

# NSX-T トラブルシューティング ガイド

変更日：2018 年 6 月 5 日

VMware NSX-T Data Center 2.2



vmware®

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

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

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

Copyright © 2017, 2018 VMware, Inc. All rights reserved. [著作権および商標情報](#)。

# 目次

## NSX-T トラブルシューティング ガイド 5

### 1 レイヤー 2 接続のトラブルシューティング 6

- NSX Manager と NSX Controller のクラスタのステータスの確認 6
- 論理ポートの確認 7
- トランスポート ノードのステータスの確認 7
- 論理スイッチのステータスの確認 8
- 論理スイッチの CCP の確認 9
- ローカルの制御プレーンのステータスの確認 9
- Config セッションの問題のトラブルシューティング 10
- L2 セッションの問題のトラブルシューティング 11
- オーバーレイ論理スイッチのデータプレーンの問題のトラブルシューティング 12
- VLAN 論理スイッチのデータプレーンの問題のトラブルシューティング 13
- オーバーレイ論理スイッチの ARP 問題のトラブルシューティング 14
- VLAN 論理スイッチのパケット ロスまたは ARP が解決された場合のパケット ロスのトラブルシューティング 14

### 2 インストールのトラブルシューティング 16

### 3 ルーティングのトラブルシューティング 20

### 4 ファイアウォールのトラブルシューティング 22

- ESXi ホストに適用されるファイアウォール ルールの確認 22
- KVM ホストに適用されるファイアウォール ルールの確認 25
- ファイアウォール パケット ログ 26

### 5 ログおよびサービス 28

- ログ メッセージ 28
  - リモート ログの設定 29
  - ログ メッセージ ID 31
- Syslog 問題のトラブルシューティング 32
- サービスの確認 33
- サポート バンドルの収集 34

### 6 その他のトラブルシューティングの方法 36

- トランスポート ノードの追加または削除の失敗 36
- トランスポート ノードが別のコントローラに接続するには約 5 分間必要 37
- NSX Manager 仮想マシンが劣化状態である 37

NSX Agent で NSX Manager との通信がタイムアウトになる	39
ESXi ホストの追加に失敗する	40
NSX Controller の不正なステータス	40
IPFIX が有効の場合 KVM 仮想マシンの管理 IP アドレスにアクセスできない	41

# NSX-T トラブルシューティング ガイド

『NSX-T トラブルシューティング ガイド』は、NSX-T 環境で発生する問題のトラブルシューティング方法についての情報を提供します。

## 対象読者

このガイドは、NSX-T のシステム管理者向けです。読者は仮想化、ネットワーク、およびデータセンターの運用に精通していることを想定しています。

## VMware の技術ドキュメントの用語集

VMware は、新しい用語を集めた用語集を提供しています。VMware 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。

# レイヤー 2 接続のトラブルシューティング

# 1

たとえば、同じ論理スイッチに接続されている 2 つの仮想インターフェイス間で通信障害が発生した場合は、仮想マシン間で ping を実行できないため、このセクションの手順に沿って障害をトラブルシューティングします。

開始する前に、2 つの論理ポート間のトラフィックをブロックするファイアウォール ルールがないことを確認します。このセクションのトピックの順序に沿って接続の問題を解決することをお勧めします。

この章には、次のトピックが含まれています。

- NSX Manager と NSX Controller のクラスタのステータスの確認
- 論理ポートの確認
- トランスポート ノードのステータスの確認
- 論理スイッチのステータスの確認
- 論理スイッチの CCP の確認
- ローカルの制御プレーンのステータスの確認
- Config セッションの問題のトラブルシューティング
- L2 セッションの問題のトラブルシューティング
- オーバーレイ論理スイッチのデータプレーンの問題のトラブルシューティング
- VLAN 論理スイッチのデータプレーンの問題のトラブルシューティング
- オーバーレイ論理スイッチの ARP 問題のトラブルシューティング
- VLAN 論理スイッチのパケット ロスまたは ARP が解決された場合のパケット ロスのトラブルシューティング

## NSX Manager と NSX Controller のクラスタのステータスの確認

NSX Manager と NSX Controller のクラスタのステータスが正常で、コントローラが NSX Manager に接続されていることを確認します。

### 手順

- 1 ステータスが安定していることを確認するには、NSX Manager で次の CLI コマンドを実行します。

```
NSX-Manager> get management-cluster status
Number of nodes in management cluster: 1
- 192.168.110.47 (UUID 45A8869B-BB90-495D-8A01-69B5FCC56086) Online
```

```
Management cluster status: STABLE
```

```
Number of nodes in control cluster: 3
```

- 192.168.110.201 (UUID 45A8869B-BB90-495D-8A01-69B5FCC56086)
- 192.168.110.202 (UUID 45A8869B-BB90-495D-8A01-69B5FCC56086)
- 192.168.110.203 (UUID 45A8869B-BB90-495D-8A01-69B5FCC56086)

- 2 ステータスがアクティブであることを確認するには、NSX Controller で次の CLI コマンドを実行します。

```
NSX-Controller1> get control-cluster status
uuid: db4aa77a-4397-4d65-ad33-9fde79ac3c5c
is master: true
in majority: true

  uuid                                address                status
  ----                                -
0cfe232e-6c28-4fea-8aa4-b3518baef00d 192.168.110.201        active
bd257108-b94e-4e6d-8b19-7fa6c012961d 192.168.110.202        active
538be554-1240-40e4-8e94-1497e963a2aa 192.168.110.203        active
```

- 3 NSX Manager に接続されていることを確認するには、NSX Controller で次の CLI コマンドを実行します。

```
NSX-Controller1> get managers
- 192.168.110.47 Connected
```

## 論理ポートの確認

論理ポートが同じ論理スイッチ上で構成され、起動した状態であることを確認します。

### 手順

- 1 NSX Manager GUI から、論理ポートの UUID を取得します。
- 2 各論理ポートに対して次の API 呼び出しを実行し、論理ポートがすべて同じ論理スイッチ上にあることを確認します。

```
GET https://<nsx-mgr>/api/v1/logical-ports/<logical-port-uuid>
```

- 3 各論理ポートに対して次の API 呼び出しを実行し、起動した状態であることを確認します。

```
GET https://<nsx-mgr>/api/v1/logical-ports/<logical-port-uuid>/status
```

## トランスポート ノードのステータスの確認

トランスポート ノードのステータスを確認します。

### 手順

- ◆ トランスポート ノードのステータスを取得するには、次の API 呼び出しを実行します。

```
GET https://<nsx-mgr>/api/v1/transport-nodes/<transport-node-ID>/state
```

呼び出しが `RPC timeout` エラーを返す場合は、次のトラブルシューティング手順を実行します。

- `/etc/init.d/nsx-opsAgent status` を実行して、`opsAgent` が動作しているかを確認します。
- `/etc/init.d/nsx-mpa status` を実行して、`nsx-mpa` が動作しているかを確認します。
- `nsx-mpa` ハートビート ログで、`nsx-mpa` が NSX Manager に接続されているかどうかを確認します。
- `nsx-opsAgent` ログで、`opsAgent` が NSX Manager に接続されているかどうかを確認します。  
`opsAgent` が NSX Manager に接続されている場合、次のメッセージが表示されます。

```
Connected to mpa, cookie: ...
```

- `nsx-opsAgent` ログで、`opsAgent` が `HostConfigMsg` の処理を停止しているかどうかを確認します。停止している場合、RMQ 要求メッセージは表示されますが、応答は送信されないか、送信されるまでに大きな遅延が発生します。
- `opsAgent` が `HostConfigMsg` の実行中にクラッシュしたかどうかを確認します。
- RMQ メッセージがホストに配信されるまでに長い時間がかかっているかを確認するには、NSX Manager とホストのログ メッセージのタイムスタンプを比較します。

呼び出しが `partial_success` エラーを返す場合、多くの原因が考えられます。まず、`nsx-opsAgent` ログを確認します。ESXi ホストでは、`hostd.log` および `vmkernel.log` を確認します。KVM では、`syslog` にすべてのログが保持されます。

## 論理スイッチのステータスの確認

論理スイッチのステータスを確認します。

### 手順

- ◆ 論理スイッチのステータスを取得するには、次の API 呼び出しを実行します。

```
GET https://<nsx-mgr>/api/v1/logical-switches/<logical-switch-ID>/state
```

呼び出しが `partial_success` エラーを返す場合、応答には、NSX Manager が論理スイッチ構成のプッシュに失敗したか、または応答を取得しなかったトランスポート ノードのリストが含まれます。トラブルシューティングの手順は、トランスポート ノードの場合の手順に似ています。以下を確認します。

- 必要なすべてのコンポーネントがインストールされ実行されている。
- `nsx mpa` が NSX Manager に接続されている。
- `nsxa` が East-West 方向のスイッチングで接続されている。
- `nsxa.log` および `nsxaVim.log` で論理スイッチ ID を `grep` 検索し、論理スイッチ構成がトランスポート ノードによって受信されているかを確認します。
- `nsxa` と `nsx-mpa` でアップタイムを確認します。Syslog ファイルで `nsxa` ログ メッセージを `grep` 検索し、`nsxa` の起動と停止の時間を確認します。



- East-West 方向のスイッチングでの nsxa の接続時間を確認します。nsxa が East-West 方向に接続されていないときに論理スイッチの構成がホストに送信されると、構成がホストに配信されないことがあります。

KVM では、論理スイッチ構成はホストにプッシュされません。したがって、論理スイッチの問題のほとんどは管理プレーンに存在する可能性があります。

ESXi では、不透明ネットワークは論理スイッチにマッピングされます。論理スイッチを使用する場合、ユーザーは vCenter Server または vSphere API を使用して仮想マシンを不透明ネットワークに接続します。

