Configuration de l'authentification sans PAC ISE 3.4 entre ISE et NAD pour Trustsec

Table des matières

Introduction

Le document décrit la configuration initiale pour la configuration sans PAC entre les clients ISE et NAD pour le téléchargement des données de l'environnement Trustsec.

Conditions préalables

Exigences

- Connaissance de Cisco TrustSec comme solution de sécurité réseau.
- Connaissance d'Identity Services Engine (ISE) pour la gestion de la sécurité du réseau.
- Compréhension de base du protocole EAP (Extensible Authentication Protocol) en tant que cadre pour le transport des informations d'authentification.

Composants utilisés

Identity Services Engine (ISE) version 3.4.x

Cisco IOS® 17.15.1 ou supérieur

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Informations

En mode sans PAC, les stratégies TrustSec sont plus faciles à mettre en oeuvre, car elles ne nécessitent pas de CAP (Protected Access Credential), généralement nécessaire pour sécuriser les communications entre les périphériques et le moteur ISE (Identity Services Engine). Cette approche est particulièrement avantageuse dans les environnements comportant plusieurs noeuds ISE. Si le noeud principal se déconnecte, les périphériques peuvent automatiquement basculer vers une sauvegarde sans avoir à rétablir leurs informations d'identification, ce qui réduit les interruptions. L'authentification sans PAC simplifie le processus, le rend plus évolutif et plus convivial, et prend en charge des méthodes de sécurité modernes alignées sur les principes Zero Trust.

Dans ce mode, les périphériques commencent par envoyer une requête qui inclut un nom d'utilisateur et un mot de passe. L'ISE répond en proposant une session sécurisée. Une fois cette session configurée, l'ISE fournit les informations importantes nécessaires à une communication sécurisée. Cela inclut une clé de sécurité et des détails tels que l'identité et la synchronisation du serveur. Ces informations sont utilisées pour garantir un accès sécurisé et continu aux politiques et données nécessaires.

Configurer

Configurations

Configuration du commutateur

Dans ce document, la configuration de l'authentification sans PAC est configurée à l'aide du commutateur Cisco C9300. Tout commutateur exécutant la version 17.15.1 ou supérieure peut effectuer une authentification sans PAC avec Identity Services Engine (ISE).

Étape 1 : Configurez le serveur RADIUS et le groupe RADIUS sur le commutateur sous le terminal de configuration du commutateur.

Serveur Radius :

```
radius server

 address ipv4


        auth-port 1812 acct-port 1813

 key
```

Groupe Radius :

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

Étape 2 : Mappez le groupe de serveurs RADIUS à l'autorisation CTS et à dot1x pour l'authentification avec PAC-less.

Mappage CTS :

<#root>

```
cts authorization list
```

cts-mlist

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

Authentification Dot1x :

<#root>

```
aaa authentication dot1x default group
```

```
aaa authorization network
```

cts-mlist

```
 group
```

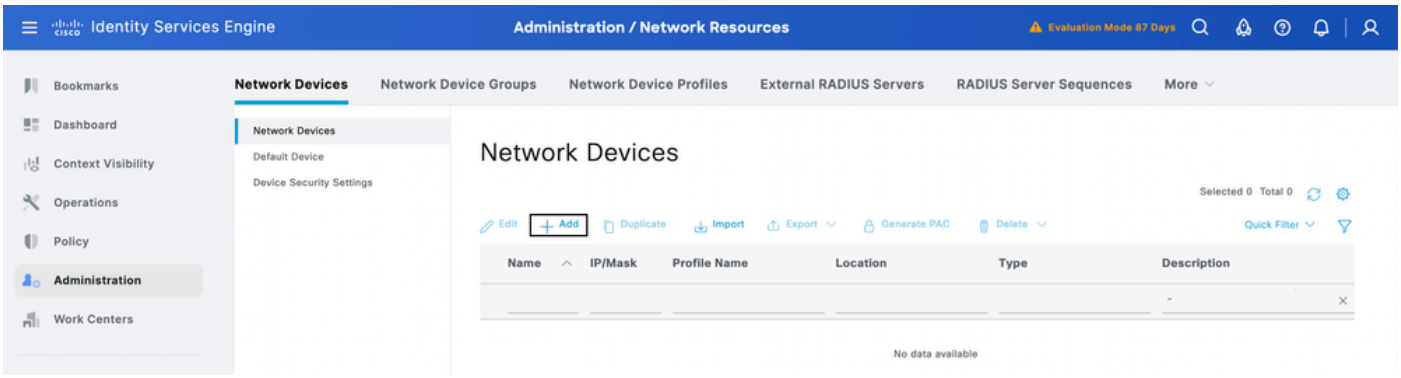
Étape 3 : Configurez l'ID CTS et le mot de passe sous le mode enable sur le commutateur

```
cts credentials id

        password
```

