

Comprensión de los registros de actualización de ISE SXP junto con los registros de depuración de Catalyst

Contenido

[Introducción](#)

[Antecedentes](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configuración](#)

[Diagrama de la red](#)

[Flujo de tráfico](#)

[Configurar switch](#)

[Configuración de ISE](#)

[Paso 1. Habilitar el servicio SXP en ISE](#)

[Paso 2. Agregar dispositivos SXP](#)

[Paso 3. Configuración de SXP](#)

[Verificación](#)

[Paso 1. Conexión SXP en el switch](#)

[Paso 2. Verificación de ISE SXP](#)

[Paso 3. Contabilización RADIUS](#)

[Paso 4. Asignaciones de ISE SXP](#)

[Paso 5. Asignaciones de SXP en el switch](#)

[Troubleshoot](#)

[Informe de ISE](#)

[Depuraciones en ISE](#)

[Depuraciones en el switch](#)

[Información Relacionada](#)

Introducción

Este documento describe cómo configurar y comprender la conexión del protocolo de intercambio de grupos de seguridad (SXP) entre ISE y el switch Catalyst 9300.

Antecedentes

SXP es el protocolo de intercambio SGT (Security Group Tag) utilizado por TrustSec para propagar las asignaciones de IP a SGT a los dispositivos TrustSec.

SXP se ha desarrollado para permitir que las redes, incluidos los dispositivos de terceros o los dispositivos antiguos de Cisco que no admiten el etiquetado en línea SGT, tengan funciones TrustSec.

SXP es un protocolo de iguales; un dispositivo puede actuar como altavoz y el otro como receptor.

El altavoz SXP es responsable de enviar los enlaces IP-SGT y el receptor es responsable de recopilar estos enlaces.

La conexión SXP utiliza el puerto TCP 64999 como protocolo de transporte subyacente y MD5 para la integridad/autenticidad del mensaje.

Prerequisites

Requirements

Cisco recomienda conocer la configuración del protocolo SXP e Identity Services Engine (ISE).

Componentes Utilizados

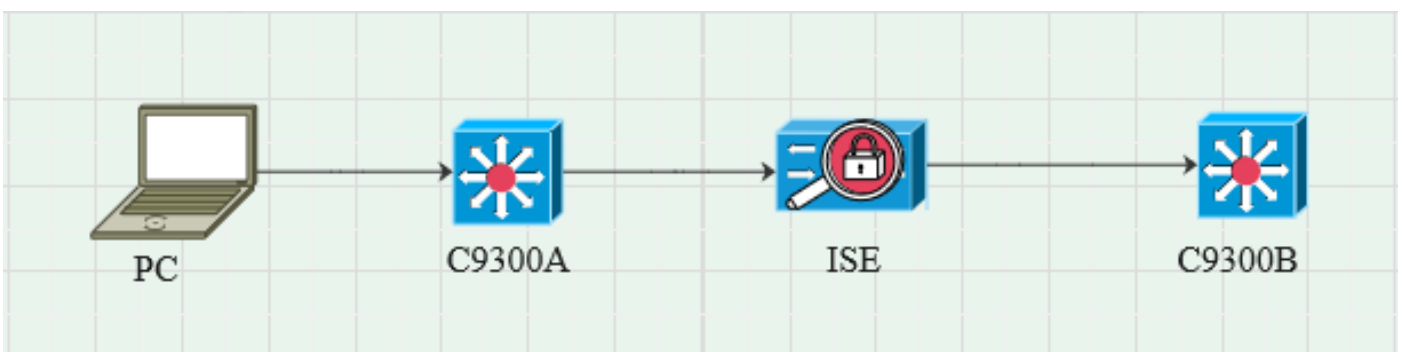
La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Switch Cisco Catalyst 9300 con software Cisco IOS® XE 17.6.5 y versiones posteriores
Cisco ISE, versión 3.1 y posteriores

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Configuración

Diagrama de la red



Flujo de tráfico

El PC se autentica con C9300A e ISE asigna SGT de forma dinámica a través de conjuntos de políticas.

Una vez que ha pasado la autenticación, se crean enlaces con una IP igual al atributo RADIUS de la dirección IP entrante y SGT, tal como se configura en la política.

