

ISE SXP更新ログとCatalystデバッグログについて

内容

[はじめに](#)

[背景説明](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[コンフィギュレーション](#)

[ネットワーク図](#)

[Traffic flow](#)

[スイッチの設定](#)

[ISE の設定](#)

[ステップ 1 : ISEでSXPサービスを有効にする](#)

[ステップ 2 : SXPデバイスの追加](#)

[ステップ 3 : SXPの設定](#)

[確認](#)

[ステップ 1 : スイッチ上のSXP接続](#)

[ステップ 2 : ISE SXPの検証](#)

[ステップ 3 : RADIUS アカウンティング](#)

[ステップ 4 : ISE SXPマッピング](#)

[ステップ 5 : スイッチでのSXPマッピング](#)

[トラブルシュート](#)

[ISEレポート](#)

[ISE でのデバッグ](#)

[スイッチのデバッグ](#)

[関連情報](#)

はじめに

このドキュメントでは、ISEとCatalyst 9300スイッチ間のSecurity Group Exchange Protocol(SXP)接続を設定し、理解する方法について説明します。

背景説明

SXPは、TrustSecがTrustSecデバイスにIPからSGTへのマッピングを伝播するために使用するSGT (セキュリティグループタグ) 交換プロトコルです。

SXPは、SGTインラインタギングをサポートしないサードパーティ製デバイスやシスコのレガシ

ーデバイスなどのネットワークでTrustSec機能を使用できるようにするために開発されました。

SXPはピアリングプロトコルです。一方のデバイスはスピーカーとして機能し、もう一方はリスナーとして機能できます。

SXPスピーカーはIP-SGTバインディングを送信し、リスナーはこれらのバインディングを収集します。

SXP接続では、基盤となるトランスポートプロトコルとしてTCPポート64999を使用し、メッセージの整合性と信頼性を確保するためにMD5を使用します。

前提条件

要件

SXPプロトコル(SXP)およびIdentity Services Engine(ISE)の設定に関する知識があることが推奨されます。

使用するコンポーネント

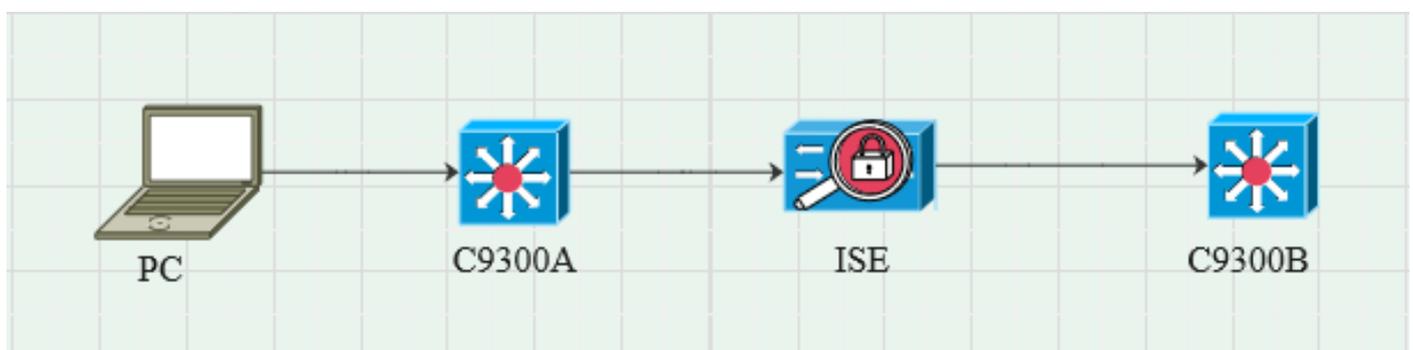
このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- ソフトウェアCisco IOS® XE 17.6.5以降が稼働するCisco Catalyst 9300スイッチ
Cisco ISE リリース 3.1 以降

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな(デフォルト)設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

