

Entender a reserva de recursos sob demanda para AD no ISE 3.3 Patch 4

Contents

[Introdução](#)

[Pré-requisitos](#)

[Componentes necessários](#)

[Informações de Apoio](#)

[Sintoma](#)

[Problema](#)

[Solução](#)

[Configuração Passo a Passo](#)

[Detalhes adicionais](#)

[Troubleshooting](#)

[Verificação](#)

[Registro](#)

[Registrar trechos](#)

[FAQ](#)

Introdução

Este documento descreve sobre a reserva de recursos sob demanda para Active Directory no ISE 3.3 Patch 4

Pré-requisitos

Conhecimento sobre o Cisco Identity Services Engine (ISE)

Conhecimento sobre o Active Directory (AD)

Conhecimento sobre ISE e integração de AD

Componentes necessários

As informações neste documento são baseadas nestas versões de software e hardware

- Cisco Identity Services Engine 3.3 Patch 4
- Microsoft Windows Active Directory 2016 ou mais recente

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma

configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

As autenticações do AD às vezes são lentas e eventualmente falham. Os possíveis motivos podem ser o início da pilha da fila ADID ou o esgotamento de todos os segmentos do pool ADID.

Mais detalhes sobre o ADID:

Um ADID, também conhecido como nome distinto (DN), é uma sequência de caracteres que identifica exclusivamente um objeto no diretório do Ative Directory. Eles são usados para localizar e gerenciar objetos no domínio do Ative Directory. Os ADIDs são cruciais para gerenciar contas de usuário, permissões e outros recursos em um ambiente do Ative Directory.

Um ADID típico deve ter esta aparência: CN=João da Silva,OU=Vendas,DC=exemplo,DC=com; where,

- CN=João da Silva: Representa o nome comum do usuário, John Doe.
- OU=Vendas: Representa a unidade organizacional (OU) à qual o usuário pertence, neste caso, o departamento de Vendas.
- dc=example,dc=com: Representa os componentes do domínio, que é example.com.

Por exemplo:

Consulte a Figura 1: Uma configuração típica de ponto de união do AD

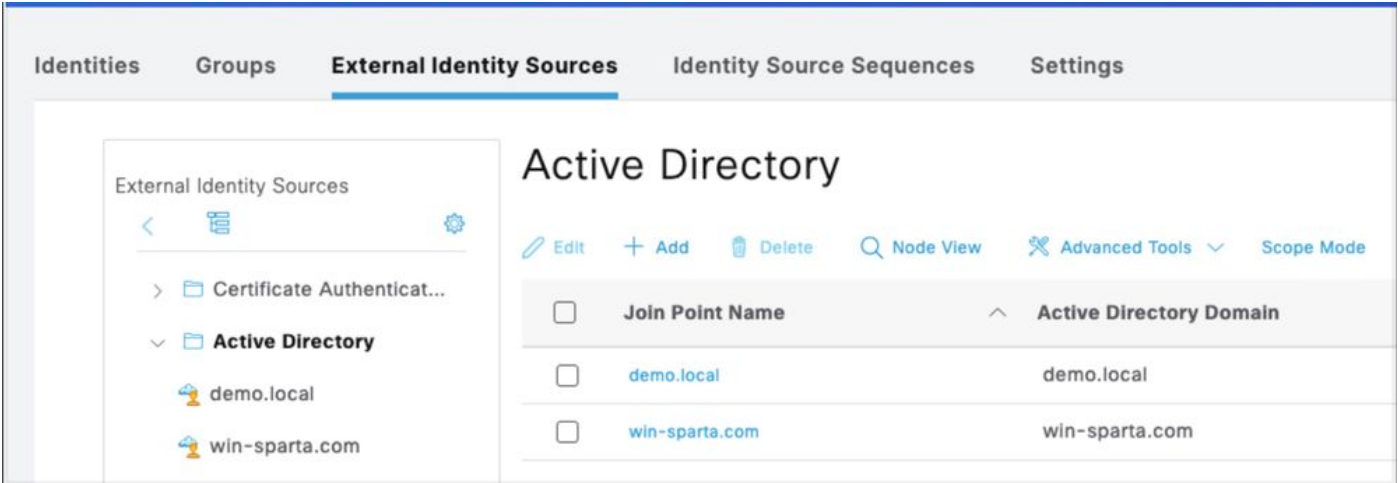


Figura 1: Pontos de junção do AD

Consulte a Figura 2: Um fluxograma típico do AD com 2 pontos de união

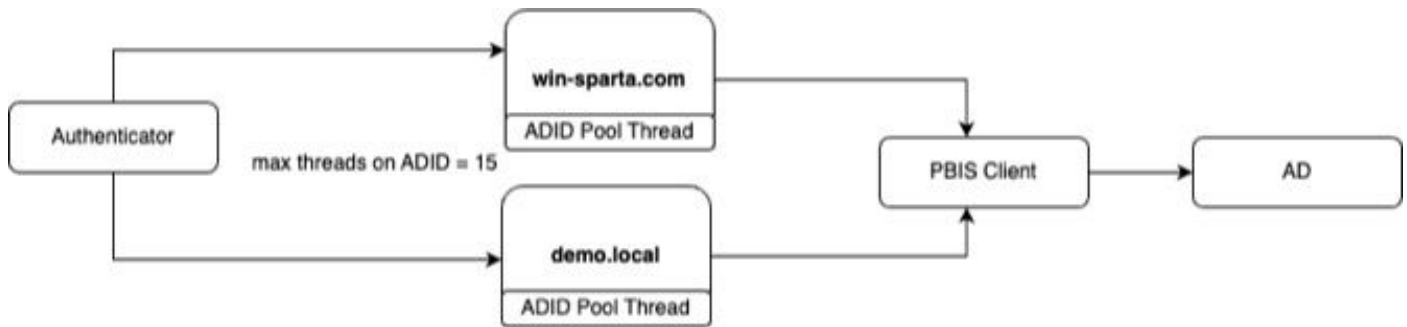


Figura 2: Um fluxograma típico do AD

Sintoma

Ponto de Junção Lento no mesmo Pool de Threads ADID

Problema

1. Quais seriam as consequências de um dos pontos de união ser muito lento? Por exemplo, se 15 autenticações forem enviadas ao ISE ao mesmo tempo para "demo.local" e "demo.local" for excepcionalmente lento, precisaremos aguardar a resposta de "demo.local" antes de lidar com a autenticação win-sparta subsequente.
2. E se ambos os pontos de junção compartilharem o mesmo pool de segmentos ADID em um ponto de junção?

