了解ISE SXP更新日志和Catalyst调试日志

目录

简介

本文档介绍如何配置和了解ISE和Catalyst 9300交换机之间的安全组交换协议(SXP)连接。

背景信息

SXP是TrustSec用于将IP到SGT的映射传播到TrustSec设备的SGT（安全组标记）交换协议。

SXP的开发允许包括第三方设备或不支持SGT内联标记的旧思科设备在内的网络具有TrustSec功能。

SXP是一种对等协议；一台设备可以用作发言者，另一台设备可以用作收听者。

SXP扬声器负责发送IP-SGT绑定，而侦听器负责收集这些绑定。

SXP连接使用TCP端口64999作为底层传输协议，使用MD5实现消息完整性/真实性。

先决条件

要求

思科建议您了解SXP协议和身份服务引擎(ISE)配置。

使用的组件

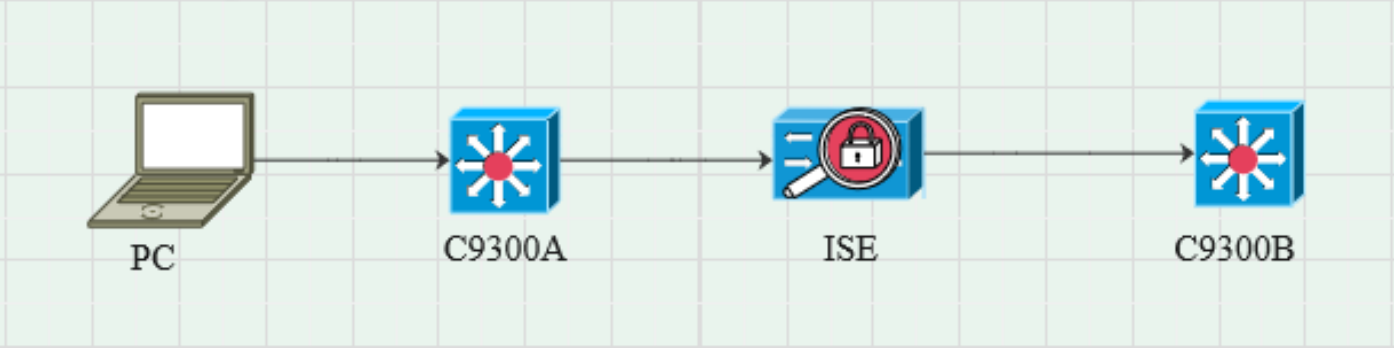
本文档中的信息基于以下软件和硬件版本：

- 装有软件Cisco IOS® XE 17.6.5及更高版本的Cisco Catalyst 9300交换机
  思科ISE版本3.1及更高版本

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

配置

网络图



流量传输

PC使用C9300A进行身份验证，ISE通过策略集动态分配SGT。
当身份验证通过时，使用与策略中配置的Framed-IP address RADIUS属性和SGT相等的IP创建绑定。
绑定在默认域下的“所有SXP绑定”中传播。
C9300B通过SXP协议接收来自ISE的SXP映射信息。

