

NSX トラブルシューティング ガイド

Update 2

変更日：2016 年 8 月 18 日

VMware NSX Data Center for vSphere 6.2



vmware®

VMware Web サイトで最新の技術ドキュメントをご確認いただけます。

<https://docs.vmware.com/jp/>

VMware の Web サイトでは、最新の製品アップデートを提供しています。

本書に関するご意見、ご要望をお寄せください。フィードバック送信先：

docfeedback@vmware.com

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
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

Copyright © 2010 – 2017 VMware, Inc. All rights reserved. [著作権および商標](#).

内容

- 1 NSX トラブルシューティング ガイド 4
- 2 インフラストラクチャの準備 5
 - NSX インフラストラクチャの準備手順 7
 - 通信チャネルの健全性の確認 20
 - NSX Manager の問題のトラブルシューティング 21
 - NSX コントローラ障害からのリカバリ 23
 - NSX ダッシュボードの使用 25
 - show host health-status コマンドの使用 27
 - NSX コンポーネントのログ レベルの設定 27
 - vSphere ESX Agent Manager 29
 - NSX CLI 参考用資料 31
- 3 トレースフロー 42
 - トレースフローについて 42
 - トラブルシューティングのためのトレースフローの使用 44
- 4 NSX のルーティング 52
 - 分散論理ルーターの理解 53
 - Edge Services Gateway によって提供されるルーティングの理解 57
 - ECMP パケットフロー 57
 - NSX のルーティングの前提条件と考慮事項 59
 - 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 62
 - 新しい NSX Edge (分散論理ルーター) 64
 - 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 68
 - NSX のルーティングのトラブルシューティング 72
- 5 Edge Appliance のトラブルシューティング 104
- 6 分散ファイアウォール 118
 - show dfw CLI の使用方法 118
 - Distributed Firewall のトラブルシューティング 120
- 7 ロード バランシング 127
 - シナリオ：ワンアーム ロード バランサの構成 128
 - ユーザー インターフェイスを使用したロード バランサのトラブルシューティング 133
 - 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 134
 - 一般的なロード バランサの問題 137

NSX トラブルシューティング ガイド

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、および必要に応じて NSX のほかのコンポーネントを使用して、VMware NSX™ 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 をインストールまたは使用する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。また、本書は VMware ESX、vCenter Server、vSphere Web Client を含む VMware Infrastructure 5.x についての知識も前提としています。

VMware の技術ドキュメントの用語集

VMware の技術ドキュメントには、新しい用語などを集約した用語集があります。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。

インフラストラクチャの準備

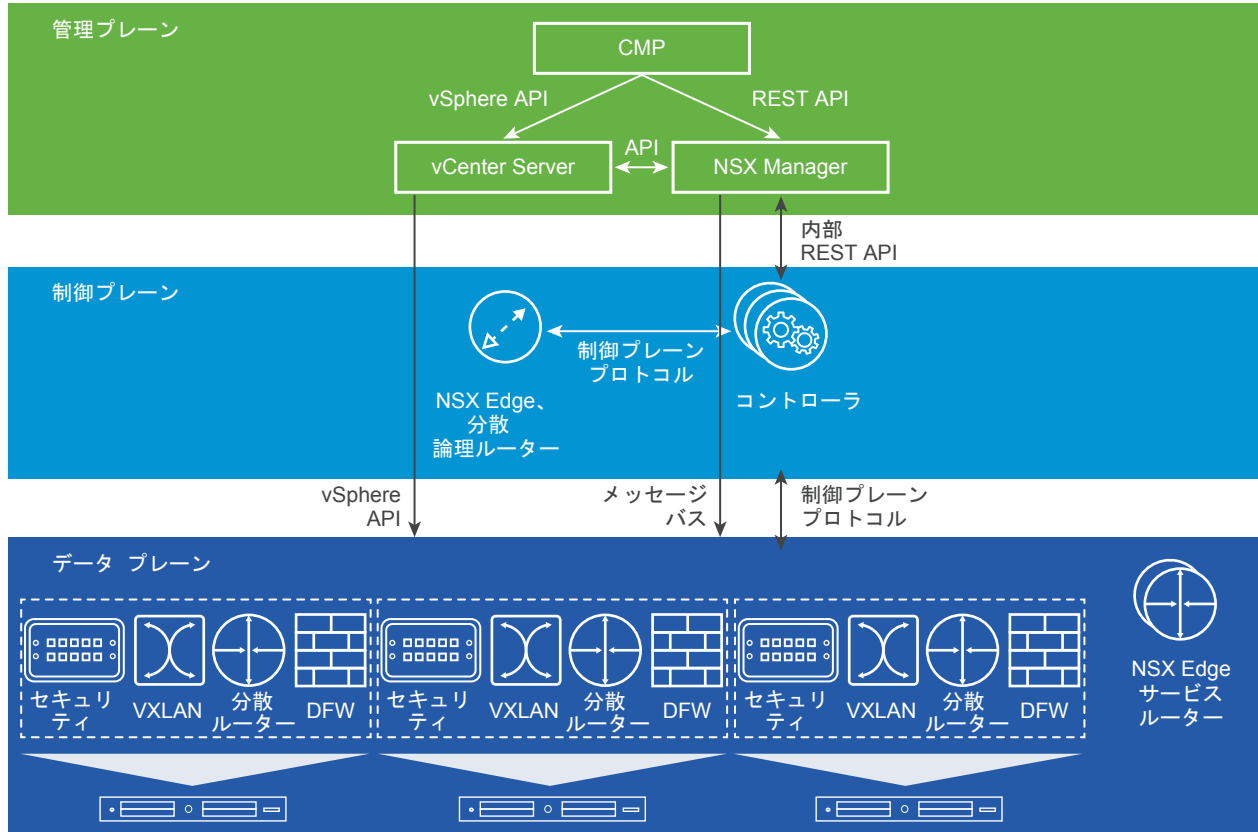
NSX の準備で使用されるコンポーネントを理解しておくことは、一般的な問題を特定し解決するために重要です。

NSX インフラストラクチャを準備するためのコンポーネント

- vSphere ESX Agent Manager (EAM)
- NSX Manager
- コントローラ クラスタ（ユニキャストを使用している場合、ハイブリッド モードまたは分散論理ルーティング）
- VTEP（ESXi ハイパーバイザー）
- ユーザー ワールド エージェント (UWA)
- vSphere Distributed Switch

NSX Manager と ESXi ハイパーバイザー ホスト間の制御プレーンの通信は、RabbitMQ ベースのメッセージングサービスによって提供されます。コントローラ クラスタと ESXi ハイパーバイザー ホスト間の制御プレーンの通信は、クライアントとしてホストで実行される netcpa ユーザー ワールド エージェントに依存します。

図 2-1. コンポーネントとその通信の概要ビュー



インフラストラクチャの準備を成功させるためのヒント

VMware 製品の相互運用性マトリックスの Web サイトでは、NSX の互換性と、バージョンの要件についての情報を提供しています。http://partnerweb.vmware.com/comp_guide2/sim/interop_matrix.php を参照してください。

バージョン 5.5 以降の vSphere Distributed Switch を使用していることを確認してください。

管理、サービス、およびゲートウェイには別々の分散仮想スイッチを使用します。

ブレードを使用する場合は、NIC チーミングの方法を慎重に選択してください。シャーシのスイッチは、最低限の機能のみがサポートされています。

インストール時には、ホストの準備を進める前に、コントローラ クラスタが展開され、すべての状態が正しいことを確認してください。

アップグレードする前にコントローラが接続されており、すべての状態が正しいことを確認します。『NSX アップグレードガイド』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。

- [NSX インフラストラクチャの準備手順](#)
- [通信チャネルの健全性の確認](#)
- [NSX Manager の問題のトラブルシューティング](#)

- [NSX コントローラ障害からのリカバリ](#)
- [NSX ダッシュボードの使用](#)
- [show host health-status コマンドの使用](#)
- [NSX コンポーネントのログ レベルの設定](#)
- [vSphere ESX Agent Manager](#)
- [NSX CLI 参考用資料](#)

NSX インフラストラクチャの準備手順

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 コントローラをデプロイします。これは、論理スイッチ、分散ルーティング、または Edge サービスでのみ必要です。Distributed Firewall (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、DFW、および DLR 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構成します。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。

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。ESXi ホストを名前別に vSphere インベントリに追加した場合は、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。機能していない場合、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。

また、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。

最初に vCenter Server にログインするときに、NSX Manager を vCenter Server にリンクするために使用したユーザー アカウントを使用する必要があります。その後、[vCenter Server ホーム (vCenter Home)] > [Networking and Security (Networking & Security)] > [NSX Manager (NSX Managers)] > {NSX Manager の IP} > [管理 (Manage)] > [ユーザー (Users)] の API を使用して、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

接続を検証するには、NSX 仮想アプライアンスから ping を実行し、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 ViInventoryThread ViInventory: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.vimomi.client.exception.ConnectionException: org.apache.http.conn.HttpHostConnectException: Connection to ht

```

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。

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 CSR : 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。

NSX コントローラのデプロイ

NSX コントローラは、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 コントローラ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。

NSX コントローラは、3 個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 コントローラをデプロイする際、次のような一般的な問題が発生する可能性があります。

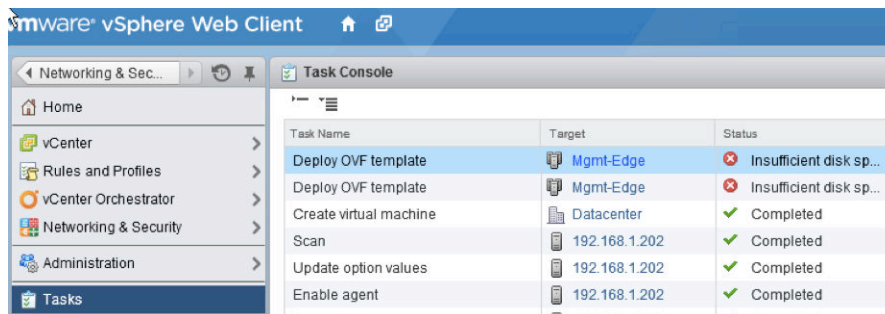
- NSX コントローラの実行が遅い。これは、リソース不足が原因で発生することがあります。NSX コントローラのシステム要件に関する問題を検出するには、**request system compatibility-report** コマンドを実行します。

```
nsx-controller # request system compatibility-report
Testing: Number of CPUs. Done.
Testing: Aggregate CPU speed. Done.
Testing: Memory. Done.
Testing: Management NIC speed. Done.
Testing: NTP configured. Done.
Testing: /var disk partition size. Done.
Testing: /var disk speed. Done.
Testing: pserver-log disk size. Done.
Testing: pserver-log disk speed. Done.
Testing: pserver-data disk size. Done.
Testing: pserver-data disk speed. Done.
Testing: logging disk size. Done.
```

Testing: logging disk speed. Done.

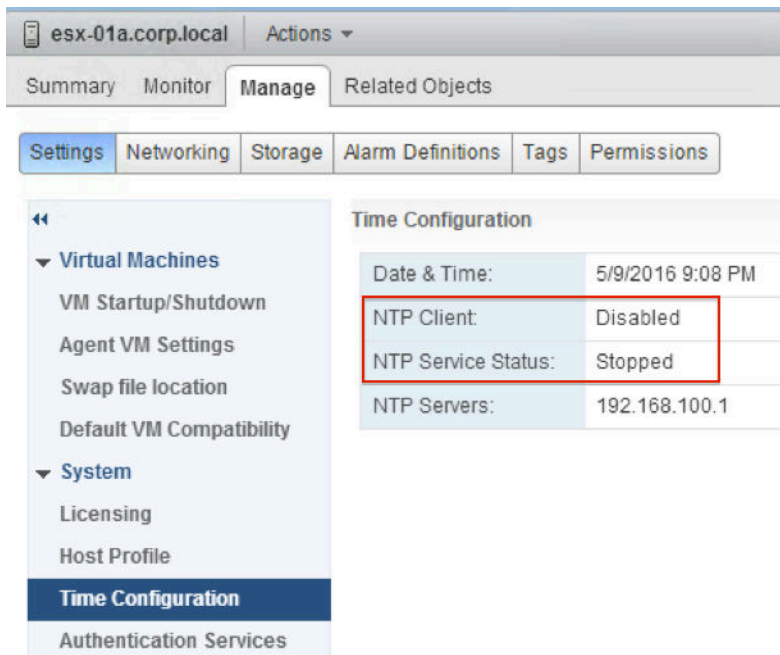
	Detected	Supported	Required
Number of CPUs	2	NO	>=8
Aggregate CPU speed	5.6 GHz	NO	>=13
Memory	1.835 GB	NO	>=63
Management NIC speed	10000 Mb/s	YES	>=1000
NTP configured	No	NO	Yes
/var disk partition size	- GB	NO	>=128
/var disk speed	- MB/s	NO	>=40
pserver-log disk size	- GB	NO	>=128
pserver-log disk speed	- MB/s	NO	>=40
pserver-data disk size	- GB	NO	>=128
pserver-data disk speed	- MB/s	NO	>=40
logging disk size	- GB	NO	>=128
logging disk speed	- MB/s	NO	>=40

- NSX Manager と NSX コントローラの間 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。
- vSphere がコントローラをホストするために使用する、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。

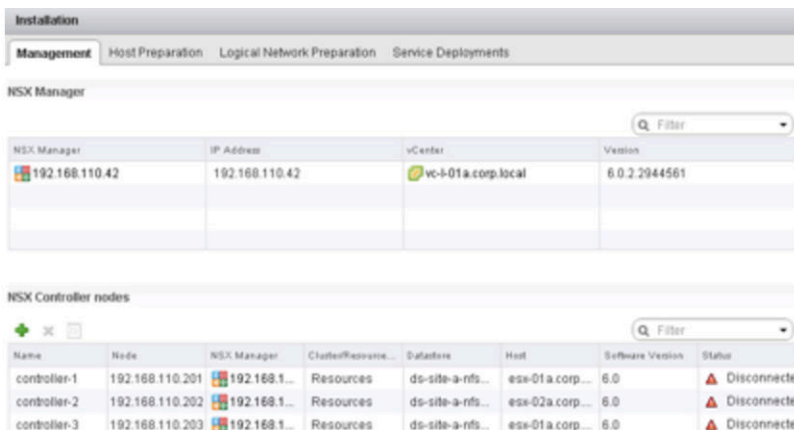


- 適切に動作しない「問題のある」コントローラ、または切断状態のアップグレード済みコントローラ。
- ESXi ホストおよび NSX Manager の DNS が適切に設定されていない。

- 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 Controller Connection
ARP Entry Count MTEP Count
-----
5000 N/A (headend replication) Enabled (multicast proxy, ARP proxy) 192.168.110.203 (down)
0 0
```

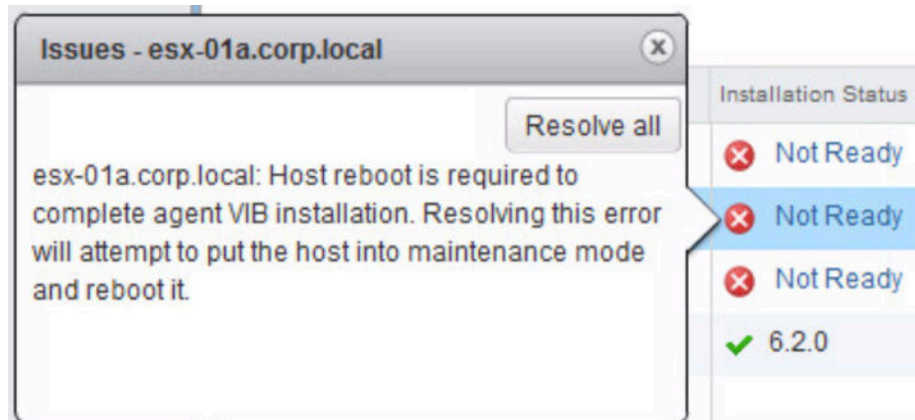
- NSX Manager CLI コマンド `show log manager follow` を実行することで、コントローラのデプロイが失敗する他の原因を特定できます。

```
2014-02-26 10:09:44.931 GMT INFO taskScheduler-25 VcConnection$VmClient:1219 - Create stub for com.vmware.vim.binding
28c5157-abf3-718e-88c5-42209f389211
2014-02-26 10:09:44.932 GMT DEBUG VcEventsReaderThread VcEventsReader$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)'.
```

ホストの準備

vSphere ESX Agent Manager は、ESXi ホストに 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。ダウンロード可能な 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、vSphere 6.0 ホストでは、<https://<NSX-Manager-IP>/bin/vdn/vibs-6.2.3/6.0-3771165/vxlan.zip> ファイルが使用されます。

```
C:\Users\Administrator>curl -k
https://nsxmgr-01a.corp.local/bin/vdn/nwfabric.properties
# 5.1 VDN EAM Info
VDN_VIB_PATH.1=/bin/vdn/vibs-6.2.3/5.1-2107743/vxlan.zip
VDN_VIB_VERSION.1=2107743
VDN_HOST_PRODUCT_LINE.1=embeddedEsx
VDN_HOST_VERSION.1=5.1.*

# 5.5 VDN EAM Info
VDN_VIB_PATH.2=/bin/vdn/vibs-6.2.3/5.5-3771174/vxlan.zip
VDN_VIB_VERSION.2=3771174
VDN_HOST_PRODUCT_LINE.2=embeddedEsx
```

```

VDN_HOST_VERSION.2=5.5.*

# 6.0 VDN EAM Info
VDN_VIB_PATH.3=/bin/vdn/vibs-6.2.3/6.0-3771165/vxlan.zip
VDN_VIB_VERSION.3=3771165
VDN_HOST_PRODUCT_LINE.3=embeddedEsx
VDN_HOST_VERSION.3=6.0.*

# 6.1 VDN EAM Info
VDN_VIB_PATH.4=/bin/vdn/vibs-6.2.3/6.1-3689890/vxlan.zip
VDN_VIB_VERSION.4=3689890
VDN_HOST_PRODUCT_LINE.4=embeddedEsx
VDN_HOST_VERSION.4=6.1.*

# Single Version associated with all the VIBs pointed by above VDN_VIB_PATH(s)
VDN_VIB_VERSION=6.2.3.3771501

# 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/

