瞭解ISE SXP更新日誌和Catalyst調試日誌

目錄

簡介

本文檔介紹如何配置和理解ISE與Catalyst 9300交換機之間的安全組交換協定(SXP)連線。

背景資訊

SXP是TrustSec用來將IP到SGT對映傳播到TrustSec裝置的SGT（安全組標籤）交換協定。

SXP的開發目的是讓包括第三方裝置在內的網路或不支援SGT內聯標籤的舊版思科裝置具有TrustSec功能。

SXP是一種對等協定；一台裝置可以充當發言者，而另一台裝置可以充當偵聽者。

SXP發言人負責傳送IP-SGT繫結，而監聽程式負責收集這些繫結。

SXP連線使用TCP埠64999作為底層傳輸協定，並使用MD5實現消息完整性/真實性。

必要條件

需求

思科建議您瞭解SXP協定和身份服務引擎(ISE)配置。

採用元件

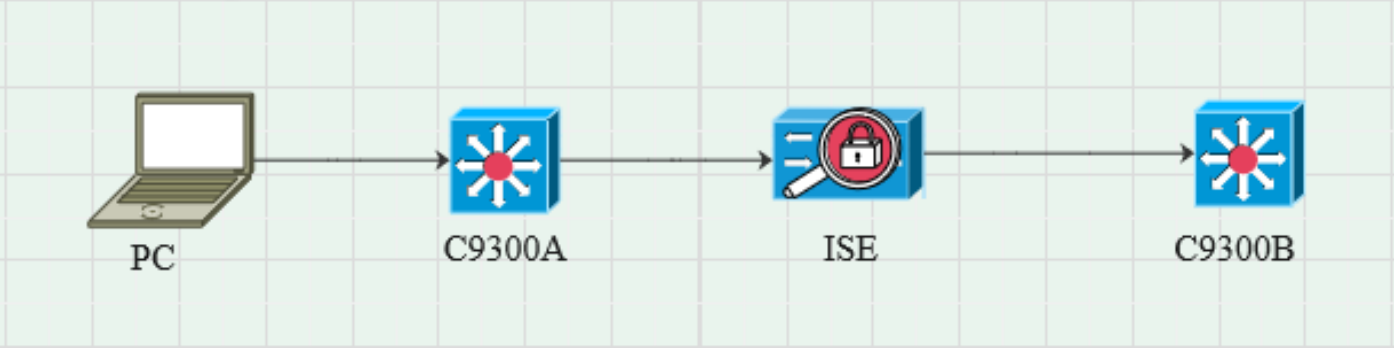
本文中的資訊係根據以下軟體和硬體版本：

- 裝有軟體Cisco IOS® XE 17.6.5及更高版本的Cisco Catalyst 9300交換機
  Cisco ISE版本3.1及更高版本

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。

組態

網路圖表



流量傳輸

PC使用C9300A進行身份驗證，ISE透過策略集動態分配SGT。
身份驗證透過後，將使用與策略中配置的Framed-IP address RADIUS屬性和SGT相同的IP建立繫結。
繫結在預設域下的「所有SXP繫結」中傳播。
C9300B透過SXP協定從ISE接收SXP對映資訊。

