Configurazione dell'autenticazione senza PAC ISE 3.4 tra ISE e NAD per Trustsec

Sommario

Introduzione

In questo documento viene descritta la configurazione iniziale per la configurazione senza PAC tra i client ISE e NAD per il download dei dati di ambiente Trustsec.

Prerequisiti

Requisiti

- Familiarità con Cisco TrustSec come soluzione per la sicurezza di rete.
- Conoscenza di Identity Services Engine (ISE) per la gestione della sicurezza della rete.
- Comprensione di base del protocollo EAP (Extensible Authentication Protocol) come framework per il trasporto delle informazioni di autenticazione.

Componenti usati

Identity Services Engine (ISE) release 3.4.x

Cisco IOS® 17.15.1 o superiore

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Informazioni

Nella modalità senza PAC, i criteri TrustSec sono più facili da implementare perché non richiedono una credenziale di accesso protetta (PAC), che è in genere necessaria per una comunicazione sicura tra i dispositivi e l'Identity Services Engine (ISE). Questo approccio è particolarmente utile negli ambienti con più nodi ISE. Se il nodo primario non è in linea, i dispositivi possono passare automaticamente a un backup senza dover ristabilire le credenziali, riducendo le interruzioni. L'autenticazione senza PAC semplifica il processo, rendendolo più scalabile e semplice da utilizzare e supporta metodi di sicurezza moderni allineati ai principi di Zero Trust.

In questa modalità, i dispositivi iniziano con l'invio di una richiesta che include un nome utente e una password. L'ISE risponde proponendo una sessione sicura. Una volta stabilita la sessione, l'ISE fornisce informazioni importanti necessarie per garantire una comunicazione sicura. Include una chiave per la protezione e dettagli quali l'identità e la tempistica del server. Queste informazioni vengono utilizzate per garantire l'accesso sicuro e continuo alle policy e ai dati necessari.

Configurazione

Configurazioni

Configurazione degli switch

In questo documento, la configurazione per l'autenticazione senza PAC è configurata utilizzando lo switch Cisco C9300. Tutti gli switch con versione 17.15.1 o successive possono eseguire l'autenticazione senza PAC con Identity Services Engine (ISE).

Passaggio 1: Configurare il server Radius e il gruppo radius sullo switch sotto il terminale di configurazione dello switch.

Server Radius:

```
radius server

 address ipv4

        auth-port 1812 acct-port 1813

 key
```

Gruppo raggio:

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

Passaggio 2: Mappare il gruppo di server radius all'autorizzazione ct e al dot1x per l'autenticazione senza PAC.

Mapping CTS:

<#root>

```
cts authorization list
```

cts-mlist

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

Autenticazione dot1x:

<#root>

```
aaa authentication dot1x default group
```

```
aaa authorization network
```

cts-mlist

```
 group
```

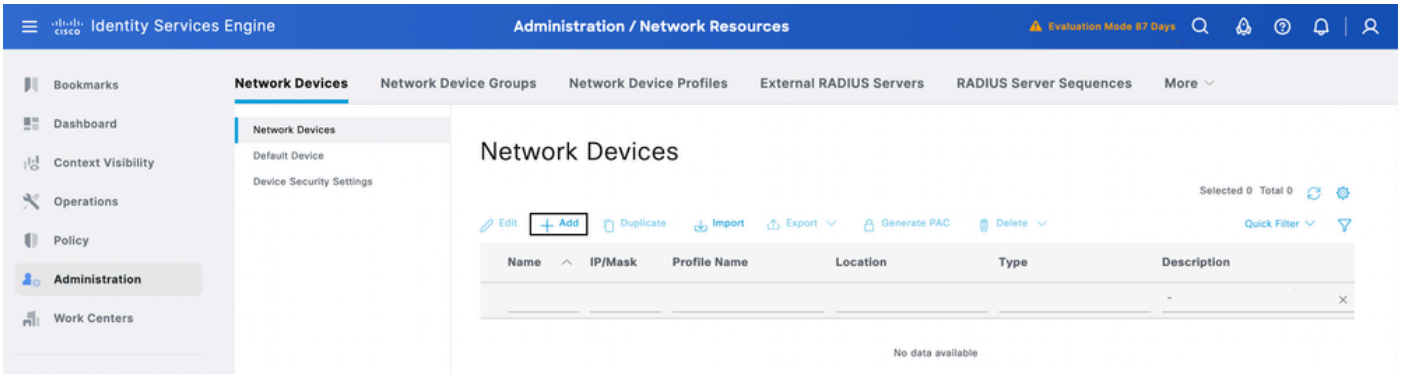
Passaggio 3: Configurare l'ID-CTS e la password nella modalità di abilitazione sullo switch

```
cts credentials id

        password
```