```

VIB の名前は、次のようになります。

- esx-vsip
- esx-vxlan

```

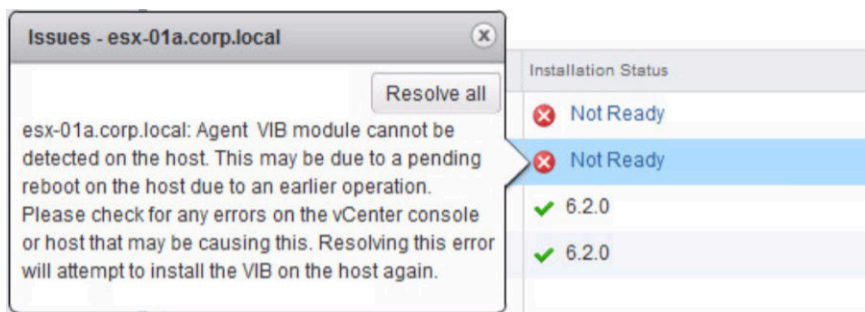
[root@esx-01a:~] esxcli software vib list | grep -e vsip -e vxlan
esx-vsip                                6.0.0-0.0.3771165                VMware  VMwareCertified
2016-04-20
esx-vxlan                                6.0.0-0.0.3771165                VMware  VMwareCertified
2016-04-20

```

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発生する一般的な問題には、次のものがあります。

- 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。

- 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する。
 - 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。

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。

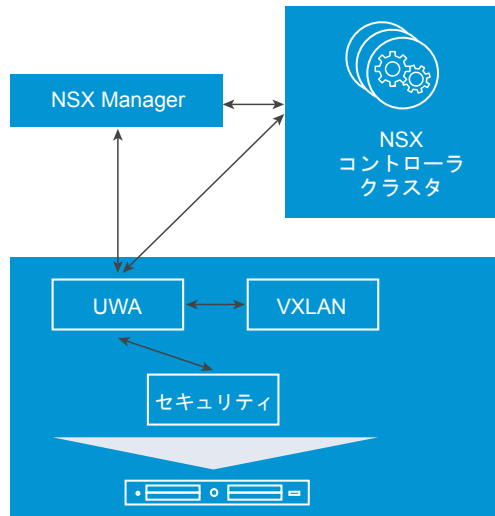
```
2016-04-28T19:02:52Z esxupdate: downloader: DEBUG: Downloading https://vcsa-01a.corp.local/tmp/tmpKT0wjN...
2016-04-28T19:03:12Z esxupdate: esxupdate: ERROR: An esxupdate error exception occurred
2016-04-28T19:03:12Z esxupdate: esxupdate: ERROR: Traceback (most recent call last):
2016-04-28T19:03:12Z esxupdate: esxupdate: ERROR:   File "/usr/sbin/esxupdate.py", line 106, in Run
2016-04-28T19:03:12Z esxupdate: esxupdate: ERROR:     cmd.Run()
2016-04-28T19:03:12Z esxupdate: esxupdate: ERROR:   File "/build/mts/release/online/packages/defaults/hosts/agent/esxupdate/Cmdline.py", line 106, in Run
2016-04-28T19:03:12Z esxupdate: esxupdate: ERROR:   File "/build/mts/release/online/packages/defaults/hosts/agent/esxupdate/Transaction.py", line 73, in DownloadMetadata
2016-04-28T19:03:12Z esxupdate: esxupdate: ERROR: MetadataDownloadError: ('https://vcsa-01a.corp.local:443/eam/vib?id=facdb160-216fd3f37ad4c', None, "('https://vcsa-01a.corp.local:443/eam/vib?id=facdb160-216fd3f37ad4c', None, 'Temporary failure in name resolution')")
2016-04-28T19:03:12Z esxupdate: esxupdate: DEBUG: <<<
```

- <https://kb.vmware.com/kb/2053782> を参照してください。

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構成します。

- 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。

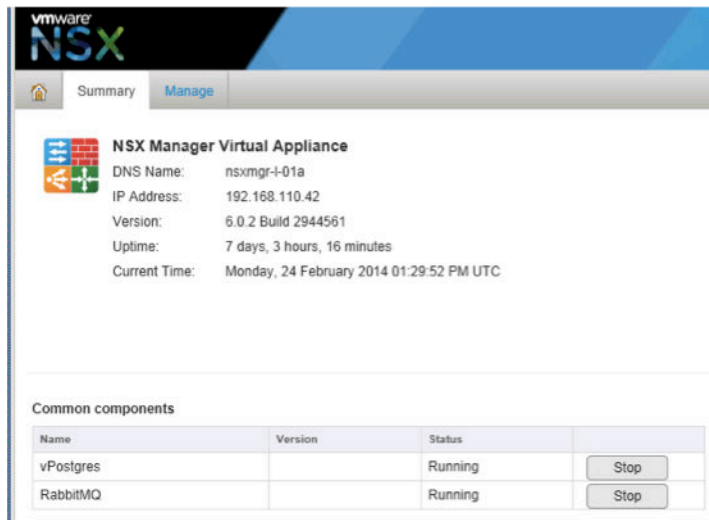
Cluster & Hosts	Installation Status	Firewall
Cluster 1	6.0 Uninstall	Error

- 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 システムのイベントを確認します。

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 つ以上の ESXi ホストが影響を受けている場合、NSX Manager アプライアンスの Web ユーザー インターフェイスの [サマリ (Summary)] タブで、メッセージング 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 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/vsfwd.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
```

netcpa ユーザー ワールド エージェントがダウンしている理由を特定するには、次の手順を実行します。

- ESXi ホストで `/etc/init.d/netcpad status` コマンドを実行して、ホスト上の netcpa 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/netcpad status
netCP agent service is running
```

- `/etc/vmware/netcpa/config-by-vsm.xml` で、netcpa ユーザー ワールド エージェントの設定を確認します。NSX コントローラの 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>
...
```

- `esxcli network ip connection list | grep 1234` コマンドを実行して、コントローラの TCP 接続を確認します。

```
>[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
```

VXLAN の準備

NSX は、ユーザーによって選択された DVS を VXLAN 用に準備します。

このときに NSX は、VTEP vmknics を使用するために、DVS で DVPortgroup を作成する必要があります。

チーミング、ロード バランスの方法、MTU、および VLAN ID は VXLAN を設定するときに選択されます。チーミングとロード バランスの方法は、VXLAN に選択された DVS 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、DVS で既に設定されているよりも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 DVS の設定によって異なります。

VXLAN を準備するときの一般的な問題

VXLAN の設定時に発生する一般的な問題には、以下があります。

- VXLAN に選択されたチーミング方法が、DVS でサポートされる方法と一致しない。『VMware NSX for vSphere Network Virtualization Design Guide』（VMware NSX for vSphere ネットワーク仮想化設計ガイド）(<https://communities.vmware.com/docs/DOC-27683>) を参照してください。
- VTEP に不正な VLAN ID が選択される。
- 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。
- vmknics の「強制同期」が設定されていない。
- vmknics の IP アドレスが不正である。

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。デフォルトでは、VXLAN UDP のポート番号は 8472 です。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、代わりに VXLAN UDP のポート番号 4789 を使用する必要があります。ポート番号は、REST API から変更できます。

```
PUT /2.0/vdn/config/vxlan/udp/port/4789
```

NSX Manager からこのホストへの通信のためにポート 80 を開けておく必要があります。これは、エージェント VIB をダウンロードするために使用します。

ESXi ホスト、vCenter Server、および NSX Data Security 間での通信で使用するポート 443/TCP

さらに、次のポートも NSX Manager で開けておく必要があります。

- 443/TCP : ESXi ホストに OVA ファイルをダウンロードしてデプロイするため、REST API および NSX Manager ユーザー インターフェイスを使用するために必要です。
- 80/TCP : vSphere SDK への接続を開始するため、また NSX Manager と NSX ホスト モジュール間のメッセージングのために必要です。
- 1234/TCP : ESXi ホストと NSX コントローラ クラスタ間の通信に必要です。
- 5671 : Rabbit MQ (メッセージング バス テクノロジー) で必要です。
- 22/TCP : CLI へのコンソール アクセス (SSH) で必要です。デフォルトでは、このポートは閉じられています。

クラスタ内のホストが vCenter Server バージョン 5.0 から 5.5 にアップグレードされた場合は、ゲスト イントロス ペクションを正しくインストールするために、これらのホストでポート 80 とポート 443 を開けておく必要があります。

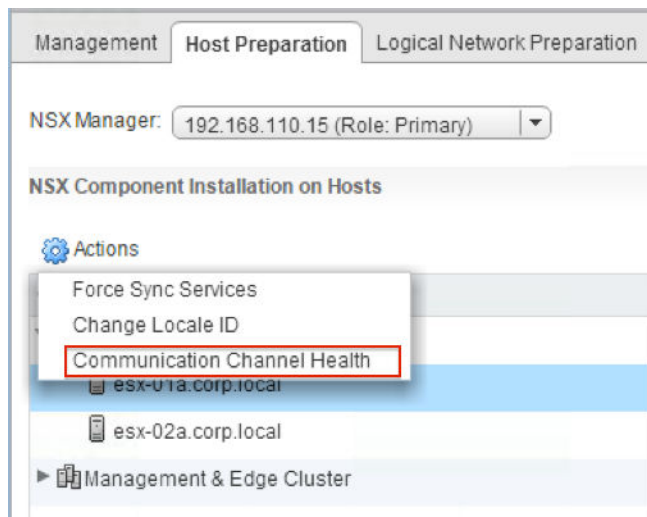
通信チャネルの健全性の確認

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、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.
```

NSX Manager の問題のトラブルシューティング

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。

ソリューション

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。

手順

- 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 との間で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 コントローラ障害からのリカバリ

NSX コントローラ障害が発生した場合でも、2 つのコントローラがまだ機能している可能性があります。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。その場合でも、3 つのコントローラをすべて削除してからすべてのコントローラを追加し直すようにしてください。それによって、完全に機能する 3 ノード クラスタが維持されます。

1 つ以上のコントローラで致命的なりカバリ不能エラーが発生した場合、または 1 つ以上のコントローラ仮想マシンがアクセス不能で修復できない状態になった場合は、コントローラ クラスタを削除することをお勧めします。

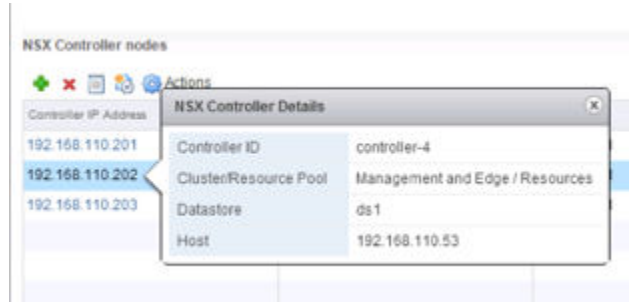
一部のコントローラが健全に動作していると思われる場合でも、すべてのコントローラを削除することをお勧めします。新しいコントローラを作成してから NSX Manager の [コントローラ状態の更新] メカニズムを使用して、2 つのコントローラの状態を同期させる方法をお勧めします。

手順

- 1 vSphere Web Client にログインします。

- 2 [Networking and Security] で、[インストール手順] > [管理] の順にクリックします。
- 3 [NSX コントローラ ノード] セクションで、各コントローラをクリックして、画面のスクリーンショットを作成するか、画面を印刷します。または、後で参照できるように設定情報をメモします。

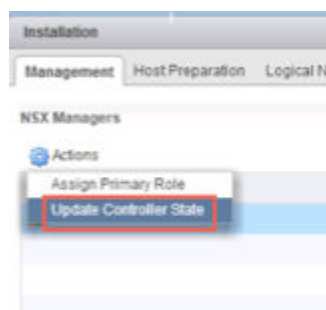
次はその例です。



- 4 [NSX コントローラ ノード] セクションで、各コントローラを選択し、[ノードの削除 (x)] アイコンをクリックして、3 つのコントローラをすべて削除します。

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。

- 5 [ノードの追加 (+)] アイコンをクリックして、3 台の新しい NSX コントローラ ノードをデプロイします。
- 6 [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、すべてのノードのステータスが [標準] になっていることを確認します。
- 7 [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。

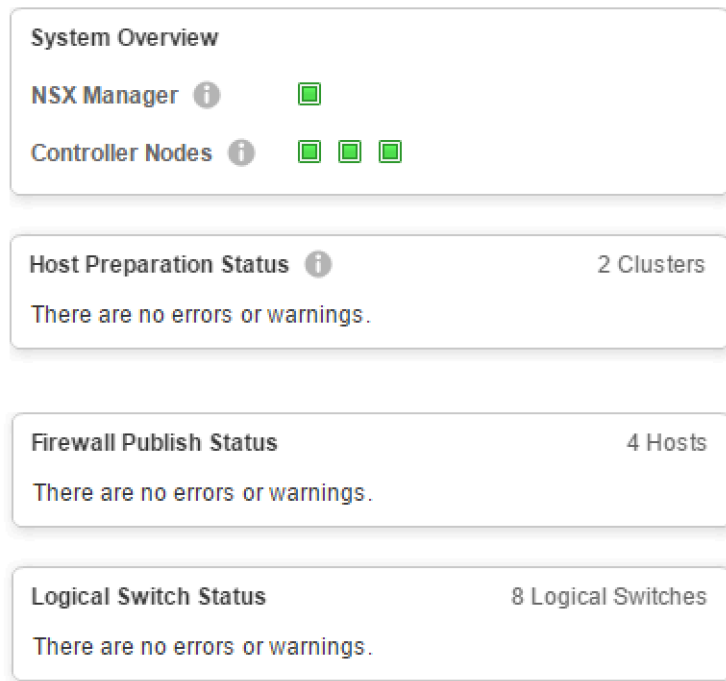


コントローラ状態の更新によって、最新の VXLAN および分散論理ルーター設定 (Cross-vCenter NSX 環境内のユニバーサル オブジェクトを含む) が、NSX Manager からコントローラ クラスタにプッシュされます。

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が 1 つのビューに表示されるため、トラブルシューティングが簡素化されます。

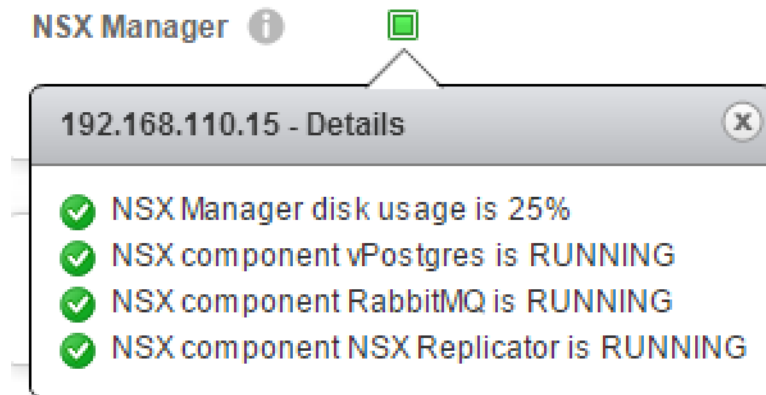
ダッシュボードを開くには、vSphere Web Client で [Networking and Security (Networking & Security)] > [ダッシュボード (Dashboard)] の順にアクセスします。



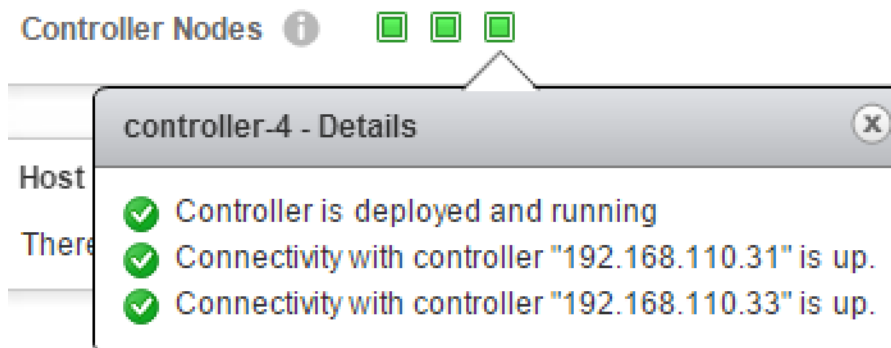
ダッシュボードで次のステータスを確認します。

- NSX インフラストラクチャ：NSX Manager のステータス
 - 次の各サービスの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
 - メッセージ バス サービス
 - レプリケーション サービス：レプリケーションのエラーも監視
 - NSX Manager のディスク使用率
 - 黄色（ディスクの使用率が 80% 以上）

- 赤色（ディスクの使用率が 90% 以上）



- NSX インフラストラクチャ：NSX コントローラのステータス
 - コントローラ ノードのステータス（実行中/デプロイ中/削除中/失敗/不明）
 - コントローラのピア接続ステータス
 - 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待ち時間のアラート



- NSX インフラストラクチャ：ホストのステータス
 - 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
 - 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赤色/黄色のクラスタ数
 - VXLAN
 - VXLAN が設定されていないクラスタ数
 - VXLAN のステータスが赤色/黄色のクラスタ数

