将UCS刀片服务器上的虚拟机配置为SPAN目标

目录

<u>简介</u> <u>先决条件</u> <u>要求</u> <u>使用的组件</u> <u>背景信息</u> 配置 <u>网络图</u> <u>具有IP地址的嗅探器虚拟机</u> <u>嗅探器VM,无IP地址</u> <u>故障场景</u> <u>验证</u> <u>故障排除</u> <u>相关信息</u>

简介

本文档介绍捕获完全在思科统一计算系统(UCS)外的流量并将其定向到在UCS内运行嗅探器工具的 虚拟机(VM)的步骤。捕获的流量的源和目标在UCS之外。捕获可以在直接连接到UCS的物理交换机 上启动,也可以在几跳之外启动。

先决条件

要求

Cisco 建议您了解以下主题:

- UCS
- VMware ESX 4.1版或更高版本
- 封装远程交换机端口分析器(ERSPAN)

使用的组件

本文档中的信息基于以下软件和硬件版本:

- •运行12.2(18)ZYA3c的Cisco Catalyst 6503
- •运行2.2(3e)的Cisco UCS B系列
- VMWare ESXi 5.5内部版本1331820

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。

背景信息

UCS没有远程SPAN(RSPAN)功能,无法从连接的交换机接收SPAN流量并将其定向到本地端口。 因此,在UCS环境中实现此目标的唯一方法是在物理交换机上使用封装RSPAN(ERSPAN)功能,并 使用IP将捕获的流量发送到虚拟机。在某些实施中,运行嗅探器工具的VM不能有IP地址。本文档说 明嗅探器VM具有IP地址时所需的配置以及没有IP地址的场景。此处的唯一限制是嗅探器VM需要能 够从发送到它的流量中读取GRE/ERSPAN封装。



网络图

本文档已考虑此拓扑:



连接到Catalyst 6500的GigabitEthernet1/1的PC正在受到监控。GigabitEthernet1/1上的流量被捕获 并发送到服务器1上Cisco UCS内部运行的嗅探器VM。6500交换机上的ERSPAN功能捕获流量,使 用GRE将其封装,然后将其发送到嗅探器VM的IP地址。

具有IP地址的嗅探器虚拟机

注意:本节中介绍的步骤也可用于嗅探器在UCS刀片上的裸机服务器中运行,而不是在VM上 运行的场景。

当嗅探器VM可以具有IP地址时,需要执行以下步骤:

- •在UCS环境中配置嗅探器VM,使用可从6500访问的IP地址
- 在虚拟机内运行嗅探器工具
- 在6500上配置ERSPAN源会话,并将捕获的流量直接发送到VM的IP地址

6500交换机上的配置步骤:

CAT6K-01(config)#monitor session 1 type erspan-source CAT6K-01(config-mon-erspan-src)#source interface gil/1 CAT6K-01(config-mon-erspan-src)#destination CAT6K-01(config-mon-erspan-src-dst)#ip address 192.0.2.2 CAT6K-01(config-mon-erspan-src-dst)#origin ip address 192.0.2.1 CAT6K-01(config-mon-erspan-src-dst)#erspan-id 1 CAT6K-01(config-mon-erspan-src-dst)#exit CAT6K-01(config-mon-erspan-src)#no shut CAT6K-01(config-mon-erspan-src)#end **在本例中**.嗅探器VM的IP地址为192.0.2.2

嗅探器VM,无IP地址

当嗅探器VM不能有IP地址时,需要执行以下步骤:

- 在UCS环境中配置嗅探器VM
- 在虚拟机内运行嗅探器工具
- •创建可在同一主机中具有IP地址的第二个VM,并使用可从6500访问的IP地址配置该VM
- 将VMWare vSwitch上的端口组配置为混合模式
- •在6500上配置ERSPAN源会话,并将捕获的流量发送到第二个VM的IP地址

以下步骤显示VMWare ESX上所需的配置:如果已配置端口组,请直接转到步骤2。

1.创建虚拟机端口组,并为其分配两个虚拟机

• 导航至"网络"选项卡,然后单击"vSphere标准交换机"下的"添加网络"

Resource Allocation Performance Configuration Tasks & Events Alarms Permissions Maps Storage Views Hardware Status

View: vSphere Standard Switch vSphere Distributed Switch
Networking

Refresh Add Networking... Properties...

