Configuración de la autenticación sin PAC de ISE 3.4 entre ISE y NAD para Trustsec

Contenido

Introducción

El documento describe la configuración inicial para la configuración sin PAC entre los clientes ISE y NAD para la descarga de datos del entorno Trustsec.

Prerequisites

Requirements

- Familiaridad con Cisco TrustSec como solución de seguridad de red.
- Conocimiento de Identity Services Engine (ISE) para gestionar la seguridad de la red.
- Comprensión básica del protocolo de autenticación extensible (EAP) como marco para transportar información de autenticación.

Componentes Utilizados

Identity Services Engine (ISE) versión 3.4.x

Cisco IOS® 17.15.1 o superior

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Información

En el modo sin PAC, las políticas de TrustSec son más fáciles de implementar porque no requieren una credencial de acceso protegido (PAC), que suele ser necesaria para una comunicación segura entre los dispositivos e Identity Services Engine (ISE). Este enfoque resulta especialmente beneficioso en entornos con varios nodos ISE. Si el nodo principal se desconecta, los dispositivos pueden cambiar automáticamente a una copia de seguridad sin necesidad de restablecer sus credenciales, lo que reduce las interrupciones. La autenticación sin PAC simplifica el proceso, haciéndolo más escalable y fácil de usar, y admite métodos de seguridad modernos alineados con los principios de confianza cero.

En este modo, los dispositivos comienzan enviando una solicitud que incluye un nombre de usuario y una contraseña. El ISE responde proponiendo una sesión segura. Una vez configurada esta sesión, ISE proporciona la información importante necesaria para una comunicación segura. Esto incluye una clave para la seguridad y detalles como la identidad y la sincronización del servidor. Esta información se utiliza para garantizar un acceso seguro y continuo a las políticas y los datos necesarios.

Configurar

Configuraciones

Configuración del switch

En este documento, la configuración para la autenticación sin PAC se configura mediante el switch Cisco C9300. Cualquier switch que ejecute la versión 17.15.1 o superior puede realizar una autenticación sin PAC con Identity Services Engine (ISE).

Paso 1: Configure el servidor Radius y el grupo Radius en el switch en el terminal de configuración del switch.

Servidor Radius:

```
radius server

 address ipv4

        auth-port 1812 acct-port 1813

 key
```

Grupo Radius:

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

Paso 2: Asigne el grupo de servidores RADIUS a la autorización CTS y dot1x para la autenticación con PAC-less.

Asignación de CTS:

<#root>

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

Autenticación Dot1x:

<#root>

```
aaa authentication dot1x default group
```

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

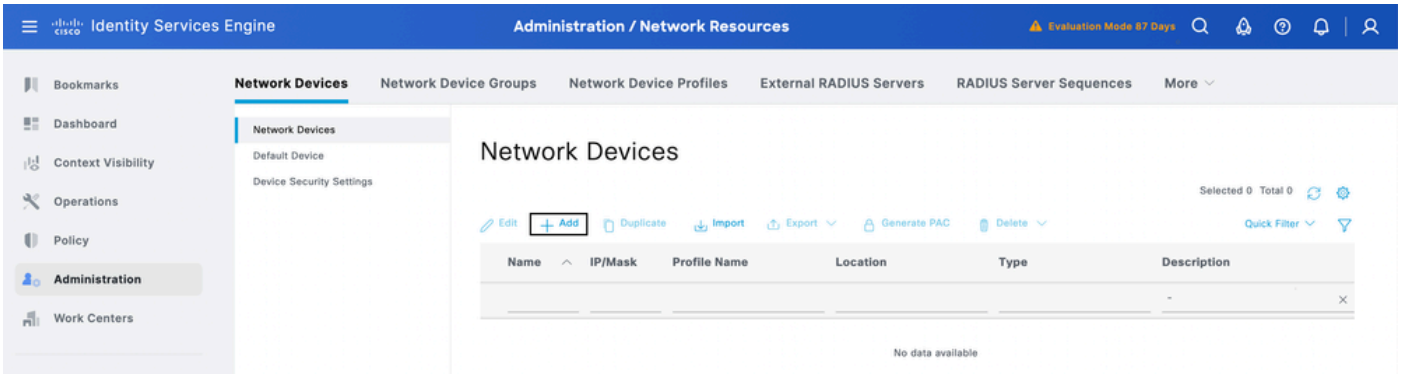
Paso 3: Configure el CTS-ID y la contraseña bajo el modo de habilitación en el switch

```
cts credentials id

        password
```