- NSX サービス：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
- NSX サービス：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
 - 仮想ワイヤーのバックিং分散仮想スイッチポートグループが削除されている場合のフラグ

show host health-status コマンドの使用

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 コンポーネントのログ レベルの設定

各 NSX コンポーネントについてログ レベルを設定できます。

次に示すように、サポートされるレベルはコンポーネントによって異なります。

```
nsxmgr> set
  hardware-gateway  Show Logical Switch Commands
  PACKAGE-NAME      Set log level
  controller         Show Logical Switch Commands
  host               Show Logical Switch Commands

nsxmgr> set hardware-gateway agent 10.1.1.1 logging-level
  ERROR
  WARN
  INFO
  DEBUG
  TRACE
```

```
nsxmgr-01a> set <package-name> logging-level
OFF
FATAL
ERROR
WARN
INFO
DEBUG
TRACE

nsxmgr> set controller 192.168.110.31
  java-domain    Set controller node log level
  native-domain  Set controller node log level

nsxmgr> set controller 192.168.110.31 java-domain logging-level
OFF
FATAL
ERROR
WARN
INFO
DEBUG
TRACE

nsxmgr> set controller 192.168.110.31 native-domain logging-level
ERROR
WARN
INFO
DEBUG
TRACE

nsxmgr> set host host-28
  netcpa  Set host node log level by module
  vdl2    Set host node log level by module
  vdr     Set host node log level by module

nsxmgr> set host host-28 netcpa logging-level
FATAL
ERROR
WARN
INFO
DEBUG

nsxmgr> set host host-28 vdl2 logging-level
ERROR
INFO
DEBUG
TRACE

nsxmgr> set host host-28 vdr logging-level
OFF
ERROR
INFO
```

vSphere ESX Agent Manager

vSphere ESX Agent Manager (EAM) は、vSphere ソリューションに必要な追加のサービスを提供する ESXi ホストの機能を拡張しながら、vSphere ESX エージェントのデプロイと管理プロセスを自動化します。

ESX エージェントは、NSX のトラブルシューティングに関係します。これは、たとえば、NSX 環境で、特定のネットワーク フィルタやファイアウォール設定を動作させる可能性があるためです。ファイアウォールの設定では、ESX エージェントを使用して、vSphere Hypervisor に接続し、その構成に固有の機能を使用してホストを拡張できます。たとえば、ESX エージェントは、ネットワーク トラフィックをフィルタしたり、ファイアウォールとして動作したり、ホスト上の仮想マシンに関するその他の情報を収集することができます。

ESX エージェント仮想マシンは、Windows や Linux におけるサービスに似ています。オペレーティング システムが起動すると、これらの仮想マシンは開始され、オペレーティング システムがシャットダウンすると、終了します。ESX エージェント仮想マシンの動作は、ユーザーに透過的となります。ESXi オペレーティング システムが起動しており、すべての ESX エージェント仮想マシンがプロビジョニングされパワーオンされたら、vSphere ホストは稼働できる状態になります。

エージェントを vSphere ESX Agent Manager に統合し、ESXi サーバの機能を拡張するには、ESX エージェントを OVF または VIB モジュールとしてパッケージ化する必要があります。

ESX Agent Manager (EAM) では、ESX エージェントの健全性を監視できるほか、ESX エージェントでのユーザーによる特定の操作（このエージェントを使用する仮想マシンへの影響があるもの）をブロックできます。また、エージェントの VIB と仮想マシンのライフサイクルを管理します。たとえば、ESX Agent Manager では、ESX エージェントの仮想マシンがパワーオフされないようにしたり、このエージェントを使用するほかの仮想マシンがある ESXi ホストから移動されないようにすることができます。

次のスクリーンショットは、ESX Agent Manager にアクセスする際のユーザー インターフェイスを示しています。

Name	vCenter Server System	Version
NSX Manager	vcsa-01b.corp.local	6.2.3.3771501
NSX Manager	vcsa-01a.corp.local	6.2.3.3771501
vService Manager	vcsa-01b.corp.local	6.0
vService Manager	vcsa-01a.corp.local	6.0
vSphere ESX Agent Manager	vcsa-01b.corp.local	6.0
vSphere ESX Agent Manager	vcsa-01a.corp.local	6.0

vSphere ESX Agent Manager (EAM) のログとサービス

EAM ログは、vCenter Server ログのバンドルに一部として含まれます。

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

vSphere ESX エージェントとエージェンシー

vSphere ESX エージェンシーは、準備済みの NSX ホスト クラスタにマッピングされます。各 ESX エージェンシーは、ESX エージェントのコンテナとして動作します。ESX エージェンシーは、管理しているエージェントの情報を集約します。このように、ESX エージェンシーは、ESX エージェントに関連するすべての問題を集約し、自身に含まれる ESX エージェントの概要を提供します。

ESX Agent Manager は、エージェンシーのランタイム情報で問題を報告します。ESX Agent Manager では、管理者が [ESX Agent Manager] タブの [問題の解決 (Resolve Issues)] をクリックすると、特定の問題を自動的に解決できます。たとえば、ESX エージェントがパワーオフされている場合には、パワーオン状態に戻すことができます。

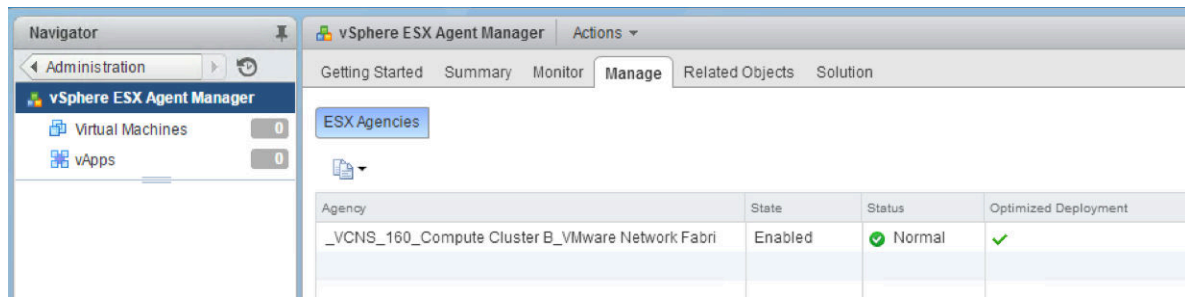
注: ESX エージェンシーのスコープが空である場合、ESX エージェントを展開するだけのコンピューティングリソースがないため、ESX エージェントはデプロイされません。この場合には、ESX エージェンシーが正しく実行しているかを ESX Agent Manager が判断し、ステータスを緑色に設定します。

各エージェンシーの設定で、エージェンシーがどのようにエージェントと VIB をデプロイするかを指定します。
<https://pubs.vmware.com/vsphere-60/index.jsp#com.vmware.eam.apiref.doc/eam.Agency.ConfigInfo.html> を参照してください。

重要: 必ず、NSX のインストールを開始する前に `bypassVumEnabled` フラグを `True` に設定し、インストール後には `False` に戻します。<https://kb.vmware.com/kb/2053782> を参照してください。

vSphere Web Client で EAM のステータスを確認するには、[管理 (Administration)] > [vCenter Server 拡張機能 (vCenter Server Extensions)] に移動します。

EAM の[管理 (Manage)] タブに、実行中のエージェンシーに関する情報が表示され、親なしのすべての 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、
https://pubs.vmware.com/vsphere-60/index.jsp#com.vmware.vsphere.ext_solutions.doc/GUID-40838DE9-6AD1-45E3-A1DE-B2B24A9E715A.html を参照してください。

NSX CLI 参考用資料

表 2-1. 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 CLUSTER-ID</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 HOST-ID</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 2-2. 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
次の 3 つの VIB がロードされています。 esx-vxlan、esx-vsip、esx-dvfilter-switch-security	<code>esxcli software vib get -- vibname <name></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>
次の 4 つのモジュールがロードされています。 vdl2、vdrb、vsip、dvfilter-switch-security	<code>esxcli system module get -m <name></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) : netcpad、vsfwd	<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	Web ユーザー インターフェイスで、[管理 (Administration)] > [vCenter ESX Agent Manager] を確認します	

表 2-3. 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 タイプ、ドライバタイプ、リンク 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
vmk NIC の IP アドレス/MAC/MTU などの情報を表示します	<code>esxcli network ip interface ipv4 get</code>	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	<code>esxcli network ip interface list</code>	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	<code>esxcli network ip interface list --netstack=vxlan</code>	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	<code>esxcli network vswitch dvs vmware vxlan list</code>	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	<code>ping ++netstack=vxlan -I vmk1 x.x.x.x</code>	VTEP 通信をトラブルシューティングするには、オプション <code>-d -s 1572</code> 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

表 2-3. 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
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。	<code>esxcli network ip route ipv4 list -N vxlan</code>	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	<code>esxcli network ip neighbor list -N vxlan</code>	VTEP 通信の問題のトラブルシューティング

表 2-4. 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	<code>show manager log follow</code>	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	<code>/var/log/esxupdate.log</code>	
ホストに関連する問題 VMkernel 警告、メッセージ、アラート、および可用性のレポート	<code>/var/log/vmkernel.log</code> <code>/var/log/vmksummary.log</code> <code>/var/log/vmkwarning.log</code>	
モジュールのロード エラーがキャプチャされます	<code>/var/log/syslog</code>	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 <code>eam.log</code>	

表 2-5. 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	<code>show logical-switch list all</code>	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 2-6. 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

表 2-6. 論理スイッチ : NSX Controller から実行するコマンド (続き)

説明	コントローラのコマンド	メモ
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 <host_mgmt_ip></code>	

表 2-7. 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パス 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	<code>esxcli software vib get --vibName esx-vxlan</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
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 2-8. 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。 config-by-vsm.xml ファイルは、netcpa プロセスによって作成されます Vsfwd は、netcpa のチャンネルのみを提供します Netcpad はポート 15002 で vsfwd に接続します
config-by-vsm.xml ファイルは、vsfwd を使用して NSX Manager によってブッシュされます 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	<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、 /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	<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
VDL2 モジュールのログは、vmkernel.log にあります	<code>/var/log/vmkernel.log</code>	<code>/var/log/vmkernel.log</code> で、VDL2 モジュールのログ「prefixed with VXLAN:」を確認します

表 2-9. 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	show edge	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	show edge	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	show logical-router	分散論理ルーターの CLI コマンドは、 show logical-router から始まります
すべての Edge を表示します	show edge all	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	show edge EDGE-ID	Edge Services Gateway の情報を表示します
Edge のコマンド オプションを表示します	show edge EDGE-ID ?	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 EDGE-ID 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 EDGE-ID 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 EDGE-ID 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

表 2-9. 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
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	<code>show logical-router host hostID dlr all</code>	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	<code>show logical-router host hostID dlr dlrID route</code>	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	<code>show logical-router host hostID dlr dlrID interface (all intName) verbose</code>	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 2-10. 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	<code>show control-cluster logical-routers instance all</code>	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	<code>show control-cluster logical-routers instance 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
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ターを表示します	<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

表 2-10. 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
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 <logical-router-id> <host-ip></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を同期します	<code>sync control-cluster logical-routers route-to-host <logical-router-id> <host-ip></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 2-11. 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 <global bgp ospf ...></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本当の 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 2-11. 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</pre> (および「EXCEPTION」と「PROBLEM」の文字列で検索)	
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</pre> (「EXCEPTION」と「PROBLEM」の文字列で検索)	

表 2-12. 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て、XML形式で保存されます	<code>/etc/vmware/netcpa/config-by-vsm.xml</code>	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、このファイルにこのインスタンスが表示されているかどうかを最初に確認します 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	<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 netcpa 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
VDL2 モジュールのログは、vmkernel.log にあります	<code>/var/log/vmkernel.log</code>	<code>/var/log/vmkernel.log</code> で、VDL2 モジュールのログ「prefixed with vxlan:」を確認します

表 2-13. 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	<code>show controller list all</code>	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 2-14. 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
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 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 2-15. 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<timestamp>.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、cloudnet_java-zookeeper 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に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、freespace 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 2-15. 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	<code>show log syslog filtered-by Active cluster members</code>	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	<code>show log cloudnet/cloudnet_java-zookeeper. 20150703-165223.3702.log</code>	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	<code>show log cloudnet/cloudnet.nsx-controller.root.log.INFO. 20150703-165223.3668</code>	LIF の作成、1234 での接続リスナー、シャーディングなど、メイン コントローラの動作に関するログ

表 2-16. 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	<code>show vm VM-ID</code>	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	<code>show vnic VNIC-ID</code>	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	<code>show dfw cluster all</code>	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	<code>show dfw cluster CLUSTER-ID</code>	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	<code>show dfw host HOST-ID</code>	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	<code>show dfw host HOST-ID filter filterID <option></code>	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	<code>show dfw vm VM-ID</code>	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	<code>show dfw vnic VNIC-ID</code>	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	<code>show dfw host hostID summarize-dvfilter</code>	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	<code>show dfw host hostID filter filterID rules show dfw vnic nicID</code>	
アドレス セットの詳細を表示します	<code>show dfw host hostID filter filterID addrsets</code>	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

表 2-16. 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
各 vNIC の spoofguard の詳細	<code>show dfw host hostID filter filterID spoofguard</code>	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
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 2-17. 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	メモ
ホストにダウンロードされた VIB を表示します	<code>esxcli software vib list grep vsip</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	<code>esxcli system module get -m vsip</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>	デーモンが実行し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 2-18. 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>	

トレースフロー

トレースフローは、パケットを挿入し、そのパケットが物理ネットワークおよび論理ネットワークを通過するときの通り道を観察する機能を提供するトラブルシューティングのためのツールです。これを観察することで、ダウンしているノードや、パケットがターゲットに届くのを妨げているファイアウォールルールを特定するなど、ネットワークに関する情報を判断できます。

この章には、次のトピックが含まれています。

- [トレースフローについて](#)
- [トラブルシューティングのためのトレースフローの使用](#)

トレースフローについて

トレースフローは、オーバーレイ ネットワークおよびアンダーレイ ネットワークの物理エンティティや論理エンティティ（ESXi ホスト、論理スイッチ、分散論理ルーターなど）をトラバースするときに、パケットを vSphere Distributed Switch (VDS) ポートに挿入し、パケットのパスに沿ったさまざまな観測ポイントを提供します。これにより、パケットが宛先に到達するまでに経由する 1 つ以上のパスを特定できます。つまり、逆にパケットが途中でドロップされた場所を特定することができます。エンティティごとに入出力のパケット処理が報告されるため、パケットの受信時に問題が発生したのか、パケットの転送時に問題が発生したのかがわかります。

トレースフローは、ゲスト仮想マシンのスタック間でやりとりされる ping の要求/応答と同じではないことに留意してください。トレースフローは、オーバーレイ ネットワークを経由するマーク付けされたパケットを観察します。各パケットがオーバーレイ ネットワークを経由して宛先ゲスト仮想マシンに到達し、配信可能状態になるまでの様子が観察されます。ただし、挿入されたトレースフロー パケットは、実際には宛先ゲスト仮想マシンに配信されません。これは、ゲスト仮想マシンがパワーオフの状態でもトレースフローが正常に動作することを意味します。

トレースフローでは、次のトラフィック タイプがサポートされています。

- レイヤー 2 ユニキャスト
- レイヤー 3 ユニキャスト
- レイヤー 2 ブロードキャスト
- レイヤー 2 マルチキャスト

カスタム ヘッダ フィールドやパケット サイズを指定してパケットを構築できます。トレースフローのソースは、常に仮想マシンの仮想 NIC (vNIC) です。ターゲット エンドポイントは、NSX オーバーレイまたはアンダーレイの任意のデバイスにすることができます。ただし、NSX Edge Services Gateway (ESG) のアップリンクの先にある宛先を選択することはできません。宛先は、同じサブネット上に存在しているか、または NSX 分散論理ルーターを経由して到達できる必要があります。

送信元 vNIC と宛先 vNIC が同じレイヤー 2 ドメイン内に存在する場合、トレースフロー操作はレイヤー 2 と見なされます。NSX の場合、これは、VXLAN ネットワーク識別子 (VNI またはセグメント ID) が同じであることを意味します。これは、2 台の仮想マシンが同じ論理スイッチに接続されている場合などに発生します。

NSX ブリッジが設定されている場合、未知のレイヤー 2 パケットは常にブリッジに送信されます。通常、ブリッジはこれらのパケットを VLAN に転送し、トレースフロー パケットを送信済みとして報告します。パケットが配信済みと報告されたからといって、必ずしもトレース パケットが指定された宛先に配信されたことを意味するわけではありません。

レイヤー 3 トレースフロー ユニキャスト トラフィックの場合、2 つのエンド ポイントは、別々の論理スイッチ上にあり、異なる VNI が設定されていて、分散論理ルーター (DLR) に接続されています。

マルチキャスト トラフィックの場合、送信元は仮想マシン vNIC で、宛先はマルチキャスト グループ アドレスになります。

トレースフローの観察では、ブロードキャストされたトレースフロー パケットが対象に含まれることがあります。ESXi ホストは、宛先ホストの MAC アドレスが不明な場合にトレースフロー パケットをブロードキャストします。ブロードキャスト トラフィックの場合、ソースは仮想マシン vNIC になります。ブロードキャスト トラフィックのレイヤー 2 ターゲット MAC アドレスは FF:FF:FF:FF:FF:FF です。ファイアウォール検査の有効なパケットを作成するために、ブロードキャスト トレースフロー操作では、サブネット プリフィックスの長さが必要になります。サブネット マスクにより、NSX はパケットの IP ネットワーク アドレスを計算できます。



警告: デプロイの論理ポート数によっては、マルチキャストおよびブロードキャスト トレースフロー操作で大量のトラフィックが生成される可能性があります。

トレースフローを使用する方法は、API と GUI の 2 種類があります。API は、GUI で使用される API と同じですが、API ではパケットを詳細に設定することができます。GUI の設定はより限定的です。

