

Comprensión de la reserva de recursos a demanda para AD en ISE 3.3, parche 4

Contenido

[Introducción](#)

[Requisitos previos](#)

[Componentes necesarios](#)

[Antecedentes](#)

[Síntoma](#)

[Problema](#)

[Solución](#)

[Configuración paso a paso](#)

[Detalles adicionales](#)

[Resolución de problemas](#)

[Verificación](#)

[Registro](#)

[Fragmentos de registro](#)

[Preguntas frecuentes](#)

Introducción

Este documento describe la Reserva de recursos a demanda para Active Directory en ISE 3.3
Parche 4

Requisitos previos

Conocimientos sobre Cisco Identity Services Engine (ISE)

Conocimientos sobre Active Directory (AD)

Conocimientos sobre ISE e integración de AD

Componentes necesarios

La información que contiene este documento se basa en estas versiones de software y hardware

- Parche 4 de Cisco Identity Services Engine 3.3
- Microsoft Windows Active Directory 2016 o posterior

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.

Antecedentes

Las autenticaciones de AD a veces son lentas y finalmente fallan. Las posibles razones pueden ser que la cola ADID comience a acumularse o que se agoten todos los subprocesos del grupo ADID.

Más detalles sobre ADID:

Un ADID, también conocido como nombre distinguido (DN), es una cadena que identifica de forma única un objeto dentro del directorio de Active Directory. Se utilizan para localizar y administrar objetos dentro del dominio de Active Directory. Los ADID son cruciales para administrar cuentas de usuario, permisos y otros recursos dentro de un entorno de Active Directory.

Un ADID típico debe tener este aspecto: CN=Juan Pérez,OU=Ventas,DC=ejemplo,DC=com; where,

CN=Juan Pérez: Representa el nombre común del usuario, Juan Pérez.

OU=Ventas: Representa la unidad organizativa (UO) a la que pertenece el usuario, en este caso, el departamento de ventas.

DC=ejemplo,DC=com: Representa los componentes del dominio, que es example.com.

Por ejemplo:

