

ISE integreren met Prime Infrastructure voor zichtbaarheid van eindpunten

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Configureren](#)

[Netwerkdigram](#)

[Configuraties](#)

[Switchconfiguratie](#)

[Configuratie Cisco Prime Infrastructure](#)

[Eindpuntconfiguratie](#)

[Verifiëren](#)

[ISE verifiëren](#)

[Controleer de NAD](#)

[Primaire infrastructuur verifiëren](#)

[Problemen oplossen](#)

Inleiding

In dit document wordt beschreven hoe ISE kan worden geïntegreerd met Prime Infrastructure om zichtbaarheid te krijgen voor geverifieerde eindpunten.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco ISE.
- Cisco Prime Infrastructure.
- Draadloze of bekabelde AAA-stroom voor eindpunten die zich verifiëren tegen ISE.
- SNMP-configuratie op NAD's (Network Access Devices) zoals Switches en WLC's.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

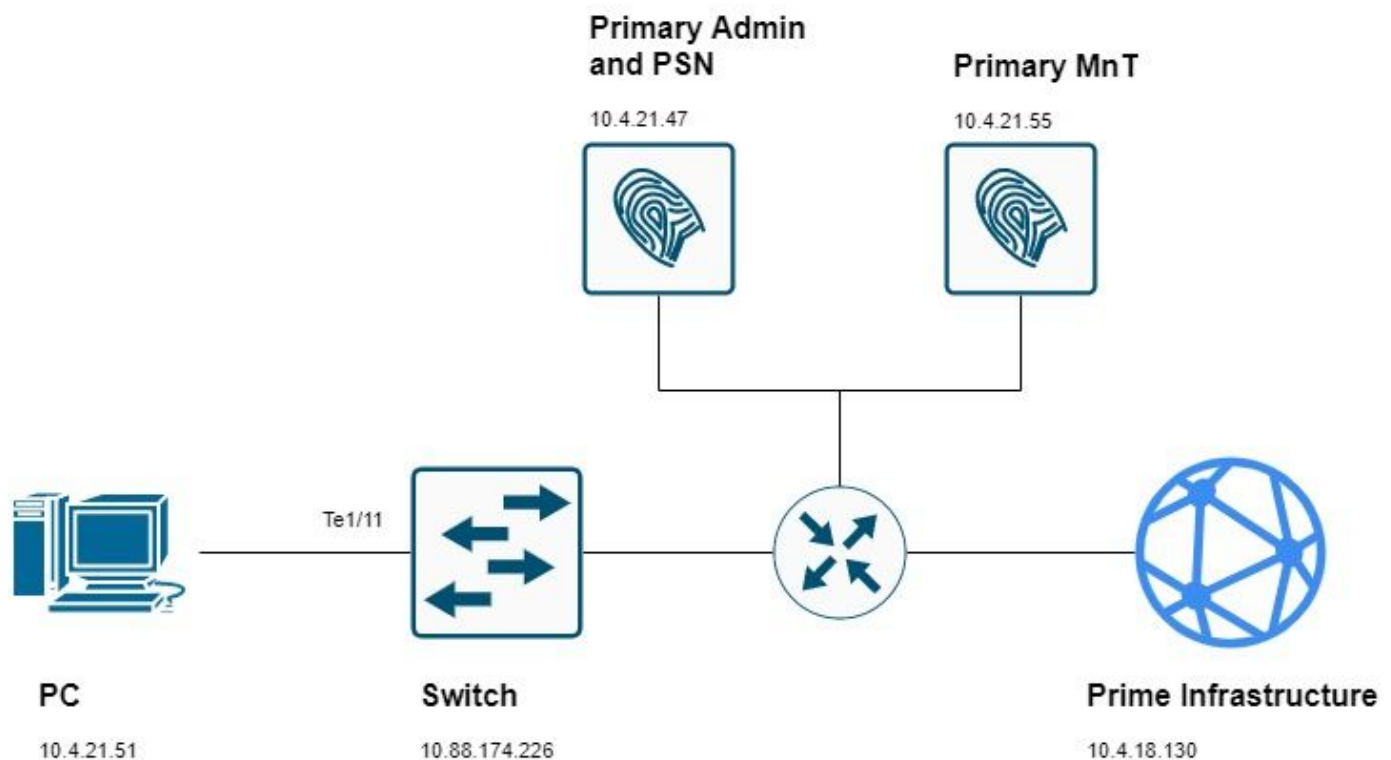
- ISE 3.1-implementatie.
- Cisco Prime Infrastructure 3.8.