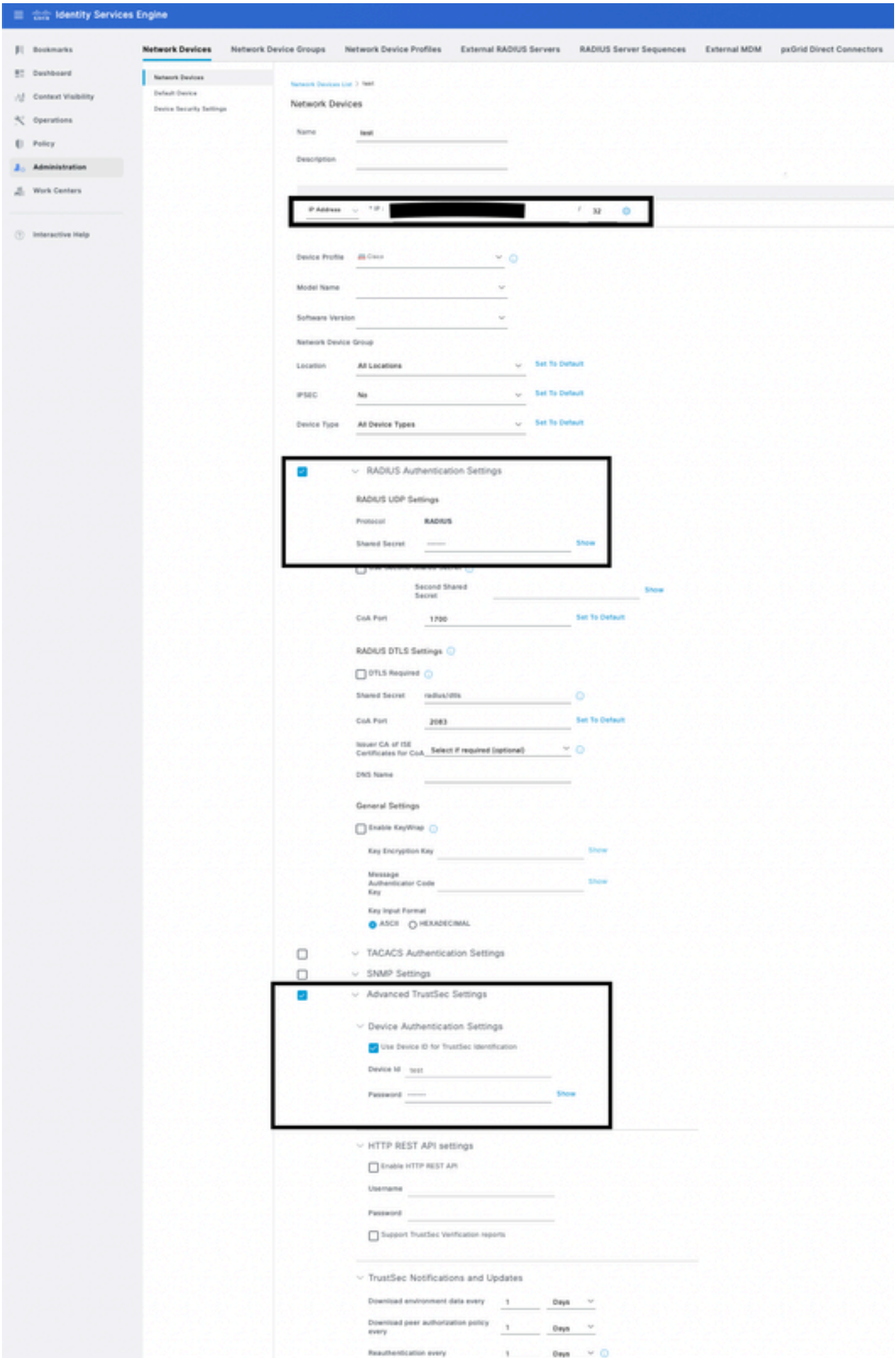
Configurazione di ISE

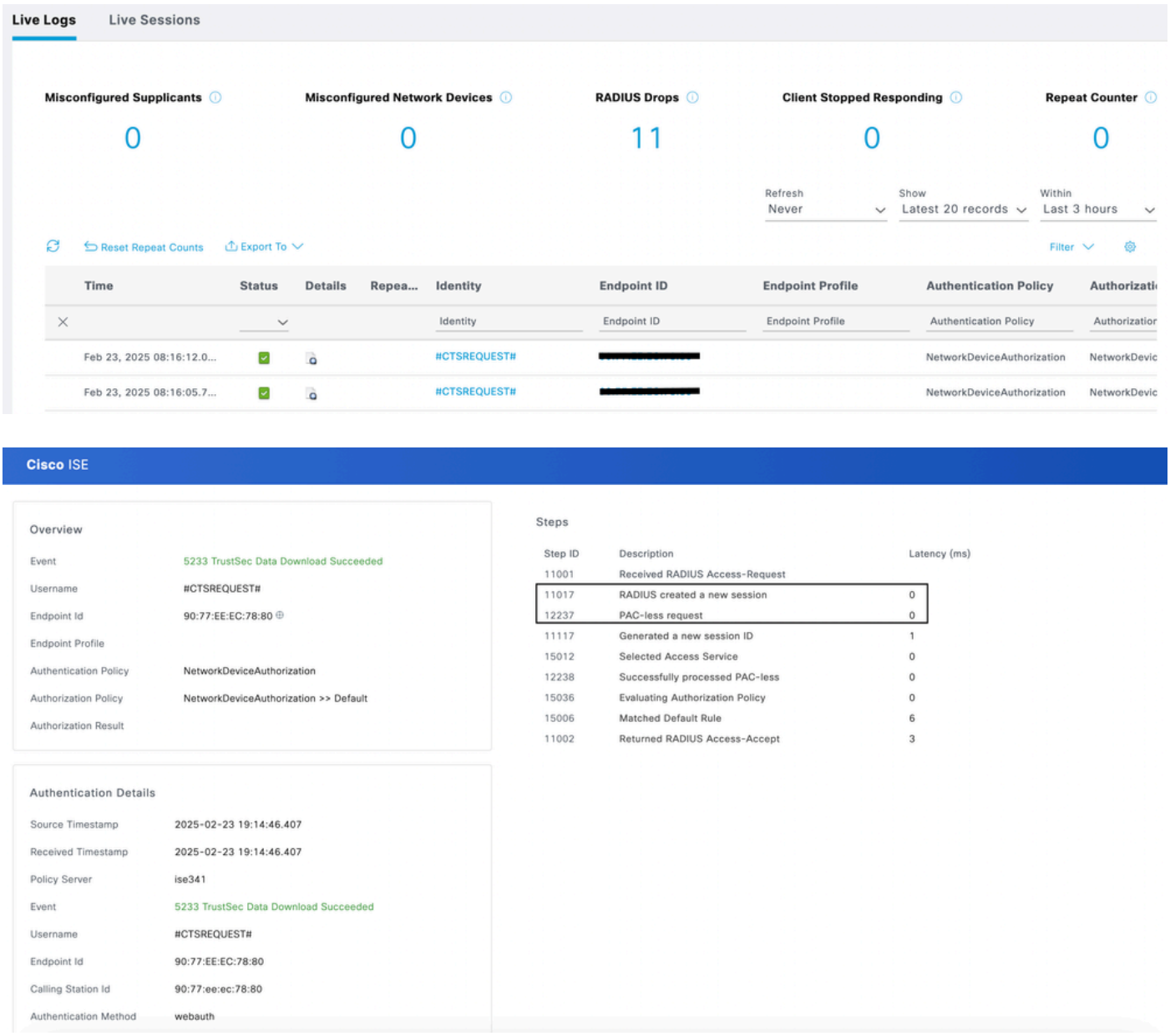
1. Su ISE, configurare il dispositivo di rete in Amministrazione > Risorse di rete > Dispositivi di rete > Dispositivi di rete. Fare clic su add (Aggiungi) per aggiungere lo switch al server ISE.