Consulte a Figura 3: Diagrama do ponto de articulação lenta

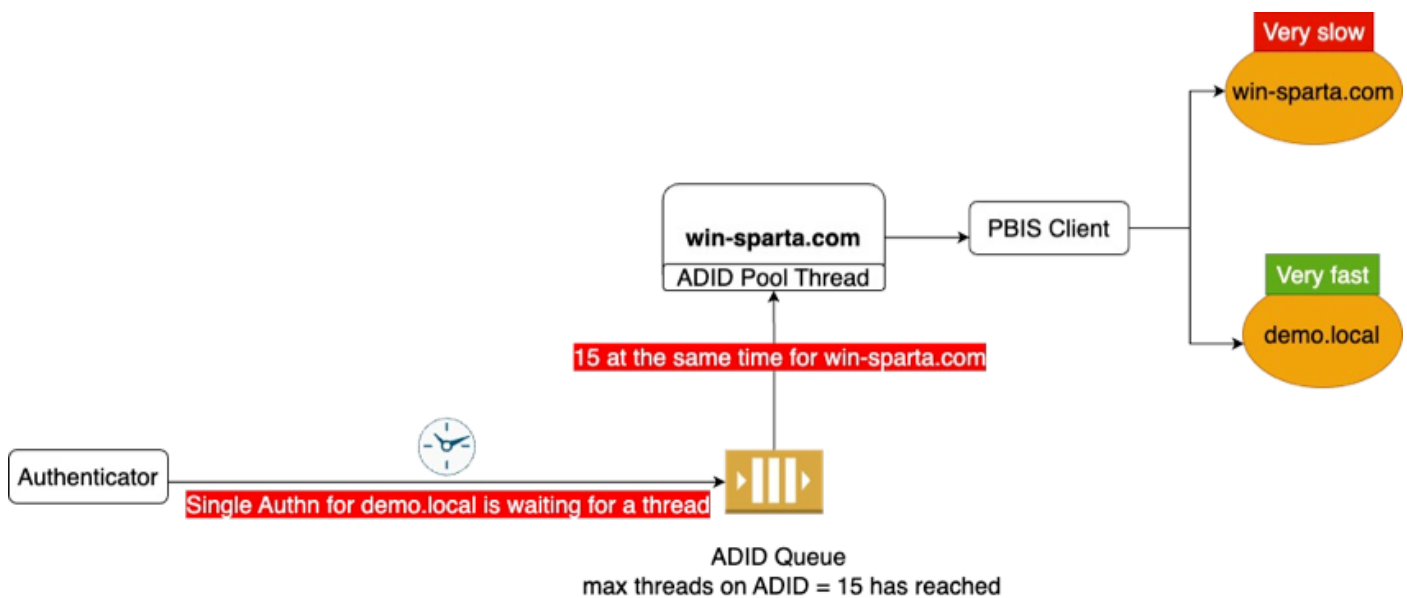


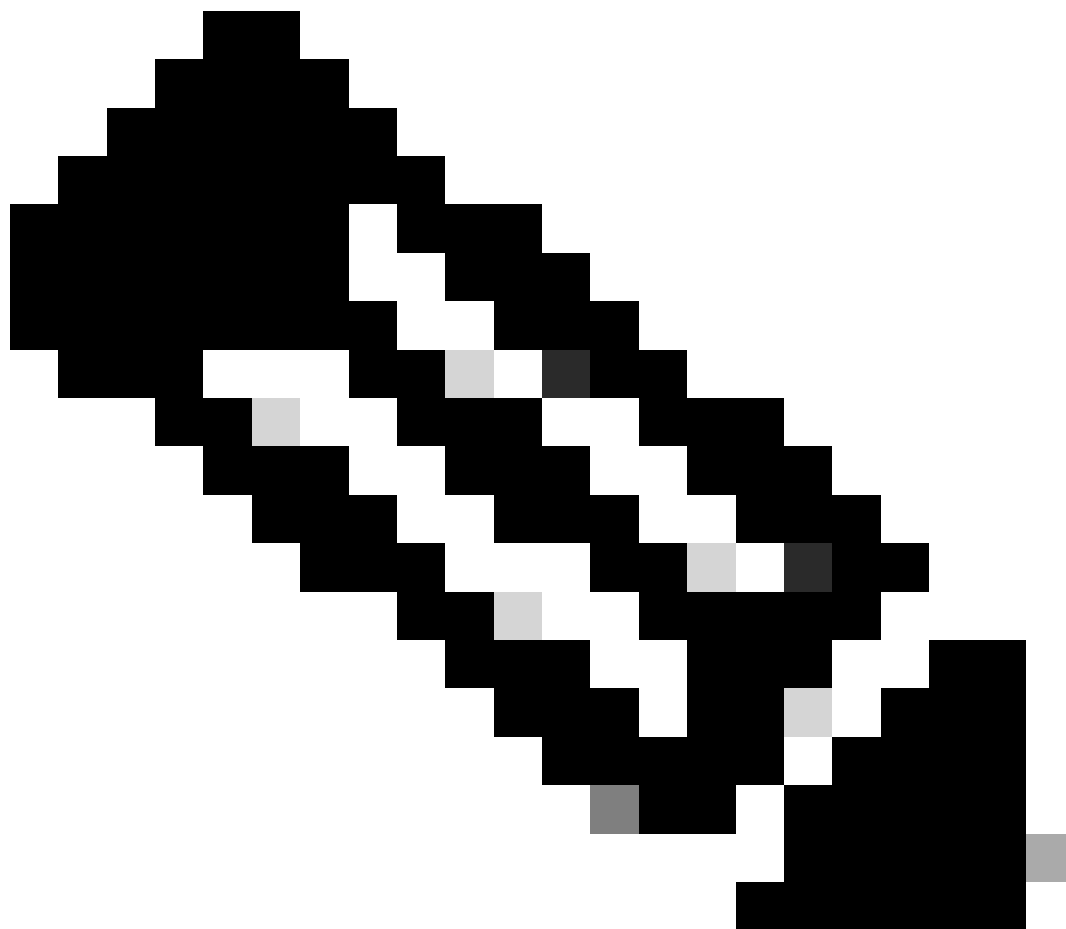
Figura 3: Fluxo problemático



Note: Aqui, todos os 15 segmentos são ocupados por win-sparta.com ao mesmo tempo, não deixando nenhum segmento para demonstração.local

Solução

- O comportamento padrão é um Pool de Threads Comum para todos os pontos de junção do AD
- No entanto, os administradores podem segmentar cada ponto de junção para ter seus próprios recursos.



Note: Quando a priorização do AD é aplicada, o padrão é 10 segmentos por pool de segmentos.

Consulte a Figura 4: Diagrama de fluxo do ponto conjunto reservado sob demanda



Figura 4: Fluxo da solução

Configuração Passo a Passo

Etapa1: Crie 2 pontos de junção do AD separados. Aqui temos, por exemplo: demo.local e win-sparta.com

Etapa 2: Criar priorização de ponto de junção após a criação do ponto de junção do AD.

Consulte a Figura 5:

