為Trustsec在ISE和NAD之間設定ISE 3.4 PAC無身份驗證

目錄

簡介

本文檔介紹在ISE和NAD客戶端之間為Trustsec環境資料下載進行無PAC配置的初始設定。

必要條件

需求

- 熟悉Cisco TrustSec作為網路安全解決方案。
- 身份服務引擎(ISE)知識，用於管理網路安全。
- 基本瞭解可擴展身份驗證協定(EAP)作為傳輸身份驗證資訊的框架。

採用元件

身分識別服務引擎(ISE)版本3.4.x

Cisco IOS® 17.15.1或更高版本

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

資訊

在無PAC模式下，TrustSec策略更容易實施，因為它們不需要保護訪問憑證(PAC)，而保護訪問憑

證通常是在裝置和身份服務引擎(ISE)之間進行安全通訊所必需的。 此方法尤其適用於具有多個ISE節點的環境。如果主節點離線，裝置可以自動切換到備份而無需重新建立其憑證，從而減少了中斷。無PAC身份驗證簡化了流程，使其更具可擴充性和使用者友好性，並支援符合零信任原則的現代安全方法。

在此模式下，裝置首先傳送包含使用者名稱和密碼的請求。ISE通過建議安全會話進行響應。設定此會話後，ISE會提供安全通訊所需的重要資訊。其中包括一個用於安全性和諸如伺服器身份和定時等詳細資訊的金鑰。此資訊用於確保安全、連續地訪問必要的策略和資料。

設定

組態

交換器組態

在本文檔中，使用Cisco C9300交換機配置無PAC身份驗證設定。任何運行版本17.15.1或更高版本的交換機都可以通過身份服務引擎(ISE)執行無PAC身份驗證。

步驟 1:在交換機的配置終端下配置交換機上的Radius伺服器和RADIUS組。

Radius伺服器：

```
radius server

 address ipv4


        auth-port 1812 acct-port 1813

 key
```

Radius群組：

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

步驟 2:將radius伺服器組對映到cts authorization和dot1x，以便使用無PAC進行身份驗證。

CTS對映：

```
<#root>
cts authorization list
cts-mlist
   // cts-mlist is the name of the authorization list
```

Dot1x身份驗證：

```
<#root>
aaa authentication dot1x default group

aaa authorization network
cts-mlist
 group
```

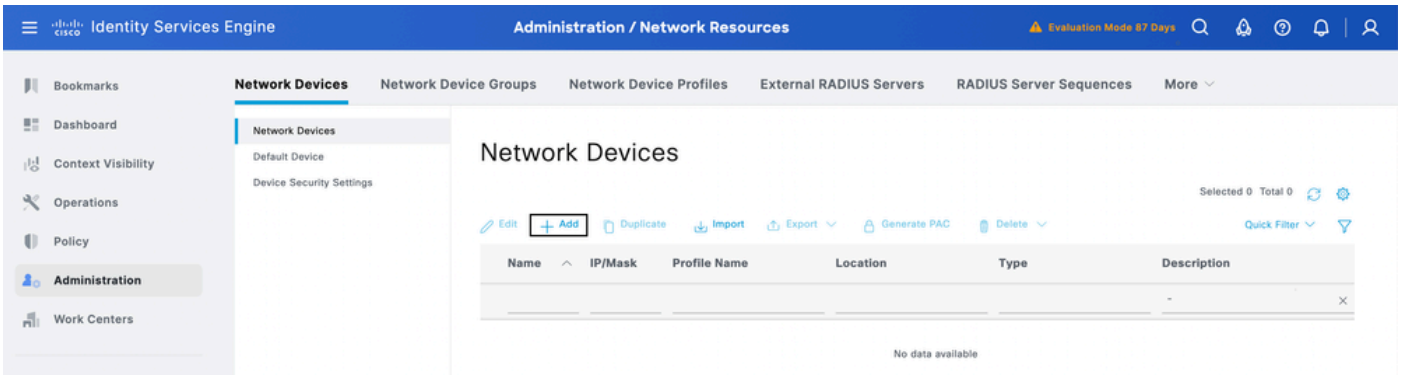
步驟 3:在交換器上的enable模式下設定CTS-ID和密碼

```
cts credentials id

        password
```