- C6816-X-LE met Cisco IOS® 15.5.
- Windows 10-systeem.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Configureren

Netwerkdigram



Configuraties

Switchconfiguratie

1. Configureer het netwerktoegangsapparaat (NAD) voor AAA-verificatie tegen ISE. In deze handleiding gebruikt u deze configuratie:

```

aaa new-model

radius server ise31
address ipv4 10.4.21.47 auth-port 1812 acct-port 1813
key Cisc0123

aaa server radius dynamic-author
client 10.4.21.47 server-key Cisc0123
  
```

```
aaa group server radius ISE
  server name ise31

aaa authentication dot1x default group ISE
aaa authorization network default group ISE
aaa accounting dot1x default start-stop group ISE

dot1x system-auth-control
```

2. Configureer Device Tracking in de switch:

```
device-tracking policy DT1
  tracking enable

device-tracking tracking auto-source
```

3. Configureer de switchport voor dot1x-verificatie en koppel het apparaattraceringsbeleid eraan:

```
interface TenGigabitEthernet1/11
  device-tracking attach-policy DT1
  authentication host-mode multi-domain
  authentication order dot1x mab webauth
  authentication priority dot1x mab webauth
  authentication port-control auto
  mab
  dot1x pae authenticator
```

4. Configureer RO SNMP-community en SNMP-traps om aan uw netwerkvereisten te voldoen (optioneel kunt u de RW-community configureren):

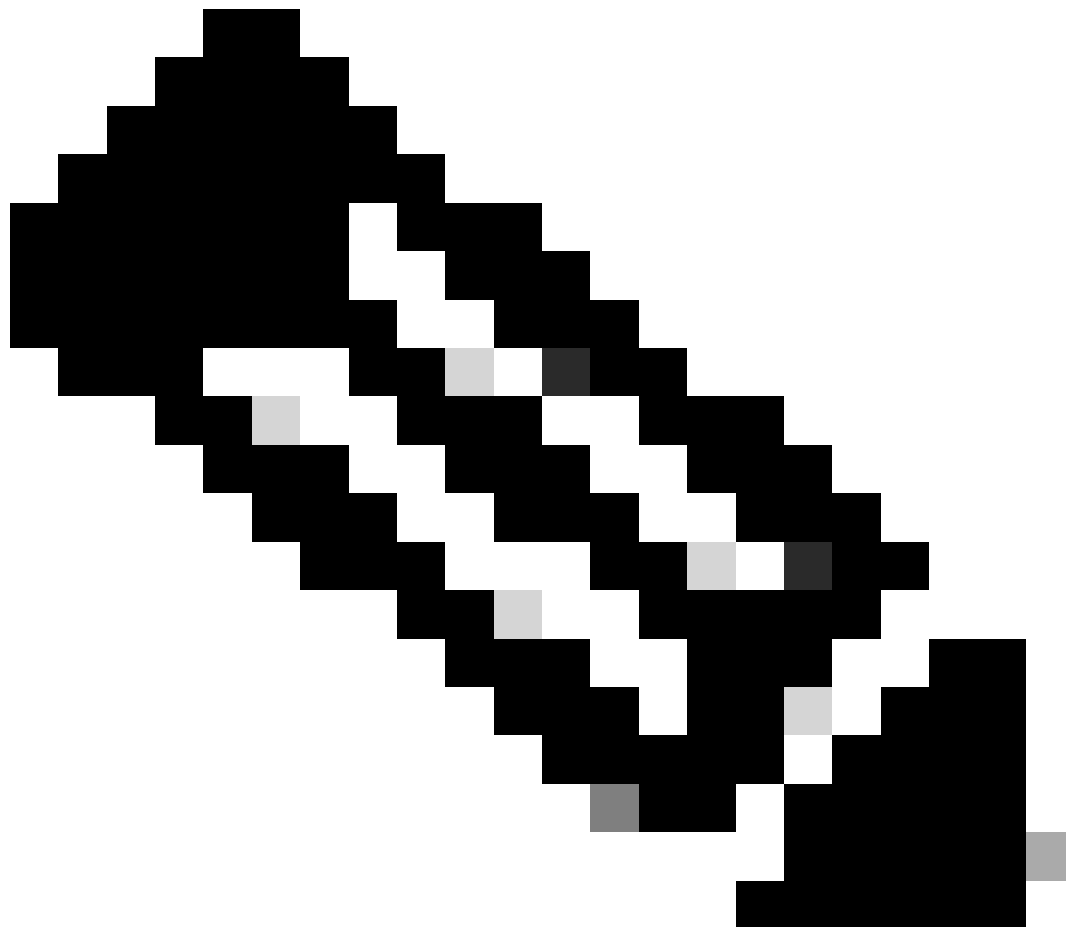
```
snmp-server community public RO
snmp-server community private RW
snmp-server trap-source TenGigabitEthernet1/16
snmp-server source-interface informs TenGigabitEthernet1/16
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps aaa_server
snmp-server enable traps trustsec authz-file-error
snmp-server enable traps auth-framework sec-violation
snmp-server enable traps port-security
snmp-server enable traps event-manager
snmp-server enable traps errdisable
snmp-server enable traps mac-notification change move threshold
snmp-server host 10.4.18.130 version 2c public udp-port 161
```

