

排除ISE警報錯誤“；分析器SNMP請求故障：伺服器= NAD地址=錯誤消息=請求超時”

目錄

[問題](#)

[環境](#)

[解析](#)

[步驟 1:確定受影響的NAD。](#)

[步驟 2:確保SNMP在受影響的網路訪問裝置和客戶端上運行](#)

[步驟 3:確保NAD和ISE中的SNMP版本和SNMP社群字串或SNMP身份驗證/隱私協定密碼匹配](#)

[步驟 4:驗證ISE PSN和NAD客戶端之間的可達性和所需的UDP埠\(161,162\)](#)

[原因](#)

[相關內容](#)

- [問題](#)
 - [環境](#)
 - [解析](#)
 - [步驟 1:確定受影響的NAD。](#)
 - [步驟 2:確保SNMP在受影響的網路訪問裝置和客戶端上運行](#)
 - [步驟 3:確保NAD和ISE中的SNMP版本和SNMP社群字串或SNMP身份驗證/隱私協定密碼匹配](#)
 - [步驟 4:驗證ISE PSN和NAD客戶端之間的可達性和所需的UDP埠\(161,162\)](#)
 - [原因](#)
 - [相關內容](#)
-

問題

檢視ISE中的警報時，您會看到以下SNMP探查器錯誤：

“Profiler SNMP Request Failure: Server= <NAD DEVICE Name> NAD Address=<x.x.x.x> Error Message=Request t

環境

- Cisco Identity Services Engine(ISE)3.0.0版及更高版本
- 已啟用ISE分析服務
- 為SNMP通訊配置的網路訪問裝置(NAD)

解析

步驟 1:確定受影響的NAD。

1. 導航到控制面板>警報
2. 檢查警報詳細資訊並記下受影響的NAD裝置名稱或IP。
3. 您可以通過引用「分析器SNMP請求失敗」錯誤消息中的「NAD地址」欄位來識別特定的NAD客戶端IP地址。

步驟 2:確保SNMP在受影響的網路訪問裝置和客戶端上運行

登入到NAD客戶端的CLI並運行此命令以檢查是否啟用了SNMP功能。

```
show running-config | include snmp
```

示例SNMP v3:

```
Switch#show running-config | include snmp
ip access-list standard snmp-access
snmp-server group my-snmp-group v3 priv read admin-view access snmp-access
snmp-server view admin-view iso included
```

示例SNMP v2c:

```
snmp-server community public R0
snmp-server community private RW
snmp-server host 192.168.1.100 version 2c public
```

步驟 3:確保NAD和ISE中的SNMP版本和SNMP社群字串或SNMP身份驗證/隱私協定密碼匹配

按照以下步驟驗證SNMP v2c配置：

1. 登入NAD使用者端CLI，並執行「show snmp community」指令。

交換機輸出：

```
Community name: public
Community Index: public
Community SecurityName: public
storage-type: nonvolatile          active
```

2. 在ISE上：導覽至Administration > Network Resources > Network Devices。
3. 編輯標識的NAD條目，以確保SNMP社群字串和SNMP版本與「show snmp community」的輸出匹配。

ISE SNMP v2c:

☒ SNMP Settings

SNMP Version

2c

SNMP RO Community

public

Hide

SNMP Username

Security Level

Auth Protocol

Auth Password

Show

Privacy Protocol

Privacy Password

Show

Polling Interval

28,800

seconds(Valid Range 600 to 86400 or zero)

☒ Link Trap Query

☒ MAC Trap Query

Originating Policy Services Node

Auto

交換器遮罩SNMP v3身份驗證/隱私密碼。要確保這些憑據保持準確，請使用以下步驟重新輸入這些憑據：

1. 登入ISE GUI。
2. 導覽至Administration > Network Resources > Network Devices。
3. 編輯標識的NAD條目並轉到SNMP設定。按一下身份驗證密碼和隱私密碼上的「Show」。你可以透露它的密碼。

☒ **SNMP Settings**

SNMP Version	3	▼
SNMP RO Community		Show
SNMP Username	test	
Security Level	Priv	▼
Auth Protocol	SHA	▼
Auth Password	test@123	Hide
Privacy Protocol	AES128	▼
Privacy Password	test@123	Hide
Polling Interval	28,800	seconds(Valid Range 600 to 86400 or zero)
☒ Link Trap Query		
☒ MAC Trap Query		
Originating Policy Services Node	Auto	▼

4. 登入到交換機CLI。

- 運行命令configure terminal。
- 之後，運行此命令以更新交換機上的SNMP v3憑證。

交換器指令：

```
snmp-server user <username> <groupname> v3 auth sha <auth-password> priv aes 128 <priv-password>
```

範例：

```
snmp-server user test snmpgroup v3 auth sha test@123 priv aes 128 test@123
```

步驟 4:驗證ISE PSN和NAD客戶端之間的可達性和所需的UDP埠(161,162)

1. 從啟用了Profiler的PSN節點到NAD客戶端執行ping測試。
2. 執行從NAD客戶端到PSN節點的ping測試。
3. 確保PSN節點和NAD之間的埠161和162處於開啟狀態。
 - 使用Telnet從NAD客戶端測試啟用了Profiler的節點，以確認埠161和162已開啟。

```
telnet <ISE IP-address> 161  
telnet <ISE IP-address> 162
```

原因

當ISE無法成功查詢網路接入裝置時，會發生SNMP請求故障警報。這通常是因為兩台裝置之間有關SNMP社群字串、版本或v3憑證的設定不相符。此外，防火牆阻止UDP埠161或162，或缺少需要NAD上的SNMP伺服器配置等網路問題經常會阻止通訊成功。

相關內容

[在網路上允許所需的ISE埠和FQDN](#)

[ISE效能分析設計手冊](#)

[設定 SNMP 社群字串](#)

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。