コンフィギュレーション

ネットワーク図



Traffic flow

PCがC9300Aで認証され、ISEがポリシーセットを使用してSGTを動的に割り当てます。

認証に合格すると、ポリシーで設定されたFramed-IPアドレスのRADIUS属性とSGTに等しいIPを持つバインディングが作成されます。

バインディングは、デフォルトドメインの下の「All SXP bindings」に表示されます。

C9300Bは、SXPプロトコルを介してISEからSXPマッピング情報を受信します。

スイッチの設定

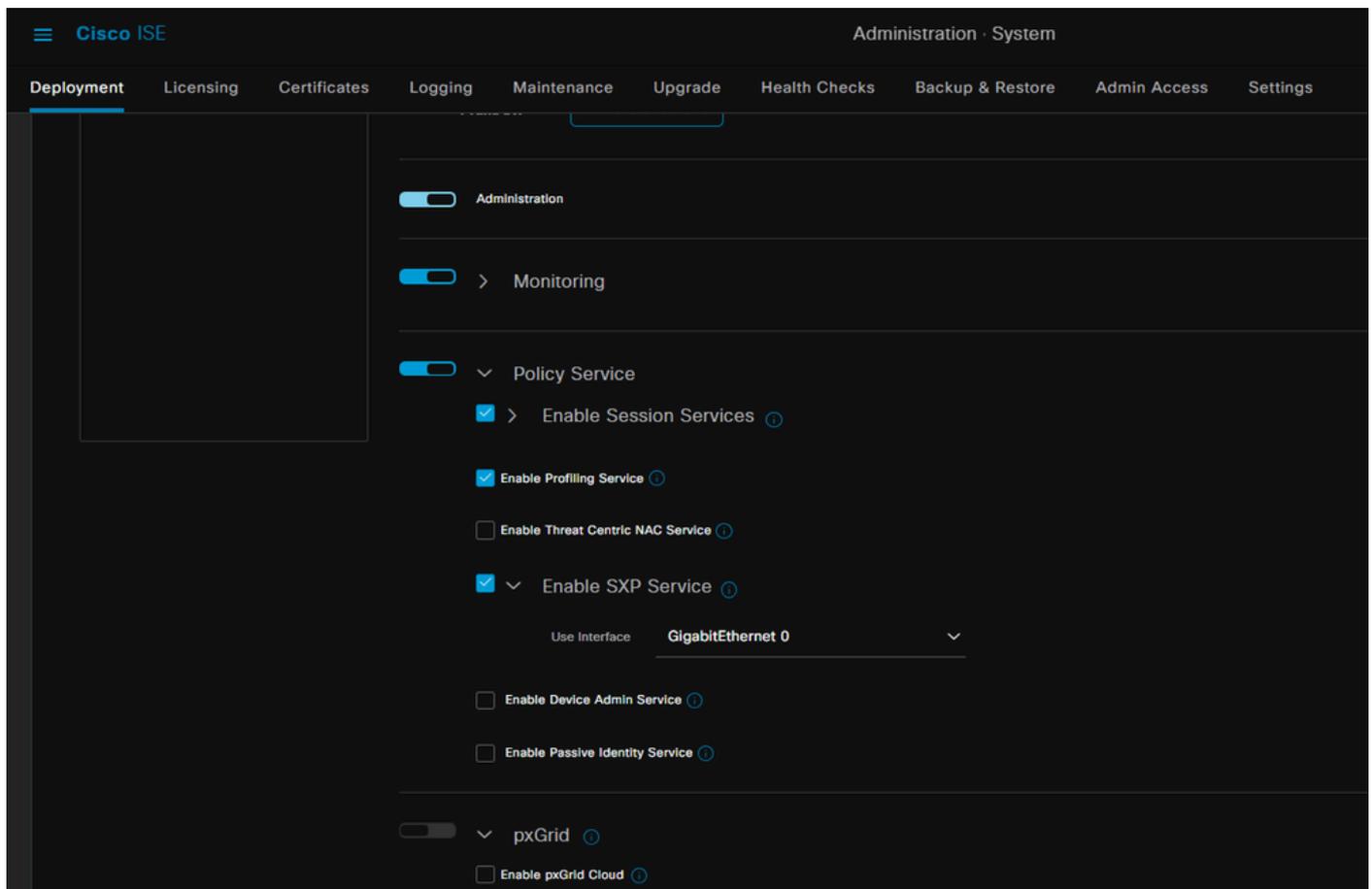
スイッチをSXPリスナーとして設定し、ISEからIP-SGTマッピングを取得します。

```
cts sxpの有効化
cts sxpデフォルトパスワードcisco
cts sxp default source-ip 10.127.213.27
cts sxp connection peer 10.127.197.53 password default mode peer hold-time 0 0 vrf Mgmt-vrf
```