2. Aggiungere l'indirizzo IP NAD nel campo dell'indirizzo IP di ISE per elaborare la richiesta radius per l'autenticazione trustsec inviata dallo switch.
3. Abilitare le impostazioni di autenticazione Radius per il client NAD e immettere la chiave privata condivisa Radius.

4. Abilitare Impostazioni Trustsec avanzate e aggiornare il nome del dispositivo con l'ID CTS e il campo della password con la password del comando (ID credenziali CTS <ID-CTS> 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



Risoluzione dei problemi

Per risolvere il problema, eseguire i seguenti debug sullo 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
```

Frammento di debug:

*Feb 23 14:48:14.974: Dati env CTS: Forza maschera di bit di aggiornamento dati di ambiente 0x2

*Feb 23 14:48:14.974: Dati env CTS: download transport-type = CTS_TRANSPORT_IP_UDP

*Feb 23 14:48:14.974: cts_env_data COMPLETATO: durante lo stato env_data_complete, è stato ricevuto l'evento 0(env_data_request)

*Feb 23 14:48:14.974: @@@ cts_env_data COMPLETATO: env_data_complete -> env_data_wait_rsp

*Feb 23 14:48:14.974: env_data_wait_rsp_enter: state = WAITING_RESPONSE

*Feb 23 14:48:14.974: La chiave di protezione è presente sul dispositivo, procedere con il download dei dati di protezione senza PAC // avviare l'autenticazione senza PAC dallo switch

*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: azione_richiesta_dati: state = WAITING_RESPONSE

*Feb 23 14:48:14.974: env_data_download_complete:

status(FALSO), req(x0), rec(x0)

*Feb 23 14:48:14.974: status(FALSO), 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)

*Feb 23 14:48:14.974: azione_richiesta_dati: stato = WAITING_RESPONSE, ricevuto = 0x0 richiesta = 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)Gruppo privato appare MORTO, tentativo gruppo pubblico

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

*Feb 23 14:48:14.974: username = #CTSREQUEST#

*Feb 23 14:48:14.974: Aggiungi attributo contesto AAA: (CTS env-data SM)attr(prova)

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

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

*Feb 23 14:48:14.974: Aggiungi attributo contesto AAA: (CTS env-data SM)attr(env-data-fragment)

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

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

*Feb 23 14:48:14.975: Aggiungi attributo contesto AAA: (CTS env-data SM)attr (supporto di IP per più server)

*Feb 23 14:48:14.975:   ct-device-capabilities = supporto ip per più server

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

*Feb 23 14:48:14.975: Aggiungi attributo contesto 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: Richiesta AAA(0x7AB57A6AA2C0) inviata correttamente all'appliance AAA.

*Feb 23 14:48:14.975: RADIUS/ENCODE(000000F):Origine tipo di componente = CTS

*Feb 23 14:48:14.975: RADIUS(000000F): Configura IP NAS: 0.0.0.0

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

*Feb 23 14:48:14.975: idb è NULL

*Feb 23 14:48:14.975: RADIUS(000000F): Configura NAS IPv6: ::

