將UCS刀鋒伺服器上的虛擬機器配置為SPAN目 標

目錄

簡介
必要條件
需求
採用元件
背景資訊
設定
網路圖表
使用IP位址的監聽器∨M
無IP位址的監聽器∨M
鼓障場景
驗證
疑難排解
相關資訊

簡介

本檔案介紹擷取完全在Cisco Unified Computing System(UCS)外部的流量並將之導向在UCS中執行 監聽器工具的虛擬機器(VM)的步驟。所捕獲流量的源和目標在UCS之外。捕獲可以在直接連線到 UCS的物理交換機上啟動,或者它可能離這裡幾跳遠。

必要條件

需求

思科建議您瞭解以下主題:

- UCS
- VMware ESX 4.1或更高版本
- 封裝遠端交換器連線埠分析器(ERSPAN)

採用元件

本文中的資訊係根據以下軟體和硬體版本:

- 執行12.2(18)ZYA3c的Cisco Catalyst 6503
- 運行2.2(3e)的Cisco UCS B系列
- VMWare ESXi 5.5內部版1331820

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除(預設))的組態來啟動。如果您的網路正在作用,請確保您已瞭解任何指令可能造成的影響。

背景資訊

UCS沒有遠端SPAN(RSPAN)功能來接收來自已連線交換器的SPAN流量並將其導向本地連線埠。 因此,在UCS環境中實現此目標的唯一方法是在物理交換機上使用封裝的RSPAN(ERSPAN)功能 ,並使用IP將捕獲的流量傳送到VM。在某些實現中,運行監聽器工具的VM不能具有IP地址。本檔 案將說明監聽器VM具有IP位址時所需的組態,以及沒有IP位址的情況。此處的唯一限制是監聽器 VM需要能夠從傳送到它的流量讀取GRE/ERSPAN封裝。



網路圖表

本檔案已考慮此拓撲:



連線到Catalyst 6500的GigabitEthernet1/1的PC正在受到監控。GigabitEthernet1/1上的流量會擷取 ,並傳送到伺服器1上在Cisco UCS中執行的監聽器VM。6500交換器上的ERSPAN功能會擷取流量 ,使用GRE將其封裝起來,然後傳送到監聽器VM的IP位址。

使用IP位址的監聽器VM

附註:本節所述的步驟也可用於監聽器在UCS刀鋒上的裸機伺服器中執行,而不是在VM上執

行的案例。

當監聽器VM可以具有IP地址時,需要執行以下步驟:

- 使用從6500可訪問的IP地址配置UCS環境中的監聽器VM
- 在VM內運行監聽器工具
- •在6500上設定ERSPAN來源作業階段,並將擷取的流量直接傳送到VM的IP位址

6500交換器上的設定步驟:

```
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,監聽器VM的IP地址為192.0.2.2
```

無IP位址的監聽器ⅤM

當監聽器VM不能具有IP地址時,需要執行以下步驟:

- 在UCS環境中配置監聽器VM
- 在VM內運行監聽器工具
- •建立可在同一主機中具有IP地址的第二台VM,並配置從6500可訪問的IP地址
- 將VMWare vSwitch上的埠組配置為混雜模式
- •在6500上設定ERSPAN來源作業階段,並將擷取的流量傳送到第二台VM的IP位址

以下步驟顯示了VMWare ESX上所需的配置:如果已配置埠組,請直接轉到步驟2。

1.建立虛擬機器埠組並將兩個虛擬機器分配給它

• 導覽至Networking索引標籤,然後按一下vSphere Standard Switch底下的Add Networking

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

View: vSphere Standard Switch vSphere Distributed Switch

Refresh Add Networking... Properties...

• 建立虛擬機器型別的埠組

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	

• 將物理介面(vmnic)分配給埠組,如下圖所示。

Add Network Wizard	and a second designed in the local division of the local divisione	-	- Art - North Street Mark	
Virtual Machines - Netwo 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 l	affic for this connection. You may also disted 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 Emulex Corporation OneConnect 10	Speed OGb NIC (be3)	Networks	
	m ic0	10000 Full	10.76.78.22-10.76.78.22	
	Preview:			
	Preview:	Physical Adapters		
		_		
Help			< Back Next >	Cancel

• 設定連線埠組的名稱,並新增相關VLAN,如下圖所示。

2 Add Network Wizard		A COLUMN TWO IS NOT	Accelerate	
Virtual Machines - Connec Use network labels to ide	tion Settings ntify 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) Physical Adapters Physical Adapters vmnic1		
Help			< Back	Next > Cancel