Los enlaces se propagan en "Todos los enlaces SXP" bajo el dominio predeterminado.

C9300B recibe la información de asignación de SXP de ISE a través del protocolo SXP.

Configurar switch

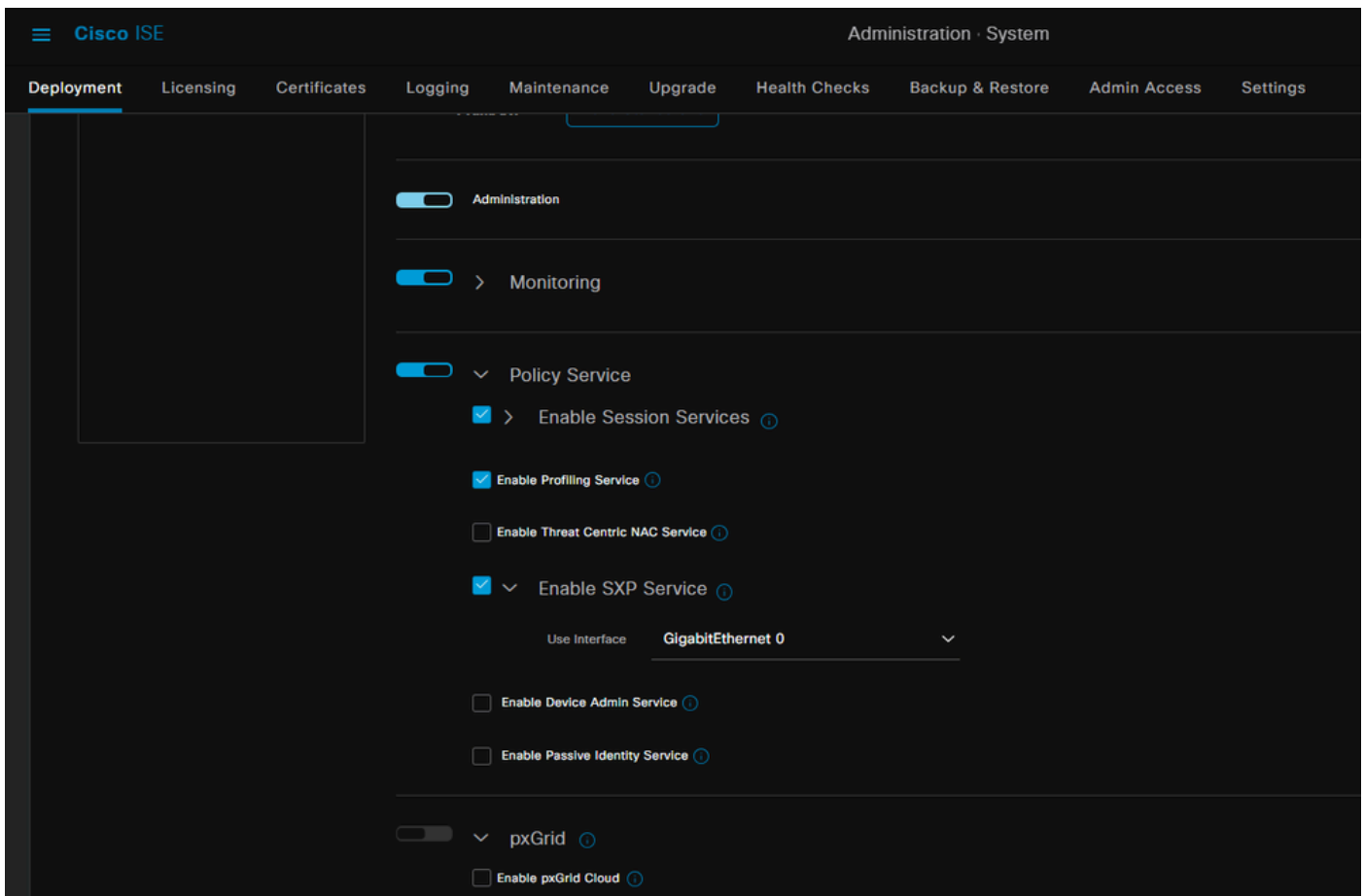
Configure el switch como un receptor SXP para obtener las asignaciones IP-SGT de ISE.

```
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 contraseña modo predeterminado par altavoz hold-time 0
vrf Mgmt-vrf
```

Configuración de ISE

Paso 1. Habilitar el servicio SXP en ISE

Vaya a Administration > System > Deployment > Edit the node y en Policy Service seleccione Enable SXP Service.



