

Sangfor Configuration Guide VMware vSTA 3.0.25c virtual device port mirroring Configuration Guide

Product VersionvSTA 3.0.25cDocument Version01Released onMar. 09, 2021





Change Log

Date	Change Description
26 - 5 -2021	Initial Release

About this Configuration guide

This Guide will assist to configure the vmware port mirroring configuration from vmware virtual switch and physical switch to vmware vSTA

CONTENTS

Change Log	i
About this Style Guide	ii
1 Document Formatting	1
1.1 Document File Name	1
1.2 Product Version	1
1.3 Fonts	1
1.3.1 Pre-Created Styles	3
1.3.2 Lists	4
1.3.3 Tables	5
1.3.4 lcons	5
1.3.5 Screenshots	6
1.4 Locale Conventions	8
1.4.1 Date and Time	8
1.4.2 Phone Numbers	8
1.4.3 Other Formatting Rules	9
1.4.4 Links and URLs	11
1.4.5 Describing Interactions with UI Elements	11
2 Grammar	
2.1 Spelling	13
2.1.1 Checking for Spelling	13
2.2 Capitalization	14
2.2.1 Headline-Style Capitalization	14
2.2.2 Sentence-Style Capitalization	15
2.2.3 Other Capitalization Rules	15
2.3 Punctuation and Symbols	16

2.3.1 Ending Punctuation	16
2.3.2 List of Symbols and Punctuation	16
2.3.3 Unacceptable Punctuation	19
2.4 Articles (A/An/The)	19
2.5 Word Usage	20
2.5.1 Acronyms	20
2.6 Sangfor Product Names	22
2.7 Sangfor Department and Position Names	23
2.8 Word List	25
3 Writing Style	
3.1 Imperative Voice	32
3.1.1 Imperative Voice	32
4 Proofing Tips	

1 Application Scenario

User has deployed the vmware vSTA in the environment, follow guide will show the configuration of the vmware to mirror the traffic from physical switch to vmware or mirror the VM traffic in between VM.



1. PC2_server is used as the server, vcenter is installed in VMware, and the configuration is operated in Vsphere client

First, right-click the virtual machine, edit the configuration, and configure 2 network adapters for PC2_server:

VM Network —— configure IP 200.200 network segment as the management port;

dvPortGroup2——Configure other network segments, such as 2.2.2.1, dedicated to communication between 2 PCs,

Remember here that network adapter 2 automatically assigns port 32

n	6	PC2_server - Virtual Machine I	Properties		_		×
ir	Har	dware Options Resources vServ	vices		Virtual Mad	hine Versi	on: 8
g		Show All Devices	Add Remove	Device Status			
ar	Ha	rdware	Summary	Connect at power on			
na s na in g:		Memory CPUs Video card VMCI device SCSI controller 0 CD/DVD drive 1 Hard disk 1 Floppy drive 1 Network adapter 1 Network adapter 2	4096 MB 2 Video card Deprecated LSI Logic Parallel Client Device Virtual Disk Client Device VM Network dvPortGroup (dvSwitch	Adapter Type Current adapter: E MAC Address 00:50:56:81:0d:3c C Automatic C M DirectPath I/O Status: N Network Connection Network label: dvPortGroup (dvSwitch3) Port 32	1000E Ianual Iot supported () Switch to ad	vanced se	▼. ttings
					OK	Canc	el

2. PC1_client, as a client

Same as above configuration

ן 🕜 PC1_client · Virtual Machine P	roperties	- 🗆 X
Hardware Options Resources vSer	vices	Virtual Machine Version: 11 🥼
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 Hard disk 2 Floppy drive 1 Network adapter 1 Network adapter 2	Summary 8192 MB 8 Video card Deprecated LSI Logic Parallel [] /vmfs/volumes/5e73 Virtual Disk Virtual Disk Client Device VM Network dvPortGroup (dvSwitch	Adapter Type Current adapter: VMXNET 3 MAC Address 00:50:56:81:5f:b1 Automatic Manual DirectPath I/O Status: Inactive To activate DirectPath I/O, go to the Resources tab and select Memory Settings to reserve all guest memory. Network Connection Network label: dvPortGroup (dvSwitch3) Port: 33 Switch to advanced settings
		OK Cancel