Consulte la Imagen 1: Una configuración de punto de unión AD típica

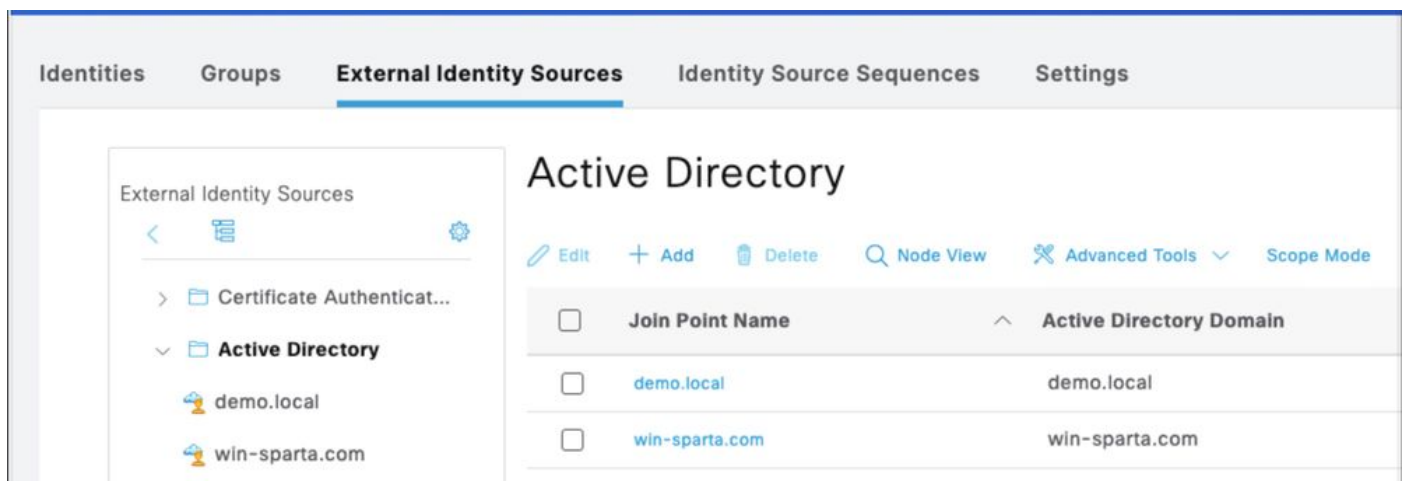


Imagen 1: Puntos de unión de AD

Consulte la Imagen 2: Un diagrama de flujo AD típico con 2 puntos de unión

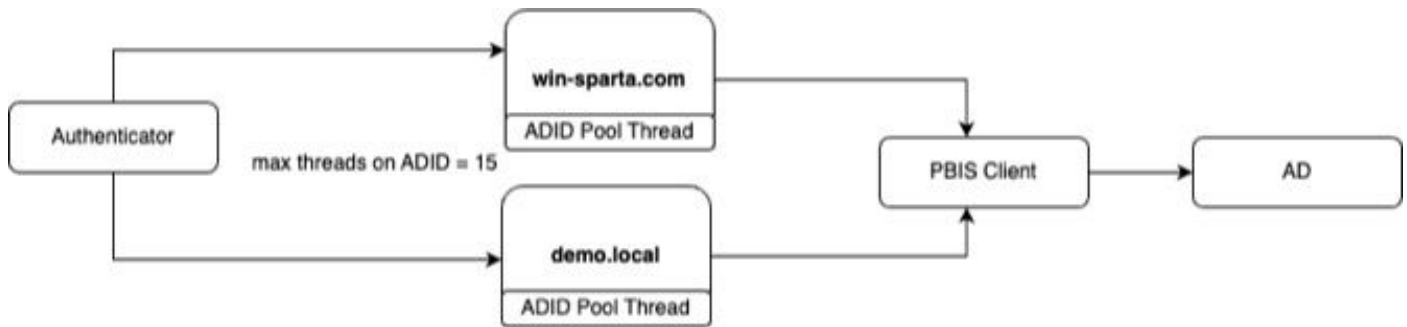


Imagen 2: Un diagrama de flujo AD típico

Síntoma

Punto de unión lento bajo el mismo conjunto de subprocesos ADID

Problema

1. ¿Cuáles serían las consecuencias de que uno de los puntos de unión sea muy lento? Por ejemplo, si se envían 15 autenticaciones a ISE al mismo tiempo para "demo.local" y "demo.local" es inusualmente lento, deberíamos esperar la respuesta de "demo.local" antes de gestionar la posterior autenticación win-sparta.
2. ¿Qué sucede si ambos puntos de unión comparten el mismo conjunto de subprocesos ADID en un punto de unión?

