

UCS Fabric Interconnect Management-Schnittstellen haben zeitweilige Verbindungsprobleme

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Problem: UCS Fabric Interconnect Management-Schnittstellen haben zeitweilige Verbindungsprobleme.](#)

[Topologie](#)

[Fabric Interconnect-IPs im VLAN 10](#)

[Problematische Gerätekommunikation für VLAN 1](#)

[Fehlerbehebung](#)

[Ursache](#)

[Lösung](#)

[Zusätzliche Informationen](#)

[Zugehörige Informationen](#)

Einführung

In diesem Dokument wird beschrieben, wie bei UCS Fabric Interconnect Management (Mgmt)-Schnittstellen gelegentliche Verbindungsprobleme bei der Kommunikation mit und von einem bestimmten IP-Bereich aufgetreten sind.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Software Unified Computing Systems Manager (UCSM)
- Unified Computing System (UCS)-Netzwerke

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- 6200 FI
- UCS Manager 4.0

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Problem: UCS Fabric Interconnect Management-Schnittstellen haben zeitweilige Verbindungsprobleme.

Die UCS Fabric Interconnect Management-Schnittstellen weisen nur gelegentlich Verbindungsverluste auf, allerdings nur, wenn die Kommunikation über einen bestimmten IP-Bereich erfolgt. Der IP-Bereich von VLAN 10.128.10.0/24 wird für die Mgmt-Schnittstellen für Fabric Interconnects (FI) und Virtual IP (VIP) verwendet. Wenn die Kommunikation zwischen dem IP-Bereich von VLAN 1 und dem IP-Bereich von 10.128.1.0/24 erfolgt, brechen die Verbindungen zu den FIs und von diesen ab. Daher kann jedes Gerät im IP-Bereich von VLAN 1 keine Verbindung mit UCSM herstellen und kann nur einen Ping-Befehl für eine FI-IP-Adresse senden. Mindestens eine FI-IP (von drei, FI-A, FI-B, VIP) kann immer kommunizieren.

Topologie

Fabric Interconnect-IPs im VLAN 10

FI-A: 10.128.10.84

FI-B: 10.128.10.85

VIP: 10.128.10.86

GW: 10.128.10.1

Problematische Gerätekommunikation für VLAN 1

Subnet 10.128.1.0/24

GW: 10.128.1.1

Fehlerbehebung

Aus dem lokalen Mgmt-Kontext beider Fabric Interconnects kann es sein Standardgateway (df) (gw) 10.128.10.1 erreichen. jedoch ist keine IP-Adresse im VLAN 1 IP-Bereich von 10.128.1.0/24 für den lokalen Mgmt-Kontext der Fabric Interconnects oder von diesem erreichbar.

Zunächst scheint es sich um ein Problem mit dem Routing am Gateway und nicht um ein UCS-Problem zu handeln, da es sich hierbei lediglich um eine Management-Schnittstelle auf Fabric Interconnects handelt und ob das Gateway und alle anderen IP-Bereiche erreicht werden können. Dies stellt ein Layer-3-Routenproblem im Upstream-Netzwerk dar.

Wenn Traceroute vom Fabric Interconnect zu einem zufälligen IP-Bereich (und einem beliebigen anderen IP-Bereich, der nicht im Bereich von VLAN 1 liegt) ausgeführt wird (z. B. eine IP-Adresse aus VLAN 20: 10.128.20.1) ist der erste Hop auf der Traceroute das 10.128.10.1-Gateway von

VLAN 10, und der Ping-Befehl ist erfolgreich.

Wenn Traceroute in den bekannten, problematischen IP-Bereich 10.128.1.x/24 ausgeführt wird, schlägt die Traceroute fehl.

- Aus diesem Grund sollten Sie sich auch auf UCS-Seite erkundigen.
- Dies sollte nicht fehlgeschlagen sein, und der erste Hop sollte der df gw der Mgmt-Schnittstelle 10.128.10.1 sein, genau wie bei 10 von 10 weiteren IPs, die getestet wurden und außerhalb des VLAN 10-IP-Bereichs lagen und sich nicht im VLAN 1-IP-Bereich befanden.

Um weiter zu untersuchen, führten Sie einen Ethalyzer durch, um zu sehen, was vor sich geht und wenn der IP-Bereich von VLAN 1 gepingt wird, wirkt ARP neugierig:

```
EWQLOVIUCS02-A(nxos)# ethalyzer local interface mgmt display-filter arp limit-captured-frames 0
```

Capturing on eth0

```
2019-12-17 11:45:50.807837 00:de:fb:a9:37:e1 -> ff:ff:ff:ff:ff:ff ARP Who has 10.128.1.77? Tell 10.128.0.142
```

```
2019-12-17 11:45:51.807835 00:de:fb:a9:37:e1 -> ff:ff:ff:ff:ff:ff ARP Who has 10.128.1.77? Tell 10.128.0.142
```

```
2019-12-17 11:45:52.807827 00:de:fb:a9:37:e1 -> ff:ff:ff:ff:ff:ff ARP Who has 10.128.1.77? Tell 10.128.0.142
```

```
2019-12-17 11:45:55.807829 00:de:fb:a9:37:e1 -> ff:ff:ff:ff:ff:ff ARP Who has 10.128.1.77? Tell 10.128.0.142
```

Das erwartete Verhalten bestand darin, zu fragen, wer über diese IP-Adresse für VLAN 1 verfügt, aber dann das Gateway für das Mgmt-VLAN 10 zu informieren.

