

在ISE 2.2上配置TrustSec多個矩陣

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[多矩陣](#)

[DefCon矩陣](#)

[設定](#)

[網路圖表](#)

[組態](#)

[1. RADIUS/CTS的基本交換機配置](#)

[2. CTS PAC](#)

[3. 交換機上的CTS配置。](#)

[4. ISE上的基本CTS配置。](#)

[5. ISE上的多個矩陣和DefCon配置。](#)

[6. SGT分類](#)

[7. CTS策略下載](#)

[驗證](#)

[多矩陣](#)

[DefCon部署](#)

[疑難排解](#)

[PAC調配](#)

[環境資料下載](#)

[CTS策略](#)

簡介

本檔案介紹在思科身分識別服務引擎(ISE)2.2中使用多個TrustSec矩陣和DefCon矩陣。這是在ISE 2.2中引入的新TrustSec功能，可改善網路中的粒度。

必要條件

需求

思科建議您瞭解以下主題：

- Cisco TrustSec(CTS)元件的基礎知識
- Catalyst交換機CLI配置基礎知識
- 身分識別服務引擎(ISE)配置體驗

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 身分識別服務引擎2.2
- Cisco Catalyst交換機3850 03.07.03.E
- Cisco Catalyst交換器3750X 15.2(4)E1
- Windows 7電腦

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。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

背景資訊

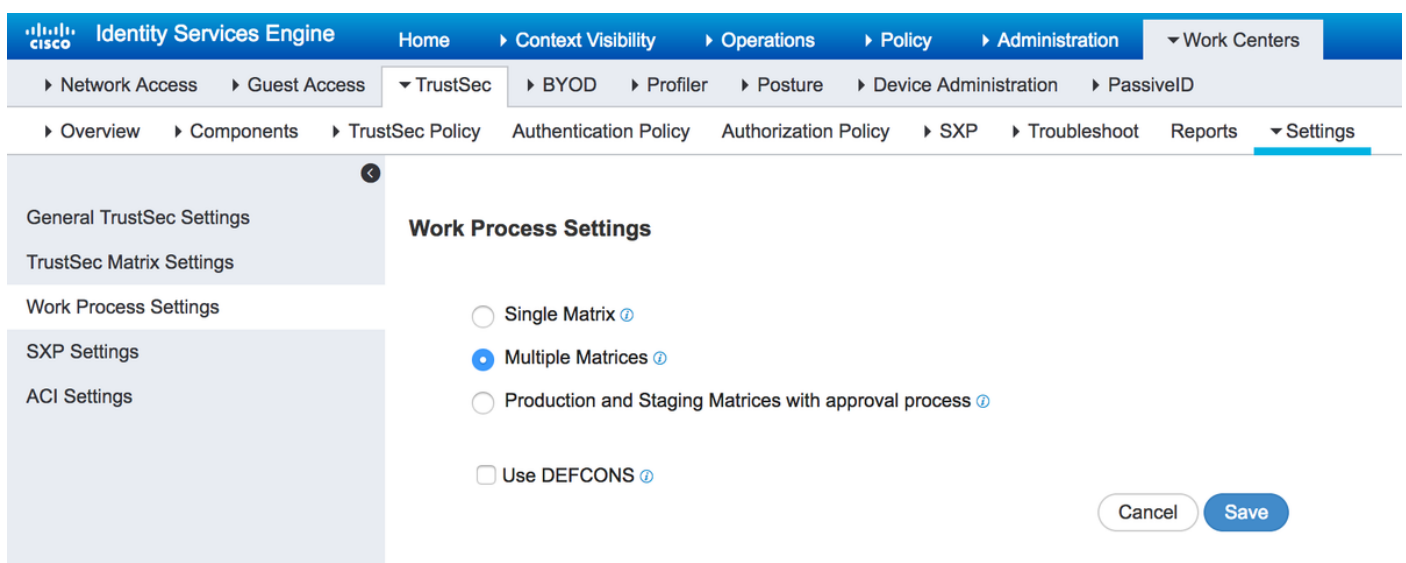
在ISE 2.0中，所有網路裝置可能僅使用一個生產TrustSec矩陣。ISE 2.1新增了稱為暫存矩陣的功能，可用於測試和實施。在暫存矩陣中建立的策略僅應用於用於測試的網路裝置。其餘裝置仍使用生產矩陣。一旦確認暫存矩陣工作正常，所有其它裝置都可以移到該暫存矩陣中，它便成為新的生產矩陣。

ISE 2.2具有兩項新的TrustSec功能：

1. 多個矩陣 — 能夠將不同的矩陣分配給網路裝置
 2. DefCon matrix — 此矩陣在特殊情況下推送到所有網路裝置，由管理員觸發
- 可以在ISE 2.2中使用單個矩陣功能或生產和分期矩陣功能。

多矩陣

若要使用多個矩陣，必須在**工作中心 > TrustSec > 設定 > 工作進程設定**下啟用此選項，如下圖所示：



The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The breadcrumb navigation is: Home > Context Visibility > Operations > Policy > Administration > Work Centers > TrustSec > BYOD > Profiler > Posture > Device Administration > PassiveID > Overview > Components > TrustSec Policy > Authentication Policy > Authorization Policy > SXP > Troubleshoot > Reports > Settings. The 'Work Process Settings' section is expanded, showing the following options:

- Single Matrix
- Multiple Matrices
- Production and Staging Matrices with approval process
- Use DEFCONS

Buttons for 'Cancel' and 'Save' are visible at the bottom right.

啟用該功能後，您可以建立新矩陣，稍後將網路裝置分配到特定矩陣。

DefCon矩陣

DefCon矩陣是特殊矩陣，隨時可以部署。部署時，所有網路裝置都會自動分配給此矩陣。ISE仍會記住所有網路裝置的最後一個生產矩陣，因此此更改可以在停用DefCon的任何時刻恢復。最多可以定義四個不同的DefCon矩陣：

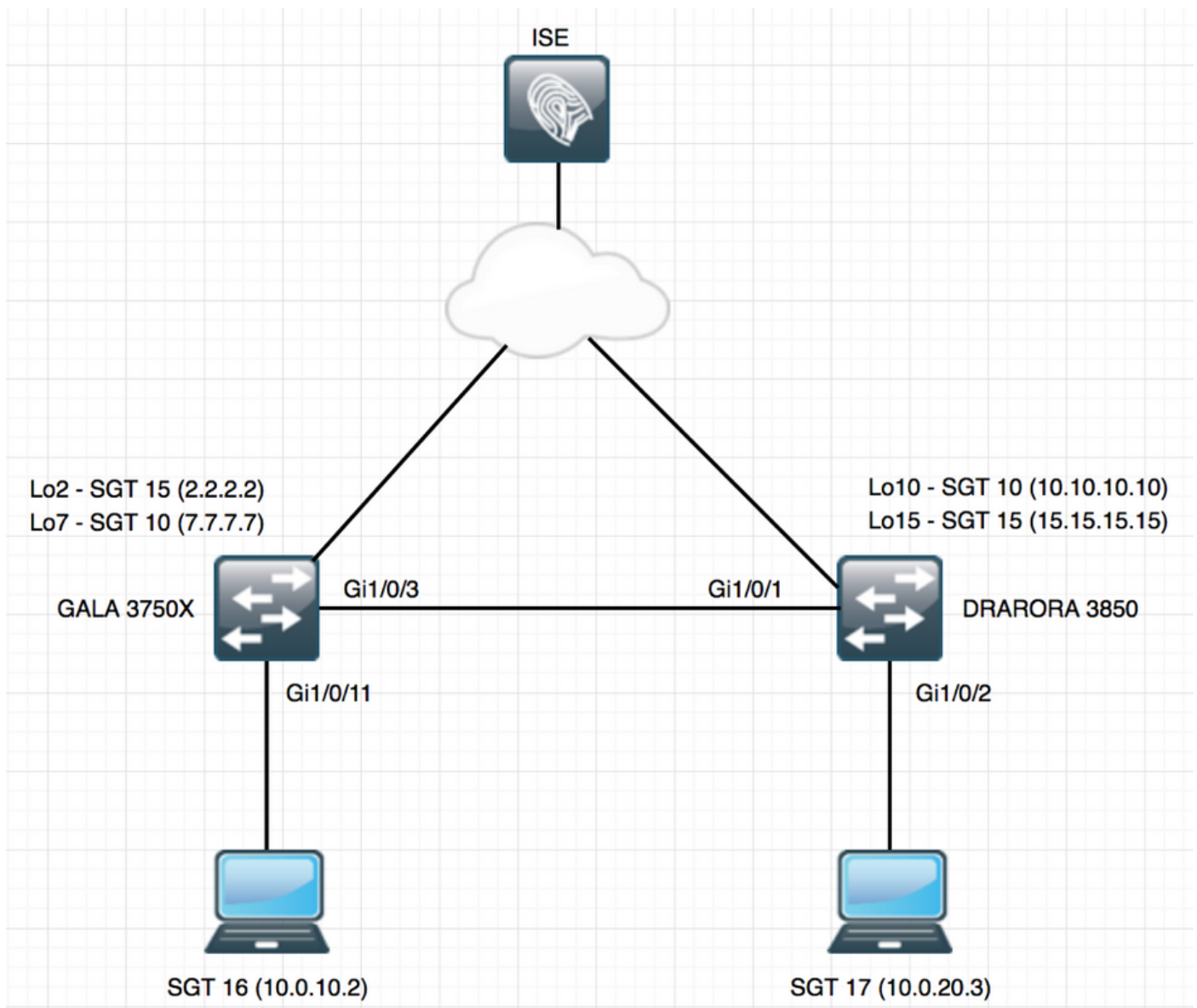
1. DefCon1 — 嚴重
2. DefCon2 — 嚴重
3. DefCon3 — 實質性
4. DefCon4 — 中等

