

NSX-T Data Center 疑難排解指南

修改日期：2018 年 9 月 19 日

VMware NSX-T Data Center 2.3



vmware®

您可以在 VMware 網站上找到最新的技術說明文件，網址為：

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

如果您對此文件有何想法，請將您的回應意見提交至：

docfeedback@vmware.com

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Copyright © 2017, 2018 VMware, Inc. 版權所有。 [版權和商標資訊](#)。

內容

NSX-T Data Center 疑難排解指南 5

1 記錄和服務 6

記錄訊息 6

對 Syslog 問題進行疑難排解 10

檢查服務 11

收集支援服務包 12

2 疑難排解第 2 層連線 14

檢查 NSX Manager 和 NSX Controller 叢集狀態 14

檢查邏輯連接埠 15

檢查傳輸節點狀態 15

檢查邏輯交換器狀態 16

檢查邏輯交換器的 CCP 17

檢查本機控制平面狀態 17

疑難排解組態工作階段問題 18

疑難排解 L2 工作階段問題 19

疑難排解覆蓋邏輯交換器的數據平面問題 19

疑難排解 VLAN 邏輯交換器的數據平面問題 21

疑難排解覆蓋邏輯交換器的 ARP 問題 21

疑難排解 VLAN 邏輯交換器或解析 ARP 時的封包遺失問題 22

3 對安裝進行疑難排解 24

4 對路由進行疑難排解 28

5 對防火牆進行疑難排解 30

判斷 ESXi 主機上套用的防火牆規則 30

判斷 KVM 主機上套用的防火牆規則 33

防火牆封包記錄 34

6 其他疑難排解案例 36

無法新增或刪除傳輸節點 36

傳輸節點連線至另一個控制器需要大約 5 分鐘 37

NSX Manager 虛擬機器已降級 37

NSX 代理程式與 NSX Manager 通訊逾時 38

無法新增 ESXi 主機 40

NSX Controller 狀態不正確 40

在已啟用 **IPFIX** 的情況下，**KVM** 虛擬機器上的管理 **IP** 無法連線 41

NSX-T Data Center 疑難排解指南

《*NSX-T Data Center 疑難排解指南*》提供如何對 NSX-T Data Center 環境中可能發生的問題進行疑難排解的相關資訊。

主要對象

本指南適用於 NSX-T Data Center 的系統管理員，前提是熟悉虛擬化、網路和資料中心作業。

VMware 技術出版品詞彙表

VMware 技術出版品將為您提供可能不熟悉的術語詞彙。如需 VMware 技術說明文件中所用專有詞彙的定義，請前往 <http://www.vmware.com/support/pubs>。

記錄和服務

記錄可能在多個疑難排解案例中非常有用。檢查服務的狀態也很重要。

本章節討論下列主題：

- 記錄訊息
- 對 Syslog 問題進行疑難排解
- 檢查服務
- 收集支援服務包

記錄訊息

所有 NSX-T Data Center 元件 (包括 ESXi 主機上執行的元件) 的記錄訊息均符合 RFC 5424 中指定的 Syslog 格式。KVM 主機的記錄訊息採用 RFC 3164 格式。記錄檔位於 /var/log 目錄中。

在 NSX-T Data Center 應用裝置上，您可以執行下列 NSX-T Data Center CLI 命令以檢視記錄：

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

在 Hypervisor 中，您可以使用 `tail`、`grep` 和 `more` 等 Linux 命令來檢視記錄。您也可以在 NSX-T Data Center 應用裝置上使用這些命令。

如需 RFC 5424 的詳細資訊，請參閱 <https://tools.ietf.org/html/rfc5424>。如需 RFC 3164 的詳細資訊，請參閱 <https://tools.ietf.org/html/rfc3164>。

RFC 5424 會定義下列記錄訊息的格式：

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

記錄訊息範例：

```
<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.
```

每個訊息都具有元件 (`comp`) 和子元件 (`subcomp`) 資訊，可協助識別訊息的來源。

NSX-T Data Center 會產生定期記錄 (設施 `local6` 具有數值 22) 以及稽核記錄 (設施 `local7`，具有數值 23)。所有 API 呼叫皆會觸發稽核記錄。

與 API 呼叫相關聯的稽核記錄具有下列資訊：

- 實體識別碼參數 **entId**，用於識別 API 的物件。
- 要求識別碼參數 **req-id**，用於識別特定的 API 呼叫。
- 外部要求識別碼參數 **ereqId**，如果 API 呼叫包含標頭 **X-NSX-EREQID:<string>**。
- 外部使用者參數 **euser**，如果 API 呼叫包含標頭 **X-NSX-EUSER:<string>**。

RFC 5424 會定義下列嚴重性層級：

嚴重性層級	說明
0	緊急：系統無法使用
1	警示：必須立即採取動作
2	嚴重：嚴重狀況
3	錯誤：錯誤狀況
4	警告：警告狀況
5	通知：一般但重要的狀況
6	資訊：資訊訊息
7	偵錯：偵錯層級訊息

