Comprendre le mécanisme de consignation SXP dans ISE–Communication Catalyst

Table des matières

Introduction

Conditions préalables

- Exigences
- Composants utilisés

Informations générales

Configuration

- Diagramme du réseau
- Flux de trafic
- Configurer le commutateur
- Configuration d'ISE
  - Étape 1 : activation du service SXP sur ISE
  - Étape 2. Ajout de périphériques SXP
  - Étape 3. Paramètres SXP

Vérifier

- Étape 1. Connexion SXP sur le commutateur
- Étape 2. Vérification ISE SXP
- Étape 3. Comptabilisation Radius
- Étape 4. Mappages ISE SXP
- Étape 5. Mappages SXP sur le commutateur

Dépannage

- Rapport ISE
- Débogages sur ISE
- Débogages sur le commutateur

Informations connexes

Introduction

Ce document décrit comment configurer et comprendre la connexion SXP (Security Group Exchange Protocol) entre ISE et le commutateur Catalyst 9300.

Conditions préalables

Exigences

Cisco vous recommande de connaître le protocole SXP et la configuration ISE (Identity Services Engine).

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Commutateur Cisco Catalyst 9300 avec logiciel Cisco IOS® XE 17.6.5 et versions ultérieures
  Cisco ISE, versions 3.1 et ultérieures

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

SXP est le protocole SGT (Security Group Tag) Exchange Protocol utilisé par TrustSec pour propager les mappages IP/SGT aux périphériques TrustSec.

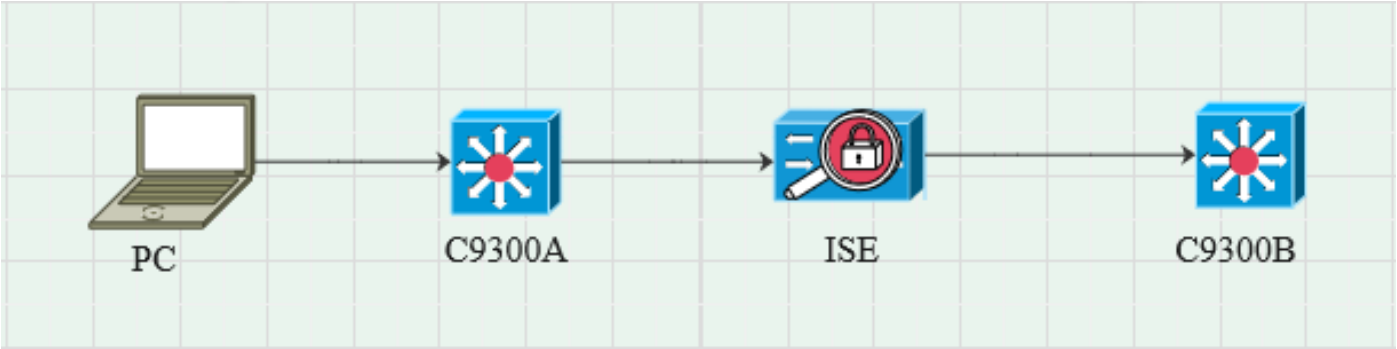
SXP a été développé pour permettre aux réseaux, y compris les périphériques tiers ou les périphériques Cisco hérités qui ne prennent pas en charge l'étiquetage en ligne SGT, de disposer de fonctionnalités TrustSec.

SXP est un protocole d'appairage ; un périphérique peut agir en tant que haut-parleur et l'autre en tant qu'écouteur :

- Le haut-parleur SXP est responsable de l'envoi des liaisons IP-SGT et l'écouteur est responsable de la collecte de ces liaisons.
- La connexion SXP utilise le port TCP 64999 comme protocole de transport sous-jacent et MD5 pour l'intégrité et l'authenticité des messages.

Configuration

Diagramme du réseau



Flux de trafic

PC s'authentifie auprès de C9300A et ISE attribue dynamiquement les balises SGT via des

ensembles de stratégies.
Une fois l'authentification terminée, les liaisons sont créées avec une adresse IP égale à l'attribut RADIUS de l'adresse IP tramée et au SGT configurés dans la stratégie.
Les liaisons se propagent dans toutes les liaisons SXP sous le domaine par défaut.
C9300B reçoit les informations de mappage SXP d'ISE via le protocole SXP.