ISE 組態

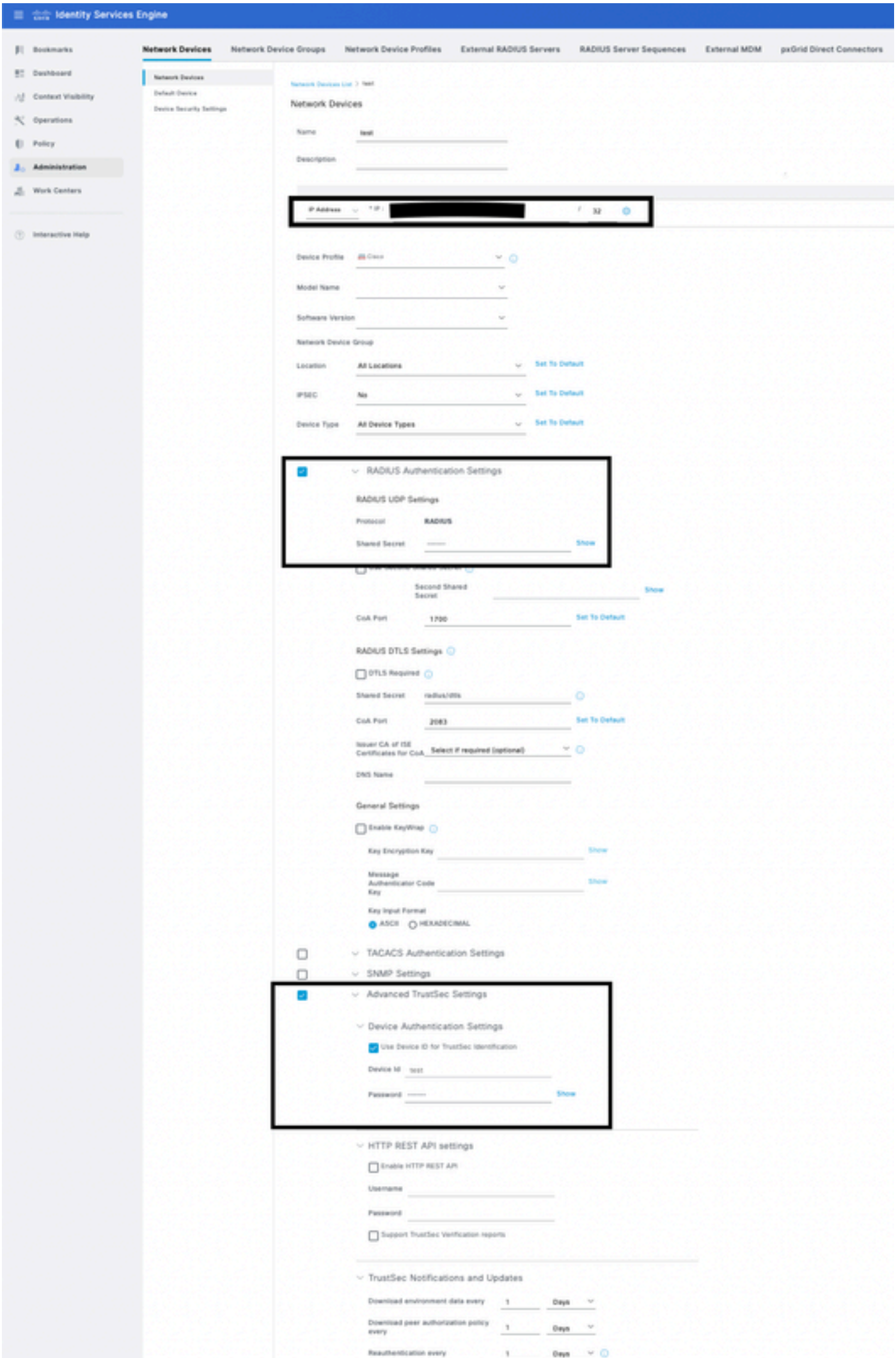
1.在ISE上，在管理>網路資源>網路裝置>網路裝置下配置網路裝置。按一下add將交換機新增到ISE伺服器。

