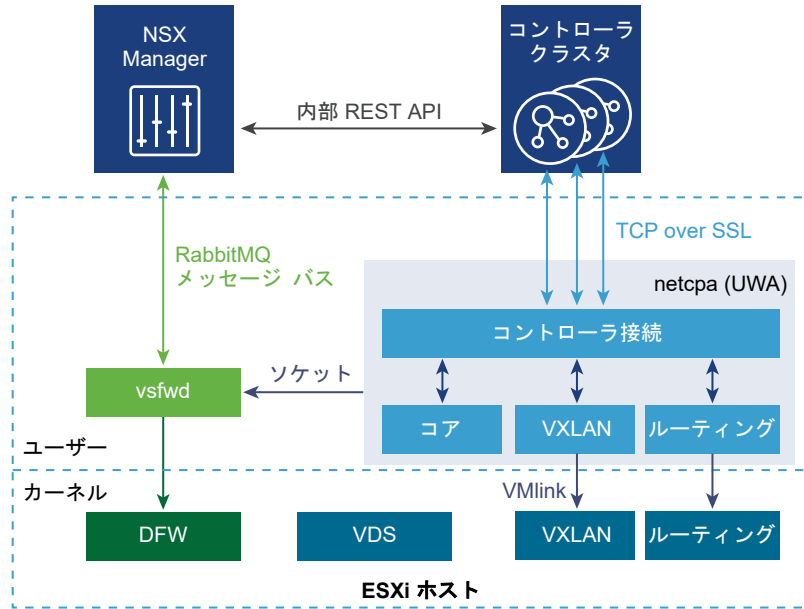
## 分散ファイアウォールについて

RabbitMQ メッセージ バスは、NSX Manager でホストされる vsfwd (RMQ クライアント) と RMQ サーバ プロセス間の通信に利用されます。メッセージ バスは NSX Manager により使用され、カーネルの分散ファイアウォールに組み込む必要があるポリシー ルールなど、さまざまな情報を ESXi ホストに送信します。

NSX 分散ファイアウォールは、ハイパーバイザー カーネルが組み込まれたファイアウォールで、仮想ワークロードや仮想ネットワークを表示および管理できます。データセンター、クラスタ、仮想マシン名、タグ、ネットワーク構造 (IP/VLAN/VXLAN アドレスなど) のような VMware vCenter オブジェクトや Active Directory のユーザー グループ ID に基づいて、アクセス制御ポリシーを作成できます。物理ホスト間で仮想マシンの vMotion が実行されたときに、ファイアウォール ルールを書き換えることなく、整合性のあるアクセス制御ポリシーが適用されるようになりました。分散ファイアウォールにはハイパーバイザーが組み込まれているため、ライン レートに近いスループットが実現し、物理サーバにおけるワークロード統合を強化できます。このファイアウォールの特性である分散性により、ホストをデータセンターに追加すると自動的にファイアウォールのキャパシティが拡張されるスケール アウト アーキテクチャが実現します。

NSX Manager Web アプリケーションと ESXi ホスト上の NSX コンポーネントは、NSX Manager Web アプリケーションと同じ仮想マシンで実行される RabbitMQ ブローカ プロセスを通じて相互に通信します。通信プロトコルとして AMQP (Advanced Message Queueing Protocol) を使用し、チャンネルは SSL を使用して保護します。ESXi ホストで、VSFWD (vShield Firewall Daemon) プロセスは、ブローカへの SSL 接続を確立および維持し、他のコンポーネントの代わりにメッセージを送受信します。この通信には IPC を使用します。

図 5-1. ESXi ホストのユーザーおよびカーネル空間の図



## 分散ファイアウォールの CLI コマンド

NSX Manager のセントラル CLI で分散ファイアウォールに関するほぼすべての情報を取得できます。

### Show dfw セントラル CLI コマンドの使用

次のコマンドを使用して、必要な情報を取得できます。

- 1 `admin` の認証情報を使用して、NSX Manager セントラル CLI にログインします。
- 2 次のコマンドを実行します。
  - a すべてのクラスタを表示するには、`show cluster all` コマンドを実行します。

```
nsxmgr>show cluster all
```

No.	Cluster Name	Cluster Id	Datacenter Name	Firewall Status
1	Compute Cluster A	domain-c33	Datacenter Site A	Enabled
2	Management & Edge Cluster	domain-c41	Datacenter Site A	Enabled

- b 特定のクラスタのホストを表示するには、`show cluster <clusterID>` コマンドを実行します。

```
nsxmgr> show cluster domain-c33
```

Datacenter: Datacenter Site A

Cluster: Compute Cluster A

No.	Host Name	Host Id	Installation Status
1	esx-02a.corp.local	host-32	Enabled
2	esx-01a.corp.local	host-28	Enabled

- c ホスト上のすべての仮想マシンを表示するには、`show host <hostID>` を実行します。

```
nsxmgr> show host host-28
Datacenter: Datacenter Site A
Cluster: Compute Cluster A
Host: esx-01a.corp.local
No.  VM Name      VM Id      Power Status
1    web-02a      vm-219     on
2    web-01a      vm-216     on
3    win8-01a     vm-206     off
4    app-02a      vm-264     on
```

- d フィルタ名と vNIC ID を含む仮想マシンの情報を表示するには、`show vm <vmID>` コマンドを実行します。

```
nsxmgr> show vm vm-264
Datacenter: Datacenter Site A
Cluster: Compute Cluster A
Host: esx-01a.corp.local
Host-ID: host-28
VM: app-02a
Virtual Nics List:
1.
Vnic Name      app-02a - Network adapter 1
Vnic Id        502ef2fa-62cf-d178-cb1b-c825fb300c84.000
Filters        nic-79396-eth0-vmware-sfw.2
```

- e vNIC ID をメモし、さらに `show dfw vnic <vnidID>` や `show dfw host <hostID> filter <filter ID> rules` などのコマンドを実行します。

```
nsxmgr> show dfw vnic 502ef2fa-62cf-d178-cb1b-c825fb300c84.000
Vnic Name      app-02a - Network adapter 1
Vnic Id        502ef2fa-62cf-d178-cb1b-c825fb300c84.000
Mac Address    00:50:56:ae:6c:6b
Port Group Id  dvportgroup-385
Filters        nic-79396-eth0-vmware-sfw.2

nsxmgr> show dfw host host-28 filter nic-79396-eth0-vmware-sfw.2 rules
ruleset domain-c33 {
  # Filter rules
  rule 1012 at 1 inout protocol any from addrset ip-securitygroup-10 to addrset ip-securitygroup-10 drop with log;
  rule 1013 at 2 inout protocol any from addrset src1013 to addrset src1013 drop;
  rule 1011 at 3 inout protocol tcp from any to addrset dst1011 port 443 accept;
  rule 1011 at 4 inout protocol icmp icmp type 8 from any to addrset dst1011 accept;
  rule 1010 at 5 inout protocol tcp from addrset ip-securitygroup-10 to addrset ip-securitygroup-11 port 8443 accept;
  rule 1010 at 6 inout protocol icmp icmp type 8 from addrset ip-securitygroup-10 to addrset ip-securitygroup-11 accept;
```



```

rule 1009 at 7 inout protocol tcp from addrset ip-securitygroup-11 to addrset ip-
securitygroup-12 port 3306 accept;
rule 1009 at 8 inout protocol icmp icmp type 8 from addrset ip-securitygroup-11 to addrset
ip-securitygroup-12 accept;
rule 1003 at 9 inout protocol ipv6-icmp icmp type 136 from any to any accept;
rule 1003 at 10 inout protocol ipv6-icmp icmp type 135 from any to any accept;
rule 1002 at 11 inout protocol udp from any to any port 67 accept;
rule 1002 at 12 inout protocol udp from any to any port 68 accept;
rule 1001 at 13 inout protocol any from any to any accept;
}

ruleset domain-c33_L2 {
# Filter rules
rule 1004 at 1 inout ethertype any from any to any accept;
}

```

## export host-tech-support セントラル CLI コマンドの使用

export host-tech-support コマンドを実行すると、指定したサーバに ESXi ホストのサポート バンドルをエクスポートできます。このコマンドは、指定されたホストについて、NSX 関連の出力とファイルを収集します。たとえば、次のような出力とファイルを収集します。

- VMkernel と vsfwd のログ ファイル
- フィルタのリスト
- 分散ファイアウォール ルールのリスト
- コンテナのリスト
- SpoofGuard の詳細
- ホストに関連する情報
- IP アドレス検出に関連する情報
- RMQ コマンド出力
- セキュリティ グループ、サービス プロファイル、インスタンスの詳細
- ESX CLI 関連の出力

また、このコマンドは NSX Manager の一時ファイルを削除します。

NSX 関連の出力とファイルを収集するには：

- 1 **admin** の認証情報を使用して、NSX Manager セントラル CLI にログインします。
- 2 次のコマンドを実行します。
  - a show cluster all：必要なホスト ID を検索します。
  - b export host-tech-support host-id scp uid@ip:/path：NSX テクニカル サポート バンドルを生成し、指定したサーバにコピーします。

詳細については、次を参照してください。

- [NSX コマンド ライン クイック リファレンス](#)

- NSX コマンド ライン インターフェイス リファレンス。

## 分散ファイアウォールのトラブルシューティング

このトピックでは、VMware NSX 6.x 分散ファイアウォール (DFW) を理解してトラブルシューティングするための情報を提供します。

### 問題

- 分散ファイアウォール ルールの発行に失敗する。
- 分散ファイアウォール ルールの更新に失敗する。

### 原因

お使いの環境において次の各トラブルシューティングの手順が当てはまるかどうかを確認します。各手順では、問題となっている原因を取り除き、必要に応じて修正のためのアクションを実行するための操作指示とドキュメントへのリンクが提供されます。問題を切り分けて適切な解決策を特定するために、操作手順には最も適切な順序が設定されています。各手順を実行した後に、分散ファイアウォール ルールの更新/発行を再試行します。

### 解決方法

- 1 クラスタにある各 ESXi ホストに NSX VIB が正常にインストールされていることを確認します。確認するには、クラスタにある各 ESXi ホストで、次のコマンドを実行します。

```
# esxcli software vib list | grep vsip
esx-vsip                6.0.0-0.0.4744062  VMware  VMwareCertified  2017-01-04

# esxcli software vib list | grep vxlan
esx-vxlan                6.0.0-0.0.4744062  VMware  VMwareCertified  2017-01-04
```

NSX 6.2 より前のバージョンの NSX では、このほかにも VIB があります。

```
# esxcli software vib list | grep dvfilter
esx-dvfilter-switch-security  5.5.0-0.0.2318233  VMware  VMwareCertified  2015-01-24
```

ESXi 6.0 以降と NSX 6.3.3 から、esx-vxlan と esx-vsip VIB は esx-nsxv に代わります。

```
# esxcli software vib list | grep nsxv
esx-nsxv                6.0.0-0.0.6216823  VMware  VMwareCertified  2017-08-10
```

- 2 ESXi ホストで、vShield-Stateful-Firewall サービスの状態が実行中になっていることを確認します。

次はその例です。

```
# /etc/init.d/vShield-Stateful-Firewall status

vShield-Stateful-Firewall is running
```

### 3 メッセージ バスが NSX Manager と適切に通信していることを確認します。

このプロセスは、ウォッチドック スクリプトによって自動的に起動され、何らかの理由で終了した場合はプロセスは再起動されます。クラスタにある各 ESXi ホストでこのコマンドを実行します。

次はその例です。

```
# ps | grep vsfwd

107557 107557 vsfwd /usr/lib/vmware/vsfw/vsfwd
```

コマンドの出力には、実行中の vsfwd プロセスが 12 個以上あるはずです。実行中のプロセス数がこれより少ない場合（たとえば 2 個のみ）、vsfwd は正常に実行されていません。

### 4 ファイアウォールの設定でポート 5671 が通信用に開いていることを確認します。

このコマンドは、RabbitMQ ブローカへの VSFWD の接続を示しています。このコマンドを ESXi ホストで実行して、ESXi ホストの VSFWD プロセスから NSX Manager への接続リストを表示します。環境におけるいずれかの外部ファイアウォールでポート 5671 が通信用に開いていることを確認します。また、ポート 5671 で少なくとも 2 つの接続が存在している必要があります。ESXi ホストにデプロイされる NSX Edge 仮想マシンも RMQ ブローカへの接続を確立するため、ポート 5671 ではさらに多くの接続が存在する場合があります。

次はその例です。

```
# esxcli network ip connection list |grep 5671

tcp          0      0 192.168.110.51:30133      192.168.110.15:5671    ESTABLISHED
10949155 newreno vsfwd
tcp          0      0 192.168.110.51:39156      192.168.110.15:5671    ESTABLISHED
10949155 newreno vsfwd
```

### 5 VSFWD が設定されていることを確認します。

このコマンドによって、NSX Manager の IP アドレスが表示されます。

```
# esxcfg-advcfg -g /UserVars/RmqIpAddress
```

### 6 この ESXi ホストに host-profile を使用している場合、RabbitMQ がホスト プロファイルで設定されていないことを確認します。

詳細については、次のドキュメントを参照してください。

- <https://kb.vmware.com/kb/2092871>
- <https://kb.vmware.com/kb/2125901>

- 7 ESXi ホストの RabbitMQ の認証情報が NSX Manager と同期していないことを確認します。NSX Manager のテクニカル サポート ログをダウンロードします。すべての NSX Manager テクニカル サポート ログを収集したら、次のようなエントリをすべてのログで検索します。

host-420 と問題があることが疑われるホストの mo-id を置換します。

```
PLAIN login refused: user 'uw-host-420' - invalid credentials.
```

- 8 このようなエントリが、問題があることが疑われる ESXi ホストのログで見つかった場合、メッセージ バスを再同期します。

メッセージ バスを再同期するには、REST API を使用します。問題を詳細に把握するためには、メッセージ バスを再同期したらすぐにログを収集します。

```
HTTP Method : POST
Headers ,
Authorization : base64encoded value of username password
Accept : application/xml
Content-Type : application/xml
Request:

POST https://NSX_Manager_IP/api/2.0/nwfabric/configure?action=synchronize

Request Body:

<nwFabricFeatureConfig>
<featureId>com.vmware.vshield.vsm.messagingInfra</featureId>
<resourceConfig>
<resourceId>{HOST/CLUSTER MOID}</resourceId>
</resourceConfig>
</nwFabricFeatureConfig>
```

- 9 `export host-tech-support <host-id> scp <uid@ip:/path>` コマンドを使用して、ホスト固有のファイアウォール ログを収集します。

次はその例です。

```
nsxmgr# export host-tech-support host-28 scp Administrator@192.168.110.10
Generating logs for Host: host-28...
```

- 10 `show dfw host host-id summarize-dvfilter` コマンドを使用して、ホストにファイアウォールのルールがデプロイされており、仮想マシンに適用されていることを確認します。

出力の `module: vsip` は、分散ファイアウォール モジュールがロードされ実行されていることを示しています。name は、各 vNIC で実行されているファイアウォールを示しています。

`show dfw cluster all` コマンドを実行してクラスタードメイン ID を取得し、次に `show dfw cluster domain-id` を実行して、ホスト ID を取得できます。

次はその例です。

```
# show dfw host host-28 summarize-dvfilter

Fastpaths:
agent: dvfilter-faulter, refCount: 1, rev: 0x1010000, apiRev: 0x1010000, module: dvfilter
agent: ESXi-Firewall, refCount: 5, rev: 0x1010000, apiRev: 0x1010000, module: esx_fw
agent: dvfilter-generic-vmware, refCount: 1, rev: 0x1010000, apiRev: 0x1010000, module: dvfilter-
generic-fastpath
agent: dvfilter-generic-vmware-swsec, refCount: 4, rev: 0x1010000, apiRev: 0x1010000, module:
dvfilter-switch-security
agent: bridgelearningfilter, refCount: 1, rev: 0x1010000, apiRev: 0x1010000, module: vdrb
agent: dvfg-igmp, refCount: 1, rev: 0x1010000, apiRev: 0x1010000, module: dvfg-igmp
agent: vmware-sfw, refCount: 4, rev: 0x1010000, apiRev: 0x1010000, module: vsip

Slowpaths:

Filters:
world 342296 vmm0:2-vm_RHEL63_srv_64-shared-846-3f435476-8f54-4e5a-8d01-59654a4e9979 vcUuid:'3f
43 54 76 8f 54 4e 5a-8d 01 59 65 4a 4e 99 79'
port 50331660 2-vm_RHEL63_srv_64-shared-846-3f435476-8f54-4e5a-8d01-59654a4e9979.eth1
vNic slot 2
  name: nic-342296-eth1-vmware-sfw.2
  agentName: vmware-sfw
  state: IOChain Attached
  vmState: Detached
  failurePolicy: failClosed
  slowPathID: none
  filter source: Dynamic Filter Creation
vNic slot 1
  name: nic-342296-eth1-dvfilter-generic-vmware-swsec.1
  agentName: dvfilter-generic-vmware-swsec
  state: IOChain Attached
  vmState: Detached
  failurePolicy: failClosed
  slowPathID: none
  filter source: Alternate Opaque Channel
port 50331661 (disconnected)
vNic slot 2
  name: nic-342296-eth2-vmware-sfw.2 <===== DFW filter
  agentName: vmware-sfw
  state: IOChain Detached
  vmState: Detached
  failurePolicy: failClosed
  slowPathID: none
  filter source: Dynamic Filter Creation
port 33554441 2-vm_RHEL63_srv_64-shared-846-3f435476-8f54-4e5a-8d01-59654a4e9979
vNic slot 2
  name: nic-342296-eth0-vmware-sfw.2<===== DFW filter
  agentName: vmware-sfw
  state: IOChain Attached
```

```

vmState: Detached
failurePolicy: failClosed
slowPathID: none
filter source: Dynamic Filter Creation

```

## 11 show dfw host hostID filter filterID rules コマンドを実行します。

次はその例です。

```

# show dfw host host-28 filter nic-79396-eth0-vmware-sfw.2 rules

ruleset domain-c33 {
  # Filter rules
  rule 1012 at 1 inout protocol any from addrset ip-securitygroup-10 to addrset ip-
securitygroup-10 drop with log;
  rule 1013 at 2 inout protocol any from addrset src1013 to addrset src1013 drop;
  rule 1011 at 3 inout protocol tcp from any to addrset dst1011 port 443 accept;
  rule 1011 at 4 inout protocol icmp icmp type 8 from any to addrset dst1011 accept;
  rule 1010 at 5 inout protocol tcp from addrset ip-securitygroup-10 to addrset ip-
securitygroup-11 port 8443 accept;
  rule 1010 at 6 inout protocol icmp icmp type 8 from addrset ip-securitygroup-10 to addrset ip-
securitygroup-11 accept;
  rule 1009 at 7 inout protocol tcp from addrset ip-securitygroup-11 to addrset ip-
securitygroup-12 port 3306 accept;
  rule 1009 at 8 inout protocol icmp icmp type 8 from addrset ip-securitygroup-11 to addrset ip-
securitygroup-12 accept;
  rule 1003 at 9 inout protocol ipv6-icmp icmp type 136 from any to any accept;
  rule 1003 at 10 inout protocol ipv6-icmp icmp type 135 from any to any accept;
  rule 1002 at 11 inout protocol udp from any to any port 67 accept;
  rule 1002 at 12 inout protocol udp from any to any port 68 accept;
  rule 1001 at 13 inout protocol any from any to any accept;
}

ruleset domain-c33_L2 {
  # Filter rules
  rule 1004 at 1 inout ethertype any from any to any accept;
}

```

## 12 show dfw host hostID filter filterID addrsets コマンドを実行します。

次はその例です。

```

# show dfw host host-28 filter nic-342296-eth2-vmware-sfw.2 addrsets

addrset dst1011 {
  ip 172.16.10.10,
  ip 172.16.10.11,
  ip 172.16.10.12,
  ip fe80::250:56ff:feae:3e3d,
  ip fe80::250:56ff:feae:f86b,
}

addrset ip-securitygroup-10 {
  ip 172.16.10.11,
  ip 172.16.10.12,
}

```

```

ip fe80::250:56ff:feae:3e3d,
ip fe80::250:56ff:feae:f86b,
}
addrset ip-securitygroup-11 {
ip 172.16.20.11,
ip fe80::250:56ff:feae:23b9,
}
addrset ip-securitygroup-12 {
ip 172.16.30.11,
ip fe80::250:56ff:feae:d42b,
}
addrset src1013 {
ip 172.16.10.12,
ip 172.17.10.11,
ip fe80::250:56ff:feae:cf88,
ip fe80::250:56ff:feae:f86b,
}

```

- 13** 上記のトラブルシューティングの各手順を確認してもホスト仮想マシンにファイアウォール ルールを発行できない場合、NSX Manager ユーザー インターフェイスまたは次の REST API 呼び出しを介してホスト レベルで強制的に再同期を実行します。

```

URL : [https:]https://<nsx-mgr-ip>/api/4.0/firewall/forceSync/<host-id>
HTTP Method : POST
Headers ,
Authorization : base64encoded value of username password
Accept : application/xml
Content-Type : application/xml

```

## 解決方法

注：

- ファイアウォール ルールが IP アドレスを使用していない場合、VMware Tools が仮想マシンで実行されていることを確認します。詳細については、<https://kb.vmware.com/kb/2084048> を参照してください。

VMware NSX 6.2.0 では DHCP スヌーピングまたは ARP スヌーピングを使用した、仮想マシンの IP アドレスを検出するためのオプションが追加されました。これらの新しい検出メカニズムにより、VMware Tools がインストールされていない仮想マシンでも、IP アドレスベースのセキュリティ ルールを適用できるようになりました。詳細は、NSX 6.2.0 リリース ノートを参照してください。

分散ファイアウォールは、ホスト準備が完了するとすぐに有効になります。仮想マシンで分散ファイアウォール サービスがまったく不要な場合、除外リスト機能に追加できます（デフォルトでは、NSX Manager、NSX Controller、および Edge Services Gateway は、分散ファイアウォール機能から自動的に除外されます）。分散ファイアウォールですべて拒否ルールを作成した後、vCenter Server へのアクセスが失敗する可能性があります。詳細については、<https://kb.vmware.com/kb/2079620> を参照してください。

- VMware テクニカル サポートと一緒に VMware NSX 6.x 分散ファイアウォール (DFW) をトラブルシューティングする場合には、以下が必要となります。
  - クラスタにある各 ESXi ホストで `show dfw host hostID summarize-dvfilter` コマンドを実行した出力。
  - [Networking and Security] > [ファイアウォール (Firewall)] > [全般 (General)] タブで [設定のエクスポート (Export Configuration)] をクリックして取得できる分散ファイアウォールの設定。これによって、分散ファイアウォールの設定が XML 形式でエクスポートされます。
  - NSX Manager のログ。詳細については、<https://kb.vmware.com/kb/2074678> を参照してください。
  - vCenter Server のログ。詳細については、<https://kb.vmware.com/kb/1011641> を参照してください。

## Identity Firewall

### 問題

Identity Firewall の発行または更新に失敗します。

### 原因

Identity Firewall (IDFW) によって、ユーザー ベースの分散ファイアウォール (DFW) ルールが利用できるようになります。

ユーザー ベースの分散ファイアウォール ルールは、Active Directory (AD) グループのメンバーシップによって決定されます。Identity Firewall (IDFW) は、Active Directory ユーザーのログイン先を監視し、ファイアウォール ルールを適用するために、分散ファイアウォールが使用する IP アドレスに対して、ログインをマッピングします。Identity Firewall では、ゲスト イントロスペクション フレームワークまたは Active Directory イベント ログ スクレイピングのいずれかが必要です。

### 解決方法

- 1 NSX Manager で Active Directory サーバの完全/差分同期が機能していることを確認します。
  - a vSphere Web Client で、NSX Manager にリンクされた vCenter Server にログインします。
  - b [ホーム (Home)] > [Networking and Security (Networking & Security)] > [NSX Manager] の順に移動し、リストから NSX Manager を選択します。
  - c [管理 (Manage)] タブ、[ドメイン (Domains)] タブの順に選択します。リストからドメインを選択します。[最後の同期状態 (Last Synchronization Status)] 列に「成功」が表示され、[最後の同期時刻 (Last Synchronization Time)] が現在の時刻であることを確認します。
- 2 ファイアウォール環境でログイン検出にイベント ログ スクレイピングを使用している場合には、次の手順を実行し、ドメインにイベント ログ サーバが設定されていることを確認します。
  - a vSphere Web Client で、NSX Manager にリンクされた vCenter Server にログインします。
  - b [ホーム (Home)] > [Networking and Security (Networking & Security)] > [NSX Manager] の順に移動し、リストから NSX Manager を選択します。



- c [管理 (Manage)] タブ、[ドメイン (Domains)] タブの順に選択します。リストからドメインを選択します。ここで、ドメインの詳細な設定を表示し、編集できます。
  - d ドメインの詳細から [イベント ログ サーバ (Event Log Servers)] を選択し、イベント ログ サーバが追加されていることを確認します。
  - e イベント ログ サーバを選択して、[最後の同期状態 (Last Sync Status)] 列に「成功」が表示され、[最後の同期時刻 (Last Sync Time)] が現在の時刻であることを確認します。
- 3 ファイアウォール環境でゲスト イントロスペクションを使用している場合、Identity Firewall で保護された仮想マシンを配置するコンピューティング クラスタにフレームワークを展開する必要があります。ユーザー インターフェイスでサービスの健全性が正常と表示されます。ゲスト イントロスペクションを使用している場合は、ナレッジベースの記事「Troubleshooting vShield Endpoint / NSX Guest Introspection (<https://kb.vmware.com/kb/2094261>)」および「Collecting logs in VMware NSX for vSphere 6.x Guest Introspection Universal Service Virtual Machine (<https://kb.vmware.com/kb/2144624>)」で診断情報について確認できます。
- 4 ログインの検出方法が正しく設定されていることを確認したら、NSX Manager がログイン イベントを受信していることを確認します
- a Active Directory ユーザーでログインします。
  - b 次のコマンドを実行して、ログイン イベントにクエリを実行します。ユーザーが結果に含まれていることを確認します。GET <https://<nsxmgr-ip>/1.0/identity/userIpMapping>

```
Example output:
<UserIpMappings>
  <UserIpMapping>
    <ip>50.1.111.192</ip>
    <userName>user1_group20</userName>
    <displayName>user1_group20</displayName>
    <domainName>cd.ad1.db.com</domainName>
    <startTime class="sql-timestamp">2017-05-11 22:30:51.0</startTime>
    <startType>EVENTLOG</startType>
    <lastSeenTime class="sql-timestamp">2017-05-11 22:30:52.0</lastSeenTime>
    <lastSeenType>EVENTLOG</lastSeenType>
  </UserIpMapping>
</UserIpMappings>
```

- 5 セキュリティ グループがファイアウォール ルールで使用されているか、セキュリティ グループにセキュリティ ポリシーが割り当てられていることを確認します。これらの条件のいずれかに該当する場合を除き、Identity Firewall でセキュリティ グループは処理されません。

- 6 Identity Firewall がログインを正しく検出することを確認したら、デスクトップ仮想マシンが配置された ESXi ホストが正しい設定を受信していることを確認します。次の手順では、NSX Manager の集中管理 CLI を使用します。[ip-securitygroup] リストに含まれるデスクトップ仮想マシンの IP アドレスを確認するには、次の手順に従います。
- a 分散ファイアウォールの CLI コマンドを参照して、デスクトップ仮想マシンに適用されたフィルタ名を取得します。
  - b `show dfw host hostID filter filterID rules` コマンドを実行して、分散ファイアウォール ルールの項目を表示します。
  - c `show dfw host hostID filter filterID addrsets` コマンドを実行して、ip-securitygroup リストに含まれる IP アドレスを表示します。リストに IP アドレスが含まれていることを確認します。

#### 解決方法

注：VMware テクニカル サポートと一緒に Identity Firewall のトラブルシューティングを行うときに、このデータは役立ちます。

- Active Directory スケール データ（イベント ログ スクレイピングを使用している場合）：
  - 1 つの NSX Manager のドメインの数
    - フォレストの数
    - ユーザーの数/フォレスト
    - ユーザーの数/ドメイン
    - ドメインごとの Active Directory グループの数
    - ユーザーの数/Active Directory グループ
    - Active Directory の数/ユーザー
    - ドメイン コントローラの数
    - Active Directory ログ サーバの数
- ユーザー ログイン スケール データ：
  - 1 分あたりのユーザーの平均数
- VDI で Identity Firewall を使用する場合のデプロイの詳細：
  - VDI デスクトップの数/vCenter Server
    - ホストの数/vCenter Server
    - VDI デスクトップの数/ホスト
- ゲスト イントロスペクションを使用している場合：
  - VMTools（ゲスト イントロスペクション ドライバ）のバージョン
    - Windows ゲスト OS のバージョン

# ロード バランシングのトラブルシューティング

## 6

NSX Edge ロード バランサを使用すると、ネットワーク トラフィックが特定の宛先まで複数のパスをたどれるようになります。負荷の配分がユーザーにとって透過的になるように、受信サービス リクエストを複数のサーバ間で均等に配分します。NSX では、ワンアーム モード（プロキシ モードとも呼ばれます）またはインライン モード（透過モードとも呼ばれます）の 2 つのタイプのロード バランシング サービスを設定できます。詳細については、『NSX 管理ガイド』を参照してください。

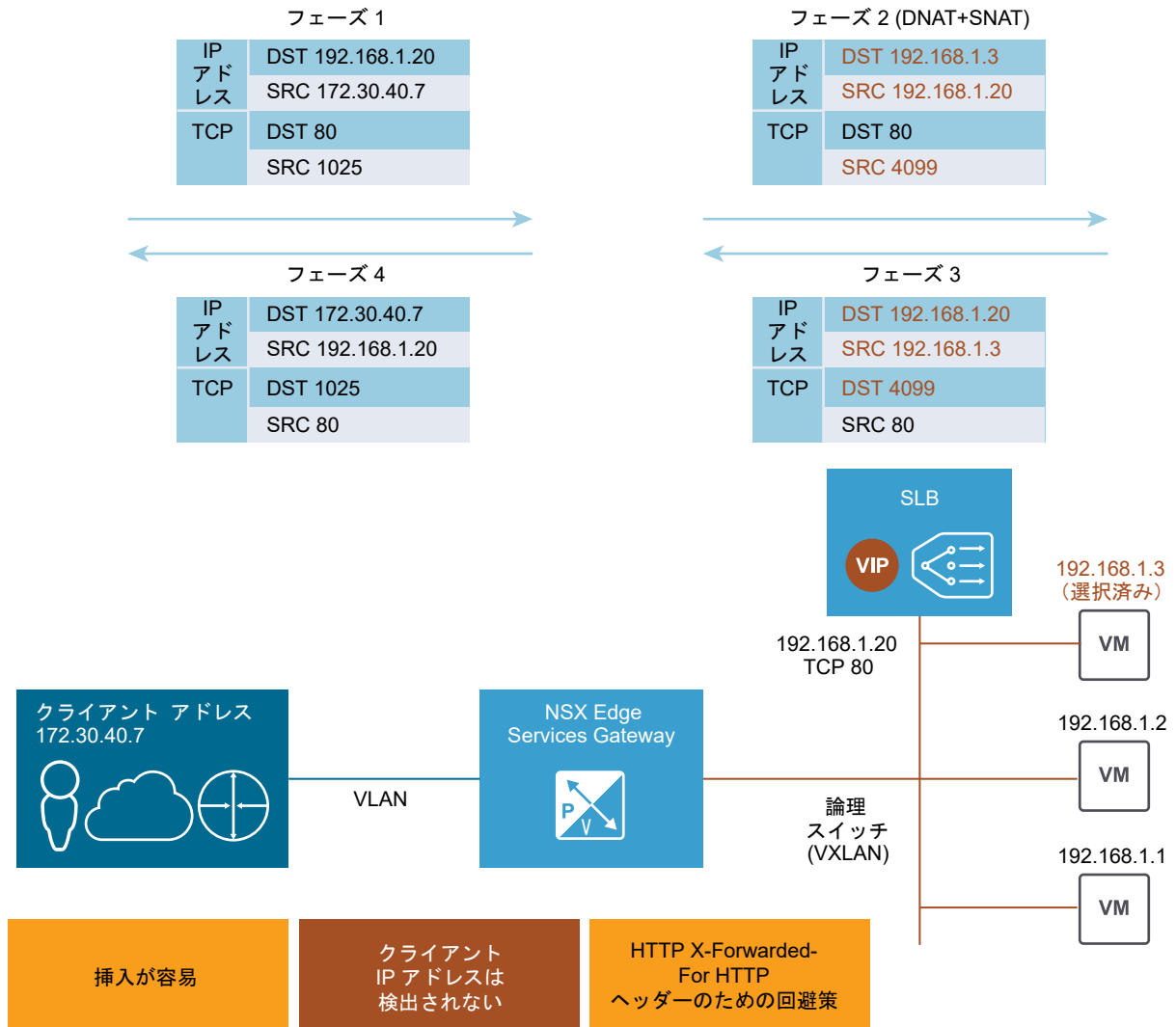
トラブルシューティングを開始して設定を確認する前に、エラーの正確な情報を取得し、クライアント、仮想サーバ、バックエンド サーバに関連するトポロジ マップを作成し、アプリケーション要件を理解しておく必要があります。たとえば、クライアントが接続できないという問題は、接続後のランダムなセッション エラーとは異なります。ロード バランサのトラブルシューティングの際は、必ず接続エラーを確認することから始めてください。

この章には、次のトピックが含まれています。

- [ワンアーム ロード バランサの設定](#)
- [ロード バランサのトラブルシューティングに関するフローチャート](#)
- [ロード バランサ設定の確認とユーザー インターフェイスを使用したトラブルシューティング](#)
- [CLI を使用したロード バランサのトラブルシューティング](#)
- [一般的なロード バランサの問題](#)