GUI では、次の値を設定できます。

- プロトコル --- TCP、UDP、ICMP。
- 存続時間 (TTL)。デフォルトは 64 ホップです。
- TCP や UDP の送信元および宛先ポート数。デフォルト値は 0 です。
- TCP フラグ。
- ICMP ID およびシーケンス番号。どちらもデフォルトは 0 です。
- トレースフロー操作の有効期限切れタイムアウト (ミリ秒単位)。デフォルトは 10,000 ミリ秒です。
- イーサネット フレーム サイズ。デフォルトは 128 バイト/フレームです。最大フレーム サイズは 1000 バイト/フレームです。
- ペイロード エンコード。デフォルトは Base64 です。

- ペイロード値。

トラブルシューティングのためのトレースフローの使用

トレースフローが役立つシナリオには、以下のように複数のシナリオがあります。

トレースフローは以下のシナリオで役立ちます。

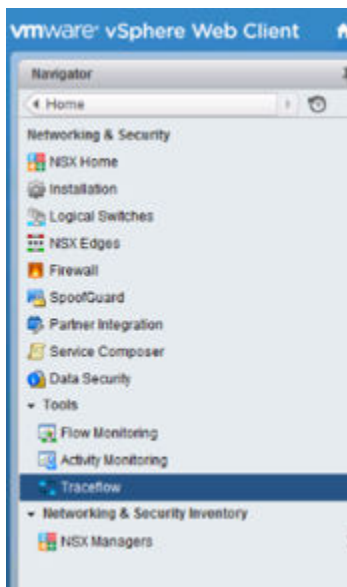
- 正確なトラフィックの経由パスを確認することによるネットワーク障害のトラブルシューティング
- リンクの使用率を確認することによるパフォーマンス監視
- ネットワークが本番環境にあるときの動作を確認することによるネットワーク計画

前提条件

- トレースフローの操作には、vCenter Server、NSX Manager、NSX Controller クラスタ、およびホスト上の netcpa ユーザー ワールド エージェント間の通信が必要です。
- トレースフローを期待どおりに動作させるには、コントローラ クラスタが接続され、健全な状態であることを確認します。

手順

- 1 vSphere Web Client で、[ホーム (Home)] > [Networking and Security (Networking & Security)] > [トレースフロー (Traceflow)] の順に移動します。



- 2 トラフィック タイプをユニキャスト、ブロードキャスト、マルチキャストから選択します。
- 3 ソース仮想マシン vNIC を選択します。

その仮想マシンが、トレースフローの実行元と同じ vCenter Server 上で管理されている場合、リストから仮想マシンと vNIC を選択できます。

4 ユニキャスト トレースフローの場合、ターゲット vNIC 情報を入力します。

ターゲットとして、ホスト、仮想マシン、分散論理ルーター、Edge Services Gateway などの NSX オーバーレイまたは NSX アンダーレイ内の任意のデバイスの vNIC を指定できます。ターゲットが VMware Tools の実行元の仮想マシンであり、トレースフローの実行元と同じ vCenter Server によって管理されている場合、リストから仮想マシンと vNIC を選択できます。

そうでない場合、ターゲット IP アドレス（さらに、ユニキャスト レイヤー 2 トレースフローの場合は MAC アドレス）を入力する必要があります。この情報は、デバイス コンソール、または SSH セッション内のデバイス自体から収集できます。たとえば、このマシンが Linux 仮想マシンの場合、IP アドレスと MAC アドレスは、Linux ターミナルで **ifconfig** コマンドを実行することで取得できます。分散論理ルーターまたは Edge Services Gateway の場合、この情報は **show interface** CLI コマンドで収集できます。

5 レイヤー 2 ブロードキャスト トレースフローの場合、サブネットのプリフィックスの長さを入力します。

パケットは、MAC アドレスのみに基づいてスイッチされます。ターゲット MAC アドレスは FF:FF:FF:FF:FF:FF です。

IP パケットがファイアウォール検査に有効であるためには、ソース IP アドレスおよびターゲット IP アドレスの両方が必要です。

6 レイヤー 2 マルチキャスト トレースフローの場合、マルチキャスト グループアドレスを入力します。

パケットは、MAC アドレスのみに基づいてスイッチされます。

IP パケットが有効であるためには、ソース IP アドレスおよびターゲット IP アドレスの両方が必要です。マルチキャストの場合、MAC アドレスは IP アドレスから推定されます。

7 その他の必須およびオプション設定を行います。

8 [トレース (Trace)] をクリックします。

例：シナリオ

次の例に、単一の ESXi ホスト上で実行されている 2 つの仮想マシンを含むレイヤー 2 トレースフローを示します。2 台の仮想マシンは、単一の論理スイッチに接続されています。

Traceflow

NSX Manager: 192.168.110.15 (Role: Primary)

Trace Parameters

Traffic Type: Unicast

Source: * web-01a - Network adapter 1 Change...
IP: 172.16.10.11, MAC: 00:50:56:ae:3e:3d

Destination: * web-02a - Network adapter 1 Change...
IP: 172.16.10.12, MAC: 00:50:56:ae:f8:6b

Advanced Options

Protocol: TCP

Source Port: 0

Destination Port: 0

TCP Flags: ☐ FIN ☒ SYN ☐ RST

Timeout (ms): 10000

Frame Size: 128

TTL: 64

Trace

Trace Result: Traceflow delivered observation(s) reported

1 Delivered

Sequence	Observation Type	Host	Component Type	Component Name
0	Injected	esx-01a.corp.local	vNIC	vNIC
1	Received	esx-01a.corp.local	Firewall	Firewall
2	Forwarded	esx-01a.corp.local	Firewall	Firewall
3	Received	esx-01a.corp.local	Firewall	Firewall
4	Forwarded	esx-01a.corp.local	Firewall	Firewall
5	Delivered	esx-01a.corp.local	vNIC	vNIC

次の例に、2 台の異なる ESXi ホスト上で実行されている 2 つの仮想マシンを含むレイヤー 2 トレースフローを示します。2 台の仮想マシンは、単一の論理スイッチに接続されています。

Traceflow

NSX Manager: 192.168.110.15 (Role: Primary)

Trace Parameters

Traffic Type: Unicast

Source: * web-01a - Network adapter 1 Change...
IP: 172.16.10.11, MAC: 00:50:56:ae:3e:3d

Destination: * web-03a - Network adapter 1 Change...
IP: 172.17.10.11, MAC: 00:50:56:ae:cf:88

▼ Advanced Options

Protocol: TCP

Source Port: 0

Destination Port: 0

TCP Flags: ☐ FIN ☒ SYN ☐ RST

Timeout (ms): 10000

Frame Size: 128

TTL: 64

Trace

Trace Result: Traceflow delivered observation(s) reported

1 Delivered

Sequence	Observation Type	Host	Component Type	Component Name
0	Injected	esx-01a.corp.local	vNIC	vNIC
1	Received	esx-01a.corp.local	Firewall	Firewall
2	Forwarded	esx-01a.corp.local	Firewall	Firewall
3	Forwarded	esx-01a.corp.local	Physical	esx-01a.corp.local
3	Forwarded	esx-01a.corp.local	Physical	esx-01a.corp.local
4	Received	esxmgt-02a.corp.local	Physical	esxmgt-02a.corp.local
4	Received	esxmgt-02a.corp.local	Physical	esxmgt-02a.corp.local
4	Received	esxmgt-02a.corp.local	Physical	esxmgt-02a.corp.local
4	Received	esxmgt-02a.corp.local	Physical	esxmgt-02a.corp.local
4	Received	esx-02a.corp.local	Physical	esx-02a.corp.local
4	Received	esx-02a.corp.local	Physical	esx-02a.corp.local
5	Received	esx-02a.corp.local	Firewall	Firewall
6	Forwarded	esx-02a.corp.local	Firewall	Firewall
7	Delivered	esx-02a.corp.local	vNIC	vNIC

次の例に、レイヤー 3 トレースフローを示します。2 つの仮想マシンは、分散論理ルーターによって分離された 2 つの異なる論理スイッチに接続されています。

Traceflow

NSX Manager: 192.168.110.15 (Role: Primary)

Trace Parameters

Traffic Type: Unicast

Source: * web-01a - Network adapter 1 Change...
IP: 172.16.10.11, MAC: 00:50:56:ae:3e:3d

Destination: * db-01a - Network adapter 1 Change...
IP: 172.16.30.11, MAC: 00:50:56:ae:d4:2b

▶ Advanced Options

Trace

Trace Result: Traceflow delivered observation(s) reported

1 Delivered

Sequence	1 ▲	Observation Type	Host	Component Type	Component Name
0		Injected	esx-01a.corp.local	vNIC	vNIC
1		Received	esx-01a.corp.local	Firewall	Firewall
2		Forwarded	esx-01a.corp.local	Firewall	Firewall
3		Forwarded	esx-01a.corp.local	Logical Switch	Web-Tier-01
4		Received	esx-01a.corp.local	Logical Router	Local-Distributed-Router
5		Forwarded	esx-01a.corp.local	Logical Router	Local-Distributed-Router
6		Received	esx-01a.corp.local	Logical Switch	DB-Tier-01
7		Forwarded	esx-01a.corp.local	Physical	esx-01a.corp.local
8		Received	esx-02a.corp.local	Physical	esx-02a.corp.local
8		Received	esx-02a.corp.local	Physical	esx-02a.corp.local
9		Received	esx-02a.corp.local	Firewall	Firewall
10		Forwarded	esx-02a.corp.local	Firewall	Firewall
11		Delivered	esx-02a.corp.local	vNIC	vNIC

次の例に、3つの仮想マシンが単一の論理スイッチに接続されているデプロイ内の、ブロードキャストトレースフローを示します。仮想マシンのうちの2つは1台のホスト(esx-01a)上にあり、もう1つは別のホスト(esx-02a)上にあります。ブロードキャストは、ホスト 192.168.210.53 上の仮想マシンのいずれかから送信されます。

Traceflow

NSX Manager: 192.168.110.15 (Role: Primary)

Trace Parameters

Traffic Type: **L2 Broadcast** ⚠ High volume of traffic may get generated for this traffic type.

Source: * web-01a - Network adapter 1 [Change...](#) Subnet Prefix Length: * **24**

IP: 172.16.10.11, MAC: 00:50:56:ae:3e:3d IP: 172.16.10.255, MAC: FF:FF:FF:FF:FF:FF

▶ Advanced Options

Trace

Trace Result: Traceflow delivered observation(s) reported

3 Delivered

Sequence	1 ▲	Observation Type	Host	Component Type	Component Name
0		Injected	esx-01a.corp.local	vNIC	vNIC
1		Received	esx-01a.corp.local	Firewall	Firewall
2		Forwarded	esx-01a.corp.local	Firewall	Firewall
3		Forwarded	esx-01a.corp.local	Logical Switch	Web-Tier-01
3		Received	esx-01a.corp.local	Firewall	Firewall
3		Forwarded	esx-01a.corp.local	Physical	esx-01a.corp.local
3		Forwarded	esx-01a.corp.local	Physical	esx-01a.corp.local
4		Received	esxmgt-02a.corp.local	Physical	esxmgt-02a.corp.local
4		Received	esxmgt-02a.corp.local	Physical	esxmgt-02a.corp.local
4		Received	esxmgt-02a.corp.local	Physical	esxmgt-02a.corp.local
4		Received	esxmgt-02a.corp.local	Physical	esxmgt-02a.corp.local
4		Forwarded	esx-01a.corp.local	Firewall	Firewall
4		Received	esx-02a.corp.local	Physical	esx-02a.corp.local
4		Received	esx-02a.corp.local	Physical	esx-02a.corp.local
5		Forwarded	esxmgt-02a.corp.local	Logical Switch	Web-Tier-01
5		Forwarded	esxmgt-02a.corp.local	Logical Switch	Web-Tier-01
5		Forwarded	esxmgt-02a.corp.local	Logical Switch	Web-Tier-01
5		Forwarded	esxmgt-02a.corp.local	Logical Switch	Web-Tier-01
5		Delivered	esxmgt-02a.corp.local	vNIC	vNIC
5		Delivered	esx-01a.corp.local	vNIC	vNIC
5		Forwarded	esx-02a.corp.local	Logical Switch	Web-Tier-01
5		Forwarded	esx-02a.corp.local	Logical Switch	Web-Tier-01
5		Received	esx-02a.corp.local	Firewall	Firewall
6		Forwarded	esx-02a.corp.local	Firewall	Firewall
7		Delivered	esx-02a.corp.local	vNIC	vNIC

次の例に、マルチキャスト構成のデプロイ環境にマルチキャストトラフィックが送信されるときに何が起きるかを示します。

Traceflow

NSX Manager: 192.168.110.15 (Role: Primary)

Trace Parameters

Traffic Type: L2 Multicast High volume of traffic may get generated for this traffic type.

Source: web-01a - Network adapter 1 [Change...](#) Destination IP: 239.0.0.1 [Change...](#) e.g. 239.0.0.1
 IP: 172.16.10.11, MAC: 00:50:56:ae:3e:3d IP: 239.0.0.1, MAC: 01:00:5e:00:00:01

▶ Advanced Options

[Trace](#)

Trace Result: Traceflow delivered observation(s) reported

3 Delivered

Sequence	1 ▲ Observation Type	Host	Component Type	Component Name
0	Injected	esx-01a.corp.local	vNIC	vNIC
1	Received	esx-01a.corp.local	Firewall	Firewall
2	Forwarded	esx-01a.corp.local	Firewall	Firewall
3	Received	esx-01a.corp.local	Firewall	Firewall
3	Forwarded	esx-01a.corp.local	Physical	esx-01a.corp.local
3	Forwarded	esx-01a.corp.local	Physical	esx-01a.corp.local
4	Received	esxmgt-02a.corp.local	Physical	esxmgt-02a.corp.local
4	Received	esxmgt-02a.corp.local	Physical	esxmgt-02a.corp.local
4	Received	esxmgt-02a.corp.local	Physical	esxmgt-02a.corp.local
4	Received	esxmgt-02a.corp.local	Physical	esxmgt-02a.corp.local
4	Forwarded	esx-01a.corp.local	Firewall	Firewall
4	Received	esx-02a.corp.local	Physical	esx-02a.corp.local
4	Received	esx-02a.corp.local	Physical	esx-02a.corp.local
5	Delivered	esxmgt-02a.corp.local	vNIC	vNIC
5	Delivered	esx-01a.corp.local	vNIC	vNIC
5	Received	esx-02a.corp.local	Firewall	Firewall
6	Forwarded	esx-02a.corp.local	Firewall	Firewall
7	Delivered	esx-02a.corp.local	vNIC	vNIC

次の例は、ターゲット アドレスに送信された ICMP トラフィックをブロックする分散ファイアウォール ルールによって、トレースフローがドロップされるときの動作です。ターゲット仮想マシンが別のホスト上にあるにもかかわらず、トラフィックは元のホストに留まります。

Traceflow

NSX Manager: 192.168.110.15 (Role: Primary)

Trace Parameters

Traffic Type: Unicast

Source: web-02a - Network adapter 1 [Change...](#) Destination: web-03a - Network adapter 1 [Change...](#)
 IP: 172.16.10.12, MAC: 00:50:56:ae:f8:6b IP: 172.17.10.11, MAC: 00:50:56:ae:cf:88

▶ Advanced Options

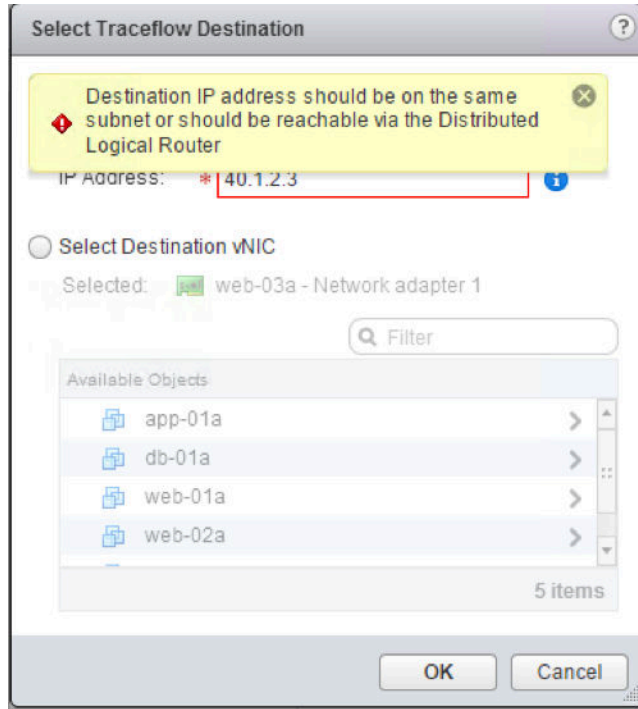
[Trace](#)

Trace Result: Traceflow dropped observation(s) reported

1 Dropped

Sequence	1 ▲ Observation Type	Host	Component Type	Component Name
0	Injected	esx-01a.corp.local	vNIC	vNIC
1	Received	esx-01a.corp.local	Firewall	Firewall
2	Dropped	esx-01a.corp.local	Firewall	Firewall (Rule - 1013)

次の例は、トレースフローのターゲットが Edge Services Gateway の外部にある場合の動作です。たとえば、インターネット上の IP アドレスや、Edge Services Gateway を介してルーティングする必要がある内部のターゲットの場合です。トレースフローは同じサブネット上にあるターゲット、あるいは分散論理ルーター (DLR) を介してアクセス可能なターゲットのいずれかでサポートされるため、トレースフローは設計上許可されません。



次の例は、トレースフロー ターゲットが別のサブネット上にあるパワーオフされた仮想マシンである場合の動作です。

Traceflow

NSX Manager: 192.168.110.15 (Role: Primary)

Trace Parameters

Traffic Type: Unicast

Source: app-01a - Network adapter 1 Change...
IP: 172.16.20.11, MAC: 00:50:56:ae:23:b9

Destination: db-01a - Network adapter 1 Change...
IP: 172.16.30.11, MAC: 00:50:56:ae:d...