## 論理スイッチの CCP の確認

論理スイッチが中央の制御プレーン (CCP) にあることを確認します。

### 手順

- ◆ NSX Controller で次の CLI コマンドを実行し、論理スイッチが存在することを確認します。

```
NSX-Controller1> get logical switches
VNI    UUID                                     Name
52104  feab22ec-94b2-46f4-88f8-f9d44a416272  ls1
```

**注：** この CLI コマンドでは、VLAN にバックアップされている論理スイッチはリストされません。

## ローカルの制御プレーンのステータスの確認

オーバーレイ論理スイッチの場合、ホストの netcpa が中央の制御プレーンに接続されていることを確認します。

### 前提条件

論理スイッチがあるコントローラを検索します。「[論理スイッチの CCP の確認](#)」を参照してください。

### 手順

- 1 論理スイッチがあるコントローラに SSH 接続します。
- 2 次のコマンドを実行し、コントローラにこの VNI に接続されているハイパーバイザーが表示されることを確認します。

```
get logical-switch 5000 connection-table
```

- 3 ハイパーバイザー上で、コマンド `/bin/nsxcli` を実行して NSX CLI を起動します。
- 4 次のコマンドを実行して、CCP セッションを取得します。

```
host1> get ccp-session
Session Index State Controller
Config 0      UP    10.33.74.163
L2      5000  UP    10.33.74.163
```

CCP クラスタ内のいずれかの CCP ノードに Config セッションが表示されます。オーバーレイ論理スイッチごとに、CCP クラスタ内のいずれかの CCP ノードに対する L2 セッションが表示されます。VLAN 論理スイッチの場合、CCP 接続はありません。

## Config セッションの問題のトラブルシューティング

CCP の Config セッションが起動していない場合は、MPA と netcpa のステータスを確認します。

### 手順

- 1 MPA が NSX Manager に接続されているかを確認するには、次の API 呼び出しを実行します。

```
GET https://<nsx-mgr>/api/v1/logical-ports/<logical-port-uuid>
```

- 2 ハイパーバイザー上で、/bin/nsxcli コマンドを実行して NSX CLI を起動します。
- 3 次のコマンドを実行して、node-uuid を取得します。

```
host1> get node-uuid
0c123dd4-8199-11e5-95e2-73cc1cd9b614
```

- 4 次のコマンドを実行して、NSX Manager が CCP 情報をホストにプッシュしたかを確認します。

```
cat /etc/vmware/nsx/config-by-vsm.xml
```

- 5 config-by-vsm.xml に CCP 情報がある場合は、トランスポート ノードがハイパーバイザー上で設定されているかを確認します。

NSX Manager はトランスポート ノードの作成ステップでハイパーバイザーのホスト証明書を送信します。CCP がホストからの接続を受け入れるには、ホスト証明書が必要です。

- 6 /etc/vmware/nsx/host-cert.pem でホスト証明書が有効かを確認します。

証明書は、NSX Manager がホストに対して保有している証明書と同じである必要があります。

- 7 次のコマンドを実行して netcpa のステータスを確認します。

ESXi の場合：

```
/etc/init.d/netcpad status
```

KVM の場合：

```
/etc/init.d/nsx-agent status
```

- 8 netcpa を起動または再起動します。

ESXi では、netcpa が動作していない場合は起動し、すでに動作している場合は再起動します。

```
/etc/init.d/netcpad start
```

```
/etc/init.d/netcpad restart
```

KVM では、netcpa が動作していない場合は起動し、すでに動作している場合は再起動します。

```
/etc/init.d/nsx-agent start
```

```
/etc/init.d/nsx-agent restart
```

- 9 Config セッションが起動していない場合は、テクニカル サポート バンドルを収集し、VMware サポートにお問い合わせください。

## L2 セッションの問題のトラブルシューティング

これは、オーバーレイ論理スイッチのみに適用されます。

### 手順

- 1 ハイパーバイザー上で、/bin/nsxcli コマンドを実行して NSX CLI を起動します。
- 2 次のコマンドを実行して論理スイッチがホストに存在するかを調べます。

```
host1> get logical-switches
```

- 3 ポートの状態が admin down でないことを確認します。

ESXi では、net-dvs を実行して応答を確認します。次はその例です。

```
port 63eADF53-ff92-4a0e-9496-4200e99709ff:
com.vmware.port.extraConfig.opaqueNetwork.id = ... <- this should match the logical switch UUID
com.vmware.port.opaque.network.id = ... <- this should match the logical switch UUID
com.vmware.port.opaque.network.type = nsx.LogicalSwitch , propType = RUNTIME
com.vmware.common.port.block = false, ... <- Make sure the value is false.
com.vmware.vswitch.port.vxlan = ...
com.vmware.common.port.volatile.status = inUse ... <- make sure the value is inUse.
```

論理ポートがブロックされた状態で終了する場合は、テクニカル サポート バンドルを収集し、VMware サポートにお問い合わせください。その一方で、次のコマンドを実行して分散仮想スイッチ名を取得します。

```
[root@host1:~] net-dvs | grep nsx-switch
com.vmware.common.alias = nsx-switch , propType = CONFIG
```

次のコマンドを実行して、ポートのブロックを解除します。

```
[root@host1:~] net-dvs -s com.vmware.common.port.block=false <DVS-NAME> -p <logical-port-ID>
```

KVM では、ovs-vsctl list interface を実行し、対応する VIF UUID とのインターフェイスが存在し、admin\_state が起動していることを確認します。external-ids:iface-id の OVSDb に VIF UUID と表示されます。

## オーバーレイ論理スイッチのデータプレーンの問題のトラブルシューティング

このセクションの手順は、構成およびランタイムの状態が正常なときに、オーバーレイ スイッチを介して、異なるハイパーバイザー上の仮想マシン間の接続の問題をトラブルシューティングを行う場合に使用します。

仮想マシンが同じハイパーバイザー上にある場合は、[オーバーレイ論理スイッチの ARP 問題のトラブルシューティング](#)に進みます。

### 手順

- 1 論理スイッチを持つコントローラ上で次のコマンドを実行し、CCP に正しい VTEP リストがあるかどうかを確認します。

```
controller1> get logical-switch 5000 vtep
```

- 2 各ハイパーバイザー上で、次の NSX CLI コマンドを実行して、正しい VTEP リストがあるかどうかを確認します。

ESXi の場合：

```
host1> get logical-switch <logical-switch-UUID> tep-table
```

または、VTEP 情報を調べるために次のシェル コマンドを実行することもできます。

```
[root@host1:~] net-vd12 -M vtep -s vds -n VNI
```

KVM の場合：

```
host1> get logical-switch <logical-switch-UUID or VNI> tep-table
```

- 3 ハイパーバイザー上の VTEP が相互に ping を実行できるかどうかを確認します。

ESXi Shell プロンプトの場合：

```
host1> ping ++netstack=vxlan <remote-VTEP-IP>
```

KVM シェル プロンプトの場合：

```
host1> ping <remote-VTEP-IP>
```

VTEP が相互に ping を実行できない場合は、

- a トランスポート ノードを作成するときに指定したトランスポート VLAN が、アンダーレイで期待されるものと一致することを確認します。アンダーレイでアクセス ポートを使用している場合は、トランスポート VLAN を 0 に設定します。トランスポート VLAN を指定する場合、ハイパーバイザーが接続するアンダーレイ スイッチ ポートは、この VLAN をトランク モードで受け入れるように設定する必要があります。
- b アンダーレイの接続を確認します。

#### 4 VTEP 間で BFD セッションが起動しているかを確認します。

ESXi では、`net-vd12 -M bfd` を実行して応答を確認します。次はその例です。

```
BFD count: 1
=====
Local IP: 192.168.48.35, Remote IP: 192.168.197.243, Local State: up, Remote State: up, Local
Diag: No Diagnostic, Remote Diag: No Diagnostic, minRx: 1000000, isDisabled: 0
```

KVM では、リモート IP アドレスへの GENEVE インターフェイスを見つけます。

```
ovs-vsctl list interface <GENEVE-interface-name>
```

インターフェイス名が不明の場合は、すべてのトンネル インターフェイスを返す `ovs-vsctl find Interface type=geneve` を実行します。BFD 情報を確認します。

リモート VTEP への GENEVE インターフェイスが見つからない場合は、`nsx-agent` が実行中で、OVS 統合ブリッジが `nsx-agent` に接続されているかを確認します。

```
[root@host1 ~]# ovs-vsctl show
96c9e543-fc68-448a-9882-6e161c313a5b
  Manager "tcp:127.0.0.1:6632"
    is_connected: true
  Bridge nsx-managed
    Controller "tcp:127.0.0.1:6633"
      is_connected: true
    Controller "unix:ovs-l3d.mgmt"
      is_connected: true
    fail_mode: secure
```

## VLAN 論理スイッチのデータプレーンの問題のトラブルシューティング

このセクションの手順は、構成およびランタイムの状態が正常なときに、アンダーレイで構成された VLAN を介して、異なるハイパーバイザー上の仮想マシン間の接続の問題のトラブルシューティングを行う場合に使用します。

仮想マシンが同じハイパーバイザー上にあり、構成およびランタイムの状態がすべて正常であれば、[オーバーレイ論理スイッチの ARP 問題のトラブルシューティング](#)に進みます。

### 手順

- ◆ アンダーレイが、トランク モードの論理スイッチの VLAN 用に設定されていることを確認します。

ESXi では、`net-dvs` を実行して論理ポートを検索し、論理ポートで VLAN が設定されていることを確認します。次はその例です。

```
port 63eadf53-ff92-4a0e-9496-4200e99709ff:
  com.vmware.common.port.volatile.vlan = VLAN 1000 propType = RUNTIME VOLATILE
```