## ワンアーム ロード バランサの設定

Edge Services Gateway (ESG) は、受信するクライアント トラフィックのプロキシとして考えることができます。



プロキシ モードでは、ロード バランサは、自身の IP アドレスを送信元アドレスとして使用して、リクエストをバックエンド サーバに送信します。バックエンド サーバには、ロード バランサから送信されるときにすべてのトラフィックが表示され、このサーバはロード バランサに直接応答します。このモードは、**SNAT モード**または**非透過モード**とも呼ばれます。詳細については、『**NSX 管理ガイド**』を参照してください。

一般的な NSX ワンアーム ロード バランサは、バックエンド サーバと同じで分散論理ルーターとは異なるサブネットにデプロイされます。NSX ロード バランサ仮想サーバは、クライアントから受信したリクエストを仮想 IP アドレスで **listen** し、バックエンド サーバにリクエストを送信します。リターン トラフィックについては、リバース NAT が必要となります。これは、バックエンド サーバの送信元 IP アドレスを仮想アドレス (VIP) に変更してから、クライアントに仮想 IP アドレスを送信するためです。この操作を行わないと、クライアントへの接続が切断されます。

ESG はトラフィックを受信した後に、仮想 IP アドレスをいずれかのロード バランサ マシンの IP アドレスに変更する宛先ネットワーク アドレス変換 (DNAT) とクライアント IP アドレスを ESG IP アドレスに交換する送信元ネットワーク アドレス変換 (SNAT) の 2 つの操作を実行します。

次に、ESG サーバはトラフィックをロード バランサ サーバに送信し、ロード バランサ サーバは応答を ESG に返し、さらにクライアントに返します。このオプションでは、インライン モードよりも大幅に容易になりますが、2 つの注意点があります。最初の注意点は、専用の ESG サーバが必要となることであり、2 番目の注意点はロード バランサは元のクライアント IP アドレスを認識しないことです。HTTP/HTTPS アプリケーションでの 1 つの回避策として、HTTP アプリケーション プロファイルで **Insert X-Forwarded-For** を有効にすることによって、バックエンド サーバに送信される要求の **X-Forwarded-For** HTTP ヘッダーにクライアント IP アドレスが追加されます。

バックエンド サーバでのクライアント IP アドレスの可視化が、HTTP/HTTPS 以外のアプリケーションで必要となる場合には、透過的になるように IP アドレス プールを設定できます。クライアントがバックエンド サーバと同じサブネットにない場合には、インライン モードが推奨されます。インライン モードを使用しない場合には、バックエンド サーバのデフォルト ゲートウェイとしてロード バランサの IP アドレスを使用する必要があります。

---

**注：** 接続の整合性を保証する方法には、通常、次の 3 つがあります。

- インライン/透過モード
- SNAT/プロキシ/非透過モード（上記で説明）
- DSR (Direct Server Return)：現在サポートされていません

DSR モードでは、バックエンド サーバが直接クライアントに応答します。現在、NSX ロード バランサは、DSR をサポートしていません。

---

#### 手順

- 1 一例として、SSL オフロードを使用したワンアームの仮想サーバを設定します。Edge をダブルクリックしてから、[管理(Manage)] > [設定(Settings)] > [証明書(Certificate)] を選択して、証明書を作成します。

- 2 [管理(Manage)] > [ロード バランサ(Load Balancer)] > [グローバル設定(Global Configuration)] > [編集(Edit)] の順に選択して、ロード バランサ サービスを有効にします。

**Edit Load balancer global configuration**

☒ Enable Load Balancer

☐ Enable Acceleration

☐ Logging

Log Level: **Info** ▼

☐ Enable Service Insertion

Service Definition:

Service Configuration:

Deployment Specification:

- 3 [管理(Manage)] > [ロード バランサ(Load Balancer)] > [アプリケーション プロファイル(Application Profiles)] を選択して、HTTPS アプリケーション プロファイルを作成します。

**New Profile** ?

Name:

Type: **HTTPS** ▼

☐ Enable SSL Passthrough

HTTP Redirect URL:

Persistence: **None** ▼

Cookie Name:

Mode:

Expires in (Seconds):

☐ Insert X-Forwarded-For HTTP header

☐ Enable Pool Side SSL

Virtual Server Certificate... **Pool Certificates**

**Service Certificates** CA Certificates CRL

☒ Configure Service Certificate

	Common Name	Issuer	Validity
<input checked="" type="radio"/>	VSM_SOLUTION_71	VSM_SOLUTION_71	Tue Sep 8 2015 - Thu
<input type="radio"/>	VSM_SOLUTION_71	VSM_SOLUTION_71	Tue Sep 8 2015 - Thu

**注：** ドキュメント作成の都合上、上記のスクリーンショットでは、自己署名の証明書が使用されています。

- 4 オプションで、[管理(Manage)] > [ロード バランサ(Load Balancer)] > [サービス モニタリング(Service Monitoring)] をクリックして、デフォルトのサービス モニタリングを編集し、必要に応じて、基本の HTTP/HTTPS から特定の URL/URI に変更します。

- 5 [管理(Manage)] > [ロード バランサ(Load Balancer)] > [プール(Pools)] を選択して、サーバ プールを作成します。

SNAT モードを使用するには、プール設定の [透過的 (Transparent)] チェック ボックスをオフのままにします。

Enabled	Name	IP Address / VC Container	Weight	Monitor Port	Port	Max Connections	Min Connections
✓	web-01a	172.16.10.11	1	443	443	0	0
✓	web-02a	172.16.10.12	1	443	443	0	0

仮想マシンが表示され有効になっていることを確認します。

- 6 オプションで、[管理(Manage)] > [ロード バランサ(Load Balancer)] > [プール(Pools)] > [プール統計の表示 (Show Pool Statistics)] をクリックして、ステータスを確認します。

メンバー ステータスが [UP] であることを確認します。

- 7 [管理(Manage)] > [ロード バランサ(Load Balancer)] > [仮想サーバ(Virtual Servers)] を選択して、仮想サーバを作成します。

UDP やさらに高パフォーマンスの TCP に L4 ロード バランサを使用する場合には、[アクセラレーションの有効化 (Enable Acceleration)] をオンにします。[アクセラレーションの有効化 (Enable Acceleration)] をオンにしている場合、L4 SNAT でファイアウォールが必要であるため、ファイアウォールのステータスがロード バランサ NSX Edge で [有効 (Enabled)] になっていることを確認します。

General Advanced

☒ Enable Virtual Server

☐ Enable Acceleration

Application Profile: \* OneArmWeb-01

Name: \* Web-Tier-VIP-01

Description:

IP Address: \* 172.16.10.10 Select IP Address

Protocol: HTTPS

Port: \* 443

Default Pool: Web-Tier-Pool-01

Connection Limit: 0

Connection Rate Limit: 0 (CPS)

IP アドレスがサーバ プールに関連付けられていることを確認します。

- 8 オプションで、アプリケーション ルールを使用している場合、[管理(Manage)] > [ロード バランサ(Load Balancer)] > [アプリケーション ルール(Application Rules)] で設定を確認します。

Add Application Rule

Name: App-Rule-1

Script: # A sample application rule to log the name of the virtual server  
capture request header Host len 32

- 9 アプリケーション ルールを使用する場合、[管理(Manage)] > [ロード バランサ(Load Balancer)] > [仮想サーバ (Virtual Servers)] > [詳細(Advanced)] で仮想サーバにアプリケーション ルールが関連付けられていることを確認します。

サポートされる例については、<https://communities.vmware.com/docs/DOC-31772> を参照してください。

Edit Virtual Server

General Advanced

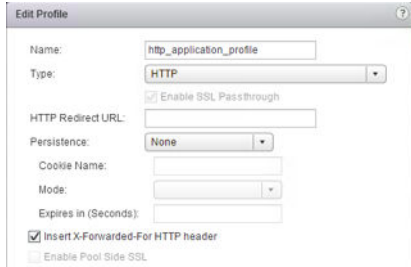
Application Rules:

+ x ≡ ≡ Filter

Rule Id	Name	Script
applicationRule-1	App-rule-1	capture request he...

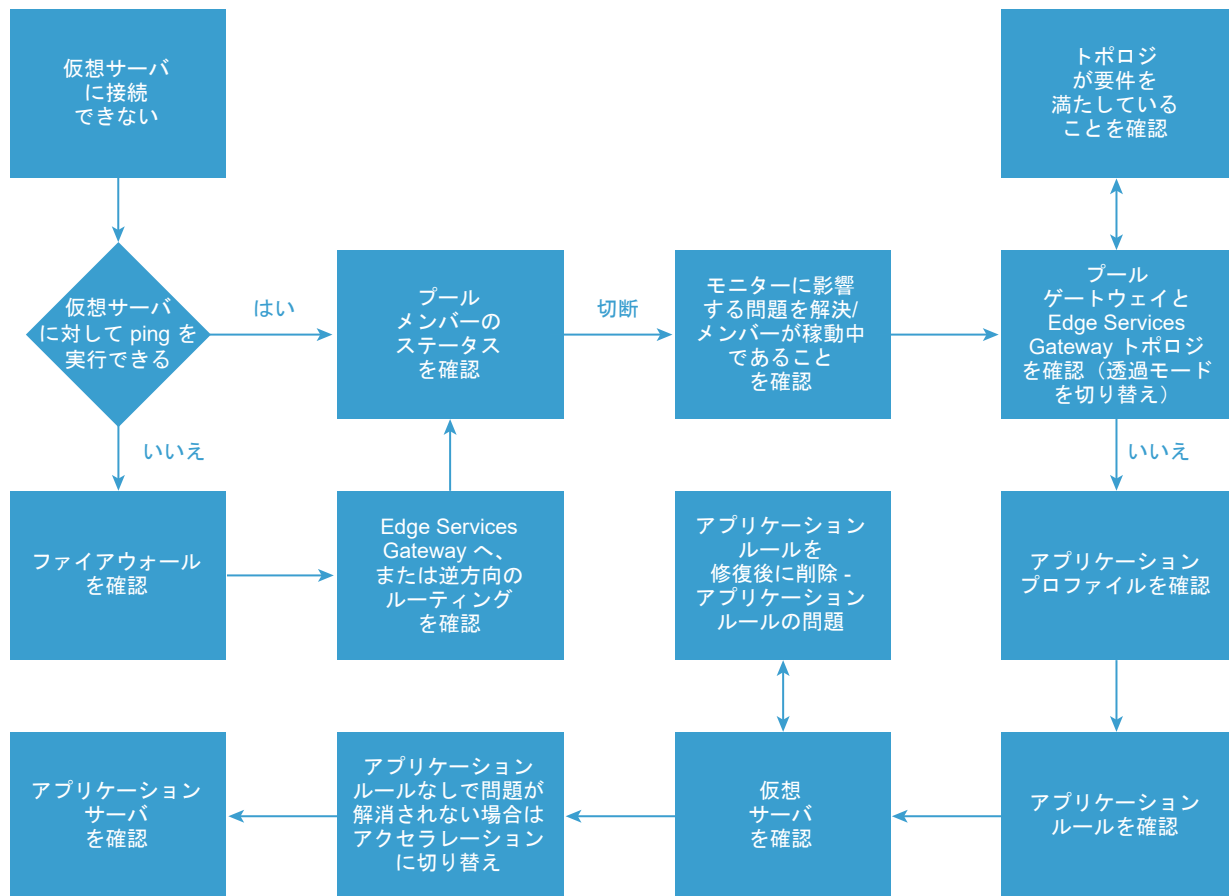


非透過モードでは、バックエンド サーバはクライアント IP アドレスを確認できませんが、ロード バランサ内部の IP アドレスは確認できます。HTTP/HTTPS トラフィックのための回避策として、[X-Forwarded-For HTTP ヘッダの挿入 (Insert X-Forwarded-For HTTP header)] をオンにします。このオプションをオンにすると、Edge ロード バランサは、クライアント 送信元 IP アドレスの値にヘッダー「X-Forwarded-For」を追加します。



## ロード バランサのトラブルシューティングに関するフローチャート

次のフローチャートは、ロード バランサに関する問題のトラブルシューティング方法の概要を示しています。



## ロード バランサ設定の確認とユーザー インターフェイスを使用した トラブルシューティング

ロード バランサ設定は vSphere Web Client を使用して確認できます。ユーザー インターフェイスを使用して、ロード バランサをトラブルシューティングできます。

何が正しい動作かを理解し、問題を定義したら、次のようにユーザー インターフェイスを使用して設定を確認します。

### 前提条件

次の情報を書き留めます。

- 仮想サーバの IP アドレス、プロトコル、およびポート。
- バックエンド アプリケーション サーバの IP アドレスおよびポート。
- 目的としていたトポロジ（インラインまたはワンアーム）詳細については、『NSX 管理ガイド』にある論理ロード バランサのトピックを参照してください。
- トレース ルートを確認し、他のネットワーク接続ツールを使用して、パケットが正しい場所 (Edge Services Gateway) に向かっていることを確認します。
- アップストリーム ファイアウォールがトラフィックを正しく許可していることを確認します。
- 直面している問題を定義します。たとえば、仮想サーバの DNS レコードは正しいがコンテンツが返されない、または誤ったコンテンツが返されるなどです。

### 問題

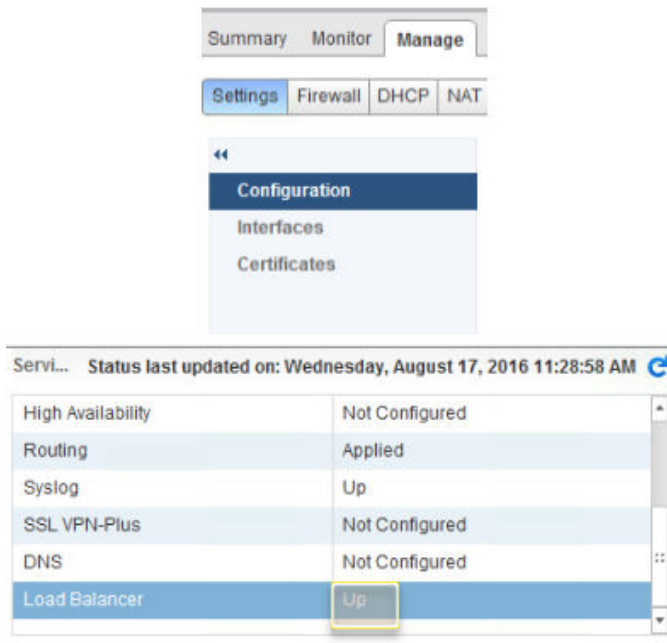
ロード バランサを期待どおりに実行できない。

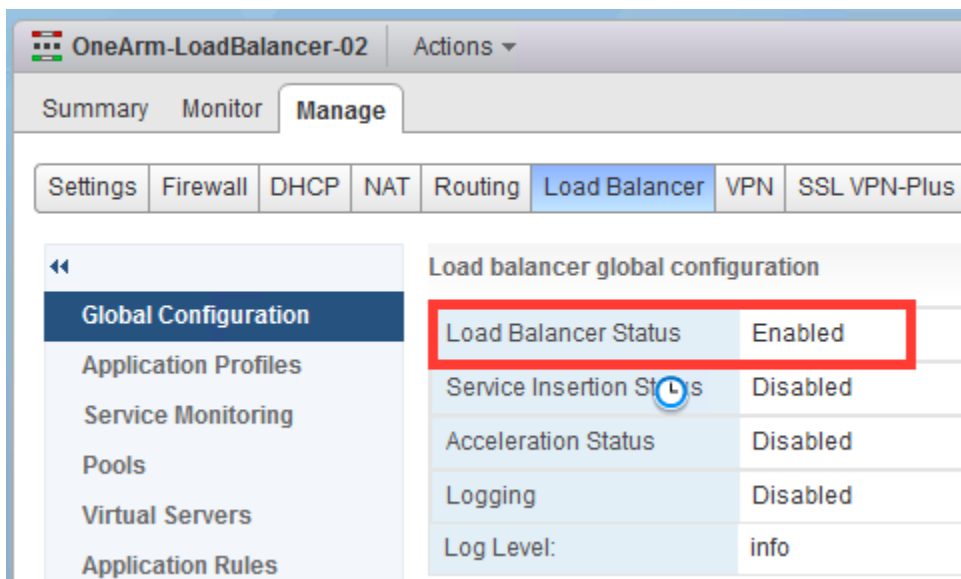
### 解決方法

- 1 ロード バランサでサポートする必要のあるプロトコル (TCP、UDP、HTTP、HTTPS)、ポート、セッション維持要件、およびプール メンバーに関する次のアプリケーション要件を確認します。
  - ロード バランサとファイアウォールは有効になっているか。Edge Services Gateway に正しいルートが設定されているか。
  - 仮想サーバが待機する必要がある IP アドレス、ポート、およびプロトコルはどれか。
  - SSL オフロードが使用されているか。バックエンド サーバとの通信の際に SSL を使用する必要があるか。
  - アプリケーション ルールを使用しているか。
  - トポロジは何か。NSX ロード バランサは、クライアントとサーバからのすべてのトラフィックを解析する必要があります。
  - NSX ロード バランサはインラインかどうか、またはクライアント ソース アドレスが変換されているか（リターントラフィックがロード バランサに確実に戻るため）。

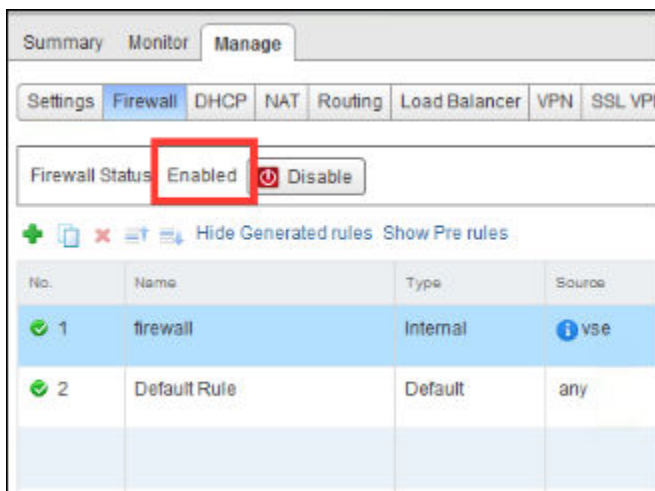
- 2 NSX Edge に移動して、ロード バランシングを有効にし、トラフィックの送信を許可するために必要な設定を確認します。次にそれを示します。

- a ロード バランサが [接続中 (Up)] としてリストされていることを確認します。





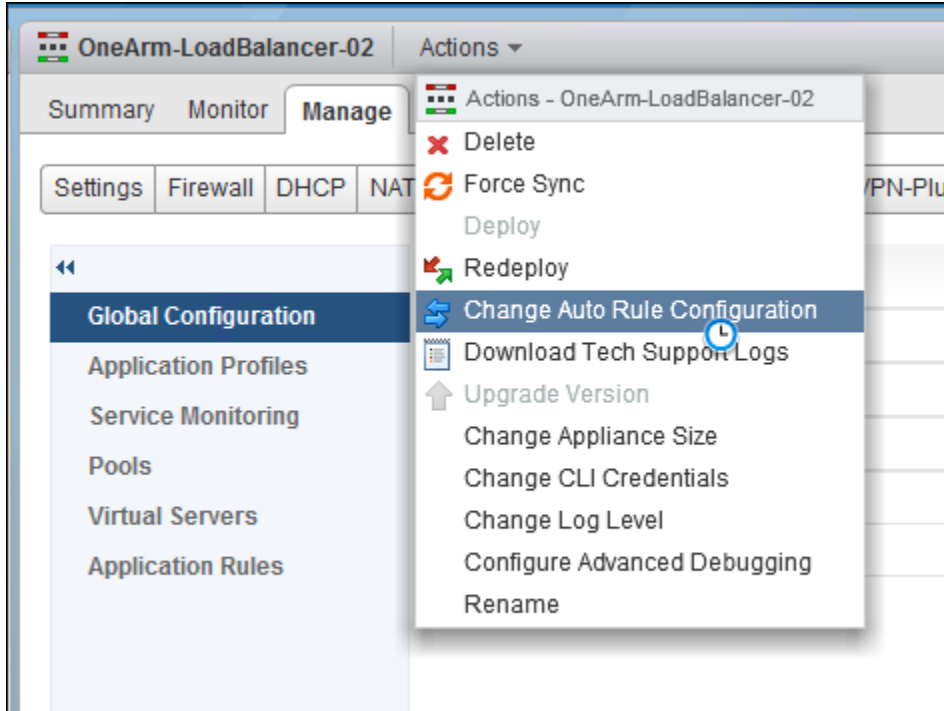
- b ファイアウォールが [有効 (Enabled)] になっていることを確認します。アクセラレーション対応の仮想サーバでは、ファイアウォールを有効にする必要があります。アクセラレーション非対応の TCP と L7 HTTP/HTTPS VIP には、トラフィックを許可するポリシーが必要です。ファイアウォール フィルタは、アクセラレーション対応の仮想サーバに影響しません。



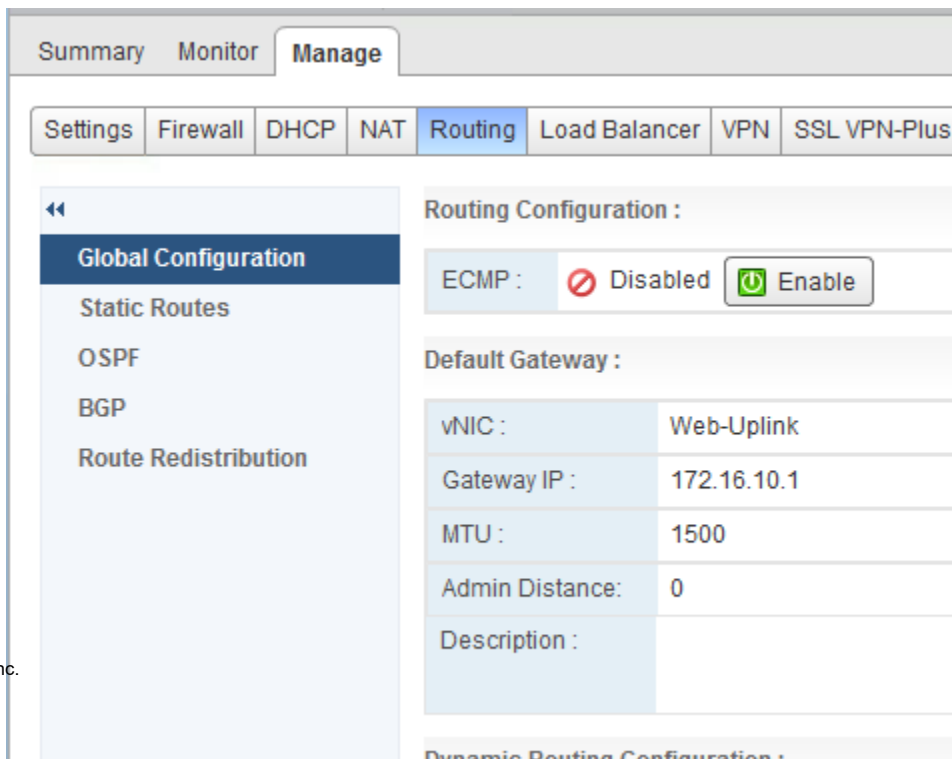
- c 仮想サーバに対して NAT ルールが作成されていることを確認します。[NAT] タブで、[内部ルールを非表示にする (Hide internal rules)] または [内部ルールを表示 (Unhide internal rules)] リンクをクリックして確認します。

**注：** ロード バランシングを有効にし、サービスを設定しても、NAT ルールを設定していない場合は、自動ルール設定が有効でなかったことを意味します。

- d 自動ルール設定は変更できます。詳細については、『NSX 管理ガイド』にある自動ルール設定の変更に関するトピックを参照してください。NSX Edge Services Gateway をデプロイする際は、自動ルールを設定するオプションを選択できます。Edge Services Gateway のデプロイ時にこのオプションを選択しなかった場合でも、ロード バランサを正しく動作させるにはこれを有効にする必要があります。ユーザー インターフェイスからプール メンバーのステータスを確認します。



- e ルーティングを確認します。また、Edge Services Gateway にクライアント システムとバックエンド サーバへのデフォルト ルートまたはスタティック ルートがあることを確認します。サーバへのルートがないと、健全性チェックに合格しません。動的ルーティング プロトコルを使用している場合は、CLI が必要になることがあります。詳細については、[NSX のルーティング CLI](#) を参照してください。
- a デフォルト ルートを確認します。



ルートです。多くの場合、アプリケーション サーバはこれらのサーバに接続されます。

⚙️ 0 Job(s) In Progress
❗ 0 Job(s) Failed

aces of this NSX Edge.

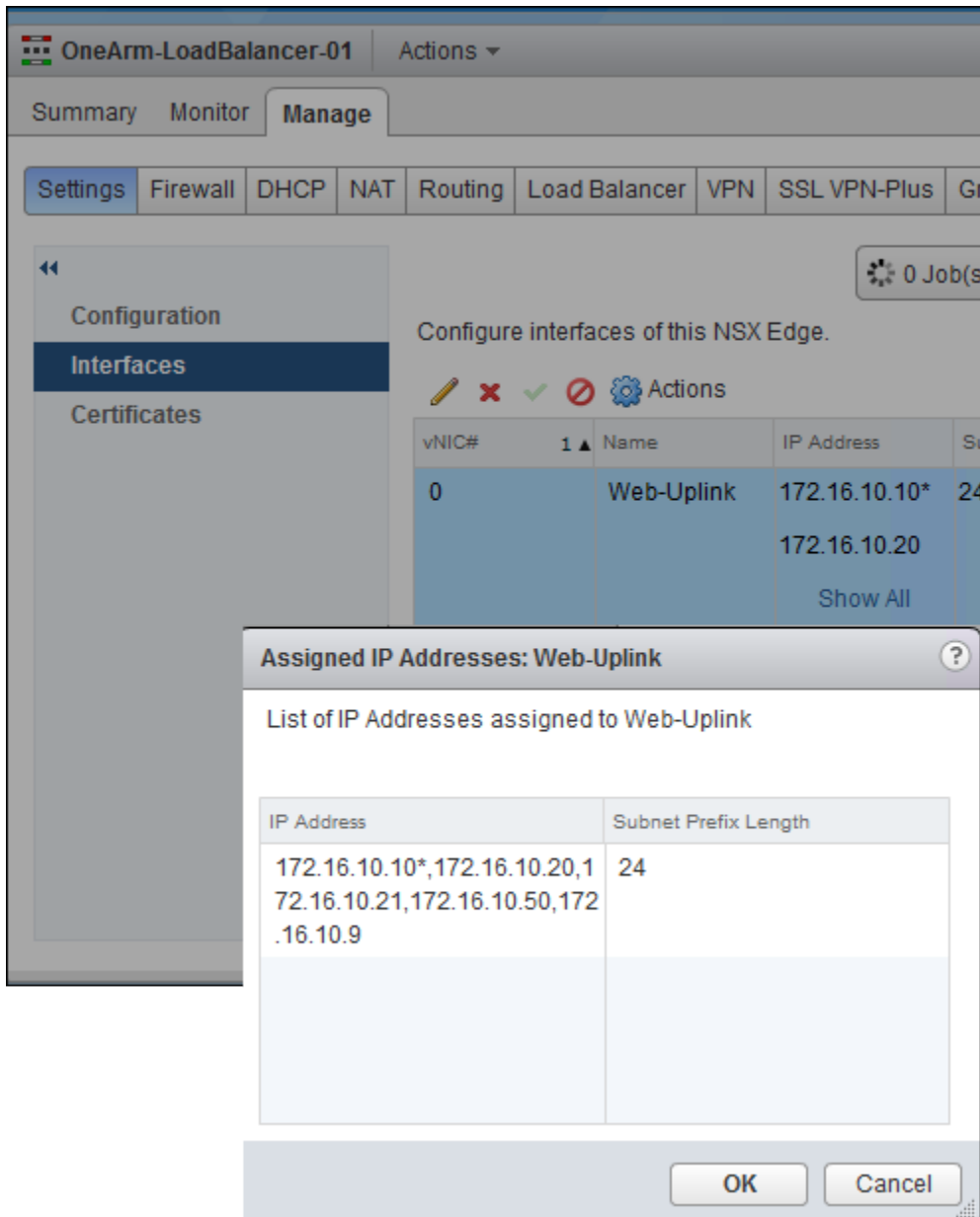
⚙️ Actions
🔍 Filter

Name	IP Address	Subnet Prefix Length	Connected To	Type	Status
Web-Uplink	172.16.10.10*	24	Web-Tier-01	Uplink	✓
	172.16.10.20				
	<a href="#">Show All</a>				
INLINE_SUBNI	172.16.100.1*	24	INLINE_SUBNI	Internal	✓
vnic2				Internal	❌
vnic3				Internal	❌
vnic4				Internal	❌
vnic5				Internal	❌

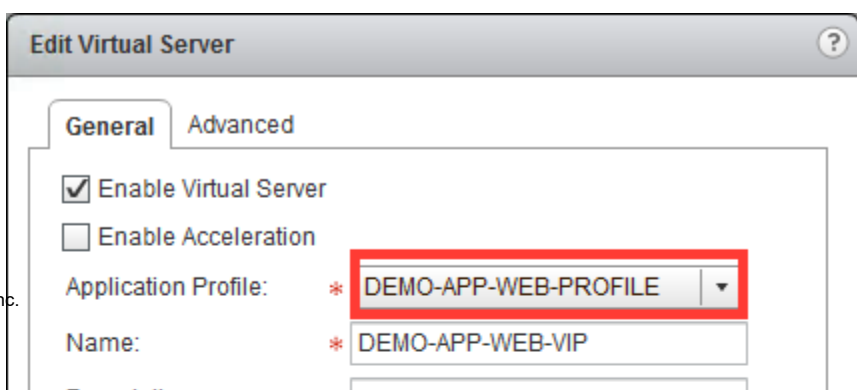
- c [ルーティング (Routing)] タブ > [スタティック ルート (Static Routes)] でスタティック ルートを確認します。

### 3 仮想サーバの IP アドレス、ポート、およびプロトコルを確認します。

- a NSX Edge をダブルクリックして、[管理 (Manage)] - [設定 (Settings)]> [インターフェイス (Interfaces)] の順に移動します。仮想サーバの IP アドレスがインターフェイスに追加されたことを確認します。



- b 仮想サーバに、アプリケーションをサポートするための適切な IP アドレス、ポート、およびプロトコルが設定されていることを確認します。
- a 仮想サーバで使用するアプリケーション プロファイルを確認します。



たは HTTPS) を書き留めます。

**Edit Virtual Server**

**General** | Advanced

☒ Enable Virtual Server  
☐ Enable Acceleration

Application Profile: \* DEMO-APP-WEB-PROFILE ▼

Name: \* DEMO-APP-WEB-VIP

Description:

IP Address: \* 172.16.10.20 × [Select IP Address](#)

Protocol: HTTPS ▼

Port: \* 443

Default Pool: Web-Tier-Pool-01 ▼

Connection Limit: 0

Connection Rate Limit: 0 (CPS)

OK Cancel



- c アプリケーション プロファイルが、サポートされるパーシステンス方法、タイプ（プロトコル）、および SSL（必要な場合）に合致していることを確認します。SSL を使用する場合は、正しい名前と有効期限の証明書を使用していることを確認します。

**Edit Profile**

Name: DEMO-APP-WEB-PROFILE

Type: HTTPS

☐ Enable SSL Passthrough

HTTP Redirect URL:

Persistence: Source IP

Cookie Name:

Mode:

Expires in (Seconds):

☒ Insert X-Forwarded-For HTTP header

☐ Enable Pool Side SSL

**Virtual Server Certificates** Pool Certificates

Service Certificates CA Certificates CRL

☒ Configure Service Certificate

	Common Name	Issuer	Validity
<input checked="" type="radio"/>	DEMO.WEB.APP.CO	DEMO.WEB.APP.CO	Wed Apr 27 2016 - Sat
<input type="radio"/>	VSM_SOLUTION_71	VSM_SOLUTION_71	Tue Sep 8 2015 - Thu
<input type="radio"/>	VSM_SOLUTION_71	VSM_SOLUTION_71	Tue Sep 8 2015 - Thu
<input type="radio"/>	psc-01a.corp.local	CA	Thu Mar 12 2015 - Thu
<input type="radio"/>	VSM_SOLUTION_49	VSM_SOLUTION_49	Tue Sep 8 2015 - Thu
<input type="radio"/>	VSM_SOLUTION_49	VSM_SOLUTION_49	Tue Sep 8 2015 - Thu

Cipher: Default

Client Authentication: Ignore

OK Cancel

- d 接続先クライアントに対して正しい証明書が使用されていることを確認します。

**Edit Profile**

Name: DEMO-APP-WEB-PROFILE

Type: HTTPS

☐ Enable SSL Passthrough

HTTP Redirect URL:

Persistence: Source IP

Cookie Name:

Mode:

Expires in (Seconds):

☒ Insert X-Forwarded-For HTTP header

☒ Enable Pool Side SSL

Virtual Server Certificates **Pool Certificates**

Service Certificates CA Certificates CRL

☒ Configure Service Certificate

	Common Name	Issuer	Validity
<input checked="" type="radio"/>	DEMO.WEB.APP.COF	DEMO.WEB.APP.COF	Wed Apr 27 2016 - Sa
<input type="radio"/>	VSM_SOLUTION_71f	VSM_SOLUTION_71f	Tue Sep 8 2015 - Thu
<input type="radio"/>	VSM_SOLUTION_71f	VSM_SOLUTION_71f	Tue Sep 8 2015 - Thu
<input type="radio"/>	psc-01a.corp.local	CA	Thu Mar 12 2015 - Th
<input type="radio"/>	VSM_SOLUTION_49c	VSM_SOLUTION_49c	Tue Sep 8 2015 - Thu
<input type="radio"/>	VSM_SOLUTION_49c	VSM_SOLUTION_49c	Tue Sep 8 2015 - Thu

