

Beheben des ISE-Alarmfehlers “Profiler SNMP Request Failure: Server= NAD Address= Error Message=Timeout der Anfrage”

Inhalt

[Problem](#)

[Umwelt](#)

[Auflösung](#)

[Schritt 1: Identifizierung der betroffenen NAD](#)

[Phase 2: Stellen Sie sicher, dass SNMP auf dem betroffenen NAD-Client des Netzwerkzugriffsgeräts ausgeführt wird.](#)

[Schritt 3: Stellen Sie sicher, dass die SNMP-Version und der SNMP Community String oder das SNMP Auth/Privacy Protocol-Kennwort übereinstimmen, und zwar sowohl auf NAD als auch in der ISE.](#)

[Schritt 4: Überprüfung der Erreichbarkeit und der erforderlichen UDP-Ports \(161.162\) zwischen ISE PSN und NAD-Client](#)

[Ursache](#)

[Verwandte Inhalte](#)

- [Problem](#)
 - [Umwelt](#)
 - [Auflösung](#)
 - [Schritt 1: Identifizierung der betroffenen NAD](#)
 - [Phase 2: Stellen Sie sicher, dass SNMP auf dem betroffenen NAD-Client des Netzwerkzugriffsgeräts ausgeführt wird.](#)
 - [Schritt 3: Stellen Sie sicher, dass die SNMP-Version und der SNMP Community String oder das SNMP Auth/Privacy Protocol-Kennwort übereinstimmen, und zwar sowohl auf NAD als auch in der ISE.](#)
 - [Schritt 4: Überprüfung der Erreichbarkeit und der erforderlichen UDP-Ports \(161.162\) zwischen ISE PSN und NAD-Client](#)
 - [Ursache](#)
 - [Verwandte Inhalte](#)
-

Problem

Beim Überprüfen von Warnmeldungen in der ISE wird folgender SNMP-Profiler-Fehler angezeigt:

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

Umwelt

- Cisco Identity Services Engine (ISE) Version 3.0.0 und höher
- ISE-Profilerstellungsdienst aktiviert
- Netzwerkzugriffsgeräte (Network Access Devices, NADs), die für die SNMP-Kommunikation konfiguriert sind

Auflösung

Schritt 1: Identifizierung der betroffenen NAD

1. Navigieren Sie zu Dashboard > Alarme
2. Überprüfen Sie die Alarmdetails, und notieren Sie sich den betroffenen NAD-Gerätenamen oder die IP-Adresse.
3. Sie können die spezifische IP-Adresse des NAD-Clients ermitteln, indem Sie in der Fehlermeldung "Profiler SNMP Request Failure" (SNMP-Anforderungsfehler des Profilers) auf das Feld "NAD Address" (NAD-Adresse) verweisen.

Phase 2: Stellen Sie sicher, dass SNMP auf dem betroffenen NAD-Client des Netzwerkzugriffsgeräts ausgeführt wird.

Melden Sie sich bei der CLI des NAD-Clients an, und führen Sie diesen Befehl aus, um zu überprüfen, ob die SNMP-Funktion aktiviert ist.

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

Beispiel für 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
```

Beispiel für SNMP v2c:

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

Schritt 3: Stellen Sie sicher, dass die SNMP-Version und der SNMP Community String oder das SNMP Auth/Privacy Protocol-Kennwort übereinstimmen, und zwar sowohl auf NAD als auch in der ISE.

Überprüfen Sie Ihre SNMP v2c-Konfiguration mit den folgenden Schritten:

1. Melden Sie sich bei der NAD-Client-CLI an, und führen Sie den Befehl "show snmp community" aus.

Switch-Ausgabe:

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

2. Auf der ISE: Navigieren Sie zu Administration > Network Resources > Network Devices.
3. Bearbeiten Sie den identifizierten NAD-Eintrag, um sicherzustellen, dass der SNMP Community String und die SNMP-Version mit der Ausgabe von "show snmp community" übereinstimmen.

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	▼

Der Switch tarnt SNMP v3-Auth-/Datenschutzkennwörter. Um sicherzustellen, dass die Anmeldeinformationen korrekt sind, geben Sie sie wie folgt erneut ein:

1. Melden Sie sich bei der ISE-GUI an.
2. Navigieren Sie zu Administration > Network Resources > Network Devices.
3. Bearbeiten Sie den angegebenen NAD-Eintrag, und wechseln Sie zu den SNMP-Einstellungen. Klicken Sie auf "Show" (Anzeigen) unter Auth Password (Authentifizierungs- und Datenschutzkennwort). Sie können das Passwort dafür offen legen.

☒ **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. Melden Sie sich bei der Switch-CLI an.

- Führen Sie den Befehl `configure terminal` aus.
- Führen Sie anschließend diesen Befehl aus, um die SNMP v3-Anmeldeinformationen auf dem Switch zu aktualisieren.

Switch-Befehl:

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

Beispiel:

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

Schritt 4: Überprüfung der Erreichbarkeit und der erforderlichen UDP-Ports (161.162) zwischen ISE PSN und NAD-Client

1. Führen Sie einen Ping-Test vom profilerfähigen PSN-Knoten zum NAD-Client durch.
2. Führen Sie einen Ping-Test vom NAD-Client zum PSN-Knoten durch.
3. Stellen Sie sicher, dass die Ports 161 und 162 zwischen dem PSN-Knoten und NAD offen sind.
 - Testen Sie, ob die Ports 161 und 162 offen sind, indem Sie Telnet vom NAD-Client zum Knoten verwenden, der für den Profiler aktiviert ist.

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

Ursache

Der Alarm "SNMP Request Failure" wird ausgelöst, wenn die ISE das Netzwerkzugriffsgerät nicht erfolgreich abfragt. Dies wird in der Regel durch Konfigurationsdiskrepanzen in Bezug auf SNMP-Community-Strings, Versionen oder v3-Anmeldedaten zwischen den beiden Geräten verursacht. Darüber hinaus verhindern Netzwerkprobleme wie Firewalls, die die UDP-Ports 161 oder 162 blockieren, oder fehlende SNMP-Serverkonfigurationen im NAD häufig eine erfolgreiche Kommunikation.

Verwandte Inhalte

[Zulassen der erforderlichen ISE-Ports und FQDNs im Netzwerk](#)

[ISE-Profilerstellungsleitfaden](#)

[Konfigurieren von SNMP Community Strings](#)

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.