• 创建类型虚拟机的端口组

2 Add Network Wizard		x
Connection Type Networking hardware can	be partitioned to accommodate each service that requires connectivity.	
Connection Type Network Access Connection Settings Summary	Connection Types ✓ Virtual Machine Add a labeled network to handle virtual machine network traffic. ✓ Vflkernel The VMkernel TCP/IP stack handles traffic for the following ESXi services: vSphere vMotion, iSCSI, NFS, and host management.	
Help	< Back Next > Cancel	

• 将物理接口(vmnic)分配给端口组,如本图所示。

Add Network Wizard	and a second designed in the local division of the local divisione	-	Acres and	_ D X
Virtual Machines - Netw Virtual machines reach	ork Access networks through uplink adapters attached to vSphe	ere standard swi	tches.	
Connection Type Network Access	Select which vSphere standard switch will handle vSphere standard switch using the unclaimed ne	e the network tra twork adapters	affic for this connection. You may also listed below.	create a new
Connection Settings Summary	Create a vSphere standard switch Emulex Corporation OneConnect 10	Speed OGb NIC (be3)	Networks	
	Vmnic1	10000 Full	10.76.78.22-10.76.78.22	
	C Use vSwitch0	Speed	Networks	
		10000 Full	10.76.78.22-10.76.78.22	
	Preview:			
	Virtual Machine Port Group VM Network 2	Physical Adapters		
Help			< Back Next >	Cancel

•为端口组配置名称,并添加相关VLAN,如图所示。

2 Add Network Wizard		A COLUMN TWO IS NOT	Accelerate	
Virtual Machines - Connect Use network labels to iden	ion Settings tify migration compatible connection	ons common to two or more hosts.		
Connection Type Network Access Connection Settings Summary	Port Group Properties Network Label: VLAN ID (Optional): Preview: Virtual Machine Port Group - SPAN_monitoring	SPAN_monitoring None (0)		
Help			< Back	Next > Cancel

•验证配置并单击"**完成**",如图所示。

Add Network Wizard	and the second sec	
Ready to Complete Verify that all new and mo	dified vSphere standard switches are configured appropriately.	
Connection Type Network Access	Host networking will include the following new and modified standard switches: Preview:	
Summary	Virtual Machine Port Group SPAN_monitoring	
Help	< Back Finish	Cancel

2.将端口组配置为混杂模式,如图所示。

- •端口组现在必须显示在"网络"选项卡下
- 单击"属**性"**

Standard Switch: vSwitch1	Remove	Properties.	
Virtual Machine Port Group SPAN_monitoring	Physical Adapters	000 Full	P

- •选择端口组并单击"编辑"
- •转到"安全"**选项卡**,将"混杂模式"设置更改为"接受",如下图所示

0	SPAN_monitoring Properties	
0 es Resource Allocation Performance Configuration Task vSwitch1 Properties Ports Network Adapters Configuration Summary vSwitch 120 Ports SPAN_monitoring Virtual Machine Find the second s	SPAN_monitoring Properties	
Add Edit Remove	OK Cancel Help	

3.从"虚拟机设置"部分将两个虚拟机分配给端口组。

Sniffer VM - Virtual Machine Prope	rties	
Hardware Options Resources Profil	es vServices	Virtual Machine Version: 8
Show All Devices	Add Remove	Device Status Connected
Hardware	Summary	Connect at power on
 Memory CPUs Video card VMCI device SCSI controller 0 CD/DVD drive 1 Hard disk 1 Floppy drive 1 Network adapter 1 (edite 	1 Video card Restricted LSI Logic SAS [ISO] Windows/SW_D Virtual Disk Client Device SPAN_monitoring	Adapter Type Current adapter: E 1000 MAC Address 00:50:56:87:0c:57 @ Automatic C Manual DirectPath I/O Status: Not supported ()
		Network Connection Network label: SPAN_monitoring Port: N/A Switch to advanced settings
Help		OK Cancel