DefCon矩陣可與所有三個工作流程選項結合使用：

The screenshot displays the Cisco Identity Services Engine (ISE) configuration interface. The top navigation bar includes 'Identity Services Engine' and tabs for 'Home', 'Context Visibility', 'Operations', 'Policy', 'Administration', and 'Work Centers'. The 'Work Centers' tab is expanded, showing sub-tabs for 'Network Access', 'Guest Access', 'TrustSec', 'BYOD', 'Profiler', 'Posture', 'Device Administration', and 'PassivID'. The 'TrustSec' sub-tab is selected, and its 'Settings' sub-tab is active. The left sidebar lists configuration categories: 'General TrustSec Settings', 'TrustSec Matrix Settings', 'Work Process Settings' (highlighted), 'SXP Settings', and 'ACI Settings'. The main content area, titled 'Work Process Settings', features three radio button options: 'Single Matrix', 'Multiple Matrices' (selected), and 'Production and Staging Matrices with approval process'. A checked checkbox labeled 'Use DEFCONS' is also present. At the bottom right, there are 'Cancel' and 'Save' buttons.

設定

網路圖表



組態

要使用多個矩陣，必須在「工作進程設定」下啟用它。在此示例中，還啟用DefCon矩陣。

1. RADIUS/CTS的基本交換機配置

```
radius server ISE
address ipv4 10.48.17.161 auth-port 1812 acct-port 1813
pac key cisco
```

```
aaa group server radius ISE
server name ISE
ip radius source-interface FastEthernet0
```

```
ip radius source-interface FastEthernet0
```

```
aaa server radius dynamic-author
client 10.48.17.161 server-key cisco
```

```
aaa new-model aaa authentication dot1x default group ISE aaa accounting dot1x default start-stop
group ISE
```

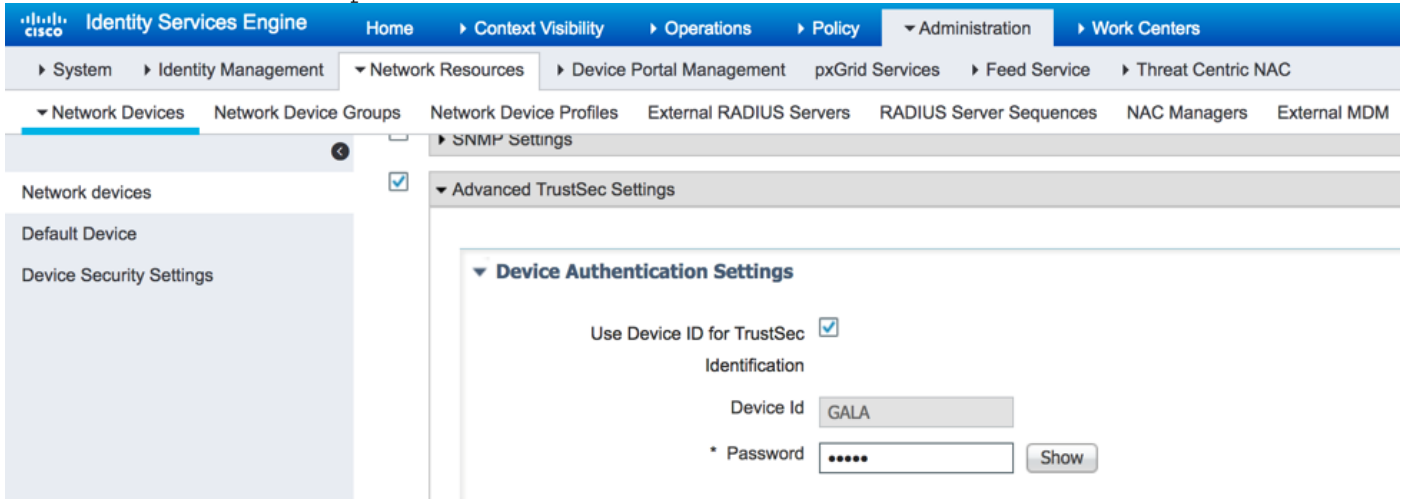
為了獲取CTS資訊，您必須建立CTS授權清單：

```
cts authorization list LIST
aaa authorization network LIST group ISE
```

2. CTS PAC

要從ISE接收CTS PAC (保護訪問憑證) ，必須在交換機和ISE上為網路裝置配置高級TrustSec配置下的相同憑證：

```
cts credentials id GALA password cisco
```



配置此配置後，交換機即可下載CTS PAC。在每個RADIUS請求中，PAC-Opaque的一部分作為AV對傳送到ISE，因此ISE可以驗證此網路裝置的PAC是否仍然有效：

```
GALA#show cts pacs
AID: E6796CD7BBF2FA4111AD9FB4FEFB5A50
PAC-Info:
  PAC-type = Cisco Trustsec
  AID: E6796CD7BBF2FA4111AD9FB4FEFB5A50
  I-ID: GALA
  A-ID-Info: Identity Services Engine
  Credential Lifetime: 17:05:50 CEST Apr 5 2017
PAC-Opaque:
000200B00003000100040010E6796CD7BBF2FA4111AD9FB4FEFB5A50000600940003010012FABE10F3DCBCB152C54FA5
BFE124CB00000013586BB31500093A809E11A93189C7BE6EBDFB8FDD15B9B7252EB741ADCA3B2ACC5FD923AEB7BDFE48
A3A771338926A1F48141AF091469EE4AFC8C3E92A510BA214A407A33F469282A780E8F50F17A271E92D1FEE1A29ED427
B985F9A0E00D6CDC934087716F4DEAF84AC11AA05F7587E898CA908463BDA9EC7E65D827
  Refresh timer is set for 11y13w
```

3. 交換機上的CTS配置。

下載PAC後，交換機可以請求其他CTS資訊 (環境資料和策略)：

```
GALA#cts refresh environment-data
```

```
GALA#show cts environment-data
```

```
CTS Environment Data
=====
Current state = COMPLETE
Last status = Successful
Local Device SGT:
  SGT tag = 0-06:Unknown
```

Server List Info:

Installed list: CTSServerList1-0001, 1 server(s):

*Server: 10.48.17.161, port 1812, A-ID E6796CD7BBF2FA4111AD9FB4FEFB5A50

Status = ALIVE

auto-test = TRUE, keywrap-enable = FALSE, idle-time = 60 mins, deadtime = 20 secs

Multicast Group SGT Table:

Security Group Name Table:

0-ce:Unknown

2-ce:TrustSec_Devices

3-ce:Network_Services

4-ce:Employees

5-ce:Contractors

6-ce:Guests

7-ce:Production_Users

8-ce:Developers

9-ce:Auditors

10-ce:Point_of_Sale_Systems

11-ce:Production_Servers

12-ce:Development_Servers

13-ce:Test_Servers

14-ce:PCI_Servers

15-ce:BYOD

255-ce:Quarantined_Systems

Environment Data Lifetime = 86400 secs

Last update time = 07:48:41 CET Mon Jan 2 2006

Env-data expires in 0:23:56:02 (dd:hr:mm:sec)

Env-data refreshes in 0:23:56:02 (dd:hr:mm:sec)

Cache data applied = NONE

State Machine is running

GALA#**cts refresh policy**

GALA#**show cts role-based permissions**

RBACL Monitor All for Dynamic Policies : FALSE

RBACL Monitor All for Configured Policies : FALSE

您可能會看到沒有從ISE下載策略，原因是交換機上未啟用CTS實施：

```
cts role-based enforcement
```

```
cts role-based enforcement vlan-list 1-4094
```

GALA#**show cts role-based permissions**

IPv4 Role-based permissions default:

Permit IP-00

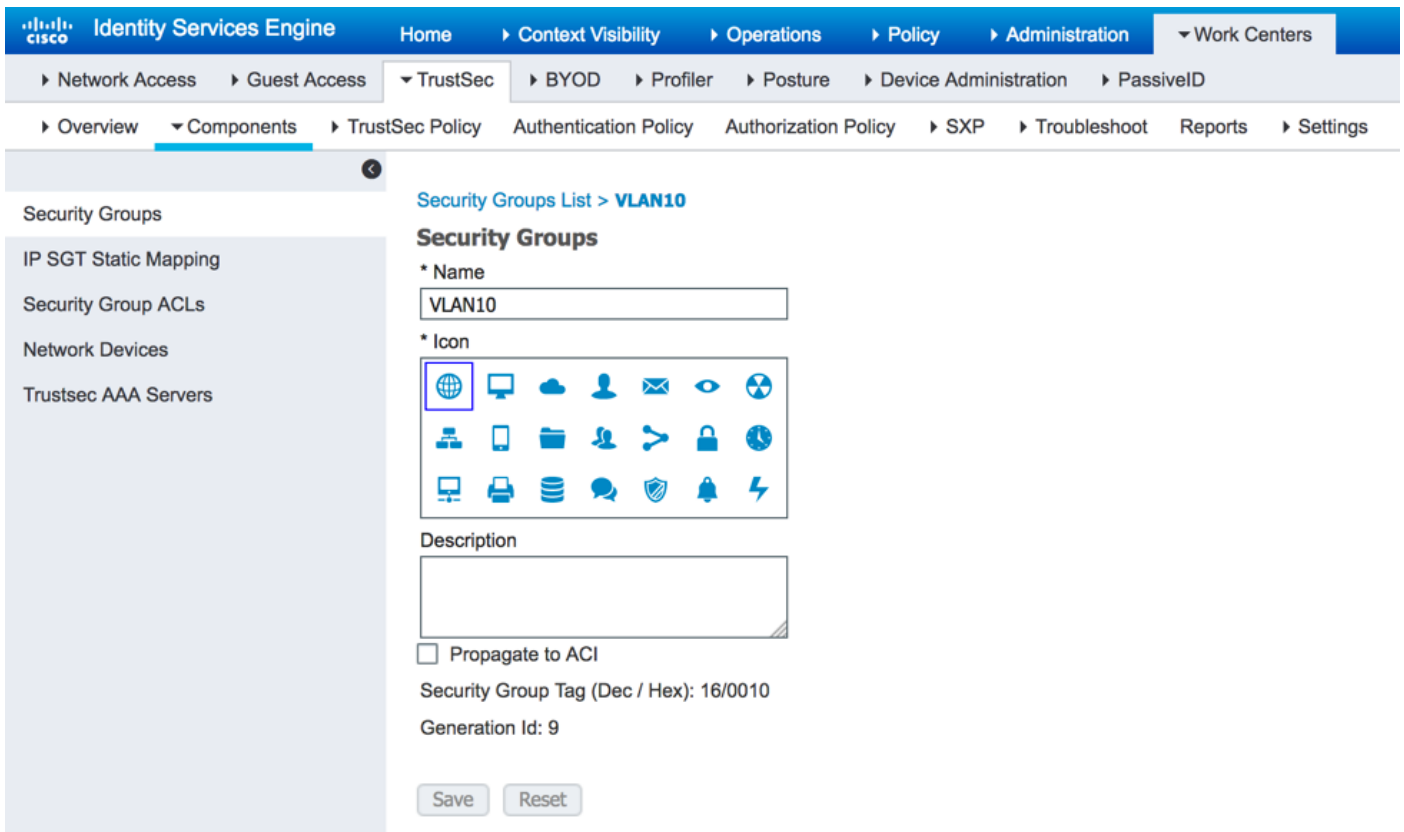
RBACL Monitor All for Dynamic Policies : FALSE

RBACL Monitor All for Configured Policies : FALSE

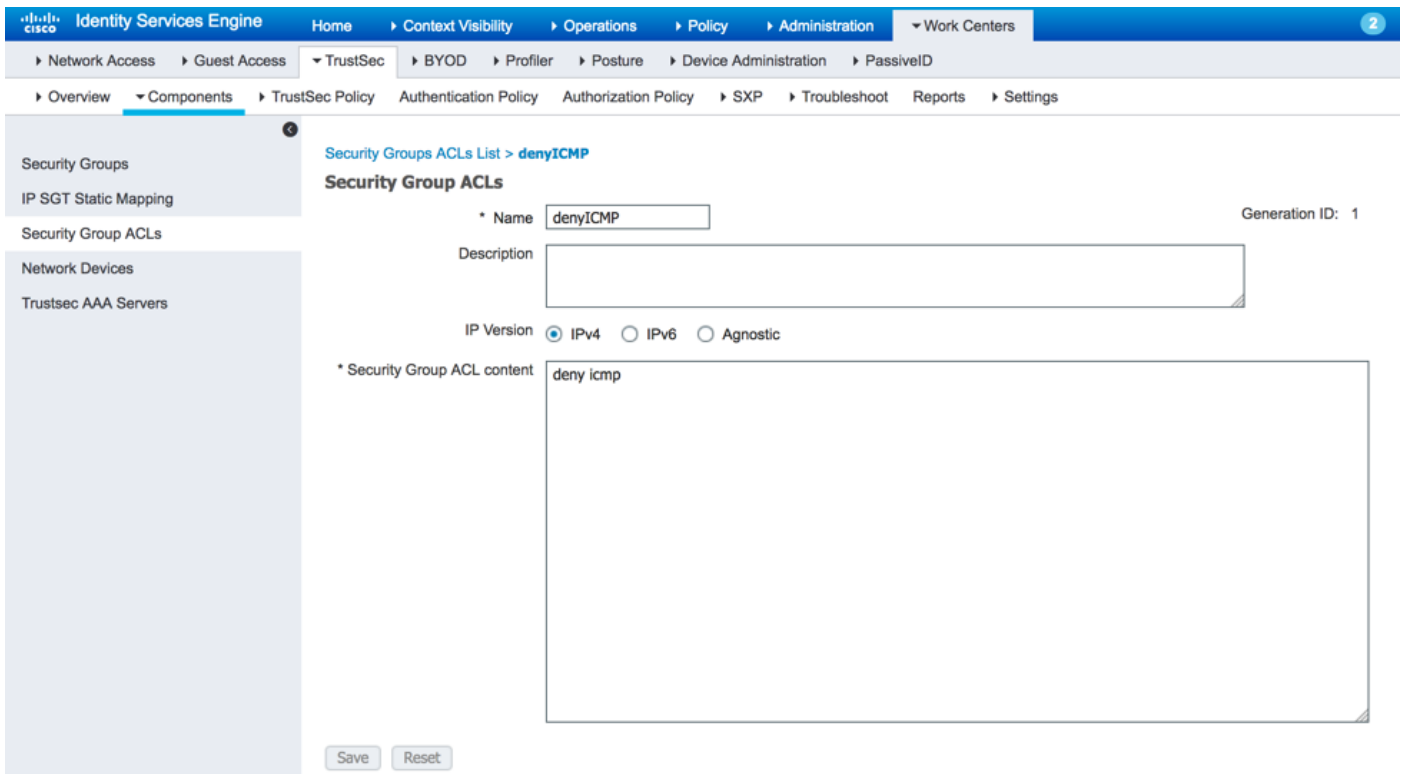
在這兩個輸出中，您都可以看到預設值 — 預設建立的SGT(0、2-15、255)和預設的允許IP策略。

4. ISE上的基本CTS配置。

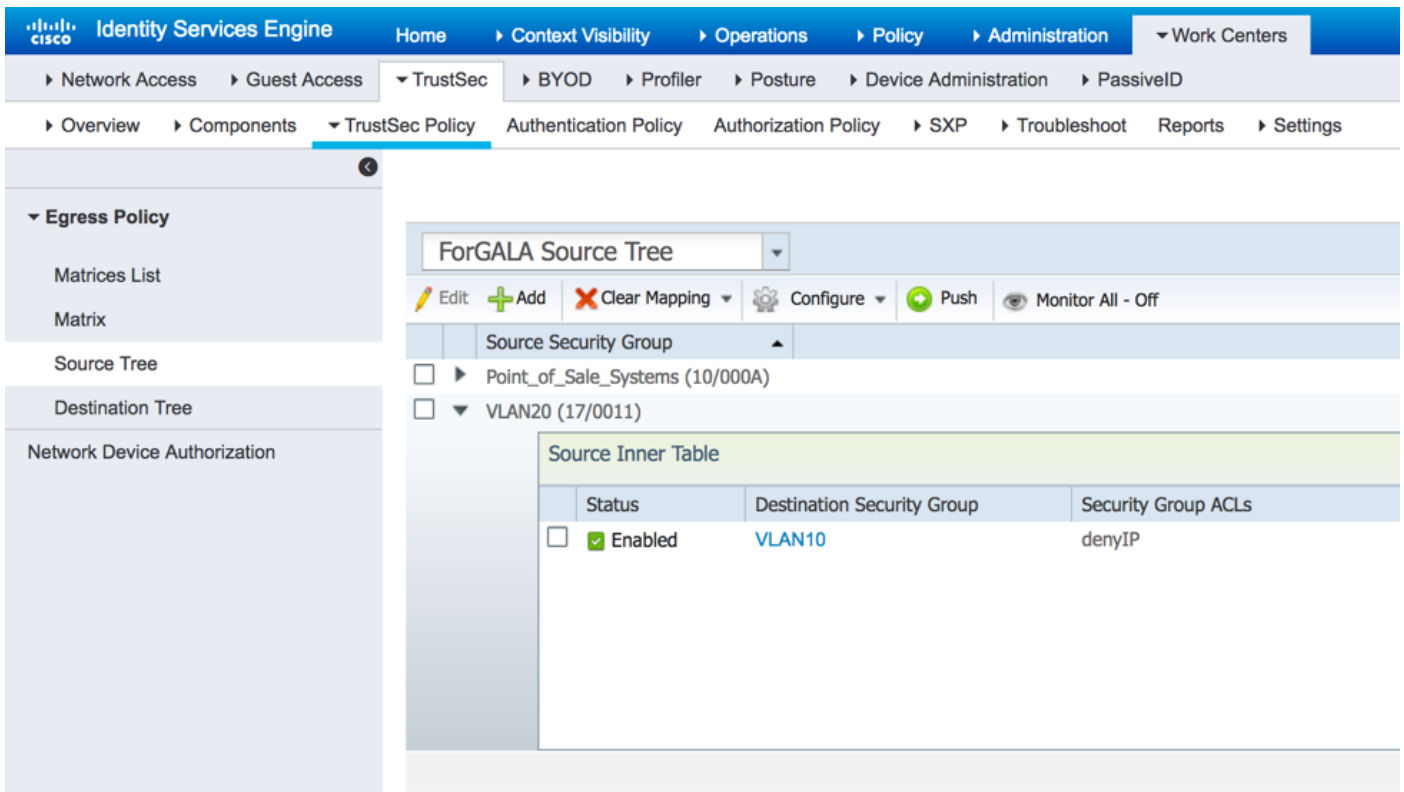
在ISE上建立新的安全組標籤(SGT)和少量策略，以便以後使用。導航到工作中心(Work Centers)> TrustSec > 元件(Components)> 安全組(Security Groups)，按一下Add以建立新的SGT:



要建立安全組訪問控制清單(SGACL)以進行流量過濾，請選擇**Security Group ACL**，如下圖所示：

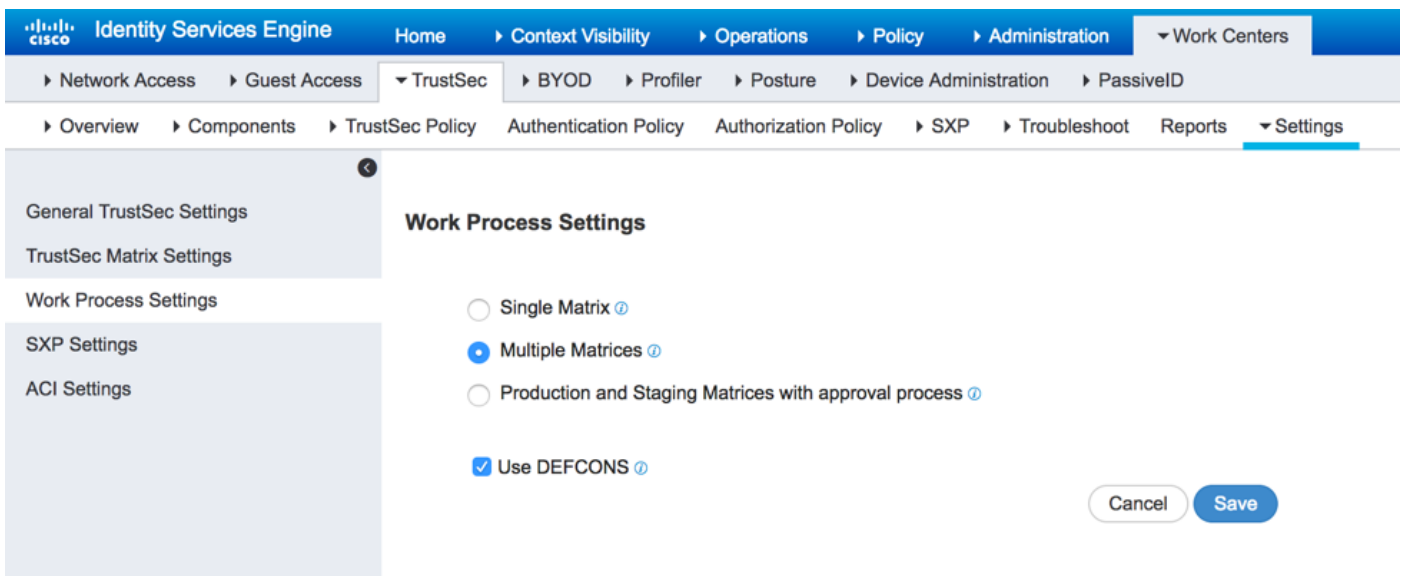


同樣，您可以建立其他SGT和SGACL。建立SGT和SGACL後，您可以在CTS策略中將它們連線在一起，為此，請導航到**Work Centers > TrustSec Policy > Egress Policy > Source Tree**，如下圖所示：



5. ISE上的多個矩陣和DefCon配置。

在本示例中，您已為矩陣ForGALA配置策略。要在矩陣之間切換，您可以使用下拉選單。要啟用多個矩陣，請導航到工作中心> TrustSec > 設定> 工作進程設定，然後啟用多個矩陣和DefCon矩陣，如下圖所示：



啟用此選項後，預設的生產矩陣將可用，但您可以建立其他矩陣。導航到工作中心(Work Centers)> TrustSec > TrustSec Policy > Egress Policy > Matrices List，然後點選Add:

Add Matrix



Name *

Description

Copy policy from

Cancel

Submit

可以選擇從現有矩陣複製應成為新矩陣一部分的策略。建立兩個矩陣 — 一個用於3750X交換機，另一個用於3850交換機。建立矩陣後，您必須將網路裝置分配給這些矩陣，因為預設情況下所有啟用TrustSec的網路訪問裝置都將分配給Production矩陣。

Identity Services Engine

Home > Context Visibility > Operations > Policy > Administration > Work Centers

TrustSec > BYOD > Profiler > Posture > Device Administration > PassiveID

TrustSec Policy > Authentication Policy > Authorization Policy > SXP > Troubleshoot > Reports > Settings

Matrices List

Refresh + Add Duplicate Trash Edit Assign NADs

Matrix Name	Description	Number of NADS	Last Modified
<input type="checkbox"/> Production		2	
<input type="checkbox"/> forDRARORA		0	Jan 11 2017 18:02
<input type="checkbox"/> forGALA		0	Jan 11 2017 18:00

要分配NAD，請點選Matrices List下的**Assign NADs**選項，選中要分配矩陣的裝置，然後從下拉選單中選擇建立的矩陣，然後點選**Assign**，如下圖所示：

Assign Network Devices

1 Select network devices. (Filters may be used)

1 Selected Rows/Page 2 / 1 / 1 Go 2 Total Rows

Name	IP	Location	Type	Matrix
<input checked="" type="checkbox"/> DRARORA	10.48.72.108/32	Location#All Locations	Device Type#All Device Types	Production
<input type="checkbox"/> GALA	10.48.72.156/32	Location#All Locations	Device Type#All Device Types	Production

2 Assign these to a matrix

Select a matrix

- Production
- forDRARORA**
- forGALA

Close Assign

您可以對其它裝置執行相同的操作，然後按一下**Assign**按鈕：

Assign Network Devices

1 Select network devices. (Filters may be used)

1 Selected Rows/Page 2 / 1 Go 2 Total Rows

Refresh Filter

Name	IP	Location	Type	Matrix
DRARORA	10.48.72.108/32	Location#All Locations	Device Type#All Device Types	forDRARORA
<input checked="" type="checkbox"/> GALA	10.48.72.156/32	Location#All Locations	Device Type#All Device Types	Production

2 Assign these to a matrix

Select a matrix

- Production
- forDRARORA
- forGALA**

Close & Send Assign

執行完所有更改後，按一下**Close&Send**，該操作會將所有更新傳送到裝置，以執行CTS策略的刷新以下載新策略。同樣，建立DefCon矩陣，您可以從現有矩陣複製：

Add DEFCON

DEFCON Level

Description

Copy policy from

DEFCON2(Severe)

DEFCON3(Substantial)

DEFCON4(Moderate)

Cancel Submit

最終策略如下：

Identity Services Engine

Home Context Visibility Operations Policy Administration Work Centers License Warning

TrustSec BYOD Profiler Posture Device Administration PassiveID

TrustSec Policy Authentication Policy Authorization Policy SXP Troubleshoot Reports Settings

Egress Policy

Matrices List

Matrices

Matrix Name	Description	Number of NADS	Last Modified
<input type="checkbox"/> Production		0	
<input type="checkbox"/> forDRARORA		1	Jan 11 2017 18:02
<input type="checkbox"/> forGALA		1	Jan 11 2017 18:00

DEFCONS

DEFCON Matrix	Description	Last Modified	Activated By	Color
<input type="checkbox"/> DEFCON1_CRITICAL		Jan 4 2017 15:42		

6. SGT分類

標籤到客戶端分配有兩種選項（建立IP-SGT對映）：

- *static* - with **cts role-based sgt-map IP_address sgt tag**
- *dynamic* — 通過dot1x驗證（成功驗證後指定標籤）

此處使用這兩個選項，兩台Windows電腦通過dot1x身份驗證獲得SGT標籤，環回介面使用靜態SGT標籤。要部署動態對映，請為終端客戶端建立授權策略：

Authorization Policy

Define the Authorization Policy by configuring rules based on identity groups and/or other conditions. Drag and drop rules to change the order. For Policy Export go to [Administration > System > Backup & Restore > Policy Export Page](#)

First Matched Rule Applies

Exceptions (0)