Consulte la Imagen 3: Diagrama de flujo del punto de unión lento

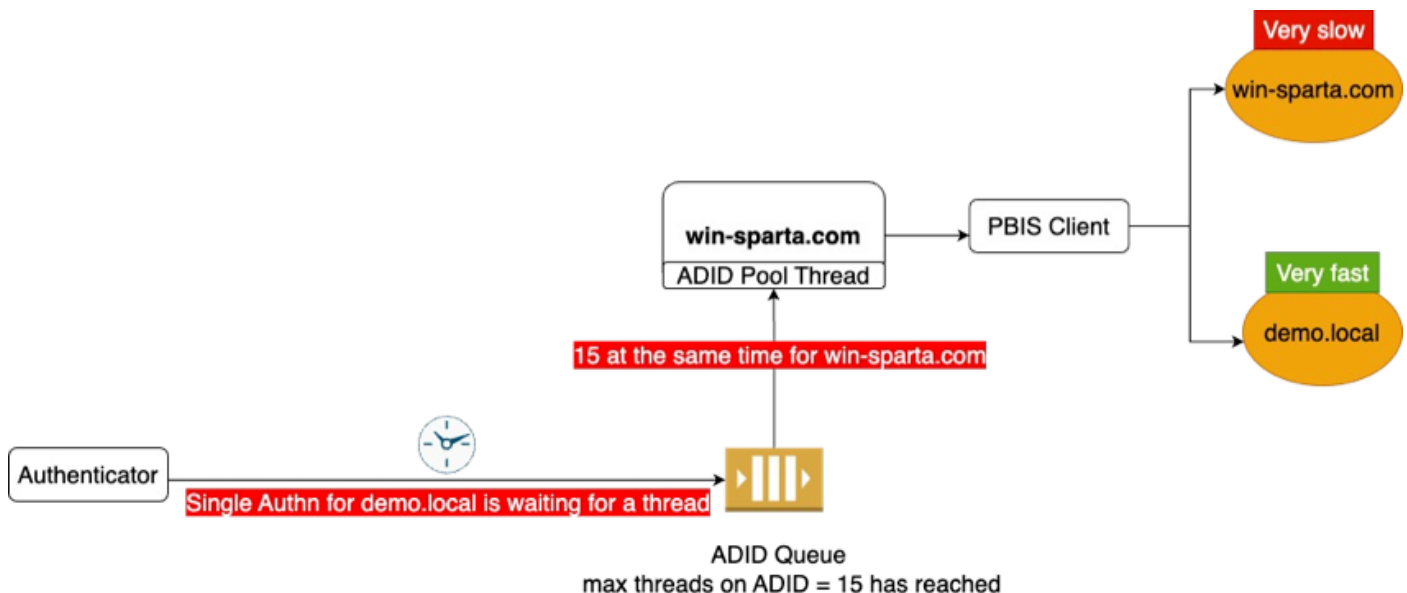


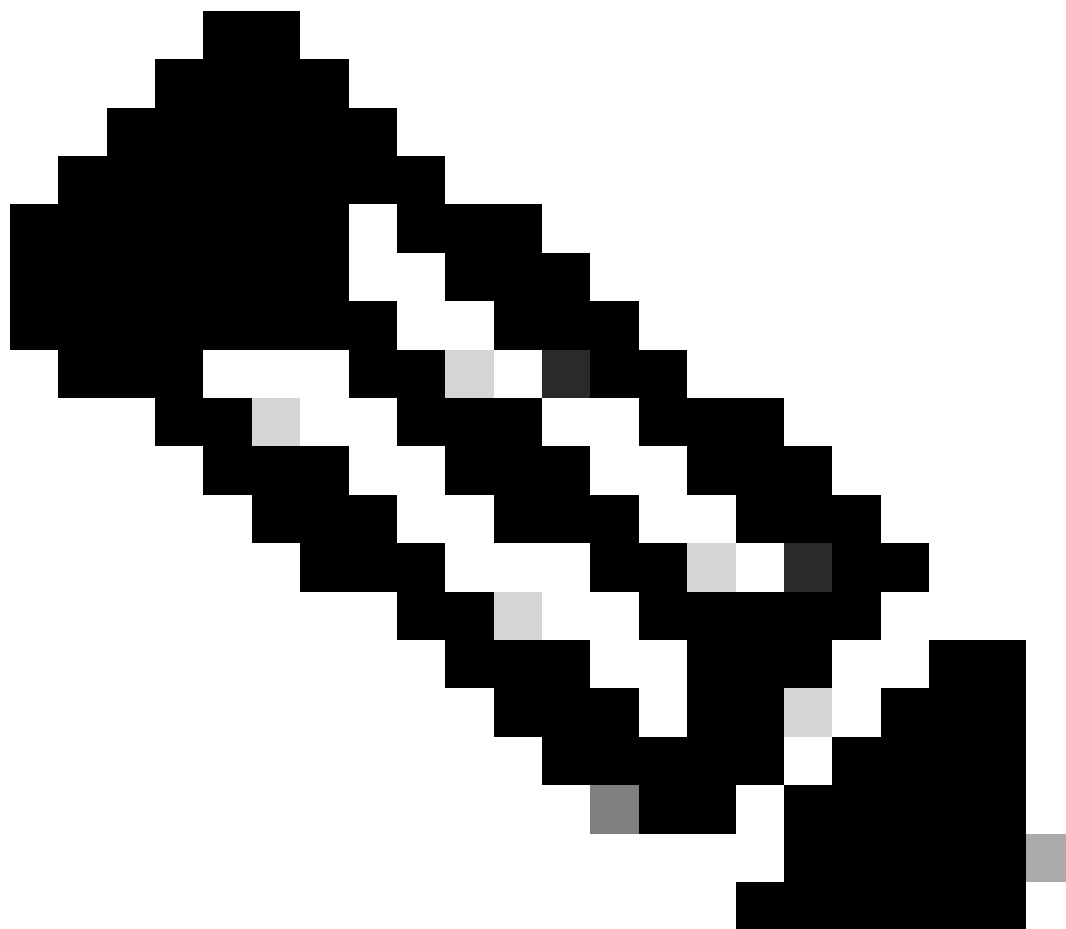
Imagen 3: Flujo problemático



Nota: Aquí, los 15 hilos están ocupados por win-sparta.com al mismo tiempo sin dejar ningún hilo para demo.local

Solución

- El comportamiento predeterminado es un grupo de subprocesos común para todos los puntos de unión de AD
- Sin embargo, los administradores pueden segmentar cada punto de unión para tener sus propios recursos.



Nota: Cuando se aplica la priorización de AD, el valor predeterminado es 10 subprocesos por grupo de subprocesos.

Consulte la Imagen 4: Diagrama de flujo del punto de unión reservado a demanda

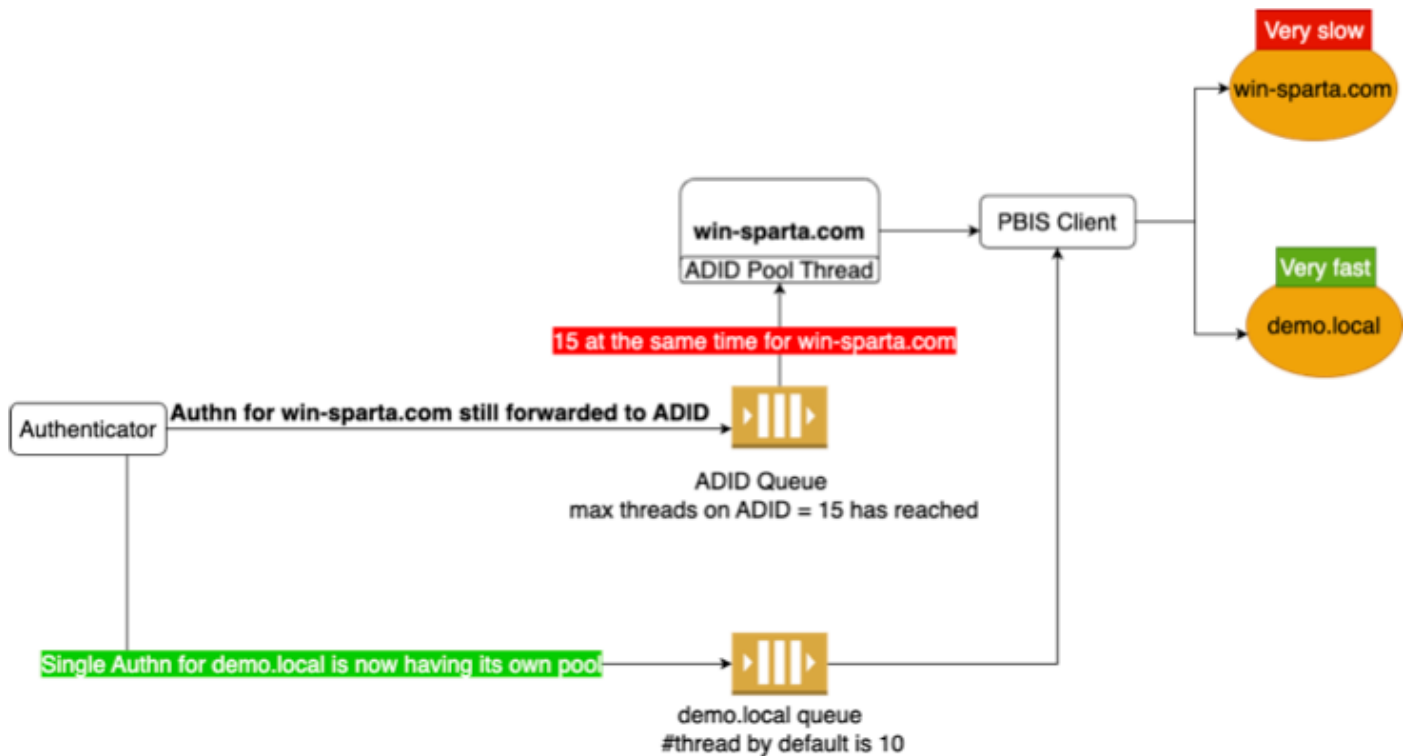


Imagen 4: Flujo de soluciones

Configuración paso a paso

Paso 1: Cree 2 puntos de unión de AD independientes. Aquí, por ejemplo, tenemos: demo.local y win-sparta.com

Paso 2: Crear prioridad de punto de unión después de la creación del punto de unión de AD.