5. Configureer een Telnet- of SSH-toegang zodat Prime het apparaat kan beheren:

```
username admin password 0 cisco!123
aaa authentication login default local
```

```
line vty 0 4
  transport input ssh
  login authentication default
```

6. (Optioneel) Voor SSH-verbindingen is een RSA-sleutel vereist. Als de NAD er geen heeft, gebruikt u deze stappen om het te genereren.

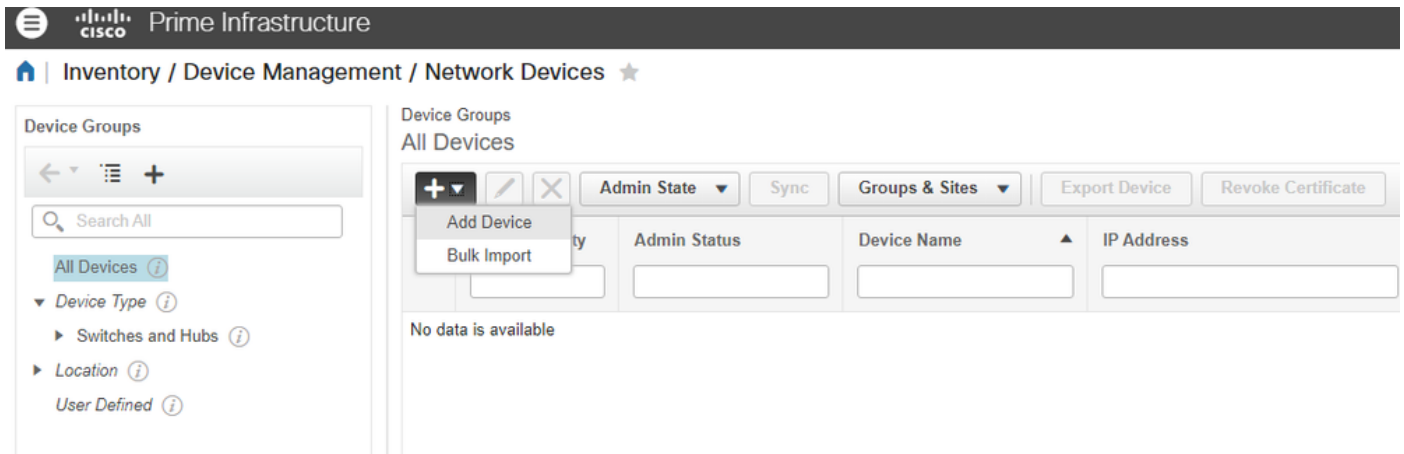


Opmerking: voor sommige apparaten is een geconfigureerd domein vereist voordat de RSA kan worden gegenereerd. Controleer of op uw apparaat een domein is geconfigureerd zodat u het bestaande domein niet overschrijft.

```
ip domain-name cisco.com
crypto key generate rsa
```

Configuratie Cisco Prime Infrastructure

7. Het netwerkkapparaat toevoegen in Voorraad > Apparaatbeheer > Netwerkkapparaten > Plusteken (+) > Apparaat toevoegen:



Verplichte velden om de inventaris te laten voltooien zijn:

Voor bekabelde apparaten:

- Algemeen: IP of DNS.
- SNMP: RO-community is vereist - zorg ervoor dat u deze ook in de Switch/WLC configureert.
- Telnet/SSH: Exec-modus en inschakelmodusreferenties.