Wenn der IP-Bereich von VLAN 1 gepingt wird, fragt ARP, wer diese IP-Adresse besitzt und 10.128.0.142 anzugeben, gehen Sie wie folgt vor:

- Dies sollte "Tell 10.128.10.1" sein, wie es bei allen anderen getesteten IP-Adressen der Fall war.
- Sie erkennen nicht einmal ein 10.128.0.x-Subnetz oder eine IP-Adresse.

Dies ist ein Problem, warum die FI 10.128.0.142 mitteilen würde, während der Untersuchung der UCS-Domäne wurde festgestellt, dass diese IP-Adresse auf den CIMC von Server 1/5 angewendet wurde:

```
EWQLOVIUCS02-B(local-mgmt)# show mgmt-ip-debug ip-tables
```

<SNIPPED>

Chain PREROUTING (policy ACCEPT 5303K packets, 360M bytes)

pkts	bytes	target	prot	opt	in	out	source	destination	
188	9776	cimcnat	tcp	--	*	*	0.0.0.0/0	0.0.0.0/0	tcp
dpt:443									
0	0	cimcnat	tcp	--	*	*	0.0.0.0/0	0.0.0.0/0	tcp
dpt:80									

0	0	DNAT	icmp	--	*	*	0.0.0.0/0	10.128.10.85	
to:127.6.1.1									
0	0	DNAT	tcp	--	*	*	0.0.0.0/0	10.128.10.85	tcp
dpt:2068 to:127.6.1.1:2068									
0	0	DNAT	udp	--	*	*	0.0.0.0/0	10.128.10.85	udp
dpt:623 to:127.6.1.1:623									
0	0	DNAT	tcp	--	*	*	0.0.0.0/0	10.128.10.85	tcp
dpt:22 to:127.6.1.1:22									
449	26940	DNAT	icmp	--	*	*	0.0.0.0/0	10.128.10.108	
to:127.6.1.2									
0	0	DNAT	tcp	--	*	*	0.0.0.0/0	10.128.10.108	tcp
dpt:2068 to:127.6.1.2:2068									
0	0	DNAT	udp	--	*	*	0.0.0.0/0	10.128.10.108	udp
dpt:623 to:127.6.1.2:623									
0	0	DNAT	tcp	--	*	*	0.0.0.0/0	10.128.10.108	tcp
dpt:22 to:127.6.1.2:22									
931	55860	DNAT	icmp	--	*	*	0.0.0.0/0	10.128.10.107	
to:127.6.1.3									
0	0	DNAT	tcp	--	*	*	0.0.0.0/0	10.128.10.107	tcp
dpt:2068 to:127.6.1.3:2068									
0	0	DNAT	udp	--	*	*	0.0.0.0/0	10.128.10.107	udp
dpt:623 to:127.6.1.3:623									
0	0	DNAT	tcp	--	*	*	0.0.0.0/0	10.128.10.107	tcp
dpt:22 to:127.6.1.3:22									
0	0	DNAT	icmp	--	*	*	0.0.0.0/0	10.128.10.104	
to:127.6.1.3									
0	0	DNAT	tcp	--	*	*	0.0.0.0/0	10.128.10.104	tcp
dpt:2068 to:127.6.1.3:2068									
0	0	DNAT	udp	--	*	*	0.0.0.0/0	10.128.10.104	udp
dpt:623 to:127.6.1.3:623									
0	0	DNAT	tcp	--	*	*	0.0.0.0/0	10.128.10.104	tcp
dpt:22 to:127.6.1.3:22									
920	55200	DNAT	icmp	--	*	*	0.0.0.0/0	10.128.10.106	
to:127.6.1.4									
0	0	DNAT	tcp	--	*	*	0.0.0.0/0	10.128.10.106	tcp
dpt:2068 to:127.6.1.4:2068									
0	0	DNAT	udp	--	*	*	0.0.0.0/0	10.128.10.106	udp
dpt:623 to:127.6.1.4:623									
0	0	DNAT	tcp	--	*	*	0.0.0.0/0	10.128.10.106	tcp
dpt:22 to:127.6.1.4:22									
912	54720	DNAT	icmp	--	*	*	0.0.0.0/0	10.128.10.105	
to:127.6.1.6									
0	0	DNAT	tcp	--	*	*	0.0.0.0/0	10.128.10.105	tcp

```

dpt:2068 to:127.6.1.6:2068

    0    0 DNAT    udp  --  *    *    0.0.0.0/0    10.128.10.105    udp
dpt:623 to:127.6.1.6:623

    0    0 DNAT    tcp  --  *    *    0.0.0.0/0    10.128.10.105    tcp
dpt:22 to:127.6.1.6:22

    0    0 DNAT    icmp --  *    *    0.0.0.0/0    10.128.0.142
to:127.6.1.5    <<---- Indicates that 10.128.0.142 is the OOB KVM IP address for server 1/5.

    0    0 DNAT    tcp  --  *    *    0.0.0.0/0    10.128.0.142    tcp
dpt:2068 to:127.6.1.5:2068

    0    0 DNAT    udp  --  *    *    0.0.0.0/0    10.128.0.142    udp
dpt:623 to:127.6.1.5:623

    0    0 DNAT    tcp  --  *    *    0.0.0.0/0    10.128.0.142    tcp
dpt:22 to:127.6.1.5:22

    910 54600 DNAT    icmp --  *    *    0.0.0.0/0    10.128.10.102
to:127.6.1.7

    0    0 DNAT    tcp  --  *    *    0.0.0.0/0    10.128.10.102    tcp
dpt:2068 to:127.6.1.7:2068

    0    0 DNAT    udp  --  *    *    0.0.0.0/0    10.128.10.102    udp
dpt:623 to:127.6.1.7:623

    0    0 DNAT    tcp  --  *    *    0.0.0.0/0    10.128.10.102    tcp
dpt:22 to:127.6.1.7:22

    908 54480 DNAT    icmp --  *    *    0.0.0.0/0    10.128.10.101
to:127.6.1.8

    0    0 DNAT    tcp  --  *    *    0.0.0.0/0    10.128.10.101    tcp
dpt:2068 to:127.6.1.8:2068

    0    0 DNAT    udp  --  *    *    0.0.0.0/0    10.128.10.101    udp
dpt:623 to:127.6.1.8:623

    0    0 DNAT    tcp  --  *    *    0.0.0.0/0    10.128.10.101    tcp
dpt:22 to:127.6.1.8:22

<SNIPPED>