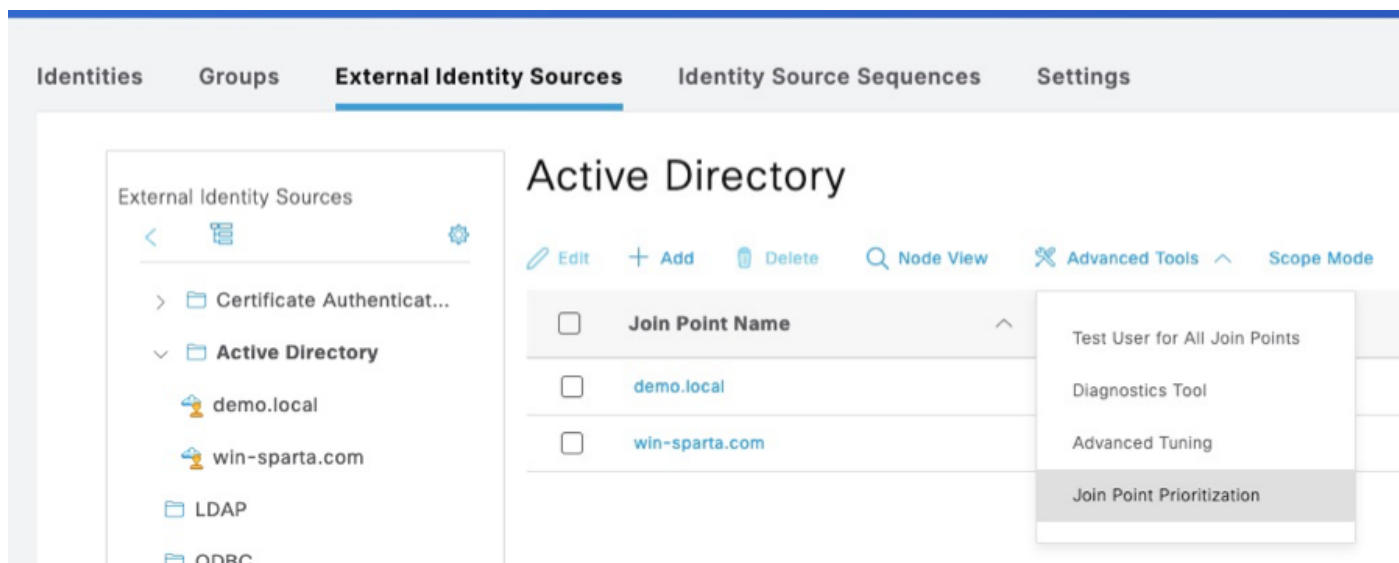


Imagem 5: Priorização de ponto de junção

Etapa 3: Em Join Point Prioritization (Priorização do ponto de adesão), selecione a PSN que você prefere reservar recursos dedicados do AD. Clique em Editar.

Consulte a Figura 6:

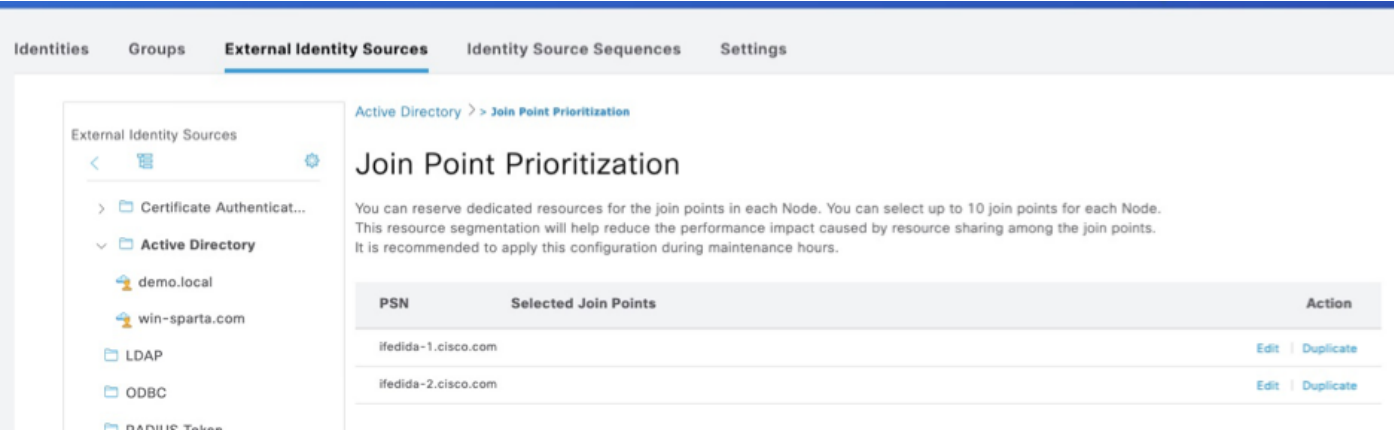


Imagem 6: Editar PSN

Etapa 4: Selecione o ponto de união preferido para o PSN preferido.

Consulte a Figura 7:

