Setup ISE 3.4 PAC-loze verificatie tussen ISE en NAD voor Trustsec

Inhoud

Inleiding

Voorwaarden

- Vereisten
- Gebruikte componenten

Informatie

Configureren

- Configuraties
  - Switchconfiguratie
  - ISE-configuratie

Verifiëren

Problemen oplossen

Inleiding

In het document wordt de initiële installatie beschreven voor configuratie zonder PAC tussen ISE- en NAD-clients voor het downloaden van Trustsec-omgevingsgegevens.

Voorwaarden

Vereisten

- Bekendheid met Cisco TrustSec als oplossing voor netwerkbeveiliging.
- Kennis van Identity Services Engine (ISE) voor het beheer van netwerkbeveiliging.
- Basiskennis van Extensible Authentication Protocol (EAP) als kader voor het transport van verificatiegegevens.

Gebruikte componenten

Identity Services Engine (ISE) release 3.4.x

Cisco IOS® 17.15.1 of hoger

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.

Informatie

In de modus zonder PAC is het beleid van TrustSec gemakkelijker te implementeren omdat er geen Protected Access Credential (PAC) voor nodig is, wat meestal nodig is voor beveiligde communicatie tussen apparaten en de Identity Services Engine (ISE). Deze benadering is met name gunstig in omgevingen met meerdere ISE-knooppunten. Als het primaire knooppunt offline gaat, kunnen apparaten automatisch switches naar een back-up zonder dat ze hun referenties opnieuw moeten instellen, waardoor onderbrekingen worden beperkt. Verificatie zonder PAC vereenvoudigt het proces, waardoor het schaalbaarder en gebruiksvriendelijker wordt, en ondersteunt moderne beveiligingsmethoden die zijn afgestemd op de beginselen van Zero Trust.

In deze modus beginnen apparaten met het verzenden van een verzoek met een gebruikersnaam en wachtwoord. De ISE reageert door een beveiligde sessie voor te stellen. Zodra deze sessie is ingesteld, biedt de ISE belangrijke informatie die nodig is voor een veilige communicatie. Dit omvat een sleutel voor veiligheid en details zoals serveridentiteit en timing. Deze informatie wordt gebruikt om een veilige en continue toegang tot de nodige beleidslijnen en gegevens te waarborgen.

Configureren

Configuraties

Switchconfiguratie

In dit document wordt de instelling voor PAC-loze verificatie geconfigureerd met de Cisco C9300-switch. Elke switch met versie 17.15.1 of hoger kan een PAC-loze verificatie uitvoeren met de Identity Services Engine (ISE).

Stap 1: Configureer de Radius-server en de radiusgroep op de switch onder de configuratiepoort van de switch.

Radiusserver:

```
radius server

 address ipv4

        auth-port 1812 acct-port 1813

 key
```

Radius-groep:

```
aaa group server radius trustsec
 server name
```

Stap 2: Breng de radiusservergroep aan cts vergunning en dot1x voor authentificatie met PAC-less in kaart.

CTS-toewijzing:

<#root>

```
cts authorization list
```

cts-mlist

```
   // cts-mlist is the name of the authorization list
```

Dot1x-verificatie:

<#root>

```
aaa authentication dot1x default group
```

```
aaa authorization network
```

cts-mlist

```
 group
```

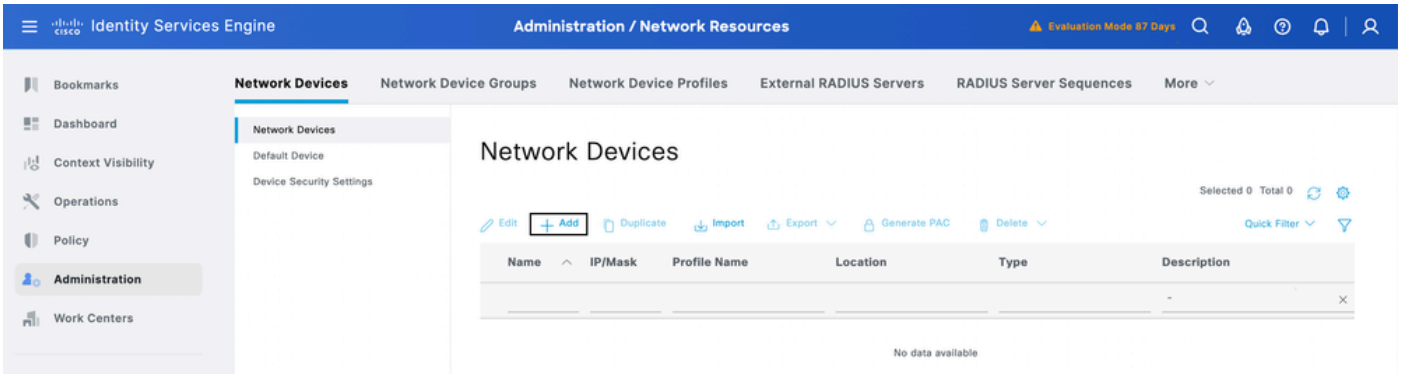
Stap 3: Configureer de CTS-ID en het wachtwoord onder de activeringsmodus van de switch

```
cts credentials id

        password
```

