Configurar a autenticação sem PAC do ISE 3.4 entre o ISE e o NAD para Trustsec

Contents

Introdução

O documento descreve a configuração inicial para a configuração sem PAC entre os clientes ISE e NAD para o download de dados do ambiente Trustsec.

Pré-requisitos

Requisitos

- Familiaridade com o Cisco TrustSec como uma solução de segurança de rede.
- Conhecimento do Identity Services Engine (ISE) para gerenciar a segurança da rede.
- Entendimento básico do EAP (Extensible Authentication Protocol) como uma estrutura para transportar informações de autenticação.

Componentes Utilizados

Identity Services Engine (ISE) versão 3.4.x

Cisco IOS® 17.15.1 ou posterior

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações

No modo sem PAC, as políticas do TrustSec são mais fáceis de implementar porque não exigem uma PAC (Protected Access Credential), que geralmente é necessária para a comunicação segura entre dispositivos e o Identity Services Engine (ISE). Essa abordagem é particularmente benéfica em ambientes com vários nós do ISE. Se o nó principal ficar off-line, os dispositivos poderão alternar automaticamente para um backup sem precisar restabelecer suas credenciais, reduzindo interrupções. A autenticação sem PAC simplifica o processo, tornando-o mais escalável e fácil de usar, além de oferecer suporte a métodos de segurança modernos alinhados com os princípios da Zero Trust.

Nesse modo, os dispositivos começam enviando uma solicitação que inclui um nome de usuário e uma senha. O ISE responde propondo uma sessão segura. Uma vez configurada essa sessão, o ISE fornece informações importantes necessárias para uma comunicação segura. Isso inclui uma chave para a segurança e detalhes como identidade e tempo do servidor. Essas informações são usadas para garantir acesso seguro e contínuo às políticas e aos dados necessários.

Configurar

Configurações

Configuração do Switch

Neste documento, a configuração para autenticação sem PAC é configurada usando o switch Cisco C9300. Qualquer switch que execute a versão 17.15.1 ou superior pode executar autenticação sem PAC com o Identity Services Engine (ISE).

Passo 1: Configure o servidor Radius e o grupo radius no switch no terminal de configuração do switch.

Servidor Radius:

```
radius server

 address ipv4

        auth-port 1812 acct-port 1813

 key
```

Grupo Radius:

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

Passo 2: Mapeie o grupo de servidores radius para autorização cts e dot1x para autenticação com sem PAC.

Mapeamento CTS:

<#root>

```
cts authorization list
```

cts-mlist

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

Autenticação Dot1x:

<#root>

```
aaa authentication dot1x default group
```

```
aaa authorization network
```

cts-mlist

```
 group
```

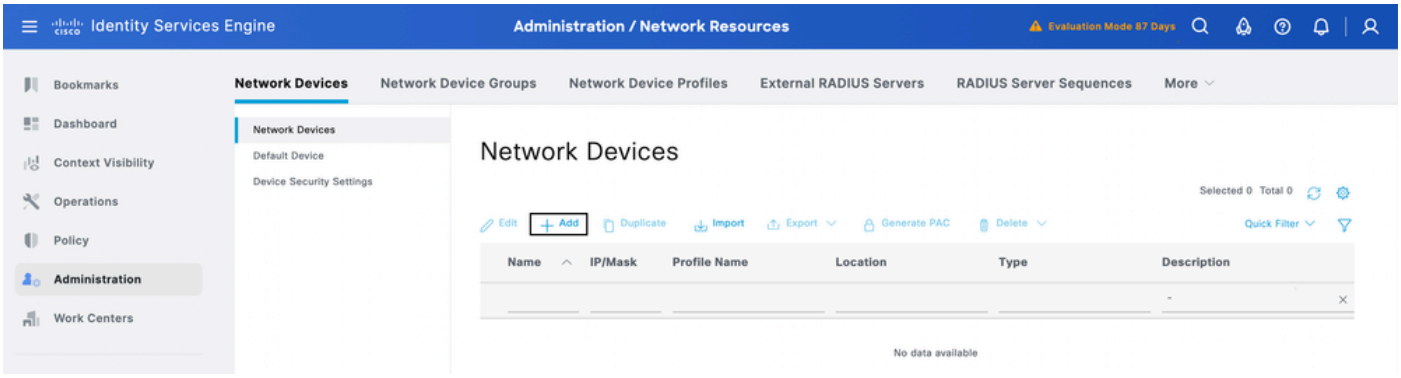
Passo 3: Configure o CTS-ID e a senha sob o modo de ativação no switch

```
cts credentials id

        password
```