Configurer le commutateur

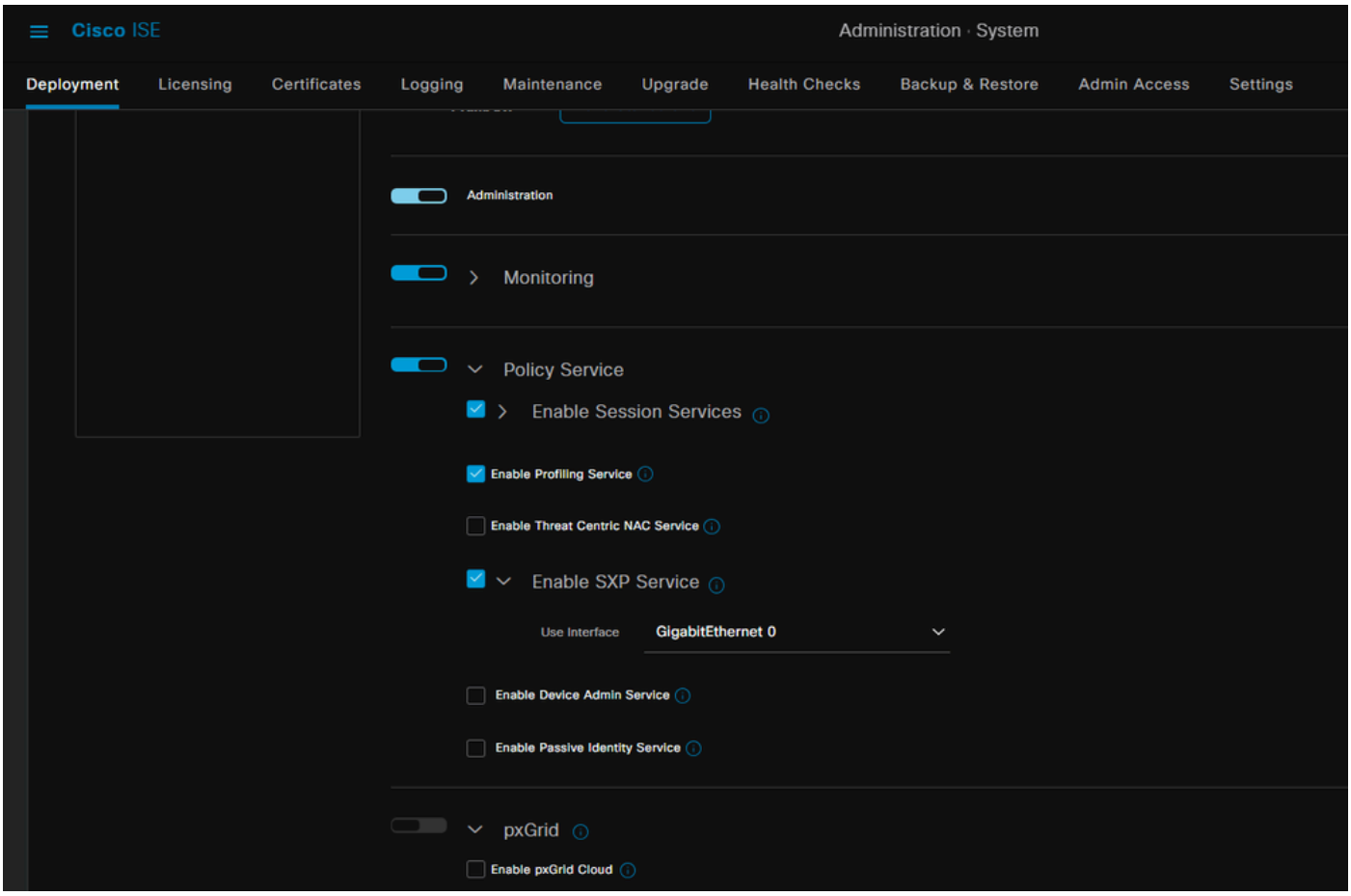
Configurez le commutateur en tant qu'écouteur SXP pour obtenir les mappages IP-SGT d'ISE.

```
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 mode par défaut peer speaker hold-time 0 0 vrf Mgmt-vrf
```