Cipher: Default

Client Authentication: Ignore

OK Cancel

- e クライアント証明書が必要かどうかを確認します。ただし、クライアントは設定されていません。さらに、暗号化範囲が狭い暗号リストを選択していないかどうかを確認します（たとえば、古いブラウザを使用しているクライアントがいる場合）。

**Edit Profile**

Name: DEMO-APP-WEB-PROFILE

Type: HTTPS

☐ Enable SSL Passthrough

HTTP Redirect URL:

Persistence: Source IP

Cookie Name:

Mode:

Expires in (Seconds):

☒ Insert X-Forwarded-For HTTP header

☐ Enable Pool Side SSL

**Virtual Server Certificates** Pool Certificates

Service Certificates CA Certificates CRL

☒ Configure Service Certificate

	Common Name	Issuer	Validity
<input checked="" type="radio"/>	DEMO.WEB.APP.CO	DEMO.WEB.APP.CO	Wed Apr 27 2016 - Sat
<input type="radio"/>	VSM_SOLUTION_71	VSM_SOLUTION_71	Tue Sep 8 2015 - Thu
<input type="radio"/>	VSM_SOLUTION_71	VSM_SOLUTION_71	Tue Sep 8 2015 - Thu
<input type="radio"/>	psc-01a.corp.local	CA	Thu Mar 12 2015 - Thu
<input type="radio"/>	VSM_SOLUTION_49	VSM_SOLUTION_49	Tue Sep 8 2015 - Thu
<input type="radio"/>	VSM_SOLUTION_49	VSM_SOLUTION_49	Tue Sep 8 2015 - Thu

Cipher: Default

Client Authentication: Ignore

OK Cancel

- f バックエンド サーバに SSL が必要かどうかを確認します。

**Edit Profile**

Name: DEMO-APP-WEB-PROFILE

Type: HTTPS

☐ Enable SSL Passthrough

HTTP Redirect URL:

#### 4 次のように、プールのステータスと設定を確認します。

- a プールのステータスを確認します。トラフィックに対応するには少なくとも 1 メンバーが稼動している必要がありますが、すべてのトラフィックに対応するには、1 メンバーでは足りない場合があります。稼動しているプール メンバーがない、または少数のみの場合は、次の手順の説明に従って問題を修正してください。

Pool and Member Status

Pool Status and Statistics:

Pool ID	Name	Status
pool-1	TENANT-1-TCP-P...	UP

Member Status and Statistics:

Name	IP Address / VC Container	Status	Member ID
SERVER-1	10.10.10.100	UP	member-1
SERVER-2	10.10.10.101	UP	member-2

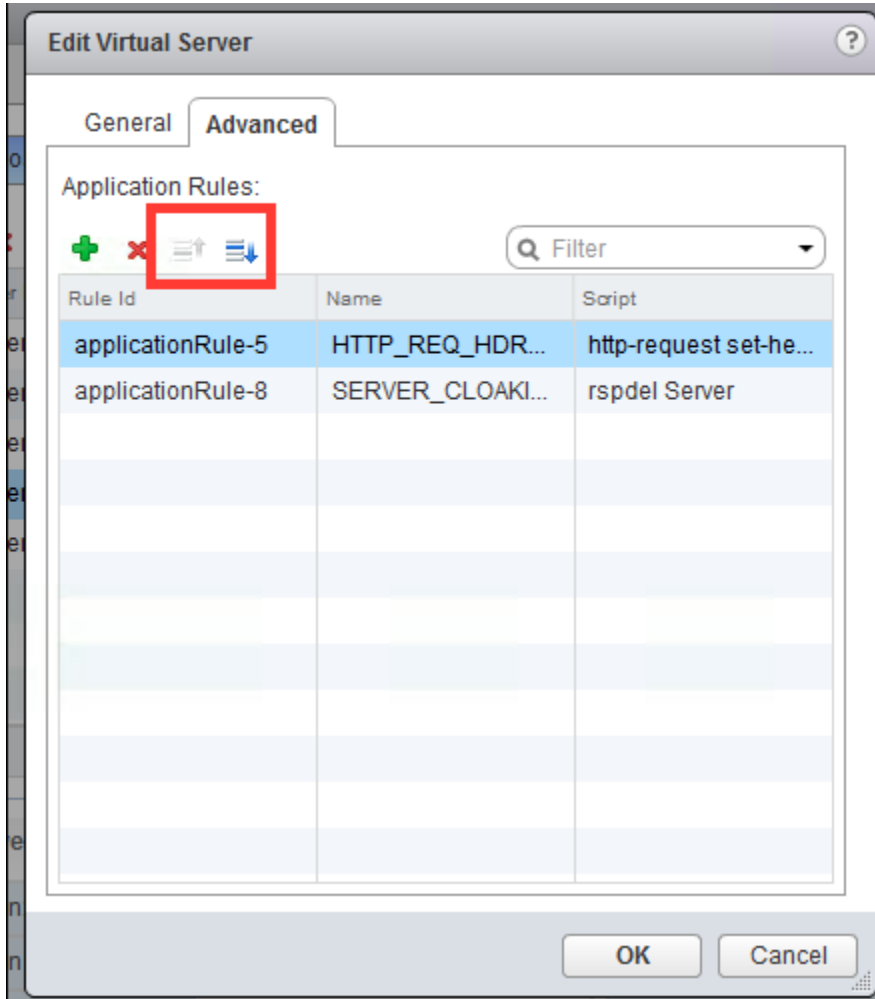
- b トポロジが正しいことを確認します。SNAT クライアントのトラフィックはプール設定で制御されます。すべてのトラフィックを確認できるようにロード バランサ機能をホストする Edge Services Gateway を配置しないと、トラフィックの制御に失敗します。クライアント ソースの IP アドレスを維持する場合は、[透過的 (Transparent)] モードを選択します。詳細については、『NSX 管理ガイド』を参照してください。

Edit Pool							
Name:	*	DEMO_APP_WEB_POOL					
Description:							
Algorithm:		ROUND-ROBIN ▼					
Algorithm Parameters:							
Monitors:		default_http_monitor ▼					
Members:							

Enabled	Name	IP Address / VC Container	Weight	Monitor Port	Port	Max Connections	M C

- 5 アプリケーション ルールを使用している場合は、ルールを確認します。必要に応じてルールを削除しながら、トラフィック フローに問題があるか確認します。
- a ルールの順序を変更して、これがトラフィック フローを中断するロジックの原因かどうかを確認します。アプリケーション ルールの追加方法と、アプリケーション ルールの例については、『NSX 管理ガイド』にあるアプリケーション ルールの追加に関するトピックを参照してください。



#### 次のステップ

問題が見つからない場合は、CLI（コマンド ライン インターフェイス）を使用して状態を確認する場合があります。詳細については、[CLI を使用したロード バランサのトラブルシューティング](#)を参照してください。

## CLI を使用したロード バランサのトラブルシューティング

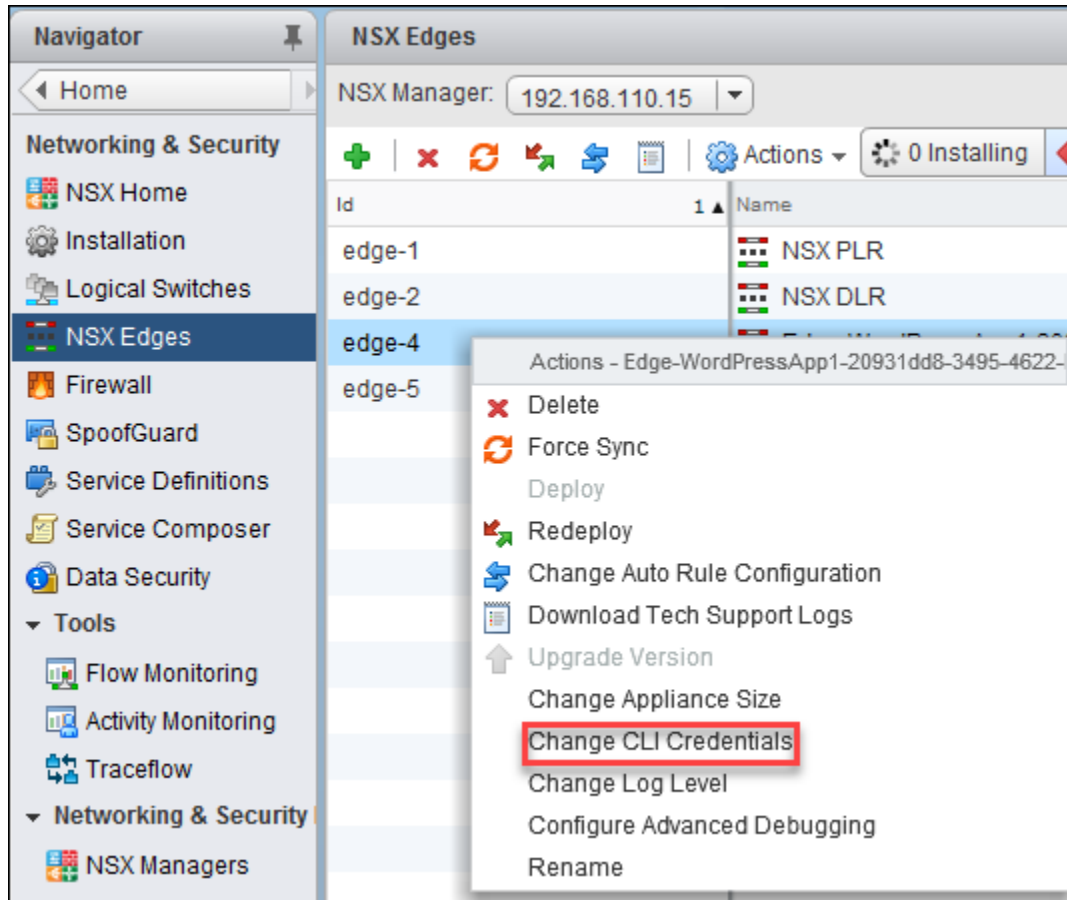
NSX CLI を使用すると、詳細なログ情報やパケットを収集し、ロード バランサのトラブルシューティングに役立つメトリックを確認できます。

#### 問題

ロード バランシングを期待とおりに機能しない

## 解決方法

- 1 仮想アプライアンスで SSH を有効にできるかどうかを確認します。Edge Services Gateway は、デプロイ時に SSH を有効にするオプションを備えた仮想アプライアンスです。SSH を有効にする必要がある場合は、必要なアプライアンスを選択し、[アクション (Actions)] メニューで [CLI 認証情報の変更 (Change CLI Credentials)] をクリックします。



- 2 Edge Services Gateway には、実行時の状態や設定状態を確認するための show コマンドが複数あります。設定情報や統計情報を表示するには、これらのコマンドを使用します。

```
nsxedge> show configuration loadbalancer
nsxedge> show configuration loadbalancer virtual [virtual-server-name]
nsxedge> show configuration loadbalancer pool [pool-name]
nsxedge> show configuration loadbalancer monitor [monitor-name]
nsxedge> show configuration loadbalancer profile [profile-name]
nsxedge> show configuration loadbalancer rule [rule-name]
```

- 3 ロード バランシングと NAT を正しく機能させるには、ファイアウォールを有効にする必要があります。#show firewall コマンドを使用してください。このコマンドを使用しても期待する情報が得られない場合は「[ロード バランサ設定の確認とユーザー インターフェイスを使用したトラブルシューティング](#)」セクションを参照してください。

```

NSX-edge-8-0> show firewall
Chain PREROUTING (policy ACCEPT 21947 packets, 7809K bytes)
:cid  pkts bytes target      prot opt in      out     source      destination
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
:cid  pkts bytes target      prot opt in      out     source      destination
)      348 67915 ACCEPT      all  --  lo      *       0.0.0.0/0    0.0.0.0/0
)      134  5360 DROP        all  --  *       *       0.0.0.0/0    0.0.0.0/0    state INVALID
)     21482 7736K block_in all  --  *       *       0.0.0.0/0    0.0.0.0/0
)     20545 7671K ACCEPT     all  --  *       *       0.0.0.0/0    0.0.0.0/0    state RELATED
)       937 65139 usr_rules  all  --  *       *       0.0.0.0/0    0.0.0.0/0
)         0 0 DROP        all  --  *       *       0.0.0.0/0    0.0.0.0/0
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
:cid  pkts bytes target      prot opt in      out     source      destination
Chain OUTPUT (policy ACCEPT 20673 packets, 1248K bytes)
:cid  pkts bytes target      prot opt in      out     source      destination
Chain POSTROUTING (policy ACCEPT 0 packets, 0 bytes)
:cid  pkts bytes target      prot opt in      out     source      destination
)      348 67915 ACCEPT      all  --  *       lo      0.0.0.0/0    0.0.0.0/0
)       34  1360 DROP        all  --  *       *       0.0.0.0/0    0.0.0.0/0    state INVALID
)     20295 1179K block_out all  --  *       *       0.0.0.0/0    0.0.0.0/0
)         0 0 ACCEPT      all  --  *       *       0.0.0.0/0    0.0.0.0/0    PHYSDEV match
)         0 0 ACCEPT      all  --  *       *       0.0.0.0/0    0.0.0.0/0    PHYSDEV match
)         0 0 ACCEPT      all  --  *       *       0.0.0.0/0    0.0.0.0/0    PHYSDEV match
)         0 0 ACCEPT      all  --  *       *       0.0.0.0/0    0.0.0.0/0    PHYSDEV match
)     14599 802K ACCEPT     all  --  *       *       0.0.0.0/0    0.0.0.0/0    state RELATED
)      5696  377K usr_rules  all  --  *       *       0.0.0.0/0    0.0.0.0/0
)         0 0 DROP        all  --  *       *       0.0.0.0/0    0.0.0.0/0
Chain block_in (1 references)
:cid  pkts bytes target      prot opt in      out     source      destination
Chain block_out (1 references)
:cid  pkts bytes target      prot opt in      out     source      destination
Chain usr_rules (2 references)
:cid  pkts bytes target      prot opt in      out     source      destination
133137 4861  333K ACCEPT      all  --  *       *       0.0.0.0/0    0.0.0.0/0    match-set 0_
133138 0 0 ACCEPT      all  --  *       *       0.0.0.0/0    0.0.0.0/0    match-set 1_
133139 936 65099 ACCEPT     all  --  *       *       0.0.0.0/0    0.0.0.0/0    match-set 2_
133141 835 43459 ACCEPT     all  --  *       *       0.0.0.0/0    0.0.0.0/0    match-set 3_
133131 1 40 LOG        all  --  *       *       0.0.0.0/0    0.0.0.0/0    LOG flags 0
133131 1 40 ACCEPT     all  --  *       *       0.0.0.0/0    0.0.0.0/0

```

- 4 ロード バランサを正しく機能させるには NAT が必要です。show nat コマンドを使用してください。このコマンドを使用しても期待する情報が得られない場合は「[ロード バランサ設定の確認とユーザー インターフェイスを使用したトラブルシューティング](#)」セクションを参照してください。

```

NSX-edge-8-0> show nat
Chain PREROUTING (policy ACCEPT 568 packets, 40044 bytes)
rid  pkts bytes target    prot opt in     out     source    destination
0      568 40044 int_dnat  all  --  *      *       0.0.0.0/0  0.0.0.0/0
0      568 40044 usr_dnat  all  --  *      *       0.0.0.0/0  0.0.0.0/0

Chain INPUT (policy ACCEPT 568 packets, 40044 bytes)
rid  pkts bytes target    prot opt in     out     source    destination

Chain OUTPUT (policy ACCEPT 896 packets, 46706 bytes)
rid  pkts bytes target    prot opt in     out     source    destination
0      896 46706 int_dnat  all  --  *      *       0.0.0.0/0  0.0.0.0/0
0      896 46706 usr_dnat  all  --  *      *       0.0.0.0/0  0.0.0.0/0

Chain POSTROUTING (policy ACCEPT 896 packets, 46706 bytes)
rid  pkts bytes target    prot opt in     out     source    destination
0      896 46706 int_snat  all  --  *      *       0.0.0.0/0  0.0.0.0/0
0      896 46706 usr_snat  all  --  *      *       0.0.0.0/0  0.0.0.0/0

Chain int_dnat (2 references)
rid  pkts bytes target    prot opt in     out     source    destination

Chain int_snat (1 references)
rid  pkts bytes target    prot opt in     out     source    destination
0      0      0 ACCEPT  all  --  *      *       0.0.0.0/0  0.0.0.0/0

Chain usr_dnat (2 references)
rid  pkts bytes target    prot opt in     out     source    destination
0      0      0 DNAT    tcp  --  vNic_2 *       0.0.0.0/0  192.168.8.20
0      0      0 LOG     all  --  vNic_2 *       0.0.0.0/0  192.168.8.11
0      0      0 DNAT    all  --  vNic_2 *       0.0.0.0/0  192.168.8.11

Chain usr_snat (1 references)
rid  pkts bytes target    prot opt in     out     source    destination
0      0      0 LOG     all  --  *      vNic_2 10.10.10.101 0.0.0.0/0
0      0      0 SNAT    all  --  *      vNic_2 10.10.10.101 0.0.0.0/0
0      0      0 LOG     all  --  *      vNic_2 10.10.10.0/24 0.0.0.0/0
0      0      0 SNAT    all  --  *      vNic_2 10.10.10.0/24 0.0.0.0/0
NSX-edge-8-0>

```

- 5 ファイアウォールを有効にし、ロード バランサに NAT ルールを適用するほか、ロード バランシング プロセスを有効にする必要もあります。ロード バランサ エンジンのステータス (L4/L7) を確認するには、show service loadbalancer コマンドを使用します。

```

nsxedge> show service loadbalancer
haIndex:          0
-----
Loadbalancer Services Status:

L7 Loadbalancer   : running
-----
L7 Loadbalancer Statistics:
STATUS    PID      MAX_MEM_MB  MAX SOCK  MAX_CONN  MAX_PIPE  CUR_CONN  CONN_RATE
CONN_RATE_LIMIT MAX_CONN_RATE
running   1580      0           2081      1024      0          0          0

```



```

0          0
-----
L4 Loadbalancer Statistics:
MAX_CONN  ACT_CONN  INACT_CONN  TOTAL_CONN
0          0          0          0

Prot LocalAddress:Port Scheduler Flags
-> RemoteAddress:Port      Forward Weight ActiveConn InActConn

```

- a `show service loadbalancer session` コマンドを使用して、ロード バランサのセッション テーブルを表示します。システムにトラフィックがある場合はセッションが表示されます。

```

nsxedge> show service loadbalancer session
-----
L7 Loadbalancer Statistics:
STATUS      PID      MAX_MEM_MB  MAX SOCK   MAX_CONN   MAX_PIPE   CUR_CONN   CONN_RATE
CONN_RATE_LIMIT MAX_CONN_RATE
running    1580      0          2081      1024       0          0          0
0          0

-----L7 Loadbalancer Current Sessions:

0x2192df1f300: proto=unix_stream src=unix:1 fe=GLOBAL be=<NONE> srv=<none> ts=09 age=0s
calls=2 rq[f=c08200h,
i=0,an=00h,rx=20s,wx=,ax=] rp[f=008000h,i=0,an=00h,rx=wx,ax=] s0=[7,8h,fd=1,ex=]
s1=[7,0h,fd=-1,ex=] exp=19s

-----
L4 Loadbalancer Statistics:
MAX_CONN  ACT_CONN  INACT_CONN  TOTAL_CONN
0          0          0          0

L4 Loadbalancer Current Sessions:

pro expire state      source      virtual      destination

```

- b `show service loadbalancer table` コマンドを使用して、ロード バランサのレイヤー 7 スティッキー テーブルのステータスを確認します。このテーブルにはアクセラレーション対応の仮想サーバの情報が表示されないことを注意してください。

```

nsxedge> show service loadbalancer table
-----
L7 Loadbalancer Sticky Table Status:

TABLE      TYPE      SIZE(BYTE)  USED(BYTE)

```

- 6 必要なすべてのサービスが正しく実行されたら、ルーティング テーブルで、クライアント向けとサーバ向けのルートが必要であることを確認します。ルートをインターフェイスにマッピングする `show ip route` コマンドと `show ip forwarding` コマンドを使用します。

```

NSX-edge-8-0> sh ip route

Codes: O - OSPF derived, i - IS-IS derived, B - BGP derived,
C - connected, S - static, L1 - IS-IS level-1, L2 - IS-IS level-2,
IA - OSPF inter area, E1 - OSPF external type 1, E2 - OSPF external type 2,
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

Total number of routes: 4

S      0.0.0.0/0          [1/1]          via 192.168.8.2
C      10.10.10.0/24      [0/0]          via 10.10.10.1
C      169.254.1.4/30     [0/0]          via 169.254.1.5
C      192.168.8.0/24     [0/0]          via 192.168.8.3
NSX-edge-8-0> sh ip forwarding
Codes: C - connected, R - remote,
      > - selected route, * - FIB route

R>* 0.0.0.0/0 via 192.168.8.2, vNic_2
C>* 10.10.10.0/24 is directly connected, vNic_0
C>* 169.254.1.4/30 is directly connected, vNic_0
C>* 192.168.8.0/24 is directly connected, vNic_2
NSX-edge-8-0>

```

- 7 `show arp` コマンドを使用して、システム（ゲートウェイやネクスト ホップなど）およびバックエンド サーバの ARP エントリがあることを確認します。

```

OneArm-LoadBalancer-01-0> show arp
-----
vShield Edge ARP Cache:
IP Address                Interface  MAC Address      State
fe80::250:56ff:feae:f86b  vNic_0    00:50:56:ae:f8:6b STALE
fe80::250:56ff:feae:5066  vNic_1    00:50:56:ae:50:66 STALE
fe80::250:56ff:feae:3e3d  vNic_0    00:50:56:ae:3e:3d STALE
172.16.100.11             vNic_1    00:50:56:ae:50:66 REACHABLE
172.16.10.1               vNic_0    02:50:56:56:44:52 REACHABLE
172.16.10.11             vNic_0    00:50:56:ae:3e:3d REACHABLE
OneArm-LoadBalancer-01-0>

```

- 8 ログは、問題の診断につながる可能性のあるトラフィックを特定するのに役立つ情報を提供します。トラフィックの特定に役立つテール ログを作成するには、`show log` コマンドまたは `show log follow` コマンドを使用します。ロード バランサは、[ログ (Logging)] を有効にして [情報 (Info)] または [デバッグ (Debug)] を設定した状態で実行する必要があります。

```

nsxedge> show log
2016-04-20T20:15:36+00:00 vShieldEdge kernel: Initializing cgroup subsys cpuset
2016-04-20T20:15:36+00:00 vShieldEdge kernel: Initializing cgroup subsys cpu
2016-04-20T20:15:36+00:00 vShieldEdge kernel: Initializing cgroup subsys cpuacct
...

```

- 9 クライアントへの正しいパスを指定した状態で、基本サービスが実行中であることを確認したら、アプリケーション層の状況を確認します。ロード バランサ エンジンのステータス (L4/L7) を確認するには、`show service loadbalancer pool` コマンドを使用します。コンテンツの提供に必要なプール メンバーは 1 つのみですが、通常は要求が単一ワークロードで対処できるキャパシティを超えるため、複数のメンバーが必要になります。組み込みの健全性チェックが健全性監視機能を提供する場合、健全性チェックに失敗すると、出力にステータスの最終変更時間と失敗した理由が表示されます。監視サービスが健全性監視を備えている場合は、上述の 2 つの出力に加え、最終チェック時間も表示されます。

```
nsxedge> show service loadbalancer pool

-----
Loadbalancer Pool Statistics:

POOL Web-Tier-Pool-01
| LB METHOD round-robin
| LB PROTOCOL L7
| Transparent disabled
| SESSION (cur, max, total) = (0, 0, 0)
| BYTES in = (0), out = (0)
+-->POOL MEMBER: Web-Tier-Pool-01/web-01a, STATUS: UP
| | HEALTH MONITOR = BUILT-IN, default_https_monitor:L7OK
| | | LAST STATE CHANGE: 2016-05-16 07:02:00
| | SESSION (cur, max, total) = (0, 0, 0)
| | BYTES in = (0), out = (0)
+-->POOL MEMBER: Web-Tier-Pool-01/web-02a, STATUS: UP
| | HEALTH MONITOR = BUILT-IN, default_https_monitor:L7OK
| | | LAST STATE CHANGE: 2016-05-16 07:02:01
| | SESSION (cur, max, total) = (0, 0, 0)
| | BYTES in = (0), out = (0)
```

- 10 サービス モニターのステータス (OK、警告、重大) を確認し、設定済みのすべてのバックエンド サーバの健全性を確認します。

```
nsxedge> show service loadbalancer monitor

-----
Loadbalancer Health Check Statistics:

MONITOR PROVIDER    POOL          MEMBER        HEALTH STATUS
built-in            Web-Tier-Pool-01  web-01a      default_https_monitor:L7OK
built-in            Web-Tier-Pool-01  web-02a      default_https_monitor:L7OK
```

`show service load balancer monitor` コマンドの場合、CLI 出力に次の 3 種類の健全性監視の値が表示されます。

- Built-in : 健全性チェックは有効で、L7 エンジン (HA プロキシ) によって実行されます。
- Monitor Service : 健全性チェックは有効で、監視サービス エンジン (NAGIOS) によって実行されます。監視サービスの実行ステータスは、`show service monitor` と `show service monitor service` CLI コマンドで確認できます。[ステータス (Status)] フィールドには、OK、警告または重大が表示されます。
- Not Defined : 健全性チェックは無効です。

このコマンドの出力で最後に表示される列は、プール メンバーの健全性ステータスです。次のステータスが表示されます。

表 6-1. 健全性ステータスとその説明

健全性ステータス	説明
組み込み	<ul style="list-style-type: none"> <li>■ UNK : 不明</li> <li>■ INI : 初期化中</li> <li>■ SOCKERR : ソケット エラー</li> <li>■ L4OK : レイヤー 4 でチェックに合格 (上位レイヤーのテストなし)</li> <li>■ L4TOUT : レイヤー 1 ~ 4 のタイムアウト</li> <li>■ L4CON : レイヤー 1 ~ 4 の接続の問題。たとえば、接続が拒否された (tcp rst)、ホストへのルートがない (icmp) など</li> <li>■ L6OK : レイヤー 6 でチェックに合格</li> <li>■ L6TOUT : レイヤー 6 (SSL) のタイムアウト</li> <li>■ L6RSP : レイヤー 6 無効な応答 - プロトコル エラー。可能性のある原因 : <ul style="list-style-type: none"> <li>■ バックエンド サーバが「SSLv3」または「TLSv1.0」のみをサポートしている、</li> <li>■ バックエンド サーバの証明書が無効である、</li> <li>■ 暗号のネゴシエーションに失敗した、など。</li> </ul> </li> <li>■ L7OK : レイヤー 7 でチェックに合格</li> <li>■ L7OKC : レイヤー 7 で条件付きでチェックに合格たとえば、「disable-on-404」を返す 404。</li> <li>■ L7TOUT : レイヤー 7 (HTTP/SMTP) のタイムアウト</li> <li>■ L7RSP : レイヤー 7 で無効な応答 - プロトコル エラー</li> <li>■ L7STS : レイヤー 7 の応答エラー。たとえば、HTTP 5xx。</li> </ul>
重大	<ul style="list-style-type: none"> <li>■ SSL プロトコル バージョン 2 が SSL ライブラリでサポートされていない</li> <li>■ サポート対象外の SSL プロトコル バージョン</li> <li>■ SSL コンテキストを作成できない</li> <li>■ SSL 接続を確立できない</li> <li>■ SSL ハンドシェイクを開始できない</li> <li>■ サーバ証明書を取得できない</li> <li>■ 証明書のサブジェクトを取得できない</li> <li>■ 証明書の時刻形式が間違っている</li> <li>■ 証明書「&lt;cn&gt;」が &lt;証明書の期限&gt; に期限切れ</li> <li>■ 証明書「&lt;cn&gt;」が今日の &lt;証明書の期限&gt; に期限切れ</li> </ul>
警告/重大	証明書「<cn>」が <証明書の残り日数/期限> で期限切れ

表 6-1. 健全性ステータスとその説明（続き）

健全性ステータス	説明
ICMP	<ul style="list-style-type: none"> <li>■ ネットワークに接続できない</li> <li>■ ホストに接続できない</li> <li>■ プロトコルに接続できない</li> <li>■ ポートに接続できない</li> <li>■ 送信元のルートに失敗した</li> <li>■ 送信元のホストが隔離された</li> <li>■ 不明なネットワーク</li> <li>■ 不明なホスト</li> <li>■ ネットワークが拒否された</li> <li>■ ホストが拒否された</li> <li>■ ネットワークのサービス タイプ (ToS) が不正</li> <li>■ ホストのサービス タイプ (ToS) が不正</li> <li>■ フィルタで禁止されている</li> <li>■ ホストの優先順位の違反</li> <li>■ 優先順位による遮断。処理に必要な最低限の優先順位</li> <li>■ 無効なコード</li> </ul>
UDP/TCP	<ul style="list-style-type: none"> <li>■ ソケットの作成に失敗</li> <li>■ アドレス xxxx、ポート xxx に接続：[Linux エラー コードを参照]</li> <li>■ ホストからデータを受信していない</li> <li>■ ホスト/ソケットからの予期しない応答を受信</li> </ul>
HTTP/HTTPS	<ul style="list-style-type: none"> <li>■ HTTP UNKNOWN： メモリ割り当てエラー</li> <li>■ HTTP CRITICAL： TCP ソケットを開くことができない（ソケットの作成またはサーバへの接続に失敗）</li> <li>■ HTTP CRITICAL： データの受信中にエラーが発生</li> <li>■ HTTP CRITICAL： ホストから受信したデータがない</li> <li>■ HTTP CRITICAL： ホストから無効な HTTP 応答を受信： &lt;ステータス行&gt;（ステータス行の形式が正しくない）</li> <li>■ HTTP CRITICAL： 無効なステータス行 &lt;ステータス行&gt;（ステータス コードが 3 桁 XXX でない）</li> <li>■ HTTP CRITICAL： 無効なステータス&lt;ステータス行&gt;（ステータス コード &gt;= 600 または &lt; 100）</li> <li>■ HTTP CRITICAL： 文字列が見つからない</li> <li>■ HTTP CRITICAL： パターンが見つからない</li> <li>■ HTTP WARNING： ページ サイズ &lt;page_length&gt; が大きすぎる</li> <li>■ HTTP WARNING： ページ サイズ &lt;page_length&gt; が小さすぎる</li> </ul>

- 11 エラー コードが L4TOUT/L4CON の場合、通常は、基盤となるネットワークで接続の問題が発生しています。これらの問題の根本原因の多くは Duplicate IP です。このエラーが発生した場合は、次のようにトラブルシューティングを行ってください。
- a 高可用性 (HA) が有効になっている場合は、Edge の高可用性ステータスを確認します。これは、両方の Edge で `show service highavailability` コマンドを使用することで行います。高可用性リンクが DOWN になっているかどうか、およびすべての Edge が Active かどうかを確認して、ネットワーク上で Edge IP アドレスが重複していないことを確認します。
  - b `show arp` コマンドを使用して Edge の ARP テーブルを確認し、バックエンド サーバの ARP エントリが 2 つの MAC アドレスの間で変更されていないかどうかを確認します。
  - c バックエンド サーバの ARP テーブルを確認するか、`arp-ping` コマンドを使用して、他のマシンが Edge IP アドレスと同じ IP アドレスを使用していないかどうかを確認します。
- 12 ロード バランサ オブジェクトの統計情報 (仮想 IP アドレス、プール、メンバー) を確認します。特定のプールに注目し、そのメンバーが実行中であることを確認します。透過モードが有効になっているかどうかを確認します。有効な場合、クライアントとサーバ間に `Edge Services Gateway` を配置する必要があります。サーバがセッション カウンタの増分を示しているかどうかを確認します。

```
nsxedge> show service loadbalancer pool Web-Tier-VIP-01
```

TIMESTAMP	SESSIONS	BYTESIN	BYTESOUT	SESSIONRATE	HTTPREQS
2016-04-27 19:56:40	00	00	00	00	00
2016-04-27 19:55:00	00	32	100	00	00

```
nsxedge> show service loadbalancer pool Web-Tier-VIP-01 | MEMBER
+-> POOL MEMBER: TENANT-1-TCP-POOL-80/SERVER-1, STATUS: UP
+-> POOL MEMBER: TENANT-1-TCP-POOL-80/SERVER-2, STATUS: UP
```

- 13 次に、仮想サーバにデフォルト プールがあるかどうかを確認し、そのプールもバインドされていることを確認します。アプリケーション ルールを介してプールを使用している場合は、`#show service loadbalancer pool` コマンドで表示される特定のプールに注意する必要があります。仮想サーバの名前を指定します。

```
nsxedge> show service loadbalancer virtual Web-Tier-VIP-01
```

```
-----
Loadbalancer VirtualServer Statistics:
```

```
VIRTUAL Web-Tier-VIP-01
| ADDRESS [172.16.10.10]:443
| SESSION (cur, max, total) = (0, 0, 0)
| RATE (cur, max, limit) = (0, 0, 0)
| BYTES in = (0), out = (0)
+->POOL Web-Tier-Pool-01
| LB METHOD round-robin
| LB PROTOCOL L7
| Transparent disabled
| SESSION (cur, max, total) = (0, 0, 0)
| BYTES in = (0), out = (0)
+->POOL MEMBER: Web-Tier-Pool-01/web-01a, STATUS: UP
```

```

| | HEALTH MONITOR = BUILT-IN, default_https_monitor:L7OK
| | | LAST STATE CHANGE: 2016-05-16 07:02:00
| | SESSION (cur, max, total) = (0, 0, 0)
| | BYTES in = (0), out = (0)
+-->POOL MEMBER: Web-Tier-Pool-01/web-02a, STATUS: UP
| | HEALTH MONITOR = BUILT-IN, default_https_monitor:L7OK
| | | LAST STATE CHANGE: 2016-05-16 07:02:01
| | SESSION (cur, max, total) = (0, 0, 0)
| | BYTES in = (0), out = (0)