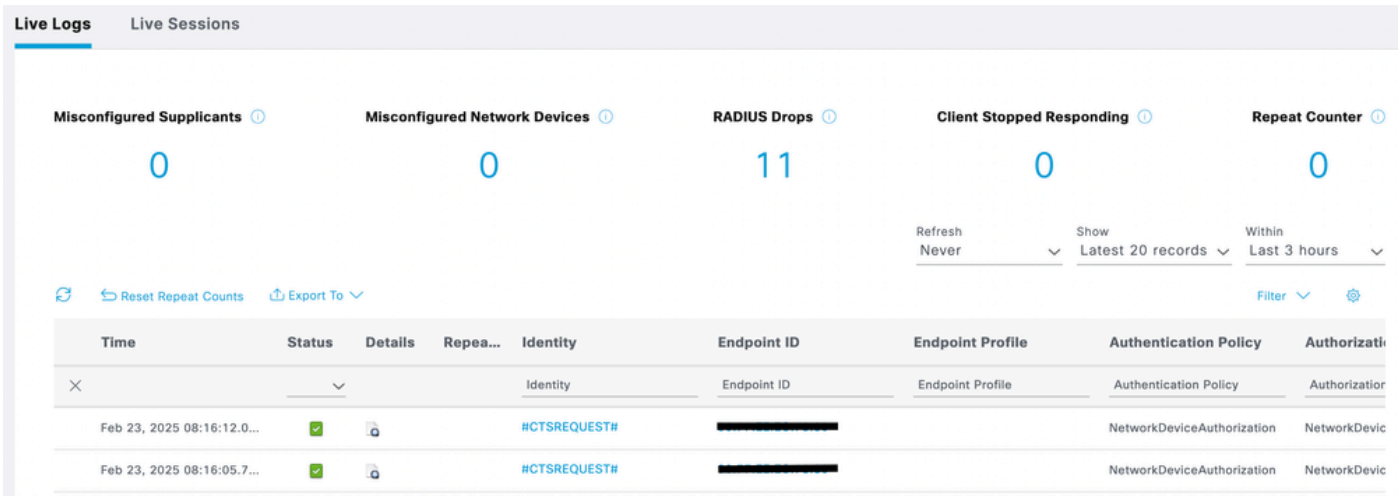


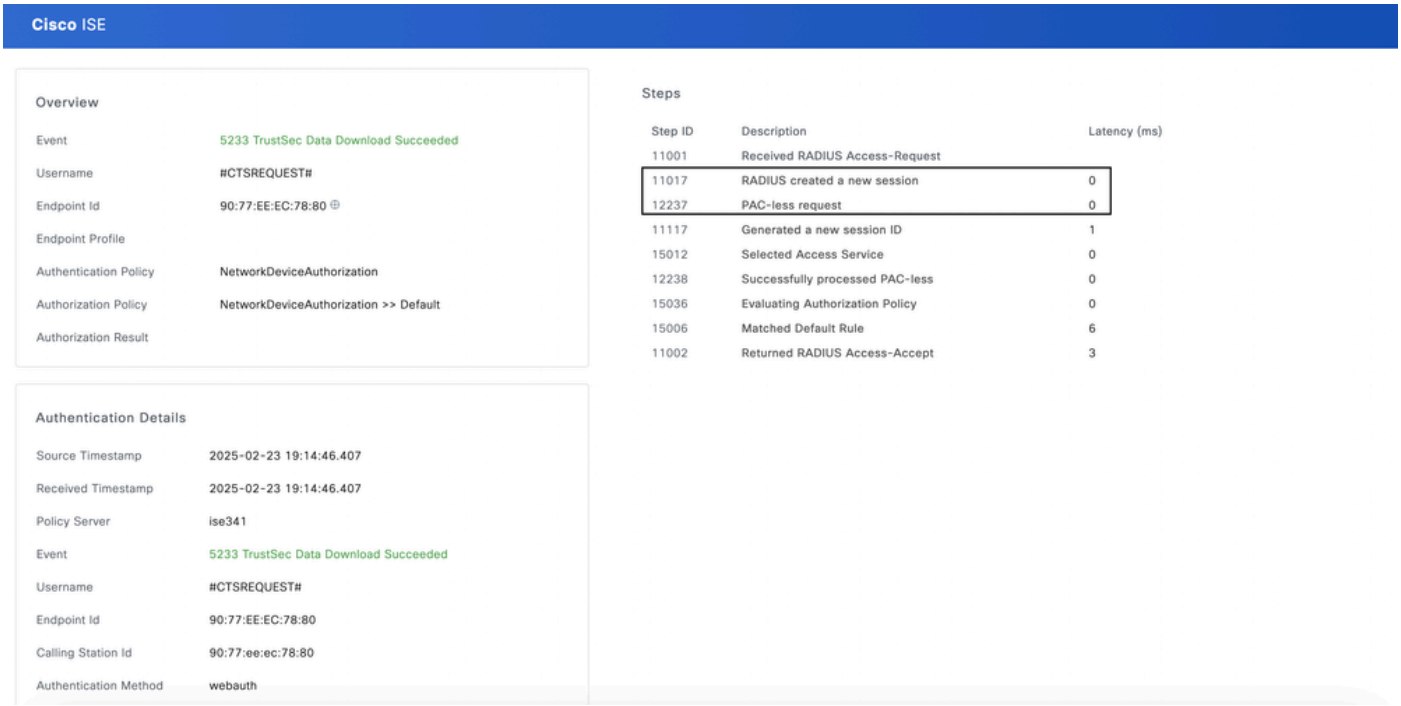
2.在ISE的ip address欄位中新增NAD IP地址，以處理來自交換機的trustsec身份驗證的radius請求。