Network adapter 2, configured as 2.2.2.2

The automatically assigned port is 33

device · Virtual Machine Prope	erties	- 🗆 X
Hardware Options Resources vServ	ices	Virtual Machine Version: 8
Show All Devices	Add Remove	Device Status
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 Network adapter 2	8192 MB 4 Video card Deprecated LSI Logic Parallel [] /vmfs/volumes/5863f Virtual Disk Client Device VM Network dvPortGroup (dvSwitch	Adapter Type Current adapter: VMXNET 3 MAC Address 00:50:56:81:40:2d Automatic Manual DirectPath I/O Status: Inactive To activate DirectPath I/O, go to the Resources tab and select Memory Settings to reserve all guest memory. Network Connection Network label: dvPortGroup (dvSwitch3) Port: 34 Switch to advanced settings
		OK Cancel

3.Latent threat perception device



Same as above, configure 2 network adapters, one as a management port, (200.200 network segment)

One used to mirror the traffic of PC1 PC2 communication

The port here is 34



3. Network adapter mirror configuration



Host and cluster switch to network, find the corresponding virtual switch (the virtual switch we configured above is dvSwitch3) enter the configuration options



4. Add a new port mirroring

JU 🕜 dvSwitch3 Settings	×
Fig Properties Network Adapters Private VLAN NetFlow CSW Session Name Status CU C C C C C C C C C C C C C C C C C C	Port Mirroring Port Mirroring Session Details Port Mirroring Session Status: Description: Port Mirroring Session Details Alloweersel 10 or destination parts
ta lin hrd nig rib	Allow normal IO on destination ports: Encapsulation VLAN: Preserve original VLAN: Mirrored packet length: Port Mirroring Session Sources Port Mirroring Session Destinations
rit Add Edit Delete	OK Cancel

Create Port Mirroring Ses	ssion			×
General Properties Specify a name and the p	properties of the port mirroring s	ession		
General Properties Specify Sources Specify Destinations Ready to Complete	General Name: Description:	ltets		
	Port Mirroring Session D Allow normal IO on Encapsulation VLAN 1 Mirrored packet len 60	Details		
Help			< Back Next >	Cancel

5. Specify the source port and destination port

	Create Port Mirroring Ses	sion					×
ł	Specify Sources Select the source ports of	the port mirroring session	1				
1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	General Properties Specify Sources Specify Destinations Ready to Complete	Traffic direction: Port IDs (e.g. 1-4. 32-33	Ingress/Egress 5, 10-21)	•	Name Port	Туре	
	Help	1			< Back	Next >	Cancel

Next step

Create Port Mirroring Session Specify Destinations Select the destination ports a	n nd uplinks of the port mirr	roring session				×
General Properties Specify Sources Specify Destinations Ready to Complete	Destination type: Port IDs (e.g. 1-4, 5, 1	ort 💌	>>> <<	Name Port Uplink		
Help				< Back	Next >	Cancel

Next step

🕜 Create Port Mirroring Se	ssion				×
Ready to Complete					
Verify the settings for the	e new port mirroring session. Then, select the check bo	x to enable this port m	irroring session.		
	_				
General Properties					
Specify Sources	Enable this port mirroring session				
Specify Destinations	Name:	test			
Ready to Complete	Preserve original VLAN:	Yes			
	Allow normal IO on destination ports:	No			
	Number of port mirroring session sources:	2			
	Number of port mirroring session destinations:	1			
	1				
I					1
1			1		1
Help			< Back	Finish	Cancel

6. Finish

		Port Mirroring Session Details		
Session Name	Status	· ·		
test	Disabled	test	Disabled	
		Status:	Disabled	
		Post Mirroring Cossion Datails	-	
		Allow pormal IO on destination ports:	No	
		Encansulation VI AN:		
		Preserve original VLAN:	Yes	
		Mirrored packet length:		
		Port Mirroring Session Sources		
		Port ID: 32	Ingress/Egress	
		Port ID: 33	Ingress/Egress	
		Port Mirroring Session Destinations	5	
		Port ID: 34		
	t Delete			
Add Ed	t Delete			

Chapter 3 Mirroring traffic mode of physical switches

1. Topology



2. Operation steps

Create a virtual switch and bind physical network ports

localhost.localdomain VMware ESXI, 6.0	0,2494585				
Getting Started Summary Virtual Machi	nes, Resource Allocation, Performance, Configuration, Users, Events, Permissions,				~
Hardware	View: vSphere Standard Switch vSphere Distributed Switch				- 1
Health Status	Networking	Refresh Ad	id Networking	Properties	
Processors					
Memory	VuAN2 VeAN2 Veral No adapters				^
Networking	win703 lo.2.123.224 a				
ourage weapters	win702_10.222.123.222 🗿				
Network Adapters					
Advanced Settings	Standard Switch: vSwitch3 Remove Properties				
Power Management	Wrual Machine Port Group Physical Adapters				
Software	VM Network 6 Det Noadapters				
Licensed Features	⇒ 1 virtue machine(s) machine 13 148				
Time Configuration	- Vena Marine Pers Graza				
DNS and Routing	VM Network 5 👲 +				
Authentication Services	Visual Machine Part Group				
Virtual Machine Swapfile Location	1 ivital machine(s)				
Security Profile	NovaSensor 🔁				
Host Cache Configuration					
System Resource Reservation	Standard Switch: vSwitch4 Remove Properties				