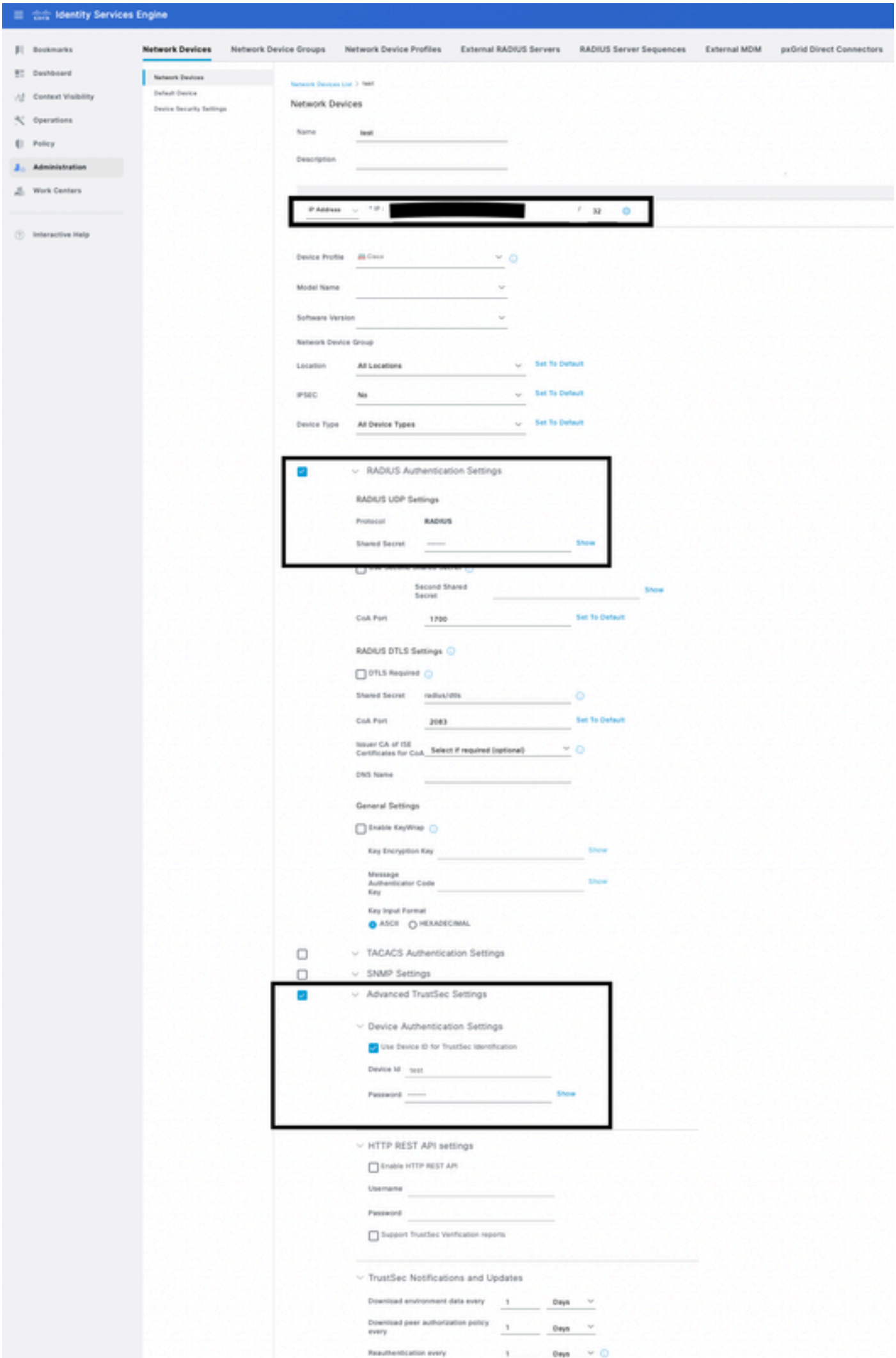
Configuración de ISE

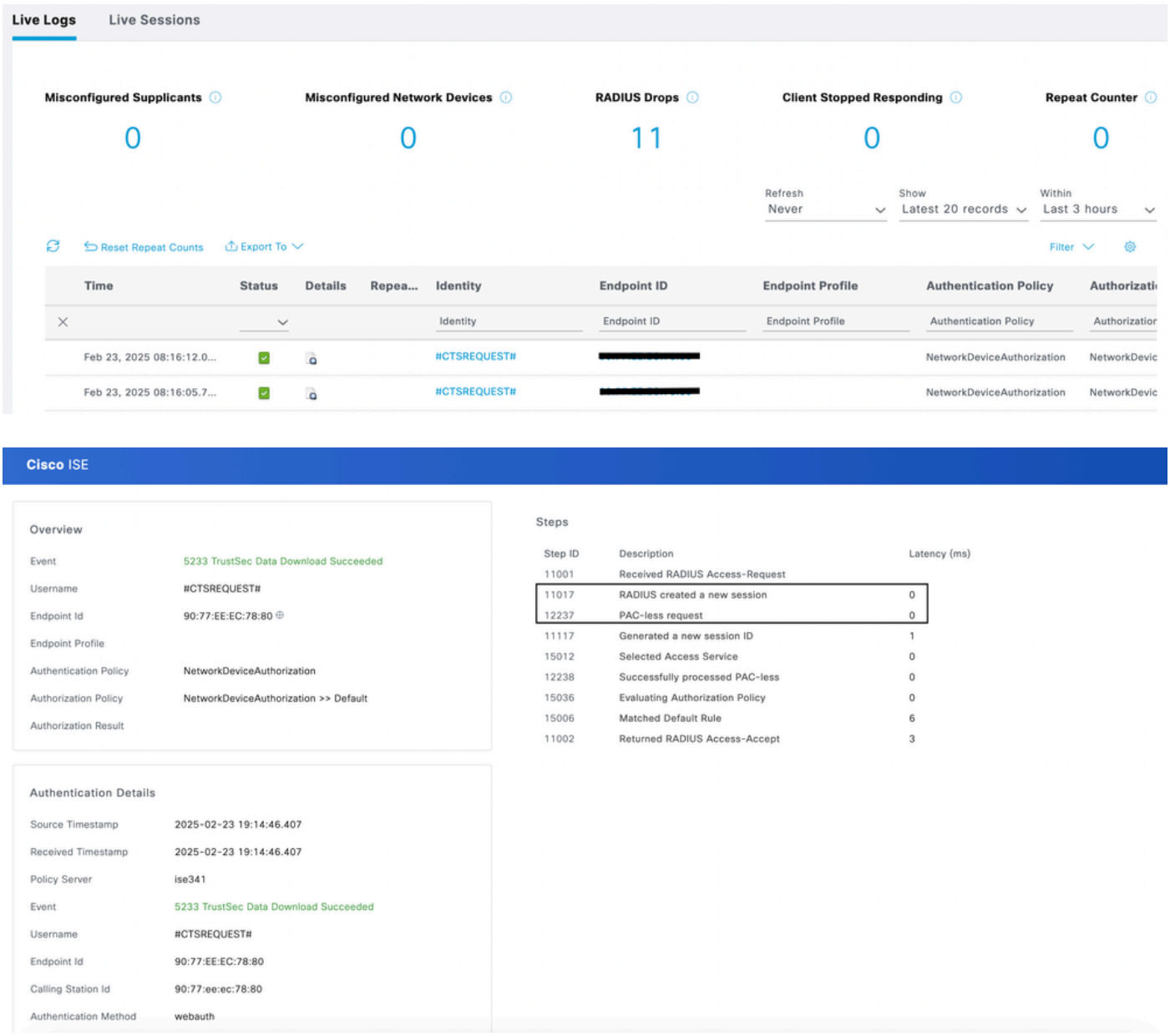
1. En ISE, configure el dispositivo de red en Administration > Network Resources > Network Devices > Network Devices. Haga clic en agregar para agregar el switch al servidor ISE.