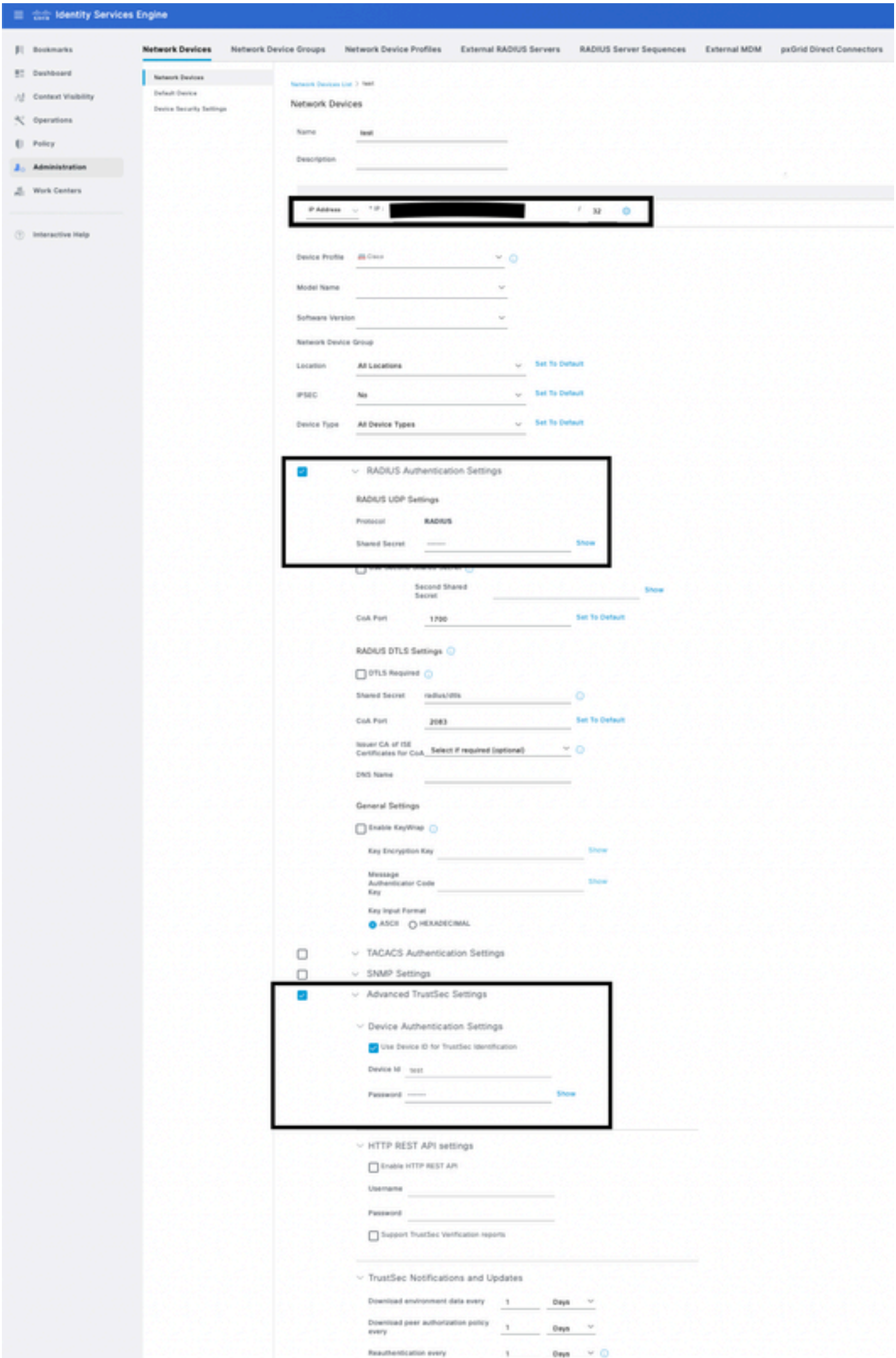
ISE-configuratie

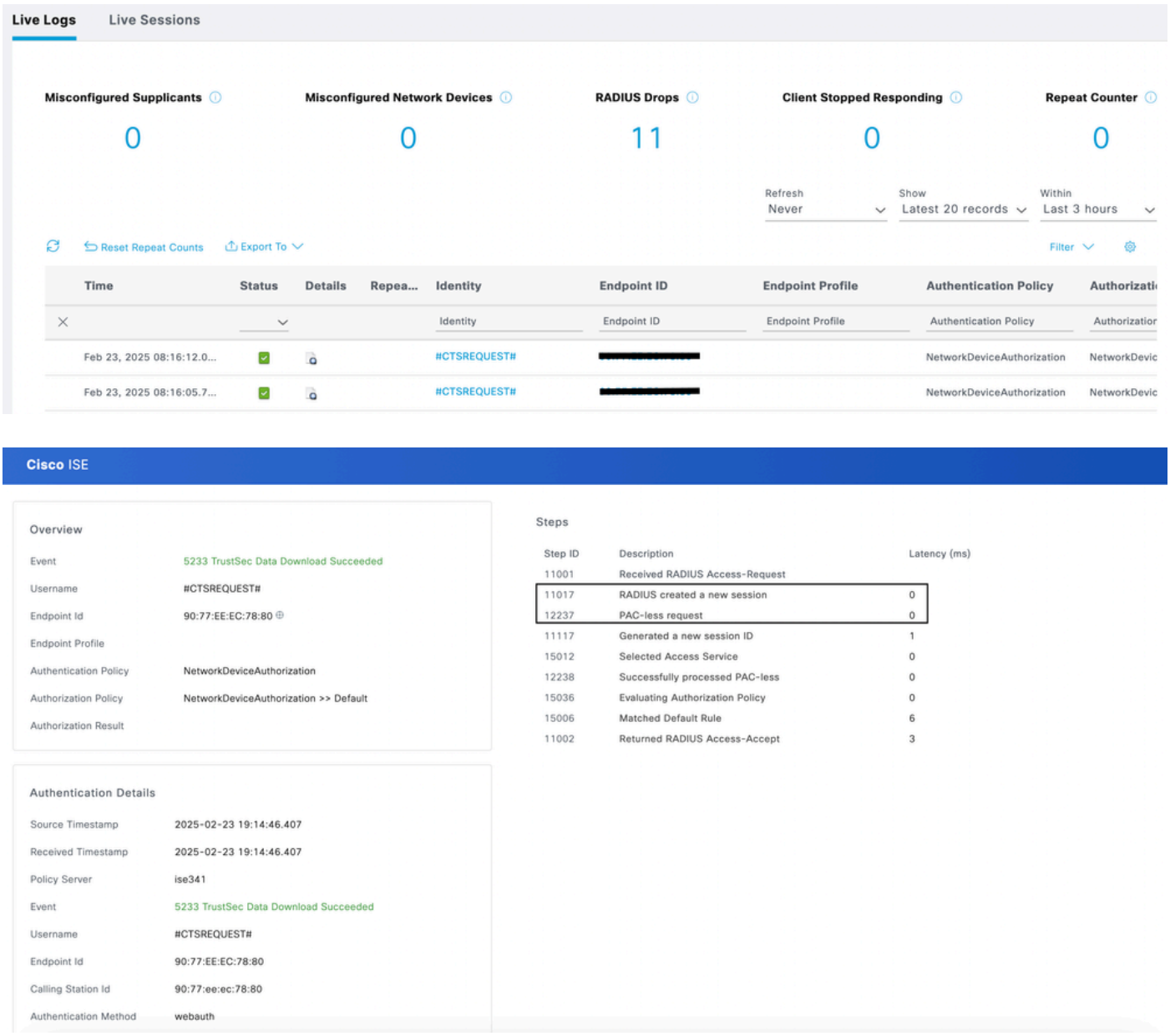
1. Configureer op ISE het netwerkapparaat onder Beheer > Netwerkbronnen > Netwerkapparaten > Netwerkapparaten. Klik op Add om de switch toe te voegen aan de ISE-server.