Voor WLC:

- Algemeen: IP of DNS.
- SNMP: RO-community is vereist - zorg ervoor dat u deze ook in de Switch/WLC configureert.

In deze handleiding gebruikt u een Cisco-Switch:

i. Algemene afdeling:

Add Device



* General ✓

* SNMP

Telnet/SSH

HTTP/HTTPS

Civic Location

* General Parameters

☒ IP Address 10.88.174.226

☐ DNS Name

License Level Full ?

Credential Profile --Select-- ?

Device Role --Select-- ?

Add to Group --Select-- ?

Add

Verify Credentials

Cancel

ii. SNMP-sectie:

Add Device



* General ✓

* SNMP ✓

Telnet/SSH

HTTP/HTTPS

Civic Location

* SNMP Parameters

Version v2c

* SNMP Retries 2

* SNMP Timeout 10 (Secs)

* SNMP Port 161

* Read Community

* Confirm Read Community

Write Community

Confirm Write Community

Add

Verify Credentials

Cancel

iii. Telnet/SSH-sectie:

Edit Device

* General ✓

* SNMP ✓

Telnet/SSH ✓

HTTP/HTTPS

Civic Location

Telnet/SSH Parameters

Protocol **SSH2**

* CLI Port **22**

* Timeout **60** (Secs)

Username **admin**

Password

Confirm Password

Enable Password ?

Confirm Enable Password

* Note: Not providing Telnet/SSH credentials may result in partial collection of inventory data.

Update

Update & Sync

Verify Credentials

Cancel

8. Zodra alle vereiste velden zijn ingevuld, moet u ervoor zorgen dat Bereikbaarheid en Inzamelstatus zijn groen en voltooid respectievelijk:

Prime Infrastructure

Inventory / Device Management / Network Devices

Device Groups

All Devices

Reachability	Admin Status	Device Name	IP Address	DNS Name	Device Type	Last Inventory Collection Status
✓	Managed	MXC-TAC.M.07-6816-01.Iv...	10.88.174.226	10.88.174.226	Cisco Catalyst C6816-X-LE Fixe...	Completed

9. Prime integreren met ISE.

i. Navigeer naar Beheer > Servers > ISE-servers.

ii. Selecteer ISE Server toevoegen in het vervolgkeuzemenu en klik vervolgens op Go:

Prime Infrastructure

Administration / Servers / ISE Servers

None detected

-- Select a command --

-- Select a command --

Add ISE Server

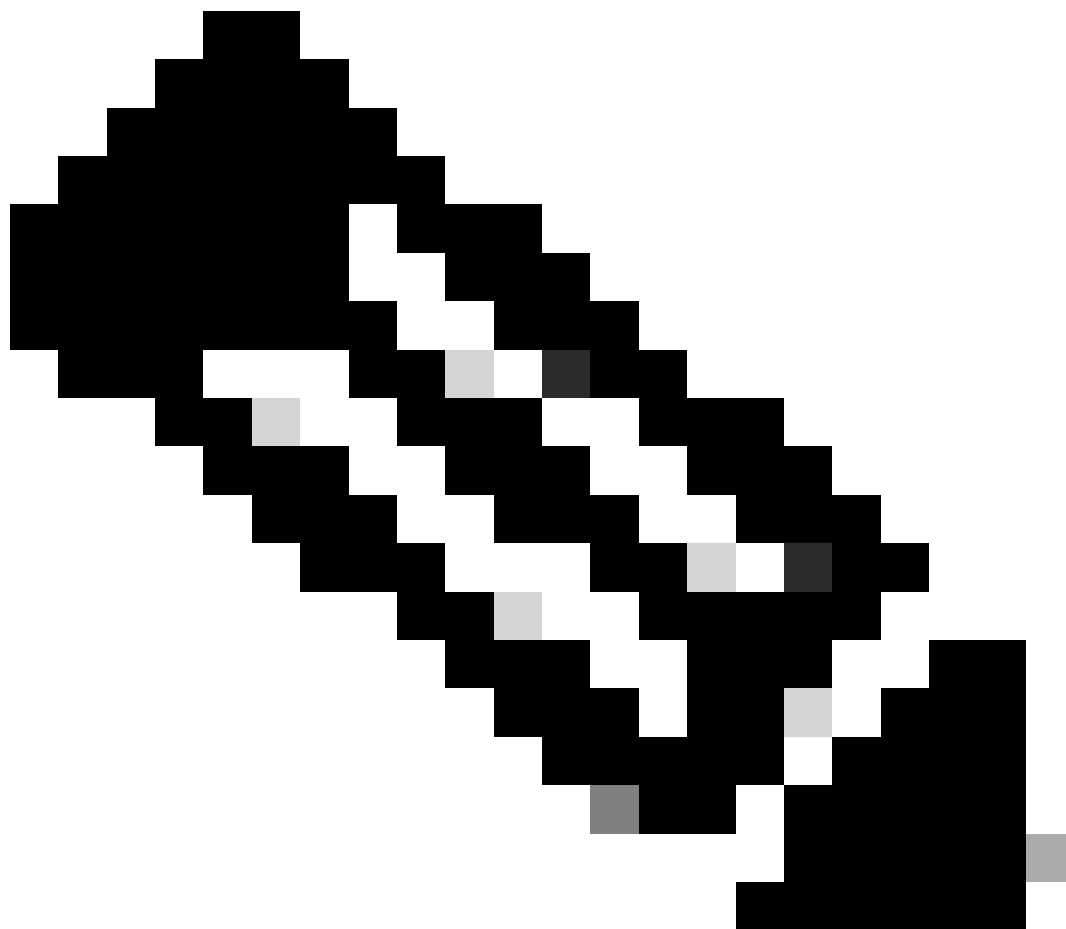
Delete ISE Server(s)

Go

iii. Vul alle velden in en klik op Opslaan.



Opmerking: De verbinding moet tot stand worden gebracht met de primaire en secundaire (indien van toepassing) ISE-bewakingsknooppunten.



Opmerking: De standaardpoort is ingesteld op 443, maar u kunt elke andere geopende poort in ISE gebruiken om de verbinding tot stand te brengen.


Prime Infrastructure

[Home](#) |
 [Administration](#) /
 [Servers](#) /
 [ISE Servers](#) /
 Add ISE Server
 

Server Address

Port

Username

Password

Confirm Password

HTTP Connection Timeout

(Max:300 secs)

iv. Navigeer terug naar de pagina ISE Server. De serverstatus zegt Bereikbaar en de rol wordt weergegeven (Standalone, Primary [MnT] of Secondary [MnT]):


Prime Infrastructure


3

roy - ROOT-DOMAIN


[Home](#) |
 [Administration](#) /
 [Servers](#) /
 [ISE Servers](#)


☐	Server Address	Port	Retries	Version	Status	Role
☐	10.4.21.55	443	1	3.1.0.518	Reachable	Primary

Eindpuntconfiguratie

10. Het eindpunt moet worden geconfigureerd om dot1x (RFC 3850)-verificatie uit te voeren. Dit kan worden bereikt door Cisco Network Access Manager (NAM) te configureren of gebruik te maken van de Native Supplicant van het besturingssysteem. Er zijn tal van handleidingen met betrekking tot deze configuratie, dus we nemen die stappen niet op in deze handleiding.

