Respuestas de Sondeo SNMP de Diferentes IP en 2GFI en comparación con 4GFI

Contenido

[Introducción](#)
[Prerequisites](#)
[Requirements](#)
[Componentes Utilizados](#)
[Antecedentes](#)
[El resultado de la prueba muestra un comportamiento diferente de FI 6200 y 6400 cuando VIP se consulta SNMP](#)
[FI 6248 con UCSM Firmware 4.0.4e](#)
[FI 6454 con firmware UCSM 4.0.4d](#)
[Información Relacionada](#)

Introducción

Este documento describe un comportamiento diferente cuando el protocolo simple de supervisión de red (SNMP) se dirige o se dirige a 6200 Fabric Interconnect (FI) en comparación con 6454 FI. Los firewalls stateful pueden bloquear las respuestas IP físicas a las rutas SNMP de IP virtuales (VIP) en FI 6200, mientras que el problema no se ve en la FI 6454.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Herramienta SNMP Walk instalada en un servidor con conectividad al dominio de Unified Computing System Manager (UCSM).
- 6248 FI y 6454 FI

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Herramienta SNMP Walk instalada en un servidor con conectividad al dominio de Unified Computing System Manager (UCSM).
- 6248 FI con firmware UCSM 4.0(4e)
- 6454 FI con firmware 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 tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Productos Relacionados

Este documento también puede utilizarse con estas versiones de software y hardware:

- Cualquier software de sondeo o marcha SNMP de terceros
- 6296 FI

Antecedentes

Los firewalls entre los servidores FI y SNMP Collectors/Walk pueden configurarse para la inspección de estado, lo que significa que cuando se envía una solicitud desde una dirección IP determinada, la respuesta sólo se permite desde esa misma dirección IP. Los Fabric Interconnects utilizan una IP virtual (VIP) a la que responde la FI principal. La inspección activa (stateful) del firewall puede bloquear las respuestas SNMP en la FI de segunda generación como el 6248 si se solicita el SNMP Get o Walk del VIP como en ese modelo si la respuesta viene de la IP física del FI primario. El firewall con inspección activa (stateful) sólo permite las respuestas de la IP de destino para que los paquetes se bloqueen. En las pruebas FI de cuarta generación como la respuesta 6454 con qué IP se solicita, el VIP o cualquier IP física responderá si son la IP de destino.

La solución alternativa para FI de 2ª generación como el 6248 y el 6296 es apuntar a la IP física del FI primario o alterar las reglas de firewall para permitir respuestas de cualquiera de las IP físicas de FI si se hace una solicitud del VIP.

El resultado de la prueba muestra un comportamiento diferente de FI 6200 y 6400 cuando VIP se consulta SNMP

FI 6248 con UCSM Firmware 4.0.4e

Salida de la Línea de Comandos de 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
```

Captura de paquetes 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)# 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

Salida de la Línea de Comandos de 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
```

Captura de paquetes FI:

```
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
```

Información Relacionada

- Guía de supervisión del sistema de Cisco UCS Manager, versión 4.0
- Soporte Técnico y Documentación - Cisco Systems