

Begrijp On-Demand Resourcereservering voor AD op ISE 3.3 Patch 4

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereiste componenten](#)

[Achtergrondinformatie](#)

[Symptoom](#)

[Probleem](#)

[Oplossing](#)

[Configuratie stap voor stap](#)

[Aanvullende gegevens](#)

[Probleemoplossing](#)

[Verificatie](#)

[Logboekregistratie](#)

[Logfragmenten](#)

[FAQ](#)

Inleiding

Dit document beschrijft ongeveer On-Demand Resource Reservation for Active Directory op ISE 3.3 Patch 4

Voorwaarden

Kennis over Cisco Identity Services Engine (ISE)

Kennis van Active Directory (AD)

Kennis over ISE- en AD-integratie

Vereiste componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies

- Patch 4 voor Cisco Identity Services Engine 3.3
- Microsoft Windows Active Directory 2016 of laatste

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een

opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

AD-verificaties verlopen soms traag en mislukken uiteindelijk. Mogelijke redenen kunnen zijn ADID Queue beginnen te stapelen of Alle ADID Pool Threads worden uitgeput.

Meer informatie over ADID:

Een ADID, ook bekend als een voorname naam (DN), is een string die een object identificeert in de Active Directory-map. Ze worden gebruikt om objecten in het Active Directory-domein te lokaliseren en te beheren. ADID's zijn van cruciaal belang voor het beheer van gebruikersaccounts, machtigingen en andere bronnen binnen een Active Directory-omgeving.

Een typische ADID moet er zo uitzien: CN=John Doe, OU=Sales, DC=example, DC=com; waarbij,

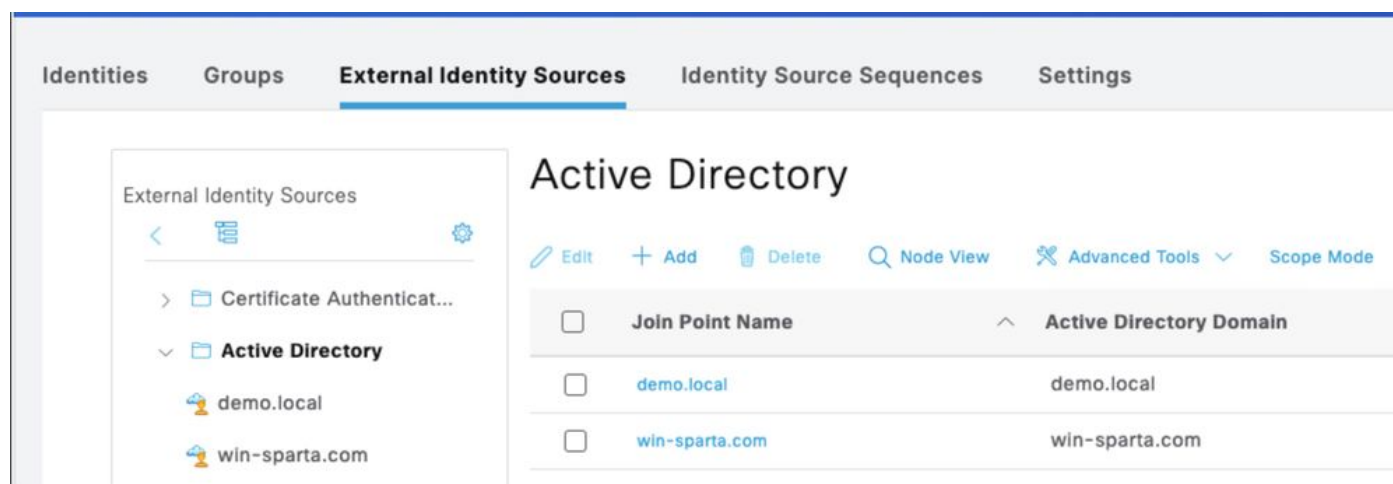
CN=onbekende schimmel: Vertegenwoordigt de algemene naam van de gebruiker, onbekende.

OU=Sales: Vertegenwoordigt de organisatorische eenheid (OU) waar de gebruiker, in dit geval, de Verkoopafdeling behoort.