4.两个虚拟机必须立即显示在"网络"选项卡下的**端口**组中。

Standard Switch: vSwitch1	Remove Properties
 Virtual Machine Port Group SPAN_monitoring 2 virtual machine(s) VM with IP Sniffer VM 	Physical Adapters Physical Adapters wmnic1 10000 Full

在本示例中,具有IP的VM是具有IP地址的第二个VM,而嗅探器VM是具有嗅探器工具且没有IP地址 的VM。

5.这显示了6500交换机上的配置步骤:

```
CAT6K-01(config-mon-erspan-src)#source interface gil/1
CAT6K-01(config-mon-erspan-src)#destination
CAT6K-01(config-mon-erspan-src-dst)#ip address 192.0.2.3
CAT6K-01(config-mon-erspan-src-dst)#origin ip address 192.0.2.1
CAT6K-01(config-mon-erspan-src-dst)#erspan-id 1
CAT6K-01(config-mon-erspan-src-dst)#exit
CAT6K-01(config-mon-erspan-src)#no shut
CAT6K-01(config-mon-erspan-src)#end
在本例中,第二个VM(具有IP的VM)的IP地址为192.0.2.3。
```

通过此配置,6500封装捕获的数据包,并使用IP地址将其发送到虚拟机。VMWare vSwitch上的混 杂模式使嗅探器VM也能查看这些数据包。

故障场景

本节介绍在物理交换机上使用本地SPAN功能而不是ERSPAN功能时的常见故障场景。此拓扑在以 下位置考虑:



从PC A到PC B的流量使用本地SPAN功能进行监控。SPAN流量的目的地被定向到连接到UCS交换 矩阵互联(FI)的端口。

带有嗅探器工具的虚拟机在服务器1的UCS内运行。

以下是6500交换机上的配置:

CAT6K-01(config)#monitor session 1 source interface gigabitEthernet 1/1, gigabitEthernet 1/2 CAT6K-01(config)#monitor session 1 destination interface gigabitEthernet 1/3

端口Gig1/1和Gig1/2上流动的所有流量将复制到端口Gig1/3。UCS FI将不知道这些数据包的源和目的MAC地址。

在UCS以太网终端主机模式下,FI会丢弃这些未知单播数据包。

在UCS以太网交换模式下,FI在连接到6500(Eth1/1)的端口上学习源MAC地址,然后将下游的数据 包泛洪到服务器。此事件序列发生:

- 1. 为便于理解,请考虑接口Gig1/1和Gig1/2上仅PC A(使用mac-address aaaa.aaaa.aaaa)和 PC B(使用mac-address bbbb.bbbb.bbbbb))之间的流量
- 2. 第一个数据包从PC A到PC B,在UCS FI Eth1/1上可以看到
- 3. FI在Eth1/1上学习mac-address aaaa.aaaa.aaaa
- 4. FI不知道目的mac-address bbbb.bbbb.bbbb,并将数据包泛洪到同一VLAN中的所有端口
- 5. 嗅探器VM(位于同一VLAN中)也会看到此数据包
- 6. 下一个数据包从PC B到PC A
- 7. 当此命中Eth1/1时,将在Eth1/1上学习mac-address bbbb.bbbb.bbbb
- 8. 数据包的目的地为mac-address aaaa.aaaa.aaaa
- 9. FI会丢弃此数据包,因为Eth1/1上获取了mac-address aaaa.aaaa.aaaa,而Eth1/1本身也收到 了该数据包

验证

当前没有可用于此配置的验证过程。

故障排除

目前没有针对此配置的故障排除信息。

相关信息

- 在虚拟交换机或端口组上配置混杂模式
- Catalyst 6500上的SPAN、RSPAN和ERSPAN
- 使用开源工具解封ERSPAN流量
- <u>技术支持和文档 Cisco Systems</u>