記錄訊息的結構化資料部分中具有緊急、警示、嚴重或錯誤嚴重性層級的所有記錄，皆包含唯一的錯誤碼。錯誤碼由字串和一個十進位數字組成。字串代表特定模組。

MSGID 欄位可識別訊息的類型。如需訊息識別碼清單，請參閱[記錄訊息識別碼](#)。

設定遠端記錄

您可以設定 NSX-T Data Center 應用裝置及 Hypervisor 以傳送記錄訊息至遠端記錄伺服器。

NSX Manager、NSX Controller、NSX Edge 和 Hypervisor 支援遠端記錄。您必須在每個節點上個別設定遠端記錄。

在 KVM 主機上，NSX-T Data Center 安裝套件透過將組態檔置於 `/etc/rsyslog.d` 目錄中，以自動設定 `rsyslog` 精靈。

先決條件

- 設定記錄伺服器來接收記錄。

程序

1 在 NSX-T Data Center 應用裝置上設定遠端記錄：

- a 執行下列命令來設定記錄伺服器和要傳送至記錄伺服器的訊息類型。您可以使用逗號分隔且無空格的清單來指定多個設施或訊息識別碼。

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

如需有關此命令的詳細資訊，請參閱《*NSX-T CLI 參考*》。您可以多次執行命令以新增多個記錄伺服器組態。例如：

```
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 您可以使用 `get logging-server` 命令檢視記錄組態。例如，

```
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 在 ESXi 主機上設定遠端記錄：

- a 執行下列命令以設定 Syslog 和傳送測試訊息：

```
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 您可以執行下列命令以顯示組態：

```
esxcli system syslog config get
```

3 在 KVM 主機上設定遠端記錄：

- a 針對您的環境編輯檔案 `/etc/rsyslog.d/10-vmware-remote-logging.conf`。
- b 將下列行新增至檔案：

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

- c 執行下列命令：

```
service rsyslog restart
```


記錄訊息識別碼

在記錄訊息中，訊息識別碼欄位可識別訊息的類型。您可以使用 `set logging-server` 命令中的 `messageid` 參數，以篩選傳送至記錄伺服器的記錄訊息。

表格 1-1. 記錄訊息識別碼

訊息識別碼	範例
FABRIC	主機節點 主機準備 Edge 節點 傳輸區域 傳輸節點 上行設定檔 叢集設定檔 Edge 叢集 橋接器叢集和端點
SWITCHING	邏輯交換器 邏輯交換器連接埠 交換設定檔 交換器安全性功能
ROUTING	邏輯路由器 邏輯路由器連接埠 靜態路由 動態路由 NAT
FIREWALL	防火牆規則 防火牆規則區段
FIREWALL-PKTLOG	防火牆連線記錄 防火牆封包記錄
GROUPING	IP 集合 Mac 集合 NSGroup NSService NSService 群組 VNI 集區 IP 集區
DHCP	DHCP 轉送

表格 1-1. 記錄訊息識別碼 (繼續)

訊息識別碼	範例
SYSTEM	應用裝置管理 (遠端 Syslog 和 ntp 等) 叢集管理 信任管理 授權 使用者和角色 工作管理 安裝 (NSX Manager、NSX Controller) 升級 (NSX Manager、NSX Controller、NSX Edge 和主機套件升級) 解析 標籤
MONITORING	SNMP 連接埠連線 Traceflow
-	所有其他記錄訊息。

對 Syslog 問題進行疑難排解

如果遠端記錄伺服器未收到記錄，請執行下列步驟。

- 確認遠端記錄伺服器的 IP 位址。
- 確認 level 參數已正確設定。
- 確認 facility 參數已正確設定。
- 如果通訊協定為 TLS，請將通訊協定設定為 UDP，以查看是否憑證不相符。
- 如果通訊協定為 TLS，請確認已在兩端開啟連接埠 6514。
- 移除訊息識別碼篩選器，並查看伺服器是否收到記錄。
- 使用命令 `restart service rsyslogd` 重新啟動 rsyslog 服務。

範例 rsyslog 組態檔 (/etc/rsyslog.conf):

```
### 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
```

檢查服務

服務若停止執行或無法啟動，則可能會導致問題。請務必確認所有服務均正常執行。

檢查 NSX Manager 服務的狀態：

```
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

```

在上述範例中，**http** 服務已停止。您可以使用下列命令啟動 **http** 服務：

```
nsxmgr> start service http
```

SSH 服務

如果在部署應用裝置時未啟用 **SSH** 服務，您可以管理員身分登入應用裝置，並使用下列命令啟用該服務：

```
start service ssh
```

您可以使用下列命令將 **SSH** 設定為在主機啟動時啟動：

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

若要啟用 **SSH** 根登入，可以根使用者身分登入應用裝置，然後編輯檔案 `/etc/ssh/sshd_config` 並取代以下行

```
PermitRootLogin prohibit-password
```

或者，也可以啟用 **SSH** 服務，並透過關閉應用裝置的電源和修改其 **vApp** 內容來啟用 **SSH** 根存取。
取代為