設定交換器

將交換機配置為SXP偵聽器以從ISE獲取IP-SGT對映。

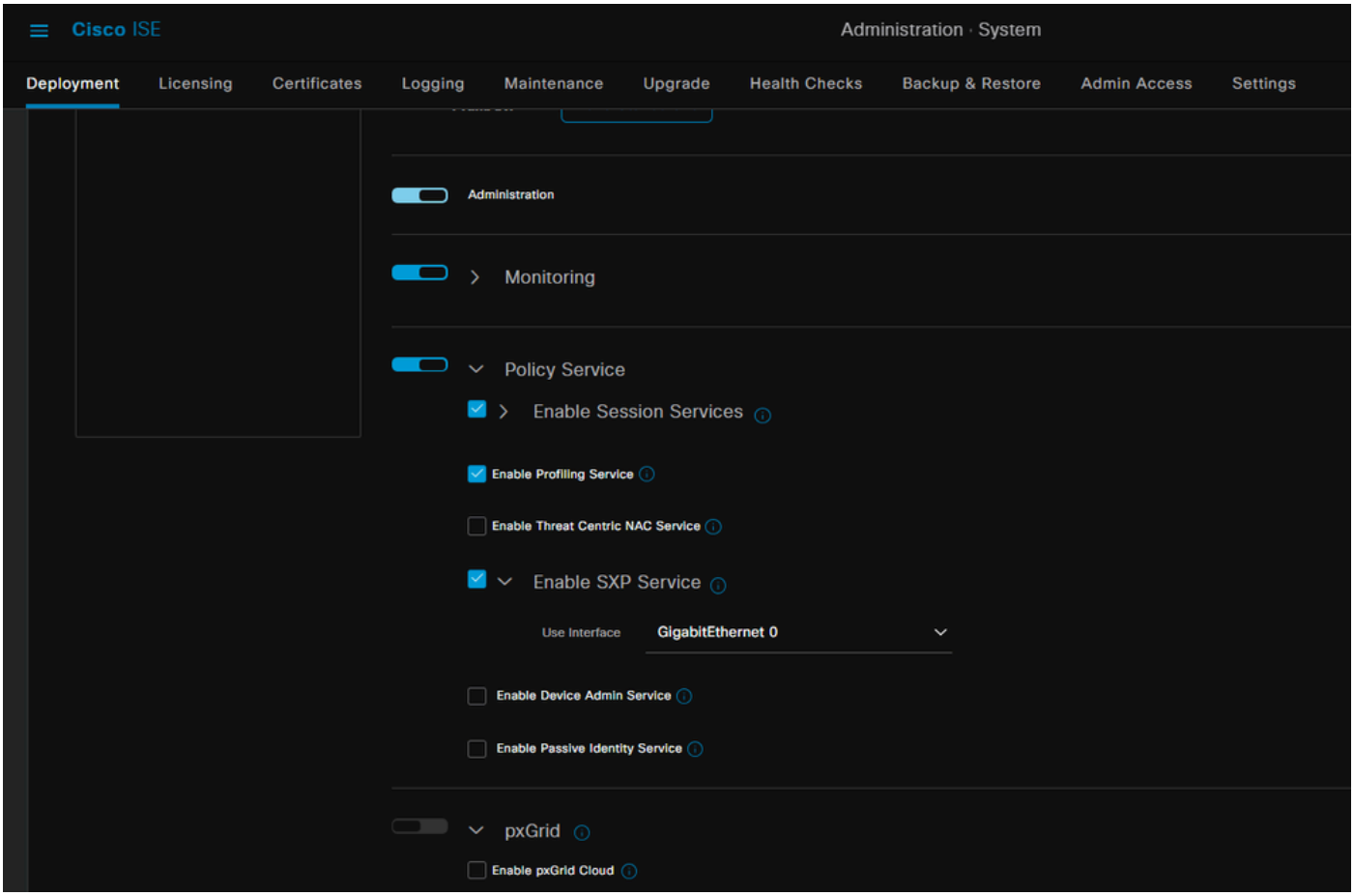
```
cts sxp enable
cts sxp預設密碼cisco
```

```
cts sxp default source-ip 10.127.213.27
cts sxp connection peer 10.127.197.53 password default mode peer speaker hold-time 0 0 vrf
Mgmt-vrf
```