配置交换机

将交换机配置为SXP侦听程序以从ISE获取IP-SGT映射。

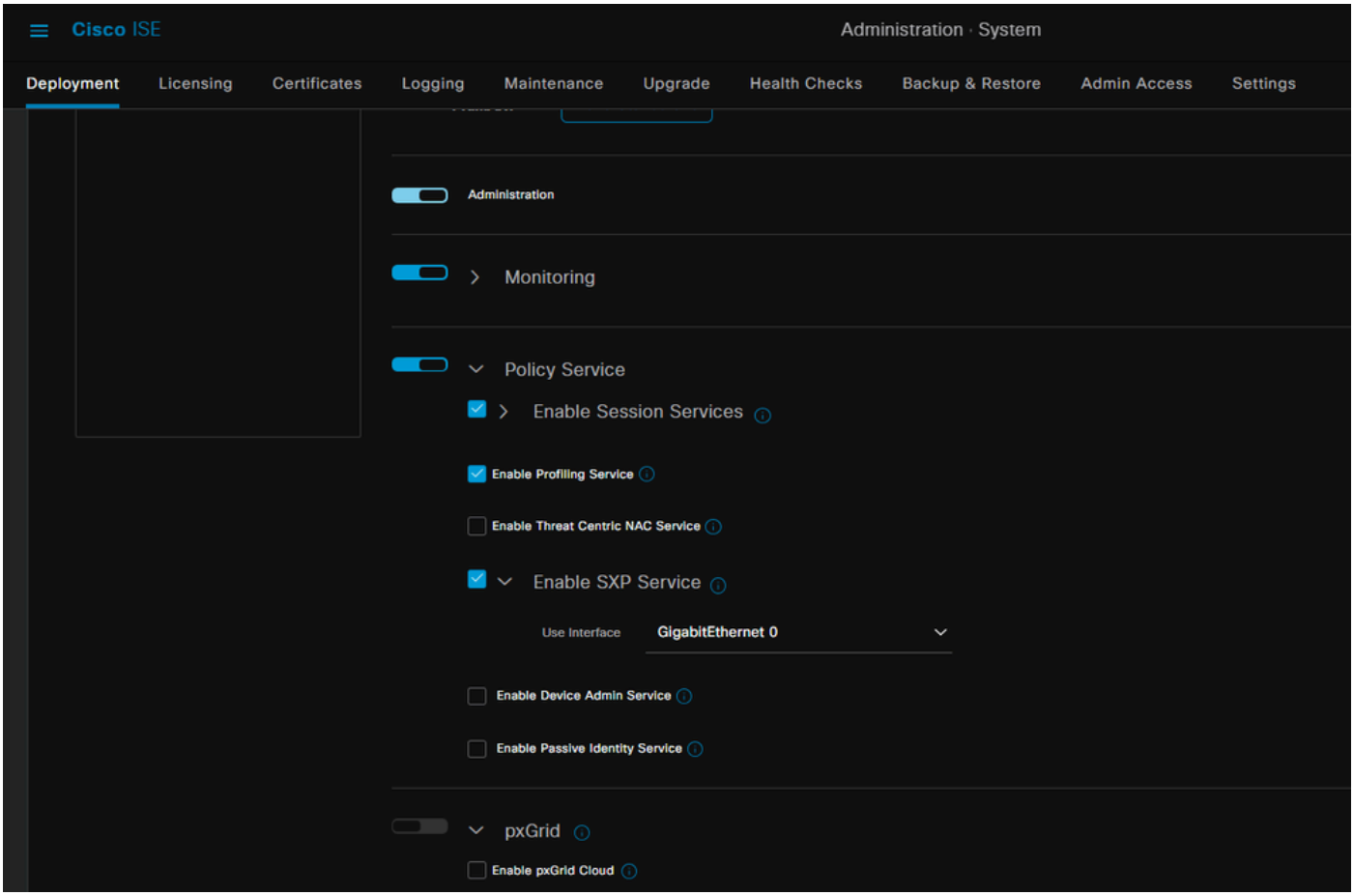
```
cts sxp enable
cts sxp default password cisco
```

```
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