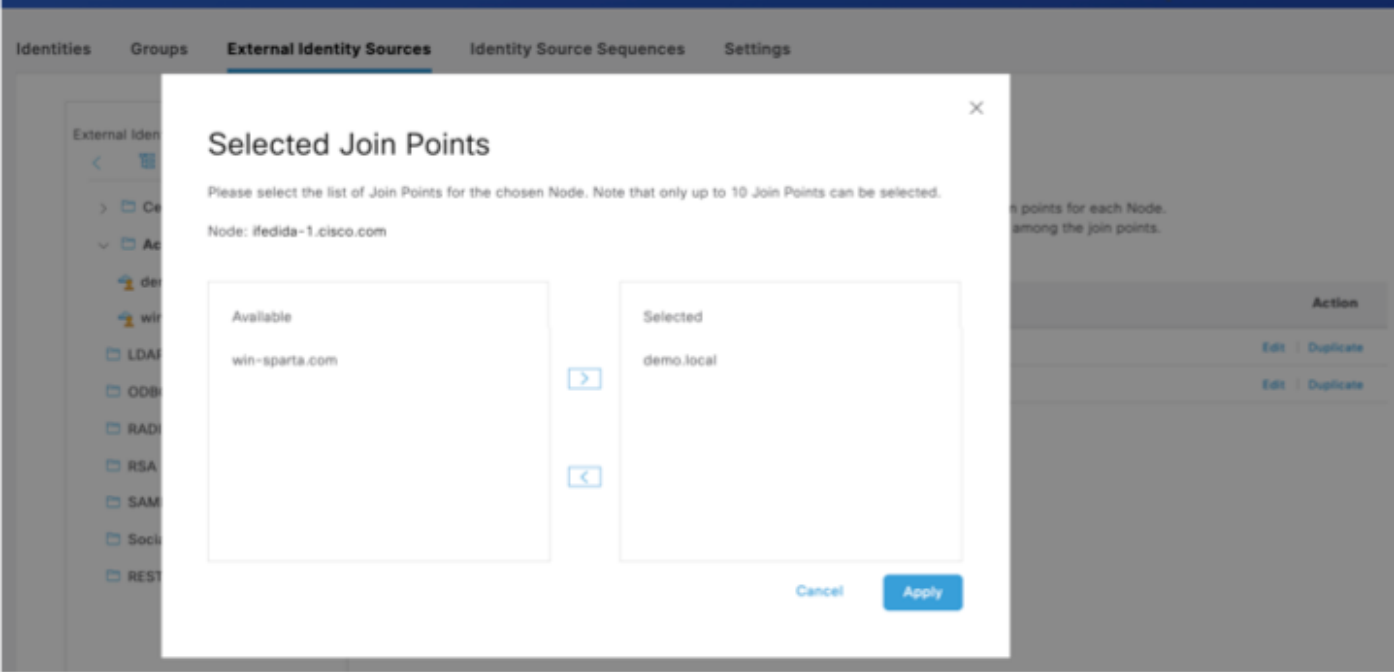


Figura 7: Ponto de Junção Selecionado



Note: Todos os pontos de junção não incluídos na priorização utilizam o pool de segmentos comuns, que tem um limite máximo de 15 segmentos.

Etapa 5: A priorização está finalizada

Consulte a Figura 8:

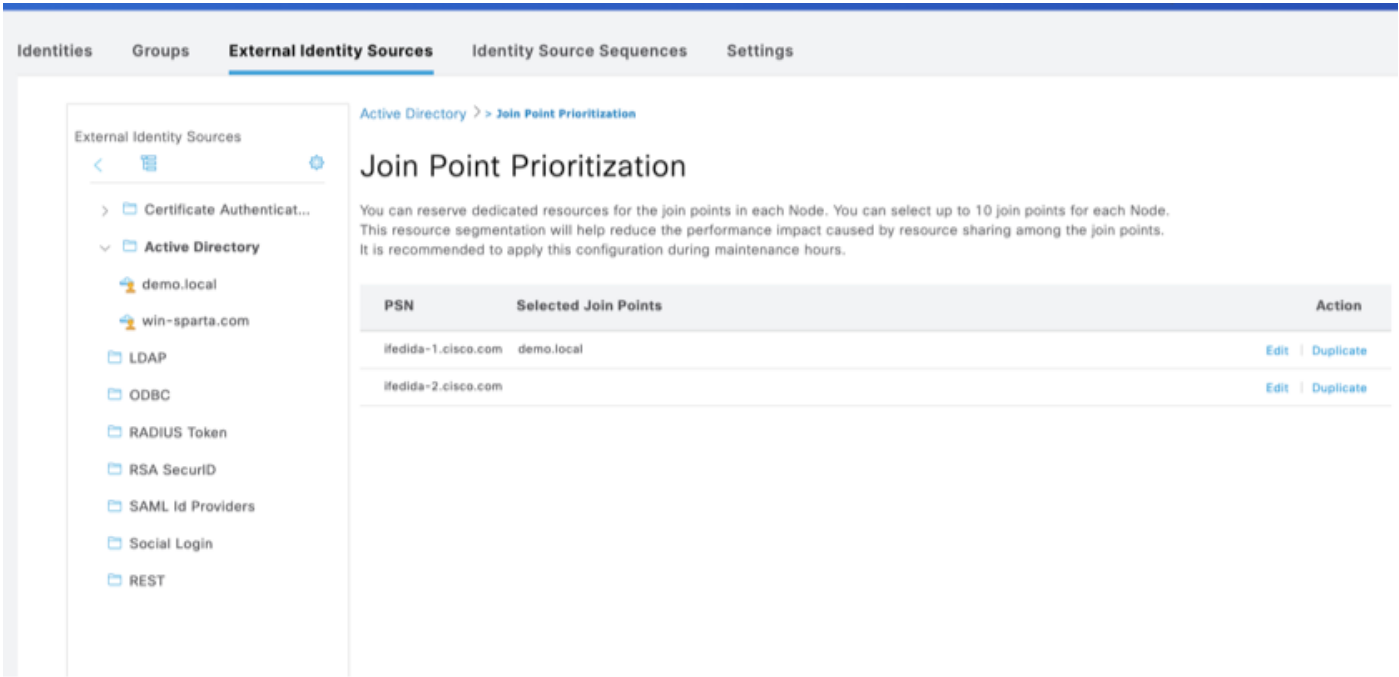
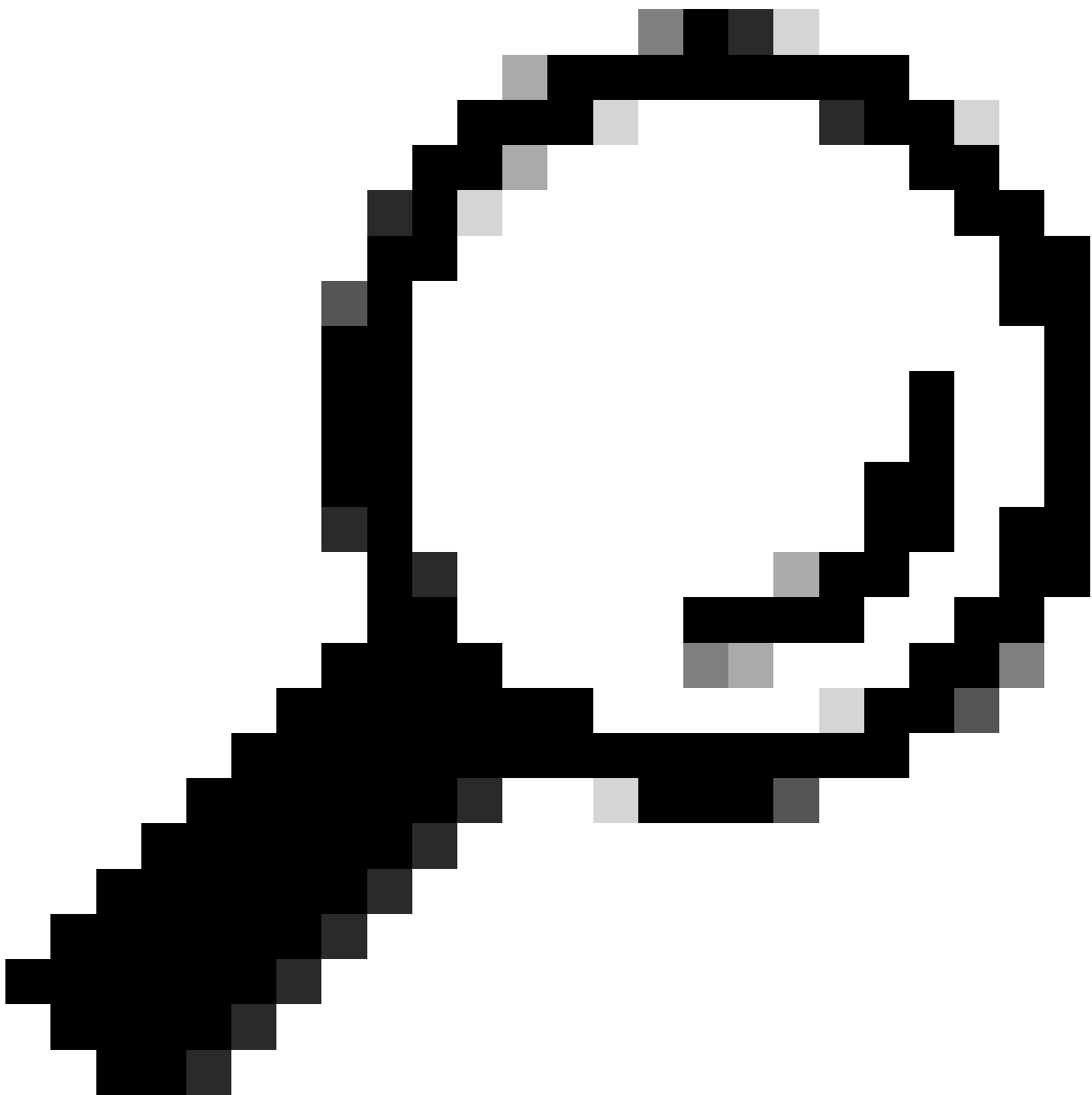


Figura 8: Configuração de priorização

Detalhes adicionais



Tip: Se desejar replicar as mesmas configurações para outras PSNs, você poderá usar a opção Duplicar. Selecione a PSN desejada e escolha o ponto de união a ser duplicado junto com a priorização original.

