Einrichtung der Authentifizierung ohne ISE 3.4 PAC zwischen ISE und NAD für TrustSec

Inhalt

Einleitung

In diesem Dokument wird die Ersteinrichtung einer Konfiguration ohne PAC zwischen ISE- und NAD-Clients für den Download von Daten in einer TrustSec-Umgebung beschrieben.

Voraussetzungen

Anforderungen

- Vertrautheit mit Cisco TrustSec als Netzwerksicherheitslösung
- Kenntnisse der Identity Services Engine (ISE) zur Verwaltung der Netzwerksicherheit
- Grundlegendes Verständnis des Extensible Authentication Protocol (EAP) als Framework für die Übertragung von Authentifizierungsinformationen

Verwendete Komponenten

Identity Services Engine (ISE) Version 3.4.x

Cisco IOS® 17.15.1 oder höher

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Informationen

Im Modus ohne PAC sind TrustSec-Richtlinien einfacher zu implementieren, da sie keine Protected Access Credential (PAC) erfordern, die in der Regel für die sichere Kommunikation zwischen Geräten und der Identity Services Engine (ISE) benötigt wird. Dieser Ansatz ist insbesondere in Umgebungen mit mehreren ISE-Knoten von Vorteil. Wenn der Primärknoten offline geht, können Geräte automatisch zu einem Backup wechseln, ohne ihre Anmeldeinformationen wiederherstellen zu müssen, wodurch Unterbrechungen reduziert werden. Die Authentifizierung ohne PAC vereinfacht den Prozess, macht ihn skalierbarer und benutzerfreundlicher und unterstützt moderne Sicherheitsmethoden, die auf die Zero Trust-Prinzipien abgestimmt sind.

In diesem Modus senden Geräte zunächst eine Anforderung mit einem Benutzernamen und einem Kennwort. Die ISE reagiert, indem sie eine sichere Sitzung vorschlägt. Nach Einrichtung dieser Sitzung stellt die ISE wichtige Informationen bereit, die für eine sichere Kommunikation erforderlich sind. Dazu gehören ein Sicherheitsschlüssel und Details wie Serveridentität und Timing. Diese Informationen werden verwendet, um einen sicheren und kontinuierlichen Zugriff auf die erforderlichen Richtlinien und Daten sicherzustellen.

Konfigurieren

Konfigurationen

Switch-Konfiguration

In diesem Dokument wird die Einrichtung für eine Authentifizierung ohne PAC mit dem Cisco Switch C9300 konfiguriert. Jeder Switch mit Version 17.15.1 oder höher kann eine Authentifizierung ohne PAC mit der Identity Services Engine (ISE) durchführen.

Schritt 1: Konfigurieren Sie den Radius-Server und die RADIUS-Gruppe auf dem Switch unter dem Konfigurationsterminal des Switches.

Radius-Server:

```
radius server

 address ipv4

        auth-port 1812 acct-port 1813

 key
```

Radius-Gruppe:

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

Phase 2: Ordnen Sie die RADIUS-Servergruppe cts-Autorisierung und dot1x für die Authentifizierung ohne PAC zu.

CTS-Zuordnung:

<#root>

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

Dot1x-Authentifizierung:

<#root>

```
aaa authentication dot1x default group
```

```
aaa authorization network
cts-mlist
 group
```