Advanced Options

Trace

Trace Result: No delivered or dropped observations reported

Sequence	1 ▲	Observation Type	Host	Component Type	Component Name
0		Injected	esx-02a.corp.local	vNIC	vNIC
1		Received	esx-02a.corp.local	Firewall	Firewall
2		Forwarded	esx-02a.corp.local	Firewall	Firewall
3		Forwarded	esx-02a.corp.local	Logical Switch	App-Tier-01
4		Received	esx-02a.corp.local	Logical Router	Local-Distributed-Router
5		Forwarded	esx-02a.corp.local	Logical Router	Local-Distributed-Router
6		Received	esx-02a.corp.local	Logical Switch	DB-Tier-01

NSX のルーティング

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。

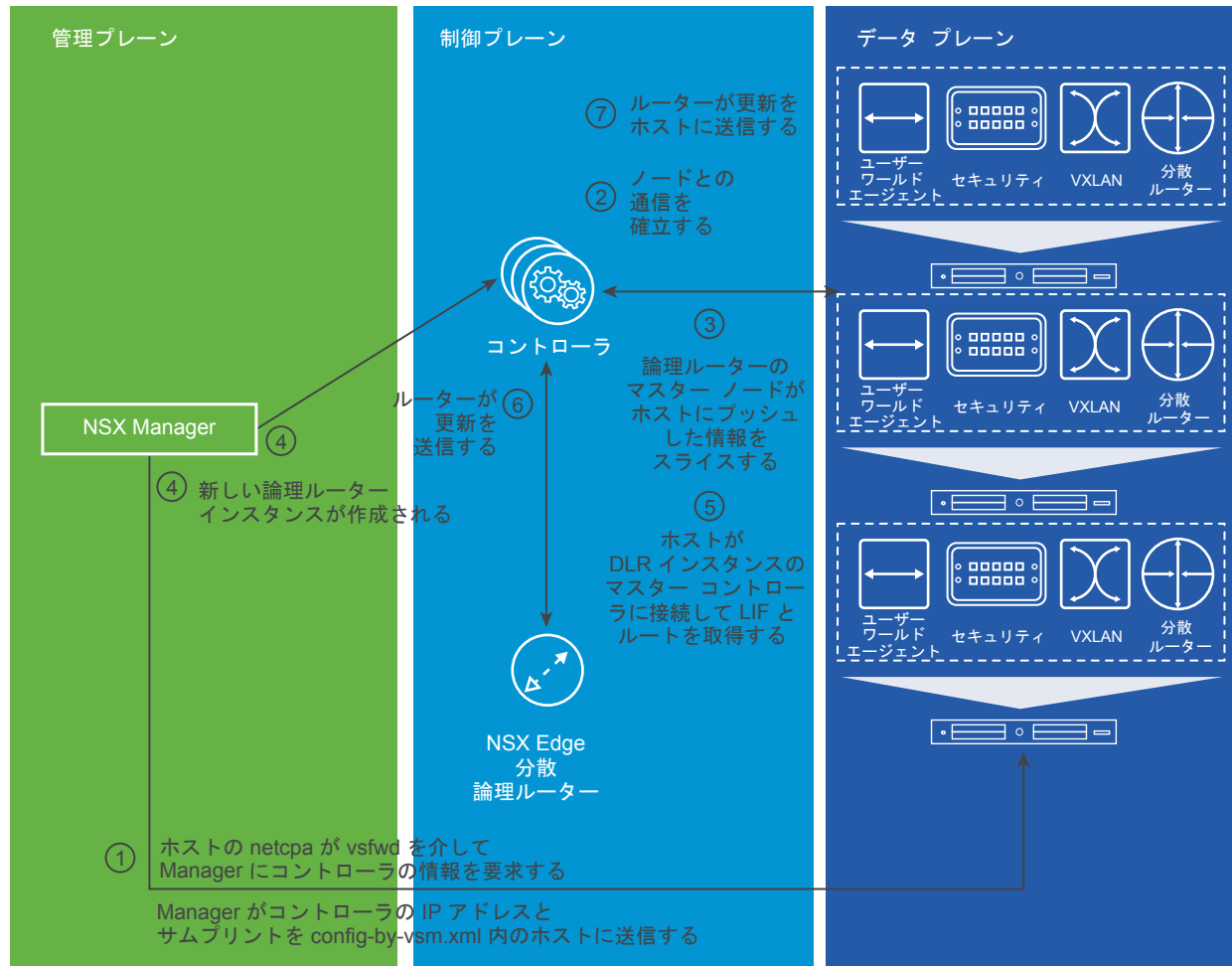
分散論理ルーターで一度に実行できるのは 1 つの動的ルーティング プロトコル（OSPF または BGP）ですが、ESG では両方のプロトコルを同時に実行できます。これは、分散論理ルーターが 1 つの出力パスを使用する「スタブ」ルーターとして機能するように設計され、より高度なルーティング設定が通常は必要とされないためです。

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 4-1. 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

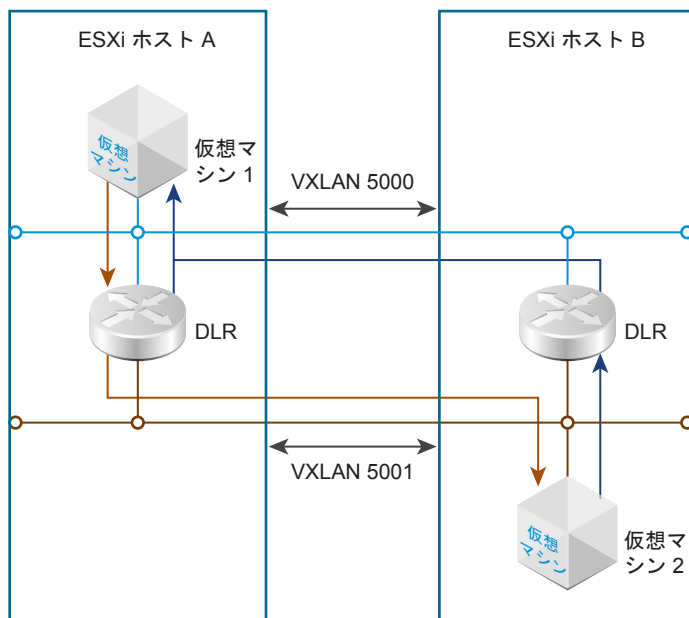
ESXi ホストには、設定済みの各分散論理ルーター インスタンスのコピーがそれぞれ関連付けられます。各分散論理ルーター インスタンスは、パケットを転送するために必要な情報を含む独自のテーブル セットが関連付けられます。この情報は、この分散論理ルーター インスタンスが存在するすべてのホスト間で同期されます。異なるホスト間の個々の分散論理ルーターのインスタンスに、正確に同じ情報が関連付けられます。

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 4-2 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 4-2. 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。

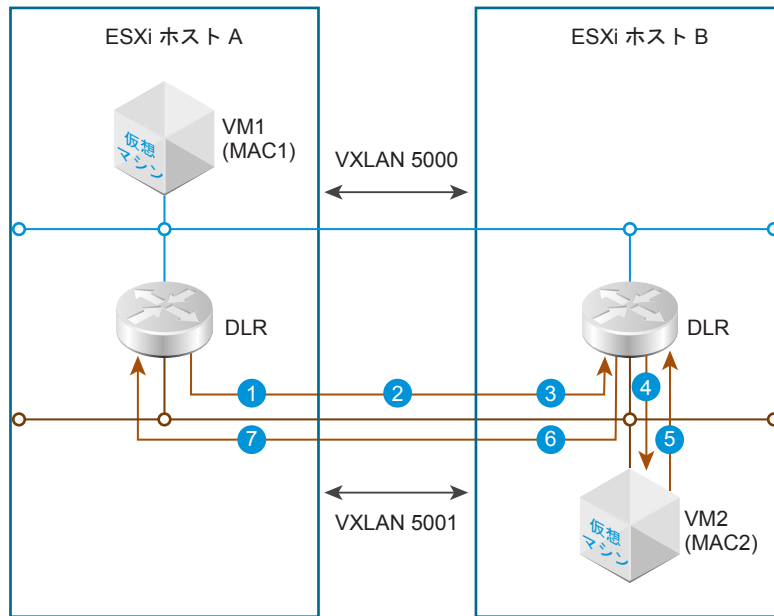
リターン トラフィックも同じ順序で処理され、VM2 からのトラフィックは ESXi ホスト B の分散論理ルーター インスタンスに転送され、VXLAN 5000 の L2 を介して配信されます。

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 4-3 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 4-3. 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` を介してフラグディングされないように「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。

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、パ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 4-4 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。

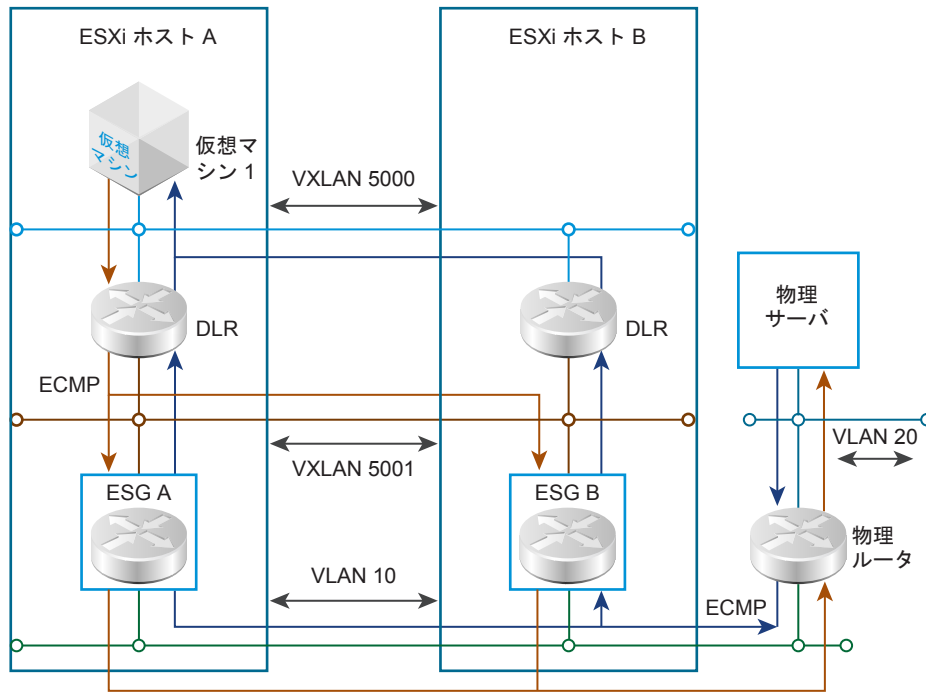
分散論理ルーターでは ECMP が有効になっており、動的ルーティング プロトコル（BGP または OSPF）を介して ESG のペア（ESG A および ESG B）から VLAN 20 の IP アドレス サブネットへ等コスト ルートを受信します。

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 4-4. 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

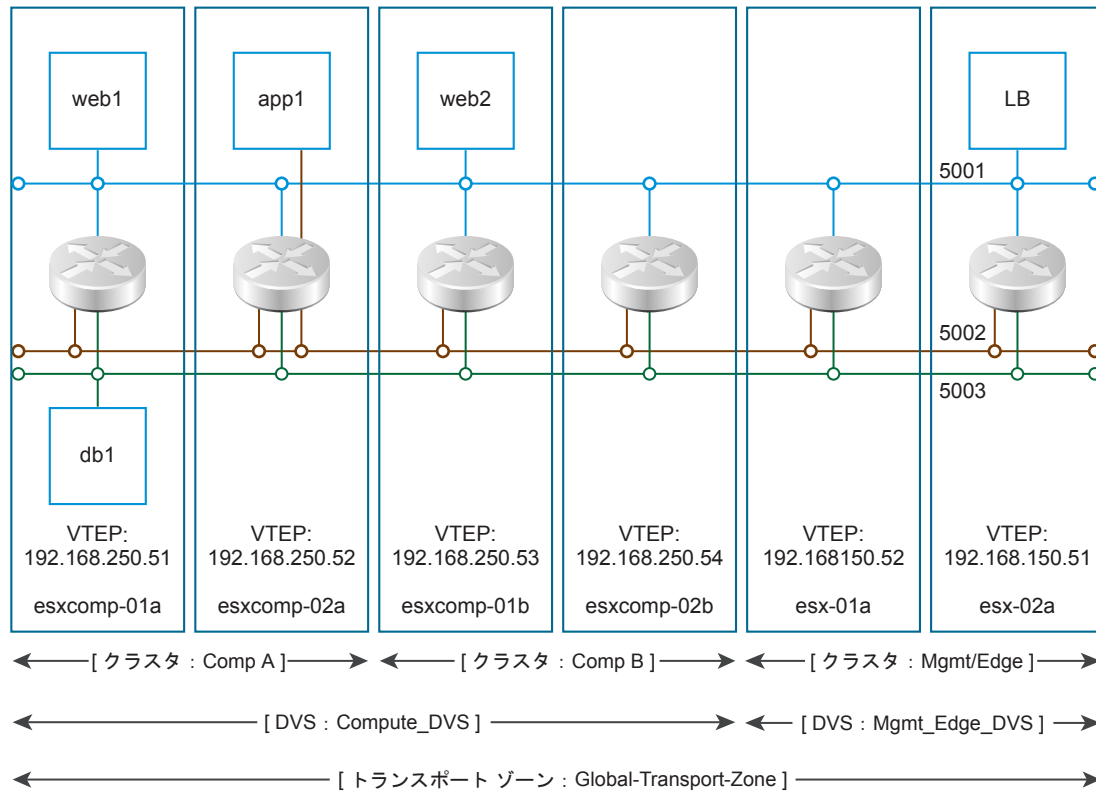
分散論理ルーターと ESG は、エンドツーエンドの接続用として dvPortgroup (VXLAN ベースおよび VLAN ベースの両方) の L2 フォワーディング サービスを提供するために、分散仮想スイッチを使用します。

これは、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、動作可能である必要があることを意味します。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 4-5. 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



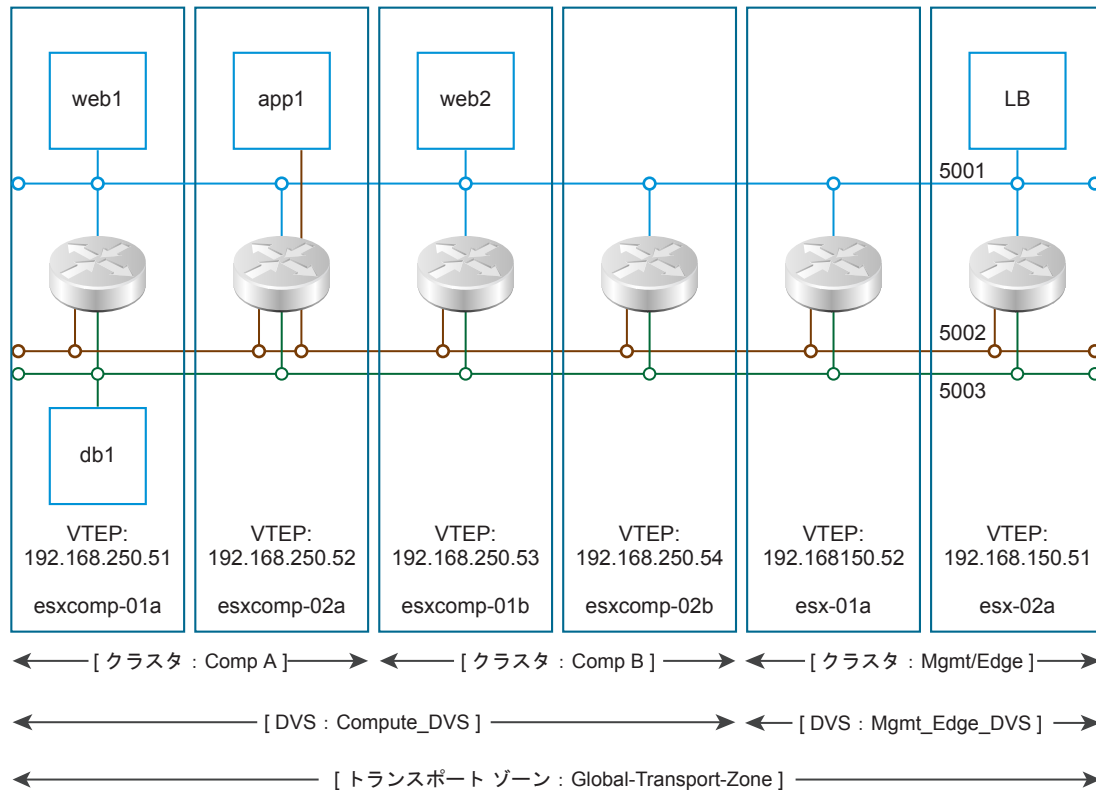
トランスポート ゾーンが分散仮想スイッチの境界と一致していないと、論理スイッチ（5001、5002、5003）とこれらの論理スイッチが接続される分散論理ルーター インスタンスの範囲の結合が解除されて、クラスタ Comp A 内の仮想マシンが分散論理ルーターの LIF にアクセスできなくなります。

上記の図では、Compute_DVS という DVS 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 4-6. 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。これは、分散論理ルーター インスタンスが Comp A のホストでは作成されないことを意味します。

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 ゾーンに存在す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 がバッキングする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。上記のとおり、これは分散論理ルーター インスタンスをホスト全体で論理スイッチと `dvPortgroup` に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 ルールにより、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、システムの稼働状況のインジケータが提供されています。

