Configuration de VLAN privé et UCS avec VMware DVS ou Cisco Nexus 1000v

Contenu

Introduction Conditions préalables **Conditions requises Components Used** Informations générales Configuration Diagramme du réseau UCS avec VMware DVS **VMware DVS** Commutateur N5k ascendant Changement de comportement avec UCS version 3.1(3) Commutateur en amont 4900 Vérification Dépannage Configuration avec Nexus 1000v avec port de promiscuité en amont N5k **Configuration UCS Configuration N1k** Configuration avec Nexus 1000v avec port de promiscuité sur le profil de port de liaison ascendante N1K **Configuration UCS** Configuration des périphériques en amont Configuration de N1K

Introduction

Ce document décrit la prise en charge des VLAN privés (PVLAN) pour Cisco Unified Computing System (UCS) dans la version 2.2(2c) et les versions ultérieures.

Attention : Il y a un changement de comportement à partir de la version 3.1(3a) du micrologiciel UCS, comme décrit dans la section Changement de comportement avec UCS version 3.1(3) et ultérieure.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- UCS
- Commutateur virtuel distribué (DVS) Cisco Nexus 1000V (N1K) ou VMware
- VMware
- Commutation de couche 2 (L2)

Components Used

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Informations générales

Un VLAN privé est un VLAN configuré pour l'isolation de couche 2 par rapport aux autres ports du même VLAN privé. Les ports qui appartiennent à un PVLAN sont associés à un ensemble commun de VLAN de support, qui sont utilisés pour créer la structure PVLAN.

II y a trois types de ports PVLAN :

- Un port proche communique avec tous les autres ports PVLAN et est le port utilisé pour communiquer avec des périphériques situés en dehors du PVLAN.
- Un port isolé a une séparation L2 complète (qui inclut les diffusions) des autres ports du même PVLAN, à l'exception du port proche.
- Un port de communauté peut communiquer avec d'autres ports du même PVLAN ainsi qu'avec le port proche. Les ports communautaires sont isolés au niveau de L2 à partir de ports d'autres communautés ou de ports PVLAN isolés. Les diffusions ne sont propagées qu'à d'autres ports de la communauté et du port proche.

Référez-vous à <u>RFC 5517</u>, <u>VLAN privés de Cisco Systems : Sécurité évolutive dans un</u> <u>environnement multiclient</u> afin de comprendre la théorie, le fonctionnement et les concepts des PVLAN.

Configuration

Diagramme du réseau

Avec Nexus 1000v ou VMware DVS



Note: Cet exemple utilise le VLAN 1750 comme principal, 1785 comme isolé et 1786 comme VLAN de communauté.

UCS avec VMware DVS

1. Afin de créer le VLAN principal, cliquez sur la case d'option **Principal** en tant que Type de partage, et entrez un **ID** de **VLAN** de 1750 comme indiqué dans l'image.

Propertie	5							
	Name:	1750			VLA	N ID: 1750		
	Native VLAN:	No			Fabri	Fabric ID: Dual		
	Network Type:	Lan			IfT	If Type: Virtual		
	Locale:	External		Transport T	ype: Ether			
	Owner:	Local						
Multica	st Policy Name:	<not set=""></not>	•		+ Create	Multicast Policy		
Multicast F	Policy Instance:	org-root/mc-pol	icy-default					
	Sharing Type:	O None O F	Primary 🔿 Isola	ted 🔿 Comr	nunity			
		0	, 0					
Secondar	v VI ANs							
🔍 Filter 🛋	Export 🗞 Prin	nt						
Name	ID	Туре	Transport	Native	VLAN Sharing	Multicast Poli 🛱		
1785	1785	Lan	Ether	No	Isolated	^		
1786	1786	Lan	Ether	No	Community			
						~		
1								

2. Créez des VLAN **isolés** et **communautaires** en conséquence, comme indiqué dans les images. Aucun de ces VLAN ne doit être un VLAN natif.