Verifiëren

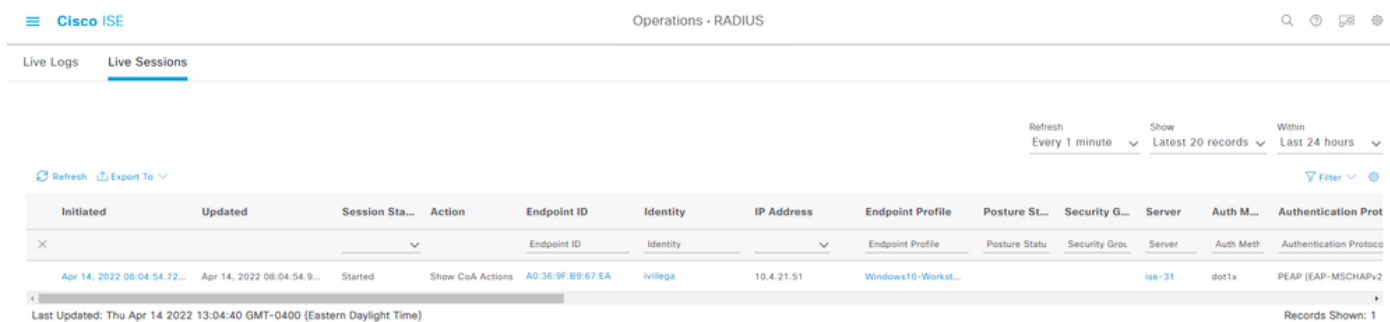
ISE verifiëren

ISE ontvangt het RADIUS-verzoek van het NAD en verifieert de gebruiker met succes.

De NAD wordt toegevoegd en geconfigureerd voor RADIUS in ISE > Beheer > Netwerkbronnen > Netwerkkapitalen.

1. Navigeer naar Bewerkingen > RADIUS > Live-sessies.

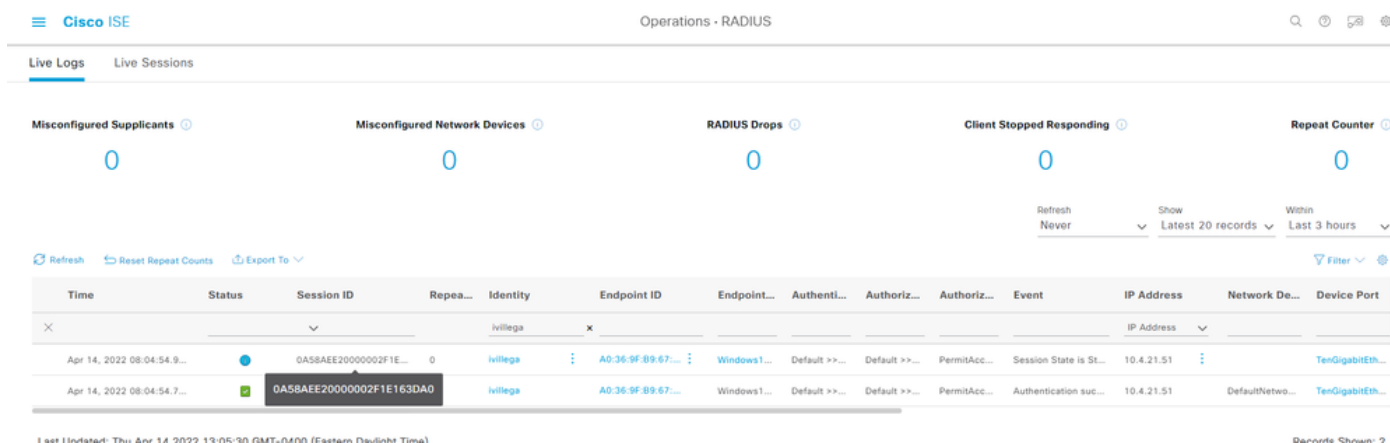
Zorg ervoor dat de live sessie van de gebruiker op deze pagina wordt weergegeven. De sessie-informatie wordt gedeeld met Prime Infrastructure.



The screenshot shows the 'Live Sessions' page in Cisco ISE. At the top, there are tabs for 'Live Logs' and 'Live Sessions', with 'Live Sessions' selected. Below the tabs, there are filters for 'Refresh' (Every 1 minute), 'Show' (Latest 20 records), and 'Within' (Last 24 hours). A table lists session details with columns: Initiated, Updated, Session Sta..., Action, Endpoint ID, Identity, IP Address, Endpoint Profile, Posture St..., Security G..., Server, Auth M..., and Authentication Prot. The first row shows a session initiated on Apr 14, 2022, at 08:04:54.72, with identity 'ivillega' and IP address '10.4.21.51'. The session is in a 'Started' state. Below the table, it says 'Last Updated: Thu Apr 14 2022 13:04:40 GMT-0400 (Eastern Daylight Time)' and 'Records Shown: 1'.