Select the type of virtual machine, the next step

🕜 Add Network Wizard	- 0	×
Connection Type Networking hardware c	an 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.	
	< Back Next > Ca	ncel

Select the bound physical network port, the bound physical network port must be the network port that diverts traffic from the physical switch

Add Network Wizard	1			_)		
Virtual Machines - Net Virtual machines read	work Access ch networks through uplink adapters attached to vSph	ere standard :	switches.					
Connection Type Network Access	Select which vSphere standard switch will handle vSphere standard switch using the undaimed ne	e the network twork adapte	traffic for this connection. Yo rs listed below.	u may also crea	ite a new			
Connection Settings	• Create a vSphere standard switch	Speed	Networks					
summary	Intel Corporation 82599EB 10-Giga	bit SFI/SFP	+ Network Connection					
	Vmnic1	Down	None					
	vmnic2	Down	None					
	Intel Corporation I350 Gigabit Netv	work Conne	ction					
	vmnic3	Down	None					
	vmnic4	Down	None					
	🖂 🔛 vmnic7	Down	None					
		Sneed	Networks					
		opeeu	Networks					
	Preview:							
	Virtual Machine Port Group	-Physical Adapte	int .					
		- • • • • • • • • • • •						
	1		15			_		
			< Back	Next >	Can	col		

Name the port group, this port group receives the traffic from the physical switch

1	🕜 Add Network Wizard				_		×
	Virtual Machines - Conn Use network labels to id	ection Settings dentify migration compatible connect	ions common to two or more hosts.				
h		, , , ,					
4	Connection Type Network Access	Port Group Properties					
	Connection Settings	Network Label:	mirrorflow				
4	Summary	VLAN ID (Optional):	None (0)	•			
F			,				
6							
ŝ		Preview:					
F		-Virtual Machine Port Group	- Physical Adapters				
1		mirrorflow	Vmnic1				
Ŋ							
4							
F							
Ř							
1							
1							
đ							
f	1	,					1
4				< Back	Next >	Can	cel
į,							
c	······	المستشفية والمستشرك					
2	ouccessfully created	a a virtual switch					

The physical network port of the demo environment is not actually connected, so the connection status is failed. After the actual connection, it will show that the connection is normal.

 Initiated by
 Requested Start Time
 Completed Time

 root
 2021/5/20 17:11:21
 2021/5/20 17:11:21
 2021/5/20 17:11:21

Name Target Status

calhost.localdomain VMware ESXi, 6	.0.0, 2494585	
Setting Started Summary Virtual Ma	chines Resource Allocation Performance	Configuration Users Events Permissions
Processors Memory Storage Networking Storage Adapters Network Adapters Advanced Settings Power Management	VLAN ID: All (4095) Standard Switch: vSwitch40 Virtual Machine Port Group ULAN ID: All (4095) VLAN ID: All (4095)	Remove Properties
Licensed Features Time Configuration DNS and Routing Authentication Services Virtual Machine Startup/Shutdown Virtual Machine Swapfile Location Security Profile Host Cache Configuration	Standard Switch: vSwitch41 Virtual Machine Port Group wgs 日 4 virtual machine(s) VLAN ID: A server2016 poc_tsa kali 遠口扫描 WAF1.0_10.254.254.254	Remove Properties Physical Adapters No adapters III (4095)
System Resource Reservation Agent VM Settings	Standard Switch: vSwitch42	Remove Properties
Advanced Settings	Virtual Machine Port Group poc 2 virtual machine(s) poc_tsa POC_WIN7	Physical Adapters No adapters
	Standard Switch: vSwitch43	Remove Properties
	Virtual Machine Port Group	-Physical Adapters
	Standard Switch: vSwitch11	Remove Properties

The configured port group name is mirrorflow. Just add this label to the mirror network port of the detection device to complete the configuration.



The mirrored traffic is drained, and the mirrored traffic from the external physical switch can be received by turning on the device

Two, VMwareweb application side configuration mirroring method

Note: The console operation of the VMware web application can only support the flow diversion method of the external entity switch, and there is no way to configure the virtual switch diversion method.