Paso 2. Agregar dispositivos SXP

Para configurar el receptor y el altavoz SXP para los switches correspondientes, navegue hasta Workcenters > Trustsec > SXP > SXP Devices.

Agregue el switch con el rol de peer como Listener y asígnelo al dominio predeterminado.

Cisco ISE Work Centers - TrustSec

Overview Components TrustSec Policy Policy Sets **SXP** ACI Troubleshoot Reports Settings

SXP Devices

All SXP Mappings

Input fields marked with an asterisk (*) are required.

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 Settings

Cancel Save

Paso 3. Configuración de SXP

Asegúrese de que Agregar asignaciones de radio a la tabla de asignación SXP IP SGT esté marcada, de modo que ISE aprenda las asignaciones IP-SGT dinámicas a través de las autenticaciones Radius.

Cisco ISE Work Centers - TrustSec

Overview Components TrustSec Policy Policy Sets SXP ACI Troubleshoot Reports **Settings**

General TrustSec Settings

TrustSec Matrix Settings

Work Process Settings

SXP Settings

ACI Settings

SXP Settings

Publish SXP bindings on PxGrid Add radius mappings into SXP IP SGT mapping table

Global Password

Verificación

Paso 1. Conexión SXP en el switch

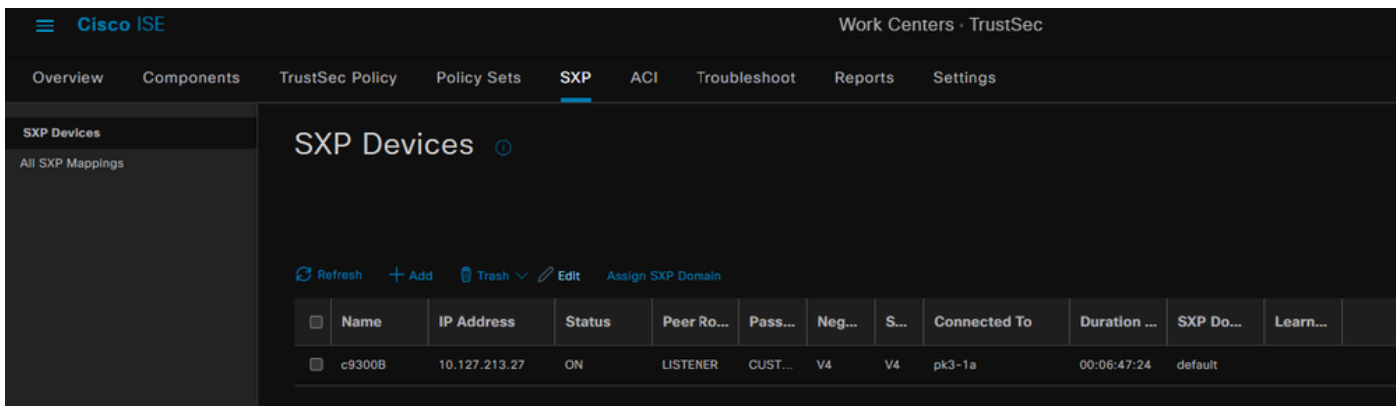
```
C9300B#show cts sxp connections vrf Mgmt-vrf
SXP: activado
Versión más alta admitida: 4
Contraseña predeterminada: establecida
Cadena de teclas predeterminada: no establecida
Nombre predeterminado de la cadena de claves: no aplicable
IP de origen predeterminada: 10.127.213.27
Período de reintento de conexión abierta: 120 segundos
Período de conciliación: 120 segundos
El temporizador de reintento abierto no se está ejecutando
Límite de recorrido de la secuencia de pares para la exportación: no establecido
Límite de recorrido de la secuencia de pares para la importación: no definido
-----
IP del mismo nivel: 10.127.197.53
IP de origen: 10.127.213.27
Estado de conexión: Activado
Versión de conexión: 4
Capacidad de conexión: Subred IPv4-IPv6
Tiempo de espera de conexión: 120 segundos
Modo local: Receptor SXP
Número de instante de conexión: 1
TCP conn fd: 1
Contraseña de conexión TCP: contraseña SXP predeterminada
Se está ejecutando el temporizador de espera
Duración desde el último cambio de estado: 0:00:23:36 (dd:hr:mm:sec)

Número total de conexiones 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> tableid:0x1
```