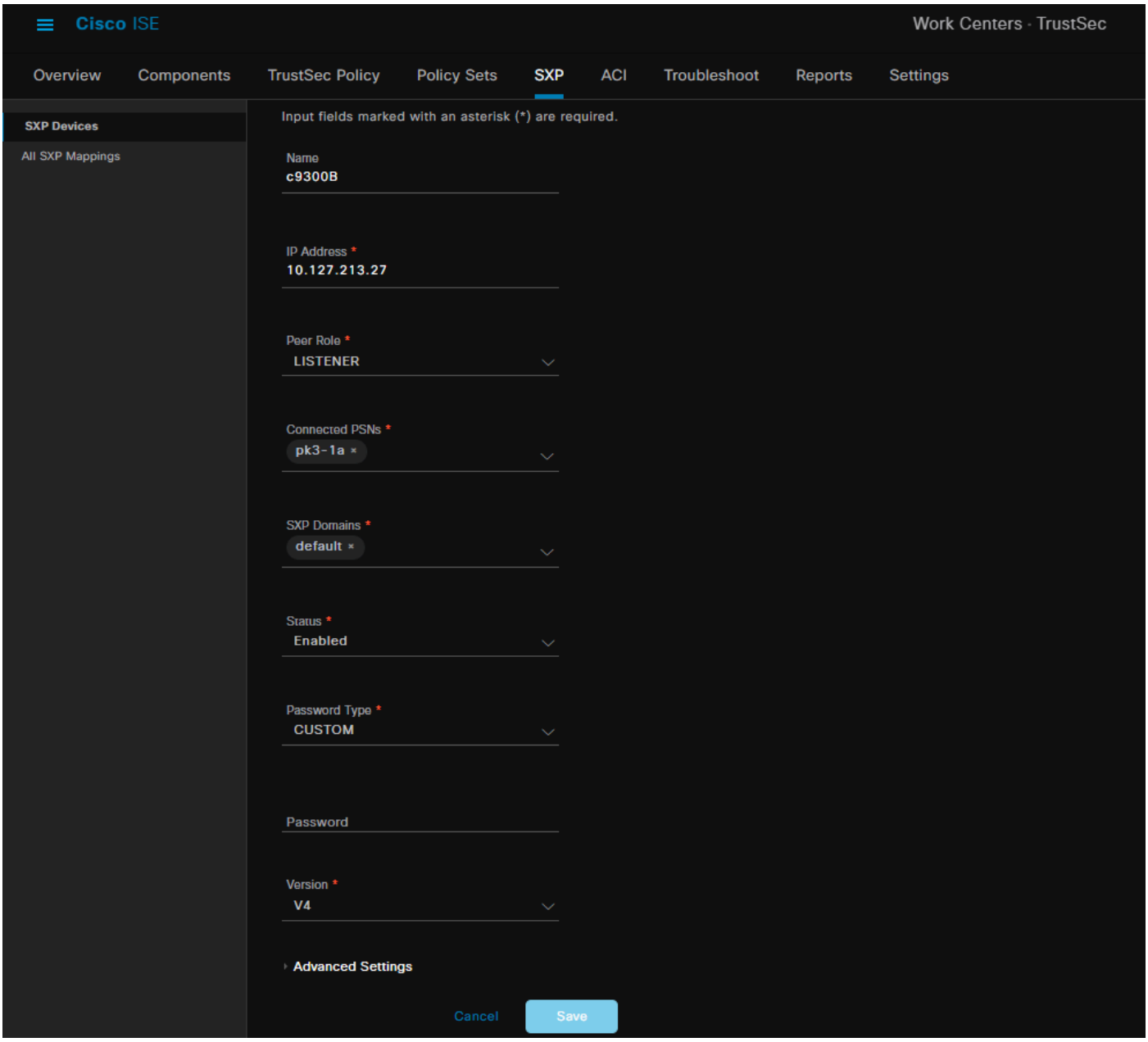
步骤1:在ISE上启用SXP服务

导航到管理>系统>部署>编辑节点，在策略服务下选择启用SXP服务。



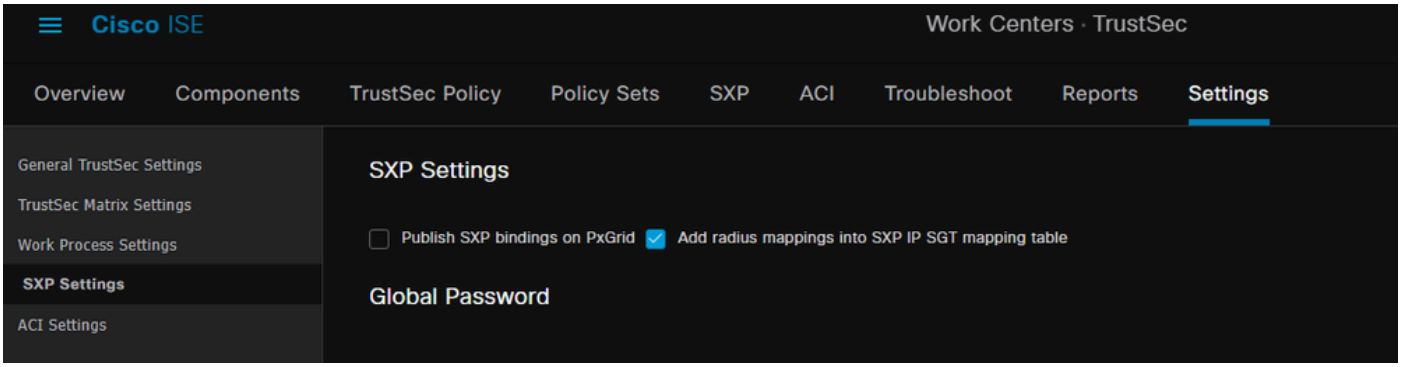
第二步：添加SXP设备

要配置相应交换机的SXP侦听器和扬声器，请导航到Workcenters > Trustsec > SXP > SXP Devices。