Properties	
Name: 1795	VI AN TO: 1795
Name: 1785	VLAN ID: 1785
Native VLAN: No	Fabric ID: Dual
Network Type: Lan	If Type: Virtual
Locale: External	Transport Type: Ether
Owner: Local	
Sharing Type: O None O Primary O Isolat	ted O Community Primary VI AN: VI AN 1750 (1750)
Duinney MIAN Dune aution	
Primary VLAN Properties	
Name: 1750	VLAN ID: 1750
Name: 1750 Native VLAN: No	VLAN ID: 1750 Fabric ID: Dual
Name: 1750 Native VLAN: No Network Type: Lan	VLAN ID: 1750 Fabric ID: Dual If Type: Virtual
Name: 1750 Native VLAN: No Network Type: Lan Locale: External	VLAN ID: 1750 Fabric ID: Dual If Type: Virtual Transport Type: Ether
Name: 1750 Native VLAN: No Network Type: Lan Locale: External Owner: Local	VLAN ID: 1750 Fabric ID: Dual If Type: Virtual Transport Type: Ether
Name: 1750 Native VLAN: No Network Type: Lan Locale: External Owner: Local Multicast Policy Name: <not set=""></not>	VLAN ID: 1750 Fabric ID: Dual If Type: Virtual Transport Type: Ether Create Multicast Policy
Name: 1750 Native VLAN: No Network Type: Lan Locale: External Owner: Local Multicast Policy Name: <not set=""></not>	VLAN ID: 1750 Fabric ID: Dual If Type: Virtual Transport Type: Ether Create Multicast Policy
Name: 1750 Native VLAN: No Network Type: Lan Locale: External Owner: Local Multicast Policy Name: <not set=""> Multicast Policy Instance: org-root/mc-policy-def</not>	VLAN ID: 1750 Fabric ID: Dual If Type: Virtual Transport Type: Ether Create Multicast Policy ault

Properties		
Name: 1786		VLAN ID: 1786
Native VLAN: No		Fabric ID: Dual
Network Type: Lan		If Type: Virtual
Locale: External		Transport Type: Ether
Owner: Local		
Sharing Type: O None O Prir	nary 🔾 Isolated 💿 Community	Primary VLAN: VLAN 1750 (1750) -
<u>-</u>		
۰		
Primary VLAN Properties		
Primary VLAN Properties Name: 1750	VLAN ID:	: 1750
Primary VLAN Properties Name: 1750 Native VLAN: No	VLAN ID: Fabric ID:	: 1750 : Dual
Primary VLAN Properties Name: 1750 Native VLAN: No Network Type: Lan	VLAN ID: Fabric ID: If Type:	: 1750 : Dual : Virtual
Primary VLAN Properties Name: 1750 Native VLAN: No Network Type: Lan Locale: Extern	VLAN ID: Fabric ID: If Type: al Transport Type:	: 1750 : Dual : Virtual : Ether
Primary VLAN Properties Name: 1750 Native VLAN: No Network Type: Lan Locale: Extern Owner: Local	VLAN ID: Fabric ID: If Type: al Transport Type:	: 1750 : Dual : Virtual : Ether
Primary VLAN Properties Name: 1750 Native VLAN: No Network Type: Lan Locale: Extern Owner: Local Multicast Policy Name: <not se<="" th=""><td>VLAN ID: Fabric ID: If Type: al Transport Type: et> Treate Multi</td><td>: 1750 : Dual : Virtual : Ether ticast Policy</td></not>	VLAN ID: Fabric ID: If Type: al Transport Type: et> Treate Multi	: 1750 : Dual : Virtual : Ether ticast Policy
Primary VLAN Properties Name: 1750 Native VLAN: No Network Type: Lan Locale: Extern Owner: Local Multicast Policy Name: <not se<br="">Multicast Policy Instance: org-roo</not>	VLAN ID: Fabric ID: If Type: al Transport Type: et>	: 1750 : Dual : Virtual : Ether ticast Policy

3. La carte d'interface réseau virtuelle (vNIC) sur le profil de service transporte des VLAN ordinaires ainsi que des PVLAN, comme le montre l'image.

General VLANs Statistics Faults Events							
🕰 Filter 🖨 Export 😸 Print							
VLAN	VLAN ID	Oper VLAN	Native VLAN				
1750	1750	fabric/lan/net-1750	0				
1785	1785	fabric/lan/net-1785	0				
1786	1786	fabric/lan/net-1786	0				
default	1	fabric/lan/net-default	\bigcirc				
qam-121	121	fabric/lan/net-qam-121	0				
qam-221	221	fabric/lan/net-qam-221	Ô				

4. Le canal de port de liaison ascendante sur UCS transporte des VLAN ordinaires ainsi que des PVLAN :

interface port-channel1 description U: Uplink switchport mode trunk pinning border switchport trunk allowed vlan 1,121,221,321,1750,1785-1786 speed 10000