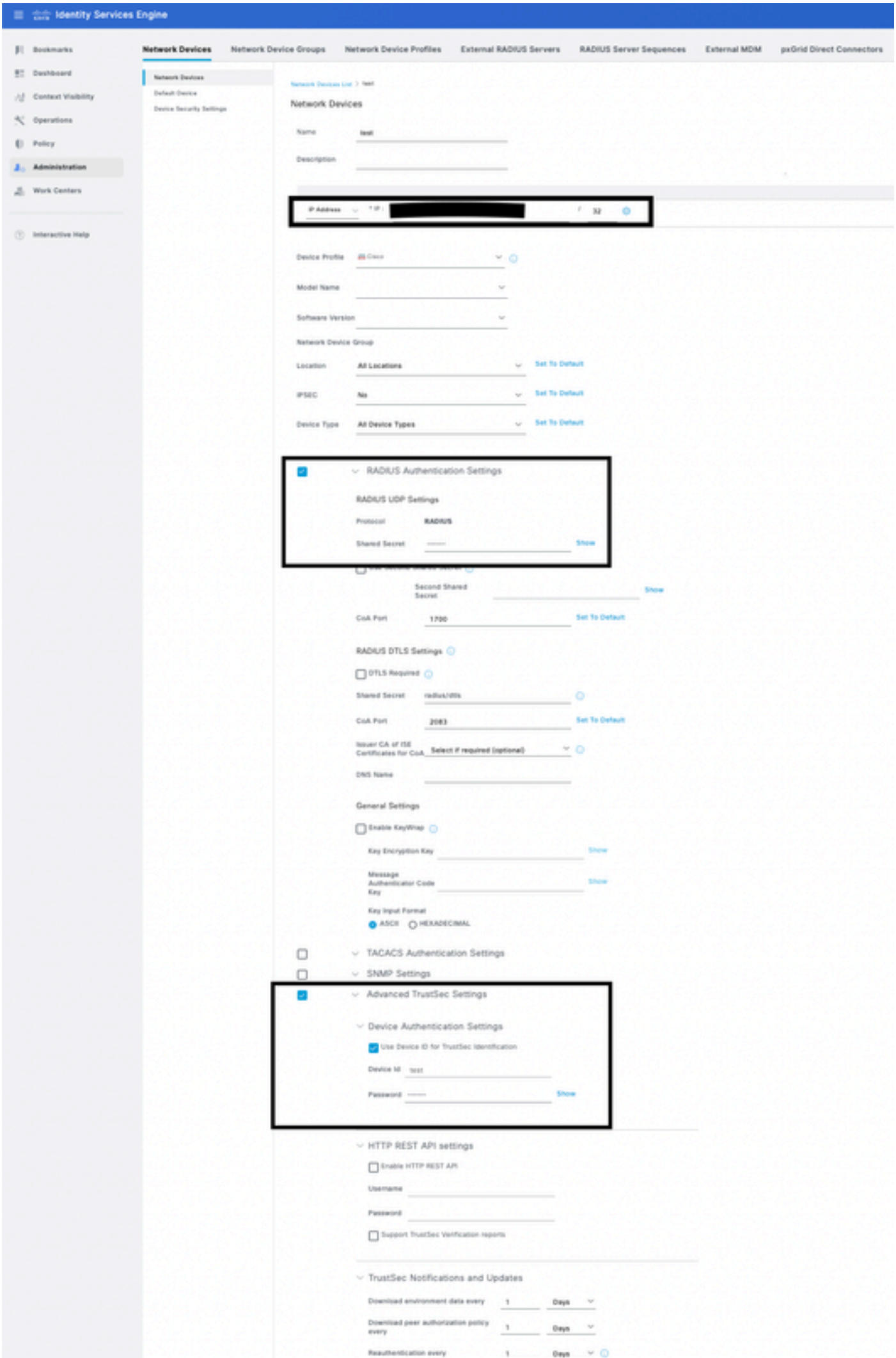
Configuration ISE

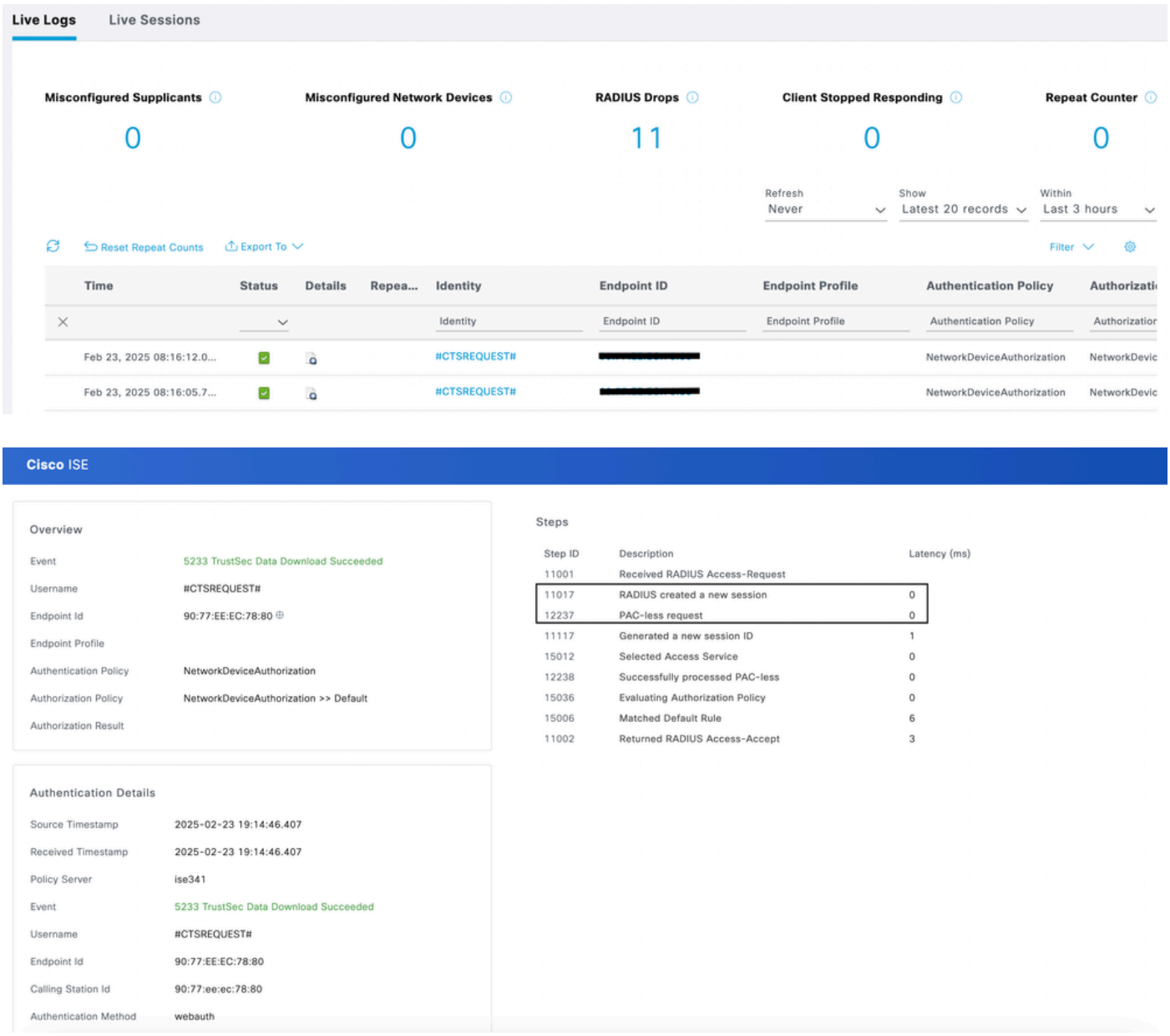
1. Sur ISE, configurez le périphérique réseau sous Administration > Network Resources > Network Devices > Network Devices. Cliquez sur add pour ajouter le commutateur au serveur ISE.