添加具有作为侦听程序的对等角色的交换机，并将其分配到默认域。



第三步：SXP设置

确保选中Add radius mappings into SXP IP SGT mapping table，以便ISE通过Radius身份验证了解动态IP-SGT映射。



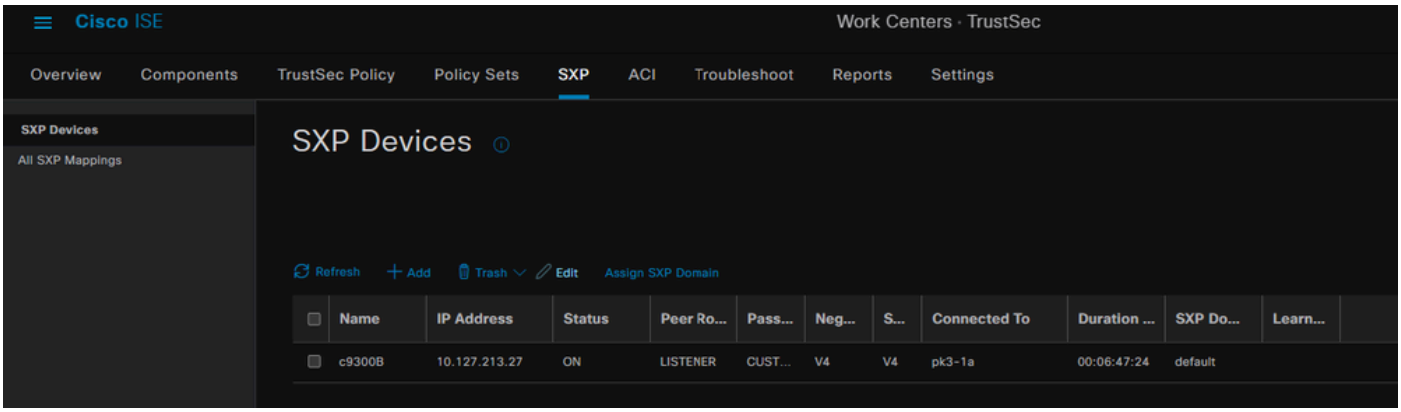
验证

步骤1:交换机上的SXP连接

