# Comprendre les journaux de mise à jour ISE SXP et les journaux de débogage Catalyst

## Table des matières

Introduction
Informations générales
Conditions préalables
Exigences
Composants utilisés
Configuration
Diagramme du réseau
Flux de trafic
Configurer le commutateur
Configuration d'ISE
Étape 1. Activer le 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. Gestion des comptes 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.

## Informations générales

SXP est le protocole d'échange SGT (Security Group Tag) utilisé par TrustSec pour propager les mappages IP vers SGT vers les 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 servir de haut-parleur et l'autre de récepteur.

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.

## 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.

## 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. Activer le service SXP sur ISE

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

≡ Cisco	ISE					Admi	inistration - System		
Deployment	Licensing	Certificates	Logging	Maintenance	Upgrade	Health Checks	Backup & Restore	Admin Access	Settings
			Adı	ministration					
			<b></b> >	Monitoring					
			<b></b> ~	Policy Service					
				> Enable Sea	ssion Service	es 🕦			
				Enable Profiling Service	<b>:e</b> ()				
				Enable Threat Centric	NAC Service 🕦				
				✓ Enable SXI	PService 🕦				
				Use Interface	GigabitEth	ernet 0	~		
				Enable Device Admin	Service 🕕				
				Enable Passive Identi	ty Service 🕕				
				pxGrid 💿					
				Enable pxGrid Cloud	<b>(</b> )				

Étape 2. Ajout de périphériques SXP

Afin de configurer l'écouteur et le haut-parleur SXP pour les commutateurs correspondants, naviguez vers Workcenters > Trustsec > SXP > SXP Devices.

Ajoutez le commutateur avec le rôle d'homologue comme écouteur et affectez-le au domaine par défaut.

≡ Cisco	ISE							Work Centers - Tr	ustSec
Overview	Components	TrustSec Policy	Policy Sets	SXP	ACI	Troubleshoot	Reports	Settings	
SXP Devices		Input fields marked	d with an asterisk (	*) are requi	red.				
All SXP Mappings		Name c9300B							
		IP Address * 10.127.213.27							
		Peer Role * LISTENER							
		Connected PSNs * pk3-1a ×							
		SXP Domains * default ×							
		Status * Enabled							
		Password Type * CUSTOM							
		Password							
		Version * V4							
		Advanced Setting	js						
				Save					

## 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.

≡ Cisco	E Cisco ISE Work Centers · TrustSec										
Overview	Components	TrustSec Policy	Policy Sets	SXP	ACI	Troubleshoot	Reports	Settings			
General TrustSec Settings SXP Settings											
Work Process Settin	ngs	Publish SXP bindi	ngs on PxGrid 🔽 A	dd radius ma	appings into	) SXP IP SGT mapping ta	able				
SXP Settings		Global Passwo	rd								
ACI Settings											

## Vérifier

Étape 1. Connexion SXP sur le commutateur

C9300B#show cts sxp connections vrf Mgmt-vrf SXP : activé Version la plus élevée prise en charge : 4 Mot de passe par défaut : défini Chaîne de clés par défaut : non définie Nom de la chaîne de clés par défaut : Sans objet Adresse IP source par défaut : 10.127.213.27 Période d'ouverture de nouvelle tentative de connexion : 120 secondes Période de rapprochement : 120 secondes Le minuteur de nouvelle tentative n'est pas actif Limite de parcours de la séquence homologue pour l'exportation : non définie Limite de parcours de la séquence homologue pour l'importation : non définie IP homologue : 10.127.197.53 IP source : 10.127.213.27 État conn : Activé Version de conversion : 4 Fonctionnalité de connexion : IPv4-IPv6-Subnet Durée d'attente de connexion : 120 secondes Mode local : écouteur SXP Inst. de connexion : 1 Fd conn TCP: 1 TCP conn password : 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 Workcenters > Trustsec > SXP > SXP Devices.

						Wor	k Cen	ters · TrustSec				
Overview Components Tru	stSec Policy	Policy Sets	SXP AC	Troub	leshoot	Repo	rts	Settings				
SXP Devices	SXP Devi	ces o										
All SXP Mappings												
£			Edit Assign									
	Name	IP Address	Status	Peer Ro	Pass	Neg	S	Connected To	Duration	SXP Do	Learn	
_	C9300B	10.127.213.27	ON	LISTENER	CUST	V4	V4	pk3-1a	00:06:47:24	default		

### Étape 3. Gestion des comptes RADIUS

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

RA From 2 Report	DIUS Accou 1024-07-18 00:00 00 0 To 2024-07- s exported in last 7 days 0	nting 18 20:47:13.	0				Add to My Reports	Export To ∨ So Filter ∨ ØRefresh
	Logged At	Deta	Account Status Type	Identity	Endpoint ID	Endpoint IP Ad	Account Authentication	O Server
×	Today 🗸 🗙		Account Status Type	Identity	Endpoint ID	Endpoint IP Ac 🗸		Server
	2024-07-18 09:55:55.0	G	Interim-Update			10.197.213.23	Remote	pk3-1a
	2024-07-18 09:55:46.0	G	Start	cisco	B4:96:91:F9:56:8B		Remote	pk3-1a

## 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.

≡ Cisco	o ISE					Work Centers	TrustSec			
Overview	Components	TrustSec Policy	Policy Sets SXP	ACI	Troubleshoot	Reports Se	ttings			
SXP Devices All SXP Mapping	15	All SXP Ma	appings ()							
		IP Address	SGT	VN	Learned Fron	n	Learned By	SXP Domain	PSNs Involved	
		2.2.2/32	Auditors (9/0009)		10.127.197.53		Local	default	pk3-1a	
		10.197.213.23/3	Contractors (5/0005)		10.127.197.53,	10.197.213.22	Session	default	pk3-1a	

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 ID de noeud SXP(généré) : 0x03030303(3.3.3.3) Mappages IP-SGT comme suit : IPv4, SGT: <2.2.2.2, 9> 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
2.2.2.9 SXP 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 permet également de générer des rapports de liaison et de connexion SXP, comme illustré dans cette image.