```
PermitRootLogin yes
```


然後，使用下列命令重新啟動 **sshd** 伺服器：

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

收集支援服務包

您可以在登錄的叢集和網狀架構節點上收集支援服務包，並將服務包下載至您的機器或將其上傳至檔案伺服器。

如果您選擇將服務包下載至您的機器，您會取得遊資訊清單檔案和每個節點之支援服務包所組成的單一封存檔案。如果您選擇將服務包上傳至檔案伺服器，則資訊清單檔案和個別服務包會分別上傳至檔案伺服器。

 **NSX Cloud 附註** 如果您想要收集 CSM 的支援服務包，請登入 CSM，移至**系統 > 公用程式 > 支援服務包**，然後按**下載**。可使用下列指示從 NSX Manager 取得 PCG 的支援服務包。PCG 的支援服務包還包含所有工作負載虛擬機器的記錄。

程序

- 1 從瀏覽器以管理員權限登入 NSX Manager，網址為 *https://nsx-manager-ip-address*。
- 2 選取導覽面板中的**系統 > 公用程式**。
- 3 按一下**支援服務包**索引標籤。
- 4 選取目標節點。
 可用的節點類型包含管理節點、控制器節點、Edge、主機和公有雲閘道。
- 5 (選擇性) 指定記錄存留期 (以天為單位) 以排除超過指定天數的記錄。
- 6 (選擇性) 切換表示要包含或排除核心檔案和稽核記錄的交換器。

備註 核心檔案和稽核記錄可能包含機密資訊，例如密碼或加密金鑰。

- 7 (選擇性) 選取核取方塊，將服務包上傳至檔案伺服器。
- 8 按一下**啟動服務包收集**以開始收集支援服務包。
 依所存在的記錄檔數目而定，每個節點可能會花費數分鐘。
- 9 監控收集程序的狀態。
 狀態欄會顯示已完成支援服務包收集的節點百分比。
- 10 如果未設定將服務包傳送至檔案伺服器的選項，請按一下**下載**以下載服務包。

疑難排解第 2 層連線

如果連線至同一邏輯交換器的兩個虛擬介面 (VIF) 之間通訊失敗，例如，無法從一個虛擬機器對另一個虛擬機器執行 Ping 動作，則可以遵循本節中的步驟來疑難排解失敗。

在開始之前，請確保沒有封鎖兩個邏輯連接埠之間流量的防火牆規則。建議您遵循本節中的主題順序來疑難排解連線問題。

本章節討論下列主題：

- 檢查 NSX Manager 和 NSX Controller 叢集狀態
- 檢查邏輯連接埠
- 檢查傳輸節點狀態
- 檢查邏輯交換器狀態
- 檢查邏輯交換器的 CCP
- 檢查本機控制平面狀態
- 疑難排解組態工作階段問題
- 疑難排解 L2 工作階段問題
- 疑難排解覆疊邏輯交換器的數據平面問題
- 疑難排解 VLAN 邏輯交換器的數據平面問題
- 疑難排解覆疊邏輯交換器的 ARP 問題
- 疑難排解 VLAN 邏輯交換器或解析 ARP 時的封包遺失問題

檢查 NSX Manager 和 NSX Controller 叢集狀態

確認 NSX Manager 和 NSX Controller 叢集的狀態正常，且控制器已連線至 NSX Manager。

程序

- 1 在 NSX Manager 上執行下列 CLI 命令，以確保狀態為 stable。