```
C9300B#show cts sxp connections vrf Mgmt-vrf
SXP：已启用
支持的最高版本：4
默认密码：Set
默认密钥链：未设置
默认密钥链名称：不适用
默认源IP：10.127.213.27
连接重试打开时间：120秒
调整期间：120秒
重试打开计时器未运行
导出对等序列遍历限制：未设置
导入的对等序列遍历限制：未设置
----------------------------------------------
对等IP：10.127.197.53
源IP：10.127.213.27
连接状态：打开
Conn版本：4
连接功能：IPv4-IPv6-Subnet
连接保持时间：120秒
本地模式：SXP侦听程序
连接实例#：1
TCP conn fd：1
TCP连接密码：默认SXP密码
保持计时器正在运行
自上次状态更改以来的持续时间：0:00:23:36 (dd：hr：mm：sec)


SXP连接总数= 1

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

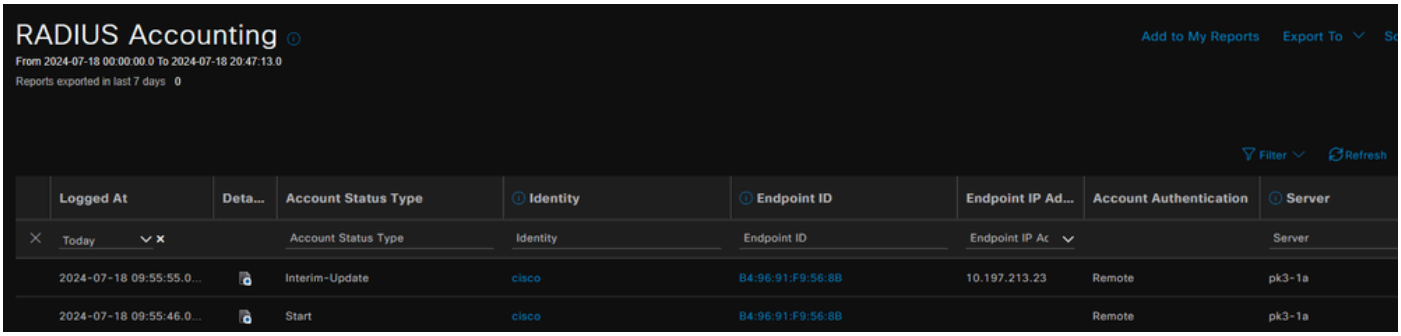
第二步：ISE SXP验证

在Workcenters > Trustsec > SXP > SXP Devices下验证交换机的SXP状态为ON。



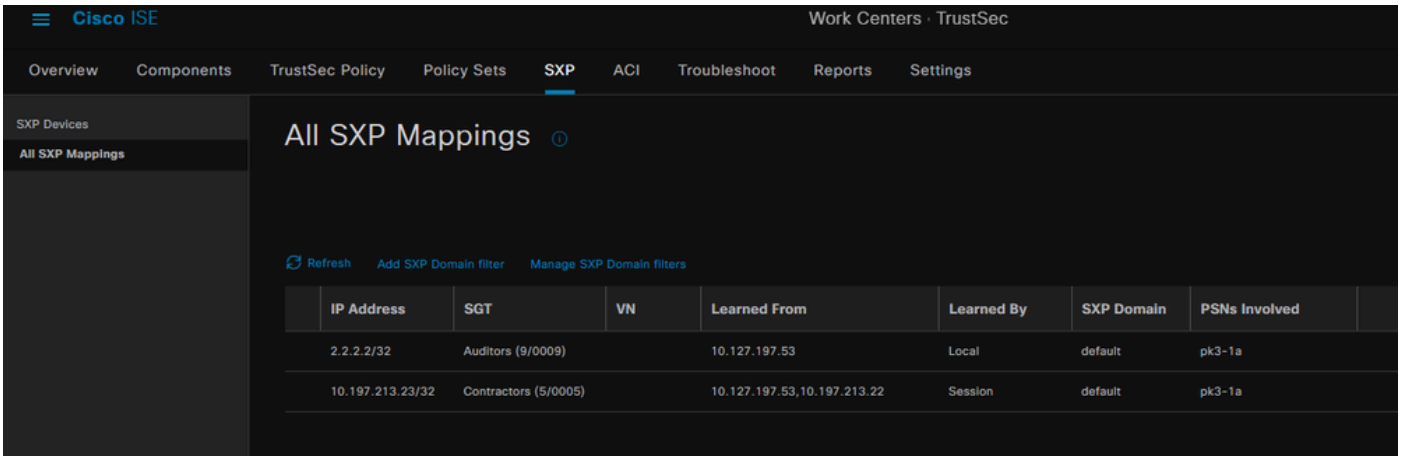
第三步：RADIUS 记帐

确保ISE在身份验证成功后从RADIUS记账数据包接收到Framed-IP address RADIUS属性。

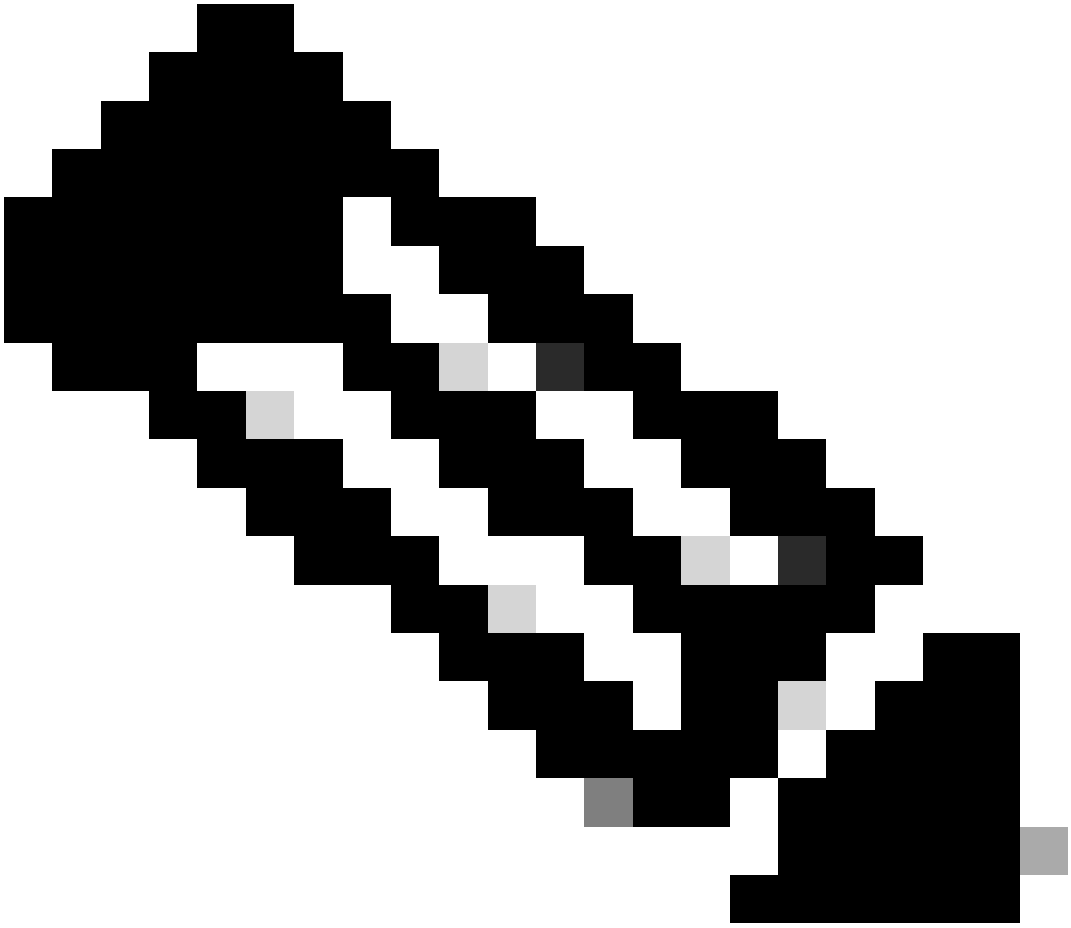