Configuration d'ISE

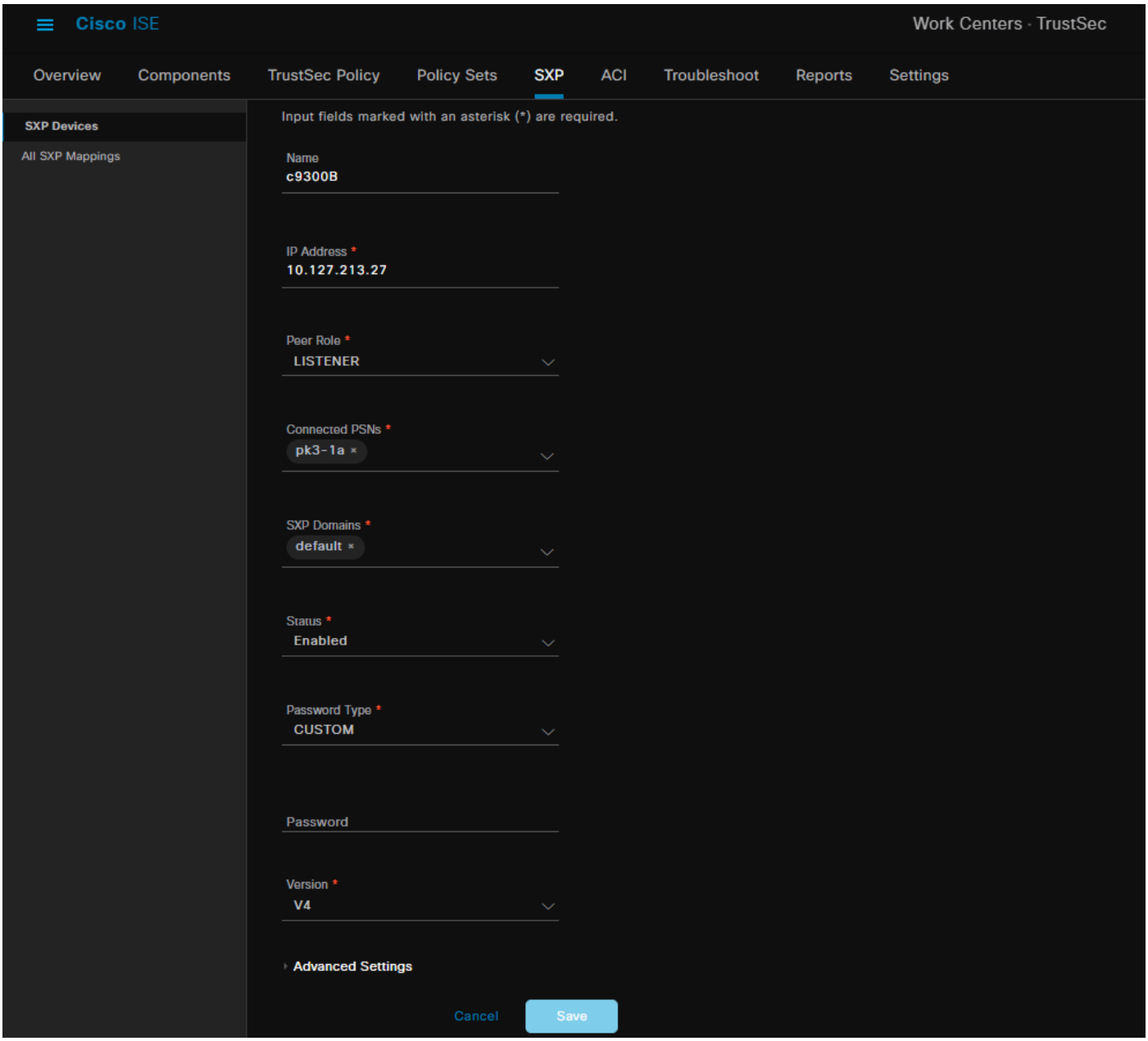
Étape 1 : activation du service SXP sur ISE

Accédez à Administration > System > Deployment > Edit the node et sous Policy Service, sélectionnez Enable SXP Service.