```

Ursache

Das Problem war eine falsch eingegebene statische CIMC-IP-Adresse für Server 1/5.

Zusätzlich wurde es im Subnetz 255.255.248.0 abgelegt.

Dadurch wurde ein unerwünschter Eintrag in der Routing-Tabelle von Fabric Interconnect erstellt. Eine, die die Bedingung erfüllt, bevor sie die Standardroute für alle IPs im Bereich von 10.128.0.1 bis 10.128.7.254 erreicht.

```
Linux(debug)# route -n

Kernel IP routing table

Destination      Gateway          Genmask         Flags Metric Ref    Use Iface
10.128.10.0      0.0.0.0         255.255.255.0  U         0      0      0 eth0
127.15.1.0      0.0.0.0         255.255.255.0  U         0      0      0 vlan4042
127.7.0.0       0.0.0.0         255.255.0.0    U         0      0      0 vlan4043
127.5.0.0       0.0.0.0         255.255.0.0    U         0      0      0 vlan4044
127.14.0.0      0.0.0.0         255.255.0.0    U         0      0      0 vlan4046
127.12.0.0      0.0.0.0         255.255.0.0    U         0      0      0 bond0
127.9.0.0       0.0.0.0         255.255.0.0    U         0      0      0 vlan4047
10.0.0.0        0.0.0.0         255.0.0.0      U         0      0      0 eth0    <<-----
Undesired route entry
10.0.0.0        0.0.0.0         255.0.0.0      U         0      0      0 eth0    <<-----
Undesired route entry
0.0.0.0         10.128.10.1    0.0.0.0        UG        0      0      0 eth0
```

Lösung

Die Lösung für diesen Fall besteht darin, UCSM aus einem nicht betroffenen IP-Bereich zu durchsuchen und die statische CIMC Out of Band (OOB)-Adresse von Server 1/5 zu verwenden. Sie wird aus dem OOB-Management-Pool entnommen und ist bereits eingerichtet. Es sollte wie jeder andere Server in der Umgebung verwendet werden.

Zusätzliche Informationen

Wenn das Fabric Interconnect neu gestartet wird, funktioniert es manchmal. Das Problem betrifft die Verwaltungsinstanz dieses Servers. Der unerwünschte Eintrag für die Routing-Tabelle wird nur auf dem Fabric Interconnect erstellt. Wenn die Management-Instanz der gleiche Fabric Interconnect war wie der primäre Fabric Interconnect, können sie den VIP oder diesen Fabric Interconnect nicht erreichen.

Die IP-Zuweisung für das CIMC-Management sollte immer im gleichen IP-Bereich wie der OOB-IP-Bereich des Fabric Interconnects liegen.

Zugehörige Informationen

- [Cisco UCS Manager Administrationsleitfaden 3.1](#)
- [Technischer Support und Dokumentation - Cisco Systems](#)