```

- 14** すべてが正しく設定されているように見えてもまだエラーが発生する場合は、トラフィックをキャプチャして何が起きているかを理解する必要があります。クライアントから仮想サーバへの接続、および Edge Services Gateway からバックエンド プール（プール レベルの透過設定は有効または無効）への 2 種類の接続があります。#show ip forwarding コマンドで vNIC インターフェイスをリスト表示し、そのデータを使用します。

たとえば、クライアント コンピュータが vNic\_0 にあり、サーバが vNic\_1 にあるとします。クライアント IP アドレスの 192.168.1.2 と、仮想 IP アドレスの 192.168.2.2（ポート 80 で実行）を使用します。ロード バランサのインターフェイス IP アドレスは 192.168.3.1、バックエンド サーバの IP アドレスは 192.168.3.3 です。パケット キャプチャ コマンドには、パケットを表示するコマンドと、パケットをダウンロード用にファイルにキャプチャするコマンドの 2 種類があります。パケットをキャプチャしてロード バランサの障害を検出します。パケットは次の 2 つの方向でキャプチャできます。

- クライアントからのパケットをキャプチャする。
- バックエンド サーバに送信されたパケットをキャプチャする。

```

#debug packet capture interface interface-name [filter using _ for space]- creates a packet
capture file that you can download
#debug packet display interface interface-name [filter using _ for space]- outputs packet data to
the console
#debug show files - to see a list of packet capture
#debug copy scp user@url:path file-name/all - to download the packet capture

```

次はその例です。

- vNIC\_0 でキャプチャ : debug packet display interface vNic\_0
- すべてのインターフェイスでキャプチャ : debug packet display interface any
- フィルタを指定して vNIC\_0 でキャプチャ : debug packet display interface vNic\_0 host\_192.168.11.3\_and\_host\_192.168.11.41
- クライアントから仮想サーバへのトラフィックでのパケット キャプチャ : #debug packet display|capture interface vNic\_0 host\_192.168.1.2\_and\_host\_192.168.2.2\_and\_port\_80
- Edge Services Gateway とサーバ間でのパケット キャプチャ（プールが透過モードの場合） : #debug packet display|capture interface vNic\_1 host 192.168.1.2\_and\_host\_192.168.3.3\_and\_port\_80
- Edge Services Gateway とサーバ間でのパケット キャプチャ（プールが透過モードでない場合） : #debug packet display|capture interface vNic\_1 host 192.168.3.1\_and\_host\_192.168.3.3\_and\_port\_80

## 一般的なロード バランサの問題

ここでは、いくつかの問題と解決方法について説明します。

NSX のロード バランシングを使用するときに発生する一般的な問題は、次のとおりです。

- TCP ポート（ポート 443 など）でのロード バランシングが機能しない。
  - トポロジを確認します。詳細については、『NSX 管理ガイド』を参照してください。
  - ping コマンドを使用して仮想サーバの IP アドレスにつながるかを確認する、またはアップストリーム ルーターを調べて ARP テーブルが設定されていることを確認します。
  - [ロード バランサ設定の確認とユーザー インターフェイスを使用したトラブルシューティング](#)します。
  - [CLI を使用したロード バランサのトラブルシューティング](#)します。
  - パケットをキャプチャします。
- ロード バランシング プールのメンバーが使用されない。
  - サーバがプール内にあり、有効になっていることを確認し、健全性ステータスを監視します。
- Edge トラフィックのロード バランシングが行われない。
  - プールとセッション維持の設定を確認します。セッション維持が設定されており、使用しているクライアント数が少ないと、バックエンド プール メンバーへの接続が均等に分散しているように見えない場合があります。
- レイヤー 7 のロード バランシング エンジンが停止する。
- 健全性監視エンジンが停止する。
  - ロード バランサ サービスを有効にします。『NSX 管理ガイド』を参照してください。
- プール メンバー監視ステータスが警告/重大になる。
  - アプリケーション サーバがロード バランサからアクセス可能であることを確認します。
  - アプリケーション サーバのファイアウォールまたは分散ファイアウォール (DFW) がトラフィックを許可していることを確認します。
  - アプリケーション サーバが、指定された健全性検査に応答できることを確認します。
- プール メンバーのステータスが無効になる。
  - プール メンバーがプール設定で有効になっていることを確認します。
- レイヤー 7 スティックテーブルがスタンバイ Edge と同期されない。
  - 高可用性 (HA) が設定されていることを確認します。
- クライアント接続はあるが、アプリケーション トランザクションを完了できない。
  - アプリケーション プロファイルで適切なセッション維持が設定されていることを確認します。
  - アプリケーションがプール内の 1 台のサーバ（2 台ではない）に対してのみ動作している場合、最も可能性が高いのはセッション維持の問題です。



## 基本的なトラブルシューティング

- 1 vSphere Web Client でロード バランサ設定のステータスを確認します。
  - a [ネットワークとセキュリティ(Networking & Security)] > [NSX Edge] をクリックします。
  - b NSX Edge をダブルクリックします。
  - c [管理 (Manage)] をクリックして、[ロード バランサ (Load Balancer)] タブをクリックします。
  - d ロード バランサのステータスおよび設定されているログ レベルを確認します。
- 2 ロード バランサ サービスのトラブルシューティングを実行する前に、NSX Manager で次のコマンドを実行して、サービスが稼動していることを確認します。

```
nsxmgr> show edge edge-4 service loadbalancer
haIndex:          0
-----
Loadbalancer Services Status:

L7 Loadbalancer      : running
-----
L7 Loadbalancer Statistics:
STATUS      PID      MAX_MEM_MB  MAX SOCK   MAX_CONN   MAX_PIPE   CUR_CONN   CONN_RATE
CONN_RATE_LIMIT MAX_CONN_RATE
running     1580      0           2081       1024        0           0           0
0            0
-----
L4 Loadbalancer Statistics:
MAX_CONN   ACT_CONN   INACT_CONN  TOTAL_CONN
0           0           0            0
-----
Prot LocalAddress:Port Scheduler Flags
-> RemoteAddress:Port      Forward Weight ActiveConn InActConn
```

**注：** show edge all を実行すると、NSX Edge の名前を検索できます。

## 設定の問題のトラブルシューティング

ロード バランサの設定操作が NSX ユーザー インターフェイスまたは REST API 呼び出しにより拒否されると、設定の問題として分類されます。

## データ プレーンの問題のトラブルシューティング

ロード バランサの設定は NSX Manager で受け入れられますが、クライアント、Edge ロード バランサ、およびサーバー間に接続またはパフォーマンスに問題があります。データ プレーンの問題には、ロード バランサのランタイム CLI の問題とロード バランサのシステム イベントの問題が含まれます。

- 1 次の REST API 呼び出しを使用して、NSX Manager での Edge のログ レベルを INFO から TRACE または DEBUG に変更します。

```
URL: https://NSX_Manager_IP/api/1.0/services/debug/loglevel/com.vmware.vshield.edge?level=TRACE
Method: POST
```

- 2 vSphere Web Client でプール メンバーのステータスを確認します。
  - a [ネットワークとセキュリティ(Networking & Security)] > [NSX Edge] をクリックします。
  - b NSX Edge をダブルクリックします。
  - c [管理 (Manage)] をクリックして、[ロード バランサ (Load Balancer)] タブをクリックします。
  - d 設定されたロード バランサ プールのサマリを表示するには、[プール (Pools)] をクリックします。
  - e ロード バランサ プールを選択します。[プール統計の表示 (Show Pool Statistics)] をクリックして、プールが稼動していることを確認します。
- 3 次の REST API 呼び出しを使用して、NSX Manager からさらに詳細なロード バランサ プールの設定の統計を取得できます。

```
URL: https://NSX_Manager_IP/api/4.0/edges/{edgeId}/loadbalancer/statistics
Method: GET
```

```
<?xml version="1.0" encoding="UTF-8"?>
<loadBalancerStatusAndStats>
  <timeStamp>1463507779</timeStamp>
  <pool>
    <poolId>pool-1</poolId>
    <name>Web-Tier-Pool-01</name>
    <member>
      <memberId>member-1</memberId>
      <name>web-01a</name>
      <ipAddress>172.16.10.11</ipAddress>
      <status>UP</status>
      <lastStateChangeTime>2016-05-16 07:02:00</lastStateChangeTime>
      <bytesIn>0</bytesIn>
      <bytesOut>0</bytesOut>
      <curSessions>0</curSessions>
      <httpReqTotal>0</httpReqTotal>
      <httpReqRate>0</httpReqRate>
      <httpReqRateMax>0</httpReqRateMax>
      <maxSessions>0</maxSessions>
      <rate>0</rate>
      <rateLimit>0</rateLimit>
      <rateMax>0</rateMax>
```

```

        <totalSessions>0</totalSessions>
    </member>
    <member>
        <memberId>member-2</memberId>
        <name>web-02a</name>
        <ipAddress>172.16.10.12</ipAddress>
        <status>UP</status>
        <lastStateChangeTime>2016-05-16 07:02:01</lastStateChangeTime>
        <bytesIn>0</bytesIn>
        <bytesOut>0</bytesOut>
        <curSessions>0</curSessions>
        <httpReqTotal>0</httpReqTotal>
        <httpReqRate>0</httpReqRate>
        <httpReqRateMax>0</httpReqRateMax>
        <maxSessions>0</maxSessions>
        <rate>0</rate>
        <rateLimit>0</rateLimit>
        <rateMax>0</rateMax>
        <totalSessions>0</totalSessions>
    </member>
    <status>UP</status>
    <bytesIn>0</bytesIn>
    <bytesOut>0</bytesOut>
    <curSessions>0</curSessions>
    <httpReqTotal>0</httpReqTotal>
    <httpReqRate>0</httpReqRate>
    <httpReqRateMax>0</httpReqRateMax>
    <maxSessions>0</maxSessions>
    <rate>0</rate>
    <rateLimit>0</rateLimit>
    <rateMax>0</rateMax>
    <totalSessions>0</totalSessions>
</pool>
<virtualServer>
    <virtualServerId>virtualServer-1</virtualServerId>
    <name>Web-Tier-VIP-01</name>
    <ipAddress>172.16.10.10</ipAddress>
    <status>OPEN</status>
    <bytesIn>0</bytesIn>
    <bytesOut>0</bytesOut>
    <curSessions>0</curSessions>
    <httpReqTotal>0</httpReqTotal>
    <httpReqRate>0</httpReqRate>
    <httpReqRateMax>0</httpReqRateMax>
    <maxSessions>0</maxSessions>
    <rate>0</rate>
    <rateLimit>0</rateLimit>
    <rateMax>0</rateMax>
    <totalSessions>0</totalSessions>
</virtualServer>
</loadBalancerStatusAndStats>

```

- 4 ロード バランサの統計情報をコマンド ラインから確認するため、NSX Edge で次のコマンドを実行します。

特定の仮想サーバを対象とする場合は、最初に `show service loadbalancer virtual` を実行して仮想サーバ名を取得します。次に `show statistics loadbalancer virtual <virtual-server-name>` を実行します。

特定の TCP プールを対象とする場合は、最初に `show service loadbalancer pool` を実行してプール名を取得します。次に `show statistics loadbalancer pool <pool-name>` を実行します。

- 5 ロード バランサの統計に障害の兆候が示されていないかどうかを確認します。

# Virtual Private Network (VPN) の トラブルシューティング

## 7

NSX Edge では複数のタイプの VPN をサポートします。ここでは、L2 VPN と SSL VPN の問題をトラブルシューティングする方法を説明します。

この章には、次のトピックが含まれています。

- [L2 VPN](#)
- [SSL VPN](#)
- [IPsec VPN](#)

## L2 VPN

L2 VPN では、SSL VPN 内のトンネリングによって、L3 境界を超えて複数の論理 L2 ネットワーク（VLAN と VXLAN の両方）を拡張できます。また、L2 VPN サーバに複数のサイトを設定できます。L2 VPN では、SSL VPN 内のトンネリングによって、L3 境界を超えて複数の論理 L2 ネットワーク（VLAN と VXLAN の両方）を拡張できます。サイトに NSX を導入しなくても、スタンドアロンの Edge をリモート サイトにデプロイすることが可能です。出力方向（Egress）の最適化機能により、Edge は出力方向を最適化した IP アドレスに送信されるすべてのパケットをローカルでルーティングし、その他すべてをブリッジすることができます。

企業は L2 VPN を使用して、VXLAN または VLAN によってバックアップされたワークロードを、物理的に離れた場所にシームレスに移行できるようになります。また、L2 VPN は、クラウド プロバイダに対しては、ワークロードやアプリケーションの既存の IP アドレスを変更せずに、各テナントのオンボードを行うためのメカニズムを提供します。

## L2 VPN の一般的な設定の問題

このトピックでは、L2 VPN に関連する一般的な設定の問題について説明します。

### 問題

一般的な設定の問題には次のものがあります。

- L2 VPN クライアントは設定されているが、宛先ポート 443 経由でトンネルを通過するトラフィックが、インターネットに接するファイアウォールで許可されない。
- L2 VPN クライアントがサーバ証明書を検証するように設定されているが、正しい CA 証明書または FQDN が設定されていない。

- L2 VPN サーバが設定されているが、インターネットに接するファイアウォールで NAT またはファイアウォール ルールが作成されていない。
- トランク インターフェイスが分散ポート グループまたは標準ポート グループでバックアップされていない。

**注：** デフォルトでは、L2 VPN サーバはポート 443 で待機します。このポートは L2 VPN サーバ設定で指定します。

デフォルトでは、L2 VPN クライアントはポート 443 を使用して外部との接続を行います。このポートは L2 VPN クライアント設定で指定できます。

#### 解決方法

- 1 L2 VPN サーバ プロセスが実行中かどうかを確認します。
  - a NSX Edge 仮想マシンにログインします。
  - b `show process monitor` コマンドを実行し、*l2vpn* という名前のプロセスが見つかるかどうかを確認します。
  - c `show service network-connections` コマンドを実行し、*l2vpn* プロセスがポート 443 で待機しているかどうかを確認します。
- 2 L2 VPN クライアント プロセスが実行中かどうかを確認します。
  - a NSX Edge 仮想マシンにログインします。
  - b `show process monitor` コマンドを実行し、*naclientd* という名前のプロセスが見つかるかどうかを確認します。
  - c `show service network-connections` コマンドを実行し、*naclientd* プロセスがポート 443 で待機しているかどうかを確認します。
- 3 インターネットから L2 VPN サーバにアクセスできるかどうかを確認します。
  - a ブラウザを開き、**https://<l2vpn-public-ip>** に移動します。
  - b ポータルのログイン ページが表示されます。ポータル ページは、インターネット経由で L2 VPN サーバに接続されると表示されます。
- 4 トランク インターフェイスが分散ポート グループまたは標準ポート グループでバックアップされているかどうかを確認します。
  - a トランク インターフェイスが分散ポート グループでバックアップされている場合は、シンク ポートが自動的に設定されます。
  - b トランク インターフェイスが標準ポート グループでバックアップされている場合は、次のように vSphere Distributed Switch を手動で設定する必要があります。
    - ポートを [無差別 (promiscuous)] モードに設定します。
    - [偽装転送 (Forged Transmits)] を [許可 (Accept)] に設定します。

## 5 L2 VPN のルーピング問題を最小にします。

- a NIC チーミングが正しく設定されていないと、MAC フラッピングとパケットの重複という 2 つの重大な問題が発生します。ルーピングを軽減するための L2VPN のオプションで説明する設定を確認してください。

## 6 L2 VPN を使用する仮想マシンが互いに通信できるかどうかを確認します。

- a L2 VPN サーバの CLI にログインし、対応するタップ インターフェイス debug packet capture interface name でパケットをキャプチャします。
- b L2 VPN クライアントにログインし、対応するタップ インターフェイス debug packet capture interface name でパケットをキャプチャします。
- c これらのキャプチャを分析して、ARP が解決されていること、およびデータトラフィックが流れていることを確認します。
- d Allow Forged Transmits: dvSwitch プロパティが L2 VPN trunk port に設定されていることを確認します。
- e シンクポートが L2 VPN trunk port に設定されていることを確認します。これを実行するには、ホストにログインして net-dvs -l コマンドを発行します。シンクプロパティセットで L2 VPN エッジ内部ポート (com.vmware.etherswitch.port.extraEthFRP = SINK) を確認します。内部ポートは、NSX Edge トランクの接続先である dvPort ポートを参照します。

net-dvs -l

ESXi

```
port 939:
  com.vmware.common.port.alias = , propType = CONFIG
  com.vmware.common.port.connectid = 323234212 , propType = CONFIG
  com.vmware.common.port.portgroupid = dvportgroup-181 , propType = CONFIG
  com.vmware.common.port.block = false , propType = CONFIG
  com.vmware.common.port.dvfilter = filters (num = 0):
    propType = CONFIG
  com.vmware.common.port.ptAllowed = 0x 0. 0. 0. 0
    propType = CONFIG
  com.vmware.etherswitch.port.txUplink = normal , propType = CONFIG
  com.vmware.common.port.volatility.persist = /vmfs/volumes/9ec6ae8b-38b8e621/.dvsData/ic ec 0e 50 02 9c a9 21-b6 d8
  fc 73 e5 79 69/939 , propType = CONFIG
  com.vmware.common.port.ptAllowedRT = 0x 0. 0. 0. 0
    propType = RUNTIME
  com.vmware.net.vxlan.trunkofg = 0x63.6f.6e.66.69.67.56.65.72.73.69.6f.6e.3d.30.2e.31.3b.61.6c.6c.6f.77.47.75.65.7
  74.56.6c.61.6e.3d.30.3b.6e.75.6d.54.72.75.6e.6b.4d.65.6d.62.65.72.73.3d.31.3b.74.72.75.6e.6b.4d.65.6d.5f.30.5f.43.70.45.6e.61.62.
  .65.64.3d.31.3b.74.72.75.6e.6b.4d.65.6d.5f.30.5f.56.6e.69.3d.35.30.30.31.3b.74.72.75.6e.6b.4d.65.6d.5f.30.5f.4d.63.61.73.74.49.70
  d.30.2e.30.2e.30.2e.31.3b
    propType = CONFIG POLICY
  com.vmware.etherswitch.port.extraEthFRP = SINK
    propType = CONFIG POLICY
  com.vmware.etherswitch.port.teaming:
    load balancing = first uplink (i.e. explicit)
    link selection = link state up;
    link behavior = notify switch; best effort on failure; shotgun on failure;
    active = dvUplink1;
    standby =
    propType = CONFIG
  com.vmware.etherswitch.port.security = deny promiscuous; deny mac change; allow forged frames
    propType = CONFIG
  com.vmware.etherswitch.port.vlan = Guest VLAN tagging
    ranges = 0
    propType = CONFIG
  com.vmware.common.port.statistics:
    pktsInUnicast = 0
    bytesInUnicast = 0
    pktsInMulticast = 6
    bytesInMulticast = 620
```

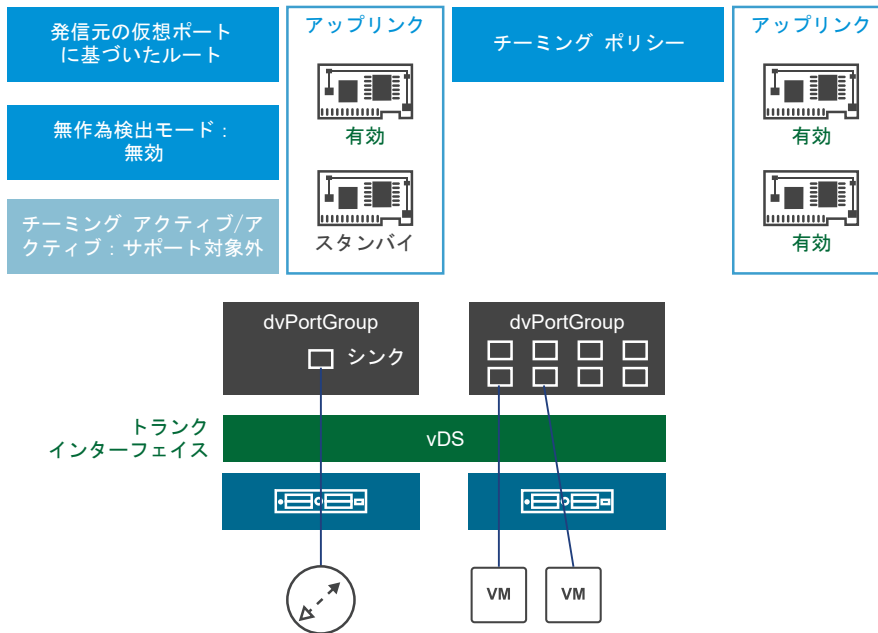
Sink port should be enabled for the dvPort where the Edge trunk is connected to

## ルーピングを軽減するための L2VPN のオプション

ルーピングを軽減するには、2つのオプションがあります。NSX Edge と仮想マシンを別々の ESXi ホストに配置するか、NSX Edge と仮想マシンを同じ ESXi ホストに配置するかです。

オプション 1：L2VPN Edge と仮想マシンを異なる ESXi ホストに配置する場合

### 1. 個別の ESXi ホストでの L2VPN Edge と仮想マシンの展開



- Edge と仮想マシンを個別の ESXi ホストでデプロイします。
- Edge の トランク vNIC に関連付けられた分散ポート グループのチーミングおよびフェイルオーバー ポリシーを次のように設定します。
  - 「発信元の仮想ポートに基づいたルート」で、ロード バランシングを行います。
  - 1つのアップリンクのみをアクティブとして、他のアップリンクをスタンバイとして設定します。
- 仮想マシンに関連付けられた分散ポート グループのチーミングおよびフェイルオーバー ポリシーを次のように設定します。
  - 任意のチーミング ポリシーを使用できます。
  - 複数のアクティブ アップリンクを設定できます。



4 シンク ポート モードを使用して トランク vNIC で無差別モードを無効にするように Edge を設定します。

**注：**

- vSphere Distributed Switch を使用している場合は、無差別モードを無効にします。
- 仮想スイッチを使用してトランク インターフェイスを設定している場合は、無差別モードを有効にします。

仮想スイッチで無差別モードが有効になっている場合は、無差別ポートが使用していないアップリンクから送信されるパケットの一部が破棄されません。使用していないアップリンクから無差別ポートに送信されるすべてのパケットを明示的に破棄するには、ReversePathFwdCheckPromisc を有効にしてから無効にする必要があります。

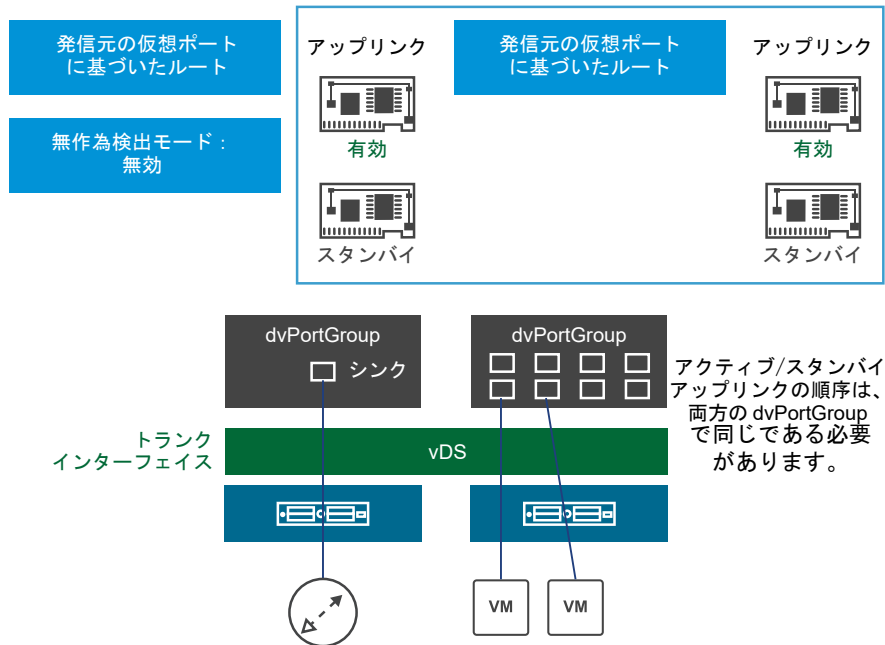
重複するパケットをブロックするには、NSX Edge が配置された ESXi の CLI から無差別モードの RPF チェックを有効にします。

```
esxcli system settings advanced set -o /Net/ReversePathFwdCheckPromisc -i 1
esxcli system settings advanced list -o /Net/ReversePathFwdCheckPromisc
Path: /Net/ReversePathFwdCheckPromisc
Type: integer
Int Value: 1
Default Int Value: 0
Max Value: 1
Min Value: 0
String Value:
Default String Value:
Valid Characters:
Description: Block duplicate packet in a teamed environment when the virtual switch is set to
Promiscuous mode.
```

[ポート グループ (PortGroup)] セキュリティ ポリシーで、[無差別モード (PromiscuousMode)] を [許可 (Accept)] から [拒否 (Reject)] に変更し、再度 [許可 (Accept)] に戻して、設定済みの変更を有効にします。

- オプション 2 : Edge と仮想マシンを同じ ESXi ホストに配置する場合

## 2.同じホストでの L2VPN Edge と仮想マシンの展開



- a Edge の トランク vNIC に関連付けられた分散ポート グループのチーミングおよびフェイルオーバー ポリシーを次のように設定します。
  - 1 「発信元の仮想ポートに基づいたルート」で、ロード バランシングを行います。
  - 2 1 つのアップリンクをアクティブとして、他のアップリンクをスタンバイとして設定します。
- b 仮想マシンに関連付けられた分散ポート グループのチーミングおよびフェイルオーバー ポリシーを次のように設定します。
  - 1 任意のチーミング ポリシーを使用できます。
  - 2 アクティブにできるアップリンクは 1 つだけです。
  - 3 アクティブ/スタンバイのアップリンクの順序は仮想マシンの分散ポート グループおよび Edge の トランク vNIC 分散ポート グループと同じである必要があります。
- c シンク ポート モードを使用するようにクライアント側のスタンドアローン Edge を設定し、トランク vNIC 上で無差別モードを無効にします。

## CLI を使用したトラブルシューティング

NSX コマンド ライン インターフェイス (CLI) を使用すると、L2 VPN の一部の問題のトラブルシューティングを実行できます。

## 問題

L2 VPN を期待どおりに実行できない。

## 解決方法

- 1 次の集中管理 CLI コマンドを使用して、設定の問題を確認します。

```
show edge <edgeID> configuration l2vpn.
```

たとえば、`show edge edge-1 configuration l2vpn.` を実行します。

- 2 クライアントとサーバの両方の Edge で次のコマンドを使用します。

- `show configuration l2vpn` - 次の 4 つのキー値をチェックして、サーバを確認します。

```

show configuration l2vpn

vShield Edge L2 VPN Config:
{
  "l2vpn" : {
    "cipher" : {
      "RC4-MD5"
    },
    "listenerPort" : 443,
    "clientVnicIndex" : null,
    "filters" : [],
    "serverPort" : null,
    "caCertificate" : null,
    "peerSiteAlgorithm" : null,
    "listenerIp" : "192.168.100.3",
    "peerSites" : [
      {
        "vseVnicNames" : [
          "vNic_10"
        ],
        "name" : "L2VPN-Site1",
        "filters" : [],
        "l2vpnUser" : {
          "password" : "*****",
          "userId" : "vpnuser1"
        }
      }
    ],
    "clientProxySetting" : null,
    "enable" : true,
    "trunkedVnicIndexes" : [
      2
    ],
    "serverVnicIndex" : null,
    "l2vpnUsers" : [],
    "serverAddress" : null,
    "logging" : {
      "enable" : false,
      "logLevel" : "info"
    },
    "vseVnicNames" : null,
    "serverCertificate" : null
  }
}
  
```

Cipher

Port

Server IP

Peer Site Configuration

- `show service l2vpn bridge` - インターフェイスの数は、L2 VPN クライアントの数に応じて変わります。次の出力では、1 つの L2 VPN クライアント (na1) が設定されています。Port1 は、`vNic_2` を示します。MAC アドレス 02:50:56:56:44:52 は `vNic_2` インターフェイスで特定されており、Edge (L2 VPN サーバ) に対してローカルではありません。次の例の 3 行目は、`na1` インターフェイスを示します。

```
plr01-0> show service l2vpn bridge
```

bridge name	bridge id	STP enabled	interfaces
br-sub	8000.0050568e19fb	no	vNic_2 na1

List of learned MAC addresses for L2 VPN bridge br-sub

port	no	mac addr	is local?	vlanid	ageing timer
1		00:50:56:8e:19:fb	yes	0	0.00
1		02:50:56:56:44:52	no	1	0.87
2		2a:56:30:31:7e:3b	yes	0	0.00

- show service l2vpn trunk table
- show service l2vpn conversion table - 次の例では、トンネル #1 に到着したイーサネット フレームの VLAN ID #1 が、パケットが vSphere Distributed Switch (vDS) に渡される前に、VLAN #5001 の VXLAN に変換されます。

```
plr01-0> show service l2vpn conversion-table
```

TunnelId	VLAN/VNI	Type
1	5001	VXLAN

vNIC#	Name	Network	VLAN / VNI	Tunnel ID	Status
10	Subint-to-W...	Web-Tier-01	5001	1	✓

- show process monitor - l2vpn プロセス（サーバ）と naclientd プロセス（クライアント）が実行中かどうかを確認します。
- show service network-connections - l2vpn プロセス（サーバ）と naclientd プロセス（クライアント）がポート 443 で待機中かどうかを確認します。

## SSL VPN

この情報は、セットアップのトラブルシューティングに利用できます。

### SSL VPN Web ポータルを開くことができない

SSL VPN ユーザーが SSL VPN Web ポータルのログイン ページを開くことができません。このため、SSL VPN-Plus Client インストール パッケージをダウンロードしてインストールできません。

#### 問題

SSL VPN Web ポータルのログイン ページが開かないか、システムのブラウザでページが正しく表示されません。

## 原因

この問題の原因としては、次のいずれかが考えられます。

- サポートされていないバージョンのブラウザ が使用されている。
- ブラウザで Cookie と JavaScript が有効になっていない。

## 解決方法

- 1 サポート対象の次のいずれかのブラウザで SSL VPN Web ポータルのログイン ページを開きます。

ブラウザ	サポートされる最小バージョン
Internet Explorer	9.0.8112.16421
Chrome	67.03396
Safari	10.x

- 2 ブラウザの設定を開き、Cookie と JavaScript が有効になっていることを確認します。
- 3 ブラウザの言語が英語に設定されていない場合、言語を英語に設定して、問題が解決したかどうか確認します。
- 4 SSL VPN サーバで AES 暗号を選択しているかどうかを確認します。一部のブラウザは、AES 暗号化をサポートしていません。

## SSL VPN-Plus：インストールの失敗

このトピックでは、SSL VPN-Plus Client 固有のインストールの問題を特定し、解決する方法について説明します。

### 問題

SSL VPN-Plus Client のインストールに関連する一般的な問題は次のとおりです。

- SSL VPN-Plus Client は正常にインストールされているが、クライアントが機能しない。
- Mac マシンでカーネル拡張機能の警告メッセージが表示される。
- Mac OS High Sierra で、次のインストール エラー メッセージが表示される。

```
/opt/sslvpn-plus/naclient/signed_kext/tap.kext failed to load - (libkern/kext)system policy
prevents
loading; check the system/kernel logs for errors or try kextutil(8).
Error: Could not load /opt/sslvpn-plus/naclient/signed_kext/tap.kext
```

```
installer[4571] <Debug>: install:didFailWithError:Error Domain=
PKInstallErrorDomain Code=112 "An error occurred while running scripts from the package
"naclient.pkg".
" UserInfo={NSFilePath=./postinstall,NSURL=file:///<pathtofile>/
naclient.pkg,PKInstallPackageIdentifier=
com.vmware.sslvpn,NSLocalizedString=An error occurred while running scripts from the
package "naclient.pkg".}

installer[4571] <Error>: Install failed: The Installer encountered an error that caused the
```

```
installation to fail. Contact the software manufacturer for assistance.
installer: The install failed (The Installer encountered an error that caused the installation to
fail.
Contact the software manufacturer for assistance.)
```

- Windows マシンで、ドライバのインストールに失敗しました。原因: E000024B。マシンを再起動してください。というエラーメッセージが表示される。

## 原因

コンピュータに正常にインストールされていても、次のいずれかの理由により SSL VPN-Plus Client でエラーが発生する場合があります。

- 構成ファイル (naclient.cfg) が存在しないか、無効になっている。
- ディレクトリ権限またはユーザー権限が正しくない。
- SSL VPN サーバにアクセスできない。
- Mac または Linux マシンで、タップ ドライバがロードされていない。

Mac マシンで、システムがカーネル拡張機能のロードをブロックすると、カーネル拡張機能の警告メッセージが表示されます。

Mac OS High Sierra の Mac マシンで kext が許可されていないと、インストール エラーが表示されます。また、kext のロードを指示するプロンプトも表示されません。

Edge SSL VPN-Plus Client インストーラで [SSL クライアント ネットワーク アダプタを非表示にする (Hide SSL client network adapter)] オプションを有効にしていると、Windows マシンにドライバのインストール エラー (E000024B) が表示されます。

## 解決方法

- 1 サポートされるオペレーティング システムに SSL VPN-Plus Client をインストールしていることを確認します。サポートされるオペレーティング システムの詳細については、『NSX 管理ガイド』の「SSL VPN-Plus の概要」を参照してください。
- 2 Windows マシンで、SSL VPN-Plus Client をインストールするユーザーに管理者権限が付与されていることを確認します。Mac または Linux マシンに SSL VPN-Plus Client をインストールするには、root 権限が必要です。また、Mac マシンで SSL VPN-Plus Client を正常に起動し、実行するには、usr/local/lib ディレクトリに execute 権限が必要です。
- 3 Linux マシンで、次のライブラリがインストールされていることを確認します。ユーザー インターフェイス (UI) を使用するには、これらのライブラリが必要です。
  - TCL
  - TK
  - NSS