ISE の設定

ステップ 1 : ISEでSXPサービスを有効にする

Administration > System > Deployment > Editの順に移動し、Policy Serviceの下でEnable SXP Serviceを選択します。



The screenshot shows the Cisco ISE Administration console interface. The top navigation bar includes 'Administration · System' and various menu items like 'Deployment', 'Licensing', 'Certificates', 'Logging', 'Maintenance', 'Upgrade', 'Health Checks', 'Backup & Restore', 'Admin Access', and 'Settings'. The 'Deployment' menu is selected. On the left, a sidebar contains a search bar and a list of categories: Administration, Monitoring, Policy Service, and pxGrid. The 'Policy Service' category is expanded, showing several sub-services. The 'Enable SXP Service' checkbox is checked. Below this, the 'Use Interface' is set to 'GigabitEthernet 0'. Other services like 'Enable Session Services', 'Enable Profiling Service', 'Enable Threat Centric NAC Service', 'Enable Device Admin Service', and 'Enable Passive Identity Service' are also visible, with their respective checkboxes.

ステップ 2 : SXPデバイスの追加

対応するスイッチのSXPリスナーおよびスピーカを設定するには、Workcenters > Trustsec > SXP > SXP Devicesの順に移動します。
ピアロールがListenerのスイッチを追加し、デフォルトドメインを割り当てます。

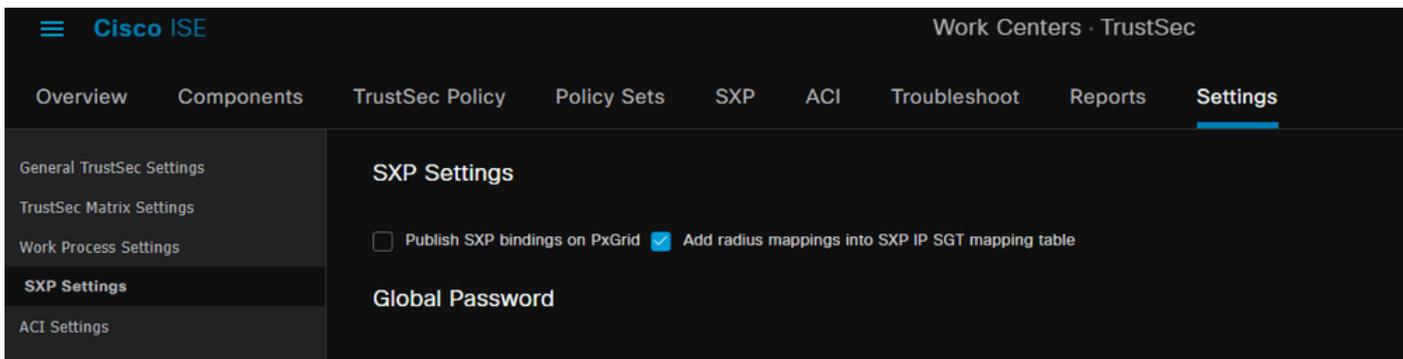
The screenshot shows the Cisco ISE configuration interface for SXP. The breadcrumb path is Work Centers > TrustSec > SXP > SXP Devices. The configuration page for device 'c9300B' is displayed. The left sidebar shows 'SXP Devices' and 'All SXP Mappings'. The main content area contains the following fields:

- Name: c9300B
- IP Address *: 10.127.213.27
- Peer Role *: LISTENER
- Connected PSNs *: pk3-1a *
- SXP Domains *: default *
- Status *: Enabled
- Password Type *: CUSTOM
- Password: (empty)
- Version *: V4

At the bottom, there is an 'Advanced Settings' section and 'Cancel' and 'Save' buttons.