•驗證組態並按一下Finish,如下圖所示。

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.將埠組配置為混雜模式,如下圖所示。

- port-group現在必須出現在Networking頁籤下
- 按一下Properties

Standard Switch: vSwitch1	Remo	ove Properties	
SPAN_monitoring	Physical Adapte	ic1 10000 Full 🖓	

- 選擇埠組並按一下Edit
- •前往**Security**索引標籤,將「Promiscuous」模式設定變更為「Accept」,如下圖所示

0 en Recourse Allocation Performance, Configuration, Task	SPAN_monitoring Properties
es Resource Allocation Performance Configuration Task es Sutich1 Properties Ports Network Adapters Configuration Summary Provember 200 Ports vSwitch 120 Ports Provember 200 Ports S SPAN_monitoring Virtual Machine Fall S Add Edit	General Security Traffic Shaping NIC Teaming Policy Exceptions Promiscuous Mode: Image: Accept Image: Accept MAC Address Changes: Image: Accept Image: Accept Image: Accept Forged Transmits: Image: Accept Image: Accept Image: Accept Image: Accept Image: Accept
	OK Cancel Help

3.從「虛擬機器設定」部分將兩個虛擬機器分配給埠組。

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.這兩個虛擬機器現在必須出現在網路頁籤下的埠組中。

Standard Switch: vSwitch1	Remove Properties
 ✓ Virtual Machine Port Group SPAN_monitoring 2 virtual machine(s) VM with IP Sniffer VM 	Physical Adapters vmnic1 10000 Full

在本示例中,具有IP的VM是具有IP地址的第二個VM,而監聽器VM是具有沒有IP地址的監聽器工具 的VM。

5.這顯示了6500交換器上的設定步驟:

```
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
在本示例中,第二台虛擬機器(具有IP的虛擬機器)的IP地址為192.0.2.3。
```

透過此設定,6500會封裝擷取封包,並使用IP位址傳送封包給虛擬機器。VMWare vSwitch上的混 雜模式使監聽器VM也能看到這些資料包。

故障場景

本節介紹在實體交換器上使用本地SPAN功能(而不是ERSPAN功能)時的常見故障情況。此處考 慮此拓撲:



使用本地SPAN功能監控從PC A到PC B的流量。SPAN流量的目的地會導向連線到UCS光纖互連 (FI)的連線埠。

具有監聽器工具的虛擬機器在伺服器1上的UCS內運行。

以下是6500交換器上的組態:

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 所有在埠Gig1/1和Gig1/2上流動的流量都會複製到埠Gig1/3。UCS FI不知道這些資料包的源和目標 mac地址。

在UCS乙太網終端主機模式下,FI會丟棄這些未知的單點傳播資料包。

在UCS乙太網交換模式下,FI會獲取連線到6500(Eth1/1)的埠的源MAC地址,然後將資料包向下游 泛洪到伺服器。發生以下事件:

- 為便於理解,請考慮介面Gig1/1和Gig1/2上僅在PCA(具有mac地址aaaa.aaaa.aaaa)和PC B(具有mac地址bbb.bbb.bbb)之間傳輸的流量
- 2. 第一個資料包是從PC A到PC B的,這在UCS FI Eth1/1上可見
- 3. FI會學習Eth1/1上的mac-address aaaa.aaaa.aaaa
- 4. FI不知道目的地mac-address bbb.bbb.bbb,並將封包湧向同一VLAN中的所有連線埠
- 5. 位於同一VLAN中的監聽器VM也會看到此封包
- 6. 下一個資料包從PC B傳送到PC A
- 7. 當這命中Eth1/1時,會在Eth1/1上獲知mac-address bbb.bbb.bbb
- 8. 封包的目的地為mac-address aaaaa.aaaa.aaaa
- 9. 在Eth1/1上獲取mac-address aaaa.aaaa.aaaa且在Eth1/1上接收資料包時,FI會丟棄此資料包
- 10. 由於相同原因,後續資料包被丟棄,這些資料包的目的地為mac-address aaaa.aaaa.aaaa或 mac-address bbb.bbb.bbb

驗證

目前沒有適用於此組態的驗證程序。

疑難排解

目前尚無適用於此組態的具體疑難排解資訊。

相關資訊

- 在虛擬交換機或埠組上配置混雜模式
- Catalyst 6500上的SPAN、RSPAN和ERSPAN
- 使用開源工具解除封裝ERSPAN流量
- 技術支援與文件 Cisco Systems