配置ISE

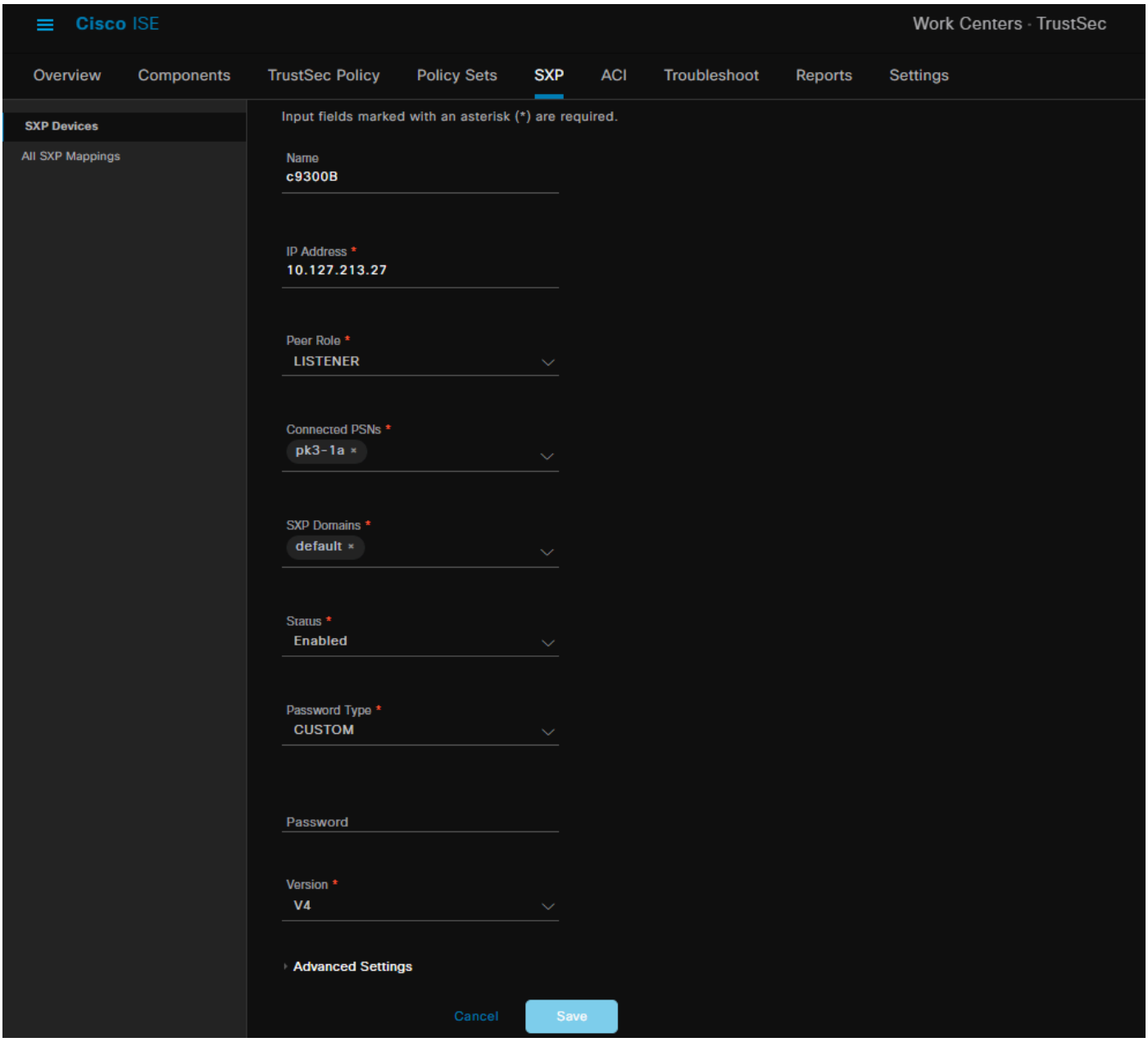
步驟 1.在ISE上啟用SXP服務

導航到管理>系統>部署>編輯節點，在策略服務下選擇啟用SXP服務。



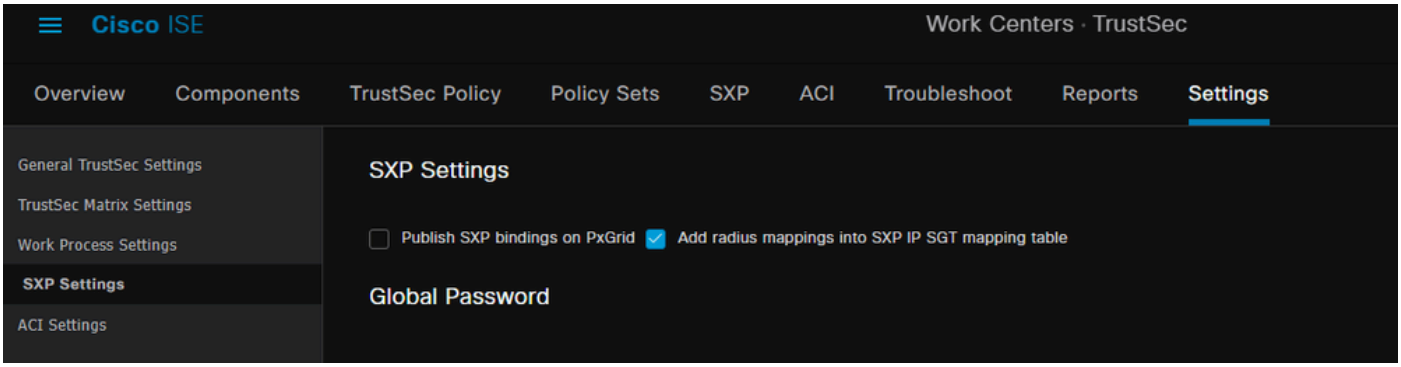
步驟 2.增加SXP裝置

要為相應交換機配置SXP偵聽器和揚聲器，請導航到Workcenters > Trustsec > SXP > SXP Devices。
增加具有對等體角色的交換機作為Listener，並分配到預設域。