ステップ 3 : SXPの設定

ISEがRadius認証を通じてダイナミックIP-SGTマッピングを学習するように、Add radius mappings into SXP IP SGT mapping tableにチェックマークが入っていることを確認します。



確認

ステップ 1 : スイッチ上のSXP接続

```
C9300B#show cts sxp connections vrf Mgmt-vrf
```

SXP : 有効

サポートされる最新バージョン : 4

デフォルトパスワード : 設定

デフォルトのキーチェーン : 未設定

デフォルトのキーチェーン名 : 該当なし

デフォルトの送信元IP:10.127.213.27

接続再試行オープン時間 : 120秒

調整期間 : 120秒

再試行オープンタイマーが実行されていません

エクスポートのピアシーケンスのトラバース制限 : 未設定

インポートのピアシーケンスのトラバース制限 : 未設定

0.-----

ピアIP:10.127.197.53

送信元IP:10.127.213.27

Connステータス : オン

Connバージョン : 4

接続機能 : IPv4-IPv6-Subnet

Conn保留時間 : 120秒

ローカルモード : SXPリスナー

接続インスタンス#:1

TCP conn fd:1

TCP conn password : デフォルトのSXPパスワード

ホールドタイマーが実行中

前回の状態変更からの継続時間 : 0:00:23:36 (dd:hr:mm:sec)