第四步：ISE SXP映射

导航到工作中心(Workcenters) > Trustsec > SXP >所有SXP映射(All SXP Mappings)，查看从Radius会话动态获取的IP-SGT映射。



学习者
本地-在ISE上静态分配的IP-SGT绑定。
会话-从Radius会话动态获取的IP-SGT绑定。



注意：ISE能够接收来自其他设备的IP-SGT绑定。这些绑定可以显示在“所有SXP映射”下由SXP获知的状态。

第五步：交换机上的SXP映射

交换机通过SXP协议从ISE获取IP-SGT映射。

```
C9300B#show cts sxp sgt-map vrf Mgmt-vrf brief
SXP节点ID（已生成）：0x03030303(3.3.3.3)
IP-SGT映射如下：
IPv4，SGT： <2.2.2.2， 9>
IPv4，SGT：<10.197.213.23， 5>
IP-SGT映射总数：2
sxp_bnd_exp_conn_list中的conn（总数：0）：
C9300B#
```

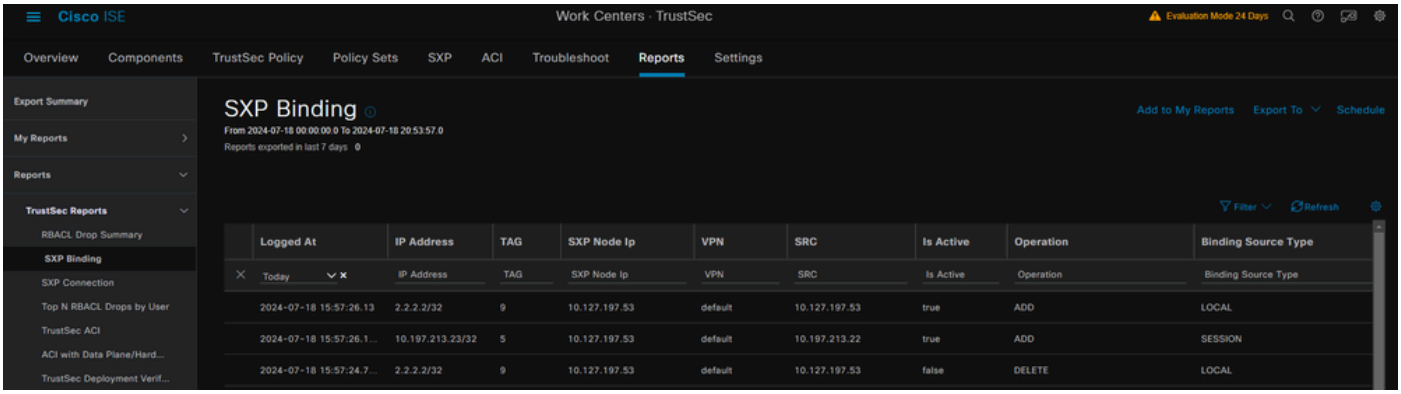
```
C9300B#show cts role-based sgt-map vrf Mgmt-vrf all
活动IPv4-SGT绑定信息

IP地址SGT源
========================================
2.2.2.2 9 SXP
10.197.213.23 5个SXP

IP-SGT活动绑定摘要
========================================
SXP绑定总数= 2
活动绑定总数= 2
```