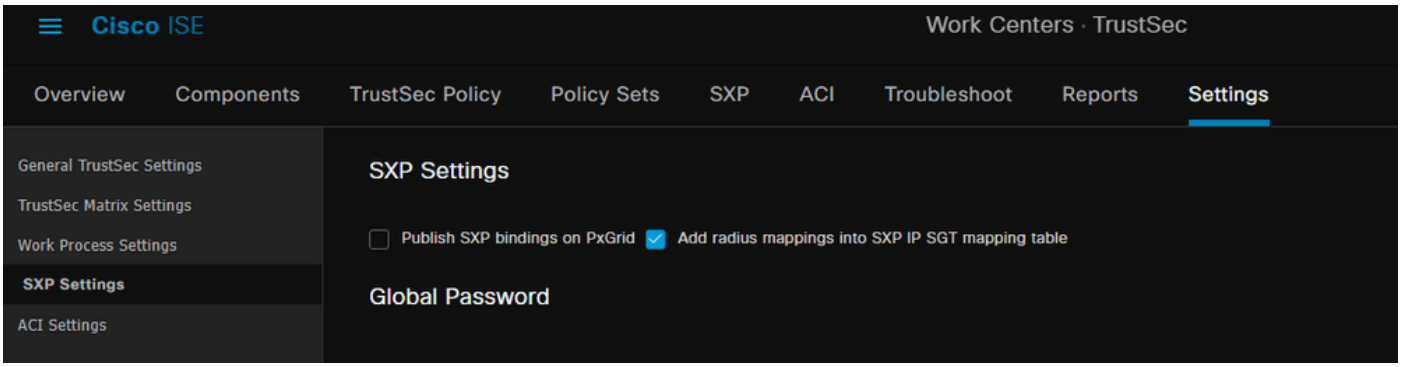
Étape 2. Ajout de périphériques SXP

Afin de configurer l'écouteur et le haut-parleur SXP pour les commutateurs correspondants, naviguez vers Work Centers > Trustsec > SXP > SXP Devices.
Ajoutez le commutateur avec le rôle homologue en tant qu'écouteur et affectez-le au domaine par défaut.



Étape 3. Paramètres SXP

Assurez-vous que l'option Add radius mappings into SXP IP SGT mapping table est cochée, afin que l'ISE apprenne les mappings IP-SGT dynamiques via les authentifications Radius.