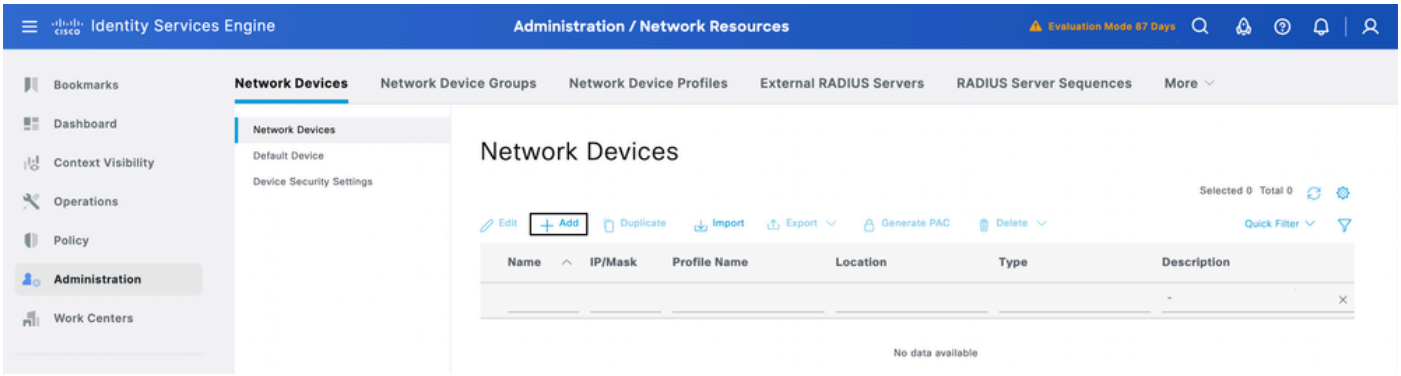
Schritt 3: Konfigurieren Sie die CTS-ID und das Kennwort im Aktivierungsmodus des Switches.

```
cts credentials id

        password
```