KVM では、VLAN 論理スイッチが統合ブリッジ上のオープンフロー ルールとして設定されています。つまり、仮想インターフェイスから受信したトラフィックの場合、VLAN X を使用してタグ付けし、パッチ ポート上で PIF ブリッジに転送します。`ovs-vsctl list interface` を実行し、NSX 管理対象ブリッジと NSX スイッチ ブリッジの間にパッチ ポートが存在することを確認します。

## オーバーレイ論理スイッチの ARP 問題のトラブルシューティング

このセクションの手順は、オーバーレイ スイッチでパケット ロスが発生している場合のトラブルシューティングで使用します。

VLAN にバックアップされている論理スイッチの場合は、[VLAN 論理スイッチのパケット ロスまたは ARP が解決された場合のパケット ロスのトラブルシューティング](#)を参照してください。

次のトラブルシューティング手順を実行する前に、各仮想マシンで `arp -n` コマンドを実行します。ARP が両方の仮想マシンで正常に解決された場合は、このセクションの手順を実行する必要はありません。次のセクション [VLAN 論理スイッチのパケット ロスまたは ARP が解決された場合のパケット ロスのトラブルシューティング](#)に進んでください。

### 手順

- ◆ 両方のエンドポイントが ESXi で、論理スイッチ上で ARP プロキシが有効になっている場合（これはオーバーレイ論理スイッチでのみサポートされます）、CCP およびハイパーバイザーの ARP テーブルを確認します。

CCP の場合：

```
controller1> get logical-switch 5000 arp-table
```

ハイパーバイザーで、NSX CLI を起動して次のコマンドを実行します。

```
host1> get logical-switch <logical-switch-UUID> arp-table
```

ARP テーブルを取得することで、ARP プロキシの状態が正しいかどうかを確認できます。ARP 応答がプロキシ経由で受信されない場合、またはホストが KVM で ARP プロキシをサポートしていない場合は、データベースが ARP 要求をブロードキャストします。この場合、BUM トラフィック転送の問題が発生している可能性があります。次の手順を試行してください。

- 論理スイッチのレプリケーション モードが MTEP の場合、NSX Manager の GUI で論理スイッチのレプリケーション モードを SOURCE に変更します。この方法で問題が解決されると、ping は正常に動作を開始します。
- 静的 ARP エントリを追加し、データベースの残りの部分が機能するかどうかを確認します。

## VLAN 論理スイッチのパケット ロスまたは ARP が解決された場合のパケット ロスのトラブルシューティング

自動トレースフロー ツールを使用するか、パケットを手動でトレースして、パケット ロスのトラブルシューティングを実行できます。

NSX Manager の GUI からトレースフロー ツールを実行するには、[ツール] - [トレースフロー]の順に移動します。詳細については、NSX-T 管理ガイドを参照してください。

## 手順

- ◆ パケットを手動でトレースするには：

ESXi では、`net-stats -l` を実行して、仮想インターフェイス (VIF) のスイッチポート ID を取得します。ソースとターゲットの仮想インターフェイスが同じハイパーバイザーにある場合は、次のコマンドを実行します。

```
pktcap-uw --switchport <src-switch-port-ID> --dir=0
pktcap-uw --switchport <dst-switch-port-ID> --dir=1
```

ソースとターゲットの仮想インターフェイスが別のハイパーバイザーにある場合は、ソースの仮想インターフェイスをホストしているハイパーバイザーで、次のコマンドを実行します。

```
pktcap-uw --switchport <src-switch-port-ID> --dir=0
pktcap-uw --uplink <uplink-name> --dir=1
```

ターゲットの仮想インターフェイスをホストしているハイパーバイザーで、次のコマンドを実行します。

```
pktcap-uw --uplink <uplink-name> --dir=0
pktcap-uw --switchport <dest-switch-port-ID> --dir=1
```

KVM では、ソースとターゲットの仮想インターフェイスが同じハイパーバイザーにある場合は、次のコマンドを実行します。

```
ovs-dpctl dump-flows
```

# インストールのトラブルシューティング

## 2

このセクションでは、インストールの問題のトラブルシューティングに関する情報を提供します。

### 基本的なインフラストラクチャ サービス

次のサービスがアプライアンスとハイパーバイザーで実行されている必要があります。また、vCenter Server をコンピュート マネージャとして使用している場合は、vCenter Server でも実行されている必要があります。

- NTP
- DNS

ファイアウォールが NSX-T コンポーネントとハイパーバイザーの間のトラフィックをブロックしていないことを確認します。コンポーネント間で必要なポートが開いていることを確認します。

NSX Manager の DNS キャッシュをフラッシュするには、SSH で root として NSX Manager にログインして次のコマンドを実行します。

```
root@nsx-mgr-01:~# /etc/init.d/resolvconf restart
[ ok ] Restarting resolvconf (via systemctl): resolvconf.service.
```

次に DNS 設定ファイルを確認できます。

```
root@nsx-mgr-01:~# cat /etc/resolv.conf
# Dynamic resolv.conf(5) file for glibc resolver(3) generated by resolvconf(8)
#     DO NOT EDIT THIS FILE BY HAND -- YOUR CHANGES WILL BE OVERWRITTEN
nameserver 192.168.253.1
search mgt.sg.lab
```

### ホストからコントローラへの通信の確認と管理

ESXi ホストでの NSX-T CLI コマンドの使用例：

```
esxi-01.corp.local> get managers
- 192.168.110.19    Connected

esxi-01.corp.local> get controllers
Controller IP      Port    SSL      Status      Is Physical Master  Session State  Controller
FQDN
192.168.110.16    1234    enabled  connected    true            up              NA
```



KVM ホストでの NSX-T CLI コマンドの使用例：

```
kvm-01> get managers
- 192.168.110.19    Connected

kvm-01> get controllers
Controller IP      Port      SSL        Status      Is Physical Master  Session State  Controller
FQDN
192.168.110.16    1234     enabled    connected                    true            up            NA
```

ESXi ホストでのホスト CLI コマンドの使用例：

```
[root@esxi-01:~] esxcli network ip connection list | grep 1234
tcp          0          0 192.168.110.53:42271          192.168.110.16:1234
ESTABLISHED  67702     newreno    netcpa
[root@esxi-01:~]
[root@esxi-01:~] esxcli network ip connection list | grep 5671
tcp          0          0 192.168.110.253:11721        192.168.110.19:5671  ESTABLISHED  2103688
newreno     mpa
tcp          0          0 192.168.110.253:30977        192.168.110.19:5671  ESTABLISHED  2103688
newreno     mpa
```

KVM ホストでのホスト CLI コマンドの使用例：

```
root@kvm-01:/home/vmware# netstat -nap | grep 1234
tcp          0          0 192.168.110.55:53686        192.168.110.16:1234  ESTABLISHED  2554/netcpa
root@kvm-01:/home/vmware#
root@kvm-01:/home/vmware#
root@kvm-01:/home/vmware# netstat -nap | grep 5671
tcp          0          0 192.168.110.55:50108        192.168.110.19:5671  ESTABLISHED  2870/mpa
tcp          0          0 192.168.110.55:50110        192.168.110.19:5671  ESTABLISHED  2870/mpa

root@kvm-01:/home/vmware# tcpdump -i ens32 port 1234 | grep kvm-01
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on ens32, link-type EN10MB (Ethernet), capture size 262144 bytes
<truncated output>
03:46:27.040461 IP nsxcontroller01.corp.local.1234 > kvm-01.corp.local.38754: Flags [P.], seq
3315301231:3315301275, ack 2671171555, win 323, length 44
03:46:27.040509 IP kvm-01.corp.local.38754 > nsxcontroller01.corp.local.1234: Flags [.], ack 44, win
1002, length 0
^C
<truncated output>
root@kvm-01:/home/vmware#

root@kvm-01:/home/vmware# tcpdump -i ens32 port 5671 | grep kvm-01
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on ens32, link-type EN10MB (Ethernet), capture size 262144 bytes
03:51:16.802934 IP kvm-01.corp.local.58954 > nsxmgr01.corp.local.amqps: Flags [P.], seq 1153:1222,
ack 1790, win 259, length 69
03:51:16.823328 IP nsxmgr01.corp.local.amqps > kvm-01.corp.local.58954: Flags [P.], seq 1790:1891,
ack 1222, win 254, length 101
^C
<truncated output>
```

## ホストの登録の失敗

NSX-T で誤った IP アドレスを使用すると、ホストの登録に失敗します。この問題は、ホストに複数の IP アドレスが割り当てられている場合に発生する可能性があります。トランスポート ノードを削除しようとする、そのノードは実体のない状態で残ります。問題の解決方法：

- [ファブリック] > [ノード] > [ホスト] の順に移動してホストを編集し、管理用を除くすべての IP アドレスを削除します。
- エラーをクリックし、[解決] を選択します。

## KVM ホストの問題

KVM ホストの問題は、ディスク容量の不足によって発生することがあります。/boot ディレクトリが短時間で容量不足になり、次のようなエラーが発生する可能性があります。

- ホストでのソフトウェアのインストールに失敗しました
- デバイスに容量が残っていません

コマンド [df-h] を実行すると、使用可能なストレージを確認できます。/boot ディレクトリが 100% である場合は、次の操作を行うことができます。

- `sudo dpkg --get-selections | grep ^ii` を実行して、インストールされているすべてのカーネルを確認します。
- `uname -r` を実行して、現在実行中のカーネルを確認します。このカーネル（linux イメージ）を削除しないでください。
- 不要となったイメージは、`apt-get purge` を使用して削除します。たとえば、`sudo apt-get purge linux-image-3.13.0-32-generic linux-image-3.13.0-33-generic` を実行します。
- ホストを再起動します。
- NSX Manager でエラーをチェックし、[解決] を選択します。
- 仮想マシンがパワーオン状態であることを確認します。