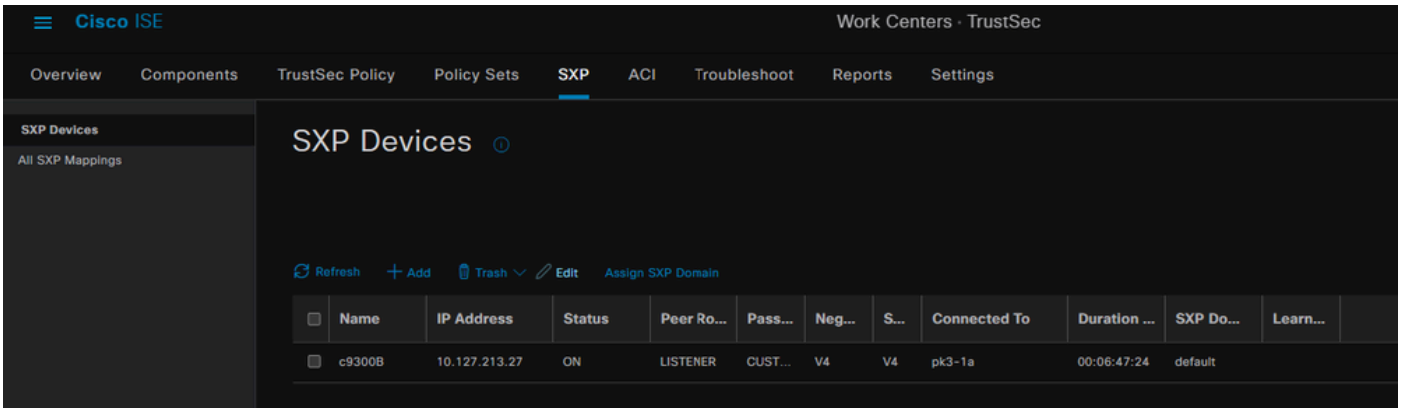
Vérifier

Étape 1. Connexion SXP sur le commutateur

```
C9300B#show cts sxp connections vrf Mgmt-vrf
SXP : Activée
Version la plus élevée prise en charge : 4
Mot de passe par défaut : Jeu
Chaîne de clés par défaut : non défini
Nom de la chaîne de clés par défaut : Sans objet
Adresse IP source par défaut : 10.127.213.27
Période d'ouverture des tentatives de connexion : 120 s
Période de rapprochement : 120 s
Le minuteur de nouvelle tentative n'est pas actif
Limite de parcours de la séquence homologue pour l'exportation : non défini
Limite de parcours de la séquence homologue pour l'importation : non défini
----------
IP homologue : 10.127.197.53
Source IP : 10.127.213.27
État du conn : On (activé)
Conn version : 4
Fonctionnalité de conn : IPv4-IPv6-Sous-réseau
Durée d'attente conn : 120 secondes
Mode local : Écouteur SXP
Inst# de connexion : 1
Fd conn TCP : 1
Mot de passe de connexion TCP : mot de passe SXP par défaut
Le minuteur de mise en attente est actif
Durée depuis le dernier changement d'état : 0:00:23:36 (jj:hr:mm:sec)


Nombre total de connexions SXP = 1

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

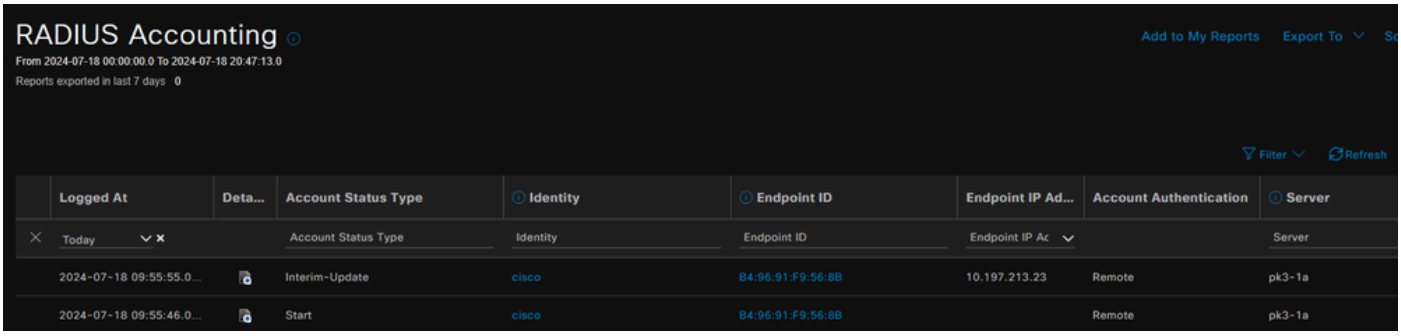
Étape 2. Vérification ISE SXP

Vérifiez que l'état SXP est ON pour le commutateur sous Work Centers > Trustsec > SXP > SXP Devices.



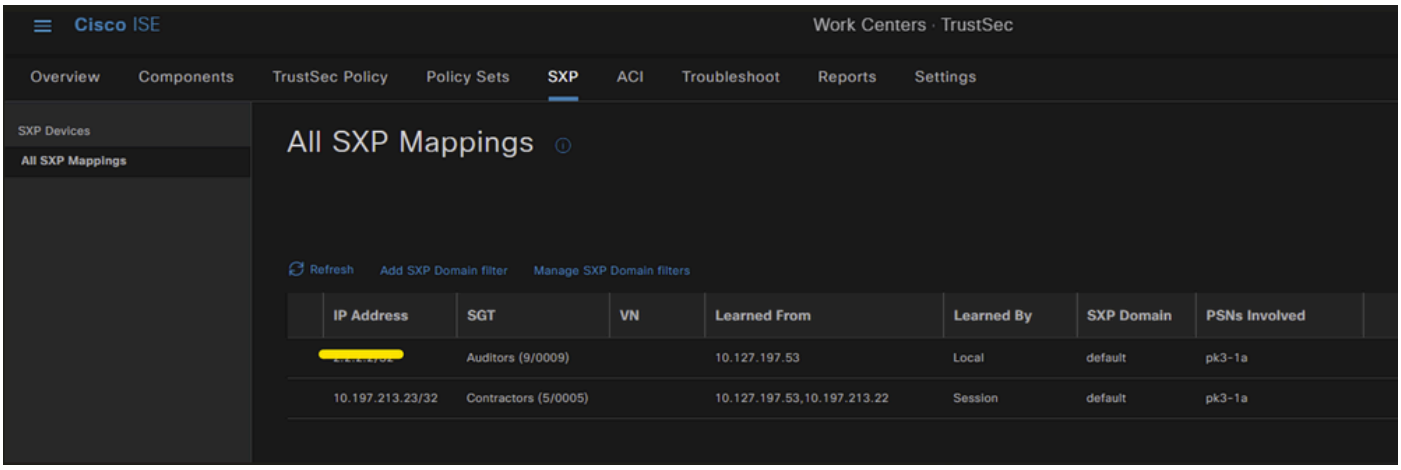
Étape 3. Comptabilisation Radius

Assurez-vous qu'ISE a reçu l'attribut RADIUS de l'adresse IP encadrée du paquet de comptabilité Radius après une authentification réussie.



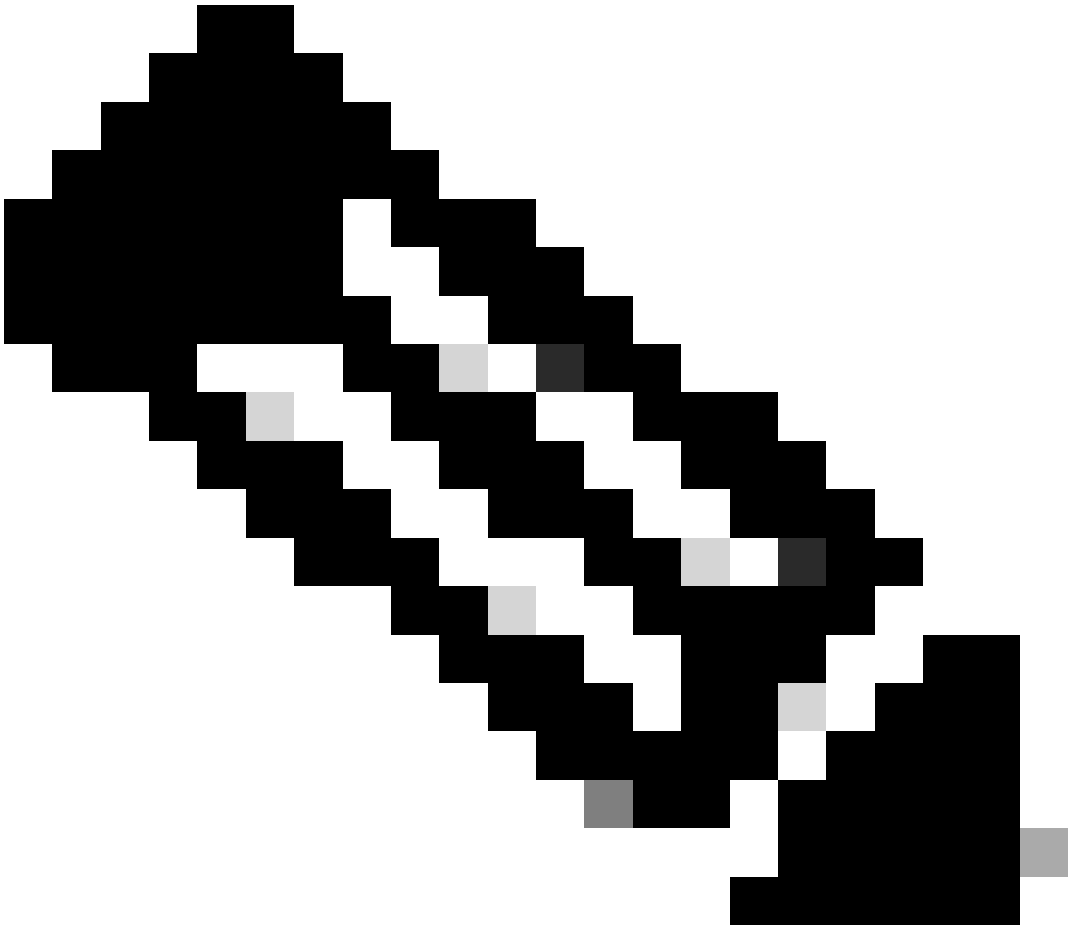
Étape 4. Mappages ISE SXP

Accédez à Workcenters > Trustsec > SXP > All SXP Mappings pour afficher les mappages IP-SGT appris dynamiquement à partir de la session Radius.



Appris par :

Local : liaisons IP-SGT attribuées de manière statique sur ISE.
Session : liaisons IP-SGT apprises dynamiquement à partir d'une session Radius.



Remarque : L'ISE peut recevoir des liaisons IP-SGT d'un autre périphérique. Ces liaisons peuvent être affichées comme Apprises par SXP sous Tous les mappages SXP.

Étape 5. Mappages SXP sur le commutateur

Le commutateur a appris les mappages IP-SGT depuis ISE via le protocole SXP.