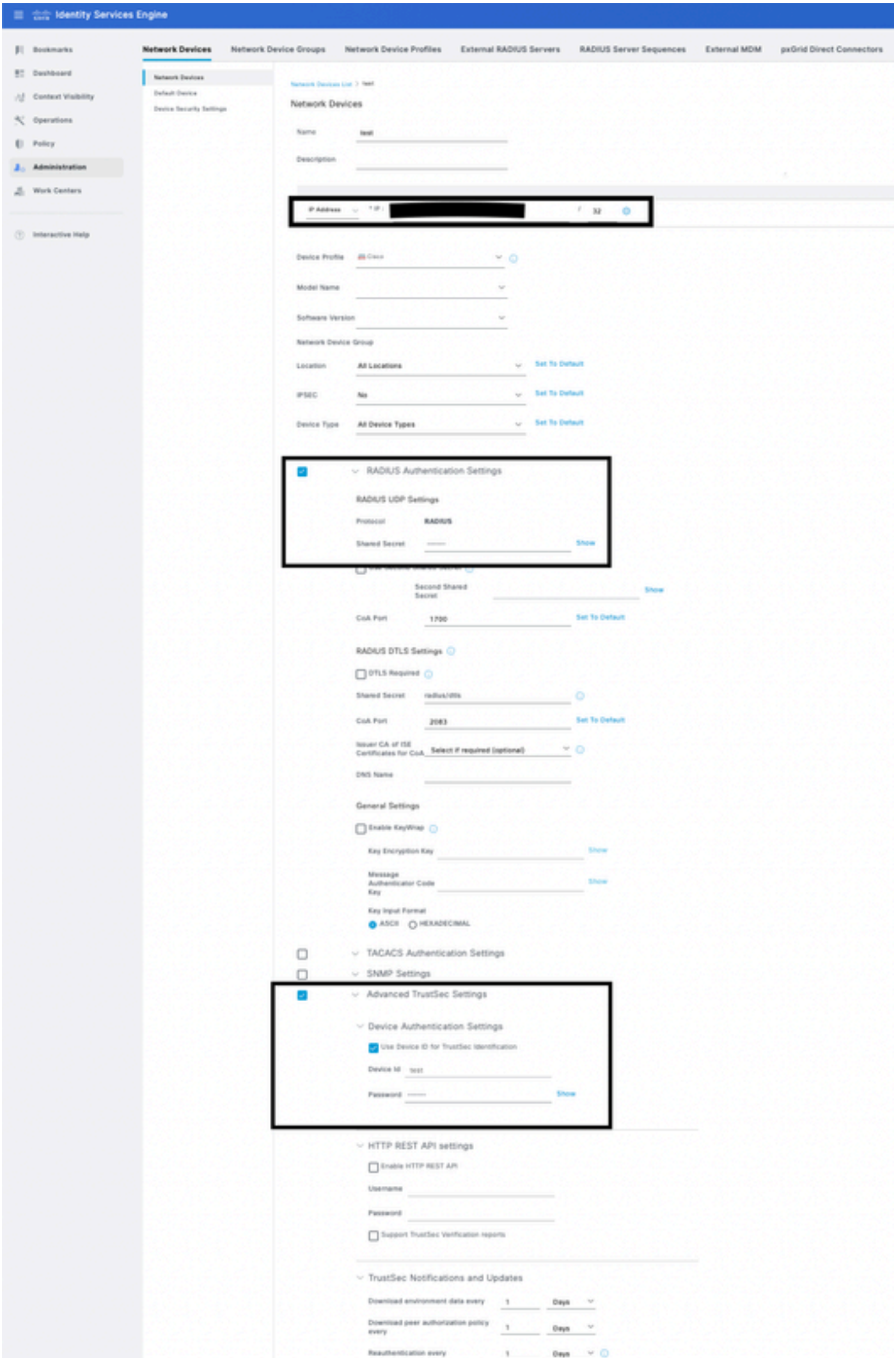
ISE-Konfiguration

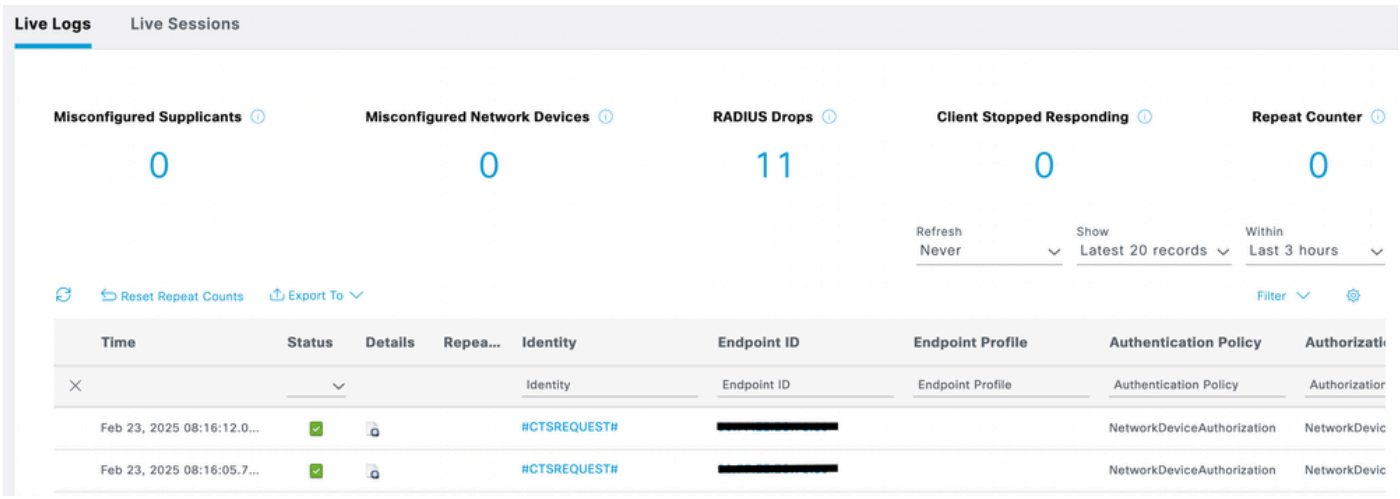
1. Konfigurieren Sie auf der ISE das Netzwerkgerät unter Administration > Network Resources > Network Devices > Network Devices. Klicken Sie auf Hinzufügen, um den Switch zum ISE-Server hinzuzufügen.