3.為NAD客戶端啟用Radius身份驗證設定，並輸入Radius共用金鑰。

4.啟用Advanced Trustsec Settings，並使用CTS-ID更新Device name，使用命令中的password(cts credentials id <CTS-ID> password <Password>)更新密碼欄位。


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





疑難排解

若要疑難排解，請在交換器上執行以下偵錯：

```
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
```

調試片段：

*2023年2月14:48:14.974:CTS環境資料：強制環境資料刷新位掩碼0x2

*2023年2月14:48:14.974:CTS環境資料：download transport-type = CTS_TRANSPORT_IP_UDP

*2023年2月14:48:14.974:　cts_env_data完成：在狀態env_data_complete期間，獲取事件0(env_data_request)

*2023年2月14:48:14.974:@@ cts_env_data完成：env_data_complete -> env_data_waiting_rsp

*2023年2月14:48:14.974:env_data_waiting_rsp_enter:state = WAITING_RESPONSE

*2023年2月14:48:14.974:裝置上存在安全金鑰，繼續無資料包環境資料下載//從交換機啟動無資料包環境身份驗證

*2023年2月14:48:14.974:cts_aaa_is_fragmented:(CTS env-data SM)NOT-FRAG attr_q(0)

*2023年2月14:48:14.974:env_data_request_action:state = WAITING_RESPONSE

*2023年2月14:48:14.974:env_data_download_complete:

狀態(FALSE)，請求(x0),rec(x0)

*2023年2月14:48:14.974:　狀態(FALSE)、req(x0)、rec(x0)、expect(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)

*2023年2月14:48:14.974:env_data_request_action:狀態= WAITING_RESPONSE，已接收= 0x0請求= 0x0

*2023年2月14:48:14.974:cts_env_data_aaa_req_setup :aaa_id = 15

*2023年2月14:48:14.974:cts_aaa_req_setup:(CTS env-data SM)私有組顯示DEAD，嘗試公用組

*2023年2月14:48:14.974:cts_aaa_attr_add:AAA請求(0x7AB57A6AA2C0)

*2023年2月14:48:14.974: 使用者名稱= #CTSREQUEST#

*2023年2月14:48:14.974:AAA內容新增屬性：(CTS env-data SM)attr（測試）

*2023年2月14:48:14.974: cts-environment-data =測試

*2023年2月14:48:14.974:cts_aaa_attr_add:AAA請求(0x7AB57A6AA2C0)

*2023年2月14:48:14.974:AAA內容新增屬性：(CTS env-data SM)attr(env-data-fragment)

*2023年2月14:48:14.974: cts-device-capability = env-data-fragment

*2023年2月14:48:14.974:cts_aaa_attr_add:AAA請求(0x7AB57A6AA2C0)

*2023年2月14:48:14.975:AAA內容新增屬性：(CTS env-data SM)attr（多伺服器 — ip-supported）

*2023年2月14:48:14.975: cts-device-capability =多伺服器 — ip支援

*2023年2月14:48:14.975:cts_aaa_attr_add:AAA請求(0x7AB57A6AA2C0)