## Edge 仮想マシン展開時の設定エラー

Edge 仮想マシンの展開後、NSX Manager に仮想マシンのステータスとして [設定エラー] が表示されます。NSX Manager のログには、次の内容のメッセージが記録されています。

```
nsx-manager NSX - FABRIC [nsx@6876 comp="nsx-manager" errorCode="MP16027" subcomp="manager"] Edge
758ad396-0754-11e8-877e-005056abf715 is not ready for configuration error occurred, error detail is
NSX Edge configuration has failed. The host does not support required cpu features: ['aes'].
```

Edge データパス サービスを再起動すると、仮想マシンによってこの問題が解決されます。

## トランスポート ノードの強制的な削除

次の API 呼び出しを実行して、実体のない状態で停止しているトランスポート ノードを削除できます。

```
DELETE https://<NSX Manager>/api/v1/transport-nodes/<TN ID>?force=true
```

NSX Manager では、ホスト上でアクティブな仮想マシンが実行されているかどうかは検証されません。N-VDS および VIB を削除するのは、管理者の責任です。コンピュート マネージャを使用して追加したノードがある場合は、最初にコンピュート マネージャを削除し、次にノードを削除します。トランスポート ノードも一緒に削除されます。

# ルーティングのトラブルシューティング

# 3

NSX-T には、ルーティングの問題をトラブルシューティングするためのツールが組み込まれています。

## トレースフロー

トレース フローを使用して、パケットのフローを検査できます。配信、ドロップ、受信、および転送されたパケットを表示できます。パケットがドロップされた場合は、理由が表示されます。たとえば、パケットは、ファイアウォール ルールによってドロップされることがあります。

## ルーティング テーブルの確認

サービス ルーターのルーティング テーブルを表示するには、次のコマンドを実行します。

```
edge01> get logical-router
Logical Route
UUID                                VRF    LR-ID  Name                                Type
Ports
736a80e3-23f6-5a2d-81d6-bbefb2786666 0       0      SR-t0-router                        TUNNEL                                3
c9393d0c-1fcf-4c34-889d-2da1eeee25b8 1       10     SR-t0-router                        SERVICE_ROUTER_TIER0                 5
9333c94e-5938-46b4-8c7d-5e6ac2c8b7b5 2       8      DR-t1-router01                     DISTRIBUTED_ROUTER_TIER1              6
c91eb7c5-0297-4fed-9c22-b96df1c9b80f 3       9      DR-t0-router                        DISTRIBUTED_ROUTER_TIER0              4

edge01> vrf 1
edge01(tier0_sr)> get route

Flags: c - connected, s - static, b - BGP, ns - nsx_static
nc - nsx_connected, rl - router_link, t0n: Tier0-NAT, t1n: Tier1-NAT
t1l: Tier1-LB VIP, t1s: Tier1-LB SNAT

Total number of routes: 25

b    10.10.20.0/24      [20/0]      via 192.168.140.1
b    10.10.30.0/24      [20/0]      via 192.168.140.1
b    10.20.20.0/24      [20/0]      via 192.168.140.1
b    10.20.30.0/24      [20/0]      via 192.168.140.1
b    30.0.0.0/8         [20/0]      via 192.168.140.1
rl   100.64.80.0/31     [0/0]       via 169.254.0.1
rl   100.64.80.2/31     [0/0]       via 169.254.0.1
rl   100.64.80.4/31     [0/0]       via 169.254.0.1
<TRUNCATED OUTPUT>
b    192.168.200.0/24   [20/0]      via 192.168.140.1
```

```

b    192.168.210.0/24    [20/0]    via 192.168.140.1
b    192.168.220.0/24    [20/0]    via 192.168.140.1
b    192.168.230.0/24    [20/0]    via 192.168.140.1
b    192.168.240.0/24    [20/0]    via 192.168.140.1

```

インターフェイスの IP アドレスを取得するには、次のコマンドを実行します。

```

edge01(tier0_sr)> get interfaces
Logical Router
UUID                                VRF  LR-ID  Name                Type
c9393d0c-1fcf-4c34-889d-2da1eeee25b8  1    10     SR-t0-router        SERVICE_ROUTER_TIER0
interfaces
  interface    : 977ac2eb-8ab7-40e9-8abe-782a438c749a
  ifuid        : 285
  name         : uplink01
  mode         : lif
  IP/Mask      : 192.168.140.3/24
  MAC          : 00:50:56:b5:d5:64
  LS port      : 14391f86-efef-4e3d-98c3-f291c17d13f8
  urpf-mode    : STRICT_MODE
  admin        : up
  MTU          : 1600

  interface    : 6af81d72-4d32-5f66-b7ae-403e617290e5
  ifuid        : 270
  mode         : blackhole

  interface    : 015e709d-6079-5c19-9556-8be2e956f775
  ifuid        : 269
  mode         : cpu

  interface    : 3f40f838-eb8a-4f35-854c-ea8bb872dc47
  ifuid        : 272
  name         : bp-sr0-port
  mode         : lif
  IP/Mask      : 169.254.0.2/28
  MAC          : 02:50:56:56:53:00
  VNI          : 25489
  LS port      : 770a208d-27fa-4f8d-afad-a9c41ca6295b
  urpf-mode    : NONE
  admin        : up
  MTU          : 1500

  interface    : 00003300-0000-0000-0000-00000000000a
  ifuid        : 263
  mode         : loopback
  IP/Mask      : 127.0.0.1/8

```

## T1 ルートのアドバタイズ

T1 ルートは、T0 ルーターおよびその上位の階層で表示されるようにアドバタイズする必要があります。NSX 接続、NAT、スタティック、LB VIP、LB SNAT など、さまざまなタイプのルートをアドバタイズすることができます。

# ファイアウォールのトラブルシューティング

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

この章には、次のトピックが含まれています。

- [ESXi ホストに適用されるファイアウォール ルールの確認](#)
- [KVM ホストに適用されるファイアウォール ルールの確認](#)
- [ファイアウォール パケット ログ](#)

## ESXi ホストに適用されるファイアウォール ルールの確認

ESXi ホストのファイアウォールの問題をトラブルシューティングする際には、ホストに適用されるファイアウォール ルールを確認します。

ESXi ホストの dvfilter のリストを取得します。

```
[root@esxi-01:~] summarize-dvfilter
<TRUNCATED OUTPUT>
world 70181 vmm0:app-01a vcUuid:'50 35 9c 70 18 8e 99 1d-3c f9 8e cc 6b 27 4c 6f'
port 50331655 app-01a.eth0
  vNic slot 2
  name: nic-70181-eth0-vmware-sfw.2
agentName: vmware-sfw
  state: IOChain Attached
  vmState: Detached
  failurePolicy: failClosed
  slowPathID: none
  filter source: Dynamic Filter Creation
world 70179 vmm0:web-02a vcUuid:'50 35 2b f3 4a 4b 10 83-54 72 50 f7 25 10 d8 64'
port 50331656 web-02a.eth0
  vNic slot 2
  name: nic-70179-eth0-vmware-sfw.2
agentName: vmware-sfw
  state: IOChain Attached
  vmState: Detached
  failurePolicy: failClosed
  slowPathID: none
  filter source: Dynamic Filter Creation
```

特定の仮想マシンの dvfilter を探します。

```
[root@esxi-01:~] summarize-dvfilter | less -p web

world 70179 vmm0:web-02a vcUuid:'50 35 2b f3 4a 4b 10 83-54 72 50 f7 25 10 d8 64'
port 50331656 web-02a.eth0
  vNic slot 2
    name: nic-70179-eth0-vmware-sfw.2
  agentName: vmware-sfw
    state: IOChain Attached
    vmState: Detached
    failurePolicy: failClosed
    slowPathID: none
    filter source: Dynamic Filter Creation
.
.
.
```

特定の dvfilter に適用されるファイアウォール ルールを確認します（この例では nic-70227-eth0-vmware-sfw.2 が dvfilter 名）。

```
[root@esxi-02:~] vsipioctl getrules -f nic-70227-eth0-vmware-sfw.2
ruleset mainrs {
rule 3072 at 1 inout protocol tcp from any to addrset 48822ec3-2670-497b-82f9-524618c16877 port 443
accept with log;
rule 3072 at 2 inout protocol tcp from any to addrset 48822ec3-2670-497b-82f9-524618c16877 port 80
accept with log;
rule 3074 at 3 inout protocol tcp from addrset 48822ec3-2670-497b-82f9-524618c16877 to addrset
8b9e75e7-bc62-4d7f-9a58-a872f393448e port 8443 accept with log;
rule 3074 at 4 inout protocol tcp from addrset 48822ec3-2670-497b-82f9-524618c16877 to addrset
8b9e75e7-bc62-4d7f-9a58-a872f393448e port 22 accept with log;
rule 3075 at 5 inout protocol tcp from addrset 8b9e75e7-bc62-4d7f-9a58-a872f393448e to addrset
b695c8df-9894-4068-a5e7-5504fe48d459 port 3306 accept with log;
rule 3076 at 6 inout protocol tcp from ip 192.168.110.10 to addrset rdst3076 port 443 accept with log;
rule 3076 at 7 inout protocol icmp typecode 8:0 from ip 192.168.110.10 to addrset rdst3076 accept
with log;
rule 3076 at 8 inout protocol tcp from ip 192.168.110.10 to addrset rdst3076 port 22 accept with log;
rule 3076 at 9 inout protocol tcp from ip 192.168.110.10 to addrset rdst3076 port 80 accept with log;
rule 2 at 10 inout protocol any from any to any accept with log;
}

ruleset mainrs_L2 {
rule 1 at 1 inout ethertype any stateless from any to any accept;
}
}
```