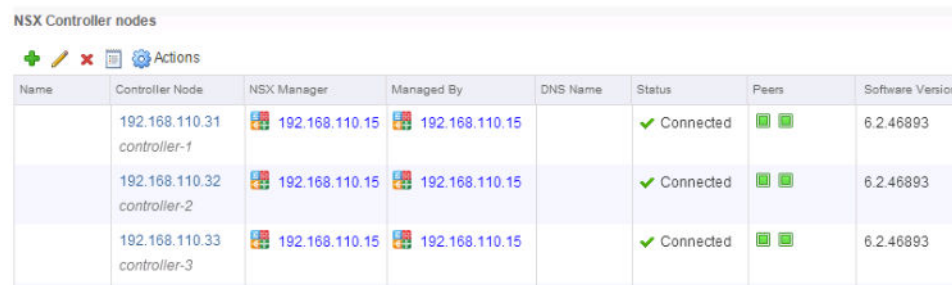
NSX のルーティング用ユーザー インターフェイス

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
esxmtg-02a.corp.l	Ready				vmk3: 192.168.120.52		
esxmtg-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。DVS 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 DVS のすべてのクラスタ 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。有効な/予期される IP アドレスが表示されていることを確認します。

一部のクラスタで DLR 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 DVS 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	Dashboard	Installation	Logical Switches	NSX Edges	Firewall	SpoolGuard		
Id	Name	Type	Version	Status	Tenant	Interfaces	Size	
edge-2	Local-Distributed-Router	Logical Router	6.2.3	Deployed	Default	4	Compact	
edge-3	Perimeter-Gateway-01	NSX Edge	6.2.3	Deployed	Default	2	Compact	
edge-4	OneArm-LoadBalancer-01	NSX Edge	6.2.3	Deployed	Default	1	Compact	
edge-5	Perimeter-Gateway-02	NSX Edge	6.2.3	Deployed	Default	2	Compact	
edge-6	OneArm-LoadBalancer-02	NSX Edge	6.2.3	Deployed	Default	1	Compact	
edge-9178...	Universal-Distributed-Router	Universal Distributed Router	6.2.3	Deployed	Default	4	Compact	

現在デプロイされているすべての DLR と 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 DLR 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 DLR に関する API 呼び出しに使用できます。
- [テナント] + [ID] で DLR 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、DLR 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 4-1. 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 DLR 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 DLR を破壊し、同じ設定を使用して新しい ESG または DLR 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 でサービスが有効にされたときに作成されます（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 DLR 制御仮想マシンからログ バンドルを作成できます。 DLR 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。
	[Appliance 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 資格情報の変更] を使用すると、オペレータは CLI 資格情報を強制更新できます。 ESG または DLR 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/DLR 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/DLR の Syslog に送信される詳細のレベルを変更できます。
	[詳細デバッグの構成] 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 DLR 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。
	DLR/ESG 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/DLR 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

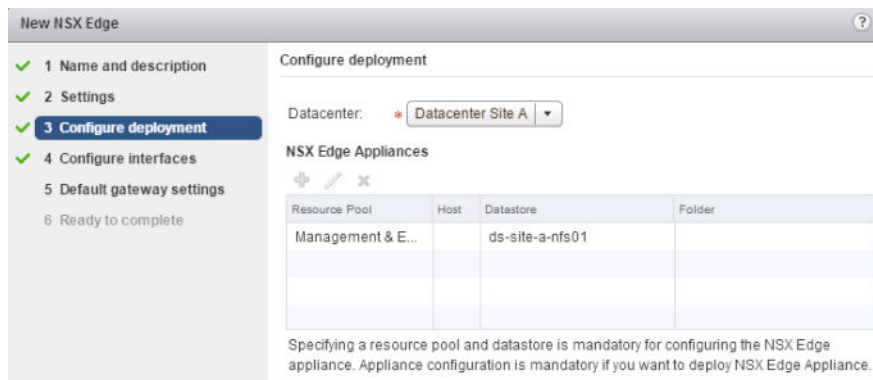
- [ユーザー名] と [パスワード] は、分散論理ルーター制御仮想マシンにアクセスするための CLI/仮想マシンの認証情報を設定します。NSX は、ESG または分散論理ルーター制御仮想マシンで AAA をサポートしません。このアカウントには、ESG/分散論理ルーター制御仮想マシンへの完全なアクセス権限がありますが、CLI/仮想マシン コンソールからは ESG/分散論理ルーターの設定は変更できません。

- [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。

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

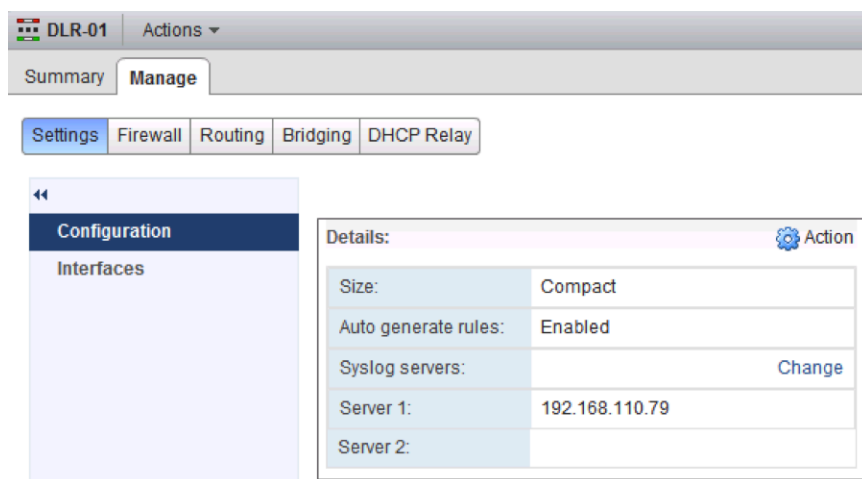
最初にデプロイした後、一般的に行われる設定がいくつかあります。

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。



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: ▼ ⓘ

MTU: 1500

Description:

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。

The screenshot shows the NSX Manager interface for DLR-01. The 'Route Redistribution' section is active. The 'Route Redistribution Status' shows OSPF as enabled (green checkmark) and BGP as disabled. The 'IP Prefixes' table is empty. The 'Route Redistribution table' contains one entry for OSPF, connected to the network, with the action 'Permit'.

Name	IP/Network
0 items	

Learner	From	Prefix	Action
OSPF	Connected	Any	Permit
1 items			

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にアクセスできます。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					
<div> + ✎ ✖ 🔄 📄 🔍 ⚙️ Actions </div>					
Name	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	0	
5005	N/A (headend replication)	Enabled (multicast proxy, ARP proxy)	192.168.110.202
(up)	1	0	
5006	N/A (headend replication)	Enabled (multicast proxy, ARP proxy)	192.168.110.203
(up)	1	0	
5007	N/A (headend replication)	Enabled (multicast proxy, ARP proxy)	192.168.110.202
(up)	1	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）。

```
~ # esxcfg-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 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。

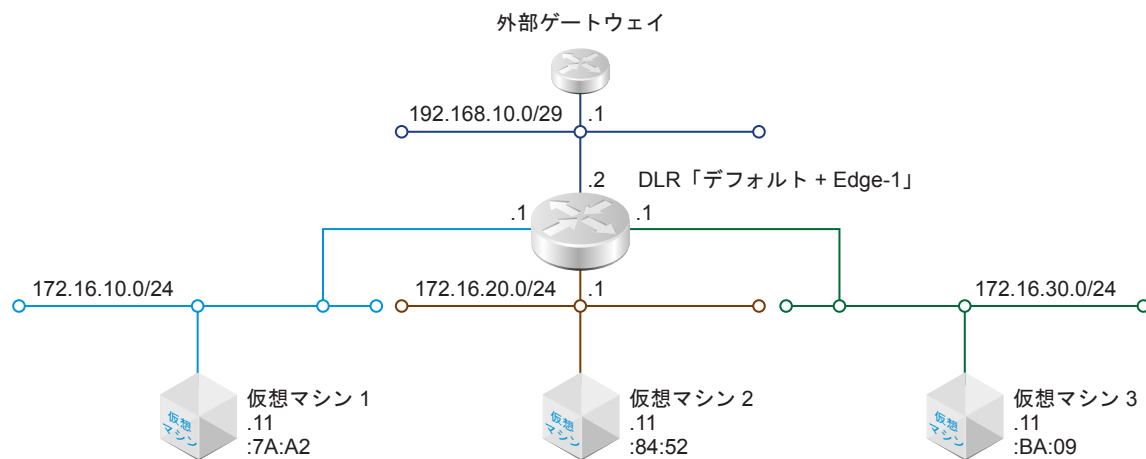
- インターフェイス テーブル（インターフェイスの IP アドレスおよびネットマスクを含む）
- ルーティング テーブル
- ARP テーブル

サンプル ルート トポロジを使用した DLR 状態の確認

このセクションでは、DLR 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取得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 DLR のセットを NSX で作成します。

図 4-7. 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 DLR 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。
- DLR 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。

[終了準備の完了] ウィザードの画面が上記の DRL に表示されます。

New NSX Edge

Ready to complete

1 Name and description
2 CLI credentials
3 Configure deployment
4 Configure interfaces
5 Configure HA
6 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

DLR 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 DLR 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 Lifes:   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 vmknics（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貫となります。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

DLR 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。DLR 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

DLR がパケットを送信するには、DLR がネクスト ホップの IP アドレスの ARP 要求を解決する必要があります。この解決プロセスの結果は、個々のホストのローカル DLR 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 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

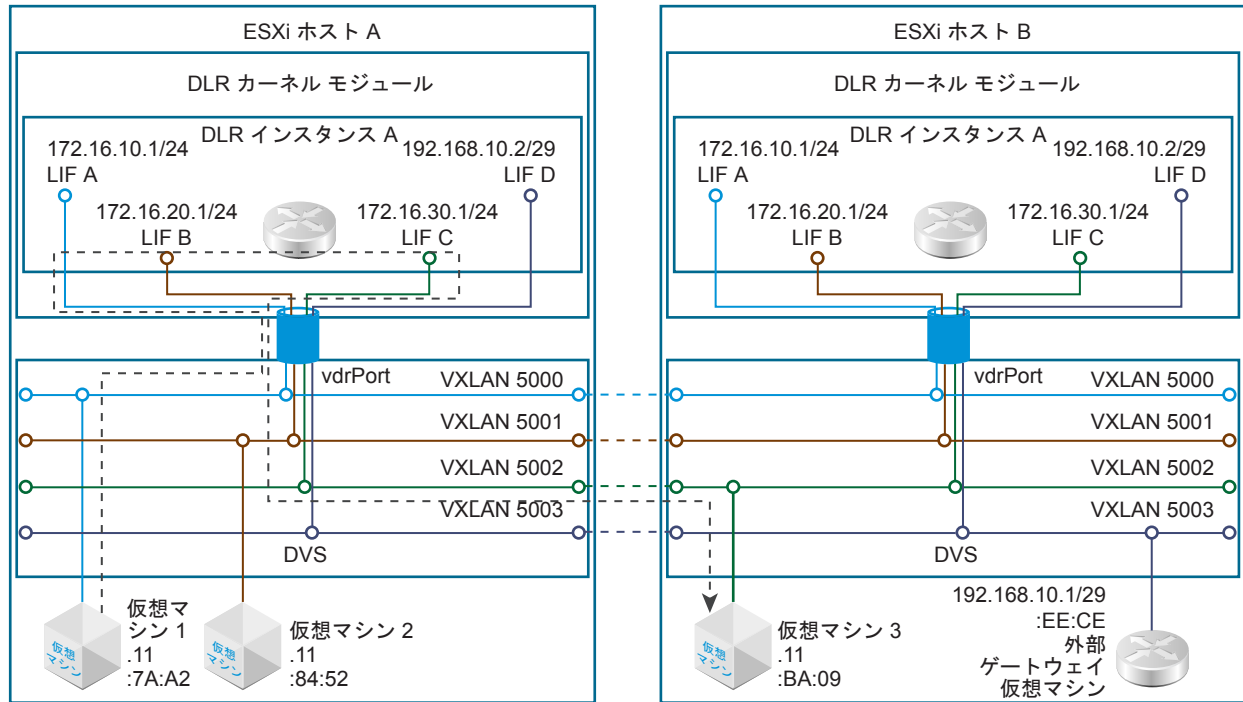
注：

- DLR 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動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、DLR 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。

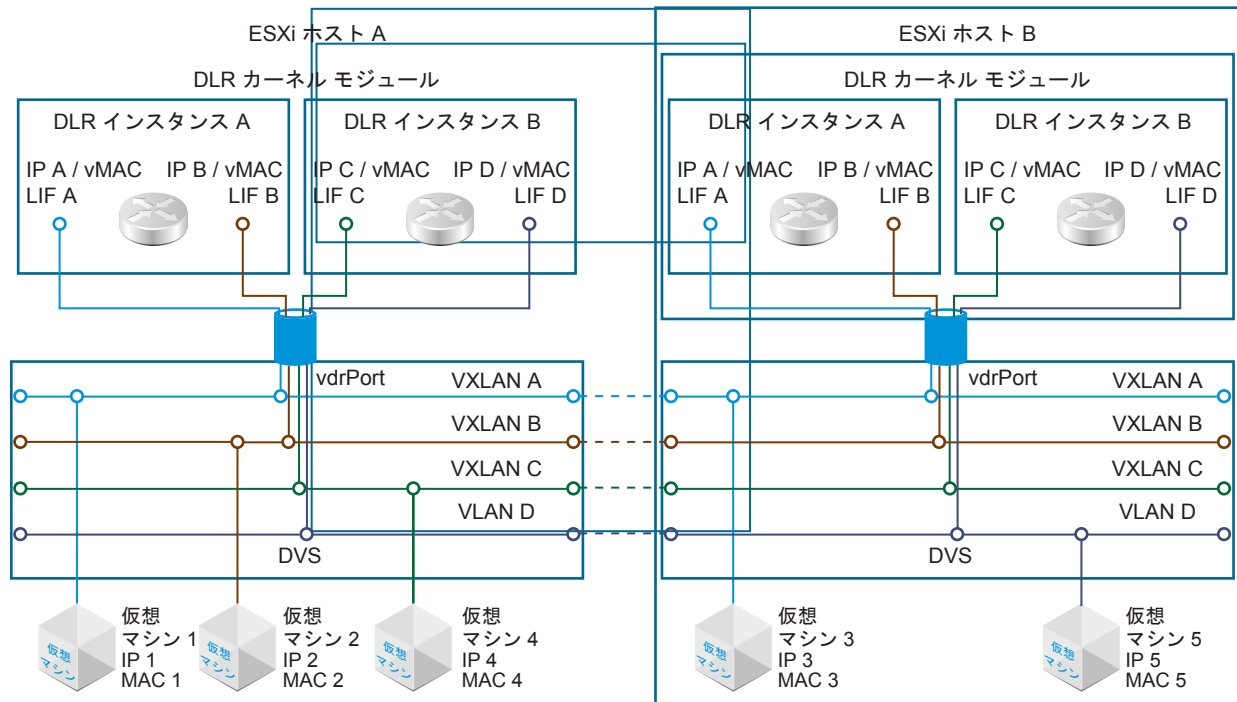
図 4-8. 2 台のホストと単一の分散論理ルーターインスタンス



- 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。

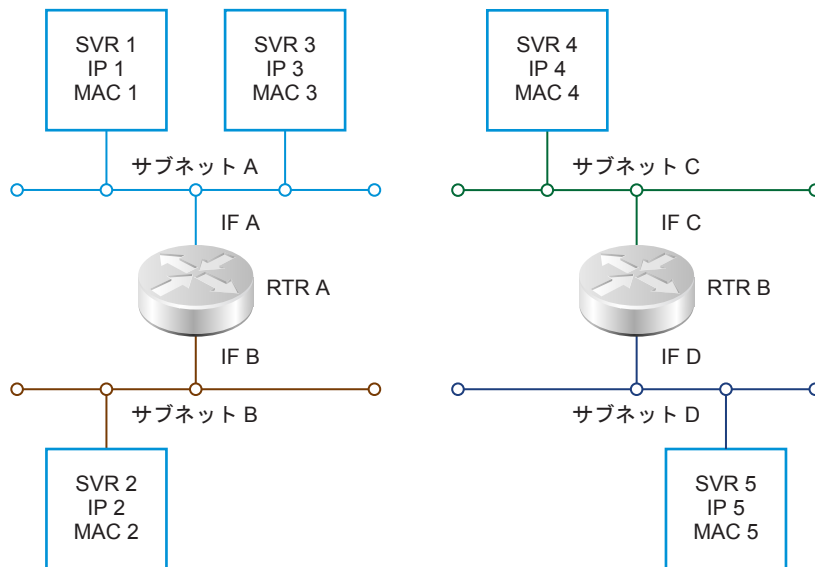
複数の分散論理ルーターインスタンスが存在する場合、次のような図になります。

図 4-9. 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 トポロジーに対応する場合があります。

図 4-10. 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 トポロジー



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）

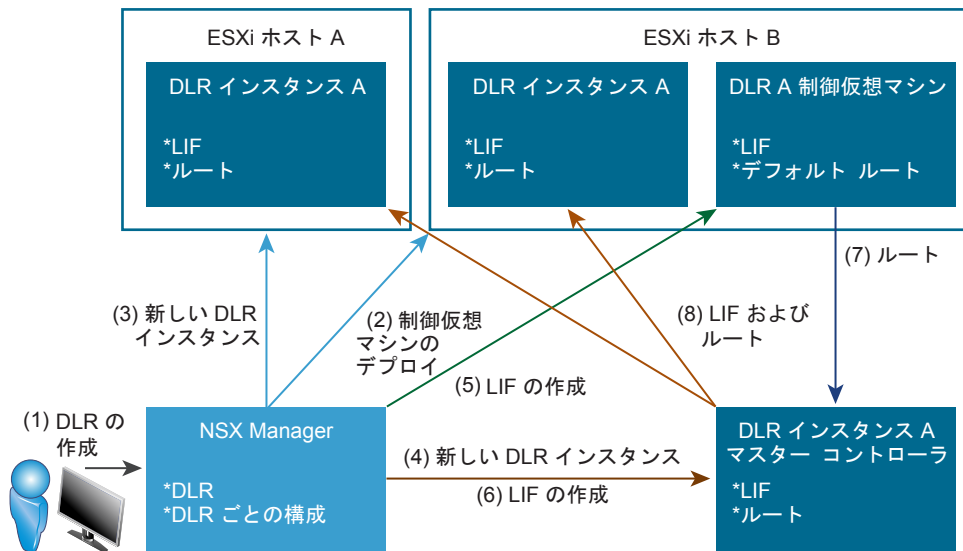
- 各サブネットのネクスト ホップ（ルーティング テーブルで検索）
- ネクスト ホップ（ARP テーブル）に到達するため、出力方向のフレームに挿入する MAC アドレス

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 4-11. 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 インターフェースのウィザードで [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。

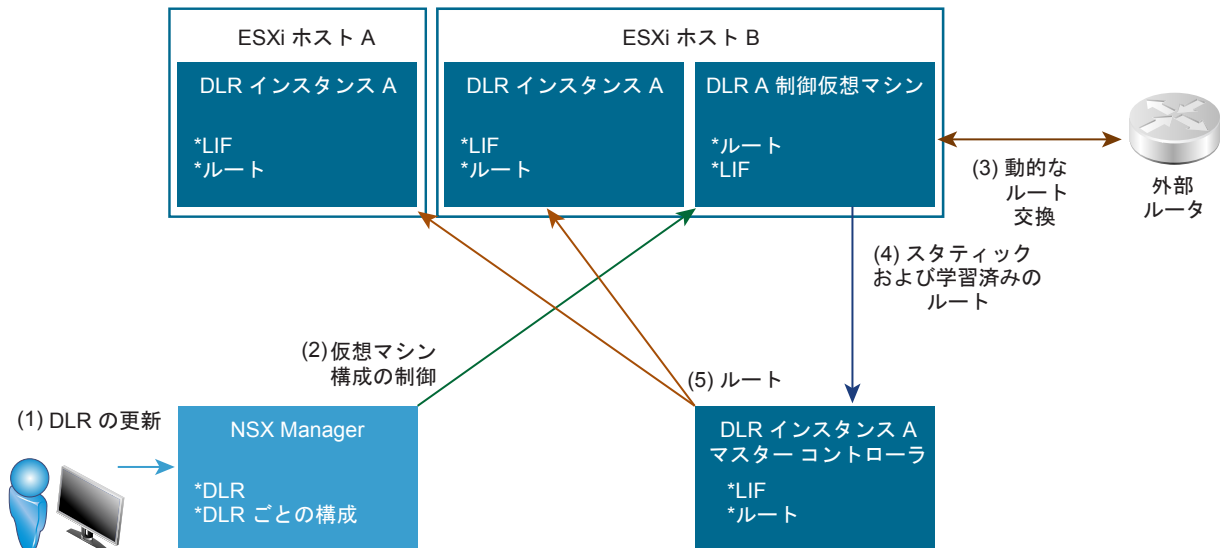
- 1 NSX Manager が、新しい分散論理ルーターをデプロイするための API 呼び出し（直接呼び出し、または vSphere Web Client ユーザー インターフェースのウィザードから呼び出し）を受信します。
- 2 NSX Manager は、リンクされている vCenter Server を呼び出し、分散論理ルーター制御仮想マシン 1 台（高可用性が要求されている場合は 2 台）をデプロイします。
 - a 設定を受信するには、分散論理ルーター制御仮想マシンをパワーオンし、NSX Manager に再接続します。
 - b 高可用性を実現するため、分散論理ルーター制御仮想マシンを 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ー リストを検索し、これらのクラスター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 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 4-12. 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。

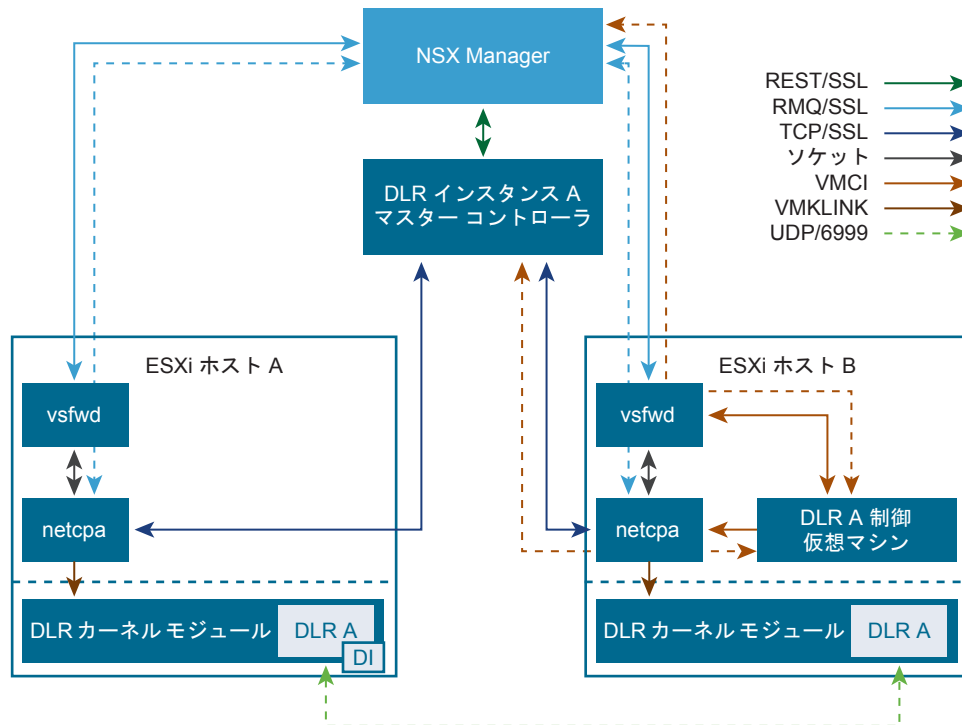
分散論理ルーター制御仮想マシンが実行している ESXi ホスト上の分散論理ルーター インスタンスは、分散論理ルーターのマスター コントローラ ノードのみから LIF とルートを受信し、分散論理ルーター制御仮想マシンや NSX Manager から直接受信することはありません。

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ンネルを示しています。

図 4-13. 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 チャンネル。このチャンネルは、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 クラスター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
              192.168.210.51
              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ー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:1c:fb/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:ae:08/64
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。

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 4-2. 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"> ■ 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 ■ データは失われない ■ データや制御プレーンは停止しない
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"> ■ 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 ■ 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 ■ データは失われない ■ データや制御プレーンは停止しない ■ 動的ルーティングの更新は引き続き動作する
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"> ■ 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 ■ データは失われない ■ データや制御プレーンは停止しない
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"> ■ 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 ■ 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 ■ 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）

コントローラ クラスタ

表 4-3. 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"> ■ 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 ■ 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 ■ 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 ■ 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
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"> ■ 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
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"> ■ 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 ■ 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
コントローラが相互の接続を失う	<ul style="list-style-type: none"> ■ 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 ■ 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 ■ 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 ■ 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働し続ける
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"> ■ コントローラ クラスタの冗長性が損なわれる ■ 管理/制御プレーンは通常どおりに稼働し続ける
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"> ■ 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

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 サンプリントを使用します。これらは、メッセージ パス (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 4-4. 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"> ■ 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
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"> ■ 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 ■ 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
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"> ■ 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 ■ 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 ■ ホストのデータパスは、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

表 4-5. 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 データパスのカーネル 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"> ■ ホストの分散ルーティングが機能しなくなる
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"> ■ 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 ■ 分散ルーティングのデータパスは、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

分散論理ルーター制御仮想マシン

表 4-6. 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"> ■ 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 ■ 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プ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
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"> ■ 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、以前に学習したプリフィックスとの間のトラフィックは影響を受けない
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"> ■ 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 ■ 動的ルーティングの更新は引き続き送信される
分散論理ルーター制御仮想マシンが、コントローラとの接続を失う	<ul style="list-style-type: none"> ■ 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

ルーティングに関連する NSX ログ

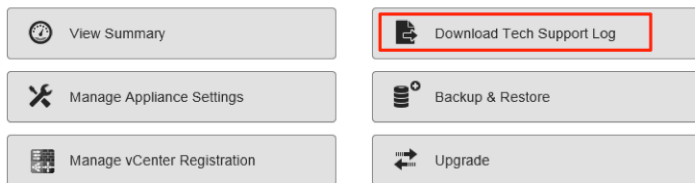
ベスト プラクティスとして、ログを中央のコレクタに送信するように NSX のすべてのコンポーネントを設定しすることをお勧めします。

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 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.<start-time-stamp>.log`
- `cloudnet/cloudnet_cpp.log.INFO`
- `cloudnet/cloudnet_cpp.log.nvp-controller.root.log.INFO.<start-time-stamp>`
- `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。

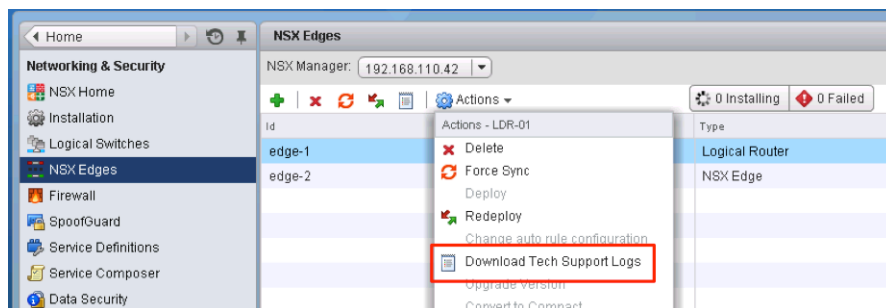
ESG/DLR 制御仮想マシンのログ

ESG および DLR 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。
 - コントローラの 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 DVS の dvUplink (チーミング ポリシー、名前、UUID)
 - ホストが把握する DLR 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、netcpa 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 4-7 に記載されています。

表 4-7. 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前を一覧表示します。
- 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。