*2023年2月14:48:14.975:AAA內容新增屬性：(CTS env-data SM)attr(wnlx)

*2023年2月14:48:14.975: clid = wnlx

*2023年2月14:48:14.975:cts_aaa_req_send:AAA請求(0x7AB57A6AA2C0)已成功傳送到AAA。

*2023年2月14:48:14.975:RADIUS/ENCODE(0000000F)：源。元件型別= CTS

*2023年2月14:48:14.975:RADIUS(0000000F):配置NAS IP:0.0.0.0

*2023年2月14:48:14.975:vrfid:[65535] ipv6 tableid:[0]

*2023年2月14:48:14.975:idb為空

*2023年2月14:48:14.975:RADIUS(0000000F):配置NAS IPv6:::

*2023年2月14:48:14.975:RADIUS/ENCODE(0000000F):acct_session_id:4003

*2023年2月14:48:14.975:RADIUS(0000000F):傳送

*2023年2月14:48:14.975:RADIUS:PAC較少模式，存在密碼

*2023年2月14:48:14.975:RADIUS:已成功將CTS pacless屬性新增到radius請求

*2023年2月14:48:14.975:RADIUS/編碼：Radius-Server 10.127.196.169的最佳本地IP地址 10.127.196.234

*2023年2月14:48:14.975:RADIUS:PAC較少模式，存在密碼

*2023年2月14:48:14.975:RADIUS(0000000F):將存取要求傳送到10.127.196.169:1812 id 1645/11,len 249 //交換器的Radius存取要求

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

*2023年2月14:48:14.975:RADIUS: User-Name [1] 14 "#CTSREQUEST#"

*2023年2月14:48:14.975:RADIUS: 思科供應商[26] 33

*2023年2月14:48:14.975:RADIUS: Cisco AVpair [1] 27 "cts-environment-data=test"

*2023年2月14:48:14.975:RADIUS: 思科供應商[26] 47

*2023年2月14:48:14.975:RADIUS: Cisco AVpair [1] 41 "cts-device-capability=env-data-fragment"

*2023年2月14:48:14.975:RADIUS: 思科供應商[26] 58

*2023年2月14:48:14.975:RADIUS: Cisco AVpair [1] 52 "cts-device-capability=multiple-server-ip-supported"

*2023年2月14:48:14.975:RADIUS: User-Password [2] 18 *

*2023年2月14:48:14.975:RADIUS: Calling-Station-Id [31] 8 "wnlx"

*2023年2月14:48:14.975:RADIUS: Service-Type [6] 6 Outbound [5]

*2023年2月14:48:14.975:RADIUS: NAS-IP-Address [4] 6 10.127.196.234

*2023年2月14:48:14.975:RADIUS: 思科供應商[26] 39

*2023年2月14:48:14.975:RADIUS: Cisco AVpair [1] 33 "cts-pac-capability=cts-pac-less" // CTS PAC Less cv-pair屬性新增到ISE處理資料包以進行無資料包身份驗證的請求

*2023年2月14:48:14.975:RADIUS(0000000F):傳送IPv4 Radius資料包

*2023年2月14:48:14.975:RADIUS(0000000F):已啟動5秒超時

*2月23日14:48:14.990:RADIUS:接收自id 1645/11 10.127.196.169:1812, Access-Accept， len 313。 //身份驗證成功

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

*2月23日14:48:14.990:RADIUS: User-Name [1] 14 "#CTSREQUEST#"

*2月23日14:48:14.990:RADIUS: 類[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]

*2月23日14:48:14.990:RADIUS: 思科供應商[26] 39

*2月23日14:48:14.990:RADIUS: Cisco AVpair [1] 33 "cts-pac-capability=cts-pac-less"

*2月23日14:48:14.990:RADIUS: 思科供應商[26] 43

*2月23日14:48:14.991:RADIUS: Cisco AVpair [1] 37 "cts:server-list=CTServerList1-0001"

*2月23日14:48:14.991:RADIUS: 思科供應商[26] 38

*2月23日14:48:14.991:RADIUS: Cisco AVpair [1] 32 "cts:security-group-tag=0002-00"

*2月23日14:48:14.991:RADIUS: 思科供應商[26] 41

*2月23日14:48:14.991:RADIUS: Cisco AVpair [1] 35 "cts:environment-data-expiry=86400"