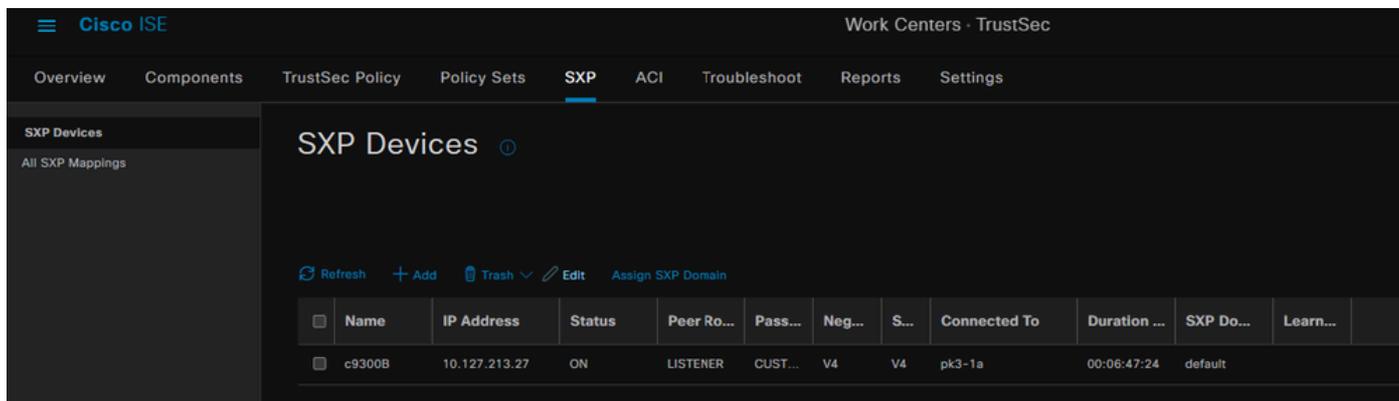
SXP接続の総数= 1

0x7F128DF555E0 VRF:Mgmt-vrf、fd:1、ピアip:10.127.197.53

cdbp:0x7F128DF555E0 Mgmt-vrf <10.127.197.53、 10.127.213.27> tableid:0x1

ステップ 2 : ISE SXPの検証

Workcenters > Trustsec > SXP > SXP Devicesで、スイッチのSXPステータスがONになっていることを確認します。

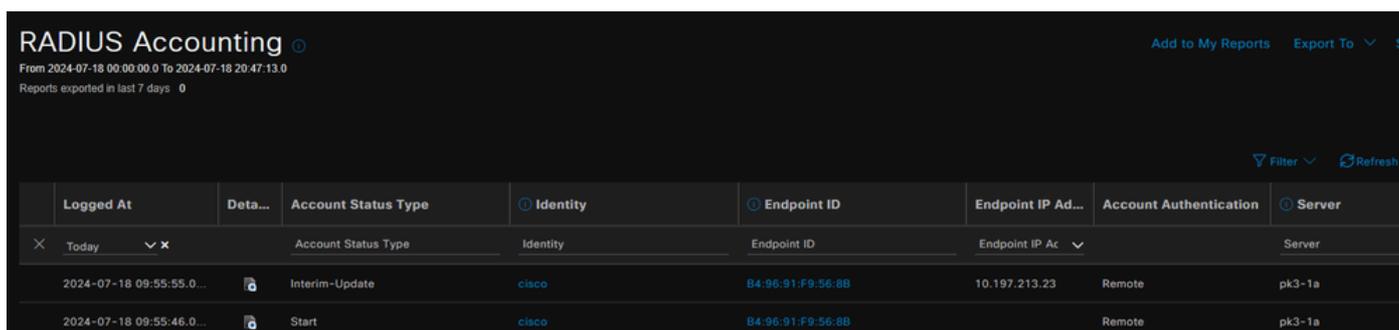


The screenshot shows the Cisco ISE interface for SXP Devices. The navigation menu includes Overview, Components, TrustSec Policy, Policy Sets, SXP (selected), ACI, Troubleshoot, Reports, and Settings. The main content area is titled 'SXP Devices' and contains a table with the following data:

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	

ステップ 3 : RADIUS アカウンティング

ISEが、認証に成功した後にRADIUSアカウンティングパケットからFramed-IPアドレスRADIUS属性を受信したことを確認します。

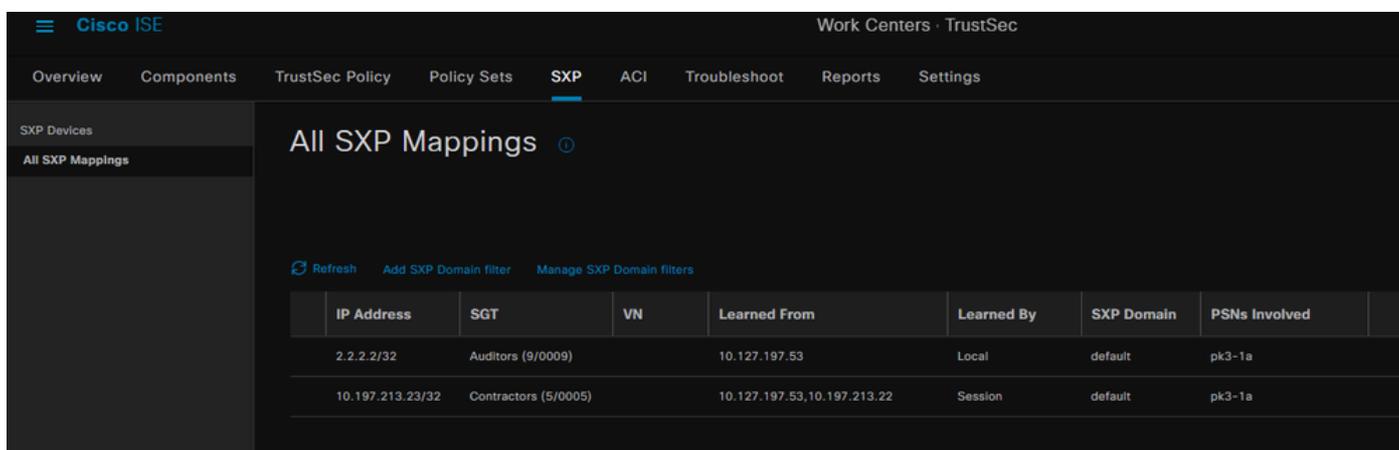


The screenshot shows the Cisco ISE interface for RADIUS Accounting. The page title is 'RADIUS Accounting' and it displays a table of accounting records for the period from 2024-07-18 00:00:00.0 to 2024-07-18 20:47:13.0. The table has the following data:

Logged At	Account Status Type	Identity	Endpoint ID	Endpoint IP Ad...	Account Authentication	Server
2024-07-18 09:55:55.0...	Interim-Update	cisco	B4:96:91:F9:56:8B	10.197.213.23	Remote	pk3-1a
2024-07-18 09:55:46.0...	Start	cisco	B4:96:91:F9:56:8B		Remote	pk3-1a