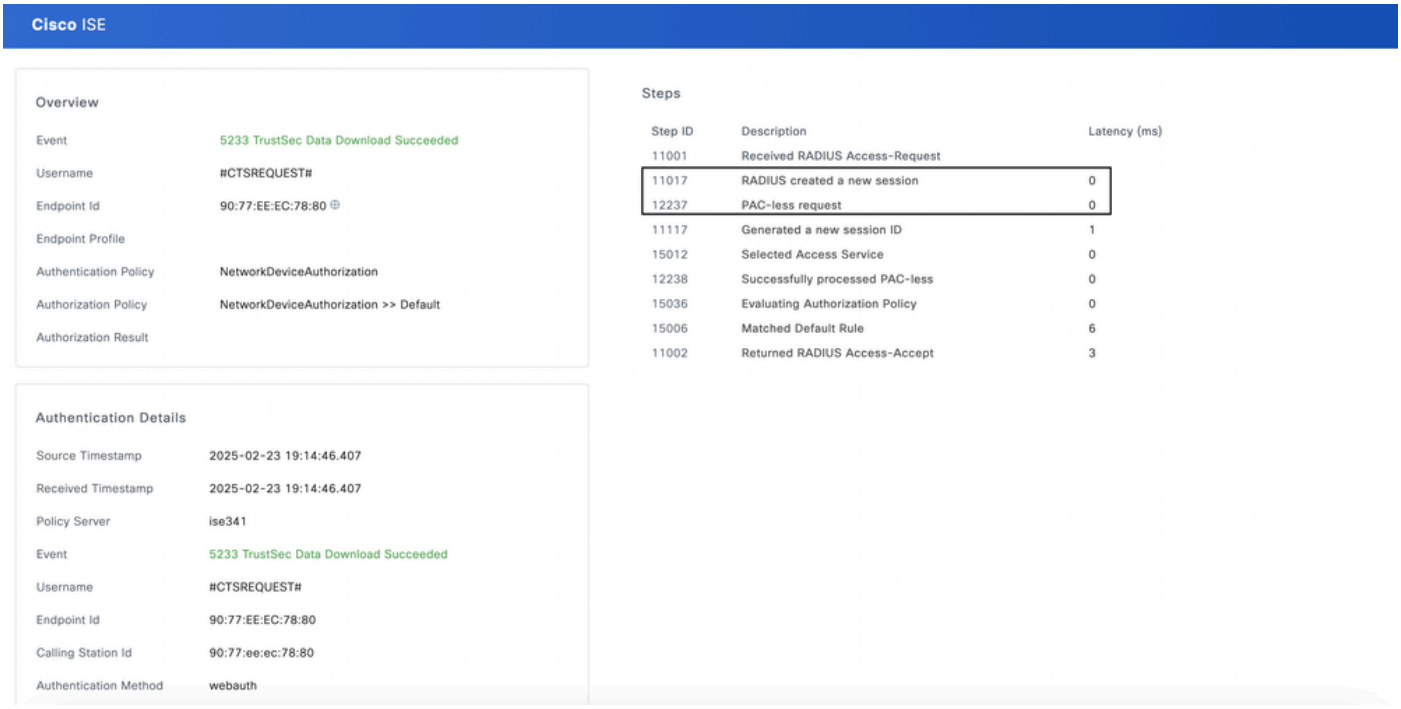


2. Fügen Sie die NAD-IP-Adresse im IP-Adressfeld für ISE hinzu, um die RADIUS-Anforderung für die TrustSec-Authentifizierung vom Switch zu verarbeiten.
3. Aktivieren Sie die Radius-Authentifizierungseinstellungen für den NAD-Client, und geben Sie den gemeinsamen geheimen Radius-Schlüssel ein.

4. Aktivieren Sie die erweiterten TrustSec-Einstellungen, und aktualisieren Sie den Gerätenamen mit CTS-ID und das Kennwortfeld mit dem Kennwort aus dem Befehl (cts dentials id <CTS-ID> password <Kennwort>).


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





Fehlerbehebung

Um das Problem zu beheben, führen Sie die folgenden Fehlerbehebungen auf dem Switch aus:

```
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
```

Debugausschnitt:

*23. Februar 14:48:14.974: CTS-Umgebungsdaten: Bitmaske zur Aktualisierung von Umgebungsdaten erzwingen 0x2

*23. Februar 14:48:14.974: CTS-Umgebungsdaten: Transporttyp herunterladen = CTS_TRANSPORT_IP_UDP

*23. Februar 14:48:14.974: cts_env_data ABGESCHLOSSEN: während Zustand env_data_complete, Ereignis 0 erhalten(env_data_request)