F240-01-09-UCS4-A(nxos)#

F240-01-09-UCS4-A(nxos)# show vlan private-vlan Primary Secondary Type Ports

1750 1785 isolated 1750 1786 community

VMware DVS

VmwareDVS Settings		— ×
Properties Network Adapters Private VLAN NetFlow Port Mir	roring	
Enter or edit primary private VLAN ID.	Enter or edit a secondary private VL	AN ID and Type.
Primary private VLAN ID	Secondary private VLAN ID	Туре
1750	1750	Promiscuous
[Enter a private VLAN ID here]	1785	Isolated
	1786	Community
	[Enter a private VLAN ID here]	Select
Range: 1-4094 Remove	Range: 1-4094	Remove
Help		OK Cancel

VmwareDVS 🚯



Commutateur N5k ascendant

vlan 1750 private-vlan primary private-vlan association 1785-1786

vlan 1785 private-vlan isolated

vlan 1786 private-vlan community

interface Vlan1750

ip address 10.10.175.252/24 private-vlan mapping 1785-1786

no shutdown

interface port-channel114

Description To UCS
switchport mode trunk
switchport trunk allowed vlan 1,121,154,169,221,269,321,369,1750,1785-1786
spanning-tree port type edge
spanning-tree bpduguard enable
spanning-tree bpdufilter enable
vpc 114 <=== if there is a 5k pair in vPC configuration only then add this line to both N5k</pre>

Changement de comportement avec UCS version 3.1(3)

Avant UCS version 3.1(3), une machine virtuelle dans le VLAN de communauté peut communiquer avec une machine virtuelle dans le VLAN principal sur le DVS VMware, où la machine virtuelle du VLAN principal réside à l'intérieur de l'UCS. Ce comportement était incorrect, car la machine virtuelle principale doit toujours être orientée vers le nord ou en dehors d'UCS. Ce comportement est documenté via l'ID de défaut <u>CSCvh87378</u>.

Àpartir de la version 2.2(2) d'UCS, en raison d'un défaut dans le code, le VLAN de communauté a pu communiquer avec le VLAN principal qui était présent derrière l'IF. Mais Isolated ne pouvait jamais communiquer avec le principal derrière l'IF. Les machines virtuelles (isolées et communautaires) sont toujours en mesure de communiquer avec le principal à l'extérieur de l'IF.

Àpartir de la version 3.1(3), ce défaut permet à la communauté de communiquer avec le principal derrière l'FI, a été corrigé et par conséquent les machines virtuelles communautaires ne pourront pas communiquer avec une machine virtuelle dans le VLAN principal qui réside dans UCS.

Pour résoudre cette situation, la machine virtuelle principale doit être déplacée (vers le nord) en dehors d'UCS. Si ce n'est pas possible, la machine virtuelle principale doit être déplacée vers un autre VLAN qui est un VLAN normal et non un VLAN privé.

Par exemple, avant le microprogramme 3.1(3), une machine virtuelle du VLAN 1786 de la communauté pouvait communiquer à une machine virtuelle du VLAN 1750 principal qui réside dans UCS, mais cette communication romprait le microprogramme 3.1(3) et ultérieur, comme

```
l'illustre l'image.
```

NOTE:

<u>CSCvh87378</u> a été traité dans les versions 3.2(3l) et 4.0.4e et ultérieures pour que nous puissions avoir un Vlan principal derrière UCS. Cependant, notez que le VLAN isolé dans UCS ne pourra pas parler au VLAN principal dans UCS. Seul le VLAN de communauté et le VLAN principal peuvent communiquer entre eux lorsque les deux sont derrière UCS.

F240-01- * 1786 F240-01-	09-UCS4-A(nxos) 0050.568e.76 09-UCS4-A(nxos)	#shown id7dy #	nac addr /namic	ess-table 440	inc 76 F F	d7 Veth3148
VLAN	MAC Address	Type	age	Secure NTFY	Ports,	/SWID.SSID.LID
* 1750 F240-01-09	0050.568e.476f 9-UCS4-B(nxos)#	dynamic	0	 F F	Veth3240	

Commutateur en amont 4900

Note: Dans cet exemple, 4900 est une interface de couche 3 vers un réseau externe. Si votre topologie pour L3 est différente, apportez les modifications nécessaires

Sur le commutateur 4900, procédez comme suit et configurez le port de promiscuité. Le PVLAN se termine par le port proche.