故障排除

本部分提供的信息可用于对配置进行故障排除。

ISE报告

ISE还允许生成SXP绑定和连接报告，如下图所示。



ISE上的调试

收集具有以下属性的ISE支持捆绑包，在调试级别进行设置：

- sxp
- sgtbinding
- nsf
- NSF会话
- trustsec

从ISE服务器对用户进行身份验证时，ISE会在访问接受响应数据包中分配SGT。用户获得IP地址后，交换机将在RADIUS记账数据包中发送成帧IP地址。

show logging application localStore/iseLocalStore.log：

2024-07-18 09:55:55.051 +05:30 0000017592 3002 RADIUS-Accounting：RADIUS记帐监视器更新，ConfigVersionId=129，设备IP地址=10.197.213.22，用户名=cisco，网络设备名称=pk，用户名=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=Type 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调试[SxpSessionNotifierThread][]
ise.sxp.sessionbinding.util.SxpBindingUtil -：：-
记录从PrrtCpmBridge收到的会话值：
操作类型==>ADD、sessionId ==> 16D5C50A00000017C425E3C6、sessionState ==>已接受、inputIp ==> 10.197.213.23、inputSgTag ==> 0005-00、nas Ip ==> 10.197.213.22null、vn ==>空

SXP节点将IP + SGT映射存储在其H2DB表中，随后PAN节点收集此IP SGT映射并在ISE GUI中的所有SXP映射中反映出来（工作中心->Trustsec -> SXP->所有SXP映射）。

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添加会话绑定批处理大小：1
2024-07-18 10:01:01,317 DEBUG [SxpNotificationSerializer-Thread] cpm.sxp.engine.services.NotificationSerializerImpl：202 -处理任务任务[add=true，notification=RestSxpLocalBinding(tag=5， groupName=null， ipAddress=10.197.213.23/32，nasIp=10.197.23.22， 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']添加新绑定： MasterBindingIdentity [ip=10.197.213.23/32， peerSequence=10.127.197.53,10.197.2，2 tag 5， isLocal=true，sessionId=16D5C50A00000017C425E3C6， vn=DEFAULT_VN]

```
2024-07-18 10:01:01,344 DEBUG [SxpNotificationSerializer-Thread]
cisco.cpm.sxp.engine.SxpEngine：1581 -添加1个绑定
2024-07-18 10:01:01,344 DEBUG [SxpNotificationSerializer-Thread]
cisco.cpm.sxp.engine.MasterDbListener：251 -向H2处理程序提交用于添加绑定的任务，绑定计数
：1
2024-07-18 10:01:01,344 DEBUG [H2_HANDLER] cisco.cpm.sxp.engine.MasterDbListener：256
- MasterDbListener正在处理onAdded - bindingsCount：1
```

SXP节点使用最新的IP-SGT绑定更新对等交换机。

```
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 to
[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]
```

交换机上的调试

在交换机上启用这些调试，以排除SXP连接和更新的故障。

debug cts sxp conn

debug cts sxp error

debug cts sxp mdb

debug cts sxp message

交换机从SXP发言人“ISE”收到SGT-IP映射。

选中**Show logging**以查看以下日志：

```
7月18日04:23:04.324：CTS-SXP-MSG：sxp_recv_update_v4 <1>对等ip：10.127.197.53
7月18日04:23:04.324：CTS-SXP-MDB：IMU添加绑定：- <conn_index = 1>来自对等体
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启动
7月18日04:23:04.324：CTS-SXP-MDB：sxp_mdb_inform_rbm表id：0x1感知：1 sgt：5对等点
：10.127.197.53
```

```
7月18日04:23:04.324：CTS-SXP-MDB：SXP MDB：已添加条目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
```

相关信息

ISE 3.1管理指南分段

Catalyst配置指南Trustsec概述

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。