```
dlr-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
```

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

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

```
dlr-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。

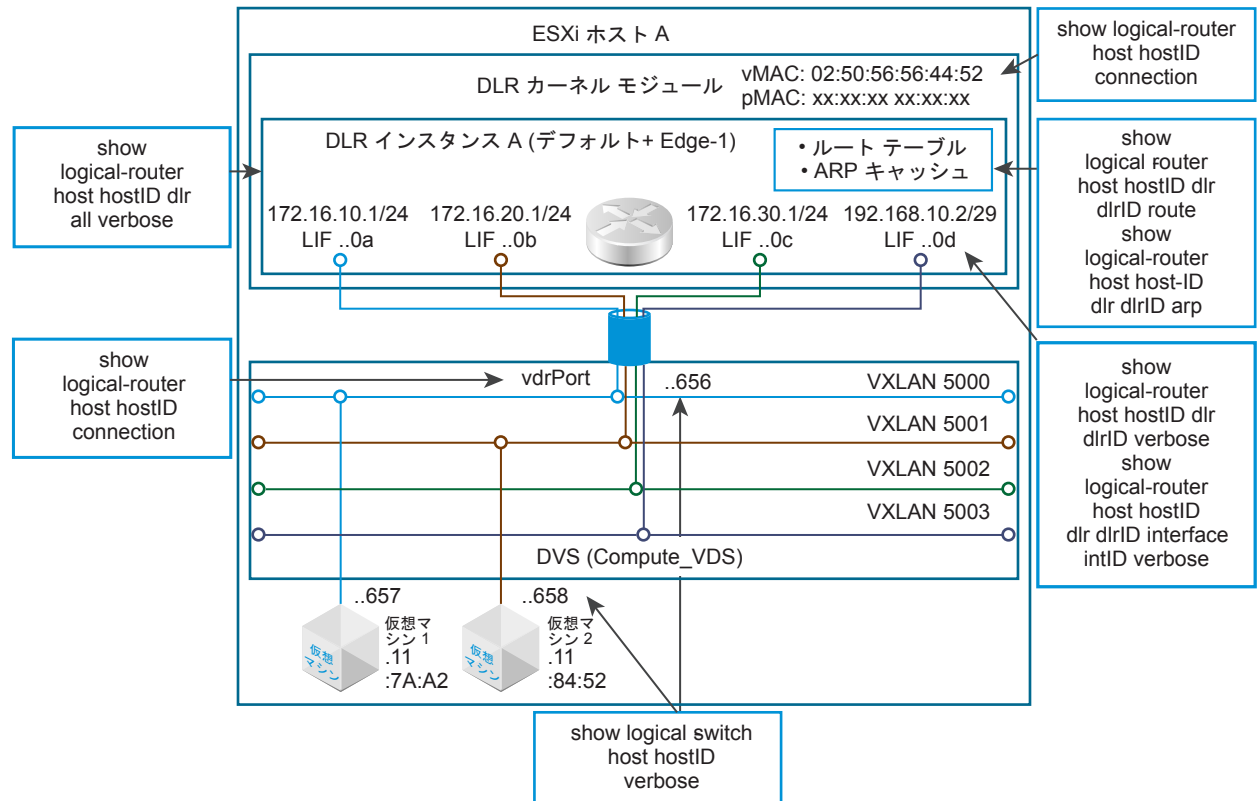
たとえば、次のコマンドは、SSH を除いて `vNic_0` を通過するすべてのトラフィックを表示し、インタラクティブセッション自体に属するトラフィックの検索は回避します。

```
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

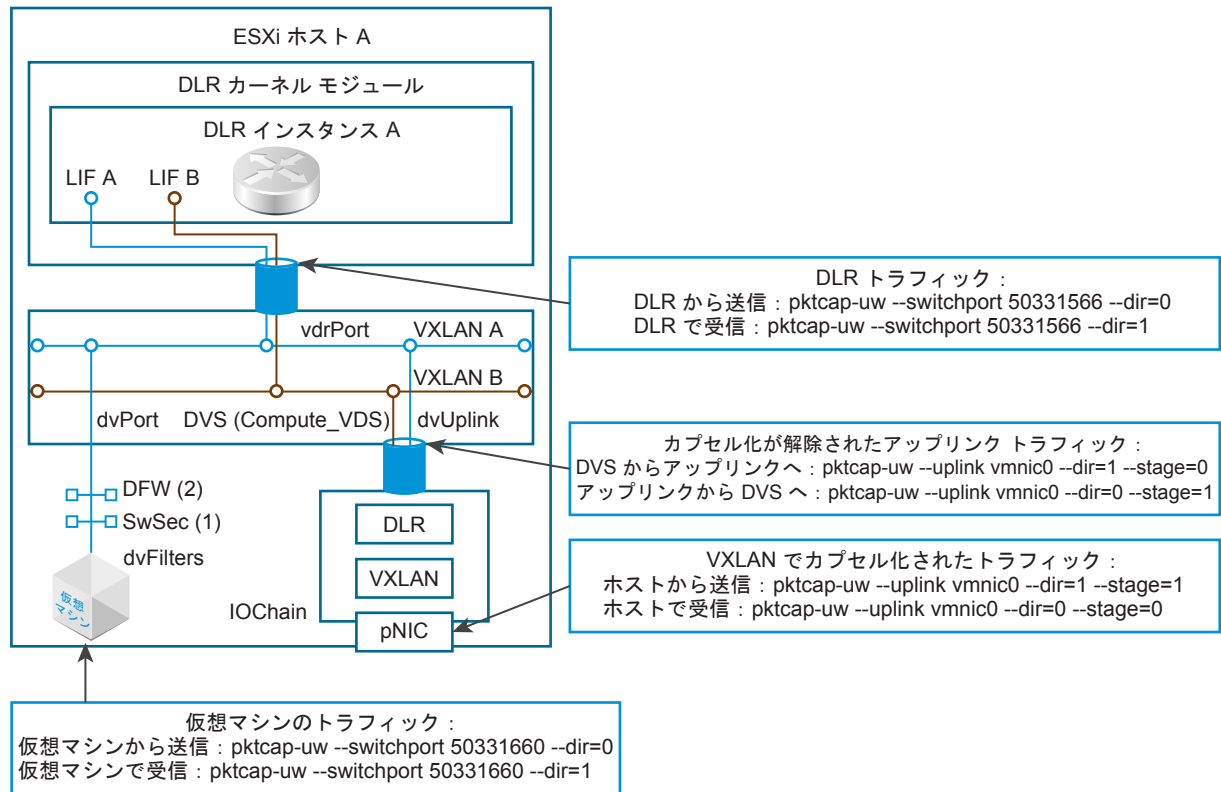
ホストは、NSX ルーティングと緊密に連携します。[図 4-14](#) は、ルーティングサブシステムに参加するコンポーネントとこれらの情報を表示するために使用される NSX Manager CLI コマンドを示しています。

図 4-14. 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 4-15 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 4-15. キャプチャ ポイントと関連する CLI コマンド



Edge Appliance のトラブルシューティング

5

このトピックでは、VMware NSX Edge Appliance 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 Appliance 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。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。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するのに、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 スイッチを調査します。

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。

ファイアウォールに関する問題

- 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。

Edge ファイアウォールでパケットがドロップする問題

- 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。一般的な理由には、非対称ルーティングの問題や TCP ベースのアプリケーションが 1 時間以上操作されていないなどがあります。非対称ルーティングの問題は、さらに次のような状況に示されます。

- Ping がある方向で動作するが、別方向では失敗する
- Ping が動作するが、TCP が動作しない

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)