- 4 Mac または Linux マシンにタップ ドライバがロードされていない場合は、シェル スクリプトを実行してドライバをロードします。

オペレーティング システム	説明
Mac	sudo 権限を使用して、/opt/sslvpn-plus/naclient/ ディレクトリから Naclient.sh シェル スクリプトを実行します。
Linux	sudo 権限を使用して、naclient.sh シェル スクリプトを実行します。このスクリプトは、linux_phat_client/linux_phat_client ディレクトリにあります。

- 5 macOS High Sierra 以降のマシンに表示されるカーネル拡張機能の警告メッセージの問題を解決するには、ユーザーの承認を明示的に行い、カーネル拡張機能 (kext) をロードする必要があります。次の操作を行います。
- Mac マシンで、[システム環境設定 (System Preferences)] - [セキュリティとプライバシー (Security & Privacy)] ウィンドウの順に開きます。
  - ウィンドウの下部に、「一部のシステム ソフトウェアの読み込みがブロックされました」というメッセージが表示されています。[許可] ボタンをクリックします。
  - インストールを続行するには、[許可 (Allow)] をクリックします。  
ユーザー承認を行い、カーネル拡張機能をロードする方法については、[https://developer.apple.com/library/content/technotes/tn2459/\\_index.html](https://developer.apple.com/library/content/technotes/tn2459/_index.html) を参照してください。
  - カーネル拡張機能のロード中に、SSL VPN-Plus Client のインストール プロセスがバックグラウンドで実行されます。SSL VPN-Plus Client のインストール後、次のエラー メッセージが表示されます。インストールに失敗しました。インストーラでエラーが発生し、インストールに失敗しました。ソフトウェアの製造元に問い合わせください。
  - このエラーを解決するには、SSL VPN-Plus Client をアンインストールして、再度インストールを行います。

## 6 Mac OS High Sierra でインストール エラー メッセージの問題を解決するには、次の操作を行います。

- a 通知が有効になっていることを確認します。[システム環境設定 (System Preferences)] - [セキュリティとプライバシー (Security & Privacy)] - [通知を許可 (Allow Notifications)] の順に移動します。

**注：** Mac OS High Sierra に初めて SSL VPN-Plus Client をインストールする場合は通知ウィンドウが開き、インストールを許可するよう求められます。通常、この通知は 30 分間有効です。[許可 (Allow)] をクリックする前に通知が消えた場合は、マシンを再起動して、SSL VPN-Plus Client を再インストールします。

システムでカーネル拡張機能 (kext) が許可されていない場合、ユーザーが kext のロードを許可するメッセージが表示されず、再インストールに失敗します。残りの手順を完了して、`tuntap kext team id` を kext の事前承認リストに追加します。

- b Mac マシンをリカバリ モードで再起動します。
  - 1 画面左上にある Apple のロゴをクリックします。
  - 2 [再起動 (Restart)] をクリックします。
  - 3 すぐに Command キーと R キーを同時に押します。Apple のロゴまたは回転する地球儀が表示されるまで押し続けてください。Mac マシンに組み込みのリカバリ システムで起動できず、インターネットに接続して macOS のリカバリを試みる場合、回転する地球儀が表示されます。Mac がリカバリ モードで起動します。
- c 上部のメニューで、[ユーティリティ (Utilities)] - [ターミナル (Terminal)] の順にクリックします。
- d `tuntap kext team id` を kext の事前承認リストに追加するには、`- spctl kext-consent add KS8XL6T9FZ` コマンドを実行します。
- e Mac マシンを通常モードで再起動します。
- f kext の事前承認リストに team-id が表示されているかどうか確認するには、`- spctl kext-consent list` コマンドを実行します。
- g SSL VPN-Plus Client パッケージをインストールします。

- 7 Windows マシンでドライバのインストール失敗エラー (E00024B) が発生した場合は、Edge SSL VPN-Plus Client インストーラで [SSL クライアント ネットワーク アダプタを非表示にする (Hide SSL client network adapter)] オプションを無効にします。このオプションを無効にする手順については、VMware ナレッジベースの記事 <https://kb.vmware.com/s/article/2108766> を参照してください。

## SSL VPN-Plus : 通信の問題

このトピックでは、SSL VPN 接続とデータパスの問題を特定し、解決する方法について説明します。

### 問題

SSL VPN 接続とデータ パスに関連する一般的な問題は次のとおりです。

- SSL VPN-Plus Client が SSL VPN サーバに接続できない。
- SSL VPN-Plus Client がインストールされているが、SSL VPN-Plus サービスが実行されない。



- ログイン ユーザー数が上限に達した。SSL VPN Web ポータルまたは SSL VPN-Plus Client に次のメッセージが表示される。

最大ユーザー数に達しました/SSL VPN ライセンスのログイン ユーザーの最大数に達しました。しばらくしてからお試しください。  
または SSL の読み取りに失敗しました。

- SSL VPN サービスが実行されているが、データ パスが機能していない。
- SSL VPN 接続が確立されているが、プライベート ネットワーク内のアプリケーションにアクセスできない。

#### 解決方法

- 1 SSL VPN-Plus Client が SSL VPN サーバに接続できない場合は、次の操作を行います。
  - SSL VPN ユーザーが正しいユーザー名とパスワードでログインしていることを確認します。
  - SSL VPN ユーザーが有効かどうかを確認します。
  - Web ポータルから SSL VPN サーバに SSL VPN ユーザーが 接続できるかどうかを確認します。
- 2 NSX Edge で次の操作を行い、SSL VPN プロセスが実行されているかどうかを確認します。
  - a CLI から NSX Edge にログインします。Edge CLI にログインする方法については、NSX コマンド ライン インターフェイス リファレンス を参照してください。
  - b `show process monitor` コマンドを実行して、`sslvpn` プロセスを探します。
  - c `show service network-connections` コマンドを実行し、ポート 443 に `sslvpn` プロセスが表示されているかどうかを確認します。

**注：** デフォルトでは、SSL トラフィックにポート 443 が使用されます。ただし、SSL トラフィックに別の TCP ポートを設定している場合は、その TCP ポート番号に `sslvpn` プロセスが設定されていることを確認します。

- 3 SSL VPN-Plus Client で、SSL VPN-Plus サービスが実行されているかどうかを確認します。

オペレーティング システム	説明
Windows	[タスク マネージャ]を開き、SSL VPN-Plus Client サービスが開始しているかどうかを確認します。
Mac	<ul style="list-style-type: none"> <li>■ デーモンの <code>naclientd</code> プロセスが開始していることを確認します。</li> <li>■ GUI で <code>naclient</code> プロセスが開始していることを確認します。</li> </ul> プロセスが実行中かどうか確認するには、 <code>ps -ef   grep "naclient"</code> コマンドを実行します。
Linux	<ul style="list-style-type: none"> <li>■ <code>naclientd</code> プロセスと <code>naclient_poll</code> プロセスが開始していることを確認します。</li> <li>■ プロセスが実行中かどうか確認するには、<code>ps -ef   grep "naclient"</code> コマンドを実行します。</li> </ul>

サービスが実行されていない場合は、次のコマンドを実行してサービスを開始します。

オペレーティング システム	コマンド
Mac	<code>sudo launchctl load -w /Library/LaunchDaemons/com.vmware.naclientd.plist</code> コマンドを実行します。
Linux	<code>sudo service naclient start</code> コマンドを実行します。

- 4 SSL VPN のログイン ユーザーが最大数に達した場合は、NSX Edge フォーム ファクタを増やして、同時実行ユーザー数 (CCU) の数を増やします。

詳細については、『NSX 管理ガイド』を参照してください。この操作を実行すると、接続中のユーザーが VPN から切断されます。

- 5 SSL VPN サービスが実行されているが、データ パスが機能していない場合は、次の操作を行います。

- a 正常に接続した後、仮想 IP アドレスが割り当てられているかどうかを確認します。
- b ルートが追加されているかどうかを確認します。

- 6 プライベート (バックエンド) ネットワーク内のアプリケーションにアクセスできない場合は、次の操作を行って問題を解決します。

- a プライベート ネットワークと IP アドレス プールが同じサブネットに属していないことを確認します。
- b 管理者が IP アドレス プールを定義していない場合や、IP アドレス プールが不足している場合は、次の操作を行います。
  - 1 vSphere Web Client にログインします。
  - 2 [ネットワークとセキュリティ (Networking & Security)] をクリックし、[NSX Edge (NSX Edges)] をクリックします。
  - 3 NSX Edge をダブルクリックし、[SSL VPN-Plus] タブをクリックします。
  - 4 『NSX 管理ガイド』の「IP アドレス プールの追加」トピックの説明に従って、固定 IP アドレス プールを追加します。[ゲートウェイ (Gateway)] テキスト ボックスに IP アドレスを追加します。*na0* インターフェイスにゲートウェイの IP アドレスが割り当てられます。TCP 以外のすべてのトラフィックが *na0* インターフェイスという名前の仮想アダプタを通過します。同じ *na0* インターフェイスに割り当てられ、異なるゲートウェイ IP アドレスを持つ複数の IP アドレス プールを作成できます。
  - 5 入力された IP アドレスを確認し、すべての IP アドレス プールが同じ *na0* インターフェイスに割り当てられているかどうか確認するには、`show interface na0` コマンドを使用します。
  - 6 クライアント マシンにログインして [SSL VPN-Plus Client - 統計 (SSL VPN-Plus Client - Statistics)] 画面に移動し、割り当てられた仮想 IP アドレスを確認します。

- c NSX Edge コマンド ライン インターフェイス (CLI) にログインし、`debug packet capture interface na0` コマンドを実行して na0 インターフェイスでパケット キャプチャを実行します。[パケット キャプチャ (Packet Capture)] ツールを使用してパケットをキャプチャすることもできます。詳細については、『NSX 管理ガイド』を参照してください。

**注：** `no debug packet capture interface na0` コマンドを実行してキャプチャを停止するまで、パケット キャプチャがバックグラウンドで実行されます。

- d TCP の最適化が有効でない場合には、ファイアウォール ルールを確認します。
  - e TCP 以外のトラフィックの場合、バックエンド ネットワークのデフォルト ゲートウェイとして Edge の内部インターフェイスが設定されていることを確認します。
  - f Mac クライアントと Linux クライアントの場合、SSL VPN クライアントがインストールされているシステムにログインし、`tcpdump -i tap0 -s 1500 -w filepath` コマンドを実行して tap0 インターフェイスまたは仮想アダプタでパケット キャプチャを実行します。Windows クライアントで、Wireshark などのパケット解析ツールを使用し、SSL VPN-Plus Client アダプタでパケットをキャプチャします。
- 7 上記のすべて手順を試しても問題が解決しない場合は、次の NSX Edge CLI コマンドを使用して、さらにトラブルシューティングを行います。

目的	コマンド
SSL VPN のステータスを確認します。	<code>show service sslvpn-plus</code>
SSL VPN 統計情報を確認します。	<code>show service sslvpn-plus stats</code>
接続されている VPN クライアントを確認します。	<code>show service sslvpn-plus tunnels</code>
SSL VPN-Plus セッションを確認します。	<code>show service sslvpn-plus sessions</code>

## SSL VPN-Plus：認証の問題

SSL VPN-Plus の認証で問題が発生しました。

### 問題

SSL VPN-Plus の認証に失敗する

### 解決方法

- ◆ 認証の問題が発生した場合には、次の設定を確認してください。
  - a NSX Edge から外部の認証サーバに到達可能なことを確認します。NSX Edge から認証サーバに ping を送信し、サーバが到達可能かどうかを確認します。
  - b LDAP ブラウザなどのツールを使用して外部認証サーバの設定を確認し、設定が機能しているかどうか確認します。LDAP ブラウザで確認できるのは、LDAP サーバと Active Directory 認証サーバだけです。
  - c 認証プロセスで設定されている場合、ローカル認証サーバが最も低い優先度に設定されていることを確認します。

- d Active Directory (AD) を使用している場合、no-ssl モードに設定し、Active Directory サーバに到達可能なインターフェイスでパケット キャプチャを実行します。
- e Syslog サーバで認証が成功した場合、次のようなメッセージが表示されます。Log Output -  

```
SVP_LOG_NOTICE,
10-28-2013,09:28:39,Authentication,a,-,-,10.112.243.61,-,PHAT,,SUCCESS,,10-28-2013,09:28:39,-,-,,,,,,,,,-,-,
```
- f Syslog サーバで認証に失敗した場合、次のようなメッセージが表示されます。Log Output -  

```
SVP_LOG_NOTICE,
10-28-2013,09:28:39,Authentication,a,-,-,10.112.243.61,-,PHAT,,FAILURE,,10-28-2013,09:28:39,-,-,,,,,,,,,-,-,
```

## SSL VPN-Plus クライアントが応答しない

TCP 最適化を有効にすると、SSL VPN-Plus クライアントが応答しなくなります。

### 問題

NSX Edge で実行される SSL VPN-Plus サービスが設定され、トンネル経由でのトラフィック送信に TCP 最適化が有効になっています。SSL VPN-Plus クライアントでネットワーク パフォーマンス計測ツール (iperf3 など) を実行すると、SSL VPN-Plus クライアントが応答不能になります。

### 原因

次のいずれかの場合、SSL VPN-Plus クライアントからデータが送信されると、トンネルで読み取りエラーが発生する可能性があります。

- バックエンド サーバが、TCP FIN シーケンスを送信して、SSL VPN サーバとの TCP 接続を終了している。
- バックエンド サーバへのデータの転送中にトンネル書き込み処理が失敗している。

トンネル読み取りエラーは、不明なプロトコル ID です。このエラーが発生すると、SSL VPN サーバと SSL VPN-Plus クライアント間のトンネルが解除されます。さらに、クライアント側で読み取り/書き込み処理が失敗し、SSL VPN-Plus クライアントが応答不能になります。

### 解決方法

- ◆ この問題を解決するには、vSphere Web Client の手順に従って、SSL VPN トンネル経由でのプライベート ネットワーク トラフィックの TCP 最適化を無効にします。
  - a SSL VPN-Plus サービスを設定している NSX Edge 仮想マシンをダブルクリックします。
  - b [SSL VPN-Plus] タブをクリックし、プライベート ネットワークを選択します。
  - c [TCP 最適化の有効化 (Enable TCP Optimization)] チェック ボックスの選択を解除します。

## 基本的なログ分析

SSL VPN-Plus ゲートウェイのログが、NSX Edge アプライアンスで設定された Syslog サーバに送信されます。SSL VPN-Plus Client のログは、リモート ユーザーのコンピュータの C:\Users\username\AppData\Local\VMware\vpn\svp\_client.log ディレクトリに格納されます。

## 基本的なログ分析： 認証

### 認証の成功

- 次のログ出力は、ネットワーク アクセス クライアントで 2016 年 10 月 28 日 9 時 28 分にユーザー *a* が正常に認証されたことを示しています。

```
SVP_LOG_NOTICE,10-28-2016,09:28:39,Authentication,a,-,-,10.112.243.61,-,PHAT,,SUCCESS,,10-28-2016,09:28:39,-,-,,,,,,,,,,,,,-,-,-
```

### 認証の失敗

- 次のログ出力は、ネットワーク アクセス クライアントで 2016 年 10 月 28 日 9 時 28 分にユーザー *a* が認証に失敗したことを示しています。

```
SVP_LOG_NOTICE,10-28-2016,09:28:39,Authentication,a,-,-,10.112.243.61,-,PHAT,,FAILURE,,10-28-2016,09:28:39,-,-,,,,,,,,,,,,,-,-,-
```

[SSL VPN-Plus：インストールの失敗](#)を参照して、認証の問題を解決してください。

## 基本的なログ分析： データ パス

### データ パスの成功

- 次のログ出力は、2016 年 10 月 28 日 9 時 41 分にユーザー *a* がネットワーク アクセス クライアントを使用してバックエンド Web サーバ 192.168.10.8 に TCP 経由で正常に接続したことを示しています。

```
SVP_LOG_INFO,10-28-2016,09:41:03,TCP
Connect,a,-,-,10.112.243.61,-,PHAT,,SUCCESS,,10-28-2013,09:41:03,-,-,192.168.10.8,80,,,,,,,,,-,-,-
```

### データ パスの失敗

- 次のログ出力は、2016 年 10 月 28 日 9 時 41 分にユーザー *a* がネットワーク アクセス クライアントを使用してバックエンド Web サーバ 192.168.10.8 に TCP 経由で接続できなかったことを示しています。

```
SVP_LOG_INFO,10-28-2016,09:41:03,TCP
Connect,a,-,-,10.112.243.61,-,PHAT,,FAILURE,,10-28-2013,09:41:03,-,-,192.168.10.8,80,,,,,,,,,-,-,-
```

## IPsec VPN

この情報は、ご使用のセットアップでネゴシエーション問題のトラブルシューティングを行うときに参考にしてください。

## 成功するネゴシエーション（フェーズ 1 とフェーズ 2 共）

次の例は、NSX Edge と Cisco デバイス間の成功したネゴシエート結果を示しています。

## NSX Edge

NSX Edge コマンドライン インターフェイスから (ipsec auto -status、show service ipsec コマンドの一部) の場合は次のようになります。

```
000 #2: "s1-c1":500 STATE_QUICK_I2 (sent QI2, IPsec SA established);
      EVENT_SA_REPLACE in 2430s; newest IPSEC; eroute owner; isakmp#1; idle;
      import:admin initiate
000 #2: "s1-c1" esp.f5f6877d@10.20.131.62 esp.7aaf335f@10.20.129.80
      tun.0@10.20.131.62 tun.0@10.20.129.80 ref=0 refhim=4294901761
000 #1: "s1-c1":500 STATE_MAIN_I4 (ISAKMP SA established); EVENT_SA_REPLACE in
      27623s; newest ISAKMP; lastdpd=0s(seq in:0 out:0); idle;
      import:admin initiate
```

## Cisco

```
ciscoasa# show crypto isakmp sa detail

Active SA: 1
Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1

IKE Peer: 10.20.129.80
Type : L2L           Role      : responder
Rekey : no           State     : MM_ACTIVE
Encrypt : 3des        Hash      : SHA
Auth : preshared      Lifetime: 28800
Lifetime Remaining: 28379
```

## フェーズ 1 ポリシーがマッチしない

以下に、フェーズ 1 ポリシーがマッチしないエラーのログを示します。

## NSX Edge

NSX Edge が STATE\_MAIN\_I1 状態でハングしています。/var/log/messages の内容を調べ、ピアが「NO\_PROPOSAL\_CHOSEN」を設定して IKE メッセージを送り返したことを示す情報があることを確認してください。

```
000 #1: "s1-c1":500 STATE_MAIN_I1 (sent MI1,
      expecting MR1); EVENT_RETRANSMIT in 7s; nodpd; idle;
      import:admin initiate
000 #1: pending Phase 2 for "s1-c1" replacing #0
Aug 26 12:31:25 weiqing-desktop ipsec[6569]:
      | got payload 0x800(ISAKMP_NEXT_N) needed: 0x0 opt: 0x0
Aug 26 12:31:25 weiqing-desktop ipsec[6569]:
      | ***parse ISAKMP Notification Payload:
Aug 26 12:31:25 weiqing-desktop ipsec[6569]:
      |   next payload type: ISAKMP_NEXT_NONE
Aug 26 12:31:25 weiqing-desktop ipsec[6569]: |   length: 96
Aug 26 12:31:25 weiqing-desktop ipsec[6569]:
      |   DOI: ISAKMP_DOI_IPSEC
Aug 26 12:31:25 weiqing-desktop ipsec[6569]: |   protocol ID: 0
```

```
Aug 26 12:31:25 weiqing-desktop ipsec[6569]: | SPI size: 0
Aug 26 12:31:25 weiqing-desktop ipsec[6569]:
| Notify Message Type: NO_PROPOSAL_CHOSEN
Aug 26 12:31:25 weiqing-desktop ipsec[6569]:
"s1-c1" #1: ignoring informational payload,
type NO_PROPOSAL_CHOSEN msgid=00000000
```

## Cisco

デバッグ クリプトが有効の場合、プロポーザルが受け入れられなかったというエラー メッセージがプリントされます。

```
ciscoasa# Aug 26 18:17:27 [IKEv1]:
IP = 10.20.129.80, IKE_DECODE RECEIVED
Message (msgid=0) with payloads : HDR + SA (1)
+ VENDOR (13) + VENDOR (13) + NONE (0) total length : 148
Aug 26 18:17:27 [IKEv1 DEBUG]: IP = 10.20.129.80,
processing SA payload
Aug 26 18:17:27 [IKEv1]: Phase 1 failure: Mismatched attribute
types for class Group Description: Rcv'd: Group 5
Cfg'd: Group 2
Aug 26 18:17:27 [IKEv1]: Phase 1 failure: Mismatched attribute
types for class Group Description: Rcv'd: Group 5
Cfg'd: Group 2
Aug 26 18:17:27 [IKEv1]: IP = 10.20.129.80, IKE_DECODE SENDING
Message (msgid=0) with payloads : HDR + NOTIFY (11)
+ NONE (0) total length : 124
Aug 26 18:17:27 [IKEv1 DEBUG]: IP = 10.20.129.80,
All SA proposals found unacceptable
Aug 26 18:17:27 [IKEv1]: IP = 10.20.129.80, Error processing
payload: Payload ID: 1
Aug 26 18:17:27 [IKEv1 DEBUG]: IP = 10.20.129.80, IKE MM Responder
FSM error history (struct &0xd8355a60) <state>, <event>:
MM_DONE, EV_ERROR-->MM_START, EV_RCV_MSG-->MM_START,
EV_START_MM-->MM_START, EV_START_MM-->MM_START,
EV_START_MM-->MM_START, EV_START_MM-->MM_START,
EV_START_MM-->MM_START, EV_START_MM
Aug 26 18:17:27 [IKEv1 DEBUG]: IP = 10.20.129.80, IKE SA
MM:9e0e4511 terminating: flags 0x01000002, refcnt 0,
tuncnt 0
Aug 26 18:17:27 [IKEv1 DEBUG]: IP = 10.20.129.80, sending
delete/delete with reason message
```

## フェーズ 2 がマッチしない

以下に、フェーズ 2 ポリシーがマッチしないエラーのログを示します。

## NSX Edge

NSX Edge は、STATE\_QUICK\_I1 状態でハングしています。ログ メッセージは、ピアが NO\_PROPOSAL\_CHOSEN メッセージを送信したことを示しています。

```
000 #2: "s1-c1":500 STATE_QUICK_I1 (sent QI1, expecting
      QR1); EVENT_RETRANSMIT in 11s; lastdpd=-1s(seq in:0 out:0);
      idle; import:admin initiate
Aug 26 12:33:54 weiqing-desktop ipsec[6933]: | got payload
      0x800(ISAKMP_NEXT_N) needed: 0x0 opt: 0x0
Aug 26 12:33:54 weiqing-desktop ipsec[6933]: | ***parse
      ISAKMP Notification Payload:
Aug 26 12:33:54 weiqing-desktop ipsec[6933]: |      next payload
      type: ISAKMP_NEXT_NONE
Aug 26 12:33:54 weiqing-desktop ipsec[6933]: |      length: 32
Aug 26 12:33:54 weiqing-desktop ipsec[6933]: |
      |      DOI: ISAKMP_DOI_IPSEC
Aug 26 12:33:54 weiqing-desktop ipsec[6933]: |      protocol ID: 3
Aug 26 12:33:54 weiqing-desktop ipsec[6933]: |      SPI size: 16
Aug 26 12:33:54 weiqing-desktop ipsec[6933]: |      Notify Message
      Type: NO_PROPOSAL_CHOSEN
Aug 26 12:33:54 weiqing-desktop ipsec[6933]: "s1-c1" #3:
      ignoring informational payload, type NO_PROPOSAL_CHOSEN
      msgid=00000000
```

## Cisco

フェーズ 1 は完了したがフェーズ 2 はポリシー ネゴシエーションの失敗により失敗したという、デバッグ メッセージが示されます。

```
Aug 26 16:03:49 [IKEv1]: Group = 10.20.129.80,
      IP = 10.20.129.80, PHASE 1 COMPLETED
Aug 26 16:03:49 [IKEv1]: IP = 10.20.129.80, Keep-alive type
      for this connection: DPD
Aug 26 16:03:49 [IKEv1 DEBUG]: Group = 10.20.129.80,
      IP = 10.20.129.80, Starting P1 rekey timer: 21600 seconds
Aug 26 16:03:49 [IKEv1]: IP = 10.20.129.80, IKE_DECODE RECEIVED
      Message (msgid=b2cdcb13) with payloads : HDR + HASH (8)
      + SA (1) + NONCE (10) + KE (4) + ID (5) + ID (5) + NONE (0)
      total length : 288
.
.
.
Aug 26 16:03:49 [IKEv1]: Group = 10.20.129.80, IP = 10.20.129.80,
      Session is being torn down. Reason: Phase 2 Mismatch
```

## PFS 不一致

以下に、PFS 不一致エラー ログを示します。



## NSX Edge

PFS はフェーズ 2 の一部としてネゴシエートされます。PFS が一致しない場合、[フェーズ 2 がマッチしない](#)で説明されている失敗ケースと類似の反応を示します。

```
000 #4: "s1-c1":500 STATE_QUICK_I1 (sent QI1, expecting
      QR1); EVENT_RETRANSMIT in 8s; lastdpd=-1s(seq in:0 out:0);
      idle; import:admin initiate
Aug 26 12:35:52 weiqing-desktop ipsec[7312]: | got payload 0x800
      (ISAKMP_NEXT_N) needed: 0x0 opt: 0x0
Aug 26 12:35:52 weiqing-desktop ipsec[7312]:
      | ***parse ISAKMP Notification Payload:
Aug 26 12:35:52 weiqing-desktop ipsec[7312]: |      next payload
      type: ISAKMP_NEXT_NONE
Aug 26 12:35:52 weiqing-desktop ipsec[7312]: |      length: 32
Aug 26 12:35:52 weiqing-desktop ipsec[7312]:
      |      DOI: ISAKMP_DOI_IPSEC
Aug 26 12:35:52 weiqing-desktop ipsec[7312]: |      protocol ID: 3
Aug 26 12:35:52 weiqing-desktop ipsec[7312]: |      SPI size: 16
Aug 26 12:35:52 weiqing-desktop ipsec[7312]: |      Notify Message
      Type: NO_PROPOSAL_CHOSEN
Aug 26 12:35:52 weiqing-desktop ipsec[7312]: "s1-c1" #1: ignoring
      informational payload, type NO_PROPOSAL_CHOSEN
      msgid=00000000
Aug 26 12:35:52 weiqing-desktop ipsec[7312]: | info:  fa 16 b3 e5
      91 a9 b0 02  a3 30 e1 d9  6e 5a 13 d4
Aug 26 12:35:52 weiqing-desktop ipsec[7312]: | info:  93 e5 e4 d7
Aug 26 12:35:52 weiqing-desktop ipsec[7312]:
      | processing informational NO_PROPOSAL_CHOSEN (14)
```

## Cisco

```
<BS>Aug 26 19:00:26 [IKEv1 DEBUG]: Group = 10.20.129.80,
      IP = 10.20.129.80, sending delete/delete with
      reason message
Aug 26 19:00:26 [IKEv1 DEBUG]: Group = 10.20.129.80,
      IP = 10.20.129.80, constructing blank hash payload
Aug 26 19:00:26 [IKEv1 DEBUG]: Group = 10.20.129.80,
      IP = 10.20.129.80, constructing blank hash payload
Aug 26 19:00:26 [IKEv1 DEBUG]: Group = 10.20.129.80,
      IP = 10.20.129.80, constructing IKE delete payload
Aug 26 19:00:26 [IKEv1 DEBUG]: Group = 10.20.129.80,
      IP = 10.20.129.80, constructing qm hash payload
Aug 26 19:00:26 [IKEv1]: IP = 10.20.129.80, IKE_DECODE SENDING
      Message (msgid=19eb1e59) with payloads : HDR + HASH (8)
      + DELETE (12) + NONE (0) total length : 80
Aug 26 19:00:26 [IKEv1]: Group = 10.20.129.80, IP = 10.20.129.80,
      Session is being torn down. Reason: Phase 2 Mismatch
```

## PSK が一致しない

以下に、PSK が一致しないエラーのログを示します。

### NSX Edge

PSK はフェーズ 1 の最後のラウンドでネゴシエートされます。PSK ネゴシエーションに失敗した場合、NSX Edge の状態は STATE\_MAIN\_I4 です。ピアは INVALID\_ID\_INFORMATION を含むメッセージを送信します。

```
Aug 26 11:55:55 weiqing-desktop ipsec[3855]:
"s1-c1" #1: transition from state STATE_MAIN_I3 to
state STATE_MAIN_I4
Aug 26 11:55:55 weiqing-desktop ipsec[3855]: "s1-c1" #1:
STATE_MAIN_I4: ISAKMP SA established
{auth=OAKLEY_PRESHARED_KEY
cipher=oakley_3des_cbc_192 prf=oakley_sha group=modp1024}
Aug 26 11:55:55 weiqing-desktop ipsec[3855]: "s1-c1" #1: Dead Peer
Detection (RFC 3706): enabled
Aug 26 11:55:55 weiqing-desktop ipsec[3855]: "s1-c1" #2:
initiating Quick Mode PSK+ENCRYPT+TUNNEL+PFS+UP+SAREFTRACK
{using isakmp#1 msgid:e8add10e proposal=3DES(3)_192-SHA1(2)_160
pfsgroup=OAKLEY_GROUP_MODP1024}
Aug 26 11:55:55 weiqing-desktop ipsec[3855]: "s1-c1" #1:
ignoring informational payload, type INVALID_ID_INFORMATION
msgid=00000000
```

### Cisco

```
Aug 26 15:27:07 [IKEv1]: IP = 10.115.199.191,
IKE_DECODE SENDING Message (msgid=0) with payloads : HDR
+ KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13)
+ VENDOR (13) + VENDOR (13) + NAT-D (130) + NAT-D (130)
+ NONE (0) total length : 304
Aug 26 15:27:07 [IKEv1]: Group = 10.115.199.191,
IP = 10.115.199.191, Received encrypted Oakley Main Mode
packet with invalid payloads, MessID = 0
Aug 26 15:27:07 [IKEv1]: IP = 10.115.199.191, IKE_DECODE SENDING
Message (msgid=0) with payloads : HDR + NOTIFY (11)
+ NONE (0) total length : 80
Aug 26 15:27:07 [IKEv1]: Group = 10.115.199.191,
IP = 10.115.199.191, ERROR, had problems decrypting
packet, probably due to mismatched pre-shared key.
Aborting
```

## 成功するネゴシエーションのためのパケットのキャプチャ

以下に、NSX Edge と Cisco デバイスの間で正常に行われたネゴシエーションでのパケット キャプチャ セッションを示します。

No.	Time	Source	Destination	Protocol	Info
9203	768.394800	10.20.129.80	10.20.131.62	ISAKMP	Identity Protection (Main Mode)
Frame 9203 (190 bytes on wire, 190 bytes captured)					

```

Ethernet II, Src: Vmware_9d:2c:dd (00:50:56:9d:2c:dd),
      Dst: Cisco_80:70:f5 (00:13:c4:80:70:f5)
Internet Protocol, Src: 10.20.129.80 (10.20.129.80),
      Dst: 10.20.131.62 (10.20.131.62)
User Datagram Protocol, Src Port: isakmp (500), Dst Port: isakmp (500)
Internet Security Association and Key Management Protocol
  Initiator cookie: 92585D2D797E9C52
  Responder cookie: 0000000000000000
  Next payload: Security Association (1)
  Version: 1.0
  Exchange type: Identity Protection (Main Mode) (2)
  Flags: 0x00
  Message ID: 0x00000000
  Length: 148
  Security Association payload
    Next payload: Vendor ID (13)
    Payload length: 84
    Domain of interpretation: IPSEC (1)
    Situation: IDENTITY (1)
    Proposal payload # 0
      Next payload: NONE (0)
      Payload length: 72
      Proposal number: 0
      Protocol ID: ISAKMP (1)
      SPI Size: 0
      Proposal transforms: 2
      Transform payload # 0
        Next payload: Transform (3)
        Payload length: 32
        Transform number: 0
        Transform ID: KEY_IKE (1)
        Life-Type (11): Seconds (1)
        Life-Duration (12): Duration-Value (28800)
        Encryption-Algorithm (1): 3DES-CBC (5)
        Hash-Algorithm (2): SHA (2)
        Authentication-Method (3): PSK (1)
        Group-Description (4): 1536 bit MODP group (5)
      Transform payload # 1
        Next payload: NONE (0)
        Payload length: 32
        Transform number: 1
        Transform ID: KEY_IKE (1)
        Life-Type (11): Seconds (1)
        Life-Duration (12): Duration-Value (28800)
        Encryption-Algorithm (1): 3DES-CBC (5)
        Hash-Algorithm (2): SHA (2)
        Authentication-Method (3): PSK (1)
        Group-Description (4): Alternate 1024-bit MODP group (2)
    Vendor ID: 4F456C6A405D72544D42754D
    Next payload: Vendor ID (13)
    Payload length: 16
    Vendor ID: 4F456C6A405D72544D42754D
  Vendor ID: RFC 3706 Detecting Dead IKE Peers (DPD)
  Next payload: NONE (0)
  Payload length: 20

```

Vendor ID: RFC 3706 Detecting Dead IKE Peers (DPD)

No.	Time	Source	Destination	Protocol Info
9204	768.395550	10.20.131.62	10.20.129.80	ISAKMP Identity Protection (Main Mode)