DC=voorbeeld, DC=com: Vertegenwoordigt de domeincomponenten, die example.com zijn.

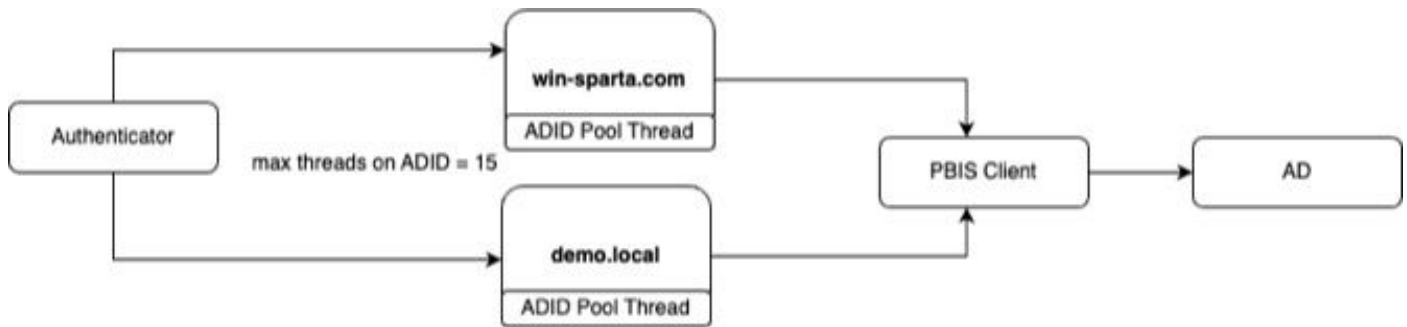
Voorbeeld:

Raadpleeg afbeelding 1: Een typische AD Join Point-configuratie



Afbeelding 1: AD Join points

Raadpleeg afbeelding 2: Een typisch AD-stroomschema met 2 verbindingspunten



Afbeelding 2: Een typisch AD Flow-diagram

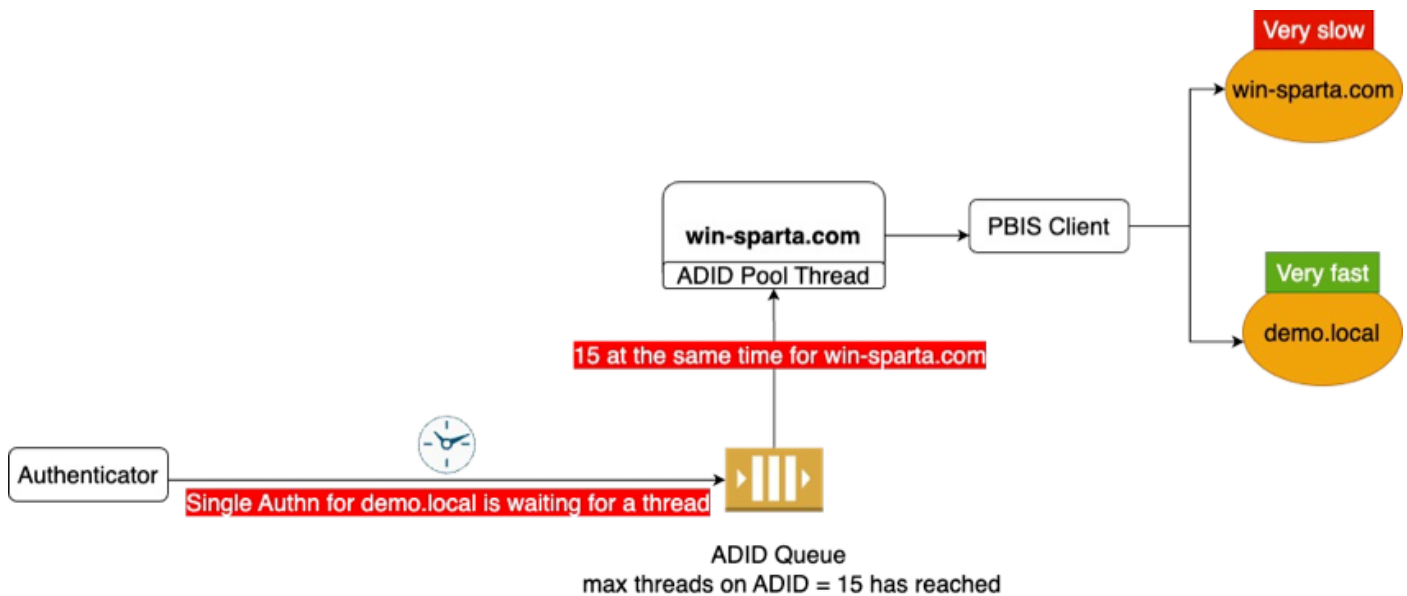
Symptoom

Langzaam toetreden tot punt onder dezelfde ADID-draadpool

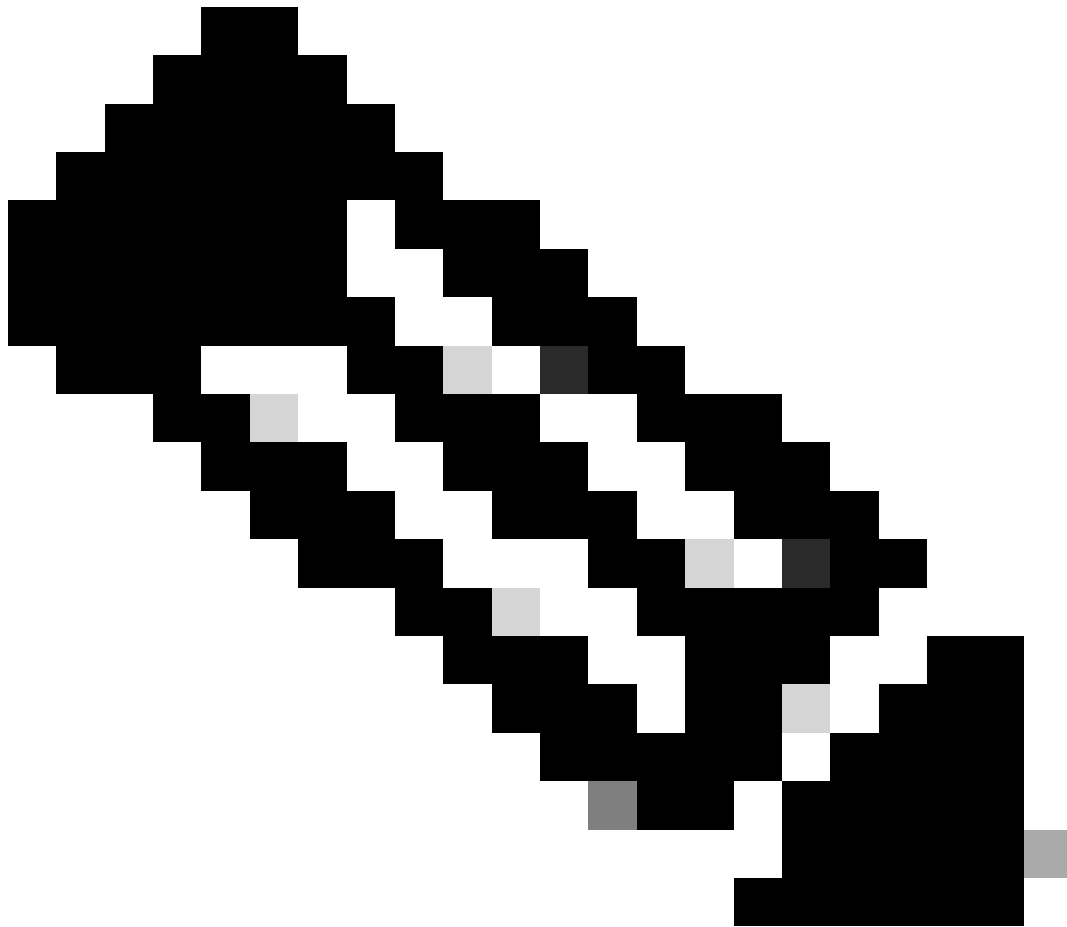
Probleem

1. Wat zouden de gevolgen zijn als een van de gemeenschappelijke punten erg traag zou zijn?
Bijvoorbeeld, als 15 authenticaties tegelijkertijd naar ISE worden verzonden voor "demo.local" en "demo.local" ongewoon traag is, zouden we moeten wachten op de reactie van "demo.local" voordat we de volgende win-sparta authenticatie behandelen.
2. Wat als beide Join Points dezelfde ADID Thread Pool delen onder One Join Point?