ステップ 4 : ISE SXPマッピング

Radiusセッションから動的に学習したIP-SGTマッピングを表示するには、Workcenters > Trustsec > SXP > All SXP Mappingsの順に移動します。



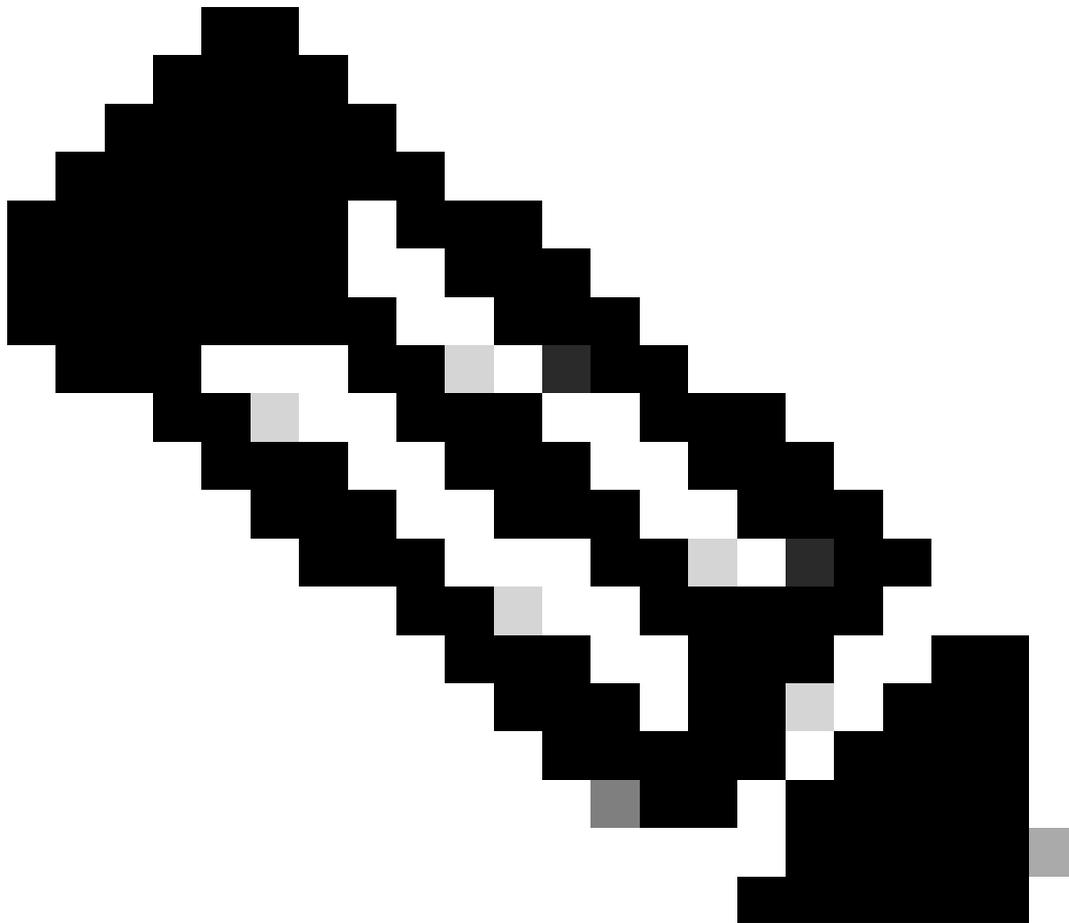
The screenshot shows the Cisco ISE interface for All SXP Mappings. The navigation menu includes Overview, Components, TrustSec Policy, Policy Sets, SXP (selected), ACI, Troubleshoot, Reports, and Settings. The main content area is titled 'All SXP Mappings' and contains a table with the following data:

IP Address	SGT	VN	Learned From	Learned By	SXP Domain	PSNs Involved
2.2.2.2/32	Auditors (9/0009)		10.127.197.53	Local	default	pk3-1a
10.197.213.23/32	Contractors (5/0005)		10.127.197.53,10.197.213.22	Session	default	pk3-1a

