UCSブレードサーバ上の仮想マシンをSPAN宛 先として設定する

内容

 概要

 前提条件

 要件

 使用するコンポーネント

 背景説明

 設定

 ネットワーク図

 IPアドレスを持つスニファVM

 PアドレスのないスニファVM

 障害シナリオ

 確認

 トラブルシュート

 関連情報

概要

このドキュメントでは、Cisco Unified Computing System(UCS)の外部にあるトラフィックフロー をキャプチャし、UCS内でスニファツールを実行する仮想マシン(VM)に転送する手順について説 明します。キャプチャされるトラフィックの送信元と宛先はUCSの外部です。キャプチャは、 UCSに直接接続されている物理スイッチで開始することも、数ホップ離れた場所で開始すること もできます。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- UCS
- VMware ESXバージョン4.1以降
- Encapsulated Remote Switch Port Analyzer(ERSPAN)

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- 12.2(18)ZYA3cを実行するCisco Catalyst 6503
- 2.2(3e)を実行するCisco UCS Bシリーズ
- VMWare ESXi 5.5ビルド1331820

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド キュメントで使用するすべてのデバイスは、初期(デフォルト)設定の状態から起動しています 。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的 な影響について確実に理解しておく必要があります。

背景説明

UCSには、接続されたスイッチからSPANトラフィックを受信し、ローカルポートに送信するリ モートSPAN(RSPAN)機能はありません。UCS環境でこれを実現する唯一の方法は、物理スイッ チでEncapsulated RSPAN(ERSPAN)機能を使用し、IPを使用してキャプチャされたトラフィック をVMに送信することです。特定の実装では、スニファツールを実行しているVMにIPアドレスを 割り当てることはできません。このドキュメントでは、スニファVMにIPアドレスがある場合に必 要な設定と、IPアドレスのないシナリオについて説明します。ここでの唯一の制限は、スニファ VMが送信されたトラフィックからGRE/ERSPANカプセル化を読み取れる必要があることです。

設定

ネットワーク図

このドキュメントでは、次のトポロジを考慮しています。



Catalyst 6500のGigabitEthernet1/1に接続されているPCがモニタされています。

GigabitEthernet1/1のトラフィックがキャプチャされ、サーバ1のCisco UCS内で稼働するスニファVMに送信されます。6500スイッチのERSPAN機能は、トラフィックをキャプチャし、GREを使用してカプセル化し、スニファVMののIPアドレスにに送信します。

IPアドレスを持つスニファVM

注:このセクションで説明する手順は、VM上で実行するのではなく、UCSブレード上のベ アメタルサーバでスニファが実行されるシナリオでも使用できます。

スニファVMにIPアドレスを設定できる場合、次の手順が必要です。

- ・UCS環境内のスニファVMに、6500から到達可能なIPアドレスを設定します
- VM内でスニファツールを実行します
- 6500でERSPAN送信元セッションを設定し、キャプチャされたトラフィックをVMのIPアドレスに直接送信します

6500スイッチの設定手順:

```
CAT6K-01(config)#monitor session 1 type erspan-source
```

- CAT6K-01(config-mon-erspan-src)#source interface gi1/1
- 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
- この例では、スニファVMのIPアドレスは192.0.2.2です

IPアドレスのないスニファVM

スニファVMにIPアドレスを設定できない場合、次の手順が必要です。

- UCS環境内のスニファVMの設定
- VM内でスニファツールを実行します
- ・同じホストにIPアドレスを持つことができる2番目のVMを作成し、6500から到達可能なIPアドレスを使用して設定します
- VMWare vSwitchのポートグループを混合モードに設定します
- 6500でERSPAN送信元セッションを設定し、キャプチャされたトラフィックを2番目のVMの IPアドレスに送信します

次の手順は、VMWare ESXで必要な設定を示しています。ポートグループがすでに設定されてい る場合は、ステップ2に直接進みます。

1.仮想マシンポートグループを作成し、2つの仮想マシンをそれに割り当てます

• [Networking]タブに移動し、[vSphere Standard Switch]の下の[Add Networking]をクリックします

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

Networking

・タイプが仮想マシ	ンのポートグループを作成します
Add Network Wizard	
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. ✓ VMkernel The VMkernel TCP/IP stack handles traffic for the following ESXI services: vSphere vMotion, ISCSI, NFS, and host management.
Help	< Back Next > Cancel

•次の図に示すように、物理インターフェイス(vmnic)をポートグループに割り当てます。

work Access h networks through uplink adapters attached to vSphe	ere standard swi	tches.	
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 isted below.	create a new
Create a vSphere standard switch	Speed	Networks	
Emulex Corporation OneConnect 10	Gb NIC (be3)		
Vmnic1	10000 Full	10.76.78.22-10.76.78.22	
O Use vSwitch0	Speed	Networks	
Emulex Corporation OneConnect 10	Gb NIC (be3)	10 76 70 00 10 76 70 00	
i vinneo	10000 Full	10.76.78.22-10.76.76.22	
Preview:			
Virtual Machine Port Group VM Network 2	Physical Adapters		
			_
	work Access h networks through uplink adapters attached to vSphere Select which vSphere standard switch will handle vSphere standard switch using the undaimed ne Create a vSphere standard switch Emulex Corporation OneConnect 10 W wmic1 Use vSwitch0 Emulex Corporation OneConnect 10 Wetwork 2 	work Access h networks through uplink adapters attached to vSphere standard switch Select which vSphere standard switch using the unclaimed network adapters of vSphere standard switch using the unclaimed network adapters of the unclaimed network a	work Access h networks through uplink adapters attached to vSphere standard switches. Select which vSphere standard switch will handle the network traffic for this connection. You may also vSphere standard switch using the unclaimed network adapters listed below. Create a vSphere standard switch Speed Networks Emulex Corporation OneConnect 10Gb NIC (be3) wmic1 10000 Full 10.76.78.22-10.76.78.22 Use vSwitch0 Speed Networks Emulex Corporation OneConnect 10Gb NIC (be3) wmic0 10000 Full 10.76.78.22-10.76.78.22 Preview: Virtual Machine Port Group VI Network 2 Physical Adapters