Consulte a Figura 9: Dica de configuração:

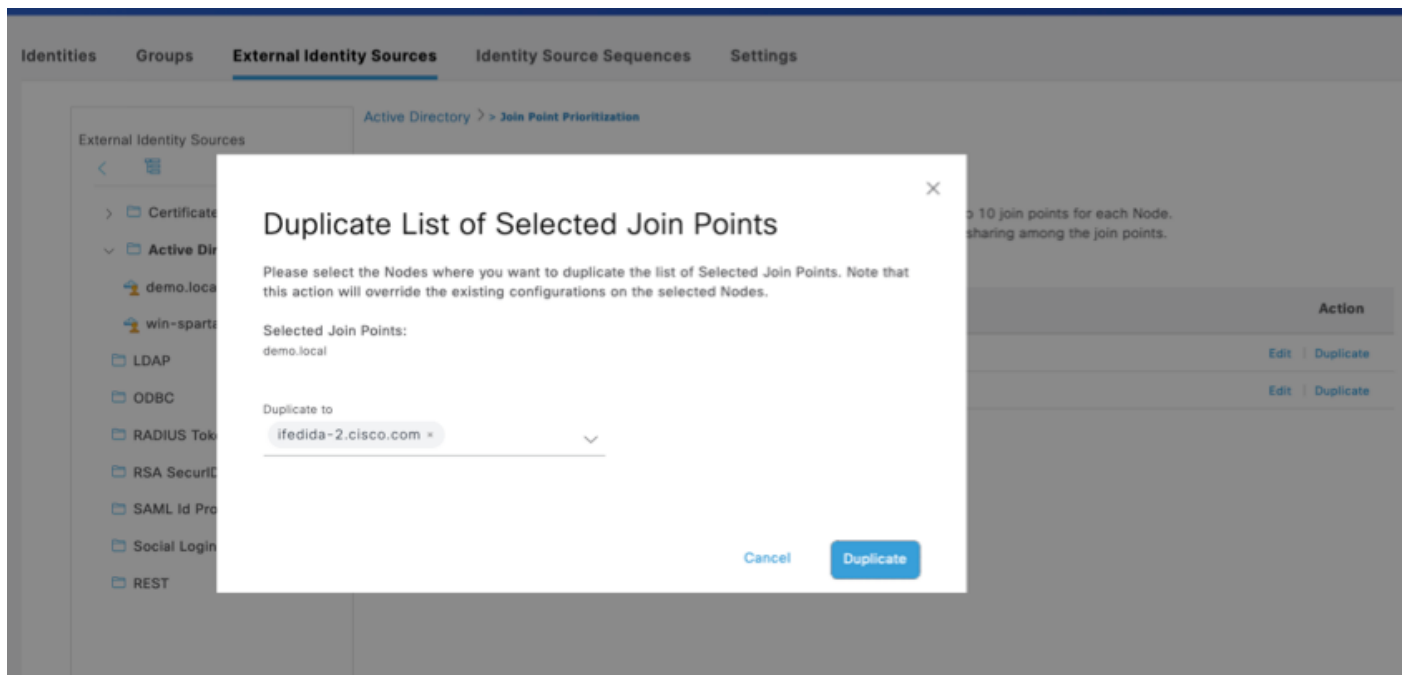


Figura 9: Configuração de Priorização Duplicada

Etapa 6: Lista Final após Duplicação

Consulte a Figura 10:

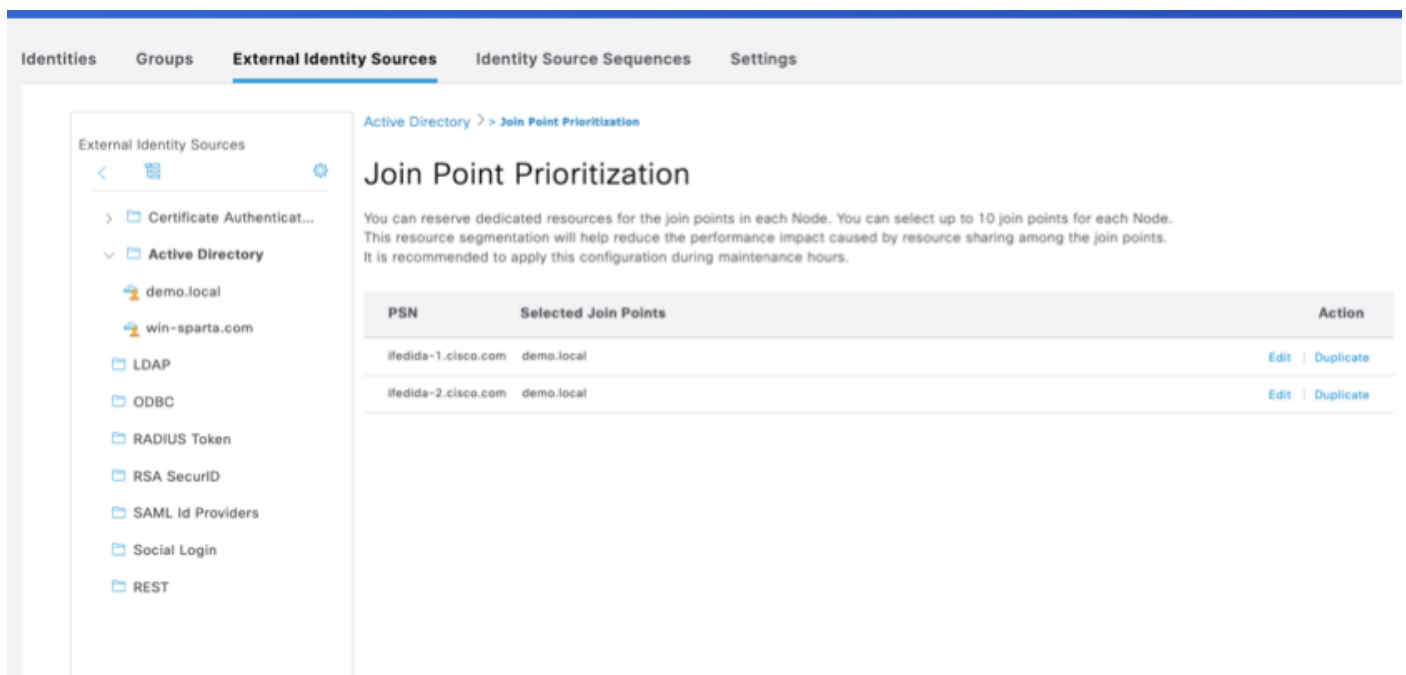


Imagem 10: Lista final após priorização

Troubleshooting

Verificação

Verifique as alterações de configuração. Navegue até: Operações > Relatórios > Auditorias > Alterar Auditoria de Configuração

Consulte a Figura 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

Imagem 11: Relatório de auditoria de configuração

Registro

- Ative o nível de depuração para logs AAA de tempo de execução.
 - Analisar prt-server.log
- Consulte a Figura 12:

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

Imagem 12: Configuração do Log de Depuração

Registrar trechos

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

EventHandler,2024-08-23 07:16:48,135,DEBUG,0x7fecd2ccc700, pool de threads padrão alocado : ADIDStore para IDP: win-sparta.com_wxETIH16Pk_106

prtr-server.log [INFO]: Quando definimos Recursos Dedicados:

- ActiveDirectoryIDStore,2024-09-08 16:52:01,048,INFO ,0x7f2452ccf700,Pool de threads alocados : ADThreadPool0 para IDP: win-sparta.com_wxETIH16Pk_106
- ActiveDirectoryIDStore,2024-09-08 16:57:11,258,INFO ,0x7f2452ccf700,Pool de threads alocados : ADThreadPool1 para IDP: demo.local_6EcNs6UzwX_89

prtr-server.log [INFO]:

- Antes de definirmos recursos dedicados:
 - EventHandler, 2024-09-02 08:45:54,673,INFO,0x7fafb793c700,Evento transmitido para o próximo pool de threads name=ADIDStore, queue size=1,EventDispatcher.cpp:757

- Depois de definirmos recursos dedicados:
 - EventHandler,2024-09-02 08:45:54,673,INFO ,0x7f4867ff9700,Evento transmitido para o próximo pool de threads name=ADThreadPool0, tamanho da fila=1,EventDispatcher.cpp:841

Para rastrear o uso do pool de threads de "ADThreadPool0":

1. 0x7f57792f7700,Evento passado para o próximo nome de pool de threads=ADThreadPool0 (poucos logs de StackID:0x7f57a4f761c0)
2. 0x7f57732c7700,Pilha: 0x7f57a4f761c0 Chamando o ActiveDirectoryIDStore: MethodCaller<ActiveDirectoryIDStore, PlainAuthenticateAndQueryEvent>
3. 0x7f57732c7700,cntx=0000210117,sens=ifedida-1/515863662/5273,CPMSessionID=C0A31430000000800018958,user=abcd,CallingStationID=[CAD] 956: CAD_PAPAuthenticate (abcd) chamado
4. 0x7f57732c7700,cntx=000210117,sens=ifedida-1/515863662/5273,CPMSessionID=C0A31430000000800018958,user=abcd,CallingStationID=[CAD] 1026: CAD_PAPAuthenticate (abcd) bem-sucedido
5. 0x7f57732c7700,Evento passado para o próximo nome de pool de threads=Principal

FAQ

Pergunta: Quantos pontos de associação do AD o ISE pode suportar?

Resposta: Você pode configurar até 50 pontos de união do Active Directory em uma única implantação do ISE.

Pergunta: Se eu tiver vários pontos de adesão ao AD, ainda posso usar a Priorização sob demanda?

Resposta: Yes

Pergunta: Qual é o tamanho de thread padrão sem Priorização para um único domínio?

Resposta: 15 segmentos

Pergunta: Se eu configurar a Priorização, como o cálculo é feito? Considere, um cenário de 3 Pontos de Junção - domain1.com, domain2.com e domain3.com com domain1.com não está configurado para Priorização e domain2.com e domain3.com estão configurados para Priorização.

Resposta: Se domain1 não estiver configurado para priorização, domain1.com utilizará os 15 segmentos comuns disponíveis, todos ao mesmo tempo. No entanto, como domain2.com e domain3.com são configurados com Priorização, eles usam 10 segmentos cada um por padrão e não seguem/utilizam o pool comum de 15 segmentos.

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.