步驟 3.SXP設定

確保選中Add radius mappings into SXP IP SGT mapping table，以便ISE透過Radius身份驗證瞭解動態IP-SGT對映。



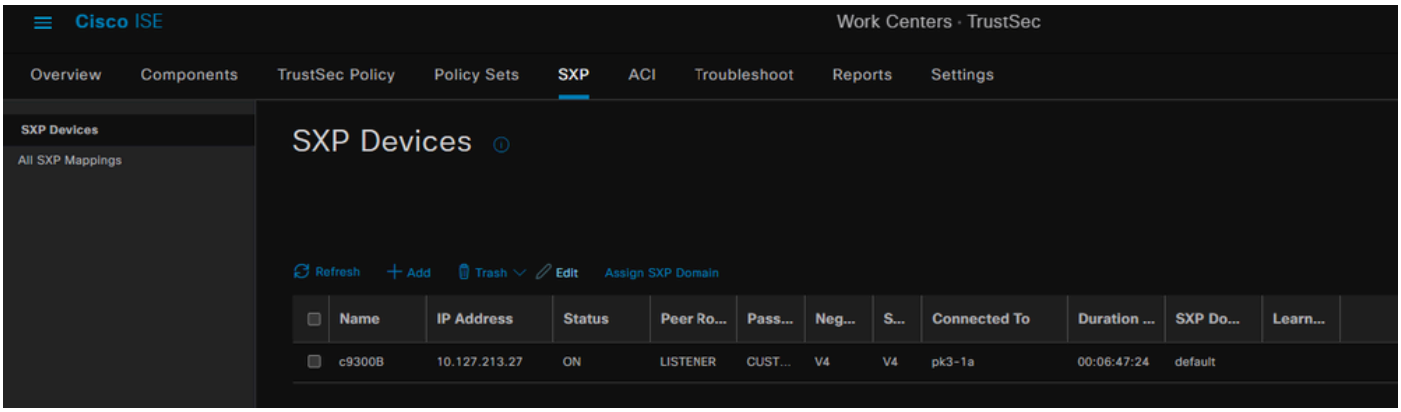
驗證

步驟 1.交換機上的SXP連線

```
C9300B#show cts sxp connections vrf Mgmt-vrf
SXP：已啟用
支援的最高版本：4
預設密碼：Set
預設金鑰鏈：未設定
預設金鑰鏈結名稱：不適用
預設源IP：10.127.213.27
連線重試開啟期間：120秒
調解期間：120秒
重試打開計時器未運行
匯出的對等順序遍歷限制：未設定
匯入的對等順序遍歷限制：未設定
----------------------------------------------
對等IP：10.127.197.53
源IP：10.127.213.27
Conn狀態：開啟
Conn版本：4
連線功能：IPv4-IPv6-子網
連線保持時間：120秒
本地模式：SXP監聽程式
連線例項#：1
TCP連線fd：1
TCP連介面令：預設SXP口令
保留計時器正在運行
自上次狀態更改以來的持續時間：0:00:23:36 (dd：hr：mm：sec)


SXP連線總數= 1

0x7F128DF555E0 VRF：Mgmt-vrf，fd：1，對等ip：10.127.197.53
cdbp：0x7F128DF555E0 Mgmt-vrf <10.127.197.53， 10.127.213.27> tableid：0x1
```