*2月23日14:48:14.991:RADIUS: 思科供應商[26] 40

*2月23日14:48:14.991:RADIUS: Cisco AVpair [1] 34 "cts:security-group-table=0001-17"

*2月23日14:48:14.991:RADIUS:PAC較少模式，存在密碼

*2月23日14:48:14.991:RADIUS(0000000F):從1645/11號案件收到

*2月23日14:48:14.991:cts_aaa_callback:(CTS env-data SM)AAA req(0x7AB57A6AA2C0)響應成功

*2月23日14:48:14.991:AAA CTX FRAG CLEAN:(CTS env-data SM)attr（測試）

*2月23日14:48:14.991:AAA CTX FRAG CLEAN:(CTS env-data SM)attr(env-data-fragment)

*2月23日14:48:14.991:AAA CTX FRAG CLEAN:(CTS env-data SM)attr（多伺服器 — ip-supported）

*2月23日14:48:14.991:AAA CTX FRAG CLEAN:(CTS env-data SM)attr(wnlx)

*2月23日14:48:14.991: AAA屬性：未知型別(450)。

*2月23日14:48:14.991: AAA屬性：未知型別(1324)。

*2月23日14:48:14.991: AAA屬性：server-list = CTSServerList1-0001。

*2月23日14:48:14.991:已收到SLIST名稱。將cts_is_slist_send_to_binos_req設定為FALSE

*2月23日14:48:14.991: AAA屬性：security-group-tag = 0002-00。

*2月23日14:48:14.991: AAA屬性：environment-data-expiry = 86400。

*2月23日14:48:14.991: AAA屬性：security-group-table = 0001-17.CTS env-data:接收AAA屬性。
  //下載環境資料

  CTS_AAA_SLIST

    在1st Access-Accept中接收的slist name(CTSServerList1)

    slist name(CTSServerList1)存在

  CTS_AAA_SECURITY_GROUP_TAG

CTS_AAA_ENVIRONMENT_DATA_EXPIRY = 86400。

CTS_AAA_SGT_NAME_LIST

表(0001)在第1次訪問中接收 — 接受

將表(0001)從已安裝複製到已接收，因為沒有更改。

新名稱(0001),gen(17)

CTS_AAA_DATA_END

*2月23日14:48:14.991: cts_env_data WAITING_RESPONSE:在狀態env_data_waiting_rsp期間，獲取事件1(env_data_received)

*2月23日14:48:14.991:@@ cts_env_data WAITING_RESPONSE:env_data_waiting_rsp -> env_data_assessing

*2月23日14:48:14.991:env_data_assessing_enter:狀態=評估

*2月23日14:48:14.991:cts_aaa_is_fragmented:(CTS env-data SM)NOT-FRAG attr_q(0)

*2月23日14:48:14.991:env_data_assessing_action:狀態=評估

*2月23日14:48:14.991:env_data_download_complete:

狀態(FALSE)，請求(x81),rec(xC87)

*2月23日14:48:14.991:期望與收到的相同

*2月23日14:48:14.991: status(TRUE)、req(x81)、rec(xC87)、expect(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)

*2月23日14:48:14.991: cts_env_data評估：狀態env_data_assessing期間，獲取事件4(env_data_complete)

*2月23日14:48:14.991:@@ cts_env_data正在評估：env_data_assessing -> env_data_complete

*2月23日14:48:14.991:env_data_complete_enter:狀態=完成

*2月23日14:48:14.991:CTS-ifc-ev:env資料包告至核心，結果：成功

*2月23日14:48:14.991:env_data_install_action:狀態=完成。型別0x0

*2月23日14:48:14.991:env_data_install_action:清除已安裝的sgt<->sgname表

*2月23日14:48:14.991:正在清理已安裝的sg-epg清單

*2月23日14:48:14.991:正在清除已安裝的預設epg清單

*2月23日14:48:14.991:env_data_install_action:mcast_sgt表已更新

*2月23日14:48:14.991:環境資料同步到備用狀態2

*2月23日14:48:14.991:SLIST與以前的刷新相同。無需將其傳送到BINOS

*2月23日14:48:14.991:CTS-sg-epg-events：將default_sg 0設定為env data

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。