Standard

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
✓	for VLAN 10 - GALA	if Radius:Calling-Station-ID ENDS_WITH 5B:D9	then PermitAccess AND VLAN10
✓	for VLAN 20 - DRARORA	if Radius:Calling-Station-ID ENDS_WITH 36:88	then PermitAccess AND VLAN20

要建立靜態IP-SGT對映，請使用命令（例如GALA交換機）：

```
interface Loopback7
 ip address 7.7.7.7 255.255.255.0

interface Loopback2
 ip address 2.2.2.2 255.255.255.0

cts role-based sgt-map 2.2.2.2 sgt 15
cts role-based sgt-map 7.7.7.7 sgt 10
```

身份驗證成功後，客戶端將訪問具有特定SGT標籤的授權策略，結果為：

```
GALA#show authentication sessions interface Gi1/0/11 details
      Interface: GigabitEthernet1/0/11
      MAC Address: 0050.5699.5bd9
      IPv6 Address: Unknown
      IPv4 Address: 10.0.10.2
      User-Name: 00-50-56-99-5B-D9
      Status: Authorized
      Domain: DATA
      Oper host mode: single-host
      Oper control dir: both
      Session timeout: N/A
      Restart timeout: N/A
      Common Session ID: 0A30489C000000120002330D
      Acct Session ID: 0x00000008
      Handle: 0xCE000001
      Current Policy: POLICY_Gi1/0/11

Local Policies:
Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)
  Security Policy: Should Secure
  Security Status: Link Unsecure

Server Policies:
      SGT Value: 16
```

Method status list:

Method	State
--------	-------

mab	Authc Success
-----	---------------

您可以使用命令**show cts role-based sgt-map all**檢查所有IP-SGT對映，其中顯示每個對映的源（LOCAL — 通過dot1x身份驗證、CLI — 靜態分配）：

```
GALA#show cts role-based sgt-map all
```

```
Active IPv4-SGT Bindings Information
```

IP Address	SGT	Source
2.2.2.2	15	CLI
7.7.7.7	10	CLI
10.0.10.2	16	LOCAL

```
IP-SGT Active Bindings Summary
```

```
=====  
Total number of CLI      bindings = 2  
Total number of LOCAL   bindings = 1  
Total number of active  bindings = 3
```

7. CTS策略下載

一旦交換機下載了CTS PAC和環境資料，就可以請求CTS策略。交換機不會下載所有策略，但只下載所需的策略（即針對發往已知SGT標籤的流量的策略），在進行GALA交換機時，它會從ISE請求這些策略：

- 到SGT 15的流量的策略
- 到SGT 10的流量的策略
- 到SGT 16的流量的策略

GALA交換機的所有策略輸出：

```
GALA#show cts role-based permissions
```

```
IPv4 Role-based permissions default:
```

```
Permit IP-00
```

```
IPv4 Role-based permissions from group 10:Point_of_Sale_Systems to group 15:BYOD:
```

```
denyIP-20
```

```
IPv4 Role-based permissions from group 17:VLAN20 to group 16:VLAN10:
```

```
denyIP-20
```

```
RBACL Monitor All for Dynamic Policies : FALSE
```

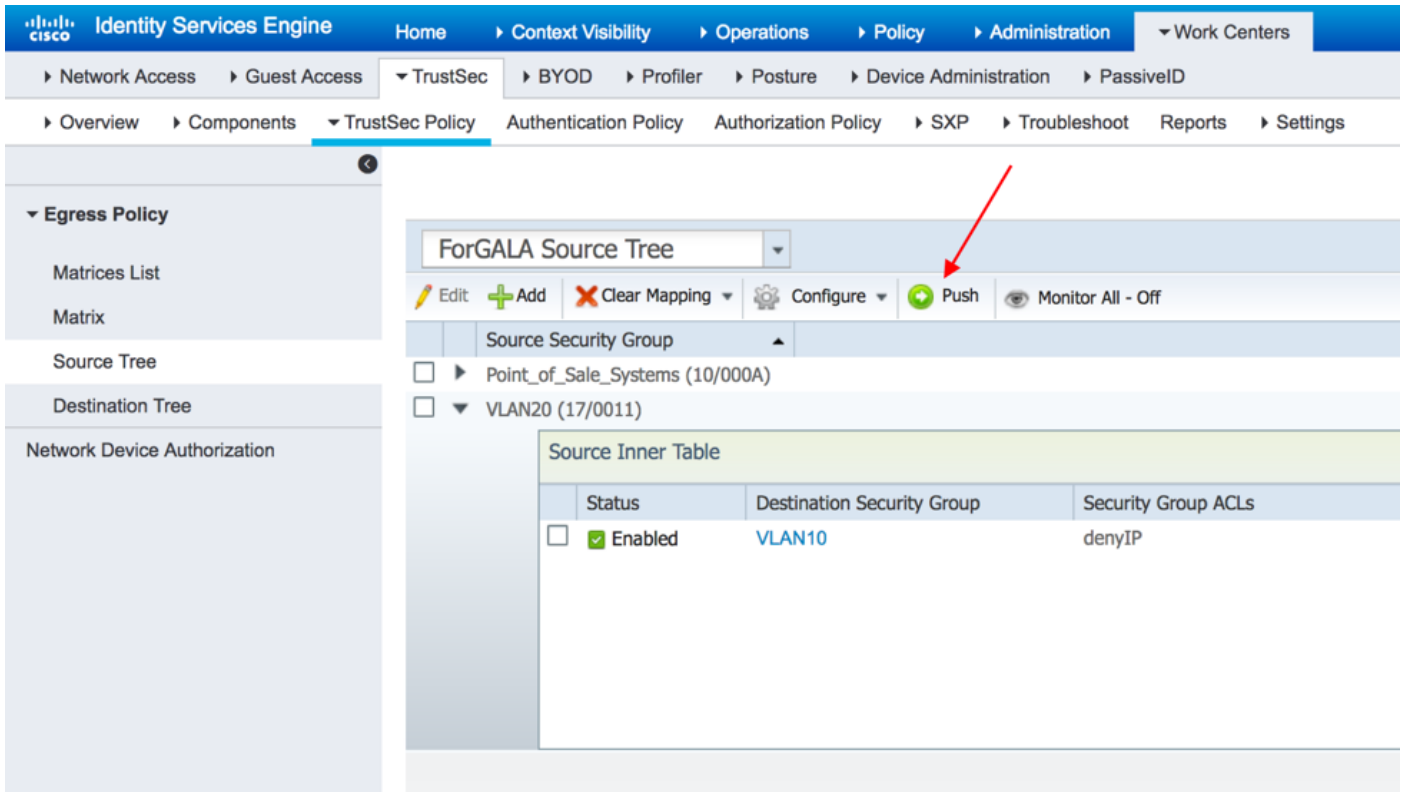
```
RBACL Monitor All for Configured Policies : FALSE
```

交換機通過兩種方式獲取策略：

- 從交換器本身刷新CTS:

```
GALA#cts refresh policy
```

- 從ISE手動推送：



驗證

多矩陣

對於此示例，兩台交換機上的最終SGT-IP對映和CTS策略：

GALA交換機：

```
GALA#show cts role-based sgt-map all
Active IPv4-SGT Bindings Information
```

```
IP Address          SGT      Source
=====
2.2.2.2             15       CLI
7.7.7.7             10       CLI
10.0.10.2           16       LOCAL
```

```
IP-SGT Active Bindings Summary
```

```
=====
Total number of CLI      bindings = 2
Total number of LOCAL   bindings = 1
Total number of active  bindings = 3
```

```
GALA#show cts role-based permissions
```

```
IPv4 Role-based permissions default:
  Permit IP-00
IPv4 Role-based permissions from group 10:Point_of_Sale_Systems to group 15:BYOD:
  denyIP-20
IPv4 Role-based permissions from group 17:VLAN20 to group 15:BYOD:
  permitIP-20
IPv4 Role-based permissions from group 17:VLAN20 to group 16:VLAN10:
  permitIP-20
RBACL Monitor All for Dynamic Policies : FALSE
RBACL Monitor All for Configured Policies : FALSE
```

```
GALA#show cts rbacl | s permitIP
name = permitIP-20
permit ip
```

```
GALA#show cts rbacl | s deny
name = denyIP-20
deny ip
```

DRARORA交換機：

```
DRARORA#show cts role-based sgt-map all
Active IPv4-SGT Bindings Information
```

IP Address	SGT	Source
10.0.20.3	17	LOCAL
10.10.10.10	10	CLI
15.15.15.15	15	CLI

```
IP-SGT Active Bindings Summary
=====
Total number of CLI bindings = 2
Total number of LOCAL bindings = 1
Total number of active bindings = 3
```

```
DRARORA#show cts role-based permissions
IPv4 Role-based permissions default:
  Permit IP-00
IPv4 Role-based permissions from group 17:VLAN20 to group 10:Point_of_Sale_Systems:
  permitIP-20
IPv4 Role-based permissions from group 10:Point_of_Sale_Systems to group 15:BYOD:
  permitIP-20
IPv4 Role-based permissions from group 17:VLAN20 to group 15:BYOD:
  permitIP-20
IPv4 Role-based permissions from group 10:Point_of_Sale_Systems to group 17:VLAN20:
  denyIP-20
IPv4 Role-based permissions from group 16:VLAN10 to group 17:VLAN20:
  permitIP-20
RBACL Monitor All for Dynamic Policies : FALSE
RBACL Monitor All for Configured Policies : FALSE
```