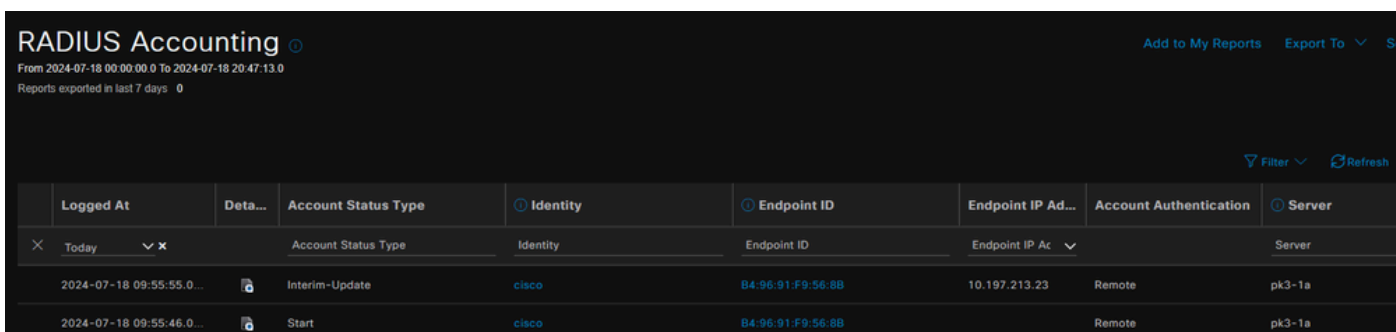
Paso 2. Verificación de ISE SXP

Verifique que el estado de SXP sea ON para el Switch en Workcenters > Trustsec > SXP > SXP Devices.



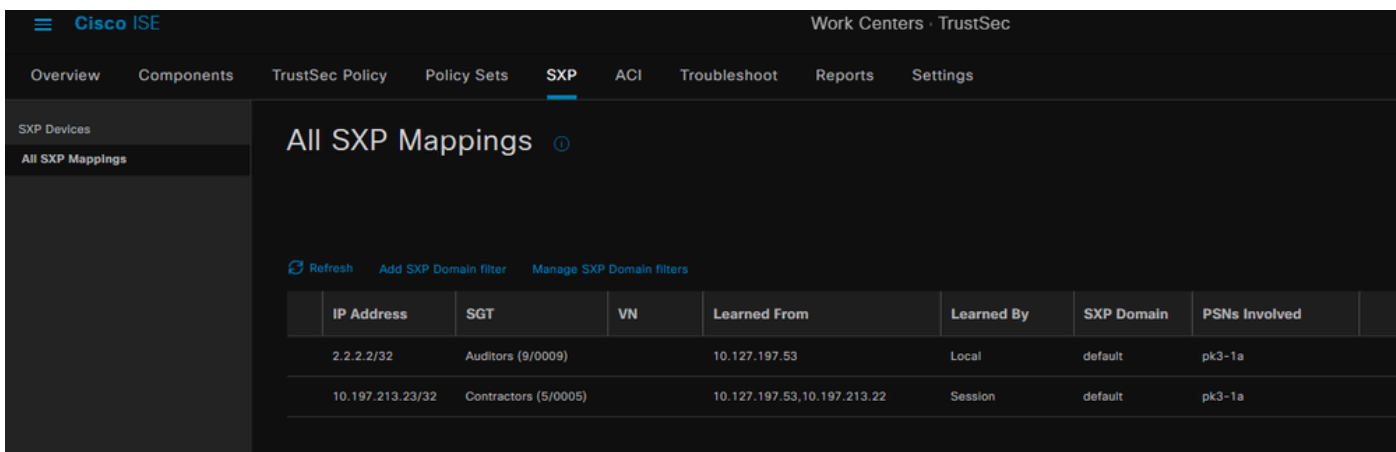
Paso 3. Contabilización RADIUS

Asegúrese de que ISE haya recibido el atributo RADIUS de la dirección IP entramada del paquete de cuentas Radius después de una autenticación exitosa.