Frame 9204 (146 bytes on wire, 146 bytes captured)  
 Ethernet II, Src: Cisco\_80:70:f5 (00:13:c4:80:70:f5),  
     Dst: Vmware\_9d:2c:dd (00:50:56:9d:2c:dd)  
 Internet Protocol, Src: 10.20.131.62 (10.20.131.62),  
     Dst: 10.20.129.80 (10.20.129.80)  
 User Datagram Protocol, Src Port: isakmp (500), Dst Port: isakmp (500)  
 Internet Security Association and Key Management Protocol  
   Initiator cookie: 92585D2D797E9C52  
   Responder cookie: 34704CFC8C8DBD09  
   Next payload: Security Association (1)  
   Version: 1.0  
   Exchange type: Identity Protection (Main Mode) (2)  
   Flags: 0x00  
   Message ID: 0x00000000  
   Length: 104  
   Security Association payload  
     Next payload: Vendor ID (13)  
     Payload length: 52  
     Domain of interpretation: IPSEC (1)  
     Situation: IDENTITY (1)  
     Proposal payload # 1  
       Next payload: NONE (0)  
       Payload length: 40  
       Proposal number: 1  
       Protocol ID: ISAKMP (1)  
       SPI Size: 0  
       Proposal transforms: 1  
       Transform payload # 1  
         Next payload: NONE (0)  
         Payload length: 32  
         Transform number: 1  
         Transform ID: KEY\_IKE (1)  
         Encryption-Algorithm (1): 3DES-CBC (5)  
         Hash-Algorithm (2): SHA (2)  
         Group-Description (4): Alternate 1024-bit MODP group (2)  
         Authentication-Method (3): PSK (1)  
         Life-Type (11): Seconds (1)  
         Life-Duration (12): Duration-Value (28800)  
     Vendor ID: Microsoft L2TP/IPSec VPN Client  
       Next payload: NONE (0)  
       Payload length: 24  
     Vendor ID: Microsoft L2TP/IPSec VPN Client

No.	Time	Source	Destination	Protocol Info
9205	768.399599	10.20.129.80	10.20.131.62	ISAKMP Identity Protection (Main Mode)

Frame 9205 (222 bytes on wire, 222 bytes captured)  
 Ethernet II, Src: Vmware\_9d:2c:dd (00:50:56:9d:2c:dd),

```

    Dst: Cisco_80:70:f5 (00:13:c4:80:70:f5)
Internet Protocol, Src: 10.20.129.80 (10.20.129.80),
    Dst: 10.20.131.62 (10.20.131.62)
User Datagram Protocol, Src Port: isakmp (500), Dst Port: isakmp (500)
Internet Security Association and Key Management Protocol
  Initiator cookie: 92585D2D797E9C52
  Responder cookie: 34704CFC8C8DBD09
  Next payload: Key Exchange (4)
  Version: 1.0
  Exchange type: Identity Protection (Main Mode) (2)
  Flags: 0x00
  Message ID: 0x00000000
  Length: 180
  Key Exchange payload
    Next payload: Nonce (10)
    Payload length: 132
    Key Exchange Data (128 bytes / 1024 bits)
  Nonce payload
    Next payload: NONE (0)
    Payload length: 20
    Nonce Data

```

No.	Time	Source	Destination	Protocol Info
9206	768.401192	10.20.131.62	10.20.129.80	ISAKMP Identity Protection (Main Mode)

```

Frame 9206 (298 bytes on wire, 298 bytes captured)
Ethernet II, Src: Cisco_80:70:f5 (00:13:c4:80:70:f5),
    Dst: Vmware_9d:2c:dd (00:50:56:9d:2c:dd)
Internet Protocol, Src: 10.20.131.62 (10.20.131.62),
    Dst: 10.20.129.80 (10.20.129.80)
User Datagram Protocol, Src Port: isakmp (500), Dst Port: isakmp (500)
Internet Security Association and Key Management Protocol
  Initiator cookie: 92585D2D797E9C52
  Responder cookie: 34704CFC8C8DBD09
  Next payload: Key Exchange (4)
  Version: 1.0
  Exchange type: Identity Protection (Main Mode) (2)
  Flags: 0x00
  Message ID: 0x00000000
  Length: 256
  Key Exchange payload
    Next payload: Nonce (10)
    Payload length: 132
    Key Exchange Data (128 bytes / 1024 bits)
  Nonce payload
    Next payload: Vendor ID (13)
    Payload length: 24
    Nonce Data
  Vendor ID: CISCO-UNITY-1.0
    Next payload: Vendor ID (13)
    Payload length: 20
    Vendor ID: CISCO-UNITY-1.0
  Vendor ID: draft-beaulieu-ike-xauth-02.txt
    Next payload: Vendor ID (13)

```

```

Payload length: 12
Vendor ID: draft-beaulieu-ike-xauth-02.txt
Vendor ID: C1B7EBE18C8CBD099E89695E2CB16A4A
Next payload: Vendor ID (13)
Payload length: 20
Vendor ID: C1B7EBE18C8CBD099E89695E2CB16A4A
Vendor ID: CISCO-CONCENTRATOR
Next payload: NONE (0)
Payload length: 20
Vendor ID: CISCO-CONCENTRATOR

```

No.	Time	Source	Destination	Protocol	Info
9207	768.404990	10.20.129.80	10.20.131.62	ISAKMP	Identity Protection (Main Mode)

```

Frame 9207 (110 bytes on wire, 110 bytes captured)
Ethernet II, Src: Vmware_9d:2c:dd (00:50:56:9d:2c:dd),
      Dst: Cisco_80:70:f5 (00:13:c4:80:70:f5)
Internet Protocol, Src: 10.20.129.80 (10.20.129.80),
      Dst: 10.20.131.62 (10.20.131.62)
User Datagram Protocol, Src Port: isakmp (500), Dst Port: isakmp (500)
Internet Security Association and Key Management Protocol
  Initiator cookie: 92585D2D797E9C52
  Responder cookie: 34704CFC8C8DBD09
  Next payload: Identification (5)
  Version: 1.0
  Exchange type: Identity Protection (Main Mode) (2)
  Flags: 0x01
  Message ID: 0x00000000
  Length: 68
  Encrypted payload (40 bytes)

```

No.	Time	Source	Destination	Protocol	Info
9208	768.405921	10.20.131.62	10.20.129.80	ISAKMP	Identity Protection (Main Mode)

```

Frame 9208 (126 bytes on wire, 126 bytes captured)
Ethernet II, Src: Cisco_80:70:f5 (00:13:c4:80:70:f5),
      Dst: Vmware_9d:2c:dd (00:50:56:9d:2c:dd)
Internet Protocol, Src: 10.20.131.62 (10.20.131.62),
      Dst: 10.20.129.80 (10.20.129.80)
User Datagram Protocol, Src Port: isakmp (500), Dst Port: isakmp (500)
Internet Security Association and Key Management Protocol
  Initiator cookie: 92585D2D797E9C52
  Responder cookie: 34704CFC8C8DBD09
  Next payload: Identification (5)
  Version: 1.0
  Exchange type: Identity Protection (Main Mode) (2)
  Flags: 0x01
  Message ID: 0x00000000
  Length: 84
  Encrypted payload (56 bytes)

```

No.	Time	Source	Destination	Protocol	Info
9209	768.409799	10.20.129.80	10.20.131.62	ISAKMP	Quick Mode

```

Frame 9209 (334 bytes on wire, 334 bytes captured)
Ethernet II, Src: Vmware_9d:2c:dd (00:50:56:9d:2c:dd),
      Dst: Cisco_80:70:f5 (00:13:c4:80:70:f5)
Internet Protocol, Src: 10.20.129.80 (10.20.129.80),
      Dst: 10.20.131.62 (10.20.131.62)
User Datagram Protocol, Src Port: isakmp (500), Dst Port: isakmp (500)
Internet Security Association and Key Management Protocol
  Initiator cookie: 92585D2D797E9C52
  Responder cookie: 34704CFC8C8DBD09
  Next payload: Hash (8)
  Version: 1.0
  Exchange type: Quick Mode (32)
  Flags: 0x01
  Message ID: 0x79a63fb1
  Length: 292
  Encrypted payload (264 bytes)

```

No.	Time	Source	Destination	Protocol	Info
9210	768.411797	10.20.131.62	10.20.129.80	ISAKMP	Quick Mode

```

Frame 9210 (334 bytes on wire, 334 bytes captured)
Ethernet II, Src: Cisco_80:70:f5 (00:13:c4:80:70:f5),
      Dst: Vmware_9d:2c:dd (00:50:56:9d:2c:dd)
Internet Protocol, Src: 10.20.131.62 (10.20.131.62),
      Dst: 10.20.129.80 (10.20.129.80)
User Datagram Protocol, Src Port: isakmp (500), Dst Port: isakmp (500)
Internet Security Association and Key Management Protocol
  Initiator cookie: 92585D2D797E9C52
  Responder cookie: 34704CFC8C8DBD09
  Next payload: Hash (8)
  Version: 1.0
  Exchange type: Quick Mode (32)
  Flags: 0x01
  Message ID: 0x79a63fb1
  Length: 292
  Encrypted payload (264 bytes)

```

No.	Time	Source	Destination	Protocol	Info
9211	768.437057	10.20.129.80	10.20.131.62	ISAKMP	Quick Mode

```

Frame 9211 (94 bytes on wire, 94 bytes captured)
Ethernet II, Src: Vmware_9d:2c:dd (00:50:56:9d:2c:dd),
      Dst: Cisco_80:70:f5 (00:13:c4:80:70:f5)
Internet Protocol, Src: 10.20.129.80 (10.20.129.80),
      Dst: 10.20.131.62 (10.20.131.62)
User Datagram Protocol, Src Port: isakmp (500), Dst Port: isakmp (500)
Internet Security Association and Key Management Protocol
  Initiator cookie: 92585D2D797E9C52
  Responder cookie: 34704CFC8C8DBD09
  Next payload: Hash (8)
  Version: 1.0
  Exchange type: Quick Mode (32)
  Flags: 0x01
  Message ID: 0x79a63fb1

```

Length: 52

Encrypted payload (24 bytes)



# NSX Controller のトラブルシューティング

## 8

このセクションでは、NSX Controller の障害の原因特定と、コントローラのトラブルシューティングに関する情報を提供します。

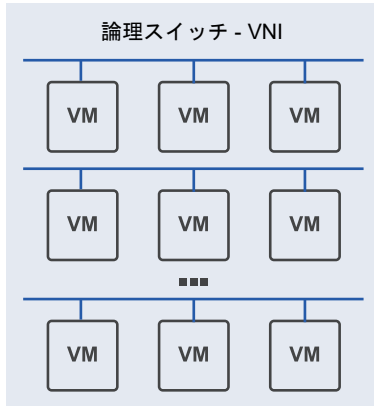
この章には、次のトピックが含まれています。

- [コントローラ クラスタ アーキテクチャについて](#)
- [NSX Controller のデプロイに関する問題](#)
- [ディスク遅延のトラブルシューティング](#)
- [NSX Controller クラスタの障害](#)
- [NSX Controller が切断された](#)
- [制御プレーン エージェント \(netcpa\) の問題](#)

## コントローラ クラスタ アーキテクチャについて

NSX Controller クラスタはスケールアウト型の分散システムで、各コントローラ ノードには、そのノードが実装できるタスクの種類を定義した一連のロールが割り当てられます。高い回復性とパフォーマンスを実現するため、コントローラ仮想マシンは 3 つの異なるホストにデプロイする必要があります。

複数の NSX Controller クラスタ ノードにワークロードを分散するため、シャーディングが使用されます。シャーディングとは、NSX Controller のワークロードを複数のシャードに分割して、NSX Controller の各インスタンスの負荷が同等になるようにすることです。



オブジェクト



シャード



これは、指定したエンティティ（論理スイッチ、論理ルーティング、その他のサービスなど）に対して、特定のコントローラ ノードがどのようにマスターとして動作するかを示しています。あるロールについて、特定の NSX Controller インスタンスがマスターに選ばれると、その NSX Controller は、論理スイッチと分散論理ルーターを、クラスタ内にある使用可能なすべての NSX Controller インスタンスに振り分けます。

「シャード」に表示されている番号付きのボックスは、マスターがワークロードを分割する際に使用するシャードを表しています。論理スイッチのマスターは、論理スイッチを複数のシャードに分割し、それらのシャードを異なる NSX Controller インスタンスに割り当てます。分散論理ルーターのマスターも、分散論理ルーターを複数のシャードに分割し、それらのシャードを異なる NSX Controller インスタンスに割り当てます。

これらのシャードは、クラスタ内の異なる NSX Controller インスタンスに割り当てられます。どの NSX Controller インスタンスをどのシャードに割り当てるかはロールのマスターが決定します。ある要求がルーターのシャード 3 に届くと、そのシャードは 3 番目の NSX Controller インスタンスに接続するように指示されます。ある要求が論理スイッチのシャード 2 に届くと、その要求は 2 番目の NSX Controller インスタンスによって処理されず。

クラスタ内のいずれかの NSX Controller インスタンスで障害が発生すると、ロールのマスターが、使用可能な残りのクラスタにシャードを再分散します。コントローラ ノードのうちの 1 つは、各ロールのマスターとして選出されます。マスターには、シャードを個々のコントローラ ノードに割り当て、ノードの障害が発生した際に他のノードにシャードを再び割り当てるといった責務があります。また、マスターはクラスタ ノードの障害を ESXi ホストに通知します。

各ロールのマスターを選出する際は、クラスタ内にある全ノード（アクティブと非アクティブを含む）の過半数票が必要です。これが、コントローラ クラスタのデプロイで常にノード数を奇数にしなければならない最大の理由です。

## ZooKeeper

ZooKeeper は、NSX Controller クラスタのメカニズムを支えるクライアント/サーバ アーキテクチャです。コントローラ クラスタは、ZooKeeper を使用して検出および作成されます。クラスタが作成される際、ZooKeeper がすべてのノードを管理します。ZooKeeper ノードは、コントローラ クラスタを形成するための選出プロセスに進みます。クラスタ内には、ZooKeeper マスター ノードが 1 台必要です。これは、ノード間選出によって行われます。

コントローラ ノードが新規作成されると、NSX Manager は、ノード情報（ノード IP アドレスと ID を含む）を現在のクラスタに伝達します。このようにして、各ノードはクラスタリングに使用できる合計ノード数を把握します。ZooKeeper マスターの選出では、各ノードが一票を投じてマスター ノードを選出します。1 つのノードがあるマジョリティ投票するまで、もう一度選択がトリガされます。たとえば、3 ノード設定のクラスタでマスター ノードになるには、2 票以上が必要です。

---

**注：** ZooKeeper マスターが選出されないという事態を避けるため、クラスタ内のノードは 3 台にする必要があります。

---

- 最初のコントローラのデプロイ時は、このコントローラがマスターになります。そのため、コントローラをデプロイする際は、最初のノードのデプロイが完了してから他のノードを追加します。
- 2 番目のコントローラを追加した時点では、ノード数が偶数になるため、特殊な状態と言えます。
- 3 番目のノードを追加すると、クラスタは安定した状態になります。

ZooKeeper で一度に許容できる障害は 1 つのみです。つまり、あるコントローラ ノードが停止したら、他の障害が発生する前にそのノードをリカバリする必要があります。そうしないと、クラスタ破損する可能性があります。

## 中央制御プレーン (CCP) のドメイン マネージャ

これは、ZooKeeper の上位にあるレイヤーで、ZooKeeper の初期設定をすべてのノードに提供します。ドメイン マネージャは、クラスタ内のすべてのノードの設定を更新した後、ZooKeeper プロセスを開始するリモート プロシージャ コールを呼び出します。

ドメイン マネージャには、すべてのドメインを開始する責務があります。クラスタに参加するため、CCP ドメインは、他のマシン上にある CCP ドメインと通信します。クラスタの初期化をサポートする CCP ドメインのコンポーネントは *zk-cluster-bootstrap* です。

## コントローラと他のコンポーネントとの関係

コントローラ クラスタは、論理スイッチ、分散論理ルーター、VTEP に関する情報を管理し、ESXi ホストに提供します。

論理スイッチが作成されると、クラスタ内のコントローラ ノードは、その論理スイッチの マスター（オーナー）となるノードを決定します。これは、分散論理ルーターが追加される際にも当てはまります。

論理スイッチまたは分散論理ルーターに対する所有権が確立すると、ノードはその所有権を、対象のスイッチまたはルーターのトランスポート ゾーンに属する ESXi ホストに送信します。所有権を決定し、所有権情報をホストに伝達する処理全体を「シャーディング」と呼びます。所有権とは、対象の論理スイッチまたは分散論理ルーターについて、ノードが NSX 関連のすべての操作に責任を持つことを意味します。他のノードは、その論理スイッチに対する操作を一切実行しません。

論理スイッチと分散論理ルーターの情報は、1 台の所有者から提供される必要があるため、複数のノードが所有者として選出されてコントローラ クラスタが破損状態になると、ネットワーク内の各ホストは、その論理スイッチまたは分散論理ルーターに関して異なる情報を持つことになる可能性があります。このような事態になると、ネットワーク障害が発生します。ネットワーク制御とデータ プレーンでは、情報は 1 つしか許可されないためです。

あるコントローラ ノードが停止すると、クラスタ内の残りのノードがシャーディングを再実行して、論理スイッチと論理ルーティングの所有権を決定します。

## NSX Controller のデプロイに関する問題

NSX Controller は、NSX Manager によって OVA 形式でデプロイされます。コントローラ クラスタを使用することで高可用性が実現します。コントローラをデプロイするには、NSX Manager、vCenter Server、および ESXi ホストに DNS と NTP が設定されている必要があります。固定 IP アドレス プールを使用して、各コントローラに IP アドレスを割り当てる必要があります。

個々のホストで NSX Controller を保持できるように、DRS の非アフィニティ ルールを実装することをお勧めします。3 台の NSX Controller をデプロイする必要があります。

### コントローラの一般的な問題

NSX Controller をデプロイする際、次のような問題が発生する可能性があります。

- NSX Controller のデプロイが失敗する。
- NSX Controller がクラスタに参加できない。
- `show control-cluster status` コマンドを実行すると、Connected to cluster majority と Interrupted connection to cluster majority との間を Majority status がフラップする。
- NSX ダッシュボードに、接続ステータスに関する問題が表示される。
- `show control-cluster status` コマンドは、コントローラがコントロール クラスタに参加したかどうかを表示するための推奨コマンドです。このコマンドを各コントローラで実行し、クラスタ全体のステータスを確認する必要があります。

```
controller # show control-cluster status
Type                Status                                     Since
-----
Join status:        Join complete                               10/17 18:16:58
Majority status:    Connected to cluster majority                     10/17 18:16:46
Restart status:     This controller can be safely restarted              10/17 18:16:51
Cluster ID:         af2e9dec-19b9-4530-8e68-944188584268
Node UUID:          af2e9dec-19b9-4530-8e68-944188584268
```

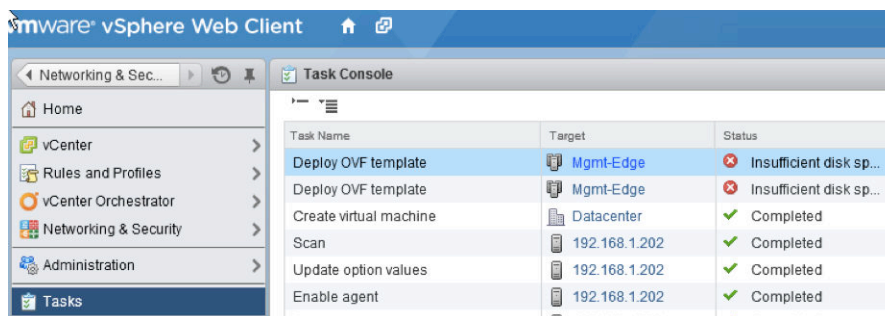
Role	Configured status	Active status
api_provider	enabled	activated
persistence_server	enabled	activated
switch_manager	enabled	activated
logical_manager	enabled	activated
dht_node	enabled	activated

**注：** コントローラ ノードが接続されていなくても、`join cluster` コマンドまたは `force join` コマンドは使用しないでください。これは、クラスタにノードを参加させるために設計されたコマンドではありません。これを実行すると、クラスタが不安定な状態になる可能性があります。

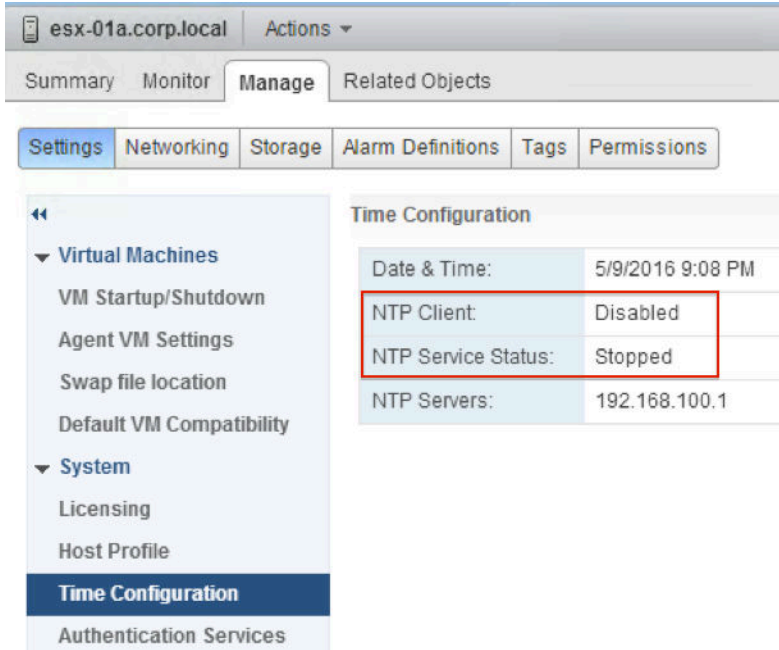
クラスタ起動ノードは、クラスタ メンバーが、起動した他のメンバーを確認するヒントにすぎません。このリストに、サービスを終了したクラスタ メンバーが含まれていても問題はありません。これはクラスタの機能には影響しません。

すべてのクラスタ メンバーに、同じクラスタ ID が割り当てられている必要があります。そうでない場合、クラスタは破損状態になるため、VMware のテクニカル サポートに相談して修復する必要があります。

- `show control-cluster startup-nodes` コマンドは、現在クラスタ内にあるすべてのノードを表示するには設計されていません。その代わりに、別のどのコントローラ ノードがこのノードで使用されていて、コントローラ プロセスが再起動したときにクラスタへのメンバーシップを自動で起動されるかが表示されます。そのため、コマンド出力には、シャットダウンしているノード、またはクラスタから除外された一部のノードが表示される場合があります。
- さらに、`show control-cluster network ipsec status` コマンドでは、ユーザーが IPsec (Internet Protocol Security) の状態を調べることができます。数分から数時間の間、コントローラ間で通信が行われない場合は、`cat /var/log/syslog | egrep "sending DPD request|IKE_SA"` コマンドを実行し、ログ メッセージでトラフィックが記録されていないことを確認してください。`ipsec statusall | egrep "bytes_i|bytes_o"` コマンドを実行して、IPsec トンネルが 2 つ確立されていないかを確認する方法もあります。コントロール クラスタで疑われる問題を VMware のテクニカル サポート担当者に報告する際は、これらのコマンドの出力とコントローラのログを提出してください。
- NSX Manager と NSX Controller の間の IP 接続の問題。これは、一般的に物理ネットワーク接続の問題、またはファイアウォールによる通信のブロックにより発生します。
- コントローラのホストに使用する、vSphere のストレージなどのリソースの不足。コントローラのデプロイ中に vCenter Server のイベントおよびタスクのログを確認することで、このような問題を特定できます。



- 適切に動作しない「問題のある」コントローラ、または [切断 (Disconnected)] 状態のアップグレード済みコントローラ。
- ESXi ホストおよび NSX Manager の DNS が適切に設定されていない。
- ESXi ホストと NSX Manager の NTP が同期されない。



- 新規に接続された仮想マシンがネットワークにアクセスできない場合は、制御プレーンで問題が発生している可能性があります。コントローラのステータスを確認します。

また、制御プレーンのステータスを確認するために、ESXi ホストで `esxcli network vswitch dvs vmware vxlan network list --vds-name <name>` コマンドを実行します。コントローラが切断されていることを確認します。

```
/etc/vmware/netcpa # esxcli network vswitch dvs vmware vxlan network list --vds-name Compute_VDS
VXLAN ID Multicast IP Control Plane
-----
5000 N/A (headend replication) Enabled (multicast proxy, ARP proxy) 192.168.110.203 (down)
```

- NSX Manager CLI コマンド `show log manager follow` を実行することで、コントローラのデプロイが失敗するその他の原因を特定できます。

```
2014-02-26 10:09:44.931 GMT INFO taskScheduler-25 VcConnection$VimClient:1219 - Create stub for com.vmware.vim.binding:
28c5157-abf3-718e-88c5-42209f389211
2014-02-26 10:09:44.932 GMT DEBUG VcEventsReaderThread VcEventsReader$VcEventsReaderThread:301 - got prop collector up
ctReference: type = PropertyFilter, value = session[d46b86a2-7a10-c17e-6ebe-8ab252ee4efd]527420f2-bdd7-529b-8ab6-17d16
6E3-4A64-96D7-5833C287588F
2014-02-26 10:09:44.937 GMT ERROR taskScheduler-25 VCUtils:184 - Error while waiting for property collector updates.
com.vmware.vim.binding.vim.fault.NoDiskSpace:
datastore = datastore1 (1)
inherited from com.vmware.vim.binding.vim.fault.FileFault:
file = [datastore1 (1)] NSX_Controller_1c3dd18d-0cd3-4d7d-896b-51247176ae77/NSX_Controller_1c3dd18d-0cd3-4d7d-896b-512
inherited from com.vmware.vim.binding.vim.fault.VimFault:
inherited from com.vmware.vim.binding.vim.fault.NoDiskSpace: Insufficient disk space on datastore 'datastore1 (1)'.
```

## ホスト接続の問題

次のコマンドを使用して、ホスト接続のエラーを確認します。これらのコマンドは、各コントローラ ノードで実行してください。

- `show log cloudnet/cloudnet_java-vnet-controller*.log filtered-by host_IP` コマンドを使用して、異常なエラーの統計情報を確認します。
- 以下のコマンドを使用して、論理スイッチ/ルーターのメッセージ統計情報または頻度の高いメッセージを確認します。
  - `show control-cluster core stats` : 全体の統計情報
  - `show control-cluster core stats-sample` : 最新の統計情報のサンプル
  - `show control-cluster core connection-stats ip` : 接続ごとの統計情報
  - `show control-cluster logical-switches stats`
  - `show control-cluster logical-routers stats`
  - `show control-cluster logical-switches stats-sample`
  - `show control-cluster logical-routers stats-sample`
  - `show control-cluster logical-switches vni-stats vni`
  - `show control-cluster logical-switches vni-stats-sample vni`
  - `show control-cluster logical-switches connection-stats ip`
  - `show control-cluster logical-routers connection-stats ip`
- `show host hostID health-status` コマンドを使用すると、準備済みクラスタにあるホストの健全性ステータスを確認できます。コントローラのトラブルシューティングでは、以下の健全性チェックがサポートされています。
  - `net-config-by-vsm.xml` がコントローラ リストと同期しているかどうかを確認する。
  - コントローラへのソケット接続があるかどうかを確認する。
  - VXLAN ネットワーク識別子 (VNI) が作成されていて、設定が正しいかどうかを確認する。
  - マスター コントローラへの VNI 接続を確認する (制御プレーンが有効な場合)。

## インストールとデプロイの問題

- クラスタに少なくとも 3 台のコントローラ ノードがデプロイされていることを確認します。VMware では、ネイティブの vSphere 非アフィニティ ルールを使用することで、同じ ESXi ホスト上に複数のコントローラ ノードをデプロイしないようにすることをお勧めしています。
- すべての NSX Controller に接続済みステータスが表示されていることを確認します。切断済みステータが表示されるコントローラ ノードがある場合は、すべてのコントローラ ノードで `show control-cluster status` コマンドを実行して、以下の情報が一貫していることを確認します。

タイプ	ステータス
Join status	参加完了
Majority status	クラスタ マジョリティに接続
Cluster ID	すべてのコントローラ ノードで同じ情報

- すべてのコントローラ ノードのすべてのロールが一貫していることを確認します。

ロール	設定されたステータス	アクティブ ステータス
api_provider	有効	アクティブ化
persistence_server	有効	アクティブ化
switch_manager	有効	アクティブ化
logical_manager	有効	アクティブ化
directory_server	有効	アクティブ化

- vnet-controller プロセスが実行中であることを確認します。すべてのコントローラ ノードで `show process` コマンドを実行し、`java-dir-server` サービスが実行中であることを確認します。
- クラスタ履歴を検証し、ホスト接続のフラッピング、VNI 参加の失敗、および異常なクラスタ メンバーシップの変更の兆候がないことを確認します。これを確認するには、`show control-cluster history` コマンドを実行します。このコマンドは、ノードが頻繁に再起動されるかどうかを示します。プロセス ID が異なる、サイズがゼロ (0) のログ ファイルが多数表示されないことを確認します。
- VXLAN ネットワーク識別子 (VNI) が設定されていることを確認します。詳細については、『VMware VXLAN Deployment Guide』の「VXLAN 準備手順」セクションを参照してください。
- SSL がコントローラ クラスタで有効になっていることを確認します。`show log cloudnet/cloudnet_java-vnet-controller*.log filtered-by sslEnabled` コマンドは、各コントローラ ノードで実行してください。

## ディスク遅延のトラブルシューティング

[管理 (Management)] タブでディスク遅延アラートを確認できます。NSX Controller は、遅延の小さいディスクで実行する必要があります。

### ディスク遅延アラートの表示

ディスク遅延アラートは、ディスクの可用性または遅延の問題を監視、報告します。ディスク遅延の詳細は、NSX Controller ごとに表示できます。読み取り遅延および書き込み遅延計算は、5 秒間 (デフォルト) 変動する平均は、順番に遅延制限に達したときにアラートをトリガーするために入力されました。平均が低しきい値を下まわるとアラートはオフになります。デフォルトで、高しきい値は 200 ミリ秒に設定され、低しきい値は 100 ミリ秒に設定されています。遅延が大きいと、各コントローラ ノードでの分散クラスタリング アプリケーションの動作に影響します。

NSX Controller のディスク遅延アラートを表示するには、次の手順を実行します。

#### 前提条件







遅延の上限に達しています。





## 手順

- 1 vSphere Web Client にログインします。
- 2 [Networking and Security (Networking & Security)] をクリックし、[インストール手順 (Installation)] をクリックします。
- 3 [管理 (Management)] にの下にある対象のコントローラに移動し、[ディスク アラート (Disk Alert)] リンクをクリックします。

[ディスク遅延アラート] ウィンドウが表示されます。

192.168.110.33 - Disk Latency Alerts				
Device Name	Latency Type	Refresh Time	Last Latency (ms)	Average Latency (ms)
 sda	Write	9/26/2016 2:15 PM	3.2	7.906
 sda	Read	9/26/2016 1:08 PM	0.0	0.0
 dm-1	Write	9/16/2016 5:11 PM	0.0	0.0
 dm-1	Read	9/22/2016 4:31 PM	0.0	0.0
 dm-0	Write	9/26/2016 2:15 PM	3.64	9.822
 dm-0	Read	9/26/2016 10:05 AM	0.0	33.334
6 items				

5	 Disk Alert	192.168.110.15	✓ Connected	 Disk Alert
---	--	----------------	-------------	--

## 結果

選択したコントローラの遅延に関する詳細を確認できます。アラート ログは `cloudnet/run/iostat/iostat_alert.log` ファイルに 7 日間保存されます。show log cloudnet/run/iostat/iostat\_alert.log コマンドを使用するとログ ファイルを表示できます。

## 次のステップ

ディスク遅延のトラブルシューティングに関する詳細については、[ディスク遅延の問題](#)を参照してください。

ログ メッセージの詳細については、「NSX のログ作成とシステム イベント」を参照してください。

## ディスク遅延の問題

コントローラは、遅延の小さいディスクで実行する必要があります。クラスタの各ノードのディスク ストレージ システムでは、ピーク時の書き込み遅延を 300 ミリ秒未満に、平均書き込み遅延を 100 ミリ秒未満にする必要があります。

### 問題

- デプロイした NSX Controller とコントローラ クラスタとの接続が切断されている。
- ディスク パーティションがいっぱいになっているため、コントローラ ログを収集できない。
- ストレージ システムがこれらの要件を満たしていない場合は、クラスタが不安定になり、システム停止の原因となる場合があります。
- 正常に機能する NSX Controller に適した TCP リスナーが、`show network connections of-type tcp` コマンドの出力に表示されなくなった。
- 切断されたコントローラが、オールゼロの UUID を使用してクラスタに参加しようとしている（この方法は無効）。

- `show control-cluster history` コマンドを実行すると、次のようなメッセージが表示される。

```
INFO.20150530-000550.1774:D0530 13:25:29.452639 1983 zookeeper_client.cc:774] Zookeeper
client disconnected!
```

- NSX Controller コンソールで `show log cloudnet/cloudnet_java-zookeeper*.log` コマンドを実行すると、次のようなエントリが表示される。

```
cloudnet_java-zookeeper.20150530-000550.1806.log-2015-05-30
13:25:07,382 47956539 [SyncThread:1] WARN
org.apache.zookeeper.server.persistence.FileTxnLog - fsync-ing the write ahead
log in SyncThread:1 took 3219ms which will adversely effect operation latency.
See the ZooKeeper troubleshooting guide
```

- NSX Controller のログに、次のようなエントリが表示される。

```
D0525 13:46:07.185200 31975
rpc-broker.cc:369] Registering address resolution for: 20.5.1.11:7777
D0525 13:46:07.185246 31975
rpc-tcp.cc:548] Handshake complete, both peers support the same
protocol
D0525 13:46:07.197654 31975
rpc-tcp.cc:1048] Rejecting a connection from peer
20.5.1.11:42195/ef447643-f05d-4862-be2c-35630df39060, cluster
9f7ea8ff-ab80-4c0c-825e-628e834aa8a5, which doesn't match our cluster
(00000000-0000-0000-0000-000000000000)
D0525 13:46:07.222869 31975
rpc-tcp.cc:1048] Rejecting a connection from peer
20.5.1.11:42195/ef447643-f05d-4862-be2c-35630df39060, cluster
9f7ea8ff-ab80-4c0c-825e-628e834aa8a5, which doesn't match our cluster
(00000000-0000-0000-0000-000000000000)
```