觀察到兩台交換機的策略不同 (即使在10到15之間在同一策略對於GALA和DRARORA交換機也是不同的)。這意味著從SGT 10到15的流量在DRARORA上被允許，但在GALA上被阻止：

```
DRARORA#ping 15.15.15.15 source Loopback 10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 15.15.15.15, timeout is 2 seconds:
Packet sent with a source address of 10.10.10.10
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

```
GALA#ping 2.2.2.2 source Loopback 7
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2.2.2.2, timeout is 2 seconds:
Packet sent with a source address of 7.7.7.7
U.U.U
Success rate is 0 percent (0/5)
```

同樣地，您可以從一個視窗訪問另一個視窗(SGT 17 -> SGT 16):

```
C:\Windows\system32\cmd.exe
C:\Users\cisco>
C:\Users\cisco>
C:\Users\cisco>
C:\Users\cisco>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    IPv6 Address. . . . . : 2001:420:44ff:ff48:398c:b07c:78b0:81a2
    Link-local IPv6 Address . . . . . : fe80::398c:b07c:78b0:81a2%11
    IPv4 Address. . . . . : 10.0.20.3
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.0.20.1

Tunnel adapter isatap.{F0A1FA7C-FEE5-4D28-9007-2A2AC1AC2DF4}:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

C:\Users\cisco>ping 10.0.10.2

Pinging 10.0.10.2 with 32 bytes of data:
Reply from 10.0.10.2: bytes=32 time<1ms TTL=127
Reply from 10.0.10.2: bytes=32 time<1ms TTL=127
Reply from 10.0.10.2: bytes=32 time<1ms TTL=127
Reply from 10.0.10.2: bytes=32 time<1ms TTL=127

Ping statistics for 10.0.10.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\cisco>
```

另一種方法(SGT 16 -> SGT 17):

```
C:\Windows\system32\cmd.exe
C:\Users\cisco>
C:\Users\cisco>
C:\Users\cisco>
C:\Users\cisco>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::2887:2c07:5cb5:2355%11
    IPv4 Address. . . . . : 10.0.10.2
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.0.10.1

Tunnel adapter isatap.{F0A1FA7C-FEE5-4D28-9007-2A2AC1AC2DF4}:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

C:\Users\cisco>ping 10.0.20.3

Pinging 10.0.20.3 with 32 bytes of data:
Reply from 10.0.20.3: bytes=32 time=41ms TTL=127
Reply from 10.0.20.3: bytes=32 time=2ms TTL=127
Reply from 10.0.20.3: bytes=32 time<1ms TTL=127
Reply from 10.0.20.3: bytes=32 time<1ms TTL=127

Ping statistics for 10.0.20.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 41ms, Average = 10ms

C:\Users\cisco>
```

要確認應用了正確的CTS策略，請檢查show cts role-based counters 輸出：

```
GALA#sh cts role-based counters
Role-based IPv4 counters
# '-' in hardware counters field indicates sharing among cells with identical policies
From      To        SW-Denied   HW-Denied   SW-Permitted  HW-Permitted

17        16        0           0           0             8
17        15        0           -           0             -

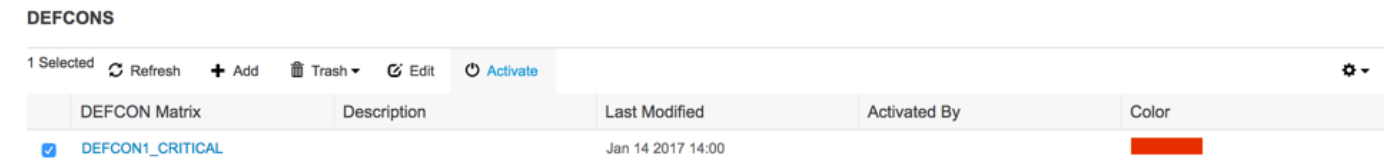
10        15        4           0           0             0

*         *         0           0           127           26
```

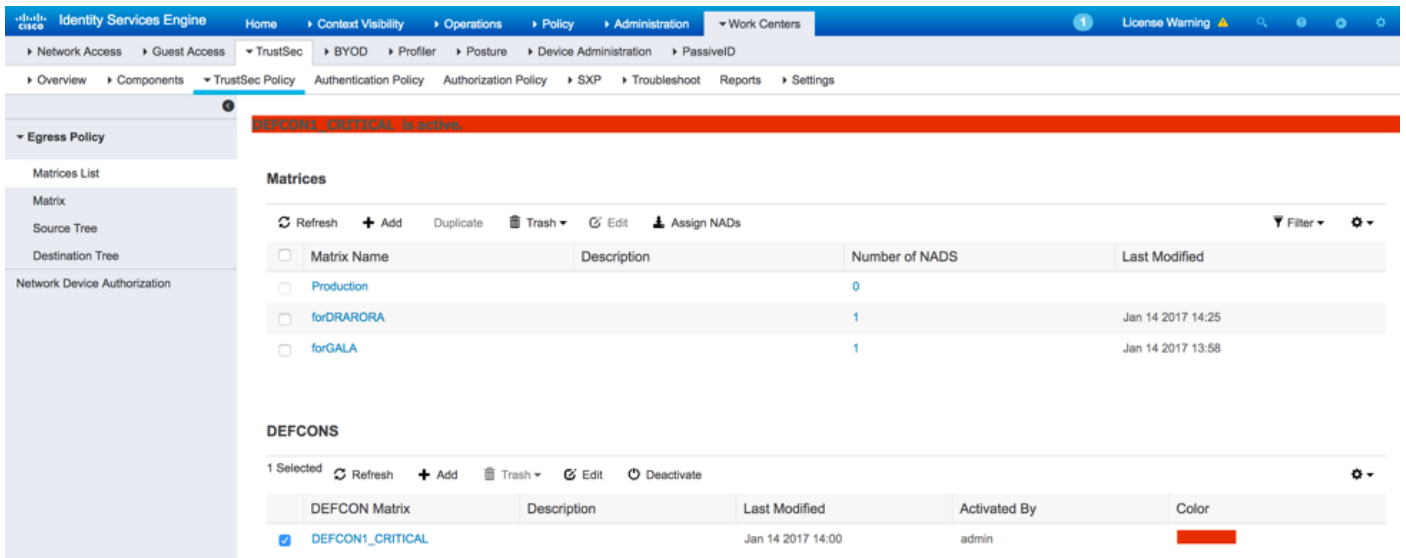
GALA有8個允許的資料包 (4個來自ping 17->16,4個來自ping 16->17)。

DefCon部署

如果需要，在Work Centers > TrustSec > TrustSec Policy > Egress Policy > Matrices List下部署DefCon矩陣，檢查您要啟用的DefCon矩陣，然後按一下Activate:



啟用DefCon後，ISE上的選單如下所示：



和交換機上的策略：