2. Ajoutez l'adresse IP NAD dans le champ d'adresse IP pour qu'ISE traite la demande radius pour l'authentification trustsec du commutateur.
3. Activez les paramètres d'authentification Radius pour le client NAD et entrez la clé secrète partagée Radius.

4. Activez Advanced Trustsec Settings et mettez à jour le nom du périphérique avec CTS-ID et le champ de mot de passe avec le mot de passe de la commande (cts credentials id <CTS-ID> password <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



Dépannage

Pour résoudre le problème, exécutez ces débogages sur le commutateur :

```
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
```

Extrait de débogage :

*Feb 23 14:48:14.974: Env-data CTS : Forcer l'actualisation des données d'environnement 0x2

*Feb 23 14:48:14.974: Env-data CTS : download transport-type = CTS_TRANSPORT_IP_UDP

*Feb 23 14:48:14.974: cts_env_data ACHEVÉE : pendant l'état env_data_complete, obtention de l'événement 0(env_data_request)

*Feb 23 14:48:14.974: @@@ cts_env_data ACHEVÉ : env_data_complete -> env_data_waiting_rsp

*Feb 23 14:48:14.974: env_data_waiting_rsp_enter : état = WAITING_RESPONSE

*Feb 23 14:48:14.974: Une clé sécurisée est présente sur le périphérique, poursuivez le téléchargement des données d'enveloppe sans CAP // lancez l'authentification sans CAP à partir du commutateur

*Feb 23 14:48:14.974: cts_aaa_is_fragmented : (CTS env-data SM)NOT-FRAG attr_q(0)

*Feb 23 14:48:14.974: env_data_request_action : état = WAITING_RESPONSE

*Feb 23 14:48:14.974: env_data_download_complete :

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

*Feb 23 14:48:14.974: status(FALSE), req(x0), rec(x0), attend(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(xC085), wait_for_default_SGT_tbl(x600085) wait_for_default_SERVICE_ENTRY_tbl(xC000085)

*Feb 23 14:48:14.974: env_data_request_action : état = WAITING_RESPONSE, reçu = 0x0 requête = 0x0

*Feb 23 14:48:14.974: cts_env_data_aaa_req_setup : aaa_id = 15

*Feb 23 14:48:14.974: cts_aaa_req_setup : (CTS env-data SM)Le groupe privé est MORT, tentative de groupe public

*Feb 23 14:48:14.974: cts_aaa_attr_add : AAA requis(0x7AB57A6AA2C0)

*Feb 23 14:48:14.974: nom d'utilisateur = #CTSREQUEST#

*Feb 23 14:48:14.974: Attribut d'ajout de contexte AAA : (CTS env-data SM)attr(test)

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

*Feb 23 14:48:14.974: cts_aaa_attr_add : AAA requis(0x7AB57A6AA2C0)

*Feb 23 14:48:14.974: Attribut d'ajout de contexte AAA : (CTS env-data SM)attr(env-data-fragment)

*Feb 23 14:48:14.974:   cts-device-capability = env-data-fragment

*Feb 23 14:48:14.974: cts_aaa_attr_add : AAA requis(0x7AB57A6AA2C0)

*Feb 23 14:48:14.975: Attribut d'ajout de contexte AAA : (CTS env-data SM)attr(multiple-server-ip-supported)

*Feb 23 14:48:14.975:   cts-device-capability = prise en charge de l'adresse ip de plusieurs serveurs

*Feb 23 14:48:14.975: cts_aaa_attr_add : AAA requis(0x7AB57A6AA2C0)

*Feb 23 14:48:14.975: Attribut d'ajout de contexte AAA : (CTS env-data SM)attr(wnlx)

*Feb 23 14:48:14.975:   clid = wnlx

*Feb 23 14:48:14.975: cts_aaa_req_send : AAA req(0x7AB57A6AA2C0) envoyé à AAA.

