在Nexus 1000V系列交换机上使用vempkt命令捕获流量

目录

[简介](#)
[先决条件](#)
[要求](#)
[使用的组件](#)
[规则](#)
[vempkt命令](#)
[开始捕获](#)
[最终捕获](#)
[文件导出](#)
[相关信息](#)

简介

本文档介绍如何使用**vempkt**命令捕获Nexus 1000V系列交换机上的流量。

Nexus 1000V系列交换机上的问题很难排除，因为没有物理交换机可供您操作。在大部分时间内，数据包捕获是确定数据包是否在上游发送的必要条件。

先决条件

要求

Cisco 建议您了解以下主题：

- Cisco Nexus 1000V系列交换机
- Cisco NX-OS软件

使用的组件

本文档中的信息基于Nexus 1000V系列交换机。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

vempkt命令

vempkt命令是可用于捕获离开Nexus 1000V交换机中特定主机的流量的**有用**命令。此命令与SPAN会话非常相似；但是，它更灵活，因为它可以应用于任何接口，而无需捕获设备。

开始捕获

要捕获流量，请在具有要捕获流量的虚拟机(VM)的ESX主机的命令行上输入**vempkt SSH**命令。输入此命令后，输入以下命令：

vempkt show info — 这显示最近捕获的信息。

vempkt capture all-stages vlan [y] ltl [x]

LTL是链路的本地目标逻辑。如果您不知道LTL或VLAN，请输入**vemcmd show port**命令和**vemcmd show port vlans命**令。思科建议使用端口通道的LTL，因为它包含离开主机并进入主机的所有流量。

您还可以捕获输入此命令的一个方向或丢弃的数据包：

vempkt捕获 `[ | | |] ltl [x] vlan [y]`

注意：如果未指定LTL，捕获将显示所有LTL，如果未指定VLAN，捕获将显示所有VLAN。

```
The ESXi Shell can be disabled by an administrative user. See the
vSphere Security documentation for more information.
~ # vempkt show info
                Enabled  : Yes
    Total Packet Entries  : 0
  Wrapped Packet Entries  : 0
     Lost Packet Entries  : 0
  Skipped Packet Entries  : 0
Available Packet Entries  : 14563
     Packet Capture Size  : 88
     Packet Capture Mode  : Un Reliable
 Stop After Packet Entry  : Not Specified
~ # vemcmd show port
  LTL   VSM Port  Admin Link  State  PC-LTL  SGID  Vem Port  Type
   17     Eth3/1     UP   UP    F/B*    305     0    vmnic0
   18     Eth3/2     UP   UP    F/B*    305     1    vmnic1
   49      Veth6     UP   UP    FWD       0     1      vmk0
   50      Veth3     UP   UP    FWD       0     1  Nexus1000V.eth2
   51      Veth2     UP   UP    FWD       0     0  Nexus1000V.eth1
   52      Veth1     UP   UP    FWD       0     0  Nexus1000V.eth0
   53      Veth5     UP   UP    FWD       0     0  Win 2K8 - 2 ethernet0
   54            DOWN   UP    BLK       0        Win 2K8 ethernet1
   55      Veth4     UP   UP    FWD       0     0  Win 2K8 ethernet0
  305        Po1     UP   UP    F/B*      0

* F/B: Port is BLOCKED on some of the vlans.
 Please run "vemcmd show port vlans" to see the details.
~ #
```

```
~ # vemcmd show port vlans
                      Native  VLAN   Allowed
  LTL   VSM Port  Mode  VLAN    State  Vlans
   17     Eth3/1   T        1   FWD    168
   18     Eth3/2   T        1   FWD    168
   49      Veth6   A      168   FWD    168
   50      Veth3   A      168   FWD    168
   51      Veth2   A      168   FWD    168
   52      Veth1   A      168   FWD    168
   53      Veth5   A      168   FWD    168
   54              A        1   BLK    1
   55      Veth4   A      168   FWD    168
  305        Po1   T        1   FWD    168
~ #
```

输入**vempkt size [mtu size]**以指定最大传输单位(MTU)大小捕获。

输入vempkt **show capture info命令**以验证捕获参数。

```
~ # vempkt show capture info
 Stage : Ingress
     LTL : 305
    VLAN : 168
    Filter : Unspecified
 Stage : Egress
     LTL : 305
    VLAN : 168
    Filter : Unspecified
 Stage : Drop
     LTL : 305
    VLAN : 168
    Filter : Unspecified
 Stage : Aipc
     LTL : Unspecified
    VLAN : Unspecified
```

输入**vempkt start**命令开始捕获。

最终捕获

完成捕获操作后，输入以下命令以结束捕获并导出文件：

1. **停车**。
2. **vempkt show info**以显示捕获的统计信息。
3. **vempkt display detail all > /tmp/vempkt_capture.txt**。此命令将捕获文件放入主机的/tmp目录。从此目录，您可以将其复制到数据存储中并通过vCenter将其导出。
4. **清场**。

文件导出

您可以从CLI将文件导出到数据包捕获(PCAP)。在主机上输入以下命令：**#vempkt pcap导** `<filename>`。此命令将文件放在您当前所在的目录中。

相关信息

- Cisco Nexus 1000V系列交换机
- 技术支持和文档 - Cisco Systems