

Problemen oplossen met de ISE Alarm Error “Profiler SNMP Request Failure: Server= NAD Address= Error Message=Request timed out”

Inhoud

[uitgifte](#)

[milieu](#)

[resolutie](#)

[Stap 1: Identificeer getroffen NAD.](#)

[Stap 2: Controleer of de SNMP wordt uitgevoerd op de betreffende NAD-client van het netwerktoegangsapparaat](#)

[Stap 3: Zorg ervoor dat de SNMP-versie en SNMP-community string of SNMP Auth/Privacy Protocol Password overeenkomen, zowel op de NAD als in ISE](#)

[Stap 4: Valideer de bereikbaarheid en vereiste UDP-poorten \(161,162\) tussen ISE PSN- en NAD-client](#)

[Oorzaak](#)

[Gerelateerde inhoud](#)

- [uitgifte](#)
 - [milieu](#)
 - [resolutie](#)
 - [Stap 1: Identificeer getroffen NAD.](#)
 - [Stap 2: Controleer of de SNMP wordt uitgevoerd op de betreffende NAD-client van het netwerktoegangsapparaat](#)
 - [Stap 3: Zorg ervoor dat de SNMP-versie en SNMP-community string of SNMP Auth/Privacy Protocol Password overeenkomen, zowel op de NAD als in ISE](#)
 - [Stap 4: Valideer de bereikbaarheid en vereiste UDP-poorten \(161,162\) tussen ISE PSN- en NAD-client](#)
 - [Oorzaak](#)
 - [Gerelateerde inhoud](#)
-

uitgifte

Tijdens het bekijken van alarmen in ISE ziet u deze SNMP-profielfout:

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

milieu

- Cisco Identity Services Engine (ISE) versie 3.0.0 en hoger
- ISE-profileringservice ingeschakeld
- Network Access Devices (NAD's) geconfigureerd voor SNMP-communicatie

resolutie

Stap 1: Identificeer getroffen NAD.

1. Navigeer naar Dashboard > Alarmen
2. Controleer de alarmgegevens en noteer de naam of het IP van het betreffende NAD-apparaat.
3. U kunt het specifieke IP-adres van de NAD-client identificeren door te verwijzen naar het veld "NAD-adres" in het foutbericht "Profiler SNMP-aanvraag mislukt".

Stap 2: Controleer of de SNMP wordt uitgevoerd op de betreffende NAD-client van het netwerktoegangsapparaat

Meld u aan bij de CLI van de NAD-client en voer deze opdracht uit om te controleren of de SNMP-functie is ingeschakeld.

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

Voorbeeld 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
```

Voorbeeld SNMP v2c:

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

Stap 3: Zorg ervoor dat de SNMP-versie en SNMP-community string of SNMP Auth/Privacy Protocol Password overeenkomen, zowel op de NAD als in ISE

Valideer uw SNMP v2c-configuratie met de volgende stappen:

1. Meld u aan bij de NAD client CLI en voer de opdracht "show snmp community" uit.

Switch-uitgang:

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

2. Op ISE: Navigeer naar Beheer > Netwerkbronnen > Netwerkapparaten.
3. Bewerk het geïdentificeerde NAD-item om ervoor te zorgen dat de SNMP-community-string en SNMP-versie overeenkomen met de uitvoer van "snmp-community weergeven".

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	▾

De switch maskeert SNMP v3 Auth/Privacy-wachtwoorden. Om ervoor te zorgen dat deze referenties accuraat blijven, voert u ze opnieuw in via de stappen:

1. Log in op de ISE GUI.
2. Ga naar Beheer > Netwerkbronnen > Netwerkkapparaten.
3. Bewerk het geïdentificeerde NAD-item en ga naar de SNMP-instellingen. Door te klikken op de 'Show' op het Auth Password en Privacy Password. Je kunt het wachtwoord hiervoor onthullen.

☒ **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. Log in op de Switch CLI.

- Voer de opdracht Terminal configureren uit.
- Voer vervolgens deze opdracht uit om de SNMP v3-referenties op de switch bij te werken.

Switch, opdracht:

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

Voorbeeld:

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

Stap 4: Valideer de bereikbaarheid en vereiste UDP-poorten (161.162) tussen ISE PSN- en NAD-client

1. Voer een ping-test uit van de PSN-node met Profiler naar de NAD-client.
2. Voer een ping-test uit van de NAD-client naar de PSN-node.
3. Zorg ervoor dat poorten 161 en 162 open zijn tussen de PSN-node en NAD.
 - Test het gebruik van telnet van de NAD-client naar de node met Profiler om te bevestigen dat poorten 161 en 162 open zijn.

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

Oorzaak

Het alarm voor het mislukken van de SNMP-aanvraag treedt op wanneer ISE er niet in slaagt het netwerktoegangsapparaat te bevragen. Dit wordt meestal veroorzaakt door configuratie mismatches met betrekking tot SNMP community strings, versies of v3 referenties tussen de twee apparaten. Bovendien verhinderen netwerkproblemen, zoals firewalls die UDP-poorten 161 of 162 blokkeren of ontbrekende SNMP-serverconfiguraties op de NAD, vaak succesvolle communicatie.

Gerelateerde inhoud

[De vereiste ISE-poorten en FQDN's op het netwerk toestaan](#)

[ISE Profiling Design Guide](#)

[SNMP-communitystrings configureren](#)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.