```
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 在 NSX Controller 上執行下列 CLI 命令，以確保狀態為 **active**。

```
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 在 NSX Controller 上執行下列 CLI 命令，以確保其已連線至 NSX Manager。

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

檢查邏輯連接埠

確認已在相同的邏輯交換器上設定邏輯連接埠，並且這些連接埠的狀態為已啟動。

程序

- 1 從 NSX Manager GUI，取得邏輯連接埠 UUID。
- 2 針對每個邏輯連接埠進行下列 API 呼叫，以確保這些邏輯連接埠位於相同的邏輯交換器上。

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

- 3 針對每個邏輯連接埠進行下列 API 呼叫，以確保狀態為已啟動。

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

檢查傳輸節點狀態

檢查傳輸節點狀態。

程序

- ◆ 執行下列 API 呼叫以取得傳輸節點狀態。

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

如果呼叫傳回錯誤 RPC 逾時，請執行下列疑難排解步驟：

- 執行 `/etc/init.d/nsx-opsAgent status` 以查看 `opsAgent` 是否正在執行。
- 執行 `/etc/init.d/nsx-mpa status` 以查看 `nsx-mpa` 是否正在執行。
- 若要查看 `nsx-mpa` 是否已連線至 NSX Manager，請檢查 `nsx-mpa` 活動訊號記錄。
- 若要查看 `opsAgent` 是否已連線至 NSX Manager，請檢查 `nsx-opsAgent` 記錄。如果 `opsAgent` 已連線至 NSX Manager，您會看到下列訊息。

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

- 若要查看 `opsAgent` 是否在處理 `HostConfigMsg` 時停滯，請檢查 `nsx-opsAgent` 記錄。若停滯的話，您會看到 RMQ 要求訊息，但未傳送回覆或長時間延遲後傳送。
- 檢查以查看在執行 `HostConfigMsg` 時 `opsAgent` 是否當機。
- 若要查看是否花費了很長時間才將 RMQ 訊息傳遞到主機，請比較 NSX Manager 和主機上記錄訊息的時間戳記。

如果呼叫傳回錯誤 `partial_success`，有許多可能的原因。從查看 `nsx-opsAgent` 記錄開始。在 ESXi 主機上，檢查 `hostd.log` 和 `vmkernel.log`。在 KVM 上，`Syslog` 會保留所有記錄。

檢查邏輯交換器狀態

檢查邏輯交換器狀態。

程序

- ◆ 執行下列 API 呼叫以取得邏輯交換器狀態。

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

如果呼叫傳回錯誤 `partial_success`，回覆將包含 NSX Manager 無法推送邏輯交換器組態或未取得回覆的傳輸節點的清單。疑難排解步驟類似於傳輸節點的疑難排解步驟。檢查下列項目：

- 所有必要元件均已安裝且正在執行。
- `nsx-mpa` 已連線至 NSX Manager。
- `nsxa` 已連線至垂直切換。
- 在 `nsxa.log` 和 `nsxaVim.log` 中對邏輯交換器識別碼執行 `grep` 命令，以查看傳輸節點是否已接收邏輯交換器組態。
- 檢查 `nsxa` 和 `nsx-mpa` 運作時間。透過在 `Syslog` 檔案中對 `nsxa` 記錄訊息執行 `grep` 命令，找出 `nsxa` 的啟動和停止時間。
- 找出 `nsxa` 與垂直切換的連線時間。如果在 `nsxa` 未連線至垂直切換的情況下傳送邏輯交換器組態到主機，則組態可能不會傳遞到主機。

在 KVM 上，沒有任何邏輯交換器組態推送到主機。因此，大部分的邏輯交換器問題可能都在管理平面。

在 ESXi 上，不透明網路會對應到邏輯交換器。若要使用邏輯交換器，使用者需使用 vCenter Server 或 vSphere API 將虛擬機器連線到不透明網路。

檢查邏輯交換器的 CCP

確認邏輯交換器位於中央控制平面 (CCP)。

程序

- ◆ 在 NSX Controller 上執行下列 CLI 命令，以確保邏輯交換器存在。

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

備註 此 CLI 命令不會列出支援 VLAN 的邏輯交換器。

檢查本機控制平面狀態

對於覆疊邏輯交換器，請確認主機上的 netcpa 已連線至中央控制平面。

先決條件

找到邏輯交換器所在的控制器。請參閱[檢查邏輯交換器的 CCP](#)。

程序

- 1 透過 SSH 找到邏輯交換器所在的控制器。
- 2 執行下列命令，並確認控制器顯示已連線到此 VNI 的 Hypervisor。

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

- 3 在 Hypervisor 上，執行 /bin/nsxcli 命令以啟動 NSX CLI。
- 4 執行下列命令以取得 CCP 工作階段。

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

您應當會在 CCP 叢集中的其中一個 CCP 節點上看到組態工作階段。對於每個覆疊邏輯交換器，您應該會在 CCP 叢集中的其中一個 CCP 節點上看到 L2 工作階段。對於 VLAN 邏輯交換器，沒有任何 CCP 連線。

疑難排解組態工作階段問題

如果 CCP 組態工作階段未啟動，請檢查 MPA 和 netcpa 的狀態。

程序

- 1 進行下列 API 呼叫以查看 MPA 是否已連線至 NSX Manager。

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

- 2 在 Hypervisor 上，執行 /bin/nsxcli 命令以啟動 NSX CLI。
- 3 執行下列命令以取得 node-uuid。

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

- 4 執行下列命令，以查看 NSX Manager 是否已將 CCP 資訊推送到主機。

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

- 5 如果 config-by-vsm.xml 具有 CCP 資訊，請檢查是否已在 Hypervisor 上設定傳輸節點。

在傳輸節點建立步驟中，NSX Manager 會傳送 Hypervisor 的主機憑證。CCP 必須具有主機憑證，才能接受來自主機的連線。

- 6 檢查 /etc/vmware/nsx/host-cert.pem 中主機憑證的有效性。

此憑證必須與 NSX Manager 用於主機之憑證相同。

- 7 執行下列命令，以檢查 netcpa 的狀態。

在 ESXi 上：

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

在 KVM 上：

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

- 8 啟動或重新啟動 netcpa。

在 ESXi 上啟動 (若未執行) 或重新啟動 (若正在執行) netcpa。

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

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

在 KVM 上啟動 (若未執行) 或重新啟動 (若正在執行) `netcpa`。

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

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

- 9 如果組態工作階段仍未啟動，請收集技術支援服務包並連絡 VMware 支援。

疑難排解 L2 工作階段問題

這僅適用於覆疊邏輯交換器。

程序

- 1 在 Hypervisor 上，執行 `/bin/nsxcli` 命令以啟動 NSX CLI。
- 2 執行下列命令，查看邏輯交換器是否存在於主機上。

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

- 3 確認連接埠的狀態不是管理員已關閉。

在 ESXi 上，執行 `net-dvs` 並查看回應。例如，