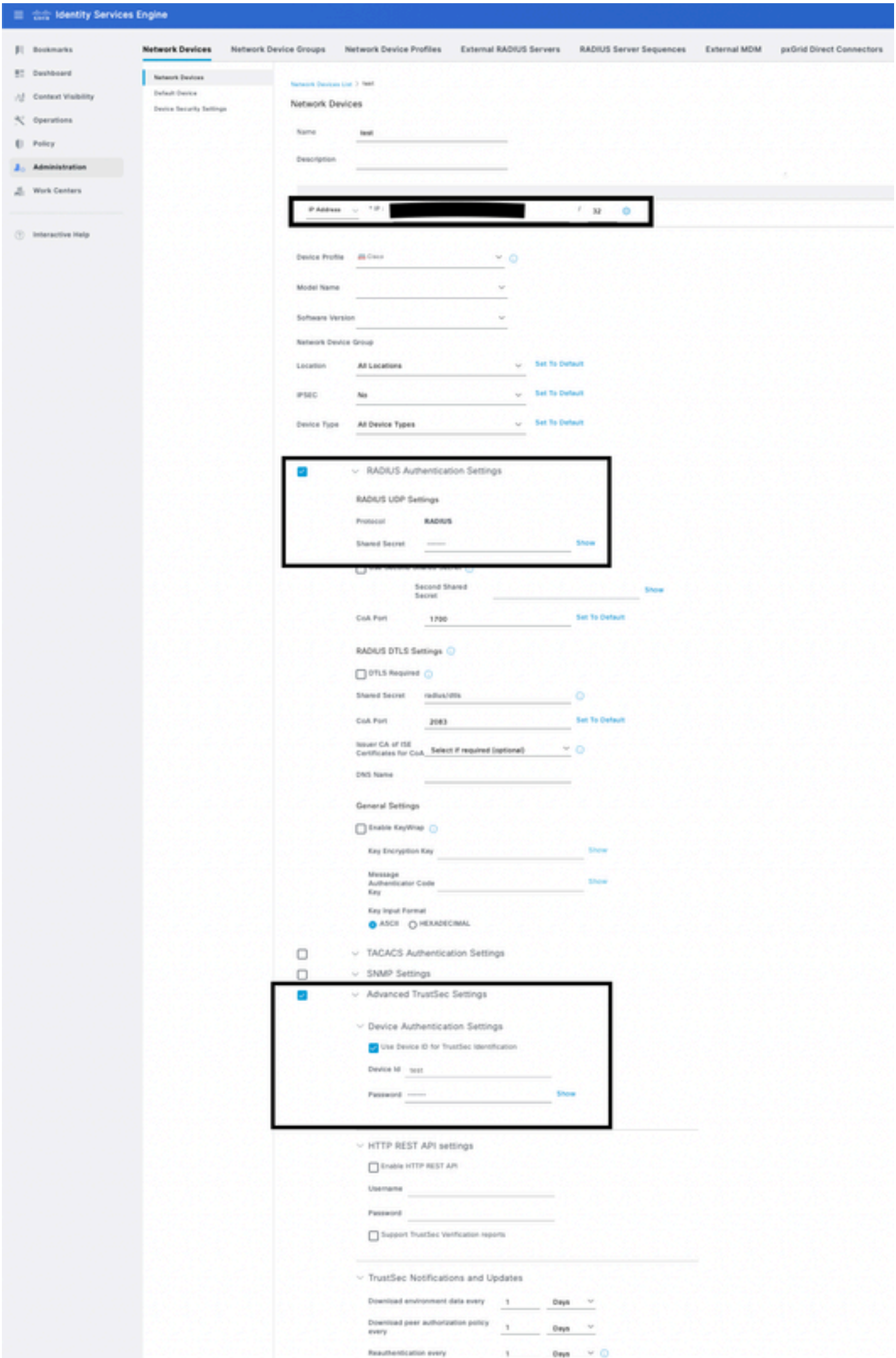
Configuração do ISE

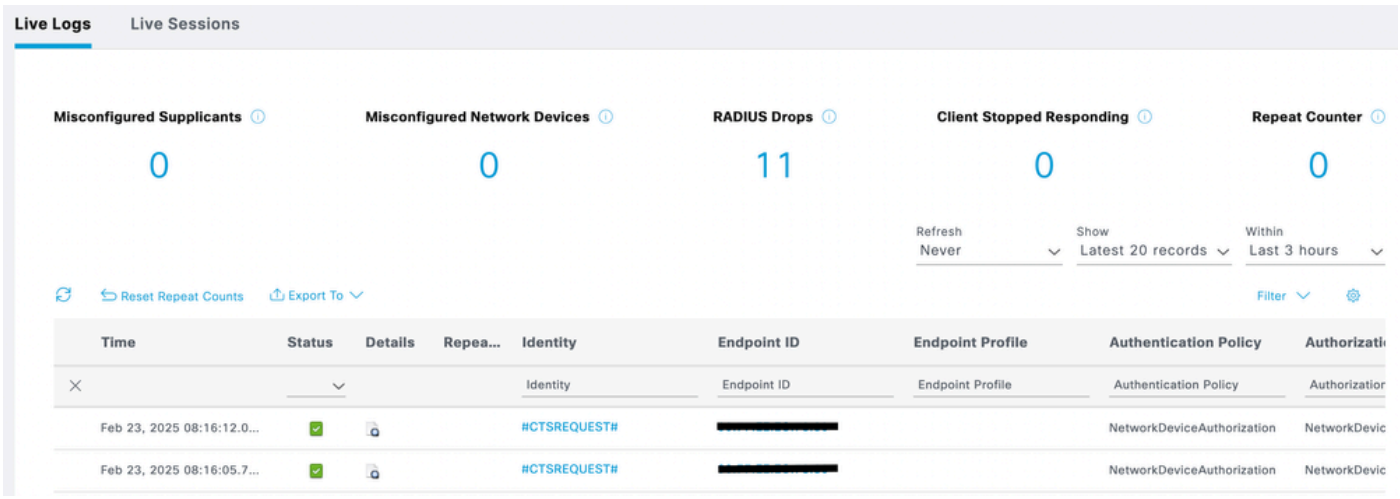
1. No ISE, configure o dispositivo de rede em Administração > Recursos de Rede > Dispositivos de Rede > Dispositivos de Rede. Clique em adicionar para adicionar o switch ao servidor ISE.