## 原因

この問題はディスクのパフォーマンス遅延が原因で発生します。これは NSX Controller クラスタに悪影響を及ぼします。

- `/var/log/cloudnet/cloudnet_java-zookeeper log` ファイルで `fsync` のメッセージを検索して、遅延が生じているディスクを確認してください。`fsync` が 1 秒を超える場合、Zookeeper は `fsync` の警告メッセージを表示し、これでディスクの大幅な遅延が発生していることがわかります。VMware では、遅延については論理ユニット番号 (LUN) をコントロール クラスタ専用にするか、ストレージ アレイをコントロール クラスタの近くに移動するか、またはその両方をお勧めしています。
- 読み取り遅延を表示し、5 秒間 (デフォルト) 変動する平均は、順番に遅延制限に達したときにアラートをトリガーするためには、入力された計算を書き込み遅延できます。平均が低しきい値を下まわるとアラートはオフになります。デフォルトで、高しきい値は 200 ミリ秒に設定され、低しきい値は 100 ミリ秒に設定されています。`show disk-latency-alert config` コマンドを使用できます。出力は次のように表示されます。

```
enabled=True    low-wm=51        high-wm=150
nsx-controller # set disk-latency-alert enabled yes
nsx-controller # set disk-latency-alert low-wm 100
nsx-controller # set disk-latency-alert high-wm 200
```

- `GET /api/2.0/vdn/controller/<controller-id>/systemStats` REST API を使用すると、コントローラ ノードの遅延アラート ステータスを取得できます。
- `GET /api/2.0/vdn/controller` REST API を使用すると、ディスク遅延アラートをコントローラ ノードで検出したかどうかを示すことができます。

## 解決方法

- 1 NSX Controller を低遅延ディスクにデプロイします。
- 2 コントローラはそれぞれ独自のディスク ストレージ サーバを使用する必要があります。2 台のコントローラで同じディスク ストレージ サーバを共有しないでください。

## 次のステップ

アラートの表示方法の詳細については、[ディスク遅延アラートの表示](#) を参照してください。

# NSX Controller クラスタの障害

クラスタ内のいずれかの NSX Controller ノードで障害が発生しても、正常に動作しているコントローラがまだ 2 つあります。クラスタの過半数が維持されているため、制御プレーンは機能し続けます。

## 問題

NSX Controller クラスタで障害が発生しました。

## 解決方法

- 1 vSphere Web Client にログインします。

- 2 [Networking and Security (Networking & Security)] で、[インストール手順 (Installation)] > [管理 (Management)] の順にクリックします。
- 3 [NSX Controller ノード] セクションで、[ピア] 列を確認します。[ピア] 列に緑色のボックスが表示された場合、クラスタ内のピア コントローラ接続にエラーがないことを示します。赤色のボックスは、ピアにエラーがあることを示します。ボックスをクリックして詳細を表示してください。
- 4 [ピア] 列に、コントローラ クラスタの問題が表示されたら、各 NSX Controller の CLI にログインして、詳細な診断を実行します。show control-cluster status コマンドを実行して、各コントローラの状態を診断してください。クラスタ内のすべてのコントローラは同じクラスタ UUID である必要がありますが、マスターコントローラの UUID と同じでなくてもかまいません。デブロイの問題については、[NSX Controller のデブロイに関する問題](#) を参照してください。
- 5 コントローラ ノードまたはコントローラ クラスタを再展開する前に、次の手順で問題の解決を試みてください。
  - a コントローラがパワーオン状態かどうかを確認します。
  - b 影響を受けるコントローラに対して、または影響を受けるコントローラから他のノードやマネージャに対して ping コマンドを実行し、ネットワーク パスを確認します。ネットワークの問題が見つかったら、[NSX Controller のデブロイに関する問題](#) の説明に従ってそれらの問題に対処します。
  - c 次の CLI コマンドを使用して、IPsec (Internet Protocol Security) のステータスを確認します。
    - show control-cluster network ipsec status コマンドを使用して、IPsec が有効かどうかを確認します。
    - show control-cluster network ipsec tunnels コマンドを使用して、IPsec トンネルのステータスを確認します。IPSec のステータス情報は、VMware のテクニカル サポートのチケットをオープンする際にも使用できます。
  - d ネットワークの問題でない場合は、再起動または再展開を選択できます。

ノードを再起動する場合、一度に再起動するのは 1 つのコントローラのみに行ってください。ただし、コントローラ クラスタで複数のコントローラ ノードが障害を起こしている場合は、すべてを同時に再起動します。良好なクラスタからノードを再起動する場合は、クラスタが正しく復元したことを再起動後に必ず確認し、再シャードイングが正しく行われたことを確認します。
- 6 コントローラを再展開する場合は、次のいずれかの方法で行います。
  - 方法 1：破損したコントローラ ノードを削除し、新しいコントローラ ノードを再展開する。
  - 方法 2：コントローラ クラスタを削除して、新しいコントローラ クラスタを再展開する。2 番目の方法をおすすめします。

#### 次のステップ

次のいずれかの方法を選択します。

- [方法 1：破損したコントローラを削除して新しいコントローラを再展開する](#)
- [方法 2：NSX Controller クラスタを再展開する](#)

## 方法 1：破損したコントローラを削除して新しいコントローラを再展開する

まず、新しい NSX Controller クラスタを再展開せずに問題の解決を試みます。この方法では、破損した NSX Controller ノードを削除してから、新しい NSX Controller ノードを展開します。

### 手順

#### 1 NSX Controller の削除

NSX Controller は、強制的に、または正常な手順で削除できます。正常な手順による削除では、ノードを削除する前に、次の状態であることが確認されます。

#### 2 NSX Controller の再デプロイ

破損したコントローラ ノードを削除したら、新しいコントローラ ノードを展開します。

### NSX Controller の削除

NSX Controller は、強制的に、または正常な手順で削除できます。正常な手順による削除では、ノードを削除する前に、次の状態であることが確認されます。

- NSX Controller ノードのアップグレード処理が実行中ではない。
- コントローラ クラスタが健全な状態であり、コントローラ クラスタ API 要求を処理できる。
- vCenter Server インベントリから取得したホスト状態が、接続済みでパワーオン状態であることを示している。
- 最後の 1 台のコントローラ ノードではない。

強制的な削除では、コントローラ ノードの削除前に、前述の状態を確認しません。

- コントローラを削除する際は、以下の点に注意してください。
  - vSphere Web Client のユーザー インターフェイスまたは API を使用してコントローラ仮想マシンを削除する前に、コントローラを削除しないでください。ユーザー インターフェイスが使用できない場合、DELETE /2.0/vdn/controller/{controllerId} API を使用してコントローラを削除します。
  - ノードの削除後は、既存のクラスタが安定していることを確認してください。
  - クラスタ内のノードをすべて削除する際、最後の 1 台のノードは [コントローラを強制的に削除します (Forcefully remove the controller)] オプションを使用して削除する必要があります。コントローラ仮想マシンの削除が成功したことを常に確認してください。成功しなかった場合、仮想マシンを手動でパワーオフし、ユーザー インターフェイスを使用してコントローラ仮想マシンを削除します。
  - 削除操作が失敗すると、仮想マシンは削除されません。そのような場合は、ユーザー インターフェイスの [コントローラを強制的に削除します (Forcefully remove the controller)] オプションを介してコントローラの削除を呼び出します。API の場合、forceRemove パラメータを *true* に設定します。強制的に削除した後、仮想マシンを手動でパワーオフし、ユーザー インターフェイスを使用してコントローラ仮想マシンを削除します。
  - マルチノード クラスタで許容されるのは 1 件の障害のみです。削除も 1 件の障害とカウントされます。削除されたノードは、別の障害が発生する前に再デプロイする必要があります。

## ■ Cross-vCenter NSX 環境の場合：

- vCenter Server では、コントローラ仮想マシンの削除、または直接的なパワーオフはサポートされません。  
[ステータス (Status)] 列には、[同期されていません (Out of sync)] と表示されます。
- コントローラの削除が部分的にのみ成功し、Cross-vCenter NSX 環境の NSX Manager データベースにエントリが残ってしまった場合は、DELETE api/2.0/vdn/controller/external API を使用してください。
- NSX Manager API を使用してコントローラがインポートされた場合は、forceRemoval オプションを指定した removeExternalControllerReference API を使用してください。
- コントローラを削除する場合、NSX は、仮想マシンの管理対象オブジェクト ID (MOID) を使用して、vCenter Server 経由でコントローラ仮想マシンの削除を要求します。vCenter Server が MOID で仮想マシンを見つけることができない場合、NSX は、コントローラ削除要求の失敗を通知し、処理を中止します。

[強制的に削除 (Forcefully Delete)] オプションを選択すると、NSX はコントローラの削除操作を中止せず、コントローラの情報をクリアします。NSX は、削除済みのコントローラを信頼しないように、すべてのホストを更新します。ただし、コントローラ仮想マシンがアクティブのままで、異なる MOID で実行される場合は、コントローラ クラスタのメンバーとして参加するための認証情報はそのまま保持されます。ESXi ホストは削除されたコントローラを信頼しないため、このシナリオでは、このコントローラ ノードに割り当てられている論理スイッチまたはルーターは適切に機能しません。

NSX Controller を削除するには、次の手順を実行します。

### 手順

- 1 vSphere Web Client にログインします。
- 2 [Networking and Security (Networking & Security)] をクリックし、[インストール手順 (Installation)] をクリックします。
- 3 [管理 (Management)] で、削除するコントローラを選択します。
- 4 [削除 (x) (Delete (x))] アイコンをクリックします。
- 5 [削除 (Delete)] または [強制的に削除 (Forcefully Delete)] を選択します。
  - ◆ [強制的に削除 (Forcefully Delete)] オプションを選択した場合、コントローラは正しい手順では削除されず、強制的に削除されます。このオプションは、発生した障害を無視し、データベースからデータを消去します。そのため、発生したと思われる障害は手動で対処する必要があります。コントローラ仮想マシンが正しく削除されたことを必ず確認してください。そうでない場合は、vCenter Server から削除する必要があります。

---

**注：** クラスタ内の最後の 1 台のコントローラを削除する場合は、[強制的に削除 (Forcefully Delete)] オプションを選択して削除する必要があります。システムにコントローラが存在なくなると、ホストはいわゆる「ヘッドレス」モードで動作します。新しい仮想マシンまたは vMotion で移動された仮想マシンは、新しいコントローラがデプロイされ同期が完了するまで、ネットワークの問題が発生した状態になります。

---

- ◆ これを選択しない場合、コントローラは正常な手順で削除されます。

- 6 [はい (Yes)] をクリックします。正常な手順による削除は、次の順序で行います。
  - a ノードをパワーオフします。
  - b クラスタの健全性を確認します。
  - c クラスタが健全な状態でない場合は、コントローラをパワーオンして、削除要求を破棄します。
  - d クラスタが健全な状態である場合は、コントローラ仮想マシンを削除し、ノードの IP アドレスを解放します。
  - e コントローラ仮想マシンの ID をクラスタから削除します。

選択したコントローラが削除されます。
- 7 [アクション (Actions)] > [コントローラ状態の更新 (Update Controller State)] の順にクリックして、コントローラの状態を再度同期します。

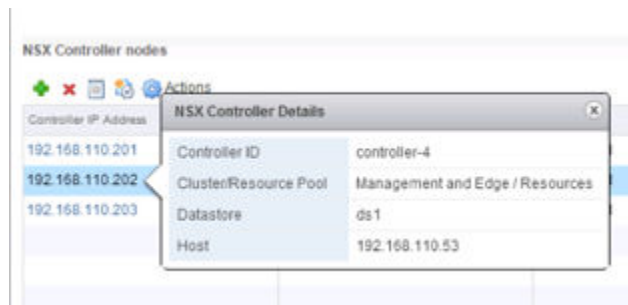
## NSX Controller の再デプロイ

破損したコントローラ ノードを削除したら、新しいコントローラ ノードを展開します。

### 手順

- 1 vSphere Web Client にログインします。
- 2 [Networking and Security (Networking & Security)] で、[インストール手順 (Installation)] > [管理 (Management)] の順にクリックします。
- 3 [NSX Controller ノード] セクションで、問題のコントローラをクリックします。後で参照できるように、[NSX Controller 詳細] 画面の構成情報をメモするか、そのスクリーンショットを作成しておきます。

次はその例です。



- 4 [ノードの追加 (+) (Add Node (+))] アイコンをクリックして、新しい NSX Controller ノードをデプロイします。
- 5 [コントローラの追加] ダイアログ ボックスで、ノードを追加するデータセンターを選択し、コントローラを設定します。
  - a 適切なクラスタを選択します。
  - b クラスタおよびストレージでホストを選択します。
  - c 分散ポートグループを選択します。

- d ノードに割り当てられる IP アドレス プールを選択します。
- e [OK] をクリックして、インストールが完了するまで待ちます。完了したら、ノードに [通常] ステータスが設定されていることを確認します。

コントローラ ノードの追加方法については、『NSX インストール ガイド』の「NSX Controller クラスタの展開」を参照してください。

- 6 [アクション]-[コントローラ状態の更新] の順にクリックして、コントローラの状態を再同期します。

コントローラ状態の更新によって、最新の VXLAN および分散論理ルーター設定（Cross-vCenter NSX 環境内のユニバーサル オブジェクトを含む）が、NSX Manager からコントローラ クラスタにプッシュされます。

## 方法 2：NSX Controller クラスタを再展開する

このアプローチでは、3 つのコントローラ ノードをすべて削除し、新しいコントローラ ノードを追加して、完全に機能する 3 ノード クラスタを維持します。

次のいずれかの条件に該当する場合は、NSX Controller クラスタの削除をおすすめします。

- 1 つ以上のコントローラ ノードで致命的なエラーまたはリカバリ不能なエラーが発生している。
- コントローラ仮想マシンにアクセスできないため、修正できない。

このような場合は、コントローラ ノードの一部が良好な状態に見えても、すべてのコントローラ ノードを削除することをおすすめします。

新しいコントローラ クラスタを再展開し、NSX Manager でコントローラの状態メカニズムを更新します。コントローラの状態を更新すると、VXLAN が再同期され、分散論理ルーターが再展開されます。

### 手順

- 1 vSphere Web Client にログインします。
- 2 [ネットワークとセキュリティ]-[インストール]-[管理] の順に移動します。
- 3 [NSX Controller ノード] セクションで、3 つのコントローラ ノードをすべて削除します。一度に 1 つのノードを選択して、[削除] (✖) アイコンをクリックします。

システムにコントローラが存在しない場合、ホストはヘッドレス モードで動作します。新しい仮想マシンまたは移行された仮想マシンは、新しいコントローラが展開されて同期が完了するまで、ネットワークの問題が発生した状態になります。

- 4 3 つの新しいコントローラ ノードを展開して、完全に機能する NSX Controller クラスタを作成します。

コントローラ クラスタの追加方法については、『NSX インストール ガイド』の「NSX Controller クラスタの展開」を参照してください。

- 5 [アクション]-[コントローラ状態の更新] の順にクリックして、コントローラの状態を再同期します。

## ファントム コントローラ

ファントム コントローラは存在しない仮想マシン (VM) とは限りません。実行中のコントローラ仮想マシンがファントム コントローラになることもあります。また、クラスタに参加している場合も、参加していない場合もあります。NSX Manager は、vCenter Server インベントリ内のすべての仮想マシンのリストを同期します。vCenter



Server またはホストが NSX Manager からの要求以外でコントローラ仮想マシンを削除したり、vCenter Server インベントリがコントローラ仮想マシンのリファレンス MOID（管理対象オブジェクト ID）を変更すると、ファントム コントローラが作成されます。

コントローラが NSX から作成されると、設定情報は NSX Manager 内に保存されます。NSX Manager は、vCenter Server を介して新しいコントローラ仮想マシンをデプロイします。

NSX の管理者は、コントローラを作成するときに、IP アドレス プールなどの設定情報を NSX Manager に提供します。vCenter Server に仮想マシンの作成要求が送信されると、NSX Manager は、プールから IP アドレスを削除し、この IP アドレスを残りのコントローラの設定情報と一っしょにプッシュします。NSX Manager は、vCenter Server が要求のステータスを確認するまで待機します。

- The controller creation process was successful: コントローラ仮想マシンが正常に作成されると、vCenter Server がコントローラ仮想マシンを起動します。NSX Manager は、仮想マシンの管理対象オブジェクト ID (MOID) と残りのコントローラの設定情報を保存します。MOID（または MO-REF）は、vCenter Server がインベントリ内のオブジェクトに割り当てて一意の識別子です。vCenter Server インベントリに残っている場合、vCenter Server は、この MOID を使用して仮想マシンを追跡します。
- The controller creation process was not successful: IP アドレスとネットワーク接続の設定に誤りがあると、NSX Manager は vCenter Server に接続できません。NSX Manager は、1 つのノード コントローラ クラスタ（最初のクラスタ）の作成または実行中のクラスタに参加する新しいコントローラの作成を、事前に設定された期間待機します。タイマーが切れると、NSX Manager は仮想マシンの削除を vCenter Server に要求します。IP アドレスがプールに戻され、NSX がコントローラの作成失敗を宣言します。

## ファントム コントローラが作成される仕組み

NSX Manager がコントローラの削除を要求すると、vCenter Server は MOID を使用して、削除対象のコントローラ仮想マシンを検索します。

ただし、vCenter Server のアクティビティで vCenter Server インベントリからコントローラ仮想マシンが削除されると、vCenter Server はこの MOID をデータベースから削除します。vCenter Server のインベントリから削除された後も、NSX Manager ではコントローラ仮想マシンが稼動しています。ただし、vCenter Server には、コントローラ仮想マシンは表示されません。vCenter Server がインベントリから仮想マシンを削除しても、仮想マシン自体は削除されていない可能性があります。仮想マシンが実行中の場合、NSX コントローラ クラスタに参加しているか、参加を試行している場合があります。

ファントム コントローラが作成される最も典型的な例は次のとおりです。

- vCenter Server の管理者がインベントリからコントローラ仮想マシンのホスト削除します。このホストは後に再度追加します。ホストが削除されると、vCenter Server がホストとその仮想マシンに関連付けられているすべての MOID を削除します。同じホストを再度追加すると、vCenter Server は、ホストと仮想マシンに新しい MOID を割り当てます。NSX のユーザーから見ると、ホストと仮想マシンは以前と変わりませんが、vCenter Server から見ると、このホストと仮想マシンは新しいオブジェクトとなります。実際には、ホストも仮想マシンも削除前と変わりません。ホストと仮想マシンで実行されるアプリケーションも変わりません。
- vCenter Server の管理者が、vCenter Server またはホストの管理を使用して、コントローラ仮想マシンを削除します。この削除は、NSX Manager が開始したものではありません。
- このような削除には、ホストやストレージの障害で仮想マシンが消失するケースも含まれます。この場合、仮想マシンが vCenter Server から切断され、クラスタと NSX Manager に対する接続も失われます。この削除は

NSX Manager が開始したものでないため、NSX Manager とコントローラ クラスタは、コントローラがまだ有効な状態だと認識します。NSX Manager には、コントローラ ノードが停止し、クラスタの一部ではなくなり、ユーザー インターフェイスに表示されないことを示すステータスが返されます。また、NSX Manager のログには、コントローラが到達不能であることが記録されます。

## ファントム コントローラが表示された場合の対処方法

- 1 **NSX Controller が切断された**の説明に従って、コントローラを同期します。
- 2 ログ エントリを確認します。コントローラ仮想マシンが誤って削除された場合または破損している場合は、[強制的に削除 (Forcefully Delete)] オプションを使用して NSX Manager データベースからエントリをクリアする必要があります。詳細については、**NSX Controller の削除**を参照してください。
- 3 コントローラを削除したら、次のことを確認します。
  - コントローラ仮想マシンが実際に削除されている。
  - `show controller-cluster startup-nodes` コマンドを使用して、有効なコントローラのみを表示する。
  - NSX Manager の Syslog エントリに、不要なコントローラが含まれていない。

NSX 6.2.7 以降では、NSX Manager が元の MOID に基づいて、vCenter Server のインベントリにコントローラ仮想マシンが残っているかどうか確認します。NSX Manager がインベントリでコントローラ仮想マシンを検出できない場合、NSX Manager は仮想マシンのインスタンス UUID を使用して仮想マシンを検索します。インスタンス UUID は仮想マシン内に保存されているため、vCenter Server のインベントリに仮想マシンが追加されても変更されません。NSX Manager が該当のインスタンス UUID を持つ仮想マシンを検出すると、NSX Manager は新しい MOID でデータベースを更新します。

ただし、コントローラ仮想マシンのクローンを作成する場合、クローン作成された仮想マシンは新しいインスタンス UUID を持ち、元の仮想マシンと同じプロパティが設定されます。NSX Manager は、クローン作成された仮想マシンの MOID を検出できません。

## ファントム コントローラのログ エントリ

ファントム コントローラを検出すると、ログに次のエラー レベルのエントリが記録されます。

- 2017-07-31 22:15:05.844 UTC ERROR NVPStatusCheck ControllerServiceImpl:2146 - Controller <#> does not exist, might be deleted already. Skip saving its connectivity info.
- 2017-07-31 22:15:05.769 UTC ERROR NVPStatusCheck ControllerServiceImpl:2580 - the node is created by this NSX Manager <#>, but database has no record and delete might be in progress.

## NSX Controller が切断された

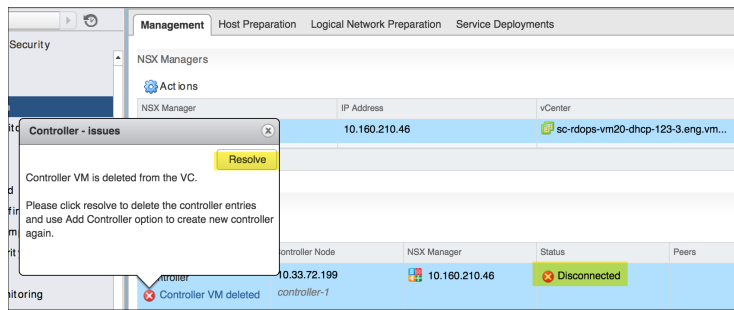
NSX Controller 仮想マシンが vCenter Server からパワーオフされた場合、またはコントローラ仮想マシンが vCenter Server から削除された場合、[インストール手順 (Installation)] > [管理 (Management)] ページの [ステータス (Status)] 列には、[同期なし (Out of sync)] ステータスが表示されます。

## 前提条件

コントローラ仮想マシンがパワーオフ状態である、またはコントローラ仮想マシンが vCenter Server から削除されています。

## 手順

- 1 vSphere Web Client で、[Networking and Security (Networking & Security)] - [インストール手順 (Installation)] > [管理 (Management)] の順に選択します。



- 2 [エラー (Error)] リンクをクリックして、非同期状態の詳しい原因を確認します。
- 3 [解決 (Resolve)] ボタンをクリックして、問題を解決します。

## 結果

コントローラ仮想マシンがパワーオフ状態の場合、管理プレーンによって、コントローラに対する power on コマンドが発行されます。

コントローラ仮想マシンが削除されると、コントローラのエントリは管理プレーンから削除され、管理プレーンはコントローラが削除されたことを中央制御プレーンに伝えます。

## 次のステップ

[ノードの追加 (Add Node)] オプションを使用して新しいコントローラを作成します。詳細については、『NSX 管理ガイド』を参照してください。

# 制御プレーン エージェント (netcpa) の問題

NSX for vSphere では、制御プレーン エージェント (netcpa) がローカル エージェント デーモンとして動作し、NSX Manager およびコントローラ クラスタと通信します。[通信チャネルの健全性 (Communication Channel Health)] 機能は、中央制御プレーンからローカル制御プレーンへのステータスを NSX Manager に定期的にレポートするプロアクティブな健全性チェックで、NSX Manager のユーザー インターフェイスに表示されます。このレポートは、NSX Manager から ESXi ホスト netcpa チャンネルへの稼働ステータスを検出する、ハートビートとしても機能します。この機能は、通信障害時のエラーの詳細を示し、チャンネルが誤ったステータスになるとイベントを生成するほか、NSX Manager からホストへのハートビート メッセージを生成します。

## 問題

制御プレーン エージェントとコントローラ間の接続の問題

## 原因

見つからない接続がある場合は、制御プレーン エージェントが正しく動作していない可能性があります。

## 解決方法

- 1 チャネルが誤ったステータスになったら、次のコマンドを使用して接続ステータスを確認します。

```
GET https://<NSX_Manager_IP>/api/2.0/vdn/inventory/host/{hostId}/connection/status
```

以下は戻り値の例です。

```
<?xml version="1.0" encoding="UTF-8"?>
<hostConnStatus>
<hostName>10.161.246.20</hostName>
<hostId>host-21</hostId>
<nsxMgrToFirewallAgentConn>UP</nsxMgrToFirewallAgentConn>
<nsxMgrToControlPlaneAgentConn>UP</nsxMgrToControlPlaneAgentConn>
<hostToControllerConn>DOWN</hostToControllerConn>
<fullSyncCount>-1</fullSyncCount>
<hostToControllerConnectionErrors>
<hostToControllerConnectionError>
<controllerIp>10.160.203.236</controllerIp>
<errorCode>1255604</errorCode>
<errorMessage>Connection Refused</errorMessage>
</hostToControllerConnectionError>
<hostToControllerConnectionError>
<controllerIp>10.160.203.237</controllerIp>
<errorCode>1255603</errorCode>
<errorMessage>SSL Handshake Failure</errorMessage>
</hostToControllerConnectionError>
</hostToControllerConnectionErrors>
</hostConnStatus>
```

次のエラー コードがサポートされています。

1255602:不完全なコントローラ証明書 1255603:SSL ハンドシェークに失敗しました 1255604:接続が拒否されました 1255605:キープ アライブ タイムアウト 1255606:SSL 例外 1255607:不正なメッセージ 1255620:不明なエラー

- 2 次のように、制御プレーン エージェントが停止している原因を特定します。

- a ESXi ホストで `/etc/init.d/netcpad status` コマンドを実行して、ホストの制御プレーン エージェントのステータスを確認します。

```
[root@esx-01a:~] /etc/init.d/netcpad status
netCP agent service is running
```

- b `more /etc/vmware/netcpa/config-by-vsm.xml` コマンドを使用して、制御プレーン エージェントの設定を確認します。NSX Controller の IP アドレスが表示されます。

```
[root@esx-01a:~] more /etc/vmware/netcpa/config-by-vsm.xml
<config>
  <connectionList>
```

```

<connection id="0000">
  <port>1234</port>
  <server>192.168.110.31</server>
  <sslEnabled>true</sslEnabled>
  <thumbprint>A5:C6:A2:B2:57:97:36:F0:7C:13:DB:64:9B:86:E6:EF:1A:7E:5C:36</thumbprint>
</connection>
<connection id="0001">
  <port>1234</port>
  <server>192.168.110.32</server>
  <sslEnabled>true</sslEnabled>
  <thumbprint>12:E0:25:B2:E0:35:D7:84:90:71:CF:C7:53:97:FD:96:EE:ED:7C:DD</thumbprint>
</connection>
<connection id="0002">
  <port>1234</port>
  <server>192.168.110.33</server>
  <sslEnabled>true</sslEnabled>
  <thumbprint>BD:DB:BA:B0:DC:61:AD:94:C6:0F:7E:F5:80:19:44:51:BA:90:2C:8D</thumbprint>
</connection>
</connectionList>
...

```

- 3 次のコマンドを使用して、制御プレーン エージェントからコントローラへの接続を検証します。各コントローラにつき 1 つの接続が出力されます。

```

>[root@esx-01a:~] esxcli network ip connection list | grep 1234
tcp      0    0  192.168.110.51:16594      192.168.110.31:1234      ESTABLISHED      36754  newreno
netcpa-worker
tcp      0    0  192.168.110.51:46917      192.168.110.33:1234      ESTABLISHED      36754  newreno
netcpa-worker
tcp      0    0  192.168.110.51:47891      192.168.110.32:1234      ESTABLISHED      36752  newreno
netcpa-worker

```

- 4 次のコマンドを使用して、制御プレーン エージェントからコントローラへの接続を検証し、CLOSED または CLOSE\_WAIT ステータスを表示します。

```

esxcli network ip
  connection list |grep "1234.*netcpa*" | egrep "CLOSED|CLOSE_WAIT"

```

- 5 制御プレーン エージェントが長時間にわたって停止している場合は、接続が存在していない可能性があります。これを検証するには、次のコマンドを実行します。各コントローラにつき 1 つの接続が出力されます。

```

esxcli network ip
  connection list |grep "1234.*netcpa*" |grep ESTABLISHED

```

- 6 制御プレーン エージェント (netcpa) の自動リカバリ メカニズム：制御プレーン エージェントの自動モニタリング プロセスは、誤ったステータスの制御プレーン エージェントを検出します。制御プレーン エージェント ステータスが正しくない場合、応答を停止し、自動リカバリを試みます。

- a 制御プレーン エージェントが応答を停止すると、ライブ コア ファイルが生成されます。このコア ファイルを次の方法で確認できます。

```
ls /var/core
netcpa-worker-zdump.000
```

- b *vmkwarning.log* ファイルに Syslog エラーがレポートされます。

```
cat /var/run/log/vmkwarning.log | grep NETCPA
2017-08-11T06:32:17.994Z cpu1:1000044539)ALERT: Critical - NETCPA is hanged
Taking live-dump & restarting netcpa process!
```

---

**注：** ステータス チェックの応答遅延により制御プレーン エージェント モニターで一時的な障害が発生すると、VMKernel ログに次のような警告メッセージがレポートされる場合があります。

```
Warning - NETCPA getting netcpa status failed!
```

この警告は無視しても問題ありません。

---

- 7 この問題から自動的に回復しない場合は、次のように制御プレーン エージェントを再起動します。

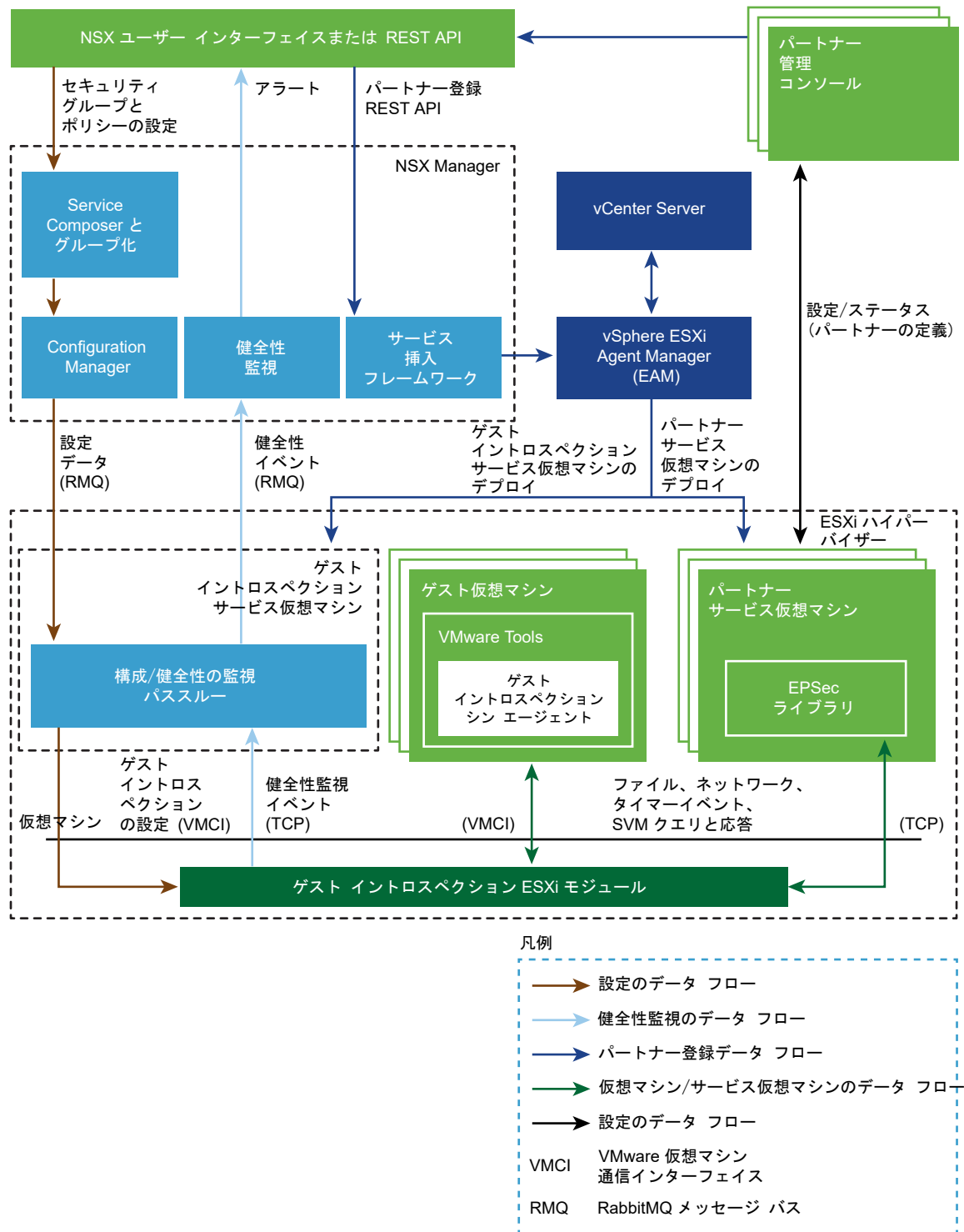
- a SSH またはコンソールを介して、ESXi ホストに root でログインします。
- b `/etc/init.d/netcpad restart` コマンドを実行して、ESXi ホストで制御プレーン エージェントを再起動します。