```
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.
```

如果邏輯連接埠在已封鎖狀態下結束，請收集技術支援服務包並連絡 VMware 支援。同時，請執行下列命令以取得 DVS 名稱：

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

執行下列命令以解除封鎖連接埠：

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

在 KVM 上，執行 `ovs-vsctl list interface` 並確認具有對應 VIF UUID 的介面已存在，並且 `admin_state` 已啟動。您可以在 `external-ids:iface-id` 的 OVSDB 中查看 VIF UUID。

疑難排解覆疊邏輯交換器的數據平面問題

本節中的步驟適用於當組態和執行階段狀態正常時，透過覆疊交換器對不同 Hypervisor 上虛擬機器之間的連線問題進行疑難排解。

如果虛擬機器位於相同的 Hypervisor 上，請移至[疑難排解覆疊邏輯交換器的 ARP 問題](#)。

程序

- 1 在具有邏輯交換器的控制器上執行下列命令，以查看 CCP 是否有正確的 VTEP 清單：

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

- 2 在每個 Hypervisor 上，執行下列 NSX CLI 命令以查看其是否有正確的 VTEP 清單：

在 ESXi 上：

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

或者，您可以執行下列 Shell 命令以取得 VTEP 資訊：

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

在 KVM 上：

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

- 3 檢查以查看 Hypervisor 上的 VTEP 是否可以互相執行 Ping 偵測。

在 ESXi Shell 提示字元中：

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

在 KVM Shell 提示字元中：

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

如果 VTEP 無法互相執行 Ping 偵測，

- a 請確定建立傳輸節點時指定的傳輸 VLAN 符合底層的預期。如果您使用底層中的存取連接埠，傳輸 VLAN 應設定為 0。如果您指定傳輸 VLAN，則 Hypervisor 連線到的底層交換器連接埠應設定為在主幹模式下接受此 VLAN。
 - b 檢查底層連線。
- 4 檢查 VTEP 之間的 BFD 工作階段是否已啟動。

在 ESXi 上，執行 `net-vd12 -M bfd` 並查看回應。例如，

```
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: 10000000, isDisabled: 0
```

在 KVM 上，找到遠端 IP 的 GENEVE 介面。

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

如果您不知道介面名稱，請執行 `ovs-vsctl find Interface type=geneve` 以傳回所有通道介面。尋找 BFD 資訊。

如果找不到遠端 VTEP 的 GENEVE 介面，請檢查 `nsx-agent` 是否正在執行，並且 OVS 整合橋接器是否已連線到 `nsx-agent`。

```
[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
```

疑難排解 VLAN 邏輯交換器的數據平面問題

本節中的步驟適用於當組態和執行階段狀態正常時，透過底層上設定的 VLAN 對不同 Hypervisor 上虛擬機器之間的連線問題進行疑難排解。

如果虛擬機器位於相同的 Hypervisor 上，並且所有組態和執行階段狀態正常，請移至[疑難排解覆疊邏輯交換器的 ARP 問題](#)。

程序

- ◆ 確認對於處於主幹模式的邏輯交換器，已針對 VLAN 設定底層。

在 ESXi 上，確認已透過執行 `net-dvs` 並尋找邏輯連接埠，在邏輯連接埠上設定 VLAN。例如：

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

在 KVM 上，VLAN 邏輯交換器會設定為整合橋接器上的開放流程規則。換句話說，對於來自 VIF 的流量，使用 VLAN X 加以標記，然後在修補程式連接埠上將其轉送到 PIF 橋接器。執行 `ovs-vsctl list interface`，確認 NSX 管理的橋接器和 NSX 交換器橋接器之間存在修補程式連接埠。

疑難排解覆疊邏輯交換器的 ARP 問題

本節中的步驟適用於疑難排解覆疊交換器遺失封包的情況。

如需 VLAN 支援的邏輯交換器，請前往[疑難排解 VLAN 邏輯交換器或解析 ARP 時的封包遺失問題](#)。

在執行下列疑難排解步驟之前，請在每個虛擬機器上執行 `arp -n` 命令。如果在兩個虛擬機器上成功解析 ARP，則無需執行本節中的步驟。請直接前往下一節[疑難排解 VLAN 邏輯交換器或解析 ARP 時的封包遺失問題](#)。

程序

- ◆ 如果兩個端點都是 ESXi，並且已在邏輯交換器 (僅支援覆疊邏輯交換器) 上啟用 ARP Proxy，請檢查 CCP 和 Hypervisor 上的 ARP 資料表。

在 CCP 上：

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

在 Hypervisor 上，啟動 NSX CLI 並執行下列命令：

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

擷取 ARP 資料表只會瞭解 ARP Proxy 的狀態是否正確。如果不會透過 Proxy 接收 ARP 回應，或者主機為 KVM 並且不支援 ARP Proxy，則資料路徑應廣播 ARP 要求。BUM 流量轉送可能出現問題。請嘗試下列步驟：

- 如果邏輯交換器的複寫模式為 MTEP，請將邏輯交換器的複寫模式從 NSX Manager GUI 變更為 SOURCE。這可能會修正此問題，並且 Ping 動作將開始正常運作。
- 新增靜態 ARP 項目，並查看剩餘資料路徑是否正常運作。

疑難排解 VLAN 邏輯交換器或解析 ARP 時的封包遺失問題

您可以使用自動 Traceflow 工具或手動追蹤封包來疑難排解封包遺失。

若要從 NSX Manager GUI 執行 Traceflow 工具，請導覽至[工具 > Traceflow](#)。如需詳細資訊，請參閱《*NSX-T 管理指南*》。

程序

- ◆ 手動追蹤封包

在 ESXi 上，執行 `net-stats -l` 以取得 VIF 的交換器連接埠識別碼。如果來源和目的地 VIF 位於相同的 Hypervisor 上，請執行下列命令：

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

如果來源和目的地 VIF 位於不同的 Hypervisor 上，請在裝載來源 VIF 的 Hypervisor 上執行下列命令：

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

在裝載目的地 VIF 的 Hypervisor 上，執行下列命令：

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

在 KVM 上，如果來源和目的地 VIF 位於相同的 Hypervisor 上，請執行下列命令：

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

對安裝進行疑難排解

本節提供對安裝問題進行疑難排解的相關資訊。

基本基礎結構服務

下列服務必須在應用裝置及 Hypervisor 上執行，同時還必須在 vCenter Server 上執行 (若用作計算管理程式)。

- NTP
- DNS

請確定防火牆未封鎖 NSX-T 元件與 Hypervisor 之間的流量。請確定元件之間已開啟所需連接埠。

若要排清 NSX Manager 上的 DNS 快取，請透過 SSH，以根使用者身分登入該管理員並執行下列命令：

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

然後，可以檢查 DNS 組態檔。