*23. Februar 14:48:14.974: @@ cts_env_data ABGESCHLOSSEN: env_data_complete -> env_data_waiting_rsp

*23. Februar 14:48:14.974: env_data_waiting_rsp_enter: state = WAITING_RESPONSE

*23. Februar 14:48:14.974: Secure Key ist auf dem Gerät vorhanden, fahren Sie mit pac-less env-data download // initiieren Sie die PAC-lose Authentifizierung vom Switch

*23. Februar 14:48:14.974: cts_aaa_is_fragmentiert: (CTS Env-Data SM)NOT-FRAG attr_q(0)

*23. Februar 14:48:14.974: env_data_request_action: state = WAITING_RESPONSE

*23. Februar 14:48:14.974: env_data_download_complete:

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

*23. Februar 14:48:14.974: status(FALSE), req(x0), rec(x0), wait(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. Februar 14:48:14.974: env_data_request_action: state = WAITING_RESPONSE, received = 0x0 request = 0x0

*23. Februar 14:48:14.974: cts_env_data_aaa_req_setup: aaa_id = 15

*23. Februar 14:48:14.974: cts_aaa_req_setup: (CTS env-data SM)Private Gruppe scheint DEAD, öffentliche Gruppe wird versucht

*23. Februar 14:48:14.974: cts_aaa_attr_add: AAA req(0x7AB57A6AA2C0)

*23. Februar 14:48:14.974: username = #CTSREQUEST#

*23. Februar 14:48:14.974: AAA-Kontext-Attribut hinzufügen: (CTS Env-Data SM)attr(Test)

*23. Februar 14:48:14.974: cts-environment-data = test

*23. Februar 14:48:14.974: cts_aaa_attr_add: AAA req(0x7AB57A6AA2C0)

*23. Februar 14:48:14.974: AAA-Kontext-Attribut hinzufügen: (CTS env-data SM)attr(env-data-fragment)

*23. Februar 14:48:14.974: cts-device-ability = env-data-fragment

*23. Februar 14:48:14.974: cts_aaa_attr_add: AAA req(0x7AB57A6AA2C0)

*23. Februar 14:48:14.975: AAA-Kontext-Attribut hinzufügen: (CTS Env-Data SM)attr(Unterstützung von mehreren Servern - IP)

*23. Februar 14:48:14.975: cts-device-ability = Multiple-Server-IP unterstützt

*23. Februar 14:48:14.975: cts_aaa_attr_add: AAA req(0x7AB57A6AA2C0)

*23. Februar 14:48:14.975: AAA-Kontext-Attribut hinzufügen: (CTS Env-Data SM)attr(wnlx)

*23. Februar 14:48:14.975: clid = wnlx

*23. Februar 14:48:14.975: cts_aaa_req_send: AAA req(0x7AB57A6AA2C0) erfolgreich an AAA gesendet.

*23. Februar 14:48:14.975: RADIUS/ENCODE(0000000F):Orig. Komponententyp = CTS

*23. Februar 14:48:14.975: RADIUS(0000000F): NAS-IP konfigurieren: 0.0.0.0

*23. Februar 14:48:14.975: vrfid: [65535] IPv6-Tabelle : [0]

*23. Februar 14:48:14.975: idb ist NULL

*23. Februar 14:48:14.975: RADIUS(0000000F): NAS-IPv6 konfigurieren: ::

*23. Februar 14:48:14.975: RADIUS/ENCODE(0000000F): acct_session_id: 4003

*23. Februar 14:48:14.975: RADIUS(0000000F): sendend

*23. Februar 14:48:14.975: RADIUS: Modus ohne PAC, geheim vorhanden

*23. Februar 14:48:14.975: RADIUS: Das CTS-Attribut "pacless" wurde der Radiusanforderung erfolgreich hinzugefügt.

*23. Februar 14:48:14.975: RADIUS/CODE: Beste lokale IP-Adresse 10.127.196.234 für Radius-Server 10.127.196.169

*23. Februar 14:48:14.975: RADIUS: Modus ohne PAC, geheim vorhanden

*23. Februar 14:48:14.975: RADIUS(0000000F): Senden Sie eine Zugriffsanfrage an

10.127.196.169:1812 id 1645/11, len 249 // Radius Access Request vom Switch.