2. Voeg het NAD IP-adres toe in het veld IP-adres voor ISE om het radiusverzoek voor de trustsec-verificatie van de switch te verwerken.
3. Schakel Radius-verificatie-instellingen voor de NAD-client in en voer de gedeelde geheime sleutel Radius in.

4. Schakel Advanced Trustsec Settings in en update de apparaatnaam met CTS-ID en het wachtwoordveld met het wachtwoord vanuit de opdracht (cts referenties-id <CTS-ID>, wachtwoord <Password>).


Identity Services Engine
Bookmarks
Dashboard
Context Visibility
Operations
Policy
Administration
Work Centers
Interactive Help
Network Devices
Network Device Groups
Network Device Profiles
External RADIUS Servers
RADIUS Server Sequences
External MDM
pxGrid Direct Connectors
Network Devices
Default Device
Device Security Settings
Network Devices List > test
Network Devices
Name
test
Description
IP Address
[redacted]
32
Device Profile
Model Name
Software Version
Network Device Group
Location
All Locations
Set To Default
IPSEC
No
Set To Default
Device Type
All Device Types
Set To Default
RADIUS Authentication Settings
RADIUS UDP Settings
Protocol
RADIUS
Shared Secret
Show
Second Shared Secret
Show
CoA Port
1700
Set To Default
RADIUS DTLS Settings
DTLS Required
Shared Secret
radius/dtls
CoA Port
2083
Set To Default
Issuer CA of ISE Certificates for CoA
Select if required (optional)
DNS Name
General Settings
Enable KeyWrap
Key Encryption Key
Show
Message Authenticator Code Key
Show
Key Input Format
ASCII
HEXADECIMAL
TACACS Authentication Settings
SNMP Settings
Advanced TrustSec Settings
Device Authentication Settings
Use Device ID for TrustSec Identification
Device Id
test
Password
Show
HTTP REST API settings
Enable HTTP REST API
Username
Password
Support TrustSec Verification reports
TrustSec Notifications and Updates
Download environment data every
1
Days
Download peer authorization policy every
1
Days
Reauthentication every
1
Days



Problemen oplossen

Als u het probleem wilt oplossen, voert u deze debugs uit op de switch:

```
Debug Command:

debug cts environment-data all
debug cts env
debug cts aaa
debug radius
debug cts ifc events


debug cts authentication details
```

```
debug cts authorization all debug
```

Debug Snippet:

*23 feb. 14.48:14.974: CTS-env-gegevens: Omgeving forceren-gegevens verversen bitmasker 0x2

*23 feb. 14.48:14.974: CTS-env-gegevens: download transport-type = CTS_TRANSPORT_IP_UDP

*23 feb. 14.48:14.974: cts_env_data COMPLEET: tijdens staat env_data_complete, kreeg gebeurtenis 0(env_data_request)

*23 feb. 14.48:14.974: @@@ cts_env_data VOLTOOID: env_data_complete -> env_data_wait_rsp

*23 feb. 14.48:14.974: env_data_wait_rsp_enter: staat = WAITING_RESPONSE

*23 feb. 14.48:14.974: Secure Key is aanwezig op het apparaat, ga verder met pac-less env-data downloaden // start de PAC-less verificatie van switch

*23 feb. 14.48:14.974: cts_aaa_is_fragmented: (CTS env-data SM)NOT-FRAG attr_q(0)

*23 feb. 14.48:14.974: env_data_request_action: staat = WAITING_RESPONSE

*23 feb. 14.48:14.974: env_data_download_complete:

status (FALSE), req(x0), rec(x0)

*23 feb. 14.48:14.974: status (FALSE), req(x0), rec(x0), verwacht(x81),

wait_for_server_list(x85), wait_for_multicast_SGT(xB5), wait_for_SGName_mapping_tbl(x1485),

wait_for_SG-EPG_tbl(x18085), wait_for_default_EPG_tbl(xC0085), wait_for_default_SGT_tbl(x600085) wait_for_default_SERVICE_entry_tbl(xC000085)