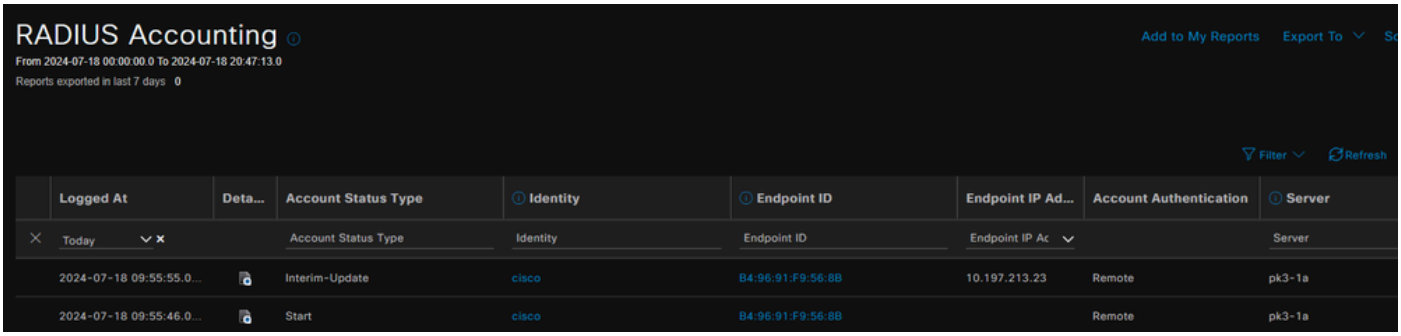
步驟 2.ISE SXP驗證

在Workcenters > Trustsec > SXP > SXP Devices下，驗證交換機的SXP狀態為ON。



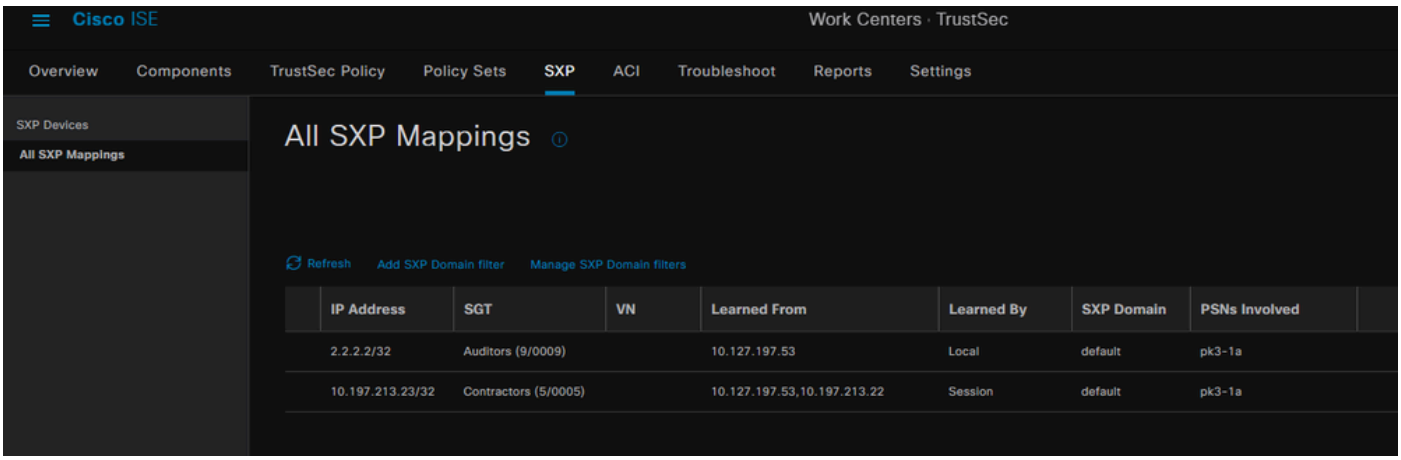
步驟 3.RADIUS 計量

在身份驗證成功後，確保ISE從RADIUS記帳資料包接收到Framed-IP address RADIUS屬性。

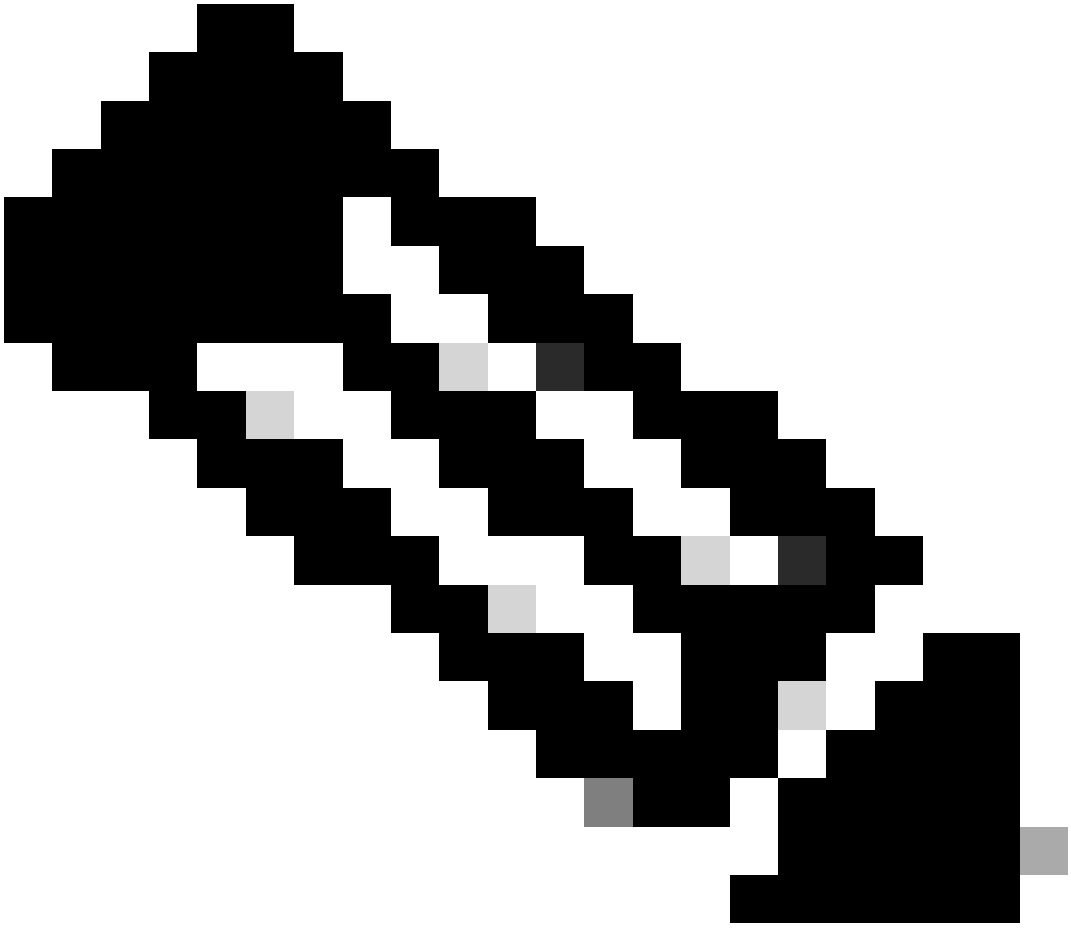


步驟 4.ISE SXP對映

導航到工作中心> Trustsec > SXP >所有SXP對映，檢視從Radius會話動態獲取的IP-SGT對映。



學習者
本地-靜態分配的ISE IP-SGT繫結。
會話-從Radius會話動態獲知的IP-SGT繫結。



注意：ISE能夠接收來自其他裝置的IP-SGT繫結。這些繫結可以在「所有SXP對映」下顯示為Learned by SXP。

步驟 5.交換機上的SXP對映

交換機透過SXP協定從ISE獲取IP-SGT對映。

```
C9300B#show cts sxp sgt-map vrf Mgmt-vrf brief
SXP節點ID（已生成）：0x03030303(3.3.3.3)
IP-SGT對映，如下所示：
IPv4，SGT： <2.2.2,9>
IPv4，SGT： <10.197.213.23， 5>
IP-SGT對映總數：2
sxp_bnd_exp_conn_list中的conn （總計：0）：
C9300B#
```