# ゲスト イントロスペクションのトラブルシューティング

この章には、次のトピックが含まれています。

- [ゲスト イントロスペクションのアーキテクチャ](#)
- [ゲスト イントロスペクションのログ](#)
- [ゲスト イントロスペクション環境とワークロードの詳細情報の収集](#)
- [Linux または Windows でのシン エージェントのトラブルシューティング](#)
- [ESX ゲスト イントロスペクション モジュール \(MUX\) のトラブルシューティング](#)
- [EPSecLib のトラブルシューティング](#)

## ゲスト イントロスペクションのアーキテクチャ



## ゲスト イントロスペクションのログ

ゲスト イントロスペクションのトラブルシューティングで、複数のログをキャプチャして使用できます。



## ESX ゲスト イントロスペクション モジュール (MUX) のログ

ESXi ホスト上の仮想マシンでゲスト イントロスペクションを使用していない場合、またはホストでサービス仮想アプライアンスとの通信に関するアラームが発生している場合は、ESXi ホスト上の ESX ゲスト イントロスペクション モジュールに問題がある可能性があります。

### ログのパスとサンプル メッセージ

#### MUX ログのパス

/var/log/syslog

var/run/syslog.log

ESX ゲスト イントロスペクション モジュール (MUX) のメッセージは、  
<timestamp>EPSecMUX<[ThreadID]>: <message> の形式で記録されます。

次はその例です。

```
2017-07-16T05:44:49Z EPSecMux[38340669]: [ERROR] (EPSEC) [38340669]
Attempted to recv 4 bytes from sd 49, errno = 104 (Connection reset by peer)
```

上記の例で

- [ERROR] はメッセージのタイプです。他のタイプとしては、[DEBUG]、[INFO] があります。
- (EPSEC) は、エンドポイント セキュリティに関連するメッセージであることを意味します。

### ログ作成の有効化とログの表示

ホストにインストールされている ESX ゲスト イントロスペクション モジュール VIB のバージョンを表示するには、`#esxcli software vib list | grep epsec-mux` コマンドを実行します。

完全なログ作成を有効にするには、ESXi ホストのコマンド シェルで次の手順を実行します。

- 1 `ps -c | grep Mux` コマンドを実行して、現在実行中の ESX ゲスト イントロスペクション モジュールを検索します。

次はその例です。

```
~ # ps -c | grep Mux
192223 192223 sh /bin/sh /sbin/watchdog.sh -s vShield-Endpoint-Mux -q 100 -t 1000000 /usr/lib/
vmware/vShield-Endpoint-Mux 900 -c 910
192233 192233 vShield-Endpoint-Mux /usr/lib/vmware/vShield-Endpoint-Mux 900 -c 910
192236 192233 vShield-Endpoint-Mux /usr/lib/vmware/vShield-Endpoint-Mux 900 -c 910
```

- 2 サービスが実行されていない場合、`/etc/init.d/vShield-Endpoint-Mux start` または `/etc/init.d/vShield-Endpoint-Mux restart` コマンドを実行すると、サービスを再起動できます。
- 3 `watchdog.sh` プロセスなど、実行中の ESX ゲスト イントロスペクション モジュールのプロセスを停止するには、`~ # kill -9 192223 192233 192236` コマンドを実行します。

ESX ゲスト イントロスペクション モジュールの 2 つのプロセスが生成されています。

- 4 新しい `-d` オプションを使用して ESX ゲスト イントロスペクション モジュールを開始します。epsec-mux ビルド 5.1.0-01255202 と 5.1.0-01814505 の ~ # `/usr/lib/vmware/vShield-Endpoint-Mux -d 900 -c 910` には `-d` オプションがありません。
- 5 ESXi ホストの `/var/log/syslog.log` ファイルで、ESX ゲスト イントロスペクション モジュールのログ メッセージを確認します。グローバル ソリューション、ソリューション ID、ポート番号に対応するエントリが正しく指定されていることを確認します。

### 例： muxconfig.xml ファイルのサンプル

```
<?xml version="1.0" encoding="UTF-8"?>

<EndpointConfig>

  <InstalledSolutions>

    <Solution>

      <id>100</id>

      <ipAddress>xxx.xxx.xxx.xxx</ipAddress>

      <listenOn>ip</listenOn>

      <port>48655</port>

      <uuid>42383371-3630-47b0-8796-f1d9c52ab1d0</uuid>

      <vmxPath>/vmfs/volumes/7adf9e00-609186d9/EndpointService (216)/EndpointService (216).vmx</vmxPath>

    </Solution>

    <Solution>

      <id>102</id>

      <ipAddress>xxx.xxx.xxx.xxx</ipAddress>

      <listenOn>ip</listenOn>

      <port>48651</port>

      <uuid>423839c4-c7d6-e92e-b552-79870da05291</uuid>

      <vmxPath>/vmfs/volumes/7adf9e00-609186d9/apoon/EndpointSVM-alpha-01/EndpointSVM-alpha-01.vmx</vmxPath>

    </Solution>

    <Solution>

      <id>6341068275337723904</id>
```

```
<ipAddress>xxx.xxx.xxx.xxx</ipAddress>

<listenOn>ip</listenOn>

<port>48655</port>

<uuid>42388025-314f-829f-2770-a143b9cbd1ee</uuid>

<vmxPath>/vmfs/volumes/7adf9e00-609186d9/DlpService (1)/DlpService (1).vmx</vmxPath>

</Solution>

</InstalledSolutions>

<DefaultSolutions/>

<GlobalSolutions>

  <solution>

    <id>100</id>

    <tag></tag>

    <order>0</order>

  </solution>

  <solution>

    <id>102</id>

    <tag></tag>

    <order>10000</order>

  </solution>

  <solution>

    <id>6341068275337723904</id>

    <tag></tag>

    <order>10001</order>

  </solution>

</GlobalSolutions>

</EndpointConfig>
```

## ゲスト イントロスペクション シン エージェントのログ

シン エージェントは、仮想マシンのゲスト OS にインストールされ、ユーザー ログインの詳細を検出します。

### ログのパスとサンプル メッセージ

シン エージェントは、ゲスト イントロスペクション ドライバの vsepflt.sys、vnetflt.sys、vnetwfp.sys (Windows 10 以降) で構成されます。

シン エージェントのログは、vCenter Server のログ バンドルの一部として、ESXi ホストに保存されます。ログのパスは、/vmfs/volumes/<datastore>/<vmname>/vmware.log です。例： /vmfs/volumes/5978d759-56c31014-53b6-1866abaace386/Windows10-(64-bit)/vmware.log

シン エージェントのメッセージは、<timestamp> <VM Name><Process Name><[PID]>: <message> の形式で記録されます。

以下の Guest: vnet or Guest:vsep のログの例では、ゲスト イントロスペクション ドライバ関連のログ メッセージの後にデバッグ メッセージが続きます。

次はその例です。

```
2017-10-17T14:25:19.877Z| vcpu-0| I125: Guest: vnet: AUDIT: DriverEntry :
vnetFilter build-4325502 loaded
2017-10-17T14:25:20.282Z| vcpu-0| I125: Guest: vsep:
AUDIT: VFileSocketMgrConnectHelper : Mux is connected
2017-10-17T14:25:20.375Z| vcpu-0| I125:
Guest: vsep: AUDIT: DriverEntry : vfileFilter build-4286645 loaded

2017-10-17T18:22:35.924Z| vcpu-0| I125: Guest: vsep: AUDIT:
VFileSocketMgrConnectHelper : Mux is connected
2017-10-17T18:24:05.258Z| vcpu-0| I125: Guest: vsep: AUDIT:
VFileFltPostOpCreate : File (\Windows\System32\Tasks\Microsoft\Windows\
SoftwareProtectionPlatform\SvcRestartTask) in a transaction, ignore
```

### 例：vShield ゲスト イントロスペクション シン エージェント ドライバのログ作成を有効にする

デバッグを設定すると、vmware.log ファイルがいっぱいになり、調整（スロットル）が行われる可能性があります。このため、必要な情報をすべて収集したらすぐにデバッグ モードを無効にすることをお勧めします。

この手順では、Windows レジストリを変更する必要があります。レジストリを変更する前に、レジストリのバックアップを行ってください。レジストリのバックアップとリストアの詳細については、Microsoft 社のナレッジベースの記事 [136393](#) を参照してください。

シン エージェント ドライバのデバッグ ログの作成を有効にするには：

- 1 [スタート(Start)] > [ファイル名を指定して実行(Run)] の順にクリックします。regedit と入力して、[OK] をクリックします。レジストリ エディターのウィンドウが開きます。詳細については、Microsoft 社のナレッジベースの記事 [256986](#) を参照してください。
- 2 レジストリ エディターで HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\services\vsepflt\parameters キーを作成します。

- 新しく作成したパラメータ キーの下に、次の DWORD を作成します。これらの値を入力するときに、16 進数が選択されていることを確認します。

```
Name: log_dest
Type: DWORD
Value: 0x2

Name: log_level
Type: DWORD
Value: 0x10
```

log\_level パラメータ キーの他の値：

```
Audit 0x1
Error 0x2
Warn 0x4
Info 0x8
Debug 0x10
```

- 管理者としてコマンド プロンプトを開きます。次のコマンドを実行して、vShield Endpoint ファイル システム ミニドライバをアンロードし、再ロードします。

- fltmc unload vsepflt
- fltmc load vsepflt

仮想マシンにある vmware.log ファイルでログ エントリを確認できます。

## vShield ゲスト イントロスペクション ネットワーク イントロスペクション ドライバのログ インを有効にする

デバッグを設定すると、vmware.log ファイルがいっぱいになり、調整が行われる可能性があります。このため、必要な情報をすべて収集したらすぐにデバッグ モードを無効にすることをお勧めします。

この手順では、Windows レジストリを変更する必要があります。レジストリを変更する前に、レジストリのバックアップを行ってください。レジストリのバックアップとリストアの詳細については、Microsoft 社のナレッジベースの記事 [136393](#) を参照してください。

- [スタート(Start)] > [ファイル名を指定して実行(Run)] の順にクリックします。regedit と入力して、[OK] をクリックします。レジストリ エディターのウィンドウが開きます。詳細については、Microsoft 社のナレッジベースの記事 [256986](#) を参照してください。
- レジストリを編集します。

```
Windows Registry Editor Version 5.0
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\vnetflt\Parameters]
"log_level" = DWORD: 0x0000001F
"log_dest" = DWORD: 0x00000001
```

- 仮想マシンを再起動します。

## vseft.sys と vnetflt.sys のログ ファイルの場所

レジストリで log\_dest が DWORD: 0x00000001 に設定されているため、エンドポイント シン エージェント ドライバのログがデバッガに出力されます。デバッガ (SysInternals の DbgView または windbg) を実行します。

あるいは、レジストリで log\_dest を DWORD:0x000000002 に設定することもできます。この場合、ドライバ ログは vmware.log に出力されます。このファイルは、ESXi ホストの該当する仮想マシンのフォルダに保存されます。

## UMC のログ作成を有効にする

ゲスト イントロスペクション ユーザー モード コンポーネント (UMC) は、保護対象の仮想マシンの VMware Tools サービス内で実行されます。

- 1 Windows XP または Windows Server 2003 で、C:\Documents and Settings\All Users\Application Data\VMware\VMware Tools\tools.conf に tools config ファイルが見つからない場合、このファイルを作成します。
- 2 Windows Vista、Windows 7 または Windows Server 2008 で、C:\ProgramData\VMware\VMware Tools\tools.conf に tools config がみつからない場合、このファイルを作成します。
- 3 次の行を tools.conf ファイルに追加して、ユーザー モード コンポーネントのロギングを有効にします。

```
[logging]
log = true
vsep.level = debug
vsep.handler = vmx
```

vsep.handler = vmx が設定されているため、ユーザー モード コンポーネントのログは vmware.log に出力されます。このファイルは、ESXi ホストで該当する仮想マシンのフォルダにあります。

次の設定を行うと、指定したログ ファイルにユーザー モード コンポーネントのログが出力されます。

```
vsep.handler = file
vsep.data = c:/path/to/vsep.log
```

## ゲスト イントロスペクション EPSecLib とサービス仮想マシンのログ

EPSecLib は、ESXi ホストの ESX ゲスト イントロスペクション モジュール (MUX) からイベントを受信します。

### ログのパスとサンプル メッセージ

#### EPSecLib のログのパス

/var/log/syslog

var/run/syslog

EPSecLib メッセージは、<timestamp> <VM Name><Process Name><[PID]>: <message> の形式で記録されます。

この例の [ERROR] はメッセージのタイプを表し、(EPSEC) は、ゲスト イントロスペクション関連のメッセージであることを表しています。

次はその例です。

```
Oct 17 14:26:00 endpoint-virtual-machine EPSecTester[7203]: [NOTICE] (EPSEC)
[7203] Initializing EPSec library build: build-00000

Oct 17 14:37:41 endpoint-virtual-machine EPSecSample: [ERROR] (EPSEC) [7533] Event
terminated reading file. Ex: VFileGuestEventTerminated@tid=7533: Event id: 3554.
```

## ログの収集

ゲスト イントロスペクション サービス仮想マシン内にあるコンポーネントの EPSec ライブラリでデバッグ ログを有効にするには：

- 1 NSX Manager からのコンソールのパスワードを取得して、ゲスト イントロスペクション サービス仮想マシンにログインします。
- 2 `/etc/epseclib.conf` ファイルを作成して、次の項目を追加します。  
  
`ENABLE_DEBUG=TRUE`  
  
`ENABLE_SUPPORT=TRUE`
- 3 `chmod 644 /etc/epseclib.conf` コマンドを実行して権限を変更します。
- 4 `/usr/local/sbin/rcusvm restart` コマンドを実行して、ゲスト イントロスペクション サービス仮想マシンを再起動します。

これにより、ゲスト イントロスペクション サービス仮想マシンで EPSecLib のデバッグ ログが有効になります。NSX for vSphere 6.2.x と 6.3.x の場合、デバッグ ログは `/var/log/messages` に保存されます。デバッグを設定すると、`vmware.log` ファイルがいっぱいになり、調整が行われる可能性があります。このため、必要な情報をすべて収集したらすぐにデバッグ モードを無効にすることをお勧めします。

## ゲスト イントロスペクション サービス仮想マシンのログ

ログをキャプチャする前に、ホスト ID またはホストの MOID を確認します。

- NSX Manager で `show cluster all` コマンドと `show cluster <cluster ID>` コマンドを実行します。

次はその例です。

```
nsxmgr-01a> show cluster all
```

No.	Cluster Name	Cluster Id	Datacenter Name	Firewall Status
1	RegionA01-COMP01	domain-c26	RegionA01	Enabled
2	RegionA01-MGMT01	domain-c71	RegionA01	Enabled

```
nsxmgr-01a> show cluster domain-c26

Datacenter: RegionA01
```

Cluster: RegionA01-COMP01

No.	Host Name	Host Id	Installation Status
1	esx-01a.corp.local	host-29	Ready
2	esx-02a.corp.local	host-31	Ready

- 現在のログの状態を確認するには、次のコマンドを実行します。

```
GET https://nsxmanager/api/1.0/usvmlogging/host-##/com.vmware.vshield.usvm
```

```
GET https://nsxmanager/api/1.0/usvmlogging/host-##/root
```

- 現在のログの状態を変更するには、次のコマンドを実行します。

```
POST https://nsxmanager/api/1.0/usvmlogging/host-##/changelevel
```

## Example to change root logger ##

```
<?xml version="1.0" encoding="UTF-8" ?>
<logginglevel>
<loggerName>root</loggerName>
<level>DEBUG</level>
</logginglevel>
```

## Example to change com.vmware.vshield.usvm ##

```
<?xml version="1.0" encoding="UTF-8" ?>
<logginglevel>
<loggerName>com.vmware.vshield.usvm</loggerName>
<level>DEBUG</level>
</logginglevel>
```

- ログを生成するには、次のコマンドを実行します。

```
GET https://NSXMGR_IP/api/1.0/hosts/host.###/techsupportlogs
```

Send と Download を選択します。

このコマンドを実行すると、ゲスト イントロスペクション サービス仮想マシンのログが生成され、techsupportlogs.log.gz という名前で保存されます。デバッグを設定すると、vmware.log ファイルがいっぱいになり、調整が行われる可能性があります。このため、必要な情報をすべて収集したらすぐにデバッグ モードを無効にすることをお勧めします。

## ゲスト イントロスペクション環境とワークロードの詳細情報の収集

コンポーネントの互換性の確認する場合、環境の詳細情報が役立ちます。

- NSX ゲスト イントロスペクションがユーザー環境で使用されているかどうかを確認します。使用されていない場合は、仮想マシンのゲスト イントロスペクション サービスを削除し、問題が解決したかどうかを確認します。
- 環境の詳細情報を収集します。
  - ESXi ビルド バージョン: ESXi ホストで `uname -a` コマンドを実行します。あるいは、vSphere Web Client でホストをクリックして、右側のペインの上部にあるビルド番号を検索します。
  - Linux の製品バージョンとビルド番号



- c `/usr/sbin/vsep -v` を実行すると、本番環境のバージョンを確認できます。

```
Build number
-----
Ubuntu
dpkg -l | grep vmware-nsx-gi-file
SLES12 and RHEL7
rpm -qa | grep vmware-nsx-gi-file
```

### 3 VMware NSX ® for vSphere ® のバージョンと次の情報：

- パートナー ソリューションの名前とバージョン番号
  - パートナー ソリューションが使用している EPSec ライブラリのバージョン番号： ゲスト イントロスペクション サービス仮想マシンにログインして、`#strings path to EPSec library/libEPSec.so | grep BUILD` を実行します。
  - 仮想マシンのゲスト オペレーティング システム
  - その他のサードパーティ アプリケーションまたはファイル システム ドライバ
- 4 ESX ゲスト イントロスペクション モジュール (MUX) のバージョン： `esxcli software vib list | grep epsec-mux` コマンドを実行します。
  - 5 サーバのタイプなどのワークロードの詳細を収集します。
  - 6 ESXi ホストのログを収集します。詳細については、[Collecting diagnostic information for VMware ESX/ESXi \(653\)](#)を参照してください。
  - 7 パートナー ソリューションのサービス仮想マシン (GI SVM) のログを収集します。ゲスト イントロスペクション サービス仮想マシンのログ収集の詳細については、パートナーに確認してください。
  - 8 問題が発生している間に、サスペンド状態のファイルを収集します。診断情報の収集については、[Suspending a virtual machine on ESX/ESX \(2005831\)](#)を参照してください。
  - 9 データを収集した後に、vSphere コンポーネントの互換性を比較します。詳細については、[VMware 製品互換性マトリクス](#)を参照してください。

## Linux または Windows でのシン エージェントのトラブルシューティング

ゲスト イントロスペクション シン エージェントは、各ゲスト仮想マシンに VMware Tools ™ とともにインストールされます。

## Linux でのシン エージェントのトラブルシューティング

仮想マシンでの読み取り/書き込み処理、ファイルの解凍または保存に時間がかかる場合は、シン エージェントに問題がある可能性があります。

- 1 関連するすべてのコンポーネントの互換性を確認します。互換性は、エンドポイントの主な問題の 1 つです。ESXi、vCenter Server、NSX Manager のビルド番号、選択したセキュリティ ソリューション（Trend Micro、McAfee、Kaspersky、Symantec など）の情報が重要です。このデータを収集して、vSphere コンポーネントの互換性を比較します。詳細については、[VMware 製品互換性マトリクス](#)を参照してください。
- 2 システムにファイル イントロスペクションがインストールされていることを確認します。
- 3 `service vsep status` コマンドを実行して、シン エージェントが実行されていることを確認します。このコマンドを実行すると、vsep サービスの実行状態が表示されます。
- 4 システムのパフォーマンス問題の原因がシン エージェントにあると思われる場合は、`service vsep stop` コマンドを実行してサービスを停止します。
- 5 テストを実行して、ベースラインを取得します。vsep サービスを開始した後で、`service vsep start` コマンドで別のテストを実行できます。
- 6 Linux シン エージェントのデバッグを有効にします。
  - a `/etc/vsep/vsep.conf` ファイルを開きます。
  - b すべてのログで `DEBUG_LEVEL=4` を `DEBUG_LEVEL=7` に変更します。
  - c ログのレベルを中程度にする場合は、`DEBUG_LEVEL=6` に設定します。
  - d デフォルトのログの出力先 (`DEBUG_DEST=2`) はホスト上の `vmware.log` です。ゲスト（例：`/var/log/message` または `/var/log/syslog`）に変更するには、`DEBUG_DEST=1` に設定します。

---

**注：** 完全なログ作成を有効にすると、ログの記録が過剰になり、`vmware.log` ファイルのサイズが非常に大きくなる可能性があります。完全なログ作成は、できるだけ早く無効にしてください。

---

## Windows でのシン エージェントのトラブルシューティング

- 1 関連するすべてのコンポーネントの互換性を確認します。ESXi、vCenter Server、NSX Manager のビルド番号、選択したセキュリティ ソリューション（Trend Micro、McAfee、Kaspersky、Symantec など）の情報が重要です。このデータをすべて収集して、vSphere コンポーネントの互換性を比較します。詳細については、[VMware 製品互換性マトリクス](#)を参照してください。
- 2 VMware Tools ™ が最新であることを確認します。特定の仮想マシンのみが影響を受ける場合は、[Installing and upgrading VMware Tools in vSphere \(2004754\)](#)を参照してください。
- 3 Powershell コマンド `fltmc` を実行して、シン エージェントがロードされていることを確認します。  
このコマンドを実行すると、ドライバのリストに「vsepflt」が表示されます。ドライバがロードされていない場合は、`fltmc load vsepflt` コマンドでドライバをロードできます。
- 4 システムのパフォーマンス問題の原因がシン エージェントにある場合には、`fltmc unload vsepflt` コマンドを実行してドライバをアンロードします。

次に、テストを実行して、ベースラインを取得します。ドライバをロードし、次のコマンドを実行して、別のテストを実行します。

```
fltmc load vsepflt.
```

シン エージェントにパフォーマンスの問題があるかどうか確認する方法については、[Slow VMs after upgrading VMware tools in NSX and vCloud Networking and Security \(2144236\)](#)を参照してください。

- 5 ネットワーク イントロスペクションを使用していない場合は、このドライバを削除するか、無効にします。  
VMware Tools インストーラの変更メニューでもネットワーク イントロスペクションを削除できます。
  - a VMware Tools インストーラをマウントします。
  - b [コントロール パネル(Control Panel)] > [プログラムと機能(Programs and Features)] の順に移動します。
  - c 右クリックして、[VMware Tools] > [変更(Modify)] の順に選択します。
  - d [完全インストール (Complete install)] を選択します。
  - e NSX ファイル イントロスペクションを検索します。ネットワーク イントロスペクションのサブフォルダにあります。
  - f [ネットワーク イントロスペクション (Network Introspection)] を無効にします。
  - g 仮想マシンを再起動して、ドライバのアンインストールを完了します。
- 6 シン エージェントのデバッグ ログを有効にします。詳細については、[ゲスト イントロスペクションのログ](#)を参照してください。すべてのデバッグ情報がその仮想マシンの vmware.log ファイルに記録されます。
- 7 procmon ログを確認して、シン エージェントのファイル スキャンを確認します。詳細については、[Troubleshooting vShield Endpoint performance issues with anti-virus software \(2094239\)](#)を参照してください。

## 環境およびワークロードの詳細を収集します。

- 1 NSX ゲスト イントロスペクションがユーザー環境で使用されているかどうかを確認します。使用されていない場合は、仮想マシンのゲスト イントロスペクション サービスを削除し、問題が解決したかどうかを確認します。ゲスト イントロスペクションが必要な場合にのみ、ゲスト イントロスペクションのトラブルシューティングを行います。
- 2 環境の詳細情報を収集します。
  - a ESXi ビルド バージョン： ESXi ホストで `uname -a` コマンドを実行します。あるいは、vSphere Web Client でホストをクリックして、右側のペインの上部にあるビルド番号を検索します。
  - b Linux の製品バージョンとビルド番号
  - c `/usr/sbin/vsep -v` を実行すると、本番環境のバージョンを確認できます。

```
Build number
```

```
-----
```

```

Ubuntu
dpkg -l | grep vmware-nsx-gi-file
SLES12 and RHEL7
rpm -qa | grep vmware-nsx-gi-file

```

### 3 VMware NSX® for vSphere® のバージョンと次の情報：

- パートナー ソリューションの名前とバージョン番号
- パートナー ソリューションが使用している EPSec ライブラリのバージョン番号： サービス仮想マシンにログインして、`#strings path to EPSec library/libEPSec.so | grep BUILD` を実行します。
- 仮想マシンのゲスト オペレーティング システム
- その他のサードパーティ アプリケーションまたはファイル システム ドライバ

### 4 ESX ゲスト イントロスペクション モジュール (MUX) のバージョン： `esxcli software vib list | grep epsec-mux` コマンドを実行します。

### 5 サーバのタイプなどのワークロードの詳細を収集します。

### 6 ESXi ホストのログを収集します。詳細については、[Collecting diagnostic information for VMware ESX/ESXi \(653\)](#)を参照してください。

### 7 パートナー ソリューションのサービス仮想マシン (SVM) のログを収集します。サービス仮想マシンのログ収集の詳細については、パートナーに確認してください。

### 8 問題が発生している間に、サスペンド状態のファイルを収集します。診断情報の収集については、[Suspending a virtual machine on ESX/ESX \(2005831\)](#)を参照してください。

## シン エージェントのクラッシュのトラブルシューティング

シン エージェントがクラッシュすると、/directory にコア ファイルが生成されます。location/directory からコア ダンプ ファイル (コア) を収集します。file コマンドを使用して、vsep によってコアが生成されているかどうかを確認します。次はその例です。

```

# file core
core: ELF 64-bit LSB core file x86-64, version 1 (SYSV), SVR4-style, from '/usr/sbin/vsep'

```

## 仮想マシンが停止またはフリーズする

サスペンド状態の仮想マシンの VMware vmss ファイルを収集します。[Suspending a virtual machine on ESX/ESXi to collect diagnostic information \(2005831\)](#) を参照するか、仮想マシンをクラッシュさせて完全なメモリ ダンプ ファイルを収集してください。VMware では、ESXi vmss ファイルをコア ダンプ ファイルに変換するユーティリティを提供しています。詳細については、[Vmss2core fling](#) を参照してください。

## ESX ゲスト イントロスペクション モジュール (MUX) のトラブルシューティング

## ESX ゲスト イントロスペクション モジュール (MUX)

ESXi ホスト上のすべての仮想マシンでゲスト イントロスペクションが機能していない場合、またはホストでゲスト イントロスペクションと SVA との通信に関するアラームが発生している場合は、ESXi ホスト上の ESX ゲスト イントロスペクション モジュールに問題がある可能性があります。

- 1 `# /etc/init.d/vShield-Endpoint-Mux status` コマンドを実行して、ESXi ホストでサービスが実行されているかどうかを確認します。

次はその例です。

```
# /etc/init.d/vShield-Endpoint-Mux status
vShield-Endpoint-Mux is running
```

- 2 サービスが実行されていない場合は、次のコマンドでサービスを再起動または開始します。

```
/etc/init.d/vShield-Endpoint-Mux start
```

または

```
/etc/init.d/vShield-Endpoint-Mux restart
```

このサービスの再起動は数秒で完了し、大きな影響を及ぼすこともないため、本番稼動中に行うほうが安全です。

- 3 ESX ゲスト イントロスペクション モジュールの処理内容や通信の状況を確認するには、ESXi ホスト上のログを確認します。ESX ゲスト イントロスペクション モジュールのログは、ホストの `/var/log/syslog` ファイルに書き込まれます。これは、ESXi ホストのサポート ログにも含まれています。

詳細については、[Collecting diagnostic information for ESX/ESXi hosts and vCenter Server using the vSphere Web Client \(2032892\)](#) を参照してください。

- 4 ESX ゲスト イントロスペクション モジュールのデフォルトのログ オプションは「情報」ですが、「デバッグ」に引き上げると、より多くの詳細を収集できます。

詳細については、[ゲスト イントロスペクションのログ](#)を参照してください。

- 5 ESX ゲスト イントロスペクション モジュールを再インストールすると、多くの問題が解決する場合があります。特に、間違ったバージョンがインストールされている場合や、以前にエンドポイントがインストールされていた環境に ESXi ホストが配置された場合には、問題が解決される可能性があります。この操作を行うには、削除と再インストールが必要になります。

VIB を削除するには、`esxcli software vib remove -n epsec-mux` コマンドを実行します。

- 6 VIB のインストールの問題を確認する場合は、ESXi ホストの `/var/log/esxupdate.log` ファイルを確認します。このログには、ドライバが正常にインストールされなかった理由など、明確な説明が記録されます。これは、ESX ゲスト イントロスペクション モジュールのインストールに関する一般的な問題です。詳細については、[Installing NSX Guest Introspection services \(ESX GI Module VIB\) on the ESXi host fails in VMware NSX for vSphere 6.x \(2135278\)](#)を参照してください。

- 7 ESXi イメージが破損しているかどうかを確認するには、次のようなメッセージを検索します。

```
esxupdate: esxupdate: ERROR: Installation Error:
(None, 'No image profile is found on the host or image profile is empty.
An image profile is required to install or remove VIBs. To install an image profile,
use the esxcli image profile install command.')
```

- 8 イメージが破損しているかどうかを確認するには、ESXi ホストで `cd /vmfs/volumes` コマンドを実行します。

- a `find * | grep imgdb.tgz` コマンドを実行して、imgdb.tgz ファイルを検索します。

このコマンドでは、通常、2 つ検索されます。次はその例です。

```
0ca01e7f-cc1ea1af-bda0-1fe646c5ceea/imgdb.tgz または edbf587b-
da2add08-3185-3113649d5262/imgdb.tgz
```

- b それぞれで `ls -l match_result` コマンドを実行します。

次はその例です。

```
> ls -l 0ca01e7f-cc1ea1af-bda0-1fe646c5ceea/imgdb.tgz -rwx-----
1 root root 26393 Jul 20 19:28 0ca01e7f-cc1ea1af-bda0-1fe646c5ceea/imgdb.tgz
> ls -l edbf587b-da2add08-3185-3113649d5262/imgdb.tgz -rwx-----
1 root root 93 Jul 19 17:32 edbf587b-da2add08-3185-3113649d5262/imgdb.tgz
```

imgdb.tgz ファイルのデフォルトのサイズは、他のファイルよりも大幅に大きくなります。ファイルのサイズが数バイトの場合は、ファイルが破損しています。この問題を解決するには、該当する ESXi ホストで ESXi を再インストールします。他の方法での解決はサポートされていません。

## EPSecLib のトラブルシューティング

この仮想マシンは、NSX Manager がデプロイします。

### EPSecLib

以前 (vShield を使用) は、サード パーティのセキュリティ仮想アプライアンス (SVA) ソリューションがデプロイしていました。現在、SVA ソリューションは NSX Manager に接続します。そして、NSX Manager が SVA をデプロイします。環境で SVA のアラームが発生した場合、NSX Manager を通じて再デプロイしてください。

- NSX Manager で構成されるため、これまでの設定はすべて失われます。
- SVA 仮想マシンは、再起動するのではなく、再デプロイすることをおすすめします。
- NSX は、ESX Agent Manager (EAM) を使用して、SVA などのホストで VIB とサービス仮想マシンの展開と監視を行います。
- EAM は、インストール ステータスを判断するための情報を提供します。
- NSX のユーザー インターフェイス (UI) では、インストール ステータスとして、VIB のインストール状態またはサービス仮想マシンのパワーオン状態のみを表示します。
- NSX ユーザー インターフェイスのサービス ステータスは、仮想マシンの機能が動作しているかどうかを示します。

## SVA のデプロイおよび NSX と vCenter Server のプロセスの関係

- 1 エンドポイントの準備のためにクラスタを選択すると、SVA をデプロイする EAM にエージェンシーが作成されます。
- 2 その後 EAM は、作成されたエージェンシーの情報がある ESXi ホストに ovf を展開します。
- 3 NSX Manager が、EAM による ovf の展開を確認します。
- 4 NSX Manager は、EAM によって仮想マシンがパワーオンされたことを確認します。
- 5 NSX Manager はパートナーの SVA Solution Manager と通信して、仮想マシンがパワーオン状態で、登録されたことを伝達します。
- 6 EAM が NSX にイベントを送信し、インストールの完了を通知します。
- 7 パートナーの SVA Solution Manager が NSX にイベントを送信し、SVA 仮想マシン内のサービスが起動し、実行中であることを通知します。
- 8 SVA で問題が発生した場合は、ログで 2 つの箇所を確認します。EAM がこれらの仮想マシンのデプロイを処理しているため、EAM のログを確認できます。詳細については、[Collecting diagnostic information for VMware vCenter Server 4.x, 5.x and 6.0 \(1011641\)](#) を参照してください。または、SVA のログを確認してください。詳細については、[ゲスト イントロスペクションのログ](#)を参照してください。
- 9 SVA 環境に問題がある場合は、EAM と NSX Manager との通信に問題が発生している可能性があります。EAM のログを確認します。最も簡単な方法は、EAM サービスを再起動することです。詳細については、[ホストの準備](#)を参照してください。
- 10 上記のすべてに問題はないが、エンドポイントの機能をテストしたい場合は、Eicar テスト ファイルを使用してテストできます。
  - 任意のラベルで新しいテキスト ファイルを作成します。例：eicar.test
  - ファイルに次の文字列のみをコピーします。  
X50!P%@AP[4\PZX54(P^)7CC)7}\$EICAR-STANDARD-ANTIVIRUS-TEST-FILE! \$H+H\*
  - ファイルを保存します。保存すると、ファイルが削除されます。これは、Endpoint ソリューションの正常な動作です。