					Work Cente	ers · TrustS	Sec			🔺 Eva	uation Mode 24 Days Q 🕜 🗔 🚭
TrustS	ec Policy	Policy Se	ts SXP	ACI Trou	ubleshoot	Reports	Settings				
SX	P Binc	ding 💿									
From 2 Report	2024-07-18 00.00 ts exported in last	100.0 To 2024-07	-18 20:53:57.0								
	Logged At		IP Address	TAG	SXP Node I	p	VPN	SRC	Is Active	Operation	Binding Source Type
			10.444		61/0 No. 1-		10741				Distant and Date
	Today	××	IP Address	TAG	SXP Node Ip		VPN	SRG	Is Active	Operation	Binding Source Type
	2024-07-18						default				LOCAL
	2024-07-18						default			ADD	SESSION
	2024-07-18						default		false	DELETE	LOCAL
	TrustS From: Report	Logged At           X         Today           2024-07-18         2024-07-18	Logged At         ×           2024-07-18         52/2024-07           2024-07-18         15/57.26.13           2024-07-18         15/57.26.13           2024-07-18         15/57.26.13           2024-07-18         15/57.26.13           2024-07-18         15/57.26.13	Compared and any of the second and any of the second and any of the second any	Cogged At         IP Address         TAG           2024-07-18         15:57:26.1         10:17:21:22/32         5           2024-07-18         15:57:26.1         10:17:21:22/32         5	Cogged At         IP Address         TAG         SXP Node Ip           2024-07-18 15:57:26.1.         10:17:21323/20         5         10:127:197.5	Korpets         Policy Sets         SXP         ACI         Troubleshoot         Reports           SXP Binding         •	Work Centers · TrustSec         TrustSec Policy       Policy Sets       SXP       ACI       Troubleshoot       Reports       Settings         SXEP Binding From 2024-07-18 000000 to 10 2024-07-18 20 53 57.0 Reports exported in last 7 days       P Address       TAG       SXP Node 1p       VPN                 Logged At               IP Address       TAG       SXP Node 1p       VPN                2024-07-18 15:57:26.13              2.2.2.2/32              9               10.127.107.53        default                2024-07-18 15:57:26.1               10.197.213.23/32               9               10.127.107.53               default	Work Centers - TrustSec           TrustSec Policy         Policy Sets         SXP         ACI         Troubleshoot         Reports         Settings           SXEP Binding Prom 2024-07-18 000000 10 2024-07-18 02 000000 10 2024-07-18 02 000000 10 2024-07-18 02 000000 10 2024-07-18 02 000000 10 2024-07-18 02 000000 10 2024-07-18 02 000000 10 2024-07-18 02 0000000 10 2024-07-18 02 0000000 10 2024-07-18 02 000000 10 2024-07-18 02 000000 10 2024-07-18 02 000000 10 2024-07-18 02 000000 10 2024-07-18 02 000000 10 2024-07-18 02 000000 10 2024-07-18 02 000000 10 2024-07-18 02 000000 10 2024-07-18 02 00000000 10 2024-07-18 02 0000000 10 2024-07-18 02 000000 10 2024-07-18 02 000000 10 2024-07-18 02 000000 10 2024-07-18 02 000000 10 2024-07-18 02 000000 10 2024-07-18 02 000000 10 2024-07-18 02 000000 10 2024-07-18 02 0000000000000000000000000000000000	Work Centers · TrustSec         TrustSec Policy       Policy Sets       SXP       ACI       Troubleshoot       Reports       Settings         SXEP Binding Prom 2024-07-18 0000000 10 20224-07-18 20 53 57.0 Reports exported in last 7 days       P Address       TAG       SXP Node Ip       VPN       SRC       Is Active	Image: Nork Centers - TrustSec         Mork Ce

### 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, ConfigVersionId=129, Device IP Address=10.197.213.22, UserName=cisco, NetworkDeviceName=pk, User-Name=cisco, NAS-IP-IP Adresse = 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 6-8B, 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=16D5C50A00000017 C425E3C6, cisco-av-pair=method=dot1x, cisco-av-pair=cts : security-group-tag=0005-00, AcsSessionID=pk3-1a/510648097/28, SelectedAccessService=Default Network Access, RequestLatency=6, Step=11004, Step=11017, Step=15049, Step=15008, Step=22085, Step=11005, NetworkDeviceGroups=IPSEC#Is IPSEC Device#No, NetworkDeviceGroups=Location#All Locations, NetworkDeviceGroups=Type#All Device Types, CPMSessionID=16D5C50A00000017C425E3C6, TotalAuthenticationLatency=6. ClientLatency=0, Network Device 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 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 ce mappage SGT IP et le reflète dans tous les mappages SXP dans l'interface utilisateur graphique ISE (Workcenters ->Trustsec -> SXP - >Tous les mappages SXP).

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.NotificationSerializerImpI: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=10.127.197.53,10.197.211 3.22, 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 SXP « ISE ».

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> depuis 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 tableid: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 Done

Informations connexes

ISE 3.1 Guide d'administration Segmentation

Guide de configuration de Catalyst - Présentation de Trustsec

#### 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.