Paso 4. Asignaciones de ISE SXP

Navegue hasta Workcenters > Trustsec > SXP > All SXP Mappings para ver las asignaciones IP-SGT aprendidas dinámicamente desde la sesión Radius.



Aprendido por

Local: enlaces IP-SGT asignados estáticamente en ISE.

Sesión: enlaces IP-SGT aprendidos dinámicamente de la sesión Radius.



Nota: ISE tiene la capacidad de recibir enlaces IP-SGT de otro dispositivo. Estas vinculaciones se pueden mostrar como aprendidas por SXP en Todas las asignaciones de SXP.

Paso 5. Asignaciones de SXP en el switch

El switch aprendió las asignaciones de IP-SGT de ISE a través del protocolo SXP.

```
C9300B#show cts sxp sgt-map vrf Mgmt-vrf brief
ID de nodo SXP(generado):0x03030303(3.3.3.3)
Asignaciones IP-SGT de la siguiente manera:
IPv4, SGT: <2.2.2.2 , 9>
IPv4, SGT: <10.197.213.23 , 5>
Número total de asignaciones de IP-SGT: 2
conn en sxp_bnd_exp_conn_list (total:0):
C9300B#
```



```
C9300B#show cts role-based sgt-map vrf Mgmt-vrf all
Información de enlaces IPv4-SGT activos
```

```
Origen de SGT de dirección IP
```

```
=====
2.2.2.2.9 SXP
10.197.213.23 5 SXP
```

```
Resumen de IP-SGT Active Bindings
```

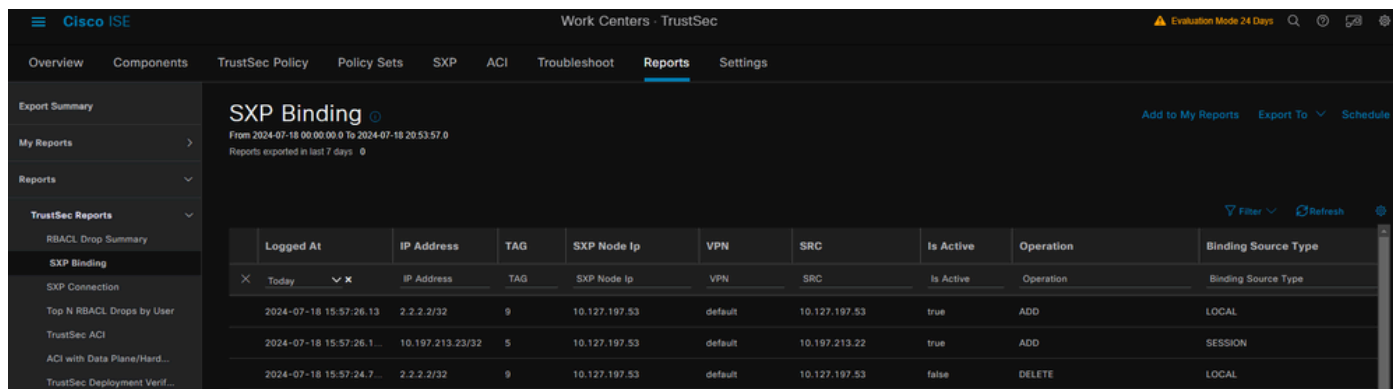
```
=====
Número total de enlaces SXP = 2
Número total de enlaces activos = 2
```

Troubleshoot

En esta sección encontrará información que puede utilizar para solucionar problemas de configuración.

Informe de ISE

ISE también permite generar informes de conexiones y enlaces SXP, como se muestra en esta imagen.



The screenshot shows the Cisco ISE Reports page for TrustSec. The main report is titled "SXP Binding" and shows a table of binding events. The table has columns for Logged At, IP Address, TAG, SXP Node Ip, VPN, SRC, Is Active, Operation, and Binding Source Type. The data shows three entries: two successful "ADD" operations and one "DELETE" operation.