Consulte la Imagen 5:

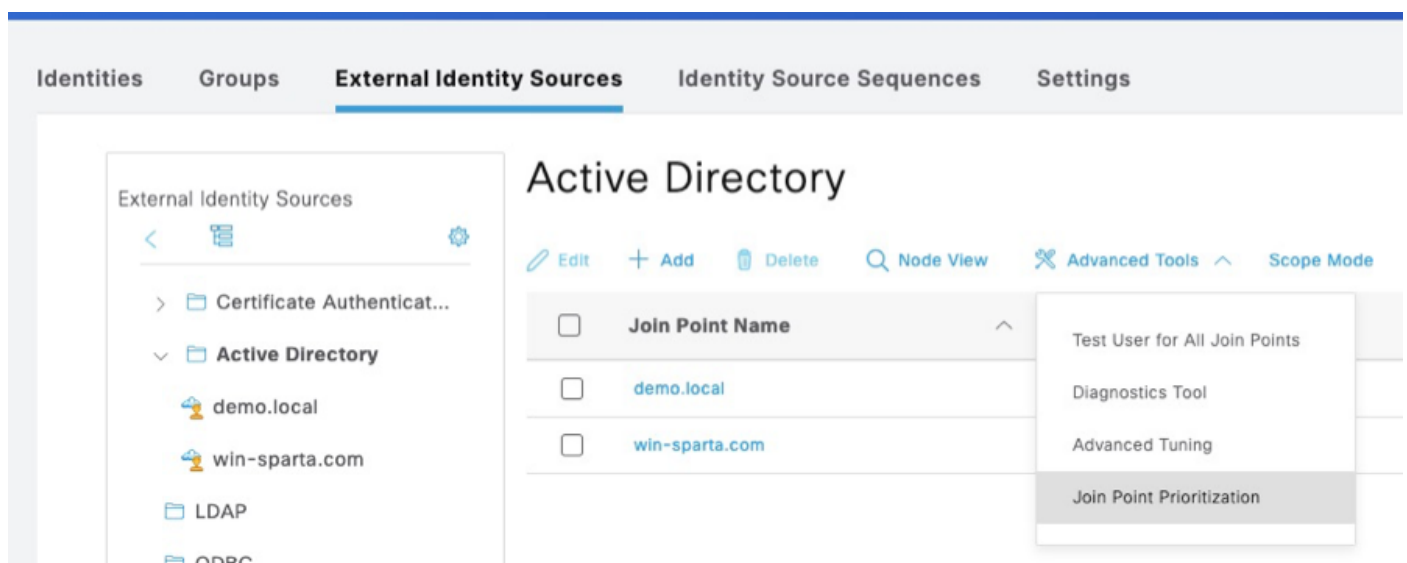


Imagen 5: Priorización de puntos de unión

Paso 3: En Priorización de punto de unión, seleccione el PSN que prefiera para reservar recursos AD dedicados. Haga clic en Editar.

Consulte la Imagen 6:

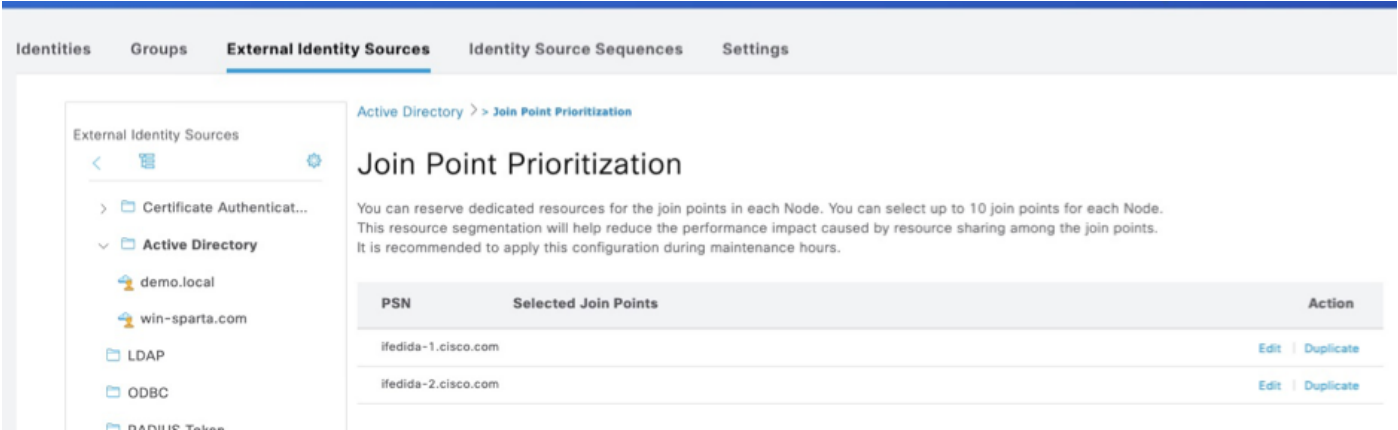


Imagen 6: Editar PSN

Paso 4: Seleccione el punto de unión preferido para el PSN preferido.