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

*23. Februar 14:48:14.975: RADIUS: Benutzername [1] 14 "#CTSREQUEST#"

*23. Februar 14:48:14.975: RADIUS: Anbieter, Cisco [26] 33

*23. Februar 14:48:14.975: RADIUS: Cisco AVpair [1] 27"cts-environment-data=test"

*23. Februar 14:48:14.975: RADIUS: Anbieter, Cisco [26] 47

*23. Februar 14:48:14.975: RADIUS: Cisco AVpair [1] 41 "cts-device-ability=env-data-fragment"

*23. Februar 14:48:14.975: RADIUS: Anbieter, Cisco [26] 58

*23. Februar 14:48:14.975: RADIUS: Cisco AVpair [1] 52"cts-device-ability=multiple-server-ip-supported"

*23. Februar 14:48:14.975: RADIUS: Benutzerkennwort [2] 18 *

*23. Februar 14:48:14.975: RADIUS: Calling-Station-ID [31] 8 "wnlx"

*23. Februar 14:48:14.975: RADIUS: Servicetyp [6] 6 Ausgehend [5]

*23. Februar 14:48:14.975: RADIUS: NAS-IP-Adresse [4] 6 10.127.196.234

*23. Februar 14:48:14.975: RADIUS: Anbieter, Cisco [26] 39

*23. Februar 14:48:14.975: RADIUS: Cisco AVpair [1] 33 "cts-pac-ability=cts-pac-less" // CTS PAC Weniger cv-pair-Attribut für die Anfrage an ISE, das Paket für eine PAC-lose Authentifizierung zu verarbeiten

*23. Februar 14:48:14.975: RADIUS(0000000F): Senden eines IPv4-RADIUS-Pakets

*23. Februar 14:48:14.975: RADIUS(0000000F): Timeout nach 5 Sekunden gestartet

*23. Februar 14:48:14.990: RADIUS: Eingegangen von ID 1645/11 10.127.196.169:1812, Access-Accept, len 313. // Authentication Success

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

*23. Februar 14:48:14.990: RADIUS: Benutzername [1] 14 "#CTSREQUEST#"

*23. Februar 14:48:14.990: RADIUS: Klasse [25] 78

RADIUS: 43 41 43 53 3A 30 61 37 66 63 34 61 39 54 37 68 [CACS:0a7fc4a9T7h]

RADIUS: 39 79 44 42 70 2F 7A 6A 64 66 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. Februar 14:48:14.990: RADIUS: Anbieter, Cisco [26] 39

*23. Februar 14:48:14.990: RADIUS: Cisco AVpair [1] 33 "cts-pac-ability=cts-pac-less"

*23. Februar 14:48:14.990: RADIUS: Anbieter, Cisco [26] 43

*23. Februar 14:48:14.991: RADIUS: Cisco AVpair [1] 37 "cts:server-list=CTSServerList1-0001"

*23. Februar 14:48:14.991: RADIUS: Anbieter, Cisco [26] 38

*23. Februar 14:48:14.991: RADIUS: Cisco AVpair [1] 32 "cts:security-group-tag=0002-00"

*23. Februar 14:48:14.991: RADIUS: Anbieter, Cisco [26] 41

*23. Februar 14:48:14.991: RADIUS: Cisco AVpair [1] 35 "cts:environment-data-expiry=86400"

*23. Februar 14:48:14.991: RADIUS: Anbieter, Cisco [26] 40

*23. Februar 14:48:14.991: RADIUS: Cisco AVpair [1] 34"cts:security-group-table=0001-17"

*23. Februar 14:48:14.991: RADIUS: Modus ohne PAC, geheim vorhanden

*23. Februar 14:48:14.991: RADIUS(0000000F): Empfangen von ID 1645/11

*23. Februar 14:48:14.991: cts_aaa_callback: (CTS Env-Data SM)AAA req(0x7AB57A6AA2C0) Antwort erfolgreich

*23. Februar 14:48:14.991: AAA CTX FRAG REINIGEN: (CTS Env-Data SM)attr(Test)

*23. Februar 14:48:14.991: AAA CTX FRAG REINIGEN: (CTS env-data SM)attr(env-data-fragment)

*23. Februar 14:48:14.991: AAA CTX FRAG REINIGEN: (CTS Env-Data SM)attr(Unterstützung von mehreren Servern - IP)

*23. Februar 14:48:14.991: AAA CTX FRAG REINIGEN: (CTS Env-Data SM)attr(wnlx)

*23. Februar 14:48:14.991: AAA ATR: Unbekannter Typ (450).