*Feb 23 14:48:14.975: RADIUS/ENCODE(000000F): acct_session_id: 4003

*Feb 23 14:48:14.975: RADIUS(000000F): invio

*Feb 23 14:48:14.975: RAGGIO: Modalità senza PAC, è presente il segreto

*Feb 23 14:48:14.975: RAGGIO: L'attributo CTS pacless è stato aggiunto alla richiesta radius

*Feb 23 14:48:14.975: RADIUS/ENCODE: Miglior indirizzo IP locale 10.127.196.234 per Radius-Server 10.127.196.169

*Feb 23 14:48:14.975: RAGGIO: Modalità senza PAC, è presente il segreto

*Feb 23 14:48:14.975: RADIUS(000000F): Inviare una richiesta di accesso allo switch 10.127.196.169:1812 id 1645/11, len 249 // Richiesta di accesso Radius

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

*Feb 23 14:48:14.975: RAGGIO: User-Name [1] 14 "#CTSREQUEST#"

*Feb 23 14:48:14.975: RAGGIO: Fornitore, Cisco [26] 33

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

*Feb 23 14:48:14.975: RAGGIO: Fornitore, Cisco [26] 47

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

*Feb 23 14:48:14.975: RAGGIO: Fornitore, Cisco [26] 58

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

*Feb 23 14:48:14.975: RAGGIO: Password utente [2] 18 *

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

*Feb 23 14:48:14.975: RAGGIO: Service-Type [6] 6 In Uscita [5]

*Feb 23 14:48:14.975: RAGGIO: Indirizzo IP-NAS [4] 6 10.127.196.234

*Feb 23 14:48:14.975: RAGGIO: Fornitore, Cisco [26] 39

*Feb 23 14:48:14.975: RAGGIO: Cisco AVpair [1] 33 "cts-pac-capabilities=cts-pac-less" // Attributo CTS PAC Less cv-pair aggiungere alla richiesta per ISE di gestire il pacchetto per l'autenticazione senza PAC

*Feb 23 14:48:14.975: RADIUS(000000F): Invio di un pacchetto Radius IPv4

*Feb 23 14:48:14.975: RADIUS(000000F): Timeout 5 sec avviato

*23 feb 14:48:14.990: RAGGIO: Ricevuto da id 1645/11 10.127.196.169:1812, Access-Accept, len 313. // Autenticazione riuscita

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

*23 feb 14:48:14.990: RAGGIO: User-Name [1] 14 "#CTSREQUEST#"

*23 feb 14:48:14.990: RAGGIO: Classe [25] 78

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

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

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

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

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

*23 feb 14:48:14.990: RAGGIO: Fornitore, Cisco [26] 39

*23 feb 14:48:14.990: RAGGIO: Cisco AVpair [1] 33 "cts-pac-capabilities=cts-pac-less"

*23 feb 14:48:14.990: RAGGIO: Fornitore, Cisco [26] 43

*23 feb 14:48:14.991: RAGGIO: Cisco AVpair [1] 37 "cts:server-list=CTServerList1-0001"

*23 feb 14:48:14.991: RAGGIO: Fornitore, Cisco [26] 38

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

*23 feb 14:48:14.991: RAGGIO: Fornitore, Cisco [26] 41

*23 feb 14:48:14.991: RAGGIO: Cisco AVpair [1] 35 "cts:environment-data-expendy=86400"

*23 feb 14:48:14.991: RAGGIO: Fornitore, Cisco [26] 40

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

*23 feb 14:48:14.991: RAGGIO: Modalità senza PAC, è presente il segreto

*23 feb 14:48:14.991: RADIUS(000000F): Ricevuto da id 1645/11