Initiated	Updated	Session Sta...	Action	Endpoint ID	Identity	IP Address	Endpoint Profile	Posture St...	Security G...	Server	Auth M...	Authentication Prot
Apr 14, 2022 08:04:54.72...	Apr 14, 2022 08:04:54.9...	Started	Show CoA Actions	A0:36:9F:B9:67:EA	ivillega	10.4.21.51	Windows10-Workst...			ise-31	dot1x	PEAP (EAP-MSCHAPv2)

2. Controleer de sessie-ID in Bewerkingen > RADIUS > Live-logs:



The screenshot shows the 'Live Logs' page in Cisco ISE. At the top, there are tabs for 'Live Logs' and 'Live Sessions', with 'Live Logs' selected. Below the tabs, there are five summary cards: 'Misconfigured Supplicants' (0), 'Misconfigured Network Devices' (0), 'RADIUS Drops' (0), 'Client Stopped Responding' (0), and 'Repeat Counter' (0). Below these cards, there are filters for 'Refresh' (Never), 'Show' (Latest 20 records), and 'Within' (Last 3 hours). A table lists log entries with columns: Time, Status, Session ID, Repea..., Identity, Endpoint ID, Endpoint..., Authenti..., Authoriz..., Authoriz..., Event, IP Address, Network De..., and Device Port. The first row shows a log entry at Apr 14, 2022, 08:04:54.9, with session ID '0A58AEE20000002F1E...' and identity 'ivillega'. The event is 'Session State is St...'. The second row shows a log entry at Apr 14, 2022, 08:04:54.7, with session ID '0A58AEE20000002F1E163DA0' and identity 'ivillega'. The event is 'Authentication suc...'. Below the table, it says 'Last Initiated: Thu Apr 14 2022 13:05:30 GMT-0400 (Eastern Daylight Time)' and 'Records Shown: 2'.

Time	Status	Session ID	Repea...	Identity	Endpoint ID	Endpoint...	Authenti...	Authoriz...	Authoriz...	Event	IP Address	Network De...	Device Port
Apr 14, 2022 08:04:54.9...		0A58AEE20000002F1E...	0	ivillega	A0:36:9F:B9:67:EA	Windows1...	Default >>...	Default >>...	PermitAcc...	Session State is St...	10.4.21.51		TenGigabitEth...
Apr 14, 2022 08:04:54.7...		0A58AEE20000002F1E163DA0		ivillega	A0:36:9F:B9:67:EA	Windows1...	Default >>...	Default >>...	PermitAcc...	Authentication suc...	10.4.21.51	DefaultNetwo...	TenGigabitEth...

Controleer de NAD

3. Controleer de sessiegegevens in het NAD. De sessie-ID komt overeen met de sessie-ID in ISE:

```
MXC.TAC.M.07-6816-01#show authentication session int Te1/11 detail
```

```
Interface: TenGigabitEthernet1/11
```

```
MAC Address: a036.9fb9.67ea
```

```
IPv6 Address: Unknown
```

```
IPv4 Address: 10.4.21.51
```

```
User-Name: ivillega
```

```
Status: Authorized
```

```
Domain: DATA
```

```
Oper host mode: multi-domain
```

```
Oper control dir: both
```

```
Session timeout: N/A
```

```
Common Session ID: 0A58AEE20000002F1E163DA0
```

```
Acct Session ID: 0x00000023
```

```
Handle: 0xD9000001
```

```
Current Policy: POLICY_Te1/11
```

```
Method status list:
```

```
Method      State
```

```
dot1x       Authc Success
```

Primaire infrastructuur verifiëren

4. Navigeer naar Monitor > Monitoring Tools > Clients and Users. Het MAC-adres van het eindpunt wordt weergegeven:

Cisco Prime Infrastructure													
Monitor / Monitoring Tools / Clients and Users													
Troubleshoot Test Disable Remove More Track Clients Identify Unknown Users													
	MAC Address	IP Address	IP Type	User Name	Type	Vendor	Location	Device Name	Interface	Interfa...	VLAN	Protocol	Status
	a0:36:9f:b9:67:ea	10.4.21.51	IPv4	ivilega		Intel C...	Unknown	MXC.TAC.M.0...	TenGigabit...		0	802.3	Disassoci...
Apr 06, 2022, 12:35:29 PM													