特定の dvfilter で使用されるアドレス セットのリストを取得します。

```
[root@esxi-02:~] vsipioctl getaddrsets -f nic-70227-eth0-vmware-sfw.2
addrset 48822ec3-2670-497b-82f9-524618c16877 {
ip 172.16.10.13,
mac 52:54:00:42:4d:38,
}
addrset 8b9e75e7-bc62-4d7f-9a58-a872f393448e {
}
```

```

addrset b695c8df-9894-4068-a5e7-5504fe48d459 {
ip 172.16.30.11,
mac 52:54:00:64:0e:4f,
}
addrset rdst3076 {
ip 172.16.10.13,
ip 172.16.30.11,
mac 52:54:00:42:4d:38,
mac 52:54:00:64:0e:4f,
}

```

特定の dvfilter のフローを確認します。

```

[root@esxi-02:~] vsipioctl getflows -f nic-75360-eth0-vmware-sfw.2
Count retrieved from kernel active(L3,L4)=20, active(L2)+inactive(L3,L4)=0, drop(L2,L3,L4)=0
a5d914f7a5b85fe5 Active tcp 0800 IN 3076 0 0 192.168.110.10:Unknown(51281) -> 172.16.10.11:ssh(22)
513 FINWAIT2:FINWAIT2 4304 5177 34 33
a5d914f7a5b86001 Active tcp 0800 OUT 2 0 0 172.16.10.11:http(80) -> 100.64.80.1:Unknown(60006) 457
SYNSENT:CLOSED 56 819 1 1
a5d914f7a5b86006 Active igmp 0800 IN 2 0 0 0.0.0.0 -> 224.0.0.1 36 0 1 0
a5d914f7a5b86011 Active tcp 0800 IN 3072 0 0 100.64.80.1:Unknown(60098) -> 172.16.10.11:http(80) 320
FINWAIT2:FINWAIT2 413 5411 9 6
a5d914f7a5b86012 Active tcp 0800 OUT 3074 0 0 172.16.10.11:Unknown(46001) ->
172.16.20.11:Unknown(8443) 815 FINWAIT2:FINWAIT2 7418 1230 10 9
a5d914f7a5b86013 Active udp 0800 OUT 2 0 0 172.16.10.11:Unknown(40080) -> 192.168.110.10:domain(53)
268 140 2 2
a5d914f7a5b86014 Active udp 0800 OUT 2 0 0 172.16.10.11:Unknown(59251) -> 192.168.110.10:domain(53)
268 140 2 2
a5d914f7a5b86015 Active ipv6-icmp 86dd OUT 2 0 0 fe80::250:56ff:feb5:a60e -> ff02::1:ff62:5ed4 135 0
0 72 0 1
a5d914f7a5b86016 Active ipv6-icmp 86dd OUT 2 0 0 fe80::250:56ff:feb5:a60e -> ff02::1:ff62:5ed4 135 0
0 72 0 1
a5d914f7a5b86017 Active tcp 0800 IN 3072 0 0 100.64.80.1:Unknown(60104) -> 172.16.10.11:http(80) 320
FINWAIT2:FINWAIT2 413 5451 9 7
a5d914f7a5b86018 Active tcp 0800 OUT 3074 0 0 172.16.10.11:Unknown(46002) ->
172.16.20.11:Unknown(8443) 815 TIMEWAIT:TIMEWAIT 7314 1230 8 9
a5d914f7a5b86019 Active tcp 0800 IN 3072 0 0 100.64.80.1:Unknown(60110) -> 172.16.10.11:http(80) 320
FINWAIT2:FINWAIT2 373 5451 8 7
a5d914f7a5b8601a Active tcp 0800 OUT 3074 0 0 172.16.10.11:Unknown(46003) ->
172.16.20.11:Unknown(8443) 815 FINWAIT2:FINWAIT2 7418 1230 10 9
a5d914f7a5b8601b Active tcp 0800 IN 3072 0 0 100.64.80.1:Unknown(60114) -> 172.16.10.11:http(80) 328
TIMEWAIT:TIMEWAIT 413 5451 9 7
a5d914f7a5b8601c Active tcp 0800 OUT 3074 0 0 172.16.10.11:Unknown(46004) ->
172.16.20.11:Unknown(8443) 815 TIMEWAIT:TIMEWAIT 7262 1218 7 9
a5d914f7a5b8601d Active tcp 0800 OUT 2 0 0 172.16.10.11:http(80) -> 100.64.80.1:Unknown(60060) 457
SYNSENT:CLOSED 56 819 1 1
a5d914f7a5b8601e Active tcp 0800 IN 3072 0 0 100.64.80.1:Unknown(60120) -> 172.16.10.11:http(80) 320
TIMEWAIT:TIMEWAIT 373 5411 8 6
a5d914f7a5b8601f Active tcp 0800 OUT 3074 0 0 172.16.10.11:Unknown(46005) ->
172.16.20.11:Unknown(8443) 815 FINWAIT2:FINWAIT2 7418 1230 10 9
a5d914f7a5b86020 Active tcp 0800 IN 3072 0 0 100.64.80.1:Unknown(60126) -> 172.16.10.11:http(80) 229
EST:EST 173 5371 3 5
a5d914f7a5b86021 Active tcp 0800 OUT 3074 0 0 172.16.10.11:Unknown(46006) ->
172.16.20.11:Unknown(8443) 815 FINWAIT2:FINWAIT2 7418 1230 10 9

```



## KVM ホストに適用されるファイアウォール ルールの確認

KVM ホストのファイアウォールの問題をトラブルシューティングする際には、ホストに適用されるファイアウォール ルールを確認します。

KVM ホストでファイアウォール ルールの対象となる VIF のリストを取得します。

```
# ovs-appctl -t /var/run/openvswitch/nsxa-ctl dfw/vif
Vif ID      : da95fc1e-65fd-461f-814d-d92970029bf0
Port name   : db-01a-eth0
Port number : 2
```

出力が空の場合は、ノードとコントローラ間の接続の問題を探します。

特定の VIF に適用されるルールのリストを取得します（この例では、da95fc1e-65fd-461f-814d-d92970029bf0 が VIF の ID）。

```
# ovs-appctl -t /var/run/vmware/nsx-agent/nsxa-ctl dfw/rules da95fc1e-65fd-461f-814d-d92970029bf0
Distributed firewall status: enabled

Vif ID      : da95fc1e-65fd-461f-814d-d92970029bf0
ruleset d035308b-cb0d-4e7e-aae5-a428b461db46 {
  rule 3072 inout protocol tcp from any to addrset 48822ec3-2670-497b-82f9-524618c16877 port 443
  accept with log;
  rule 3072 inout protocol tcp from any to addrset 48822ec3-2670-497b-82f9-524618c16877 port 80 accept
  with log;
  rule 3074 inout protocol tcp from addrset 48822ec3-2670-497b-82f9-524618c16877 to addrset 8b9e75e7-
  bc62-4d7f-9a58-a872f393448e port 8443 accept with log;
  rule 3074 inout protocol tcp from addrset 48822ec3-2670-497b-82f9-524618c16877 to addrset 8b9e75e7-
  bc62-4d7f-9a58-a872f393448e port 22 accept with log;
  rule 3075 inout protocol tcp from addrset 8b9e75e7-bc62-4d7f-9a58-a872f393448e to addrset
  b695c8df-9894-4068-a5e7-5504fe48d459 port 3306 accept with log;
}

ruleset 3027fed3-60b1-483e-aa17-c28719275704 {
  rule 3076 inout protocol tcp from 192.168.110.10 to addrset b695c8df-9894-4068-a5e7-5504fe48d459
  port 443 accept with log;
  rule 3076 inout protocol icmp type 8 code 0 from 192.168.110.10 to addrset b695c8df-9894-4068-
  a5e7-5504fe48d459 accept with log;
  rule 3076 inout protocol tcp from 192.168.110.10 to addrset b695c8df-9894-4068-a5e7-5504fe48d459
  port 22 accept with log;
  rule 3076 inout protocol tcp from 192.168.110.10 to addrset b695c8df-9894-4068-a5e7-5504fe48d459
  port 80 accept with log;
  rule 3076 inout protocol tcp from 192.168.110.10 to addrset 8b9e75e7-bc62-4d7f-9a58-a872f393448e
  port 443 accept with log;
  rule 3076 inout protocol icmp type 8 code 0 from 192.168.110.10 to addrset 8b9e75e7-bc62-4d7f-9a58-
  a872f393448e accept with log;
  rule 3076 inout protocol tcp from 192.168.110.10 to addrset 8b9e75e7-bc62-4d7f-9a58-a872f393448e
  port 22 accept with log;
  rule 3076 inout protocol tcp from 192.168.110.10 to addrset 8b9e75e7-bc62-4d7f-9a58-a872f393448e
  port 80 accept with log;
  rule 3076 inout protocol tcp from 192.168.110.10 to addrset 48822ec3-2670-497b-82f9-524618c16877
  port 443 accept with log;
  rule 3076 inout protocol icmp type 8 code 0 from 192.168.110.10 to addrset
```

```

48822ec3-2670-497b-82f9-524618c16877 accept with log;
  rule 3076 inout protocol tcp from 192.168.110.10 to addrset 48822ec3-2670-497b-82f9-524618c16877
port 22 accept with log;
  rule 3076 inout protocol tcp from 192.168.110.10 to addrset 48822ec3-2670-497b-82f9-524618c16877
port 80 accept with log;
}

ruleset 5e9bdc3-adba-4f67-a680-5e6ed5b8f40a {
  rule 2 inout protocol any from any to any accept with log;
}

ruleset ddf93011-4078-4006-b8f8-73f979d7a717 {
  rule 1 inout ethertype any stateless from any to any accept;
}