*Feb 23 14:48:14.975: RADIUS/ENCODE(0000000F) : Orig. type de composant = CTS

*Feb 23 14:48:14.975: RADIUS(0000000F) : Config NAS IP : 0.0.0.0

*Feb 23 14:48:14.975: vrfid : [65535] ipv6 tableid : [0]

*Feb 23 14:48:14.975: idb est NULL

*Feb 23 14:48:14.975: RADIUS(0000000F) : Config NAS IPv6 : ::

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

*Feb 23 14:48:14.975: RADIUS(0000000F) : émetteur

*Feb 23 14:48:14.975: RADIUS: Mode sans PAC, secret présent

*Feb 23 14:48:14.975: RADIUS: Attribut CTS pacless ajouté à la demande radius

*Feb 23 14:48:14.975: RADIUS/ENCODE : Meilleure adresse IP locale 10.127.196.234 pour serveur Radius 10.127.196.169

*Feb 23 14:48:14.975: RADIUS: Mode sans PAC, secret présent

*Feb 23 14:48:14.975: RADIUS(0000000F) : Envoyer la demande d'accès à 10.127.196.169:1812 id 1645/11, len 249 // Demande d'accès Radius du commutateur

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

*Feb 23 14:48:14.975: RADIUS: Nom d'utilisateur [1] 14 "#CTSREQUEST#"

*Feb 23 14:48:14.975: RADIUS: Fournisseur, Cisco [26] 33

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

*Feb 23 14:48:14.975: RADIUS: Fournisseur, Cisco [26] 47

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

*Feb 23 14:48:14.975: RADIUS: Fournisseur, Cisco [26] 58

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

*Feb 23 14:48:14.975: RADIUS: Mot de passe utilisateur [2] 18 *

*Feb 23 14:48:14.975: RADIUS: Calling-Station-Id [31] 8 "wnlx"

*Feb 23 14:48:14.975: RADIUS: Type de service [6] 6 Sortant [5]

*Feb 23 14:48:14.975: RADIUS: Adresse IP NAS [4] 6 10.127.196.234

*Feb 23 14:48:14.975: RADIUS: Fournisseur, Cisco [26] 39

*Feb 23 14:48:14.975: RADIUS: Cisco AVpair [1] 33 "cts-pac-capability=cts-pac-less" // CTS PAC L'attribut cv-pair Less s'ajoute à la demande pour qu'ISE gère le paquet pour l'authentification sans PAC

*Feb 23 14:48:14.975: RADIUS(0000000F) : Envoi d'un paquet Radius IPv4

*Feb 23 14:48:14.975: RADIUS(0000000F) : Délai d'attente de 5 secondes démarré

*Feb 23 14:48:14.990: RADIUS: Reçu de l'ID 1645/11 10.127.196.169:1812, Access-Accept, len 313. // Authentification réussie

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

*Feb 23 14:48:14.990: RADIUS: Nom d'utilisateur [1] 14 "#CTSREQUEST#"

*Feb 23 14:48:14.990: RADIUS: Classe [25] 78

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

*Feb 23 14:48:14.990: RADIUS: Fournisseur, Cisco [26] 39

*Feb 23 14:48:14.990: RADIUS: Cisco AVpair [1] 33 "cts-pac-capability=cts-pac-less"

*Feb 23 14:48:14.990: RADIUS: Fournisseur, Cisco [26] 43

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

*Feb 23 14:48:14.991: RADIUS: Fournisseur, Cisco [26] 38

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

*Feb 23 14:48:14.991: RADIUS: Fournisseur, Cisco [26] 41

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

*Feb 23 14:48:14.991: RADIUS: Fournisseur, Cisco [26] 40

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

*Feb 23 14:48:14.991: RADIUS: Mode sans PAC, secret présent

*Feb 23 14:48:14.991: RADIUS(0000000F) : Reçu de id 1645/11

*Feb 23 14:48:14.991: cts_aaa_callback : (CTS env-data SM)Réponse AAA req(0x7AB57A6AA2C0) réussie