Consulte la Imagen 7:

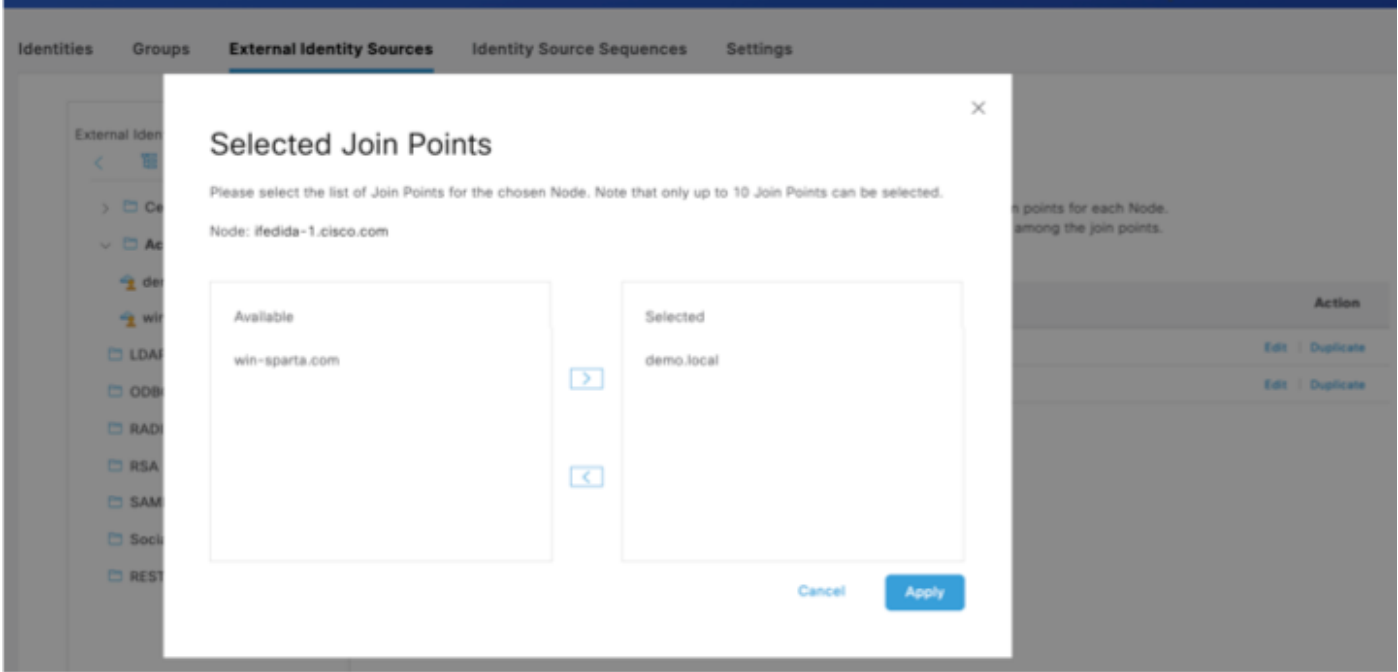


Imagen 7: Punto de unión seleccionado



Nota: Los puntos de unión no incluidos en la priorización utilizan el grupo de subprocesos comunes, que tiene un límite máximo de 15 subprocesos.

Paso 5: Priorización finalizada

Consulte la Imagen 8:

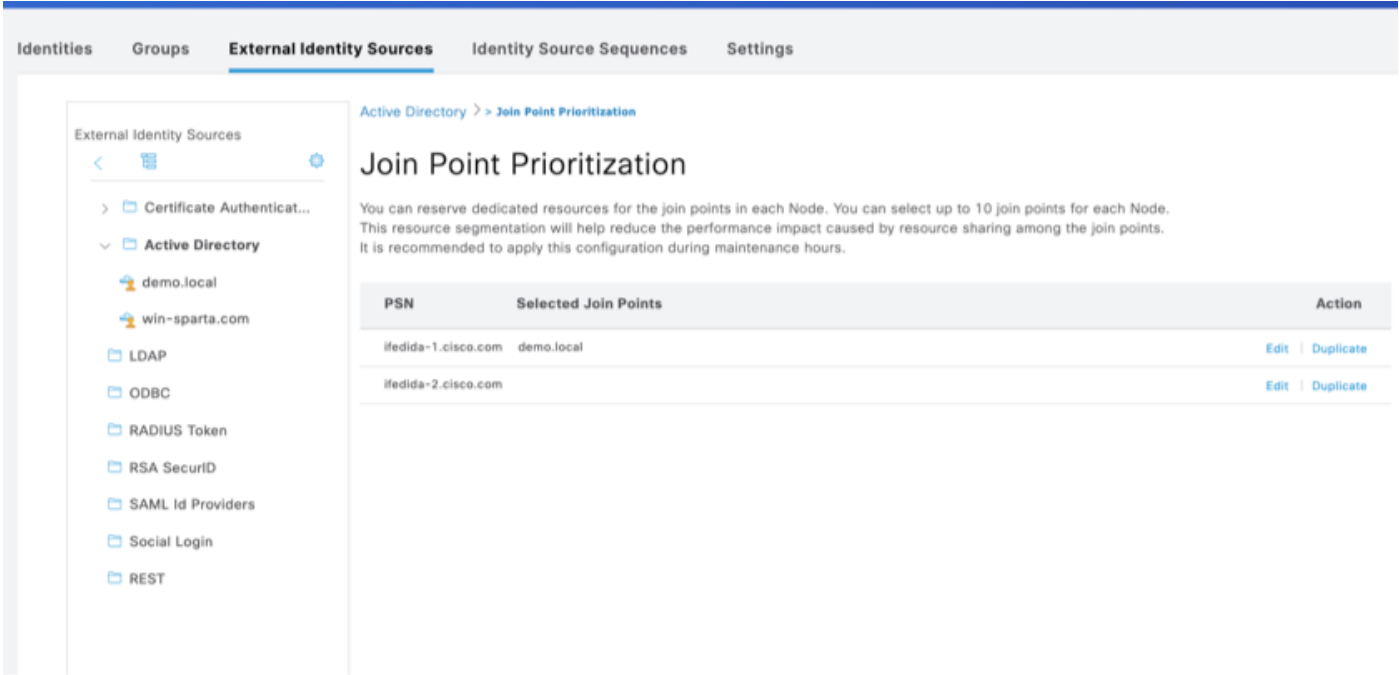
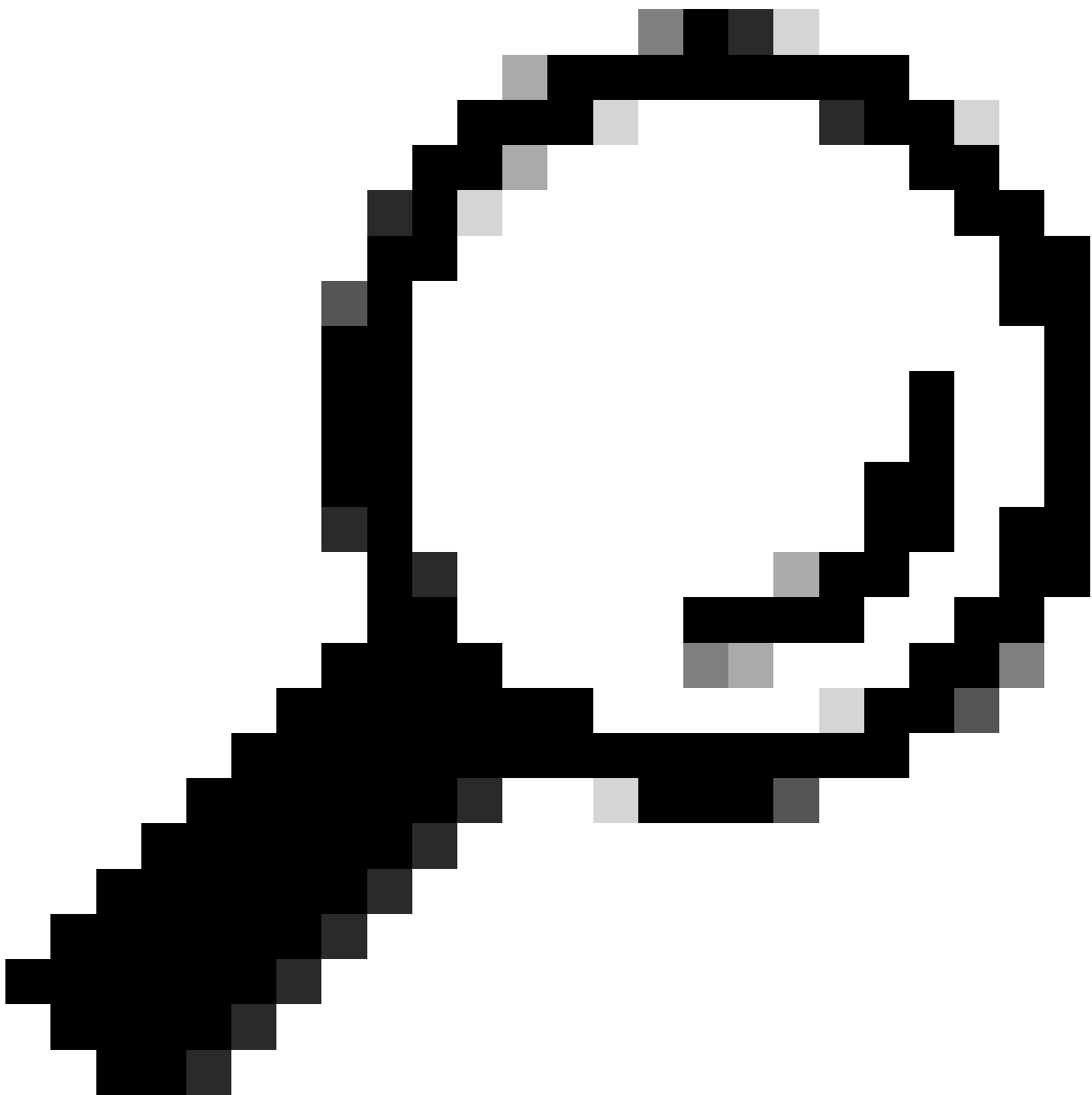


Imagen 8: Configuración de priorización

Detalles adicionales



Consejo: Si desea replicar la misma configuración en otros PSN, puede utilizar la opción Duplicar. Seleccione el PSN deseado y elija el punto de unión que se va a duplicar junto con la priorización original.