- 1. Activez la fonction PVLAN si nécessaire.
- 2. Créez et associez les VLAN comme sur le Nexus 5K.
- 3. Créez le port proche sur le port de sortie du commutateur 4900. À partir de ce point, les paquets des VLAN 1785 et 1786 sont vus sur VLAN 1750 dans ce cas.

Switch(config-if)#switchport mode trunk switchport private-vlan mapping 1785-1786 switchport mode private-vlan promiscuous

Sur le routeur en amont, créez une sous-interface pour le VLAN 1750 uniquement. À ce niveau, les exigences dépendent de la configuration réseau que vous utilisez :

interface GigabitEthernet0/1.1

encapsulation dot1Q 1750

IP address10.10.175.254/24

Vérification

Aucune procédure de vérification n'est disponible pour cette configuration.

Dépannage

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Cette procédure décrit comment tester la configuration de VMware DVS avec l'utilisation de PVLAN.

1. Exécutez des requêtes ping vers d'autres systèmes configurés dans le groupe de ports, ainsi que vers le routeur ou un autre périphérique au niveau du port proche. Les requêtes ping envoyées au périphérique au-delà du port proche doivent fonctionner, tandis que celles envoyées aux autres périphériques du VLAN isolé doivent échouer, comme le montrent les images.

1	🛃 wi	n_175()_vm	w_isola	ted on	.12	21.12						
	File	View	VM										
				6	$\overline{\mathbb{O}}$		Ĩ	>		B 2			
	E _n s	erver	Mana	iger									
	File	Acti	on	View	Help								
			•	?									
		Server	Mana	ner (WII	N-OHHTS	S16UTT	Serve	ar Man		(WIN-O	IHTS	1611704)	
		Fea	es iture:	Cit. Adi Au	itoco	ator:C nfigu	rati	na Pro on Er	nable	ed		. : Yes	
	+	Dia Cor	gnos nfigur	C:\Us C:\Us	ers\ ers\	Admin Admin	istra istra	ator) ator)	> >ping	y 10.1	0.1	75.252	
:		3.0	laye	Pingi Reply Reply Reply Reply	ng 10 fro fro fro fro	0.10. m 10. m 10. m 10. m 10.	175. 10.1 10.1 10.1 10.1	252 v 75.29 75.29 75.29 75.29	with 52:] 52:] 52:] 52:]	32 by bytes= bytes= bytes= bytes=	tes 32 32 32 32 32	of data: time=1ms TTL=255 time<1ms TTL=255 time<1ms TTL=255 time<1ms TTL=255	
1				Ping I Appro	stat: Packer xima linim	istic ts: S te ro um =	s fo ent und Øms,	r 10. = 4, trip Maxi	.10.1 Rece time imum	l75.25 eived es in = 1ms	2: = 4 mil , A	, Lost = 0 (0% loss), li-seconds: verage = 0ms	
				C∶∖Us	ers	Admin	istra	ator)	>ping	y 10.1	0.1	75.132	
				Pingi Reply Reply Reply Reply	ng 1 fro fro fro fro	0.10. m 10. m 10. m 10. m 10.	175. 10.1 10.1 10.1 10.1	132 v 75.13 75.13 75.13 75.13	vith 31:] 31:] 31:] 31:]	32 by Destin Destin Destin Destin	tes ati ati ati	of data: on host unreachable. on host unreachable. on host unreachable. on host unreachable.	
				Ping I	stat Packe	istic ts: S	s fo ent	r 10. = 4,	.10.1 Rece	175.13 eived	2: = 4	, Lost = 0 (0% loss),	
ľ	::\II	ser	s\A	C:\Us dmin	ers∖ istr	Admin ator	istra ⊳≻in	ator) conf	> ia	/a11			
	lind	0.140	TD	Con	fim	wate	ion		-3				
	"TIIU	ows	11	GUII	r ryu	irat.	LOII						
	H P N I W	ost rim ode P R INS	Na ary Ty out Pr	me . Dns pe . ing oxy	Suf Enat Enat	fix led	· · ·					WIN-QHHISI60104 Hybrid No No	
	Ethe	rne	t a	dapt	er I	oca]	l Ar	ea (Conn	ecti	DN	4:	
	C D P D A I S D	onn esc: hys HCP uto Pv4 ubn efa	ect rip En con Ad et	ion- tion l Ad able figu dres Mask Gat	spec dres d. rati s.	ific s. on I	Enab	S Su led		.× .		vmxnet3 Ethernet Adapter #3 00-50-56-8E-57-7F No Yes 10.10.175.131(Preferred) 255.255.255.0 10.10.175.252	

Vérifiez les tables d'adresses MAC afin de voir où votre adresse MAC est apprise. Sur tous les commutateurs, l'adresse MAC doit se trouver dans le VLAN isolé, sauf sur le commutateur avec le port proche. Sur le commutateur proche, l'adresse MAC doit se trouver dans le VLAN principal.