*23. Februar 14:48:14.991: AAA ATR: Unbekannter Typ (1324).

*23. Februar 14:48:14.991: AAA ATR: server-list = CTSServerList1-0001:

*23. Februar 14:48:14.991: Empfangener SLIST-Name. cts_is_slist_send_to_binos_req wird auf FALSE gesetzt

*23. Februar 14:48:14.991: AAA ATR: security-group-tag = 0002-00:

*23. Februar 14:48:14.991: AAA ATR: environment-data-expiry = 86400.

*23. Februar 14:48:14.991: AAA ATR: security-group-table = 0001-17.CTS env-data: AAA-Attribute werden empfangen. // Downloading the environment data

CTS_AAA_SLIST

slist name(CTSServerList1) received in 1st Access-Accept

list name(CTSServerList1) existiert

CTS_AAA_SECURITY_GROUP_TAG

CTS_AAA_ENVIRONMENT_DATA_EXPIRY = 86400.

CTS_AAA_SGT_NAME_LIST

table(0001) received in 1st Access-Accept

Kopieren Sie die Tabelle (0001) von installiert nach empfangen, da keine Änderung erfolgt.

neuer Name (0001), gen(17)

CTS_AAA_DATEN_ENDE

*23. Februar 14:48:14.991: cts_env_data WAITING_RESPONSE: während des Zustands env_data_waiting_rsp, Ereignis 1 empfangen(env_data_received)

*23. Februar 14:48:14.991: @@ cts_env_data WAITING_RESPONSE: env_data_waiting_rsp -> env_data_assessment

*23. Februar 14:48:14.991: env_data_assessment_enter: state = ASSESSING

*23. Februar 14:48:14.991: cts_aaa_is_fragmentiert: (CTS Env-Data SM)NOT-FRAG attr_q(0)

*23. Februar 14:48:14.991: env_data_assessment_action: state = ASSESSING

*23. Februar 14:48:14.991: env_data_download_complete:

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

*23. Februar 14:48:14.991: Gleiche erwarten wie empfangen

*23. Februar 14:48:14.991: status(TRUE), req(x81), rec(xC87), wait(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. Februar 14:48:14.991: cts_env_data ANALYSE: während des Zustands env_data_assessment, bekam Ereignis 4(env_data_complete)

*23. Februar 14:48:14.991: @@ cts_env_data ANALYSE: env_data_assessment -> env_data_complete

*23. Februar 14:48:14.991: env_data_complete_enter: Zustand = ABGESCHLOSSEN

*23. Februar 14:48:14.991: CTS-ifc-ev: env-Daten melden an Kern, Ergebnis: Erfolgreich

*23. Februar 14:48:14.991: env_data_install_action: state = COMPLETE completed.types 0x0

*23. Februar 14:48:14.991: env_data_install_action: saubere installierte sgt<->sgname-Tabelle

*23. Februar 14:48:14.991: Bereinigen der installierten sg-epg-Liste

*23. Februar 14:48:14.991: Bereinigen der installierten Standard-EPG-Liste

*23. Februar 14:48:14.991: env_data_install_action: mcast_sgt-Tabelle aktualisiert

*23. Februar 14:48:14.991: Umschalten von Daten mit Standby-Status 2

*23. Februar 14:48:14.991: SLIST entspricht der vorherigen Aktualisierung. Es ist nicht notwendig, es an BINOS zu senden

*23. Februar 14:48:14.991: CTS-sg-epg-events:default_sg 0 auf umgebung setzen

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.