Raadpleeg afbeelding 3: Stroomschema van het langzame gewrichtspunt



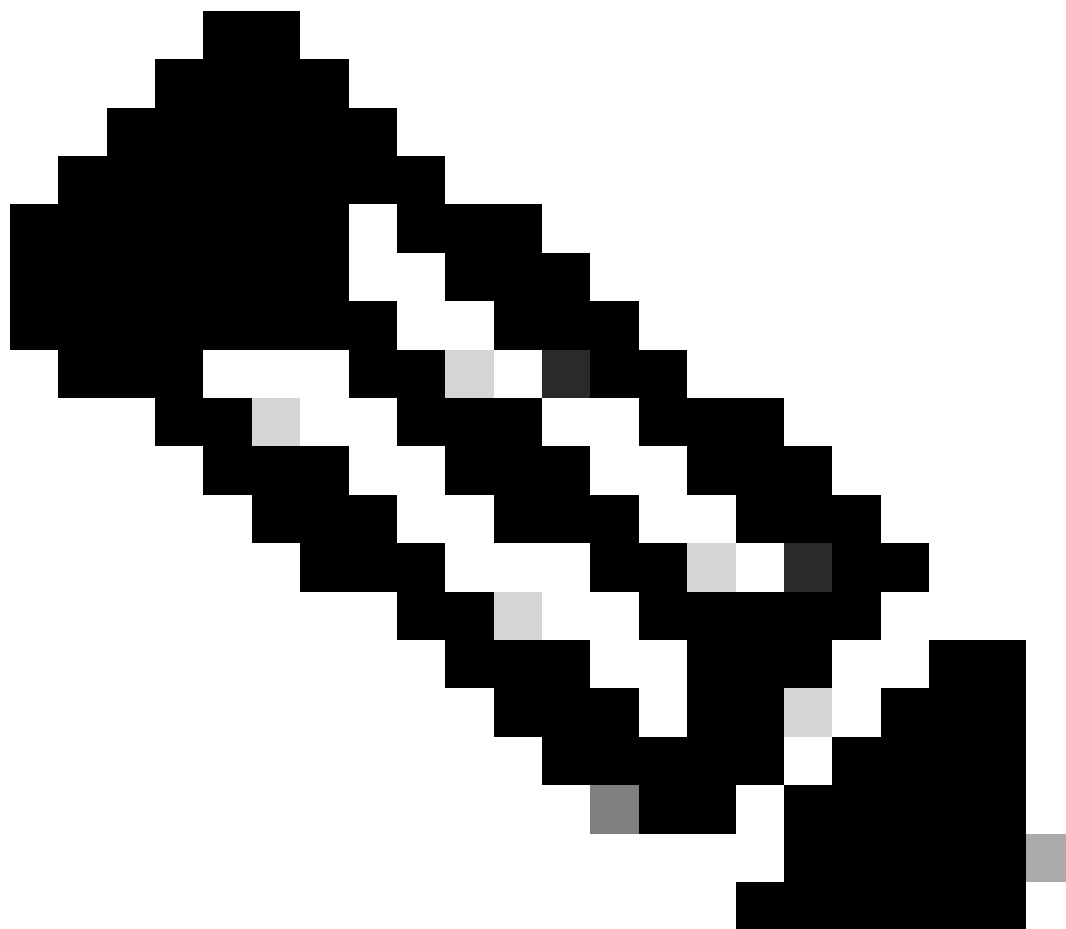
Afbeelding 3: Problematische stroom



Opmerking: Hier worden alle 15 Threads tegelijk bezet door win-sparta.com zonder thread voor demo.local