2. UCS comme l'illustre l'image.

Putty 191.75 - Putty								
F240-01-09-UCS4-A(nxos)#								
F240-01-09-UCS4-A(nxos)#								
F240-01-09-UCS4-A(nxos)#								
F240-01-09-UCS4-A(nxos)#								
F240-01-09-UCS4-A(nxos)#								
F240-01-09-UCS4-A(nxos)#								
F240-01-09-UCS4-A(nxos)#								
F240-01-09-UCS4-A(nxos)#	show mac address-table vlan 1785							
Legend:								
* - primary entry	, G - Gateway MAC, (R) - Routed MAC, O - Overlay MAC							
age - seconds sin	ce last seen, + - primary entry using VPC Peer-Link							
VLAN MAC Address	Type age Secure NITI Ports/SwiD.SSID.Lib							
* 1785 0050.568e.577f	dynamic 0 F F Veth2486							
F240-01-09-UCS4-A(nxos)#								
F240-01-09-UCS4-A(nxos)#	show mac address-table vlan 1786							
Legend:								
* - primary entry	, G - Gateway MAC, (R) - Routed MAC, O - Overlay MAC							
age - seconds sin	ce last seen, + - primary entry using vPC Peer-Link							
VLAN MAC Address	Type age Secure NTFY Ports/SWID.SSID.LID							
* 1700 0050 500- 70-0								
* 1786 UUSU.568e.73c2	dynamic 0 F F Vetn2486							
~ 1/00 UUSU.S68E./6d/	dynamic 0 F F Veth2486							
1240-01-09-0C94-A(IIX08)#								

3. Vérifiez que la sortie n5k en amont est identique à celle de la sortie précédente sur n5k et comme le montre l'image.

f241-01-08-5596-a# show mac address-table | inc 577f 0050.568e.577f * 1785 dynamic 170 F F Po114 f241-01-08-5596-a# f241-01-08-5596-a# show mac address-table | inc 73c2 * 1786 0050.568e.73c2 dynamic 10 F F Po114 f241-01-08-5596-a# show mac address-table | inc 76d7 * 1786 0050.568e.76d7 dynamic 30 F F Po114 f241-01-08-5596-a#

Configuration avec Nexus 1000v avec port de promiscuité en amont N5k

Configuration UCS

La configuration UCS (qui inclut la configuration vNIC du profil de service) reste la même que dans l'exemple de VMware DVS.

Configuration N1k

feature private-vlan

vlan 1750 private-vlan primary private-vlan association 1785-1786

vlan 1785 private-vlan isolated

vlan 1786 private-vlan community

same uplink port-profile is being used for regular vlans & pvlans. In this example vlan 121 & 221 are regular vlans but you can change them accordingly

port-profile type ethernet pvlan-uplink-no-prom switchport mode trunk mtu 9000 switchport trunk allowed vlan 121,221,1750,1785-1786 channel-group auto mode on mac-pinning

system vlan 121 no shutdown state enabled vmware port-group

port-profile type vethernet pvlan_1785 switchport mode private-vlan host switchport private-vlan host-association 1750 1785 switchport access vlan 1785 no shutdown state enabled vmware port-group

port-profile type vethernet pvlan_1786 switchport mode private-vlan host switchport access vlan 1786 switchport private-vlan host-association 1750 1786 no shutdown state enabled vmware portgroup

Cette procédure décrit comment tester la configuration.

1. Exécutez des requêtes ping vers d'autres systèmes configurés dans le groupe de ports, ainsi que vers le routeur ou un autre périphérique au niveau du port proche. Les requêtes ping envoyées au périphérique au-delà du port proche doivent fonctionner, tandis que celles envoyées aux autres périphériques du VLAN isolé doivent échouer, comme indiqué dans la section précédente et dans les images.