```
C9300B#show cts sxp sgt-map vrf Mgmt-vrf brief
Mappages IP-SGT comme suit :
IPv4,SGT : <10.197.213.23, 5>
Nombre total de mappages IP-SGT : 2
```

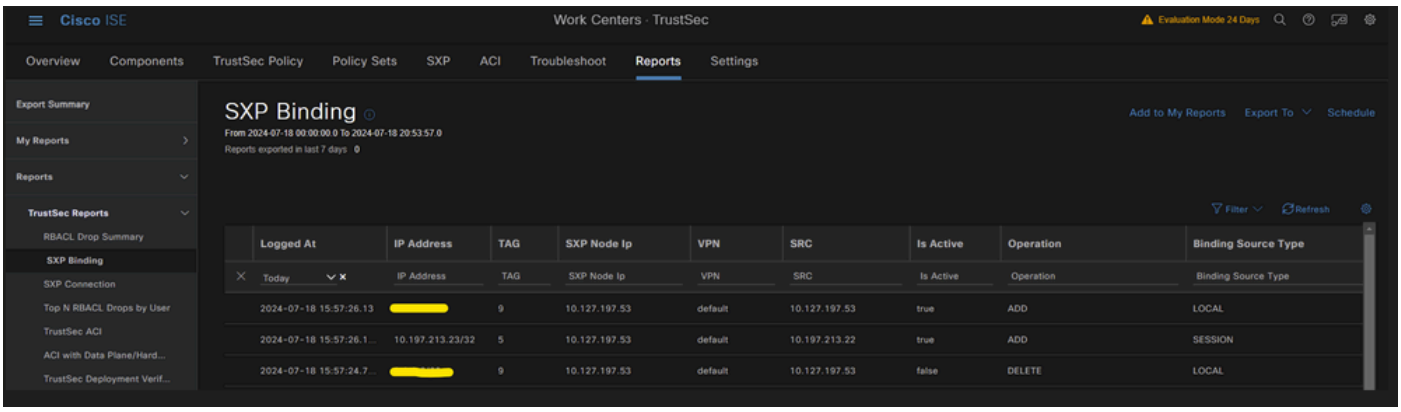
```
conn dans la liste sxp_bnd_exp_conn_list (total:0) :
C9300B#