```
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
```

檢查從主機到控制器和管理程式的通訊

在 ESXi 主機上使用 NSX-T CLI 命令：

```
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	1235	enabled	connected	true	up	NA

在 KVM 主機上使用 NSX-T CLI 命令：

```
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	1235	enabled	connected	true	up	NA

在 ESXi 主機上使用主機 CLI 命令：

```
[root@esxi-01:~] esxcli network ip connection list | grep 1235
tcp          0      0 192.168.110.53:42271      192.168.110.16:1235
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
```

在 KVM 主機上使用主機 CLI 命令：

```
root@kvm-01:/home/vmware# netstat -nap | grep 1235
tcp          0      0 192.168.110.55:53686      192.168.110.16:1235 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 1235 | 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.1235 > 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.1235: 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>
```

主機登錄失敗

如果 NSX-T 使用錯誤的 IP 位址，主機登錄便會失敗。如果某個主機有多個 IP 位址，可能會發生此情況。嘗試刪除傳輸節點會使它處於孤立狀態。解決此問題：

- 前往**網狀架構 > 節點 > 主機**，編輯主機，然後移除所有 IP 位址 (管理位址除外)。
- 按一下錯誤，然後選取**解決**。

KVM 主機問題

KVM 主機問題有時由磁碟空間不足所致。/boot 目錄會快速填滿並導致錯誤發生，例如：

- 無法在主機上安裝軟體
- 裝置上沒有剩餘空間

您可以執行命令 **df-h** 來檢查可用儲存區。如果 /boot 目錄顯示為 100%，您可以執行下列操作：

- 執行 **sudo dpkg --get-selections | grep ^ii** 以查看所有已安裝的核心。
- 執行 **uname -r** 以查看目前執行中的核心。請勿移除此核心 (linux-image)。
- 使用 **apt-get purge** 移除您不再需要的映像。例如，執行 **sudo apt-get purge linux-image-3.13.0-32-generic linux-image-3.13.0-33-generic**。
- 將主機重新開機。
- 在 NSX Manager 中，檢查錯誤並選取**解決**。
- 請確保虛擬機器已開啟電源。

部署 Edge 虛擬機器時的組態錯誤

部署 Edge 虛擬機器後，NSX Manager 會將虛擬機器的狀態顯示為**組態錯誤**。管理員記錄包含類似下列內容的訊息：

```
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'].
```

重新啟動 Edge 資料路徑服務，虛擬機器應會解決此問題。

強制移除傳輸節點

您可以藉由下列 API 呼叫，移除停滯在孤立狀態的傳輸節點：

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

NSX Manager 不會執行任何驗證，來確認是否有任何作用中的虛擬機器正在主機上執行。您要負責刪除 N-VDS 和 VIB。如果您已透過計算管理程式新增節點，請先刪除計算管理程式，然後刪除節點。傳輸節點也會一併刪除。

對路由進行疑難排解

NSX-T 具有可用來對路由問題進行疑難排解的內建工具。

Traceflow

您可以使用 **Traceflow** 檢查封包流程。您可以查看傳遞、捨棄、接收和轉送的封包。如果封包已捨棄，則會顯示原因。例如，封包可能因防火牆規則而捨棄。

檢查路由表

若要查看服務路由器上的路由表，請執行下列命令：