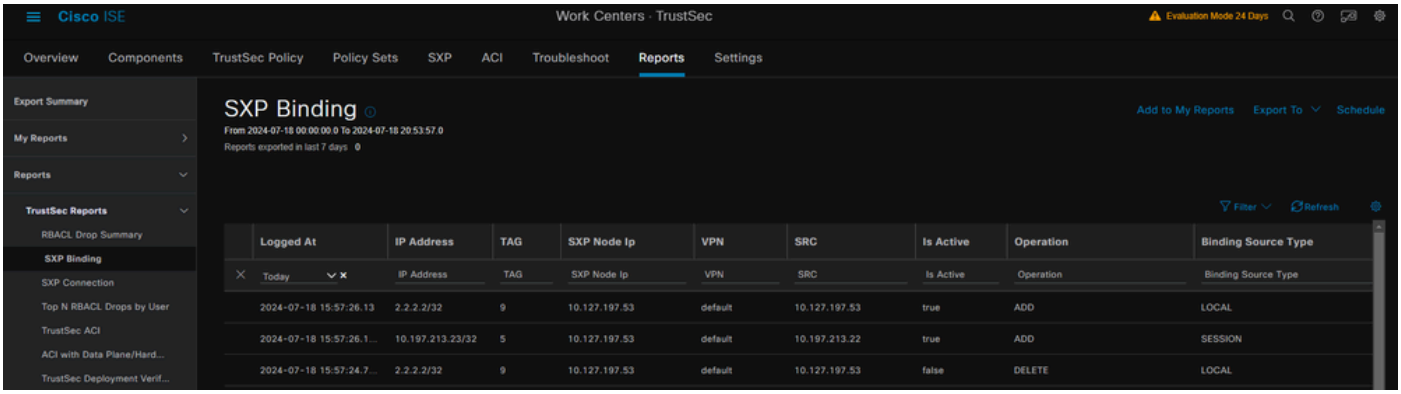
```
C9300B#show cts role-based sgt-map vrf Mgmt-vrf all
活動IPv4-SGT繫結資訊

IP Address SGT Source
========================================
2.2.2.2 9 SXP
10.197.213.23 5 SXP

IP-SGT活動繫結摘要
========================================
SXP繫結總數= 2
作用中繫結總數= 2
```

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

ISE報告

ISE還允許生成SXP繫結和連線報告，如下圖所示。



ISE上的調試

收集具有以下屬性的ISE支援捆綁包，以在調試級別進行設定：

- sxp
- sgtbinding
- nsf
- nsf-session
- trustsec

當從ISE伺服器對使用者進行身份驗證時，ISE會在訪問接受響應資料包中分配SGT。使用者獲取IP地址後，交換機將在RADIUS記賬資料包中傳送成幀IP地址。

show logging application localStore/iseLocalStore.log：

2024-07-18 09:55:55.051 +05:30 000017592 3002通知Radius-Accounting： RADIUS記帳監視器更新，ConfigVersionId=129，裝置IP地址=10.197.213.22，使用者名稱=cisco，網路裝置名稱=pk，使用者名稱=cisco， nas-IP-Address=10.197.213.22、NAS-Port=50124、Framed-IP-Address=10.197.213.23、Class=CACS：16D5C50A00000017C425E3C6：pk3-1a/510648097/25、Called-Station-ID=C4-B2-39-ED-AB-18、 calling-Station-ID=B4-96-91-F9-56-8B， Acct-Status-Type=Interim-Update， Acct-Delay-Time=0， Acct-Input-Octets=413， Acct-Output-Octets=0， Acct-Session-Id=00000007， Acct-Authentic=Remote， Acct-Input-Packets=4， Acct-Output-Packets=0， Event-Timestamp=1721277745， NAS-Port-Type=Ethernet NAS-Port-Id=TenGigabitEthernet1/0/24、cisco-av-pair=audit-session-id=16D5C50A00000017C425E3C6、cisco-av-pair=method=dot1x、cisco-av-pair=cts：security-group-tag=0005-00、AcsSessionID=pk3-1a/510648097/28、SelectedAccessService=Default Network Access、Latency=6、Step=11004 Step=11017， Step=15049， Step=15008， Step=22085， NetworkDeviceGroups=IPSEC#Is IPSEC Device#No， NetworkDeviceGroups=Location#All Locations， NetworkDeviceGroups=Device Type#All Device Types， CPMSessionID=16D5C50A1100500000017 C425E3C6， TotalAuthenLatency=6， ClientLatency=0， Network Device Profile=Profile cisco， Location=Location#All Locations， Device Type=Device Type#All Device Types， IPSEC=IPSEC#Is IPSEC Device#No，

show logging application ise-psc.log：

2024-07-18 09:55:55,054調試[SxpSessionNotifierThread][]
ise.sxp.sessionbinding.util.SxpBindingUtil -： ：-
記錄從PrrtCpmBridge接收的會話值：
操作型別==>ADD， sessionId ==> 16D5C50A00000017C425E3C6， sessionState ==> ACCEPTED，inputIp ==> 10.197.213.23， inputSgTag ==> 0005-00，nas Ip ==> 10.197.213.22null， vn ==> null