*23 feb 14:48:14.991: cts_aaa_callback: (CTS env-data SM)Risposta AAA richiesta (0x7AB57A6AA2C0) riuscita

*23 feb 14:48:14.991: AAA CTX FRAG CLEAN (PULITO FRAG AAA CTX): (CTS env-data SM)attr(prova)

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

*23 feb 14:48:14.991: AAA CTX FRAG CLEAN (PULITO FRAG AAA CTX): (CTS env-data SM)attr (supporto di IP per più server)

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

*23 feb 14:48:14.991:   Attributo AAA: Tipo sconosciuto (450).

*23 feb 14:48:14.991:   Attributo AAA: Tipo sconosciuto (1324).

*23 feb 14:48:14.991:   Attributo AAA: server-list = CTSServerList1-0001.

*23 feb 14:48:14.991: Nome SLIST ricevuto. Impostazione di cts_is_slist_send_to_binos_req su FALSE

*23 feb 14:48:14.991:   Attributo AAA: security-group-tag = 0002-00.

*23 feb 14:48:14.991:   Attributo AAA: ambiente-dati-scadenza = 86400.

*23 feb 14:48:14.991: Attributo AAA: security-group-table = 0001-17.CTS env-data: Ricezione degli attributi AAA. // Download dei dati di ambiente

CTS_AAA_SLIST

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

slist name(CTSServerList1) esiste

TAG_CTS_AAA_SECURITY_GROUP

CTS_AAA_ENVIRONMENT_DATA_EXPIRY = 86400.

CTS_AAA_SGT_NAME_LIST

table(0001) ricevuta in 1st Access-Accept

Copia tabella(0001) da installata a ricevuta perché nessuna modifica.

new name(0001), gen(17)

CTS_AAA_DATA_END

*23 feb 14:48:14.991: cts_env_data WAITING_RESPONSE: durante lo stato env_data_wait_rsp, ricevuto l'evento 1(env_data_received)

*23 feb 14:48:14.991: @@@ cts_env_data WAITING_RESPONSE: env_data_wait_rsp -> valutazione_dati_inv

*23 feb 14:48:14.991: env_data_evaluation_enter: state = VALUTAZIONE

*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: azione_valutazione_dati: state = VALUTAZIONE

*23 feb 14:48:14.991: env_data_download_complete:

stato(FALSO), rich.(x81), reg.(xC87)

*23 feb 14:48:14.991: Previsto uguale a ricevuto

*23 feb 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 feb 14:48:14.991: cts_env_data ASSESSMENT: durante lo stato env_data_assessment, è stato ricevuto l'evento 4(env_data_complete)

*23 feb 14:48:14.991: @@@ cts_env_data ASSESSMENT: env_data_assessment ->

env_data_complete

*23 feb 14:48:14.991: env_data_complete_enter state = COMPLETE

*23 feb 14:48:14.991: CTS-ifc-ev: env data reporting to core, risultato: Operazione riuscita

*23 feb 14:48:14.991: azione_installazione_dati: state = COMPLETE COMPLETED.types 0x0

*23 feb 14:48:14.991: azione_installazione_dati: tabella clean installed sgt<->sgname

*23 feb 14:48:14.991: Pulizia elenco sg-epg installato

*23 feb 14:48:14.991: Pulizia dell'elenco di pagine predefinito installato

*23 feb 14:48:14.991: azione_installazione_dati: tabella mcast_sgt aggiornata

*23 feb 14:48:14.991: Sincronizzazione dati busta con stato standby 2

*23 feb 14:48:14.991: SLIST equivale all'aggiornamento precedente. Non è necessario inviarlo a BINOS

*23 feb 14:48:14.991: CTS-sg-epg-events:impostazione di default_sg 0 su env data

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).