```
GALA#show cts role-based permissions
IPv4 Role-based permissions default:
Permit IP-00
IPv4 Role-based permissions from group 15:BYOD to group 10:Point_of_Sale_Systems:
denyIP-20
IPv4 Role-based permissions from group 15:BYOD to group 16:VLAN10:
denyIP-20
IPv4 Role-based permissions from group 17:VLAN20 to group 16:VLAN10:
```


denyIP-20

RBACL Monitor All for Dynamic Policies : FALSE

RBACL Monitor All for Configured Policies : FALSE

DRARORA#show cts role-based permissions

IPv4 Role-based permissions default:

Permit IP-00

IPv4 Role-based permissions from group 15:BYOD to group 10:Point_of_Sale_Systems:

denyIP-20

IPv4 Role-based permissions from group 10:Point_of_Sale_Systems to group 17:VLAN20:

permitIP-20

RBACL Monitor All for Dynamic Policies : FALSE

RBACL Monitor All for Configured Policies : FALSE

兩台交換器都不允許從SGT 15到SGT 10的流量：

DRARORA#ping 10.10.10.10 source Loopback 15

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 10.10.10.10, timeout is 2 seconds:

Packet sent with a source address of 15.15.15.15

U.U.U

Success rate is 0 percent (0/5)

GALA#ping 7.7.7.7 source Loopback 2

Type escape sequence to abort.

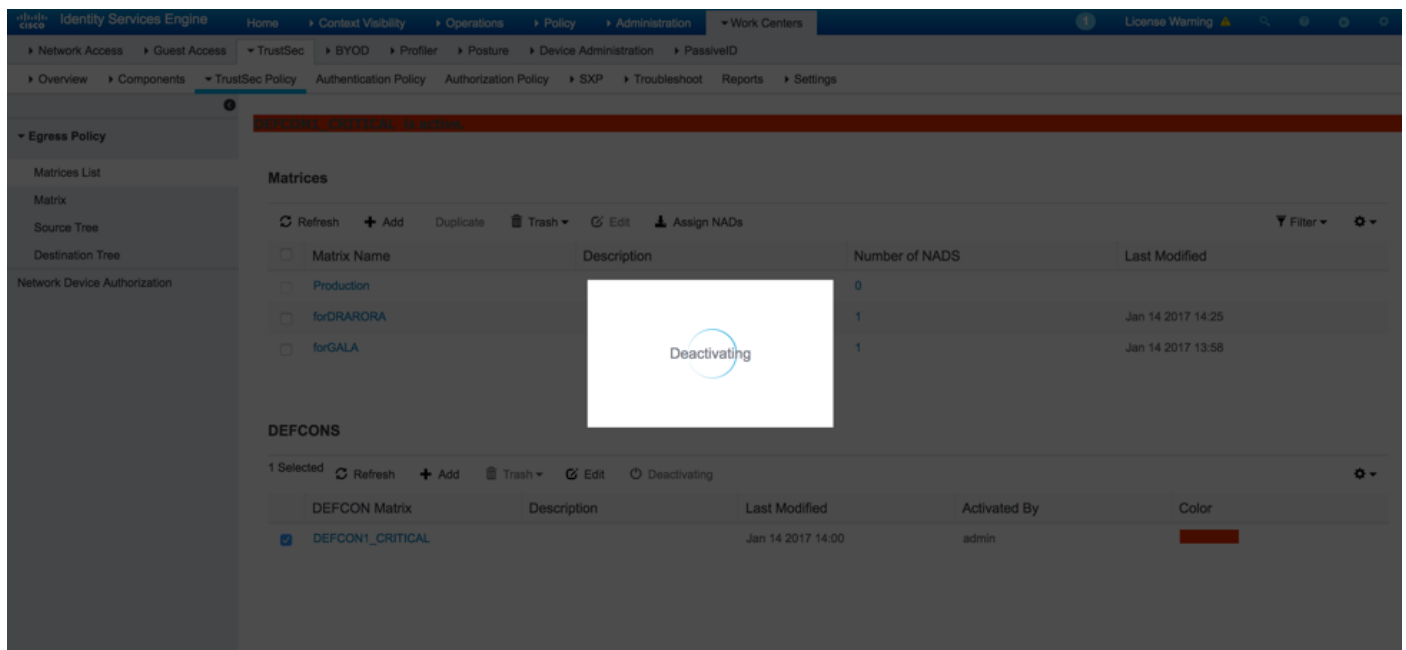
Sending 5, 100-byte ICMP Echos to 7.7.7.7, timeout is 2 seconds:

Packet sent with a source address of 2.2.2.2

U.U.U

Success rate is 0 percent (0/5)

部署再次穩定後，可以停用DefCon和交換機請求舊策略。要停用DefCon，請導航到工作中心(Work Centers)> TrustSec > TrustSec Policy > Egress Policy > Matrices List，檢查活動的DefCon矩陣，然後按一下Deactivate:



兩台交換機都立即請求舊策略：

DRARORA#show cts role-based permissions

IPv4 Role-based permissions default:

Permit IP-00

```
IPv4 Role-based permissions from group 17:VLAN20 to group 10:Point_of_Sale_Systems:
permitIP-20
IPv4 Role-based permissions from group 10:Point_of_Sale_Systems to group 15:BYOD:
permitIP-20
IPv4 Role-based permissions from group 17:VLAN20 to group 15:BYOD:
permitIP-20
IPv4 Role-based permissions from group 10:Point_of_Sale_Systems to group 17:VLAN20:
denyIP-20
IPv4 Role-based permissions from group 16:VLAN10 to group 17:VLAN20:
permitIP-20
RBACL Monitor All for Dynamic Policies : FALSE
RBACL Monitor All for Configured Policies : FALSE
```

GALA#show cts role-based permissions

```
IPv4 Role-based permissions default:
Permit IP-00
IPv4 Role-based permissions from group 10:Point_of_Sale_Systems to group 15:BYOD:
denyIP-20
IPv4 Role-based permissions from group 17:VLAN20 to group 15:BYOD:
permitIP-20
IPv4 Role-based permissions from group 17:VLAN20 to group 16:VLAN10:
permitIP-20
RBACL Monitor All for Dynamic Policies : FALSE
RBACL Monitor All for Configured Policies : FALSE
```

疑難排解

PAC調配

這是成功的PAC調配的一部分：

GALA#debug cts provisioning packets

GALA#debug cts provisioning events

```
*Jan  2 04:39:05.707: %SYS-5-CONFIG_I: Configured from console by console
*Jan  2 04:39:05.707: CTS-provisioning: Starting new control block for server 10.48.17.161:
*Jan  2 04:39:05.707: CTS-provisioning: cts_provi_init_socket: Checking for any vrf associated
with 10.48.17.161
*Jan  2 04:39:05.707: CTS-provisioning: New session socket: src=10.48.72.156:65242
dst=10.48.17.161:1812
*Jan  2 04:39:05.716: CTS-provisioning: cts_provi_init_socket: Checking for any vrf associated
with 10.48.17.161
*Jan  2 04:39:05.716: CTS-provisioning: cts_provi_init_socket: Adding vrf-tableid: 0 to socket
*Jan  2 04:39:05.716: CTS-provisioning: New session socket: src=10.48.72.156:65242
dst=10.48.17.161:1812
*Jan  2 04:39:05.716: CTS-provisioning: Sending EAP Response/Identity to 10.48.17.161
*Jan  2 04:39:05.716: CTS-provisioning: OUTGOING RADIUS msg to 10.48.17.161:
1E010EE0:      01010090 64BCBC01 7BEF347B
1E010EF0: 1E32C02E 8402A83D 010C4354 5320636C
1E010F00: 69656E74 04060A30 489C3D06 00000000
1E010F10: 06060000 00021F0E 30303037 37643862
1E010F20: 64663830 1A2D0000 00090127 4141413A
1E010F30: 73657276 6963652D 74797065 3D637473
1E010F40: 2D706163 2D70726F 76697369 6F6E696E
1E010F50: 674F1102 00000F01 43545320 636C6965
1E010F60: 6E745012 73EBE7F5 CDA0CF73 BFE4AFB6
1E010F70: 40D723B6 00
*Jan  2 04:39:06.035: CTS-provisioning: INCOMING RADIUS msg from 10.48.17.161:
1EC68460:      0B0100B5 E4C3C3C1 ED472766
```

```

1EC68470: 183F41A9 026453ED 18733634 43504D53
1EC68480: 65737369 6F6E4944 3D306133 30313161
1EC68490: 314C3767 78484956 62414976 37316D59
1EC684A0: 525F4D56 34517741 4C362F69 73517A72
1EC684B0: 7A586132 51566852 79635638 3B343353
1EC684C0: 65737369 6F6E4944 3D766368 72656E65
1EC684D0: 6B2D6973 6532322D 3432332F 32373238
1EC684E0: 32373637 362F3137 37343B4F 1C017400
1EC684F0: 1A2B2100 040010E6 796CD7BB F2FA4111
1EC68500: AD9FB4FE FB5A5050 124B76A2 E7D34684
1EC68510: DD8A1583 175C2627 9F00
*Jan 2 04:39:06.035: CTS-provisioning: Received RADIUS challenge from 10.48.17.161.
*Jan 2 04:39:06.035: CTS-provisioning: A-ID for server 10.48.17.161 is
"e6796cd7bbf2fa4111ad9fb4fefb5a50"
*Jan 2 04:39:06.043: CTS-provisioning: Received TX_PKT from EAP method
*Jan 2 04:39:06.043: CTS-provisioning: Sending EAPFAST response to 10.48.17.161
*Jan 2 04:39:06.043: CTS-provisioning: OUTGOING RADIUS msg to 10.48.17.161:
<...>
*Jan 2 04:39:09.549: CTS-provisioning: INCOMING RADIUS msg from 10.48.17.161:
1EC66C50: 0309002C 1A370BBB 58B828C3
1EC66C60: 3F0D490A 4469E8BB 4F06047B 00045012
1EC66C70: 7ECF8177 E3F4B9CB 8B0280BD 78A14CAA
1EC66C80: 4D
*Jan 2 04:39:09.549: CTS-provisioning: Received RADIUS reject from 10.48.17.161.
*Jan 2 04:39:09.549: CTS-provisioning: Successfully obtained PAC for A-ID
e6796cd7bbf2fa4111ad9fb4fefb5a50

```

由於PAC設定已成功完成，因此應該出現RADIUS拒絕。

環境資料下載

以下顯示從交換器成功下載環境資料：

```
GALA#debug cts environment-data
```

```

GALA#
*Jan 2 04:33:24.702: CTS env-data: Force environment-data refresh
*Jan 2 04:33:24.702: CTS env-data: download transport-type = CTS_TRANSPORT_IP_UDP
*Jan 2 04:33:24.702: cts_env_data START: during state env_data_complete, got event
0(env_data_request)