*23 feb. 14.48:14.974: env_data_request_action: staat = WAITING_RESPONSE, ontvangen = 0x0 verzoek = 0x0

*23 feb. 14.48:14.974: cts_env_data_aaa_req_setup : aaa_id = 15

*23 feb. 14.48:14.974: cts_aaa_req_setup: (CTS env-data SM)Private groep lijkt DOOD, poging publieke groep

*23 feb. 14.48:14.974: cts_aaa_attr_add: AAA req (0x7AB57A6AA2C0)

*23 feb. 14.48:14.974: gebruikersnaam = #CTSREQUEST#

*23 feb. 14.48:14.974: AAA-context - kenmerk toevoegen: (CTS env-data SM)tr(test)

*23 feb. 14.48:14.974:   cts-milieu-gegevens = test

*23 feb. 14.48:14.974: cts_aaa_attr_add: AAA req (0x7AB57A6AA2C0)

*23 feb. 14.48:14.974: AAA-context - kenmerk toevoegen: (CTS env-data SM)tar(env-data-fragment)

*23 feb. 14.48:14.974:   cts-apparaat-mogelijkheid = env-data-fragment

*23 feb. 14.48:14.974: cts_aaa_attr_add: AAA req (0x7AB57A6AA2C0)

*23 feb. 14.48:14.975: AAA-context - kenmerk toevoegen: (CTS env-data SM)tar (ondersteuning voor meerdere servers-ip)

*23 feb. 14.48:14.975:   CT-apparaat-mogelijkheid = meerdere servers-ip-ondersteund

*23 feb. 14.48:14.975: cts_aaa_attr_add: AAA req (0x7AB57A6AA2C0)

*23 feb. 14.48:14.975: AAA-context - kenmerk toevoegen: (CTS env-data SM)tar (wnlx)

*23 feb. 14.48:14.975:   clid = wnlx

*23 feb. 14.48:14.975: cts_aaa_req_send: AAA req (0x7AB57A6AA2C0) met succes verzonden naar AAA.

*23 feb. 14.48:14.975: RADIUS/ENCODE (0000000F):Orig. component type = CTS

*23 feb. 14.48:14.975: RADIUS(0000000F): Config NAS IP: 0.0.0.0

*23 feb. 14.48:14.975: vrfid: [65535] ipv6-tabel : [0]

*23 feb. 14.48:14.975: idb is NULL

*23 feb. 14.48:14.975: RADIUS(0000000F): Config NAS IPv6: :

*23 feb. 14.48:14.975: RADIUS/ENCODE (0000000F): acct_sessie_id: 4003

*23 feb. 14.48:14.975: RADIUS(0000000F): verzenden

*23 feb. 14.48:14.975: RADIUS: PAC minder modus, geheim is aanwezig

*23 feb. 14.48:14.975: RADIUS: Toegevoegd met succes CTS pacless attribuut aan het radiusverzoek

*23 feb. 14.48:14.975: RADIUS/ENCODE: Beste lokale IP-adres 10.127.196.234 voor Radius-server 10.127.196.169

*23 feb. 14.48:14.975: RADIUS: PAC minder modus, geheim is aanwezig

*23 feb. 14.48:14.975: RADIUS(0000000F): Verzend toegangsaanvraag naar 10.127.196.169:1812 id 1645/11, len 249 // Radius access aanvraag van de switch

RADIUS: verificator 78 8A 70 5C E5 D3 DD F1 - B4 82 57 E2 1F 95 3B 92

*23 feb. 14.48:14.975: RADIUS: Gebruikersnaam [1] 14 "#CTSREQUEST#"

*23 feb. 14.48:14.975: RADIUS: Verkoper, Cisco [26] 33

*23 feb. 14.48:14.975: RADIUS: Cisco AV-paar [1] 27 "cts-environment-data=test"

*23 feb. 14.48:14.975: RADIUS: Verkoper, Cisco [26] 47

*23 feb. 14.48:14.975: RADIUS: Cisco AV-paar [1] 41 "cts-apparaat-mogelijkheid=env-data-fragment"

