

Réponses d'interrogation SNMP provenant de différentes adresses IP dans 2GFI par rapport à 4GFI

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Informations générales](#)

[Le résultat du test présente un comportement différent de 6200 et 6400 FI lorsque VIP est interrogé par SNMP](#)

[FI 6248 avec microprogramme UCSM 4.0.4e](#)

[FI 6454 avec microprogramme UCSM 4.0.4d](#)

[Informations connexes](#)

Introduction

Ce document décrit un comportement différent lorsque le protocole SNMP (Simple Network Monitoring Protocol) marche ou se dirige vers 6200 Fabric Interconnect (FI) par rapport au protocole 6454 FI. Les pare-feu avec état peuvent bloquer les réponses IP physiques aux passerelles d'adresses IP virtuelles (VIP) SNMP dans FI 6200, alors que le problème n'est pas visible dans 6454 FI.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- SNMP Walk Tool installé sur un serveur avec connectivité au domaine UCSM (Unified Computing System Manager).
- 6248 FI et 6454 FI

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- SNMP Walk Tool installé sur un serveur avec connectivité au domaine UCSM (Unified Computing System Manager).
- 6248 FI avec microprogramme UCSM 4.0(4e)
- 6454 FI avec microprogramme UCSM 4.0(4f)

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. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Produits connexes

Ce document peut également être utilisé avec les versions de matériel et de logiciel suivantes :

- Tout logiciel d'interrogation ou de marche SNMP tiers
- 6296 FI

Informations générales

Les pare-feu entre les serveurs FI et SNMP Collector/Walk peuvent être configurés pour l'inspection dynamique, ce qui signifie que lorsqu'une requête est envoyée à partir d'une certaine adresse IP, la réponse est uniquement autorisée à partir de cette même adresse IP. Les interconnexions de fabric utilisent une adresse IP virtuelle (VIP) à laquelle répond l'FI principal. L'inspection dynamique du pare-feu peut bloquer les réponses SNMP dans une FI de 2e génération comme le 6248 si le SNMP Get ou Walk est demandé au VIP comme dans ce modèle si la réponse provient de l'IP physique de l'FI principal. Le pare-feu avec inspection avec état autorise uniquement les réponses de l'adresse IP ciblée de sorte que les paquets soient bloqués. Dans les tests, une FI de 4e génération comme la réponse 6454 avec laquelle IP est demandée, le VIP ou l'une ou l'autre IP physique répondra s'il s'agit de l'IP cible.

La solution de contournement pour les FI de 2e génération, comme les modèles 6248 et 6296, consiste à cibler l'IP physique de l'FI principal ou à modifier les règles de pare-feu pour autoriser les réponses de l'une ou l'autre IP physique de l'IF si une demande est faite du VIP.

Le résultat du test présente un comportement différent de 6200 et 6400 FI lorsque VIP est interrogé par SNMP

FI 6248 avec microprogramme UCSM 4.0.4e

Sortie de ligne de commande du serveur Walk SNMP :

```
[SNMP Walk Server]$ snmpwalk -c 'xxx' 172.16.0.52 <<< SNMP Walk of the Physical IP of FI
snmpwalk: No securityName specified <<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<< No network errors so successful reply
[SNMP Walk Server]$ snmpwalk -c 'xxx' 172.16.0.53 <<< SNMP Walk of the Virtual IP
snmpwalk: Timeout <<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<< Network Error
```

Capture de paquets FI :

```
FI-B(nxos)# ethanalyzer local interface mgmt capture-filter "host 10.0.45.154" limit-captured-frames 0
Capturing on eth0
2020-01-06 11:44:00.739413 10.0.45.154 -> 172.16.0.52 SNMP get-request <<< SNMP Walk of the Physical IP of FI
2020-01-06 11:44:01.274570 172.16.0.52 -> 10.0.45.154 SNMP report <<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<< FI replies with Physical IP of Primary FI
```

```

FI-B(nxos)# ethalyzer local interface mgmt capture-filter "host 10.0.45.154" limit-captured-frames 0
Capturing on eth0
2020-01-06 11:44:50.886972 10.0.45.154 -> 172.16.0.53 SNMP get-request <<< SNMP Walk of the Virtual IP
2020-01-06 11:44:50.887350 172.16.0.52 -> 10.0.45.154 SNMP report <<<<<<<< FI Replies with the IP of the Primary FI Physical IP Stateful Firewall may block this reply
2020-01-06 11:44:51.886878 10.0.45.154 -> 172.16.0.53 SNMP get-request
2020-01-06 11:44:51.887223 172.16.0.52 -> 10.0.45.154 SNMP report
2020-01-06 11:44:52.887808 10.0.45.154 -> 172.16.0.53 SNMP get-request
2020-01-06 11:44:52.888161 172.16.0.52 -> 10.0.45.154 SNMP report
2020-01-06 11:44:53.888741 10.0.45.154 -> 172.16.0.53 SNMP get-request
2020-01-06 11:44:53.889087 172.16.0.52 -> 10.0.45.154 SNMP report
2020-01-06 11:44:54.889477 10.0.45.154 -> 172.16.0.53 SNMP get-request
2020-01-06 11:44:54.889816 172.16.0.52 -> 10.0.45.154 SNMP report
2020-01-06 11:44:55.890280 10.0.45.154 -> 172.16.0.53 SNMP get-request
2020-01-06 11:44:55.890623 172.16.0.52 -> 10.0.45.154 SNMP report

```

FI 6454 avec microprogramme UCSM 4.0.4d

Sortie de ligne de commande du serveur Walk SNMP :

```

[SNMP Walk Server]$ snmpwalk -c 'fgING$df' 172.16.0.94 <<< SNMP Walk of the Physical IP of FI
snmpwalk: No securityName specified <<<<<<<<<<<<<<< No network errors so successful reply
[SNMP Walk Server]$ snmpwalk -c 'fgING$df' 172.16.0.93 <<< SNMP Walk of the Virtual IP
snmpwalk: No securityName specified <<<<<<<<<<<<<<< No network errors so successful reply

```

Capture de paquets FI :

```

stha99u11-B(nx-os)# ethalyzer local interface mgmt capture-filter "host 10.0.45.154" limit-captured-frames 0

Capturing on mgmt0
2020-01-06 12:01:31.866959 10.0.45.154 -> 172.16.0.94 SNMP get-request <<< SNMP Walk of the Physical IP of FI
2020-01-06 12:01:31.868620 172.16.0.94 -> 10.0.45.154 SNMP report 1.3.6.1.6.3.15.1.1.4.0 <<< FI replies from Physical IP no issues with Stateful Firewall
2020-01-06 12:01:47.647205 10.0.45.154 -> 172.16.0.93 SNMP get-request <<< SNMP Walk of the Virtual IP
2020-01-06 12:01:47.648800 172.16.0.93 -> 10.0.45.154 SNMP report 1.3.6.1.6.3.15.1.1.4.0 <<< FI replies from IP of Virtual IP no issues with Stateful Firewall

```

Informations connexes

- [Guide de surveillance du système Cisco UCS Manager, version 4.0](#)
- [Support et documentation techniques - Cisco Systems](#)