5. Als u erop klikt, ziet u de sessiegegevens van de gebruiker en de ISE-serverinformatie:

Cisco Prime Infrastructure

Monitor / Monitoring Tools / Clients and Users / a0:36:9f:b9:67:ea

Test | Disa

OverviewISEEventsTroubleshoot and DebugLocation

Attributes

a0:36:9f:b9:67:ea

MXC.TAC.M.07-6816-01.ivilega.com

Client Attributes

General

User Nameivilega

MAC Addressa0:36:9f:b9:67:ea

IP Address10.4.21.51

VendorIntel Corporate

Endpoint TypeWindows10-Workstation

HostnameData Not Available

Media TypeWired

CDP Device IDData Not Available

Software VersionData Not Available

ModelData Not Available

UDIData Not Available

Session

StatusDisassociated

VLAN ID0

VLAN NameData Not Available

InterfaceTenGigabitEthernet1/11

Interface DescriptionData Not Available

Switch NameMXC.TAC.M.07-6816-01.ivil

Switch IP AddressData Not Available

Wired Speed1Gbps

On NetworkNo

Security

Authenticating ISEise-31

Authentication Method802.1X

Auth StatusAuthorization Succeeded

Authorization Profile NamePermitAccess

Posture StatusUnknown

TrustSec Security GroupData Not Available

Audit Session ID0A58AEE2000000B00026CA4

Windows AD DomainData Not Available

EAP TypeUnknown

Traffic

Last Accounting Time2022-Apr-07, 22:48:21 UTC

Bytes Tx/Rx0/0

6. Er is ook een tabblad met het label ISE om de sessiegebeurtenissen voor dit specifieke eindpunt op te halen. U kunt een tijdsbestek selecteren dat door Prime Infrastructure wordt gebruikt om gebeurtenissen op te halen uit ISE:

Cisco Prime Infrastructure

Monitor / Monitoring Tools / Clients and Users / a0:36:9f:b9:67:ea

Test | Disa

OverviewISEEventsTroubleshoot and DebugLocation

Last 5 Hours

Between 4/14/2022 13:06:59

And 4/14/2022 13:06:59

Submit

Authentication Records

Date	Status	Failure Reason	ISE
Apr 14, 2022 01:04 PM	Authentication Passed	None	ise-31
Apr 14, 2022 01:04 PM	Authentication Passed	None	ise-31

2 records

Problemen oplossen

1. De connectiviteit tussen ISE en Prime Infrastructure testen met pings. Als er geen connectiviteit is, kunt u traceroutes van ISE of PI gebruiken om het probleem op te sporen.
2. Controleer of de in stap 9 geconfigureerde poort is geopend in de ISE MnT-node (standaardpoort is 443):

```
ise-31-1/admin# show ports | include :443  
tcp: 0.0.0.0:80, 0.0.0.0:19444, 0.0.0.0:19001, 0.0.0.0:443
```

Als de poort in de uitvoer wordt vermeld, betekent dit dat ISE MnT de poort heeft geopend.

Als er geen uitvoer is of de poort niet wordt vermeld, betekent dit dat ISE MnT die poort heeft gesloten. In een dergelijk geval kunt u het proberen met een andere haven of een TAC-zaak openen met het ISE-team om te controleren waarom de haven niet wordt geopend.



Opmerking: de ISE MnT-node gebruikt slechts enkele poorten. Er is geen manier om poorten te openen in de ISE MnT-node die niet worden vermeld in de ISE-installatiehandleiding, sectie poortreferentie.

3. Test de in stap 9 geconfigureerde poort met Telnet van Prime-infrastructuur:

```
prime-testcom/admin# telnet 10.4.21.55 port 443
Trying 10.4.21.55...
Connected to 10.4.21.55.
```

Als de uitvoer van de telnet-test is verbonden met <ISE MnT IP/FQDN>, betekent dit dat de test succesvol was.

Als de uitvoer van de telnet-test vastloopt bij Proberen <ISE MnT IP/FQDN>, betekent dit dat de test is mislukt. Dit kan gerelateerd zijn aan ACL's in uw intermediaire netwerkapparaten of met

firewallregeln.

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.