```

特定の VIF で使用されるアドレス セットのリストを取得します。

```

# ovs-appctl -t /var/run/vmware/nsx-agent/nsxa-ctl dfw/addrsets da95fc1e-65fd-461f-814d-d92970029bf0
48822ec3-2670-497b-82f9-524618c16877 {
  mac 52:54:00:42:4d:38,
  ip 172.16.10.13,
}

8b9e75e7-bc62-4d7f-9a58-a872f393448e {
}

b695c8df-9894-4068-a5e7-5504fe48d459 {
  mac 52:54:00:64:0e:4f,
  ip 172.16.30.11,
}

```

Linux の Conntrack モジュールを使用して接続を確認します。この例では、2 つの特定の IP アドレス間のフローを探します。

```

# ovs-appctl -t ovs-l3d conntrack/show | grep 192.168.110.10 | grep 172.16.10.13
ACTIVE
icmp,orig=(src=192.168.110.10,dst=172.16.10.13,id=1,type=8,code=0),reply=(src=172.16.10.13,dst=192.168
.110.10,id=1,type=0,code=0),start=2018-03-26T04:43:28.325,id=3122159040,zone=23119,status=SEEN_REPLY|
CONFIRMED,timeout=29,mark=3076,labels=0x1f

```

## ファイアウォール パケット ログ

ファイアウォール ルールのログが有効な場合は、ファイアウォール パケット ログを確認して問題のトラブルシューティングを行うことができます。

ESXi ホストと KVM ホストのログ ファイルはいずれも `/var/log/dfwpktlogs.log` です。

```

# tail -f /var/log/dfwpktlogs.log
2018-03-27T10:23:35.196Z INET TERM 3072 IN TCP FIN 100.64.80.1/60688->172.16.10.11/80 8/7 373/5451
2018-03-27T10:23:35.196Z INET TERM 3074 OUT TCP FIN 172.16.10.11/46108->172.16.20.11/8443 8/9
1178/7366
2018-03-27T10:23:35.196Z INET TERM 3072 IN TCP RST 100.64.80.1/60692->172.16.10.11/80 9/6 413/5411
2018-03-27T10:23:35.196Z INET TERM 3074 OUT TCP RST 172.16.10.11/46109->172.16.20.11/8443 9/7

```

```

1218/7262
2018-03-27T10:23:37.442Z 71d32787 INET match PASS 3074 IN 60 TCP 172.16.10.12/35770-
>172.16.20.11/8443 S
2018-03-27T10:23:38.492Z INET match PASS 2 OUT 1500 TCP 172.16.10.11/80->100.64.80.1/60660 A
2018-03-27T10:23:39.934Z INET match PASS 3072 IN 52 TCP 100.64.80.1/60720->172.16.10.11/80 S
2018-03-27T10:23:39.944Z INET match PASS 3074 OUT 60 TCP 172.16.10.11/46114->172.16.20.11/8443 S
2018-03-27T10:23:39.944Z 71d32787 INET match PASS 3074 IN 60 TCP 172.16.10.11/46114-
>172.16.20.11/8443 S
2018-03-27T10:23:42.449Z 71d32787 INET match PASS 3074 IN 60 TCP 172.16.10.12/35771-
>172.16.20.11/8443 S
2018-03-27T10:23:44.712Z INET TERM 3074 IN TCP RST 172.16.10.11/46109->172.16.20.11/8443 9/7 1218/7262
2018-03-27T10:23:44.712Z INET TERM 3074 IN TCP FIN 172.16.10.12/35766->172.16.20.11/8443 9/10
1233/7418
2018-03-27T10:23:44.712Z INET TERM 3074 IN TCP FIN 172.16.10.11/46110->172.16.20.11/8443 9/9 1230/7366
2018-03-27T10:23:44.712Z INET TERM 3074 IN TCP FIN 172.16.10.12/35767->172.16.20.11/8443 9/10
1233/7418
2018-03-27T10:23:44.939Z INET match PASS 3072 IN 52 TCP 100.64.80.1/60726->172.16.10.11/80 S
2018-03-27T10:23:44.957Z INET match PASS 3074 OUT 60 TCP 172.16.10.11/46115->172.16.20.11/8443 S
2018-03-27T10:23:44.957Z 71d32787 INET match PASS 3074 IN 60 TCP 172.16.10.11/46115-
>172.16.20.11/8443 S
2018-03-27T10:23:45.480Z INET TERM 2 OUT TCP TIMEOUT 172.16.10.11/80->100.64.80.1/60528 1/1 1500/56

```

# ログおよびサービス

# 5

トラブルシューティングでは、多くの場合、ログが役立ちます。サービスのステータスの確認も重要です。

この章には、次のトピックが含まれています。

- ログ メッセージ
- Syslog 問題のトラブルシューティング
- サービスの確認
- サポート バンドルの収集

## ログ メッセージ

ESXi ホストで実行されているものを含むすべての NSX-T コンポーネントのログ メッセージは、RFC 5424 で指定された Syslog 形式に準拠しています。KVM ホストからのログ メッセージは RFC 3164 形式です。ログ ファイルは、`/var/log` ディレクトリにあります。

NSX-T アプライアンスでは、次の NSX-T CLI コマンドを実行してログを表示できます。

```
get log-file <auth.log | http.log | kern.log | manager.log | node-mgmt.log | syslog> [follow]
```

ハイパーバイザーでは、`tac`、`tail`、`grep`、および `more` などの Linux コマンドを使用してログを表示できます。NSX-T アプライアンスでもこれらのコマンドを使用できます。

RFC 5424 の詳細については、<https://tools.ietf.org/html/rfc5424> を参照してください。RFC 3164 の詳細については、<https://tools.ietf.org/html/rfc3164> を参照してください。

RFC 5424 は、ログ メッセージのに次の形式を定義します。

```
<facility * 8 + severity> version UTC-TZ hostname APP-NAME procid MSGID [structured-data] msg
```

ログ メッセージのサンプル：

```
<187>1 2016-03-15T22:53:00.114Z nsx-manager NSX - SYSTEM [nsx@6876 comp="nsx-manager"
errorCode="MP4039" subcomp="manager"] Connection verification failed for broker '10.160.108.196'.
Marking broker unhealthy.
```

すべてのメッセージには、メッセージの送信元を識別するためのコンポーネント (`comp`) 情報とサブコンポーネント (`subcomp`) 情報が含まれます。

NSX-T は、通常のログ（ファシリティ local6、数値 22）および監査ログ（ファシリティ local7、数値 23）を生成します。すべての API 呼び出しは、監査ログをトリガします。

API 呼び出しに関連付けられた監査ログには、次の情報が含まれます。

- API のオブジェクトを識別するためのエンティティ ID パラメータ `entId`。
- 特定の API 呼び出しを識別するためのリクエスト ID パラメータ `req-id`。
- API 呼び出しにヘッダー `X-NSX-EREQID:<string>` が含まれている場合は、外部リクエスト ID パラメータ `ereqId`。
- API 呼び出しにヘッダー `X-NSX-EUSER:<string>` が含まれている場合は、外部ユーザー パラメータ `euser`。

RFC 5424 は次の重要度レベルを定義します。

重要度	説明
0	緊急：システムが不安定な状態
1	アラート：迅速な対応が必要な状態
2	重大：重大な問題がある状況
3	エラー：エラーが発生した状態
4	警告：警告が発生した状態
5	通知：正常ではあっても注意を要する状態
6	情報：情報メッセージ
7	デバッグ：デバッグレベルのメッセージ

重要度が緊急、アラート、重大、またはエラーのすべてのログには、ログ メッセージの構造化データに、一意のエラー コードが記載されます。エラー コードは文字列と 10 進数で構成されます。文字列は特定のモジュールを表わします。

MSGID フィールドは、メッセージの種類を識別するものです。メッセージ ID のリストについては、[ログ メッセージ ID](#) を参照してください。

## リモート ログの設定

NSX-T アプライアンスおよびハイパーバイザーを設定して、リモート ログ サーバにログ メッセージを送信することができます。

リモート ログは、NSX Manager、NSX Controller、NSX Edge、およびハイパーバイザーでサポートされています。各ノードで個別にリモート ログを設定する必要があります。

KVM ホストでは、NSX-T インストール パッケージにより `/etc/rsyslog.d` ディレクトリ内に構成ファイルが配置され、rsyslog デーモンが自動的に構成されます。

### 前提条件

- ログを受信するログ サーバを設定します。

## 手順

## 1 NSX-T アプライアンスでリモート ログを設定する方法：

- a 次のコマンドを実行して、ログ サーバと、ログ サーバに送信するメッセージのタイプを設定します。複数のファシリティまたはメッセージ ID は、スペースなしのカンマ区切りのリストとして指定することができます。

```
set logging-server <hostname-or-ip-address[:port]> proto <proto> level <level> [facility <facility>] [messageid <messageid>] [certificate <filename>] [structured-data <structured-data>]
```

詳細については、『NSX-T Command-Line Interface Reference』を参照してください。コマンドを複数回実行し、複数のログ サーバ設定を追加することができます。次はその例です。

```
nsx> set logging-server 192.168.110.60 proto udp level info facility syslog messageid SYSTEM,FABRIC
nsx> set logging-server 192.168.110.60 proto udp level info facility auth,user
```

- b get logging-server コマンドを実行してログの設定を表示できます。次はその例です。

```
nsx> get logging-servers
192.168.110.60 proto udp level info facility syslog messageid SYSTEM,FABRIC
192.168.110.60 proto udp level info facility auth,user
```