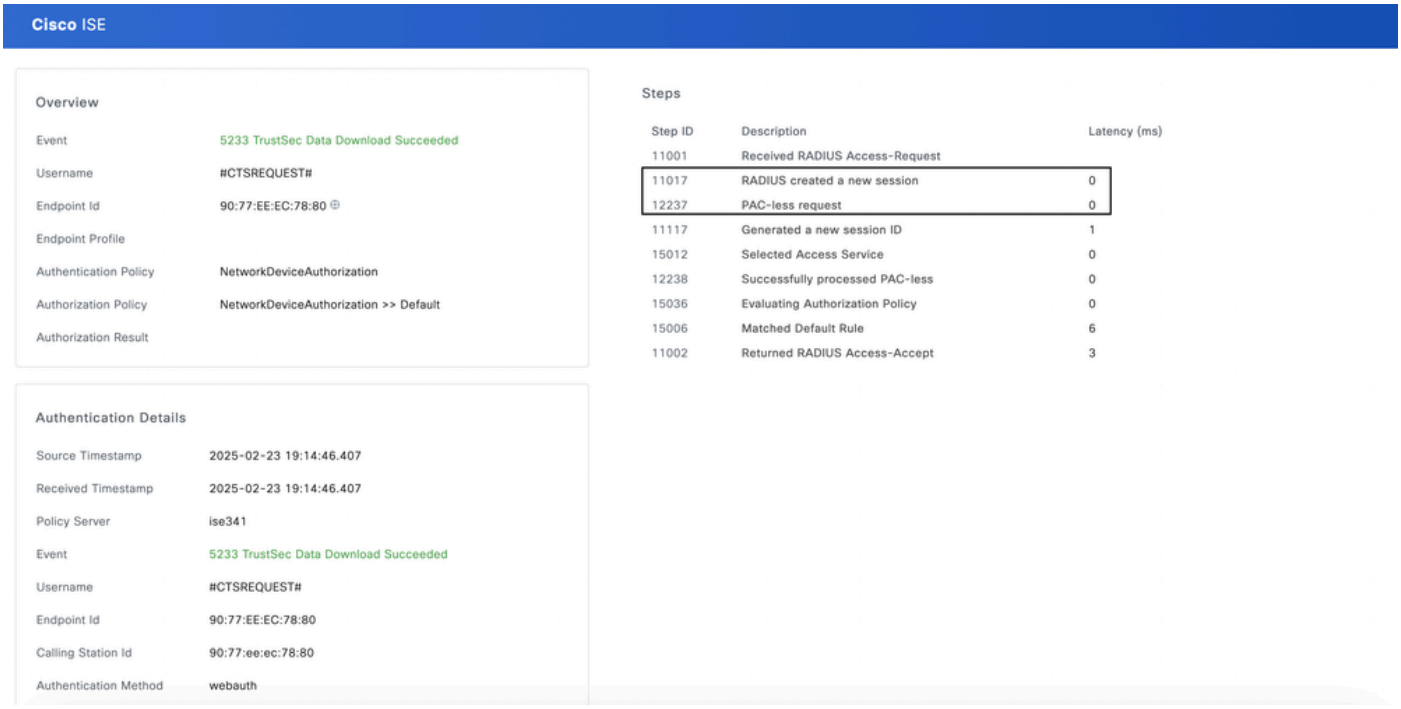


2. Adicione o endereço IP NAD no campo do endereço IP para que o ISE processe a solicitação radius para a autenticação trustsec do switch.
3. Ative Radius Authentication Settings para o cliente NAD e insira a chave secreta compartilhada Radius.

4. Habilite Configurações avançadas do Trustsec e atualize o Nome do dispositivo com o CTS-ID e o campo de senha com a senha do comando (identificação de credenciais cts <CTS-ID> senha <Senha>).