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

Depuraciones en ISE

Recopile el paquete de soporte de ISE con estos atributos que se establecerán en el nivel de depuración:

- sxp
- sgtbinding
- nsf
- nsf-session
- TrustSec

Cuando un usuario se autentica desde un servidor ISE, ISE asigna una SGT en el paquete de respuesta de aceptación de acceso. Una vez que el usuario obtiene la dirección IP, el switch

envía la dirección IP entramada en el paquete de contabilidad Radius.

show logging application localStore/iseLocalStore.log:

```
2024-07-18 09:55:55.051 +05:30 000017592 3002 AVISO Radius-Accounting: Actualización de
vigilancia de contabilidad RADIUS, ConfigVersionId=129, Dirección IP del
dispositivo=10.197.213.22, UserName=cisco, NetworkDeviceName=pk, Nom-NAS=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, Llamadas E-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, RequestLatency=6, Step=11004, Step=11017,
Step=15049, Step=15008 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 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 -:::-
registrando los valores de sesión recibidos desde PortCpmBridge :
Tipo de operación ==>ADD, sessionId ==> 16D5C50A00000017C425E3C6, sessionState ==>
ACCEPTED, inputIp ==> 10.197.213.23, inputSgTag ==> 0005-00, nasIp ==> 10.197.213.22null,
vn ==> null
```

El nodo SXP almacena la asignación IP + SGT en su tabla H2DB y el nodo PAN posterior recopila esta asignación SGT IP y se refleja en Todas las asignaciones SXP en la GUI de ISE (Workcenters ->Trustsec -> SXP->Todas las asignaciones 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 Agregar enlaces de sesión por lotes-tamaño: 1
2024-07-18 10:01:01,317 DEBUG [SxpNotificationSerializer-Thread]
cpm.sxp.engine.services.NotificationSerializerImpl:202 - tarea de procesamiento Tarea [add=true,
notification=RestSxpLocalBinding(tag=5, groupName=null, ipAddress=10.197.213.23/32,
```

```
naslp=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'] Agregando nuevo enlace:
```

```
MasterBindingIdentity [ip=10.197.213.23/32, peerSequence=10.127.197.53,10.197.8.213.22,
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 - Adición de 1 enlace(s)
```

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

```
cisco.cpm.sxp.engine.MasterDbListener:251 - Envío de la tarea al controlador H2 para agregar
enlaces, número de enlaces: 1
```

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

El nodo SXP actualiza el switch de par con los últimos enlaces 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 a
[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 CORRECTO para
[ISE:10.127.197.53][10.127.197.53:64999/10.127.213.27:31025][O|Sv4]
```

Depuraciones en el switch

Habilite estos debugs en el switch para resolver problemas de conexiones y actualizaciones de SXP.

```
debug cts sxp conn
```

```
debug cts sxp error
```

```
debug cts sxp mdb
```

```
debug cts sxp message
```

Switch recibió las asignaciones SGT-IP del altavoz SXP "ISE".

Marque **Show logging** para ver estos registros:

```
18 de julio 04:23:04.324: CTS-SXP-MSG:sxp_rcv_update_v4 <1> peer ip: 10.127.197.53
```

```
Jul 18 04:23:04.324: CTS-SXP-MDB:IMU Añadir enlace:- <conn_index = 1> desde el peer
10.127.197.53
18 de julio 04:23:04.324: CTS-SXP-MDB:mdb_send_msg <IMU_ADD_IPSGT_DEVID>
18 de julio 04:23:04.324: CTS-SXP-INTNL:mdb_send_msg mdb_process_add_ipsgt_devid Inicio
18 de julio 04:23:04.324: CTS-SXP-MDB:sxp_mdb_inform_rbm tableid:0x1 sense:1 sgt:5
peer:10.127.197.53
18 de julio 04:23:04.324: CTS-SXP-MDB:SXP MDB: Entrada añadida ip 10.197.213.23 sgt
0x0005
18 de julio 04:23:04.324: CTS-SXP-INTNL:mdb_send_msg mdb_process_add_ipsgt_devid
Finalizado
```

Información Relacionada

[Segmentación de la guía de administración de ISE 3.1](#)

[Guía de configuración de Catalyst Descripción general de Trustsec](#)

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).