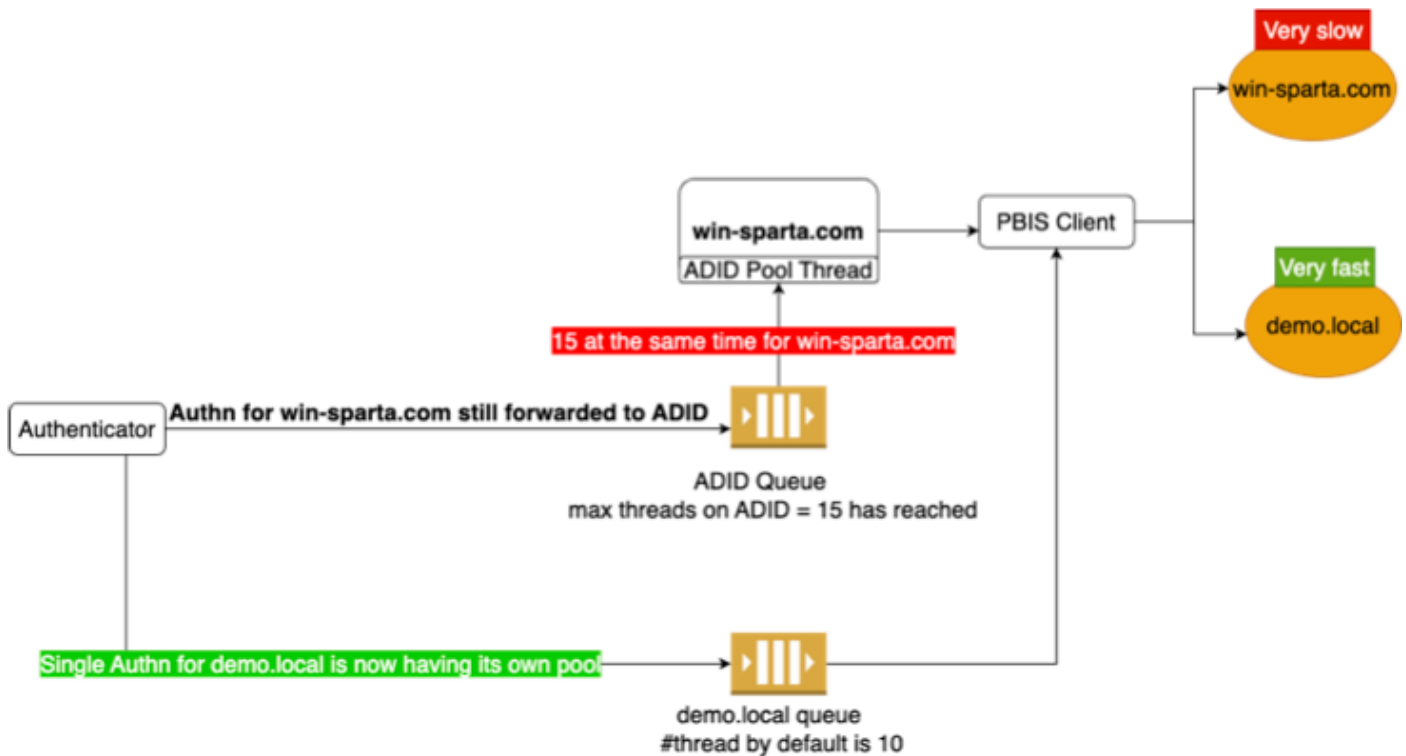
Oplossing

- Standaardgedrag is een gemeenschappelijke draadpool voor alle AD-samenvoegpunten
- Admins kan echter elk samenwerkingspunt segmenteren om eigen middelen te hebben.



Opmerking: Als AD Priorization wordt toegepast, is de standaardinstelling 10 Threads per Thread Pool.