C9300B#show cts role-based sgt-map vrf Mgmt-vrf all
Informations sur les liaisons IPv4-SGT actives

Adresse IP source SGT
=============================================
10.197.213.23.5 SXP

Résumé des liaisons actives IP-SGT
=============================================
Nombre total de liaisons SXP = 2
Nombre total de liaisons actives = 2
```

Dépannage

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Rapport ISE

ISE vous permet également de générer des rapports de liaison et de connexion SXP, comme illustré dans cette image.



Débogages sur ISE

Collectez le bundle de support ISE avec ces attributs à définir au niveau du débogage :

- sxp
- reliure sgt
- nsf
- nsf-session
- trustsec

Lorsqu'un utilisateur est authentifié à partir du serveur ISE, ISE attribue un SGT dans le paquet de réponse d'acceptation d'accès. Une fois que l'utilisateur obtient l'adresse IP, le commutateur

envoie l'adresse IP tramée dans le paquet de comptabilité Radius.

show logging application localStore/iseLocalStore.log:

```
2024-07-18 09:55:55.051 +05:30 000017592 3002 NOTICE Radius-Accounting : Mise à jour de
surveillance de la comptabilité RADIUS, ID de version de configuration=129, adresse IP du
périphérique=10.197.213.22, nom d'utilisateur=cisco, nom de périphérique réseau=pk, nom
d'utilisateur=cisco, adresse IP NAS=10.197.213.22, port NAS=50124, adresse IP
tramée=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=Authentique, Acct-00000007 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=pk3-18a
SelectedAccessService=Default Network Access, RequestLatency=6, Step=11004, Step=11017,
Step=15049, Step=510648097, Step=15008, Step=22085, NetworkDeviceGroups=IPSEC#Is
IPSEC Device#No, NetworkDeviceGroups=Location#All Locations,
NetworkDeviceGroups=Device Type#All Device Types,
CPMSessionID=16D5C50A1100500000017 C425E3C6, TotalAuthenticationLatency=6,
ClientLatency=0, Network Device Profile=Cisco, Location=Location#All Locations#All
Type=Device Types de périphériques, IPSEC=IPSEC#Est un périphérique IPSEC#Non,
```

show logging application ise-psc.log :