*Feb 23 14:48:14.991: AAA CTX FRAG CLEAN : (CTS env-data SM)attr(test)

*Feb 23 14:48:14.991: AAA CTX FRAG CLEAN : (CTS env-data SM)attr(env-data-fragment)

*Feb 23 14:48:14.991: AAA CTX FRAG CLEAN : (CTS env-data SM)attr(multiple-server-ip-supported)

*Feb 23 14:48:14.991: AAA CTX FRAG CLEAN : (CTS env-data SM)attr(wnlx)

*Feb 23 14:48:14.991:   Attribut AAA : Type inconnu (450).

*Feb 23 14:48:14.991:   Attribut AAA : Type inconnu (1324).

*Feb 23 14:48:14.991:   Attribut AAA : server-list = CTSServerList1-0001.

*Feb 23 14:48:14.991: Nom SLIST reçu. Définition de cts_is_slist_send_to_binos_req sur FALSE

*Feb 23 14:48:14.991:   Attribut AAA : security-group-tag = 0002-00.

*Feb 23 14:48:14.991:   Attribut AAA : environment-data-expiry = 86400.

*Feb 23 14:48:14.991:   Attribut AAA : security-group-table = 0001-17.CTS env-data : Réception des attributs AAA.   // Téléchargement des données d'environnement

  LISTE_LISTE_AAA_CTS

slist name(CTSServerList1) reçu dans 1st Access-Accept

slist name(CTSServerList1) existe

BALISE_GROUPE_SÉCURITÉ_CTS_AAA

CTS_AAA_ENVIRONMENT_DATA_EXPIRY = 86400.

LISTE_NOM_SGT_AAA_CTS

table(0001) reçue dans 1st Access-Accept

Copiez la table (0001) de l'installation à la réception car aucune modification n'a été apportée.

nouveau nom(0001), gen(17)

CTS_AAA_DATA_END

*Feb 23 14:48:14.991: cts_env_data WAITING_RESPONSE : pendant l'état env_data_waiting_rsp, obtention de l'événement 1(env_data_received)

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

*Feb 23 14:48:14.991: env_data_assessment_enter : état = ÉVALUATION

*Feb 23 14:48:14.991: cts_aaa_is_fragmented : (CTS env-data SM)NOT-FRAG attr_q(0)

*Feb 23 14:48:14.991: env_data_assessment_action : état = ÉVALUATION

*Feb 23 14:48:14.991: env_data_download_complete :

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

*Feb 23 14:48:14.991: Attendez-vous au même résultat

*Feb 23 14:48:14.991: status(TRUE), req(x81), rec(xC87), attend(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(xC085), wait_for_default_SGT_tbl(x600085) wait_for_default_SERVICE_ENTRY_tbl(xC000085)

*Feb 23 14:48:14.991: cts_env_data ÉVALUATION : pendant l'état env_data_assessment, obtention de l'événement 4(env_data_complete)

*Feb 23 14:48:14.991: @@@ cts_env_data ÉVALUATION : env_data_assessment -> env_data_complete

*Feb 23 14:48:14.991: env_data_complete_enter : état = TERMINÉ

*Feb 23 14:48:14.991: CTS-ifc-ev : env data reporting to core, résultat : Réussi

*Feb 23 14:48:14.991: env_data_install_action : état = TERMINÉ.types 0x0

*Feb 23 14:48:14.991: env_data_install_action : table sgt<->sgname installée propre

*Feb 23 14:48:14.991: Nettoyage de la liste sg-epg installée

*Feb 23 14:48:14.991: Nettoyage de la liste des pages par défaut installées

*Feb 23 14:48:14.991: env_data_install_action : mcast_sgt, table mise à jour

*Feb 23 14:48:14.991: Synchronisation des données Env avec état de veille 2

*Feb 23 14:48:14.991: SLIST est identique à l'actualisation précédente. Pas besoin de l'envoyer au BINOS

*Feb 23 14:48:14.991: CTS-sg-epg-events:définition de default_sg 0 sur données env

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.