*Jan 2 04:33:24.702: cts_aaa_attr_add: AAA req(0x5F417F8)
*Jan 2 04:33:24.702: username = #CTSREQUEST#
*Jan 2 04:33:24.702: cts_aaa_context_add_attr: (CTS env-data SM)attr(GALA)
*Jan 2 04:33:24.702: cts-environment-data = GALA
*Jan 2 04:33:24.702: cts_aaa_attr_add: AAA req(0x5F417F8)
*Jan 2 04:33:24.702: cts_aaa_context_add_attr: (CTS env-data SM)attr(env-data-fragment)
*Jan 2 04:33:24.702: cts-device-capability = env-data-fragment
*Jan 2 04:33:24.702: cts_aaa_req_send: AAA req(0x5F417F8) successfully sent to AAA.
*Jan 2 04:33:25.474: cts_aaa_callback: (CTS env-data SM)AAA req(0x5F417F8) response success
*Jan 2 04:33:25.474: cts_aaa_context_fragment_cleanup: (CTS env-data SM)attr(GALA)
*Jan 2 04:33:25.474: cts_aaa_context_fragment_cleanup: (CTS env-data SM)attr(env-data-fragment)

*Jan 2 04:33:25.474: AAA attr: Unknown type (450).
*Jan 2 04:33:25.474: AAA attr: Unknown type (274).
*Jan 2 04:33:25.474: AAA attr: server-list = CTSServerList1-0001.
*Jan 2 04:33:25.482: AAA attr: security-group-tag = 0000-10.
*Jan 2 04:33:25.482: AAA attr: environment-data-expiry = 86400.
*Jan 2 04:33:25.482: AAA attr: security-group-table = 0001-19.
*Jan 2 04:33:25.482: CTS env-data: Receiving AAA attributes
CTS_AAA_SLIST
slist name(CTSServerList1)received in 1st Access-Accept

```

```

    slist name(CTSServerList1) created
CTS_AAA_SECURITY_GROUP_TAG - SGT = 0-10:unicast-unknown
CTS_AAA_ENVIRONMENT_DATA_EXPIRY = 86400.
CTS_AAA_SGT_NAME_LIST
    table(0001) received in 1st Access-Accept
    need a 2nd request for the SGT to SG NAME entries
    new name(0001), gen(19)
CTS_AAA_DATA_END

*Jan  2 04:33:25.784: cts_aaa_callback: (CTS env-data SM)AAA req(0x8853E60) response success
*Jan  2 04:33:25.784: cts_aaa_context_fragment_cleanup: (CTS env-data SM)attr(0001)
*Jan  2 04:33:25.784:   AAA attr: Unknown type (450).
*Jan  2 04:33:25.784:   AAA attr: Unknown type (274).
*Jan  2 04:33:25.784:   AAA attr: security-group-table = 0001-19.
*Jan  2 04:33:25.784:   AAA attr: security-group-info = 0-10-00-Unknown.
*Jan  2 04:33:25.784:   AAA attr: security-group-info = ffff-13-00-ANY.
*Jan  2 04:33:25.784:   AAA attr: security-group-info = 9-10-00-Auditors.
*Jan  2 04:33:25.784:   AAA attr: security-group-info = f-32-00-BYOD.
*Jan  2 04:33:25.784:   AAA attr: security-group-info = 5-10-00-Contractors.
*Jan  2 04:33:25.784:   AAA attr: security-group-info = 8-10-00-Developers.
*Jan  2 04:33:25.784:   AAA attr: security-group-info = c-10-00-Development_Servers.
*Jan  2 04:33:25.784:   AAA attr: security-group-info = 4-10-00-Employees.
*Jan  2 04:33:25.784:   AAA attr: security-group-info = 6-10-00-Guests.
*Jan  2 04:33:25.784:   AAA attr: security-group-info = 3-10-00-Network_Services.
*Jan  2 04:33:25.784:   AAA attr: security-group-info = e-10-00-PCI_Servers.
*Jan  2 04:33:25.784:   AAA attr: security-group-info = a-23-00-Point_of_Sale_Systems.
*Jan  2 04:33:25.784:   AAA attr: security-group-info = b-10-00-Production_Servers.
*Jan  2 04:33:25.793:   AAA attr: security-group-info = 7-10-00-Production_Users.
*Jan  2 04:33:25.793:   AAA attr: security-group-info = ff-10-00-Quarantined_Systems.
*Jan  2 04:33:25.793:   AAA attr: security-group-info = d-10-00-Test_Servers.
*Jan  2 04:33:25.793:   AAA attr: security-group-info = 2-10-00-TrustSec_Devices.
*Jan  2 04:33:25.793:   AAA attr: security-group-info = 10-24-00-VLAN10.
*Jan  2 04:33:25.793:   AAA attr: security-group-info = 11-22-00-VLAN20.
*Jan  2 04:33:25.793: CTS env-data: Receiving AAA attributes
CTS_AAA_SGT_NAME_LIST
    table(0001) received in 2nd Access-Accept
    old name(0001), gen(19)
    new name(0001), gen(19)
CTS_AAA_SGT_NAME_INBOUND - SGT = 0-68:unicast-unknown
    flag (128) sname (Unknown) added
    name (0001), request (1), receive (1)
cts_env_data_aaa_sgt_sname, name = 0001, req = 1, rcv = 1
    Setting SG Name receiving bit CTS_ENV_DATA_SGT_NAME_ENTRY on
CTS_AAA_SGT_NAME_INBOUND - SGT = 65535-68:unicast-default
    flag (128) sname (ANY) added
    name (0001), request (1), receive (1)
cts_env_data_aaa_sgt_sname, name = 0001, req = 1, rcv = 1
    Setting SG Name receiving bit CTS_ENV_DATA_SGT_NAME_ENTRY on
CTS_AAA_SGT_NAME_INBOUND - SGT = 9-68
    flag (128) sname (Auditors) added
    name (0001), request (1), receive (1)
cts_env_data_aaa_sgt_sname, name = 0001, req = 1, rcv = 1
    Setting SG Name receiving bit CTS_ENV_DATA_SGT_NAME_ENTRY on
CTS_AAA_SGT_NAME_INBOUND - SGT = 15-68
    flag (128) sname (BYOD) added
    name (0001), request (1), receive (1)
cts_env_data_aaa_sgt_sname, name = 0001, req = 1, rcv = 1
    Setting SG Name receiving bit CTS_ENV_DATA_SGT_NAME_ENTRY on
CTS_AAA_SGT_NAME_INBOUND - SGT = 5-68
    flag (128) sname (Contractors) added
    name (0001), request (1), receive (1)
cts_env_data_aaa_sgt_sname, name = 0001, req = 1, rcv = 1
    Setting SG Name receiving bit CTS_ENV_DATA_SGT_NAME_ENTRY on
CTS_AAA_SGT_NAME_INBOUND - SGT = 8-68

```

```

    flag (128) sname (Developers) added
    name (0001), request (1), receive (1)
cts_env_data_aaa_sgt_sname, name = 0001, req = 1, rcv = 1
    Setting SG Name receiving bit CTS_ENV_DATA_SGT_NAME_ENTRY on
CTS_AAA_SGT_NAME_INBOUND - SGT = 12-68
    flag (128) sname (Development_Servers) added
    name (0001), request (1), receive (1)
cts_env_data_aaa_sgt_sname, name = 0001, req = 1, rcv = 1
    Setting SG Name receiving bit CTS_ENV_DATA_SGT_NAME_ENTRY on
CTS_AAA_SGT_NAME_INBOUND - SGT = 4-68
    flag (128) sname (Employees) added
    name (0001), request (1), receive (1)
cts_env_data_aaa_sgt_sname, na
*Jan  2 04:33:25.793:      cts_env_data WAITING_RESPONSE: during state env_data_waiting_rsp, got
event 1(env_data_received)
*Jan  2 04:33:25.793: @@@ cts_env_data WAITING_RESPONSE: env_data_waiting_rsp ->
env_data_assessing
*Jan  2 04:33:25.793: env_data_assessing_enter: state = ASSESSING
*Jan  2 04:33:25.793: cts_aaa_is_fragmented: (CTS env-data SM)NOT-FRAG attr_q(0)
*Jan  2 04:33:25.793: env_data_assessing_action: state = ASSESSING
*Jan  2 04:33:25.793: cts_env_data_is_complete: FALSE, req(x1085), rec(x1487)
*Jan  2 04:33:25.793: cts_env_data_is_complete: TRUE, req(x1085), rec(x1487), expect(x81),
completel(x85), complete2(xB5), complete3(x1485)
*Jan  2 04:33:25.793:      cts_env_data ASSESSING: during state env_data_assessing, got event
4(env_data_complete)
*Jan  2 04:33:25.793: @@@ cts_env_data ASSESSING: env_data_assessing -> env_data_complete
*Jan  2 04:33:25.793: env_data_complete_enter: state = COMPLETE
*Jan  2 04:33:25.793: env_data_install_action: state = COMPLETE

```

CTS策略

CTS策略作為RADIUS消息的一部分被推送，因此runtime-AAA日誌記錄元件在ISE上設定為調試 (Administration > Logging > Debug Log Configuration)，並且在交換機上的調試下應足以解決與CTS相關的任何問題：

```

debug cts coa
debug radius

```

此外，檢查交換機上匹配的策略 — 3750X:

```

GALA#show cts role-based counters
Role-based IPv4 counters
# '-' in hardware counters field indicates sharing among cells with identical policies
From      To      SW-Denied      HW-Denied      SW-Permitted      HW-Permitted

10        15        5                0                0                0

*         *         0                0                815              31

17        15        0                0                0                0
17        16        0                -                0                -

```

由於Cisco bug ID [CSCuu32958](#)，您無法在3850上使用相同的命令。