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





Troubleshooting

Para solucionar o problema, execute estas depurações no 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
```

Trecho de depuração:

*23 de fevereiro 14:48:14.974: Dados de ambiente CTS: Forçar máscara de bits de atualização de dados do ambiente 0x2

*23 de fevereiro 14:48:14.974: Dados de ambiente CTS: download transport-type = CTS_TRANSPORT_IP_UDP

*23 de fevereiro 14:48:14.974: cts_env_data COMPLETE: durante o estado env_data_complete, evento 0 obtido (env_data_request)

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

*23 de fevereiro 14:48:14.974: env_data_waiting_rsp_enter: estado = WAITING_RESPONSE

*23 de fevereiro 14:48:14.974: A chave segura está presente no dispositivo, continue com o download de dados de env sem pac // inicie a autenticação sem PAC do switch

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

*23 de fevereiro 14:48:14.974: env_data_request_action: estado = WAITING_RESPONSE

*23 de fevereiro 14:48:14.974: env_data_download_complete:

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

*23 de fevereiro 14:48:14.974: status(FALSE), req(x0), rec(x0), expected(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 de fevereiro 14:48:14.974: env_data_request_action: estado = WAITING_RESPONSE, recebido = 0x0 solicitação = 0x0

*23 de fevereiro 14:48:14.974: cts_env_data_aaa_req_setup : aaa_id = 15

*23 de fevereiro 14:48:14.974: cts_aaa_req_setup: (CTS env-data SM)O grupo privado aparece DEAD, tente o grupo público

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

*23 de fevereiro 14:48:14.974: nome de usuário = #CTSREQUEST#

*23 de fevereiro 14:48:14.974: Atributo de adição de contexto AAA: (CTS env-data SM)attr(test)

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

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

*23 de fevereiro 14:48:14.974: Atributo de adição de contexto AAA: (CTS env-data SM)attr(env-data-fragment)

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

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

*23 de fevereiro 14:48:14.975: Atributo de adição de contexto AAA: (CTS env-data SM)attr(suporte a IP de vários servidores)

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

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

*23 de fevereiro 14:48:14.975: Atributo de adição de contexto AAA: (CTS env-data SM)attr(wnlx)

*23 de fevereiro 14:48:14.975:   clid = wnlx

*23 de fevereiro 14:48:14.975: cts_aaa_req_send: AAA req(0x7AB57A6AA2C0) enviado com êxito para AAA.

*23 de fevereiro 14:48:14.975: RADIUS/ENCODE(0000000F):Orig. tipo de componente = CTS

*23 de fevereiro 14:48:14.975: RAIO(0000000F): Config NAS IP: 0.0.0.0

*23 de fevereiro 14:48:14.975: vrfid: [65535] id da tabela ipv6: [0]

*23 de fevereiro 14:48:14.975: idb é NULL

*23 de fevereiro 14:48:14.975: RAIO(0000000F): Configuração do NAS IPv6: ::

*23 de fevereiro 14:48:14.975: RAIO/CODIFICAÇÃO(0000000F): acct_session_id: 4003

*23 de fevereiro 14:48:14.975: RAIO(0000000F): enviando

*23 de fevereiro 14:48:14.975: RADIUS: Modo sem PAC, segredo está presente

*23 de fevereiro 14:48:14.975: RADIUS: Atributo pacless CTS adicionado com êxito à solicitação radius

*23 de fevereiro 14:48:14.975: RAIO/CODIFICAÇÃO: Melhor endereço IP local 10.127.196.234 para servidor Radius 10.127.196.169

*23 de fevereiro 14:48:14.975: RADIUS: Modo sem PAC, segredo está presente

*23 de fevereiro 14:48:14.975: RAIO(0000000F): Enviar solicitação de acesso para

10.127.196.169:1812 id 1645/11, len 249 // Solicitação de acesso Radius do switch

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

*23 de fevereiro 14:48:14.975: RADIUS: Nome de usuário [1] 14 "#CTSREQUEST#"

*23 de fevereiro 14:48:14.975: RADIUS: Fornecedor, Cisco [26] 33

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

*23 de fevereiro 14:48:14.975: RADIUS: Fornecedor, Cisco [26] 47

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

*23 de fevereiro 14:48:14.975: RADIUS: Fornecedor, Cisco [26] 58

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

*23 de fevereiro 14:48:14.975: RADIUS: Senha do usuário [2] 18 *

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

*23 de fevereiro 14:48:14.975: RADIUS: Tipo de serviço [6] 6 saída [5]

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

*23 de fevereiro 14:48:14.975: RADIUS: Fornecedor, Cisco [26] 39

*23 de fevereiro 14:48:14.975: RADIUS: Cisco AVpair [1] 33 "cts-pac-capability=cts-pac-less" // CTS PAC Menos atributo cv-pair adicione à solicitação do ISE para manipular o pacote para autenticação sem PAC

