4GFIと比較した2GFIの異なるIPからのSNMPポーリング応答

目次

[はじめに](#)
[前提条件](#)
[要件](#)
[使用するコンポーネント](#)
[背景説明](#)
[VIPがSNMPポーリングされた場合のテスト出力に6200と6400 FIのさまざまな動作が示される](#)
[FI 6248 wWith UCSM Firmware 4.0.4e](#)
[UCSMファームウェア4.0.4dを搭載したFI 6454](#)
[関連情報](#)

はじめに

このドキュメントでは、Simple Network Monitoring Protocol(SNMP)が6454 FIと比較して6200 Fabric Interconnect(FI)に移動または受信する場合のさまざまな動作について説明します。ステートフルファイアウォールは、FI 6200の仮想IP(VIP)のSNMPウォークに対する物理IP応答をブロックする可能性がありますが、6454 FIではこの問題は見られません。

前提条件

要件

次の項目に関する知識が推奨されます。

- Unified Computing System Manager(UCSM)ドメインへの接続が可能なサーバにSNMP Walk Toolがインストールされている。
- 6248 FIおよび6454 FI

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- Unified Computing System Manager(UCSM)ドメインへの接続が可能なサーバにSNMP Walk Toolがインストールされている。
- UCSMファームウェア4.0(4e)を搭載した6248 FI
- 6454 FI(UCSMファームウェア4.0(4f))

本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

関連製品

このドキュメントは、次のバージョンのハードウェアとソフトウェアにも使用できます。

- サードパーティ製SNMPウォークまたはポーリングソフトウェア
- 6296 FI

背景説明

FIサーバとSNMP Collector/Walkサーバ間のファイアウォールは、ステートフルインスペクション用に設定できます。つまり、特定のIPアドレスから要求が送信されると、そのIPアドレスからの応答のみが許可されます。ファブリックインターコネクトは、プライマリFIが応答する仮想IP(VIP)を使用します。ファイアウォールのステートフルインスペクションは、VIPに対してSNMP GetまたはWalkが要求された場合、6248のような第2世代FIでSNMP応答をブロックする可能性があります。モデルFIでは、応答はプライマリFIの物理IPから送信されます。ステートフルインスペクションを使用したファイアウォールでは、ターゲットIPからの応答のみが許可されるため、パケットはブロックされます。テストでは、6454のような第4世代FIが、VIPに要求されたIPに応答するか、物理IPがターゲットIPの場合に応答します。

6248および6296のような第2世代FIの回避策は、プライマリFIの物理IPをターゲットにするか、またはVIPから要求が行われた場合にFIの物理IPからの応答を許可するようにファイアウォールルールを変更します。

VIPがSNMPポーリングされた場合のテスト出力に6200と6400 FIのさまざまな動作が示される

FI 6248 wWith UCSM Firmware 4.0.4e

SNMP Walk Serverコマンドライン出力：

```
[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パケットキャプチャ：

```
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
```

UCSMファームウェア4.0.4dを搭載したFI 6454

SNMP Walk Serverコマンドライン出力：

```
[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パケットキャプチャ：

```
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
```

関連情報

- Cisco UCS Managerシステムモニタリングガイド、リリース4.0
- テクニカル サポートとドキュメント – Cisco Systems