*23 feb. 14.48:14.975: RADIUS: Verkoper, Cisco [26] 58

*23 feb. 14.48:14.975: RADIUS: Cisco AV-paar [1] 52 "cts-apparaat-mogelijkheid=multiple-server-ip-ondersteund"

*23 feb. 14.48:14.975: RADIUS: Gebruikerswachtwoord [2] 18 *

*23 feb. 14.48:14.975: RADIUS: Bel-station-id [31] 8 "wnlx"

*23 feb. 14.48:14.975: RADIUS: Service-type [6] 6 uitgaand [5]

*23 feb. 14.48:14.975: RADIUS: NAS-IP-adres [4] 6.127.196.234

*23 feb. 14.48:14.975: RADIUS: Verkoper, Cisco [26] 39

*23 feb. 14.48:14.975: RADIUS: Cisco AV-paar [1] 33 "cts-pac-mogelijkheid=cts-pac-less" // CTS PAC Minder cv-paar attributen toevoegen aan het verzoek om ISE voor PAC-loze verificatie van het pakket

*23 feb. 14.48:14.975: RADIUS(0000000F): Een IPv4 Radius-pakket verzenden

*23 feb. 14.48:14.975: RADIUS(0000000F): Time-out 5 seconden gestart

*23 feb. 14.48:14.990: RADIUS: Ontvangen van ID 1645/11 10.127.196.169:1812, Access-Accept, len 313. // Verificatie geslaagd

RADIUS: verificator 92 4C 21 5C 99 28 64 8B - 23 06 4B 87 F6 FF 66 3C

*23 feb. 14.48:14.990: RADIUS: Gebruikersnaam [1] 14 "#CTSREQUEST#"

*23 feb. 14.48:14.990: RADIUS: Klasse [25] 78

RADIUS: 43 41 43 53 3A 30 61 37 66 34 61 39 54 37 68 [CACS:0a7fc4a9T7h]

RADIUS: 39 79 44 42 70 2F 7A 6A 64 66 56 49 55 74 4D [9YDBp/zjdffVIUtM]

RADIUS: 78 34 68 63 50 4C 4A 45 49 76 75 79 51 62 4C 70 [x4hcPLJEIvuyQbLp]

RADIUS: 31 48 7A 35 50 45 39 38 3A 69 73 65 33 34 31 2F [1Hz5PE98:ise341/]

RADIUS: 35 32 39 36 36 39 30 32 31 2F 32 31 [529669021/21]

*23 feb. 14.48:14.990: RADIUS: Verkoper, Cisco [26] 39

*23 feb. 14.48:14.990: RADIUS: Cisco AV-paar [1] 33 "cts-pac-mogelijkheid=cts-pac-zonder"

*23 feb. 14.48:14.990: RADIUS: Verkoper, Cisco [26] 43

*23 feb. 14.48:14.991: RADIUS: Cisco AV-paar [1] 37 "cts:server-list=CTServerList1-0001"

*23 feb. 14.48:14.991: RADIUS: Verkoper, Cisco [26] 38

*23 feb. 14.48:14.991: RADIUS: Cisco AV-paar [1] 32 "cts:security-group-tag=0002-00"

*23 feb. 14.48:14.991: RADIUS: Verkoper, Cisco [26] 41

*23 feb. 14.48:14.991: RADIUS: Cisco AV-paar [1] 35 "cts:environment-data-lapse=86400"

*23 feb. 14.48:14.991: RADIUS: Verkoper, Cisco [26] 40

*23 feb. 14.48:14.991: RADIUS: Cisco AV-paar [1] 34 "cts:security-group-table=0001-17"

*23 feb. 14.48:14.991: RADIUS: PAC minder modus, geheim is aanwezig

*23 feb. 14.48:14.991: RADIUS(0000000F): Ontvangen van ID 1645/11

*23 feb. 14.48:14.991: cts_aaa_callback: (CTS env-data SM)AAA req(0x7AB57A6AA2C0) respons succes

*23 feb. 14.48:14.991: AAA CTX FRAG SCHOON: (CTS env-data SM)tr(test)

*23 feb. 14.48:14.991: AAA CTX FRAG SCHOON: (CTS env-data SM)tar(env-data-fragment)

*23 feb. 14.48:14.991: AAA CTX FRAG SCHOON: (CTS env-data SM)tar (ondersteuning voor meerdere servers-ip)

*23 feb. 14.48:14.991: AAA CTX FRAG SCHOON: (CTS env-data SM)tar (wnlx)

*23 feb. 14.48:14.991: AAA-kanaal: Onbekend type (450).