2. Agregue la dirección IP de NAD en el campo de dirección IP para que ISE procese la solicitud de RADIUS para la autenticación trustsec del switch.
3. Habilite Radius Authentication Settings para el cliente NAD e ingrese la clave secreta compartida Radius.

4. Habilite Advanced Trustsec Settings y actualice el Device name con CTS-ID y el campo password con la contraseña del comando (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



Troubleshoot

Para solucionar el problema, ejecute estas depuraciones en el 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
```

Fragmento de depuración:

*Feb 23 14:48:14.974: Datos de env. CTS: Force environment-data refresh bitmask 0x2

*Feb 23 14:48:14.974: Datos de env. CTS: download transport-type = CTS_TRANSPORT_IP_UDP

*Feb 23 14:48:14.974: cts_env_data COMPLETE: durante el estado env_data_complete, se obtuvo el evento 0(env_data_request)

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

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

*Feb 23 14:48:14.974: La clave de seguridad está presente en el dispositivo. Continúe con la descarga de datos envolventes sin paquetes // Inicie la autenticación sin PAC desde el 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: env_data_request_action: estado = 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), 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: env_data_request_action: estado = WAITING_RESPONSE, recibido = 0x0 petición = 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)El grupo privado aparece MUERTO, intente el grupo público

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

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

*Feb 23 14:48:14.974: Atributo AAA Context Add: (CTS env-data SM)attr(prueba)

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

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

*Feb 23 14:48:14.974: Atributo AAA Context Add: (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 req(0x7AB57A6AA2C0)

*Feb 23 14:48:14.975: Atributo AAA Context Add: (CTS env-data SM)attr(compatible con ip de varios servidores)

*Feb 23 14:48:14.975:   cts-device-capability = multiple-server-ip-supported

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

*Feb 23 14:48:14.975: Atributo AAA Context Add: (CTS env-data SM)attr(wnlx)

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

*Feb 23 14:48:14.975: cts_aaa_req_send: Solicitud AAA (0x7AB57A6AA2C0) enviada correctamente a AAA.

*Feb 23 14:48:14.975: RADIUS/ENCODE(0000000F):Origen tipo de componente = CTS

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

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

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

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

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

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

*Feb 23 14:48:14.975: RADIUS: Modo PAC less, secreto presente

*Feb 23 14:48:14.975: RADIUS: El atributo de paquetes CTS se agregó correctamente a la solicitud RADIUS

*Feb 23 14:48:14.975: RADIUS/ENCODE: Mejor dirección IP local 10.127.196.234 para Radius-Server 10.127.196.169

*Feb 23 14:48:14.975: RADIUS: Modo PAC less, secreto presente

*Feb 23 14:48:14.975: RADIUS (0000000F): Send Access-Request to 10.127.196.169:1812 id 1645/11, len 249 // Radius Access Request from the switch

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

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

*Feb 23 14:48:14.975: RADIUS: Proveedor, 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: Proveedor, 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: Proveedor, 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: User-Password [2] 18 *

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

*Feb 23 14:48:14.975: RADIUS: Tipo de servicio [6] 6 Saliente [5]

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

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