*23 de fevereiro 14:48:14.975: RAIO(0000000F): Enviando um pacote IPv4 Radius

*23 de fevereiro 14:48:14.975: RAIO(0000000F): Iniciado o tempo limite de 5 segundos

*23 de fevereiro 14:48:14.990: RADIUS: Recebido da id 1645/11 10.127.196.169:1812, Access-Accept, len 313. // Êxito na autenticação

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

*23 de fevereiro 14:48:14.990: RADIUS: Nome de usuário [1] 14 "#CTSREQUEST#"

*23 de fevereiro 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 [CACS:0a7fc4a9T7h]

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

RADIUS: 8 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 de fevereiro 14:48:14.990: RADIUS: Fornecedor, Cisco [26] 39

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

*23 de fevereiro 14:48:14.990: RADIUS: Fornecedor, Cisco [26] 43

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

*23 de fevereiro 14:48:14.991: RADIUS: Fornecedor, Cisco [26] 38

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

*23 de fevereiro 14:48:14.991: RADIUS: Fornecedor, Cisco [26] 41

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

*23 de fevereiro 14:48:14.991: RADIUS: Fornecedor, Cisco [26] 40

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

*23 de fevereiro 14:48:14.991: RADIUS: Modo sem PAC, segredo está presente

*23 de fevereiro 14:48:14.991: RAIO(0000000F): Recebido da id 1645/11

*23 de fevereiro 14:48:14.991: cts_aaa_callback: (CTS env-data SM)AAA req(0x7AB57A6AA2C0) resposta com êxito

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

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

*23 de fevereiro 14:48:14.991: AAA CTX FRAG CLEAN: (CTS env-data SM)attr(suporte a IP de vários servidores)

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

*23 de fevereiro 14:48:14.991: AAA attr: Tipo desconhecido (450).

*23 de fevereiro 14:48:14.991: AAA attr: Tipo desconhecido (1324).

*23 de fevereiro 14:48:14.991: AAA attr: server-list = CTSServerList1-0001.

*23 de fevereiro 14:48:14.991: Nome SLIST recebido. Definindo cts_is_list_send_to_binos_req como FALSE

*23 de fevereiro 14:48:14.991: AAA attr: security-group-tag = 0002-00.

*23 de fevereiro 14:48:14.991: AAA attr: expiração de dados de ambiente = 86400.

*23 de fevereiro 14:48:14.991: AAA attr: security-group-table = 0001-17.CTS env-data: Recebendo atributos AAA. // Baixando os dados do ambiente

CTS_AAA_SLIST

nome da lista (CTSServerList1) recebido no 1º Access-Accept

nome da lista (CTSServerList1) existe

CTS_AAA_SECURITY_GROUP_TAG

CTS_AAA_ENVIRONMENT_DATA_EXPIRY = 86400.

CTS_AAA_SGT_NAME_LIST

table(0001) recebido no 1o Access-Accept

Copie a tabela (0001) de instalada para recebida porque não houve alteração.

novo nome(0001), gen(17)

CTS_AAA_DATA_END

*23 de fevereiro 14:48:14.991: cts_env_data WAITING_RESPONSE: durante o estado env_data_waiting_rsp, evento 1 recebido (env_data_received)

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

*23 de fevereiro 14:48:14.991: env_data_assessment_enter: estado = AVALIANDO

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

*23 de fevereiro 14:48:14.991: env_data_assessment_action: estado = AVALIANDO

*23 de fevereiro 14:48:14.991: env_data_download_complete:

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

*23 de fevereiro 14:48:14.991: Esperar o mesmo que recebido

*23 de fevereiro 14:48:14.991: status(TRUE), req(x81), rec(xC87), expected(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 de fevereiro 14:48:14.991: cts_env_data AVALIANDO: durante o estado env_data_assessment, evento 4 obtido (env_data_complete)

*23 de fevereiro 14:48:14.991: @@ cts_env_data AVALIAÇÃO: env_data_assessment -> env_data_complete

*23 de fevereiro 14:48:14.991: env_data_complete_enter: estado = COMPLETO

*23 de fevereiro 14:48:14.991: CTS-ifc-ev: relatório de dados env para núcleo, resultado: Bem-sucedido

*23 de fevereiro 14:48:14.991: env_data_install_action: estado = CONCLUÍDO concluído.tipos 0x0

*23 de fevereiro 14:48:14.991: env_data_install_action: limpe a tabela sgt<->sgname instalada

*23 de fevereiro 14:48:14.991: Limpando lista sg-epg instalada

*23 de fevereiro 14:48:14.991: Limpando lista de epg padrão instalada

*23 de fevereiro 14:48:14.991: env_data_install_action: tabela mcast_sgt atualizada

*23 de fevereiro 14:48:14.991: Sincronização de dados de ambiente para status de espera 2

*23 de fevereiro 14:48:14.991: SLIST é igual à atualização anterior. Não há necessidade de enviá-lo para o BINOS

*23 de fevereiro 14:48:14.991: CTS-sg-epg-events:definição de default_sg 0 como env data

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.