1. Topological diagram (same as the method in the previous section)

2. Operation steps

The newly created virtual machine is bound to the network card that actually accesses the physical switch traffic

/m ware ⁻ ESXi ⁻				root@10.222.88.52 - Help +
T Navigator n	Q localhost.localdomain - Networking			
 Host Manage 	Port groups Virtual switches Frysical NICs VMkernel NICs	TCP/IP stacks Firewall rules		
Monitor	📥 Add standard virtual switch 📲 Add uplink: 🥖 Edit settings 🕴 C Ref	resh 🛛 🔅 Actions		
- Virtual Machines 8	wame	Port groups	 Uplinks 	 Туре
▼ 前 10.222.3.85(server20	📾 vSwitch0			Standard vSwitch
Monitor	m 69SPT			Standard vSwitch
 iiii 10.222.3.85(vcenter) 	a 24SPT	- Add standard vidual switch mi	· · · · · · · · · · · · · · · · · · ·	Standard vSwitch
 3.0.57iso 	a 34SPT	and Add standard virtual switch - In	iois	Standard vSwitch
▶ □ 10.222.88.21	III 稳定型流量	🙇 Add uplink		Standard vSwitch
H Storage	▲ 将来图放	vSwitch Name	mirrors	Standard vSwitch
database1		MTU	1500	
Monitor		the first of		
More storage		Opank 1	vmnic0 - Down v	
> m vSwitch0		* Link discovery		
 ・ ・ ・		Mode	Listen ~	
		Protocol	Cisco discovery protocol (CDP)	
		- Security		
		Promiscuous mode	● Accept O Reject	
		MAC address changes	O Accept S Reject	
		Forged transmits	O Accept Reject	
			Add Cancel	
	E Recent tasks			
			 Queued Started 	 Result

Add port group



Created

🧕 Add port group 🅜 Edit settings 🕴 🥑 Refr	esh 🚯 Actions					Q Search
Name	~	Active ports ~	VLAN ID ~	Type ~	vSwitch ~	VMs
g mirrorflow		0	0	Standard port group	m vSwitch0	N/A
VM NOWNER		/	0	Standard port group	AND A PARTY AND A	0
Management Network		1	0	Standard port group	cm vSwitch0	N/A
G 69flow		0	0	Standard port group	69SPT	0
Q 2410W		2	0	Standard port group	a 24SPT	3
34flow		0	0	Standard port group	a 34SPT	0
2 900Mflow		2	0	Standard port group	·····································	2
e kell_replay		0	0	Standard port group	am 科莱园放	0

Select the corresponding port group label for the mirrored network port of the virtual detection device

10.222.88.21						
😴 Console 🔤 Monitor 📔	Power on E Shut down II Suspen	nd 🖸 Restart 🛛 🖉 Edit 🗍 📢 Re	fresh 🏟 Actions			
Goddi Lhom 2 (Gord) werd 3 (B. & H17) 19 Jul7) 48 Jul en en 48 Jul Godhard Ingue	10.222.88 Guest OS Compatibi VMware Tr CPUs Memory Hort nome	CentOS 7 (Inty ESXI 7.0 vi pools Yes 8 8 GB b combert lo	94-bit) tual machine			
	li di	Edit settings - 10.222.88.21 (ESXi)	7.0 virtual machine)		_	
		→ → Hard disk 2	1024 GB ~		0	
	d	SCSI Controller 0	VMware Paravirtual			
		SATA Controller 0			0	
A The configured guest O	S (CentOS 7 (64-bit)) for this virtual i	USB controller 1		~	0	allow for guest-specific optimizations. 🖨 Actions
General Information		INN Network Adapter 1	VM Network	Connect	0	
🗝 🧕 Networking		Network Adapter 2	000145000	Connect	0	Is
Host name	localhost.localdomain		24flow	Connect	0	
IP addresses	1. 10.251.251.251	Network Adapter 3	34flow	Connect	0	
	2. 10.222.88.21 3. fe80::20c:29ff:fec8:b642	▶ (a) CD/DVD Drive 1	900Mflow	Connect	۲	3B 0
> 📾 VMware Tools	VMware Tools is not managed	• I Video Card	mirrorflow			work (Connected)
I Storage	2 disks					w (Connected)
Notes			Hereomgarou		0	(Connected)
- Performance summary la	st hour			Save	Cancel	atabase1] 3.0.27CISO/STA-3.0.27.iso
🗈 Recent tasks						
Task	 Target 		tiator ~ Queued	~ Started		✓ Result ▲

Click Save, and the flow is completed after completion, and the detection device can receive the mirrored traffic from the physical switch at this time