SXP節點將IP + SGT對映儲存在其H2DB表中，之後的PAN節點收集此IP SGT對映並在ISE GUI中的所有SXP對映中反映出來（工作中心->Trustsec -> SXP ->所有SXP對映）。

show logging application sxp_appserver/sxp.log：

2024-07-18 10:01:01,312 INFO [sxpservice-http-96441] cisco.ise.sxp.rest.SxpGlueRestAPI：147 - SXP-PEERF增加會話繫結batch-size： 1
2024-07-18 10:01:01,317 DEBUG [SxpNotificationSerializer-Thread] cpm.sxp.engine.services.NotificationSerializerImpl：202 -處理任務任務[add=true， notification=RestSxpLocalBinding(tag=5， groupName=null， ipAddress=10.197.213.23/32， nasIp=10.197.213.22， session2， sessionId=16 c50A00000017C425E3C6， peerSequence=null， sxpBindingOpType=null， sessionExpiryTimeInMillis=0， apic=false， routable=true， vns=[])]

2024-07-18 10:01:01,344 DEBUG [SxpNotificationSerializer-Thread] cisco.cpm.sxp.engine.SxpEngine：1543 - [VPN： 'default']增加新繫結： MasterBindingIdentity

```
[ip=10.197.213.23/32， peerSequence=10.127.197.53,10.197.22，2 5， isLocal=true，
sessionId=16D5C50A00000017C425E3C6， vn=DEFAULT_VN]
2024-07-18 10:01:01,344 DEBUG [SxpNotificationSerializer-Thread]
cisco.cpm.sxp.engine.SxpEngine：1581 -增加1個繫結
2024-07-18 10:01:01,344 DEBUG [SxpNotificationSerializer-Thread]
cisco.cpm.sxp.engine.MasterDbListener：251 -向H2處理程式提交用於增加繫結的任務，繫結計數
： 1
2024-07-18 10:01:01,344 DEBUG [H2_HANDLER] cisco.cpm.sxp.engine.MasterDbListener：256
- MasterDbListener正在處理onAdded - bindingsCount：1
```

SXP節點使用最新的IP-SGT繫結更新對等交換機。

```
2024-07-18 10:01:01,346 DEBUG [pool-7-thread-4]
opendaylight.sxp.core.service.UpdateExportTask：93 -
SXP_PERF：SEND_UPDATE_BUFFER_SIZE=32
2024-07-18 10:01:01,346 DEBUG [pool-7-thread-4]
opendaylight.sxp.core.service.UpdateExportTask：116 - SENT_UPDATE到
[ISE：10.127.197.53][10.127.197.53:64999/10.127.213.27:31025][O|Sv4]
2024-07-18 10:01:01,346 DEBUG [pool-7-thread-4]
opendaylight.sxp.core.service.UpdateExportTask：137 - SENT_UPDATE SUCCESSFUL TO
[ISE：10.127.197.53][10.127.197.53:64999/10.127.213.27:31025][O|Sv4]
```

交換機上的調試

在交換機上啟用這些調試以排除SXP連線和更新的故障。

debug cts sxp conn

debug cts sxp error

debug cts sxp mdb

debug cts sxp message

交換機從SXP發言人「ISE」收到SGT-IP對映。

選中Show logging以檢視以下日誌：

```
7月18日04:23:04.324： CTS-SXP-MSG：sxp_recv_update_v4 <1>對等ip：10.127.197.53
7月18日04:23:04.324：CTS-SXP-MDB：IMU增加繫結：- <conn_index = 1>來自對等體
10.127.197.53
7月18日04:23:04.324： CTS-SXP-MDB：mdb_send_msg <IMU_ADD_IPSGT_DEVID>

7月18日04:23:04.324： CTS-SXP-INTNL：mdb_send_msg mdb_process_add_ipsgt_devid開始
```

```
7月18日04:23:04.324： CTS-SXP-MDB：sxp_mdb_inform_rbm表格ID：0x1 sense：1 sgt：5
peer：10.127.197.53
7月18日04:23:04.324：CTS-SXP-MDB：SXP MDB：增加了Entry ip 10.197.213.23 sgt 0x0005
7月18日04:23:04.324：CTS-SXP-INTNL：mdb_send_msg mdb_process_add_ipsgt_devid完成
```

相關資訊

ISE 3.1管理指南分段

Catalyst配置指南Trustsec概述

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）。