```
2024-07-18 09:55:55,054 DEBUG [SxpSessionNotifierThread][]
ise.sxp.sessionbinding.util.SxpBindingUtil -:::-
consignation des valeurs de session reçues de PortCpmBridge :
Type d'opération ==>ADD, sessionId ==> 16D5C50A00000017C425E3C6, sessionState ==>
ACCEPTED, inputIp ==> 10.197.213.23, inputSgTag ==> 0005-00, nasIp ==> 10.197.213.22null,
vn ==> null
```

Le noeud SXP stocke le mappage IP + SGT dans sa table H2DB et le noeud PAN ultérieur collecte le mappage IP + SGT et le reflète dans Work Centers >Trustsec > SXP > All SXP Mappings.

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 Add Session Bindings taille de lot : 1
2024-07-18 10:01:01,317 DEBUG [SxpNotificationSerializer-Thread]
cpm.sxp.engine.services.NotificationSerializerImpl:202 - tâche de traitement [add=true,
notification=RestSxpLocalBinding(tag=5, groupName=null, ipAddress=10.197.213.23/32,
```

```
nasIp=10.197.213.22, sessionId=16D5C50A00000017C425E3C6, 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'] Ajout d'une nouvelle liaison :
MasterBindingIdentity [ip=10.197.213.23/32, peerSequence=10.127.197.53,10.197.213.22,
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 - Ajout de 1 liaison(s)
2024-07-18 10:01:01,344 DEBUG [SxpNotificationSerializer-Thread]
cisco.cpm.sxp.engine.MasterDbListener:251 - Envoi de la tâche au gestionnaire H2 pour l'ajout
de liaisons, nombre de liaisons : 1
2024-07-18 10:01:01,344 DEBUG [H2_HANDLER] cisco.cpm.sxp.engine.MasterDbListener:256 -
MasterDbListener Processing onAdded - bindingsCount : 1
```

Le noeud SXP met à jour le commutateur homologue avec les dernières liaisons IP-SGT.

```
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 vers
[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 RÉUSSI vers
[ISE:10.127.197.53][10.127.197.53:64999/10.127.213.27:31025][O|Sv4]
```

Débogages sur le commutateur

Activez ces débogages sur le commutateur pour dépanner les connexions et les mises à jour SXP.

debug cts sxp conn

debug cts sxp error

debug cts sxp mdb

debug cts sxp message

Le commutateur a reçu les mappages SGT-IP du haut-parleur ISE SXP.

Cochez la case Show logging pour afficher ces journaux :

```
18 juil 04:23:04.324: CTS-SXP-MSG:sxp_recv_update_v4 <1> peer ip: 10.127.197.53
18 juil 04:23:04.324: CTS-SXP-MDB:IMU Ajouter une liaison:- <conn_index = 1> de l'homologue
10.127.197.53
18 juil 04:23:04.324: CTS-SXP-MDB : mdb_send_msg <IMU_ADD_IPSGT_DEVID>

18 juil 04:23:04.324: CTS-SXP-INTNL : mdb_send_msg mdb_process_add_ipsgt_devid Début
18 juil 04:23:04.324: CTS-SXP-MDB:sxp_mdb_inform_rbm ID table:0x1 sense:1 sgt:5
peer:10.127.197.53
18 juil 04:23:04.324: CTS-SXP-MDB:SXP MDB: Entrée ajoutée ip 10.197.213.23 sgt 0x0005
18 juil 04:23:04.324: CTS-SXP-INTNL : mdb_send_msg mdb_process_add_ipsgt_devid terminé
```

Informations connexes

- Guide de l'administrateur de Cisco Identity Services Engine, version 3.1
- Guide de configuration de Cisco TrustSec, Cisco IOS XE Bengaluru 17.6.x (commutateurs Catalyst 9300)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d’un service mondial permettant à nos utilisateurs d’obtenir le contenu d’assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.