```
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

若要取得介面的 IP 位址，請執行下列命令：

```
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
```

通告 T1 路由

您必須通告 T1 路由，以便這些路由在 T0 及以上路由器中可見。您可以通告不同類型的路由：**NSX** 已連線、NAT、靜態、LB VIP 以及 LB SNAT。

對防火牆進行疑難排解

本節提供對防火牆問題進行疑難排解的相關資訊。

本章節討論下列主題：

- 判斷 ESXi 主機上套用的防火牆規則
- 判斷 KVM 主機上套用的防火牆規則
- 防火牆封包記錄

判斷 ESXi 主機上套用的防火牆規則

若要疑難排解 ESXi 主機的防火牆問題，您可以查看主機上套用的防火牆規則。

取得 ESXi 主機上的 dvfilter 清單：

```
[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
```

尋找特定虛擬機器的 dvfilter:

```
[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
.
.
.
```

判斷套用到特定 dvfilter 的防火牆規則 (在此範例中, nic-70227-eth0-vmware-sfw.2 為 dvfilter 名稱):

```
[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;
}
}
```

取得特定 dvfilter 中使用的位址集清單:

```
[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,
}

```

檢查流經特定 `dvfilter` 的流量：

```

[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

```


判斷 KVM 主機上套用的防火牆規則

若要疑難排解 KVM 主機的防火牆問題，您可以查看主機上套用的防火牆規則。

取得受限於 KVM 主機上的防火牆規則的 VIF 清單：

```
# 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
```

如果輸出空白，請尋找節點和控制器之間的連線問題。

取得套用至特定 VIF 的規則清單 (在此範例中，da95fc1e-65fd-461f-814d-d92970029bf0 為 VIF 識別碼)：

```
# 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 5e9bdc3b-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;
}

```

取得特定 VIF 中使用的位址集清單：

```

# 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,
}

```

透過 Linux Conntrack 模組檢查連線。在此範例中，尋找兩個特定 IP 位址之間經過的流量。

```

# 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

```

防火牆封包記錄

如果已為防火牆規則啟用記錄，則可以查看防火牆封包記錄來對問題進行疑難排解。

ESXi 和 KVM 主機的記錄檔為 `/var/log/dfwpktlogs.log`。

```

# 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

其他疑難排解案例

本節說明如何疑難排解各種錯誤情況。

本章節討論下列主題：

- 無法新增或刪除傳輸節點
- 傳輸節點連線至另一個控制器需要大約 5 分鐘
- NSX Manager 虛擬機器已降級
- NSX 代理程式與 NSX Manager 通訊逾時
- 無法新增 ESXi 主機
- NSX Controller 狀態不正確
- 在已啟用 IPFIX 的情況下，KVM 虛擬機器上的管理 IP 無法連線

無法新增或刪除傳輸節點

您無法刪除或新增傳輸節點。

問題

在下列情況下會發生錯誤：

- 1 ESXi 主機為網狀架構節點和傳輸節點。
- 2 主機做為傳輸節點遭到移除。但是，傳輸節點刪除失敗。傳輸節點的狀態為孤立。
- 3 主機做為網狀架構節點立即遭到移除。
- 4 主機重新新增為網狀架構節點。
- 5 主機新增為具有新傳輸區域和交換器的傳輸節點。此步驟會導致錯誤失敗/部分成功。

原因

在步驟 2 中，如果等待幾分鐘，將會成功刪除傳輸節點，因為 NSX Manager 會重試刪除。若您立即刪除網狀架構節點，NSX Manager 將無法重試，因為主機已從 NSX-T Data Center 移除。這會導致主機的清理不完整，交換器組態仍然存在，從而造成步驟 5 失敗。

解決方案

- 1 在連線至 NSX-T Data Center 交換器的主機上，從 vCenter Server 刪除所有 vmknics。
- 2 使用 `esxcfg-vswitch -l` CLI 命令取得交換器名稱。例如：

```
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 使用 `esxcfg-vswitch -d <switch-name> --dvswitch` CLI 命令刪除交換器名稱。例如：

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

傳輸節點連線至另一個控制器需要大約 5 分鐘

如果 ESXi 傳輸節點的已連線控制器發生故障，傳輸節點連線至另一個控制器則會需要大約 5 分鐘。

問題

ESXi 傳輸節點通常會連線至控制器叢集中的特定控制器。您可以使用 CLI 命令 `get controllers` 找到已連線的控制器。如果已連線的控制器發生故障，傳輸節點連線至另一個控制器則會需要大約 5 分鐘。