学習者

ローカル : ISEで静的に割り当てられたIP-SGTバインディング。

Session:Radiusセッションから動的に学習されたIP-SGTバインディング。



注:ISEには、別のデバイスからIP-SGTバインディングを受信する機能があります。これらのバインディングは、「All SXP Mappings」の下の「Learned by SXP」として表示できます。

ステップ 5 : スイッチでのSXPマッピング

スイッチは、SXPプロトコルを介してISEからIP-SGTマッピングを学習しました。

```
C9300B#show cts sxp sgt-map vrf Mgmt-vrf brief
SXPノードID (生成済み) :0x03030303(3.3.3.3)
IP-SGTマッピングは次のとおりです。
IPv4,SGT: <2.2.2.2 , 9>
IPv4,SGT: <10.197.213.23 , 5>
```

IP-SGTマッピングの総数 : 2
sxp_bnd_exp_conn_listのconn (合計 : 0) :
C9300B番号

C9300B#show cts role-based sgt-map vrf Mgmt-vrf all
アクティブなIPv4-SGTバインディング情報

IPアドレスSGTソース

=====
2.2.2.2 9 SXP
10.197.213.23 5 SXP

IP-SGTアクティブバインディングの概要

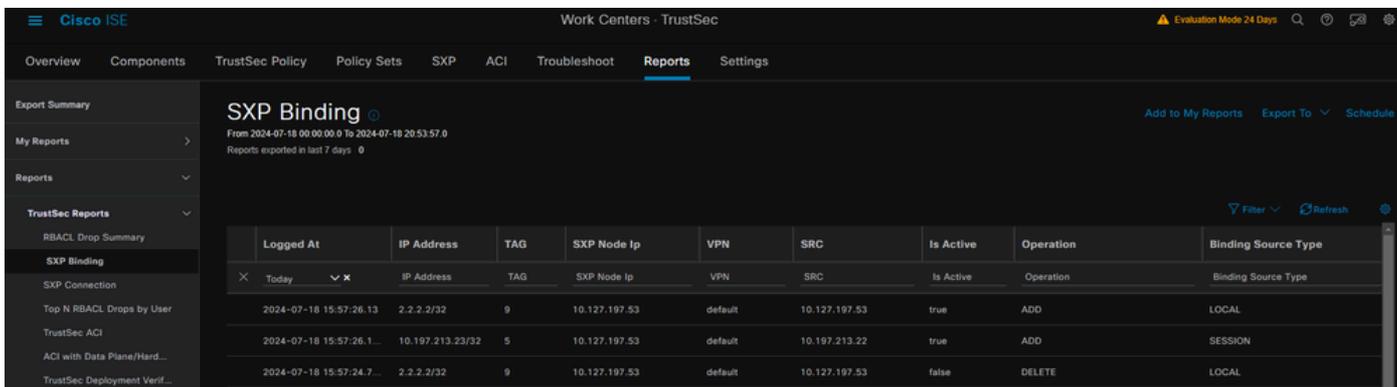
=====
SXPバインディングの総数= 2
アクティブなバインディングの総数= 2

トラブルシュート

このセクションでは、設定のトラブルシューティングに役立つ情報を紹介します。

ISEレポート

ISE では、SXP バインディングや接続レポートを生成することもできます (次の図を参照) 。



The screenshot shows the Cisco ISE interface with the 'Reports' tab selected. The main content area displays 'SXP Binding' reports. A table lists the binding details for three entries.

Logged At	IP Address	TAG	SXP Node Ip	VPN	SRC	Is Active	Operation	Binding Source Type
2024-07-18 15:57:26.13	2.2.2.2/32	9	10.127.197.53	default	10.127.197.53	true	ADD	LOCAL
2024-07-18 15:57:26.1...	10.197.213.23/32	5	10.127.197.53	default	10.197.213.22	true	ADD	SESSION
2024-07-18 15:57:24.7...	2.2.2.2/32	9	10.127.197.53	default	10.127.197.53	false	DELETE	LOCAL