*23 feb. 14.48:14.991: AAA-kanaal: Onbekend type (1324).

*23 feb. 14.48:14.991: AAA-kanaal: server-list = CTSserverList1-0001.

*23 feb. 14.48:14.991: Naam van ontvangen lijst. Zet cts_is_slist_send_to_binos_req op FALSE

*23 feb. 14.48:14.991: AAA-kanaal: veiligheidsgroep-tag = 0002-00.

*23 feb. 14.48:14.991: AAA-kanaal: omgevings-gegevens-vervaldatum = 86400.

*23 feb. 14.48:14.991: AAA-kanaal: security-group-table = 0001-17.CTS env-data: AAA-kenmerken ontvangen. // Het downloaden van de omgevingsgegevens

CTS_AAA_SLIST

Naam slist (CTSServerList1) ontvangen in 1st Access-Accept

Naam lijst (CTSServerList1) bestaat

CTS_AAA_SECURITY_GROUP_TAG

CTS_AAA_ENVIRONMENT_DATA_EXPXING = 86400.

CTS_AAA_SGT_NAME_LIST

tabel (0001) ontvangen in 1st Access-Accept

Tabel (0001) kopiëren van geïnstalleerd naar ontvangen omdat er geen wijzigingen zijn aangebracht.

nieuwe naam (0001), gen(17)

CTS_AAA_DATA_END

*23 feb. 14.48:14.991: cts_env_data WAITING_RESPONSE: tijdens staat env_data_wait_rsp, kreeg gebeurtenis 1(env_data_Received)

*23 feb. 14.48:14.991: @@@ cts_env_data WAITING_RESPONSE: env_data_wait_rsp -> env_data_assessment

*23 feb. 14.48:14.991: env_data_assessment_enter: toestand = BEOORDELING

*23 feb. 14.48:14.991: cts_aaa_is_fragmented: (CTS env-data SM)NOT-FRAG attr_q(0)

*23 feb. 14.48:14.991: env_data_assessment_action: toestand = BEOORDELING

*23 feb. 14.48:14.991: env_data_download_complete:

status (FALSE), req(x81), rec(xC87)

*23 feb. 14.48:14.991: Verwacht hetzelfde als ontvangen

*23 feb. 14.48:14.991: status (TRUE), req(x81), rec(xC87), verwacht(x81),

wait_for_server_list(x85), wait_for_multicast_SGT(xB5), wait_for_SGName_mapping_tbl(x1485),

wait_for_SG-EPG_tbl(x18085), wait_for_default_EPG_tbl(xC0085), wait_for_default_SGT_tbl(x600085) wait_for_default_SERVICE_entry_tbl(xC000085)

*23 feb. 14.48:14.991: cts_env_data ASSESSING: tijdens state env_data_assessment, kreeg event 4(env_data_complete)

*23 feb. 14.48:14.991: @@@ cts_env_data BEOORDELING: env_data_assessment -> env_data_complete

*23 feb. 14.48:14.991: env_data_complete_enter: staat = VOLLEDIG

*23 feb. 14.48:14.991: CTS-ifc-ev: env-gegevensrapportage naar kern, resultaat: Geslaagd

*23 feb. 14.48:14.991: env_data_install_action: staat = COMPLEET voltooid.types 0x0

*23 feb. 14.48:14.991: env_data_install_action: Geïnstalleerde sgt reinigen<->sgname-tabel

*23 feb. 14.48:14.991: De geïnstalleerde sg-pg-lijst opschonen

*23 feb. 14.48:14.991: De standaard epg-lijst opschonen

*23 feb. 14.48:14.991: env_data_install_action: mcast_sgt tabel bijgewerkt

*23 feb. 14.48:14.991: Env data sync voor standby status 2

*23 feb. 14.48:14.991: SLIST is hetzelfde als de vorige vernieuwing. Geen noodzaak om het naar BINOS te sturen

*23 feb. 14.48:14.991: CTS-sg-epg-events:instelling van default_sg 0 voor env data

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.