## 2 ESXi ホストでリモート ログを設定する方法：

- a Syslog を設定してテスト メッセージを送信するには、次のコマンドを実行します。

```
esxcli network firewall ruleset set -r syslog -e true
esxcli system syslog config set --loghost=udp://<log server IP>:<port>
esxcli system syslog reload
esxcli system syslog mark -s "This is a test message"
```

- b 設定を表示するには、次のコマンドを実行します。

```
esxcli system syslog config get
```

## 3 KVM ホストでリモート ログを設定するには、次の操作を行います。

- a お使いの環境の /etc/rsyslog.d/10-vmware-remote-logging.conf ファイルを編集します。
- b 次の行をファイルに追加します。

```
*.* @<ip>:514;RFC5424fmt
```

- c 次のコマンドを実行します。

```
service rsyslog restart
```

## ログ メッセージ ID

ログ メッセージのメッセージ ID のフィールドは、メッセージの種類を識別します。`set logging-server` コマンドの `messageid` パラメータを使用して、どのログ メッセージをログ サーバに送信するかをフィルタすることができます。

表 5-1. ログ メッセージ ID

メッセージ ID	例
FABRIC	ホスト ノード ホストの準備 Edge ノード トランスポート ゾーン トランスポート ノード アップリンク プロファイル クラスタ プロファイル Edge クラスタ ブリッジ クラスタとエンドポイント
SWITCHING	論理スイッチ 論理スイッチ ポート スイッチング プロファイル スイッチ セキュリティ機能
ROUTING	分散論理ルーター 分散論理ルーター ポート 固定ルーティング 動的ルーティング NAT
FIREWALL	ファイアウォール ルール ファイアウォール ルール セクション
FIREWALL-PKTLOG	ファイアウォール接続ログ ファイアウォール パケット ログ
GROUPING	IP セット MAC セット NSGroup NSService NSService グループ VNI プール IP アドレス プール
DHCP	DHCP リレー

表 5-1. ログ メッセージ ID (続き)

メッセージ ID	例
SYSTEM	アプライアンス管理 (リモート Syslog、ntp など) クラスタ管理 信頼管理 ライセンス ユーザーとロール タスク管理 インストール (NSX Manager、NSX Controller) アップグレード (NSX Manager、NSX Controller、NSX Edge およびホスト パッケージのアップグレード) 認識 タグ
MONITORING	SNMP ポート接続 トレースフロー
-	その他のすべてのログ メッセージ

## Syslog 問題のトラブルシューティング

ログがリモート ログ サーバに受信されない場合、次の手順を実行します。

- リモート ログ サーバの IP アドレスを確認します。
- level パラメータが適切に設定されていることを確認します。
- facility パラメータが適切に設定されていることを確認します。
- プロトコルが TLS の場合は、プロトコルを UDP に設定して証明書に不一致があるかどうかを確認します。
- プロトコルが TLS の場合は、ポート 6514 が両端で開いていることを確認します。
- メッセージ ID フィルタを解除して、ログがサーバで受信されているかどうかを確認します。
- `restart service rsyslogd` コマンドを使用して rsyslog サービスを再起動します。

rsyslog 構成ファイル (/etc/rsyslog.conf) の例 :

```
### rsyslog config file. Customized by VMware.
### Do not edit this file by hand. Use the API to make changes.
$PreserveFQDN on
$ModLoad imklog
$ModLoad immark
module(load="imuxsock" sysSock.useSpecialParser="off")
$RepeatedMsgReduction on
$FileOwner syslog
$FileGroup adm
$FileCreateMode 0640
$DirCreateMode 0755
$Umask 0022
$ActionFileDefaultTemplate RSYLOG_SyslogProtocol23Format
```



```
$IncludeConfig /etc/rsyslog.d/*.conf
$template RFC5424fmt,"%<%PRI%>1 %TIMESTAMP:::date-rfc3339% %HOSTNAME% %APP-NAME% %PROCID% %MSGID%
%STRUCTURED-DATA% %msg%\n"
$WorkDirectory /var/spool/rsyslog
$ModLoad imudp
$UDPServerAddress 127.0.0.1
$UDPServerRun 514
$PrivDropToUser syslog
$ActionQueueType LinkedList # nsx exporter: e7347687-8be7-4519-a8e1-73c5192c9b43
*.info @1.2.3.4:514;RFC5424fmt # nsx exporter: e7347687-8be7-4519-a8e1-73c5192c9b43
```

## サービスの確認

サービスの実行停止または起動の失敗は、問題の原因になります。すべてのサービスが正常に実行されていることを確認することは重要です。

NSX Manager サービスのステータスを確認するには、以下を実行します。

```
nsxmgr> get services
Service name:      cm-inventory
Service state:     stopped

Service name:      http
Service state:     stopped
Session timeout:   1800
Connection timeout: 30
Redirect host:     (not configured)

Service name:      install-upgrade
Service state:     stopped
Enabled:           True

Service name:      liagent
Service state:     stopped

Service name:      manager
Service state:     stopped
Logging level:     info

Service name:      mgmt-plane-bus
Service state:     running

Service name:      node-mgmt
Service state:     running

Service name:      nsx-message-bus
Service state:     running

Service name:      nsx-upgrade-agent
Service state:     running

Service name:      ntp
Service state:     running
```

```

Service name:      search
Service state:     stopped

Service name:      snmp
Service state:     stopped

Start on boot:     False
Service name:      ssh

Service state:     running
Start on boot:     True

Service name:      syslog
Service state:     running

```

上記の例では、HTTP サービスが停止しています。次のコマンドで、HTTP サービスを開始できます。

```
nsxmgr> start service http
```

## SSH サービス

アプライアンスの展開時に SSH サービスが有効でない場合は、アプライアンスに管理者としてログインし、次のコマンドを実行して有効にすることができます。

```
start service ssh
```

次のコマンドを使用して、ホストの起動時に SSH が起動するように設定できます。

```
set service ssh start-on-boot
```

SSH の root ログインを有効にするには、アプライアンスに root としてログインし、ファイル `/etc/ssh/sshd_config` を編集して次の行を置き換えます。

```
PermitRootLogin prohibit-password
```

あるいは、アプライアンスをパワーオフして、vApp のプロパティを変更することで、SSH サービスを有効にし、SSH の root アクセスを有効にできます。

次のコマンドを使用して

```
PermitRootLogin yes
```

次のコマンドを使用して SSHD サーバを再起動します。

```
/etc/init.d/ssh restart
```

## サポート バンドルの収集

登録されたクラスタおよびファブリック ノード上のサポート バンドルを収集し、バンドルをマシンにダウンロードするか、ファイル サーバにアップロードすることができます。

バンドルをマシンにダウンロードする場合は、各ノードのマニフェスト ファイルおよびサポート バンドルが含まれる単一のアーカイブ ファイルを入手できます。バンドルをファイル サーバにアップロードする場合は、マニフェスト ファイルおよび個々のバンドルがファイル サーバに個別にアップロードされます。

---

**NSX Cloud のメモ** CSM のサポート バンドルを収集する場合、CSM にログインして、[システム] - [ユーティリティ] - [サポート バンドル] の順に移動し、[ダウンロード] をクリックします。PCG のサポート バンドルは、次の手順を実行して NSX Manager から入手できます。PCG のサポート バンドルには、すべてのワークロード仮想マシンのログも含まれています。

---

#### 手順

- 1 ブラウザから、NSX Manager (<https://nsx-manager-ip-address>) に管理者権限でログインします。
- 2 ナビゲーション パネルから、[システム] - [ユーティリティ] の順に選択します。
- 3 [サポート バンドル] タブをクリックします。
- 4 収集対象のノードを選択します。  
指定可能なノードのタイプは、管理ノード、コントローラ ノード、Edge、ホスト、および Public Cloud Gateway です。
- 5 (オプション) ログの収集期間 (日) を指定し、指定した日数以前の古いログを除外します。
- 6 (オプション) スイッチを切り替えて、コア ファイルおよび監査ログを含めるか除外するかを指定します。

---

**注：** コア ファイルおよび監査ログには、パスワードまたは暗号化キーのような機密情報が含まれている場合があります。

---

- 7 (オプション) チェックボックスをクリックして、バンドルをファイル サーバにアップロードするオプションを選択します。
- 8 [バンドル収集を開始] をクリックして、サポート バンドルの収集を開始します。  
存在するログ ファイルの数によっては、各ノードの収集に数分ずつかかる場合があります。
- 9 収集プロセスのステータスを監視します。  
ステータス フィールドには、サポート バンドルの収集を完了したノードの割合が表示されます。
- 10 ファイル サーバにバンドルを送信するオプションを指定していない場合は、[ダウンロード] をクリックしてバンドルをダウンロードします。

## その他のトラブルシューティングの方法

このセクションでは、さまざまなエラーのトラブルシューティングの方法について説明します。

この章には、次のトピックが含まれています。

- [トランスポート ノードの追加または削除の失敗](#)
- [トランスポート ノードが別のコントローラに接続するには約 5 分間必要](#)
- [NSX Manager 仮想マシンが劣化状態である](#)
- [NSX Agent で NSX Manager との通信がタイムアウトになる](#)
- [ESXi ホストの追加に失敗する](#)
- [NSX Controller の不正なステータス](#)
- [IPFIX が有効の場合 KVM 仮想マシンの管理 IP アドレスにアクセスできない](#)

### トランスポート ノードの追加または削除の失敗

トランスポート ノードを追加または削除することができない。

#### 問題

次のシナリオでエラーが発生する。

- 1 ESXi ホストがファブリック ノードであると同時にトランスポート ノードである。
- 2 ホストがトランスポート ノードとして削除された。しかし、トランスポート ノードの削除に失敗する。トランスポート ノードの状態が **Orphaned** になる。
- 3 ホストがファブリック ノードとしてすぐに削除される。
- 4 ホストがもう一度ファブリック ノードとして追加される。
- 5 ホストが、新しいトランスポート ゾーンとスイッチを持つトランスポート ノードとして追加される。この手順を実行すると、**Failed/Partial Success** エラーが発生する。

