Risposte al polling SNMP da diversi IP in 2GFI rispetto a 4GFI

Sommario

[Introduzione](#)
[Prerequisiti](#)
[Requisiti](#)
[Componenti usati](#)
[Premesse](#)
[L'output del test mostra un comportamento diverso di 6200 e 6400 FI quando viene eseguito il polling di VIP SNMP](#)
[FI 6248 con firmware UCSM 4.0.4e](#)
[FI 6454 con firmware UCSM 4.0.4d](#)
[Informazioni correlate](#)

Introduzione

Questo documento descrive i diversi comportamenti quando l'SNMP (Simple Network Monitoring Protocol) cammina o raggiunge 6200 Fabric Interconnect (FI) rispetto a 6454 FI. I firewall stateful possono bloccare le risposte IP fisiche alle passeggiate SNMP di IP virtuali (VIP) in FI 6200, mentre il problema non è visibile in 6454 FI.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- SNMP Walk Tool installato su un server con connettività al dominio UCSM (Unified Computing System Manager).
- 6248 FI e 6454 FI

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- SNMP Walk Tool installato su un server con connettività al dominio UCSM (Unified Computing System Manager).
- 6248 FI con firmware UCSM 4.0(4e)
- 6454 FI con firmware UCSM 4.0(4f)

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali

conseguenze derivanti dall'uso dei comandi.

Prodotti correlati

Il presente documento può essere utilizzato anche per le seguenti versioni hardware e software:

- Qualsiasi software di monitoraggio o polling SNMP di terze parti
- 6296 FI

Premesse

Èpossibile impostare i firewall tra i server di raccolta/monitoraggio FI e SNMP per l'ispezione con conservazione dello stato. Ciò significa che quando si invia una richiesta da un determinato indirizzo IP, la risposta è consentita solo dallo stesso indirizzo IP. Le interconnessioni fabric utilizzano un IP virtuale (VIP) al quale l'URI primario risponde. L'ispezione stateful del firewall può bloccare le risposte SNMP nella FI di seconda generazione come la 6248 se viene richiesto il protocollo SNMP Get o Walk al VIP, come in quel modello, se la risposta proviene dall'IP fisico della FI primaria. Il firewall con ispezione stateful consente solo risposte dall'IP di destinazione in modo che i pacchetti vengano bloccati. Nei test di 4a generazione FI come il 6454 rispondono con quale IP è richiesto il VIP o o l'IP fisico risponderà se sono l'IP di destinazione.

La soluzione alternativa per FI di seconda generazione, come i modelli 6248 e 6296, consiste nel prendere di mira l'IP fisico dell'FI primario o modificare le regole del firewall per consentire le risposte da entrambi gli IP fisici dell'FI se viene fatta una richiesta dell'VIP.

L'output del test mostra un comportamento diverso di 6200 e 6400 FI quando viene eseguito il polling di VIP SNMP

FI 6248 con firmware UCSM 4.0.4e

Output della riga di comando di SNMP Walk Server:

```
[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
```

FI Packet Capture:

```
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)# ethanalyzer 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 con firmware UCSM 4.0.4d

Output della riga di comando di SNMP Walk Server:

```
[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
```

FI Packet Capture:

```
stha99u11-B(nx-os)# ethanalyzer 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
```

Informazioni correlate

- Guida al monitoraggio del sistema Cisco UCS Manager, versione 4.0
- Documentazione e supporto tecnico – Cisco Systems