Consulte la imagen 9: Sugerencia de configuración:

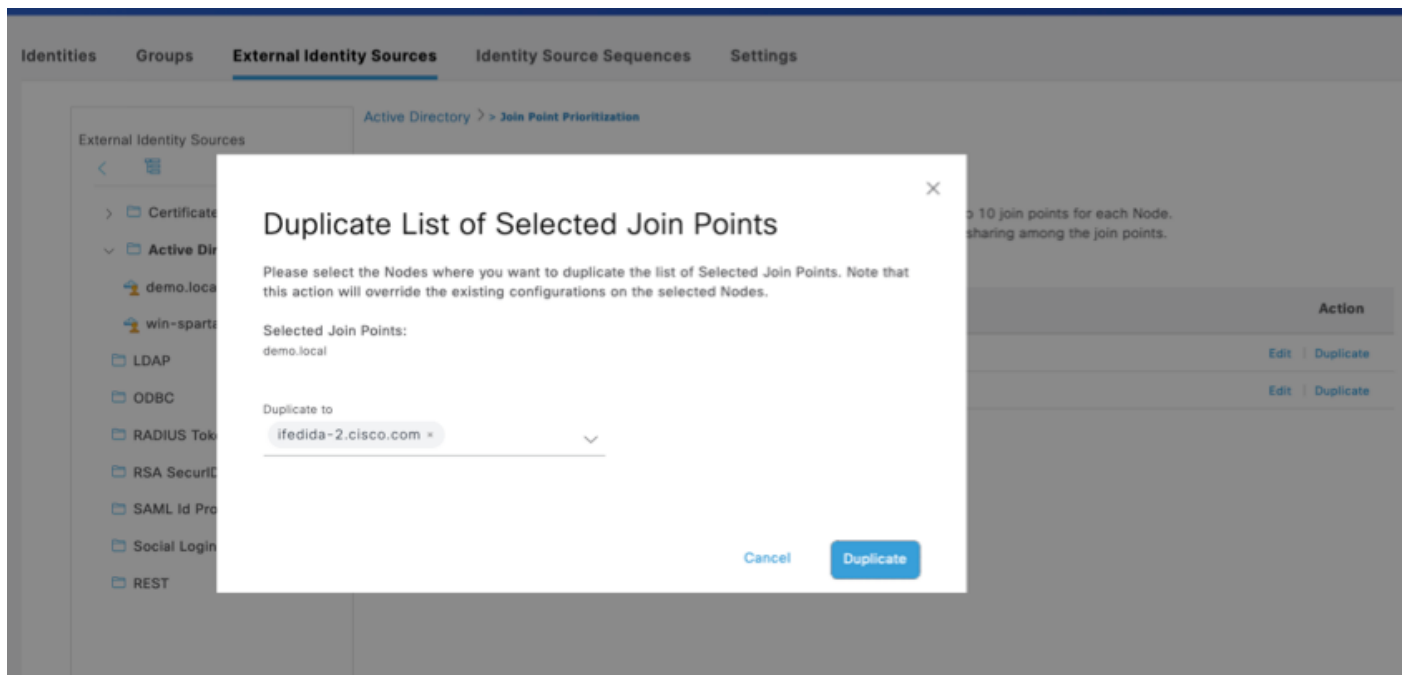


Imagen 9: Configuración de priorización duplicada

Paso 6: Lista final después de la duplicación

Consulte la Imagen 10:

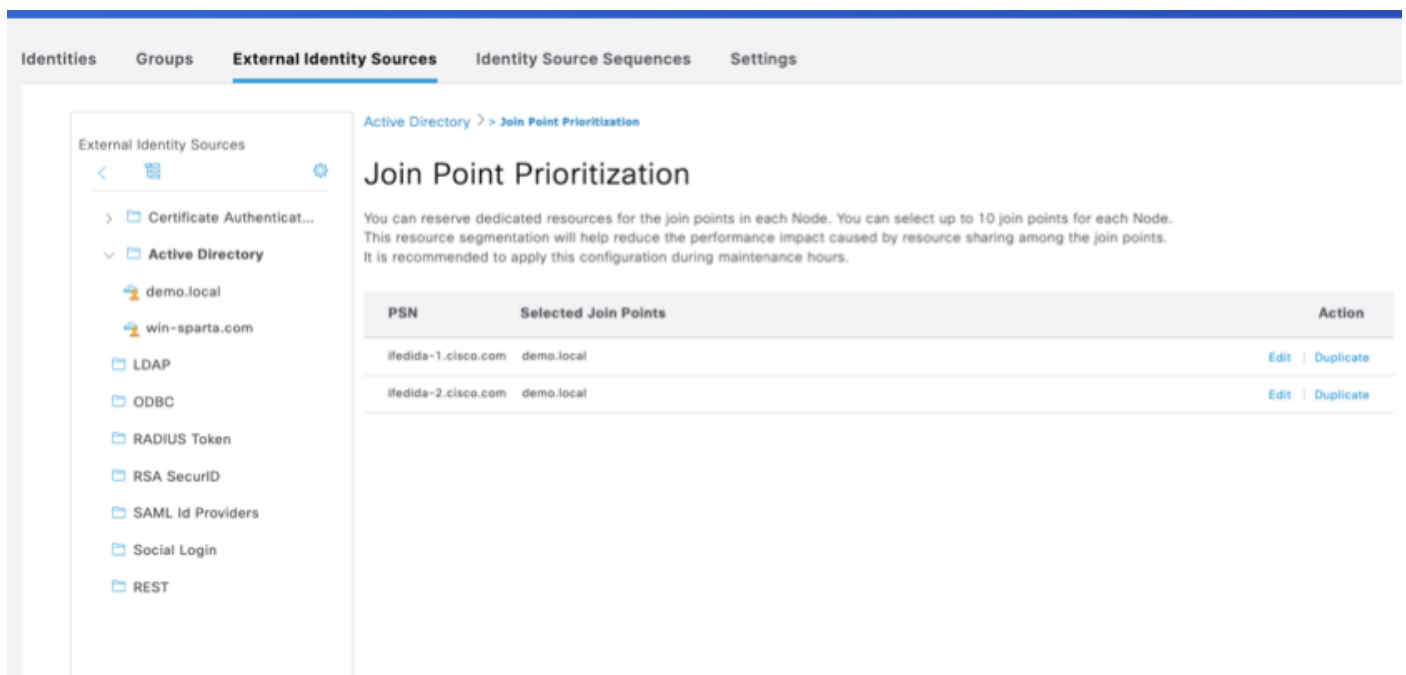


Imagen 10: Lista final después de la priorización

Resolución de problemas

Verificación

Verifique los cambios de configuración. Navegue hasta: Operaciones > Informes > Auditorías > Cambiar auditoría de configuración