• 図に示すように、ポートグループの名前を設定し、関連するVLANを追加します。

Add Network Wizard		A CONTRACTOR OF THE OWNER	Acres in the	
Virtual Machines - Conne Use network labels to id	ction Settings entify migration compatible connecti	ions 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

・設定を確認し、図に示すように[Finish]をクリックします。

2 Add Network Wizard	and the second s	
Ready to Complete Verify that all new and m	odified 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.図に示すように、ポートグループを無差別モードに設定します。

・ポートグループは、[Networking]タブの下に表示される必要があります

• [プロパティ]をクリックします

Standard Switch: vSwitch1		Remove.	Pro	pertie	s
SPAN_monitoring	Physical	Adapters - vmnic1	10000	Full	P

- ・ポートグループを選択し、[Edit]をクリックします
- 次の図に示すように、[**Security**]タブに移動し、[Promiscuous mode]の設定を[Accept]に変更 します

0	SPAN_monitoring Properties
res Resource Allocation Performance Configuration Task Image: Configuration Summary Provide the second sec	SPAN_monitoring Properties
Add Edit Remove	OK Cancel Help

3.2台の仮想マシンを、仮想マシン設定セクションからポートグループに割り当てます。

Sniffer VM - Virtual Machine Prope	rties	
Hardware Options Resources Profile	es vServices	Virtual Machine Version: 8
Show All Devices	Add Remove	Device Status Connected
Hardware	Summary	Connect at power on
Hardware Memory CPUs Video card VMCI device SCSI controller 0 CD/DVD drive 1 Hard disk 1 Floppy drive 1 Network adapter 1 (edite	Summary 1024 MB 1 Video card Restricted LSI Logic SAS [ISO] Windows/SW_D Virtual Disk Client Device SPAN_monitoring	Adapter Type Current adapter: E1000 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

4.2台の仮想マシンがポートグループのNetworkingタブに表示されます。

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

この例では、IPアドレスを持つ2番目のVMがIPを持つVMであり、Sniffer VMはIPアドレスを持た ないスニファツールを持つVMです。

5.6500スイッチの設定手順を次に示します。

```
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
この例では、2番目のVM(IPを持つVM)のIPアドレスは192.0.2.3です。
```

この設定では、6500はキャプチャされたパケットをカプセル化し、IPアドレスを持つVMに送信 します。VMWare vSwitchの混合モードでは、スニファVMがこれらのパケットも表示できます。

障害シナリオ

この項では、ERSPAN機能の代わりに物理スイッチでローカルSPAN機能を使用する場合の一般 的な障害シナリオについて説明します。次のトポロジが考慮されます。



PC AからPC Bへのトラフィックは、ローカルSPAN機能を使用してモニタされます。SPANトラ フィックの宛先は、UCSファブリックインターコネクト(FI)に接続されたポートに向けられます 。

スニファツールを備えた仮想マシンは、サーバ1のUCS内で動作します。

6500スイッチの設定を次に示します。

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 ポートGig1/1およびGig1/2を流れるすべてのトラフィックは、ポートGig1/3に複製されます。こ れらのパケットの送信元と宛先のMACアドレスは、UCS FIでは認識されません。 UCSイーサネットエンドホストモードでは、FIがこれらの不明なユニキャストパケットをドロッ プします。

UCSイーサネットスイッチングモードでは、FIは6500(Eth1/1)に接続されたポートの送信元 MACアドレスを学習し、ダウンストリームのパケットをサーバにフラッディングします。次の一 連のイベントが発生します。

- 1. 理解しやすいように、PC A(mac-address aaaa.aaaa.aaaa)とPC B(mac-address bbbb.bbbb.bbbb)の間(Gig1/1とGig1/2のインターフェイス)でのみ行われるトラフィック を検討します
- 2. 最初のパケットはPC AからPC Bに送信され、これはUCS FI Eth1/1に表示されます
- 3. FlはEth1/1でmac-address aaaa.aaaa.aaaaを学習します
- 5. 同じVLAN内のスニファVMにも、このパケットが表示されます
- 6. 次のパケットはPC BからPC Aです
- 7. これがEth1/1にヒットすると、mac-address bbbb.bbbb.bbbbがEth1/1で学習されます
- 8. パケットの宛先はmac-address aaaa.aaaa.aaaaです
- 9. FIは、Eth1/1でmac-address aaaa.aaaa.aaaaが学習され、パケットがEth1/1自体で受信され たとして、このパケットをドロップします
- 10. mac-address aaaa.aaaa.aaaaまたはmac-address bbbb.bbbb.bbbbb宛ての後続のパケットも、同じ理由で廃棄されます

確認

現在、この設定に使用できる確認手順はありません。

トラブルシュート

現在、この設定に関する特定のトラブルシューティング情報はありません。

関連情報

- ・仮想スイッチまたはポートグループでの無差別モードの設定
- <u>Catalyst 6500でのSPAN、RSPAN、およびERSPAN</u>
- オープンソースツールによるERSPANトラフィックのカプセル化解除
- <u>テクニカル サポートとドキュメント Cisco Systems</u>