*Feb 23 14:48:14.975: RADIUS: Cisco AVpair [1] 33 "cts-pac-capability=cts-pac-less" // CTS PAC Less cv-pair attribute add to the request for ISE to handle the packet for PAC-less authentication

*Feb 23 14:48:14.975: RADIUS (0000000F): Envío de un Paquete Radius IPv4

*Feb 23 14:48:14.975: RADIUS (0000000F): Tiempo de espera iniciado 5 s

*Feb 23 14:48:14.990: RADIUS: Recibido desde id 1645/11 10.127.196.169:1812, Access-Accept, len 313. // Éxito de autenticación

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

*Feb 23 14:48:14.990: RADIUS: User-Name [1] 14 "#CTSREQUEST#"

*Feb 23 14:48:14.990: RADIUS: Clase [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]

*Feb 23 14:48:14.990: RADIUS: Proveedor, 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: Proveedor, 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: Proveedor, 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: Proveedor, 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: Proveedor, 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: Modo PAC less, secreto presente

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

*Feb 23 14:48:14.991: cts_aaa_callback: (CTS env-data SM)AAA requiere respuesta satisfactoria (0x7AB57A6AA2C0)

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

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

*Feb 23 14:48:14.991: AAA CTX FRAG LIMPIO: (CTS env-data SM)attr(compatible con ip de varios servidores)

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

*Feb 23 14:48:14.991:   Atajos AAA: Tipo desconocido (450).

*Feb 23 14:48:14.991:   Atajos AAA: Tipo desconocido (1324).

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

*Feb 23 14:48:14.991: Nombre de SLIST recibido. Configuración de cts_is_list_send_to_binos_req en FALSE

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

*Feb 23 14:48:14.991:   Atajos AAA: vencimiento de datos de entorno = 86400.

*Feb 23 14:48:14.991:   Atajos AAA: security-group-table = 0001-17.CTS env-data: Recepción de atributos AAA.   // Descargando los datos del entorno

CTS_AAA_LIST

nombre de lista(CTSServerList1) recibido en 1st Access-Accept

slist name(CTSServerList1) existe

CTS_AAA_SECURITY_GROUP_TAG

CTS_AAA_ENVIRONMENT_DATA_EXPIRY = 86400.

CTS_AAA_SGT_NAME_LIST

table(0001) recibido en 1st Access-Accept

Copie la tabla (0001) de instalada a recibida porque no hay cambios.

nuevo nombre(0001), gen(17)

CTS_AAA_DATA_END

*Feb 23 14:48:14.991: cts_env_data_WAITING_RESPONSE: durante el estado env_data_waiting_rsp, se obtuvo el evento 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: estado = EVALUANDO

*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: estado = EVALUANDO

*Feb 23 14:48:14.991: env_data_download_complete:

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

*Feb 23 14:48:14.991: Se espera igual que el recibido

*Feb 23 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)

*Feb 23 14:48:14.991: cts_env_data EVALUACIÓN: durante el estado env_data_assessment, se obtuvo el evento 4(env_data_complete)

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

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

*Feb 23 14:48:14.991: CTS-ifc-ev: informe de datos de env al núcleo, resultado: Satisfactorio

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

*Feb 23 14:48:14.991: env_data_install_action: clean installed sgt<->sgname table

*Feb 23 14:48:14.991: Limpiando la lista de sg-epg instalada

*Feb 23 14:48:14.991: Limpiando la lista de páginas predeterminadas instaladas

*Feb 23 14:48:14.991: env_data_install_action: tabla mcast_sgt actualizada

*Feb 23 14:48:14.991: Sincronización de datos Env con estado en espera 2

*Feb 23 14:48:14.991: SLIST es igual que la actualización anterior. No es necesario enviarlo a BINOS

*Feb 23 14:48:14.991: CTS-sg-epg-events:configurar default_sg 0 como datos env

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).