Consulte la Imagen 11:

Reports

Export Summary

My Reports

Reports

Audit

Adaptive Network Control Audit NLS

Administrator Logins

Change Configuration Audit

Cisco Support Diagnostics Audit

Data Purging Audit

Endpoints Purge Activities

Internal Administrator Summary

IPSec Audit Logging

Change Configuration Audit

From 2024-09-04 00:00:00.0 To 2024-09-04 15:42:38.0

Reports exported in last 7 days: 0

Add to My Reports

Export

Filter

Logged At	Administrator	Server	Interface	Object Type	Object Name	Event
Today	Administrator	Server		Object Type	Object Name	
2024-09-04 15:41:20.5...	admin	ifedida-2	GUI	AD Join point prioritization settings	AD Join point prioritization	Changed configuration
2024-09-04 15:41:20.4...	admin	ifedida-2	GUI	AD Join point prioritization settings	AD Join point prioritization	Changed configuration

Imagen 11: Informe de auditoría de configuración

Registro

- Habilite el nivel de depuración para los registros AAA en tiempo de ejecución.
- Analice prrt-server.log

Consulte la imagen 12:

☐	runtime-AAA	DEBUG	AAA runtime messages (prrt)	prrt-server.log
-----------------------	-------------	-------	-----------------------------	-----------------

Imagen 12: Configuración del registro de depuración

Fragmentos de registro

prrt-server.log [DEBUG]: Default Log:

EventHandler,2024-08-23 07:16:48,135,DEBUG,0x7fec2ccc700,Grupo de subprocessos predeterminado asignado: ADIDStore a IDP : win-sparta.com_wxETIH16Pk_106

prrt-server.log [INFO]: Cuando configuramos Recursos Dedicados:

- ActiveDirectoryIDStore,2024-09-08 16:52:01,048,INFO ,0x7f2452ccf700,Grupo de subprocessos asignado : ADThreadPool0 a IDP : win-sparta.com_wxETIH16Pk_106
- ActiveDirectoryIDStore,2024-09-08 16:57:11,258,INFO ,0x7f2452ccf700,Grupo de subprocessos asignado : ADThreadPool1 a IDP: demo.local_6EcNs6UzwX_89

prrt-server.log [INFO]:

- Antes de haber establecido recursos dedicados:
 - EventHandler, 2024-09-02 08:45:54,673,INFO,0x7fafb793c700,Evento pasado al siguiente nombre del grupo de subprocessos=ADIDStore, tamaño de la cola=1,EventDispatcher.cpp:757

- Una vez que hayamos establecido los recursos dedicados:
 - EventHandler,2024-09-02 08:45:54,673,INFO ,0x7f4867ff9700,Evento Passed al siguiente grupo de subprocesos name=ADThreadPool0, queue size=1,EventDispatcher.cpp:841

Para realizar un seguimiento del uso del grupo de subprocesos de "ADThreadPool0":

1. 0x7f57792f7700,Evento pasado al siguiente grupo de subprocesos name=ADThreadPool0 (algunos registros devuelven StackID:0x7f57a4f761c0)
2. 0x7f57732c7700, Pila: 0x7f57a4f761c0 Llamando a ActiveDirectoryIDStore: Method MethodCaller<ActiveDirectoryIDStore, PlainAuthenticateAndQueryEvent>
3. 0x7f57732c7700,cntx=0000210117,sesn=ifedida-1/515863662/5273,CPMSessionID=C0A31430000000800018958,user=abcd,CallingStationID=[CAD] 956: CAD_PAPAuthenticate (abcd) called
4. 0x7f57732c7700,cntx=000210117,sesn=ifedida-1/515863662/5273,CPMSessionID=C0A31430000000800018958,user=abcd,CallingStationID=[CAD] 1026: CAD_PAPAuthenticate (abcd) correcto
5. 0x7f57732c7700,Evento Passed al siguiente nombre del grupo de subprocesos=Principal

Preguntas frecuentes

Pregunta: ¿Cuántos puntos de unión AD admite ISE?

Respuesta: Puede configurar hasta 50 puntos de unión de Active Directory en una sola implementación de ISE.

Pregunta: Si tengo varios puntos de unión de AD, ¿puedo seguir usando la priorización a demanda?

Respuesta: Yes

Pregunta: ¿Cuál es el tamaño de subproceso predeterminado sin priorización para un único dominio?

Respuesta: 15 hilos

Pregunta: Si configuro la priorización, ¿cómo se realiza el cálculo? Tenga en cuenta que un escenario de 3 puntos de unión (domain1.com, domain2.com y domain3.com con domain1.com) no está configurado para la priorización y domain2.com y domain3.com sí lo está.

Respuesta: Si el dominio 1 no está configurado para la priorización, domain1.com utiliza los 15 subprocesos comunes disponibles, todos al mismo tiempo. Sin embargo, dado que domain2.com y domain3.com se configuran con la priorización, utilizan 10 subprocesos cada uno de forma predeterminada y no siguen/utilizan el conjunto de 15 subprocesos común.

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).