原因

傳輸節點會嘗試重新連線至已關閉的控制器，經過一定的時間後會放棄並連線到另一個控制器。整個程序大約需要 5 分鐘。這是預期的行為。

NSX Manager 虛擬機器已降級

KVM 主機上部署的 NSX Manager 在執行 `get service` 和 `get interface` 等 CLI 命令時傳回錯誤。

問題

CLI 命令 `get service` 傳回錯誤。例如，

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

其他 CLI 命令也可能會傳回錯誤。get support-bundle 命令表示 /tmp 目錄已變成唯讀狀態。例如，

```
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> 記錄包含如下的訊息：

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

原因

NSX Manager 應用裝置上的一或多個檔案系統已損毀。一些可能的原因已記錄在 <https://access.redhat.com/solutions/22621>。

若要解決此問題，您可以修復損毀的檔案系統或從備份執行還原。

解決方案

1 選項 1：修復損毀的檔案系統。以下步驟專門針對 KVM 主機上執行的 NSX Manager。

- a 執行 `virsh destroy` 命令以停止 NSX Manager 虛擬機器。
- b 針對 qcow2 映像，以寫入模式執行 `virt-rescue` 命令。例如，

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

- c 在 `virt-rescue` 命令提示字元中，執行 `e2fsck` 命令以修正 tmp 檔案系統。例如，

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

- d 如有必要，請再次執行 `e2fsck /dev/nsx/tmp` 直到沒有更多錯誤。
- e 使用 `virsh start` 重新啟動 NSX Manager。

2 選項 2：從備份執行還原。

如需指示，請參閱《NSX-T 管理指南》。

NSX 代理程式與 NSX Manager 通訊逾時

在 ESXi 主機上具有許多傳輸節點和虛擬機器的大型環境中，ESXi 主機上執行的 NSX 代理程式在與 NSX Manager 通訊時可能會逾時。

問題

某些作業 (例如虛擬機器 vnic 嘗試附加至邏輯交換器) 會失敗。/var/run/log/nsx-opsagent.log 包含如下的訊息：

```
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

在大型環境中，部分作業可能花費的時間比平時要長，並因為超過預設逾時值而失敗。

解決方案

1 增加 NSX 代理程式逾時值。

- a 在 ESXi 主機上，使用下列命令停止 NSX opsAgent：

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

- b 編輯檔案 /etc/vmware/nsx-opsagent/nsxa.json，並變更 vifOperationTimeout 的值，例如從 25 變更為 55。

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

備註 此逾時值必須小於您在步驟 2 中設定的 hostd 逾時值。

- c 使用下列命令啟動 NSX opsAgent：

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

2 增加 hostd 逾時值。

- a 在 ESXi 主機上，使用下列命令停止 hostd 代理程式：

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

- b 編輯檔案 `/etc/vmware/hostd/config.xml`。在 `<opaqueNetwork>` 下，取消 `<taskTimeout>` 項目的註解並變更值，例如從 30 變更為 60。

```
<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 使用下列命令啟動 hostd 代理程式：

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

無法新增 ESXi 主機

您無法將 ESXi 主機新增至 NSX-T Data Center 網狀架構。

問題

從 NSX Manager GUI 新增 ESXi 主機失敗，並顯示錯誤「... 的檔案路徑已由多個非覆疊 VIB 宣告」。記錄檔顯示如下的訊息：

```
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/vmkmod/nsx-vsip' is claimed
by multiple non-overlay VIBs
```

原因

先前安裝的一些 VIB 仍在主機上，可能是未執行完整解除安裝。

解決方案

- 1 從錯誤訊息取得導致失敗的 VIB 的名稱。
- 2 使用 ESXi 命令解除安裝 VIB。

NSX Controller 狀態不正確

NSX Controller 叢集中的一些控制器報告其中一個控制器的狀態不正確。

問題

當某個控制器數次關閉並開啟電源後，其他控制器會將此控制器報告為非作用中，而它實際上已啟動且正在執行。

原因

當某個控制器關閉並開啟電源時，有時會發生涉及 ZooKeeper 模組的內部錯誤，導致此控制器與叢集中其他控制器之間的通訊失敗。

解決方案

- ◆ 從叢集移除報告為非作用中的控制器節點，從節點移除叢集組態並將節點重新加入叢集。如需詳細資訊，請參閱《NSX-T 管理指南》中的〈取代 NSX Controller 叢集的成員〉一節。

在已啟用 IPFIX 的情況下，KVM 虛擬機器上的管理 IP 無法連線

在 KVM 主機上的多個虛擬機器上啟用 IPFIX 且取樣速率為 100% 時，某些虛擬機器上的管理 IP 可能會間歇性地無法連線。

問題

當您為同一主機上的多個虛擬機器啟用 IPFIX 且取樣速率設為 100% 時，會有大量 IPFIX 流量。這會影響管理流量，導致管理 IP 間歇性地無法連線，即使生產流量與管理流量經過不同的 OVS 亦是如此。

原因

此工作負載對於主機和虛擬機器而言非常大。

解決方案

- ◆ 透過減少啟用 IPFIX 的虛擬機器數目或降低取樣速率，來減輕主機的負載。