ISE でのデバッグ

次の属性を持つISEサポートバンドルを収集し、デバッグレベルに設定します。

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

ユーザがISEサーバから認証されると、ISEはAccess Accept応答パケットにSGTを割り当てます

。ユーザがIPアドレスを取得すると、スイッチはRadius Accounting Packetでフレーム化されたIPアドレスを送信します。

show logging application localStore/iseLocalStore.logの出力を示します。

```
2024-07-18 09:55:55.051 +05:30 000017592 3002お知らせRadius-Accounting: RADIUS Accounting watchdog update, ConfigVersionId=129, Device IP Address=10.197.213.22, UserName=cisco, NetworkDevice=Name pk、 User-Name=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、 t-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 3-1a/510648097/28、 SelectedAccessService=既定のネットワークアクセス、 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=Device Type#All Device Types、 CPMSessionID=16D5C50A00000017C425E3C6、 TotalAuthenLatency=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 -:::-
prrtCpmBridgeから受信したセッション値をロギングします。
操作タイプ==>ADD、 sessionId ==> 16D5C50A00000017C425E3C6、 sessionState ==>
ACCEPTED、 inputIp ==> 10.197.213.23、 inputSgTag ==> 0005-00、 nasIp ==>
10.197.213.22null、 vn ==> null
```

SXPノードはIP + SGTマッピングをH2DBテーブルに保存し、後でPANノードがこのIP SGTマッピングを収集して、ISE GUIのすべてのSXPマッピングに反映します (Workcenters ->Trustsec -> SXP->すべてのSXPマッピング)。

show logging application sxp_appserver/sxp.logの出力を示します。

```
2024-07-18 10:01:01,312 INFO [sxp-service-http-96441] cisco.ise.sxp.rest.SxpGlueRestAPI:147 -
SXP-PEERFセッションバイディングの追加バッチサイズ : 1
2024-07-18 10:01:01,317 DEBUG [SxpNotificationSerializer-Thread]
cpm.sxp.engine.services.NotificationSerializerImpl:202 - タスクの処理[add=true,
```

```
notification=RestSxpLocalBinding(tag=5, groupName=null, ipAddress=10.197.213.23/32,
nasIp=10.197.213.22, Id=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']新しいバインドの追加 :
```

```
MasterBindingIdentity [ip=10.197.213.23/32, peerSequence=10.127.197.53,10.197.2 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 - 1つのバインディングの追加
```

```
2024-07-18 10:01:01,344 DEBUG [SxpNotificationSerializer-Thread]
```

```
cisco.cpm.sxp.engine.MasterDbListener:251 - バインディングを追加するためにH2ハンドラにタ
スクを送信しています。バインディング数 : 1
```

```
2024-07-18 10:01:01,344 DEBUG [H2_HANDLER] cisco.cpm.sxp.engine.MasterDbListener:256 -
MasterDbListener Processing onAdded - bindingsCount: 1
```

SXPノードは、最新のIP-SGTバインディングでピアスイッチを更新します。

```
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を
```

```
[[SE: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
```

```
[[SE:10.127.197.53][10.127.197.53:64999/10.127.213.27:31025]][O|Sv4]
```

スイッチのデバッグ

SXPの接続とアップデートのトラブルシューティングを行うには、スイッチで次のデバッグを有効にします。

```
debug cts sxp conn
```

```
debug cts sxpエラー
```

```
デバッグ cts sxp mdb
```

```
debug cts sxpメッセージ
```

スイッチがSXPスピーカー「ISE」からSGT-IPマッピングを受信しました。

次のログを表示するには、**Show logging**をチェックします。



```
Jul 18 04:23:04.324: CTS-SXP-MSG:xsp_rcv_update_v4 <1>ピアip: 10.127.197.53
7月18日04:23:04.324: CTS-SXP-MDB:IMU追加binding:- <conn_index = 1>ピア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:xsp_mdb_inform_rbm tableid:0x1 sense:1 sgt:5
peer:10.127.197.53
7月18日04:23:04.324: CTS-SXP-MDB:SXP MDB:エントリがip 10.197.213.23 sgt 0x0005を追加
7月18日04:23:04.324: CTS-SXP-INTNL:mdb_send_msg mdb_process_add_ipsgt_devid完了
```

関連情報

[ISE 3.1管理ガイドのセグメンテーション](#)

[CatalystコンフィギュレーションガイドTrustsecの概要](#)

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。