## 原因

手順 2 で数分間待機すると、NSX Manager が削除を再試行するのでトランスポート ノードの削除に成功します。ファブリック ノードをすぐに削除すると、ホストが NSX-T から削除されるため、NSX Manager は再試行できません。その結果、ホストのクリーンアップが不完全になり、スイッチの構成は保持されたままになるため、手順 5 が失敗します。

## 解決方法

- 1 NSX-T スイッチに接続されているホスト上の vCenter Server からすべての vmknics を削除します。
- 2 `esxcfg-vswitch -l` CLI コマンドを使用して、スイッチ名を取得します。次はその例です。

```
esxcfg-vswitch -l
```

Switch Name	Num Ports	Used Ports	Configured Ports	MTU	Uplinks
vSwitch0	1536	4	128	1500	vmnic0

  

PortGroup Name	VLAN ID	Used Ports	Uplinks
VM Network	0	0	vmnic0
Management Network	0	1	vmnic0

  

Switch Name	Num Ports	Used Ports	Uplinks
nsxvswitch	1536	4	

- 3 `esxcfg-vswitch -d <switch-name> --dvswitch` CLI コマンドを使用して、スイッチ名を削除します。次はその例です。

```
esxcfg-vswitch -d nsxvswitch --dvswitch
```

## トランスポート ノードが別のコントローラに接続するには約 5 分間必要

ESXi トランスポート ノードに接続されているコントローラに障害が発生した場合、このトランスポート ノードが別のコントローラに接続するには約 5 分間かかります。

## 問題

ESXi トランスポート ノードは、通常コントローラ クラスタ内の特定のコントローラに接続されます。接続先のコントローラは、CLI コマンド `get controllers` を使用して探すことができます。接続先のコントローラに障害が発生した場合、このトランスポート ノードが別のコントローラに接続するには約 5 分間かかります。

## 原因

トランスポート ノードは一定時間、障害が発生したコントローラへの再接続を試行してから、試行を中止して別のコントローラに接続します。このプロセス全体で、約 5 分間かかります。これは、想定どおりの動作です。

## NSX Manager 仮想マシンが劣化状態である

KVM ホストに展開されている NSX Manager は、`get service` や `get interface` などの CLI コマンドが実行されると、エラーを返します。

## 問題

CLI コマンド `get service` がエラーを返します。次はその例です。

```
nsx-manager-1> get service
% An error occurred while processing the service command
```

その他の CLI コマンドもエラーを返すことがあります。`get support-bundle` コマンドにより、`/tmp` ディレクトリが読み取り専用になったことが示されます。次はその例です。

```
nsx-manager-1> get support-bundle file failed-to-get-service.tgz
% An error occurred while retrieving the support bundle: [Errno 30] Read-only file system: '/tmp/
tmpHzXF1u'
```

`/var/log/messages-<timestamp>` ログに次のようなメッセージが表示されます。

```
Nov 17 07:26:48 no kernel: NMI watchdog: BUG: soft lockup - CPU#5 stuck for 23s! [qemu-kvm:4386]
```

## 原因

NSX Manager アプライアンスの 1 つ以上のファイル システムが破損しています。<https://access.redhat.com/solutions/22621> に、可能性のある原因がいくつか記載されています。

この問題を解決するには、破損したファイル システムを修復するか、バックアップからリストアします。

## 解決方法

- オプション 1: 破損したファイル システムを修復する次の手順は、KVM ホストで実行されている NSX Manager に固有のものです。

- `virsh destroy` コマンドを実行して NSX Manager 仮想マシンを停止します。
- qcow2 イメージに対し、書き込みモードで `virt-rescue` コマンドを実行します。次はその例です。

```
virt-rescue --rw -a nsx-unified-appliance-2.0.0.0.6522097.phadniss-p0-DK-to-DGo-on-rhel-
prod_nsx_manager_1.qcow2
```

- `virt-rescue` コマンド プロンプトで `e2fsck` コマンドを実行して `tmp` ファイル システムを修復します。次はその例です。

```
<rescue> e2fsck /dev/nsx/tmp
```

- 必要に応じて、エラーがなくなるまで `e2fsck /dev/nsx/tmp` を実行します。
- `virsh start` を実行して NSX Manager を再起動します。

- オプション 2: バックアップからリストアする

手順については、『NSX-T 管理ガイド』を参照してください。

## NSX Agent で NSX Manager との通信がタイムアウトになる

ESXi ホスト上に多くのトランスポート ノードと仮想マシンがある大規模な環境では、ESXi ホスト上で実行される NSX Agent が NSX Manager との通信中にタイムアウトになる可能性があります。

### 問題

仮想マシンの vNIC が論理スイッチに接続する場合などで、処理に失敗する。/var/run/log/nsx-opsagent.log に次のようなメッセージが表示される。

```
level="ERROR" errorCode="MPA41542" [MP_AddVnicAttachment] RPC call [0e316296-13-14] to NSX
management plane timeout
2017-05-15T05:32:13Z nsxa: [nsx@6876 comp="nsx-esx" subcomp="NSXA[VifHandlerThread:-2282640]"
tid="1000017079" level="ERROR" errorCode="MPA42003" [DoMpVifAttachRpc] MP_AddVnicAttachment()
failed: RPC call to NSX management plane timeout
```

### 原因

大規模な環境では、一部の処理が通常よりも長い時間がかかったり、デフォルトのタイムアウト値を超えるために失敗することがあります。

### 解決方法

- 1 NSX Agent のタイムアウト値を増やします。

- a ESXi ホストでは、次のコマンドを使用して NSX opsAgent を停止します。

```
/etc/init.d/nsx-opsagent stop
```

- b /etc/vmware/nsx-opsagent/nsxa.json ファイルを編集し、vifOperationTimeout の値を 25 からたとえば 55 に変更します。

```
"mp" : {
  /* timeout for VIF operation */
  "vifOperationTimeout" : 25,
```

**注：** このタイムアウト値は、手順 2 で設定した hostd タイムアウト値よりも小さい値にする必要があります。

- c 次のコマンドを使用して NSX opsAgent を起動します。

```
/etc/init.d/nsx-opsagent start
```

## 2 hostd のタイムアウト値を増やします。

- a ESXi ホストでは、次のコマンドを使用して hostd エージェントを停止します。

```
/etc/init.d/hostd stop
```

- b /etc/vmware/hostd/config.xml ファイルを編集します。<opaqueNetwork> で、<taskTimeout> のエントリのコメントを外し、値を 30 からたとえば 60 に変更します。

```
<opaqueNetwork>
  <!-- maximum message size allowed in opaque network manager IPC, in bytes. -->
  <!-- <maxMsgSize> 65536 </maxMsgSize> -->
  <!-- maximum wait time for opaque network response -->
  <!-- <taskTimeout> 30 </taskTimeout> -->
```

- c 次のコマンドを使用して hostd エージェントを起動します。

```
/etc/init.d/hostd start
```

## ESXi ホストの追加に失敗する

ESXi ホストを NSX-T ファブリックに追加できない。

### 問題

NSX Manager GUI から ESXi ホストを追加しようとする、[File path of ... is claimed by multiple non-overlay VIBs] というエラーで失敗する。ログ ファイルには、次のようなメッセージが表示される。

```
Failed to install software on host. Failed to install software on host. 10.172.120.60 :
java.rmi.RemoteException: [DependencyError] File path of '/usr/lib/vmware/vmkmmod/nsx-vsip' is claimed
by multiple non-overlay VIBs
```

### 原因

前回のインストールの VIB がホスト上に残っています。クリーン アンインストールが行われなかった可能性があります。

### 解決方法

- 1 エラー メッセージから、失敗の原因となっている VIB の名前を取得します。
- 2 ESXi コマンドを使用して VIB をアンインストールします。

## NSX Controller の不正なステータス

NSX Controller クラスタのコントローラの一部が、いずれかのコントローラのステータスが不正であることを報告する。

### 問題

コントローラのパワーオフとオンを何度も繰り返すと、実際には起動していても他のコントローラによって無効であると報告される。



## 原因

コントローラをパワーオフしてからオンにすると、クラスタ内の他のコントローラとの間で通信障害が発生し、ZooKeeper モジュールを含む内部エラーが発生することがあります。

## 解決方法

- ◆ 無効であると報告されたコントローラ ノードをクラスタから削除し、クラスタ構成をノードから削除して、再度ノードをクラスタに参加させることができます。詳細については、『NSX-T 管理ガイド』の「NSX Controller クラスタのメンバーの置き換え」セクションを参照してください。

## IPFIX が有効の場合 KVM 仮想マシンの管理 IP アドレスにアクセスできない

KVM ホストの複数の仮想マシンで IPFIX が有効になっていて、サンプリング レートが 100% の場合、一部の仮想マシンの管理 IP アドレスが断続的にアクセス不能になることがあります。

## 問題

同じホスト上の複数の仮想マシンに対して IPFIX を有効にして、サンプリング レートを 100% に設定すると、大量の IPFIX トラフィックが発生することがあります。これは管理トラフィックに影響を与えるため、本番トラフィックと管理トラフィックが別々の OVS を経由する場合でも、管理 IP アドレスが断続的にアクセス不能になることがあります。

## 原因

ワークロードによってホストと仮想マシンに大きな負荷が発生しています。

## 解決方法

- ◆ IPFIX が有効になっている仮想マシンの数を減らすか、サンプリング レートを下げることによってホストの負荷を減らしてください。