```

- 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。

```
6:26:46pm up 28 days 20:01, 548 worlds, 3 VMs, 3 vCPUs; CPU load average: 0.14, 0.12, 0.12
PCPU USED(%): 7.2 32 AVG: 19
PCPU UTIL(%): 6.2 37 AVG: 21
```

ID	GID	NAME	NWLD	%USED	%RUN	%SYS	%WAIT	%VMWAIT	%RDY	%IDLE	%OVRP	%CSTP	%MLMTD	%SWFP
2	2	system	131	5.43	28.79	0.00	12908.50	-	35.03	0.00	24.03	0.00	0.00	0.00
88295638	88295638	esxtop.11413506	1	3.05	2.52	0.01	95.50	-	0.32	0.00	0.03	0.00	0.00	0.00
371958	371958	web-02a	6	1.18	0.84	0.34	588.66	0.00	0.27	97.90	0.00	0.00	0.00	0.00
368736	368736	web-01a	6	0.92	0.92	0.04	591.45	0.00	0.44	98.26	0.05	0.00	0.00	0.00
362728	362728	app-02a	6	0.60	0.62	0.01	589.15	0.89	0.23	96.68	0.00	0.00	0.00	0.00
14826	14826	netcpa.35043	21	0.30	0.30	0.00	2063.89	-	0.28	0.00	0.00	0.00	0.00	0.00
793	793	vmsyslogd.32996	5	0.28	0.27	0.00	491.39	-	0.16	0.00	0.00	0.00	0.00	0.00
8176	8176	hostd.34168	34	0.16	0.27	0.00	3340.26	-	0.42	0.00	0.00	0.00	0.00	0.00
19890	19890	vmttoolsd.35736	2	0.08	0.08	0.00	196.31	-	0.15	0.00	0.00	0.00	0.00	0.00
17967	17967	logchannellogge	1	0.07	0.07	0.00	98.31	-	0.05	0.00	0.00	0.00	0.00	0.00
6024	6024	storageRM.33890	1	0.07	0.01	0.05	98.36	-	0.00	0.00	0.00	0.00	0.00	0.00

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。

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。

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 Appliance 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。

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 vserdd
  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
...
```

また、**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できます。

```
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 -----

```

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

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。

メッセージバスのデバッグ

メッセージバスは、ESXi ホストの準備ができていないときに、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 ブローカーに接続できません。**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
```

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 Command Line Interface Reference』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
OutDestUnreaches : 152
OutParmProbs : 0
InSrcQuenches : 0
InRedirects : 0
OutSrcQuenches : 0
InDestUnreaches : 151
OutErrors : 0
InParmProbs : 0

```

Firewall Drop Counters

```
=====
```

Ipv4 Rules

```
=====
```

Chain - INPUT

```

rid pkts bytes target prot opt in out source destination state
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

```

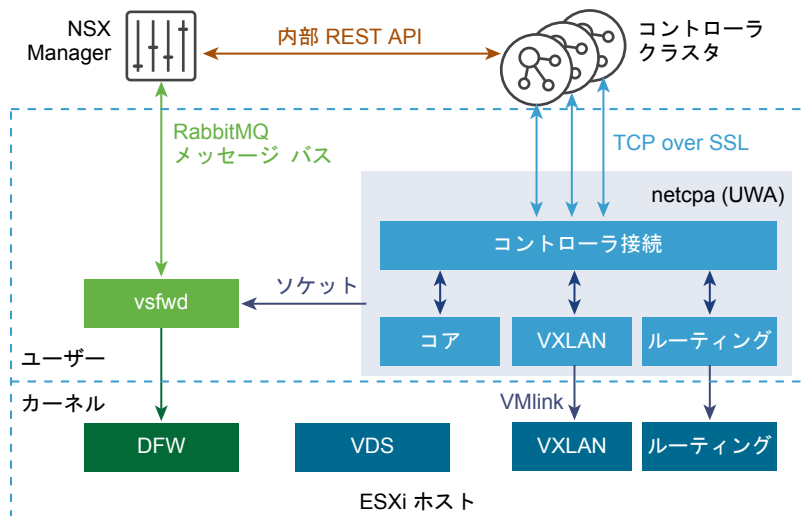
NSX Edge の管理において予期される動作

vSphere Web Client で、NSX Edge に L2 VPN を設定し、[サイト構成の詳細] 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。これは予期される動作です。

分散ファイアウォール

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。

図 6-1. ESXi ホストのユーザーおよびカーネル空間の図



この章には、次のトピックが含まれています。

- [show dfw CLI の使用方法](#)
- [Distributed Firewall のトラブルシューティング](#)

show dfw CLI の使用方法

NSX Manager の集中管理 CLI で Distributed Firewall に関するほぼすべての情報を取得できます。

次のコマンドを使用して、必要な情報を取得できます。

- 1 すべてのクラスタを表示：`show cluster all`
- 2 次に、特定のクラスタにあるホストを表示：`show cluster clusterID`
- 3 次に、ホストにあるすべての仮想マシンを表示：`show host hostID`
- 4 次に、フィルタ名および vNIC ID を含む仮想マシンの情報を表示：`show vm vmID`

次はその例です。

```
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

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

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

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

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 icmptype 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 icmptype 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;
}

```

Distributed Firewall のトラブルシューティング

このトピックでは、VMware NSX 6.x Distributed Firewall (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

Distributed Firewall ルールの発行に失敗する。

Distributed Firewall ルールの更新に失敗する。

原因

NSX Distributed Firewall 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、クラスター、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。Distributed Firewall 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され、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分散特性により、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容量が拡張されるスケール アウト アーキテクチャを実現できます。

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 ブローカー プロセスを通じて相互に通信します。使用される通信プロトコルは AMQP (Advanced Message Queueing Protocol) であり、チャンネルは SSL を使用して保護されます。ESXi ホストで、VSFW (vShield Firewall Daemon) プロセスは、ブローカーへの SSL 接続を確立して維持し、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。このときには、IPC を介して通信されます。

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、Distributed Firewall ルールの更新/発行を再試行します。

ソリューション

- 1 Distributed Firewall (DFW) を実行する前提条件を満たしていることを確認します。
 - VMware vCenter Server 5.5
 - VMware ESXi 5.1 または ESXi 5.5
 - VMware NSX 6.0 以降
- 2 DFW VIB がクラスタにある各 ESXi ホストに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。

以下はその例です。

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

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

- 3 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。

以下はその例です。

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

vShield-Stateful-Firewall is running
```

- 4 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。

以下はその例です。

```
# ps | grep vsfwd

107557 107557 vsfwd /usr/lib/vmware/vsfw/vsfwd
107574 107557 vsfwd /usr/lib/vmware/vsfw/vsfwd
107575 107557 vsfwd /usr/lib/vmware/vsfw/vsfwd
107576 107557 vsfwd /usr/lib/vmware/vsfw/vsfwd
107577 107557 vsfwd /usr/lib/vmware/vsfw/vsfwd
107578 107557 vsfwd /usr/lib/vmware/vsfw/vsfwd
```

- 5 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。

以下はその例です。

```
# 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
```

- 6 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
```

- 7 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>

- 8 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.
```

- 9 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>
```

- 10 `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。

以下はその例です。

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

- 11 `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、DFW 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。

以下はその例です。

```
# 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: esxfw
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
agentName: vmware-sfw          <===== DFW filter
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
agentName: vmware-sfw          <===== DFW filter
state: IOChain Attached
vmState: Detached
failurePolicy: failClosed
slowPathID: none
filter source: Dynamic Filter Creation

```

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

以下はその例です。

```

# 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;

```

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

以下はその例です。

```

# 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,
}

```

14 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

```

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導入されました。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 アドレススペ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。

DFW 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 DFW 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 コントローラ、および Edge Services Gateway は、DFW 機能から自動的に除外されます）。DFW 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 Distributed Firewall (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 (Networking and Security)] > [ファイアウォール (Firewall)] > [全般 (General)] タブで [構成のエクスポート (Export Configuration)] をクリックして取得できる Distributed Firewall の設定。これによって、Distributed Firewall 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。

ロード バランシング

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送信先まで複数のパスをたどれるようになります。受信サービス リクエストは、負荷配分がユーザーにとって透過的になるように、複数のサーバ間で均等に配分されます。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。

NSX のロード バランシングでは、以下の機能を利用できます。

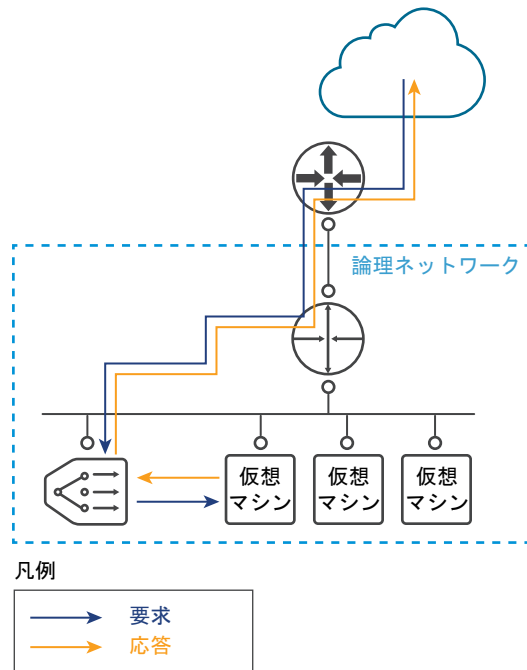
- プロトコル：TCP、HTTP、HTTPS
- アルゴリズム：重み付きラウンド ロビン、IP ハッシュ、URI、最小接続数
- AES-NI アクセラレーションによる SSL Termination
- SSL ブリッジ（クライアント側 SSL + サーバ側 SSL）
- SSL 証明書管理
- クライアントの識別のための X-header 転送
- L4/L7 透過モード
- 接続スロットリング
- メンテナンスのために個々のサーバ（プール メンバー）を有効/無効にできる
- 健全性チェックの方法（TCP、HTTP、HTTPS）
- 拡張健全性チェック モニター
- 永続的/継続的な方法：SourceIP、MSRDP、COOKIE、SSLSESSIONID
- ワンアーム モード
- URL の書き換えとリダイレクト
- iRule タイプのトラフィック シェーピングやコンテンツ切り替えのアプリケーション ルール
- L7 プロキシ ロード バランシングでの高可用性セッションの継続的なサポート
- IPv6 のサポート
- トラブルシューティングのための拡張ロード バランサ CLI
- すべてのサイズの Edge で利用可能
- 高パフォーマンス SLB で最適に調整された X-Large サイズ

この章には、次のトピックが含まれています。

- シナリオ：ワンアーム ロード バランサの構成
- ユーザー インターフェイスを使用したロード バランサの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

シナリオ：ワンアーム ロード バランサの構成

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。

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 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、VIP 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 モードよりも構成が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。

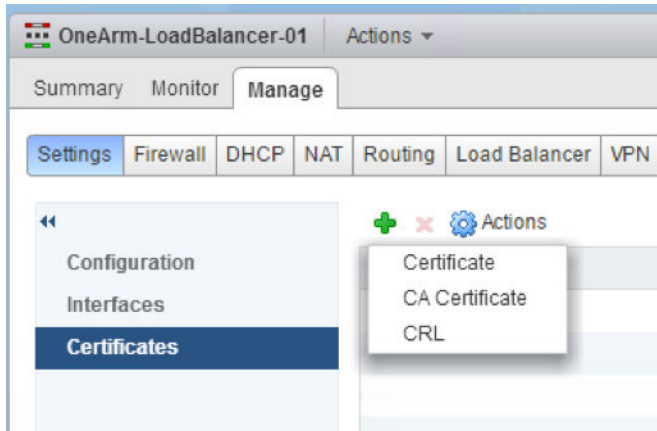
注: 接続の整合性を保証する方法には、通常、次の 2 つがあります。

- SNAT/プロキシ/非透過モード（上記で説明）
- DSR (Direct Server Return)

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 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 バランサー (Load Balancer)] > [グローバル構成 (Global Configuration)] > [編集 (Edit)] を選択して、ロード バランサー 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 バランサー (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 Certifica... **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 バランサー (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 バランサー (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。

Edit Pool

Name: * Web-Tier-Pool-01

Description:

Algorithm: ROUND-ROBIN

Algorithm Parameters:

Monitors: default_https_monitor

Members:

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

☐ Transparent

OK Cancel

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 バランサー (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 バランサー (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。

The screenshot shows the 'General' tab of a Virtual Server configuration. The 'Enable Virtual Server' checkbox is checked. Below it is the 'Enable Acceleration' checkbox, which is unchecked. The configuration fields are as follows:

- Application Profile: OneArmWeb-01 (dropdown menu)
- Name: Web-Tier-VIP-01 (text field)
- Description: (empty text field)
- IP Address: 172.16.10.10 (text field with a 'Select IP Address' button)
- Protocol: HTTPS (dropdown menu)
- Port: 443 (text field)
- Default Pool: Web-Tier-Pool-01 (dropdown menu)
- Connection Limit: 0 (text field)
- Connection Rate Limit: 0 (text field) (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。

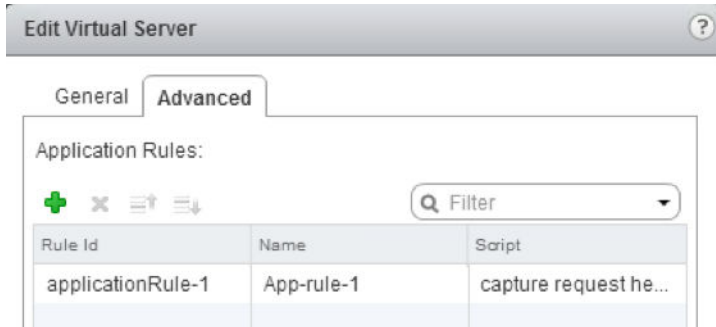
- 8 オプションで、アプリケーション ルールを使用している場合、[管理 (Manage)] > [ロード バランサー (Load Balancer)] > [アプリケーション ルール (Application Rules)] で設定を確認します。

The screenshot shows the 'Add Application Rule' dialog box. The 'Name' field contains 'App-Rule-1'. The 'Script' field contains the following text:

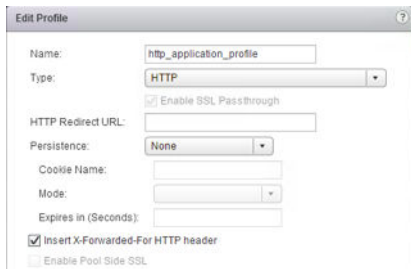
```
# A sample application rule to log the name of the
virtual server
capture request header Host len 32
```

- 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 バランサー (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。



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 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 ソース IP アドレスの値にヘッダー「X-Forwarded-For」を追加します。



ユーザー インターフェイスを使用したロード バランサのトラブルシューティング

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。

問題

期待どおりにトラブルシューティングできない

ソリューション

- 1 ユーザー インターフェイスから設定を確認します。
- 2 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。
- 3 デフォルトの HTTP/HTTPS ポート 80/443 が他のサービスに（SSL VPN など）によって使用されていないことを確認します。
- 4 メンバー ポートと監視ポートの設定を確認します。

設定に誤りがあると、健全性チェックでエラーが発生する場合があります。

- 5 レイヤー 4 ロード バランサ エンジンを使用している場合、以下を確認します。
 - a トラフィックが TCP プロトコルを使用している。
 - b データ保全またはレイヤー 7 が設定されていない。
 - c ロード バランサのグローバル設定で [アクセラレーションの有効化 (Enable Acceleration)] がオンになっている。
- 6 プールが透過（インライン）モードにある場合、Edge がリターン パスの内側にあることを確認します。仮想ワークロードのデフォルト ゲートウェイがロード バランサ ESG 以外の ESG を指定している場合、Edge はリターン パスの外側にある場合があります。

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

NSX CLI 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。

問題

ロード バランシングを期待とおりに実行できない

ソリューション

- 1 設定情報と統計情報を表示します。

```
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]
```

- 2 ロード バランサ エンジンのステータス (L4/L7) を確認します。

```
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
```

3 ロード バランサ プールのステータス (L4/L7) を確認します。

```
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)
```

4 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。

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)
```

```
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
```

- 5 サービス モニターのステータス (OK、WARNING、CRITICAL) 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
```

- 6 ログを確認します。

```
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
...
```

- 7 ロード バランサのセッション テーブルを確認します。

```
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
-----	--------	-------	--------	---------	-------------

- 8 ロード バランサ レイヤー 7 のスティッキー テーブル (sticky-table) のステータスを確認します。

```
nsxedge> show service loadbalancer table
```

L7 Loadbalancer Sticky Table Status:

TABLE	TYPE	SIZE(BYTE)	USED(BYTE)
-------	------	------------	------------

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 443 でロード バランシングが動作しない。
- ロード バランシング プールのメンバーが使用されない。
- Edge トラフィックのロード バランシングが行われない。
- レイア 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。
- プール メンバー監視ステータスが警告/重大になる。
- プール メンバーのステータスが無効になる。
- レイア 7 スティッキー テーブルがスタンバイ Edge と同期されない。

基本的なトラブルシューティング

- 1 vSphere Web Client でロード バランサの設定ステータスを確認します。
 - a [Networking and Security(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)] をクリックします。
 - d [ロード バランサー (Load Balancer)] タブをクリックします。
 - e 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 [Networking and Security (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)] をクリックします。

- d [ロード バランサー (Load Balancer)] タブをクリックします。
 - e 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。
 - f 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 この 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>
  </pool>
</loadBalancerStatusAndStats>
```

```

<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 コマンドラインからロードバランサの統計を確認するには、NSX Edge で次のコマンドを実行します。

特定の仮想マシンを対象とする場合は、最初に **show service loadbalancer virtual** を実行して仮想マシン名を取得します。次に **show statistics loadbalancer virtual <virtual-machine-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。