Raadpleeg afbeelding 4: Stroomschema van het gereserveerde verbindingspunt op verzoek



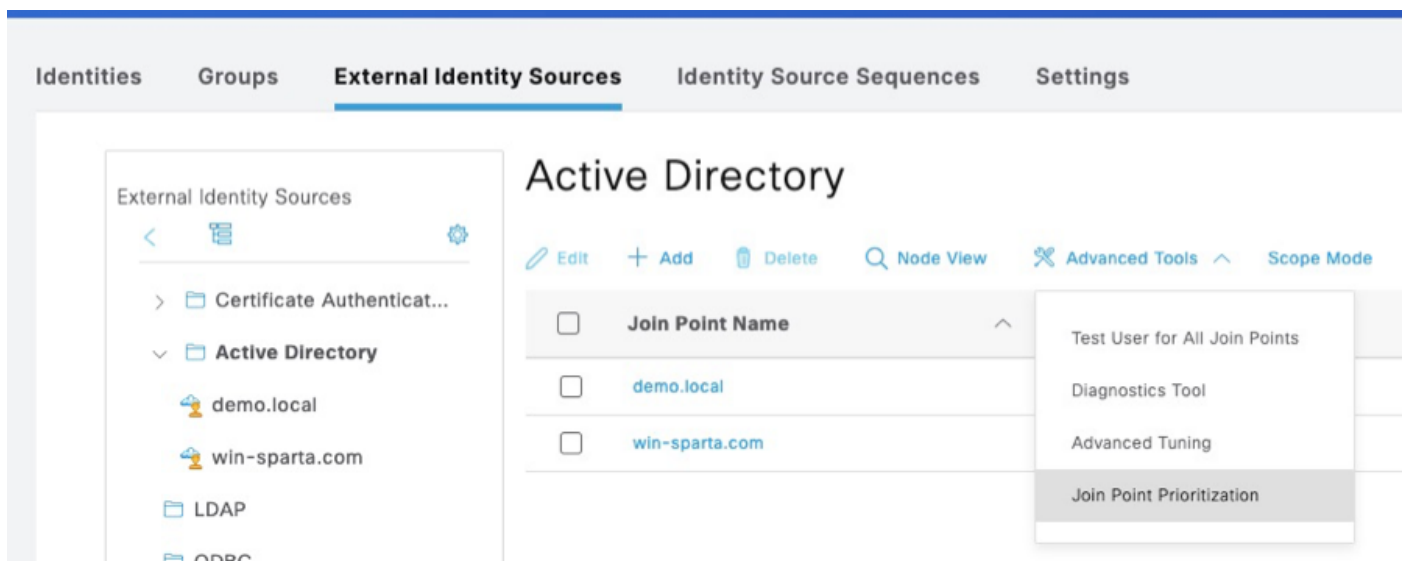
Afbeelding 4: Flow van oplossing

Configuratie stap voor stap

Stap 1: Maak 2 afzonderlijke AD Join points. Hier hebben we bijvoorbeeld: demo.local en win-sparta.com

Stap 2: Prioritering samenvoegen na samenvoegen van AD-punt maken

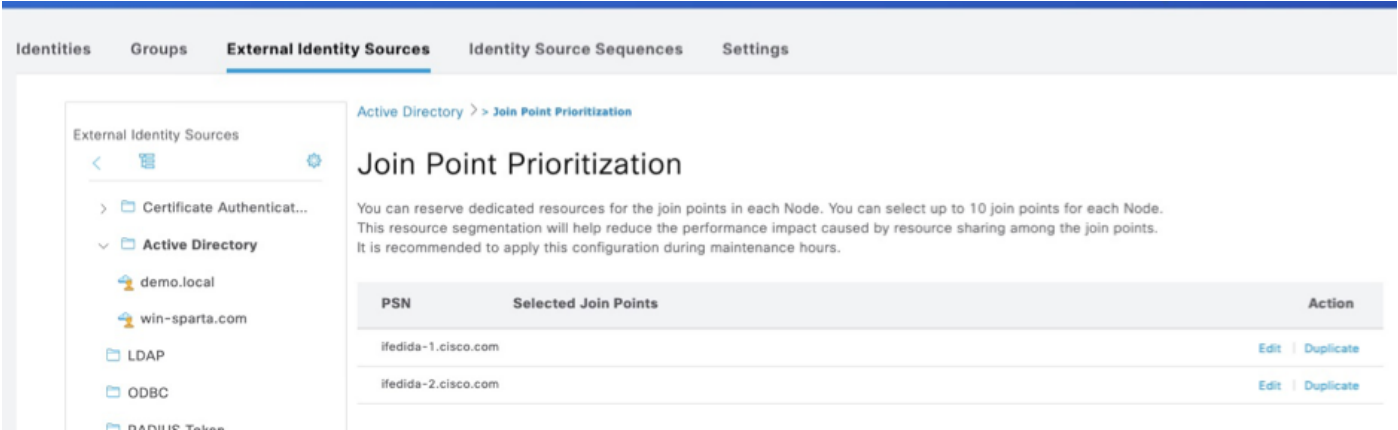
Raadpleeg afbeelding 5:



Afbeelding 5: Prioritering samenvoegen

Stap 3: Selecteer onder Prioritering samenvoegen de PSN die u wilt reserveren voor speciale AD-bronnen. Klik op Edit (Bewerken).

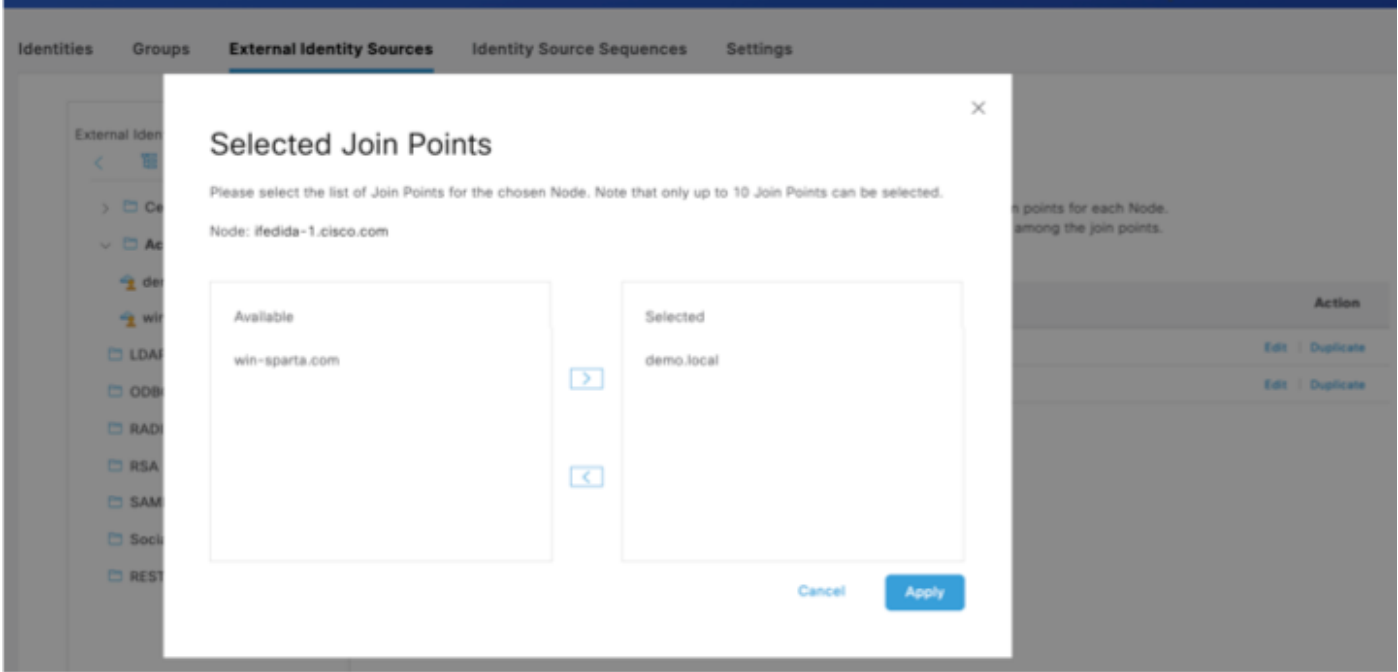
Raadpleeg afbeelding 6:



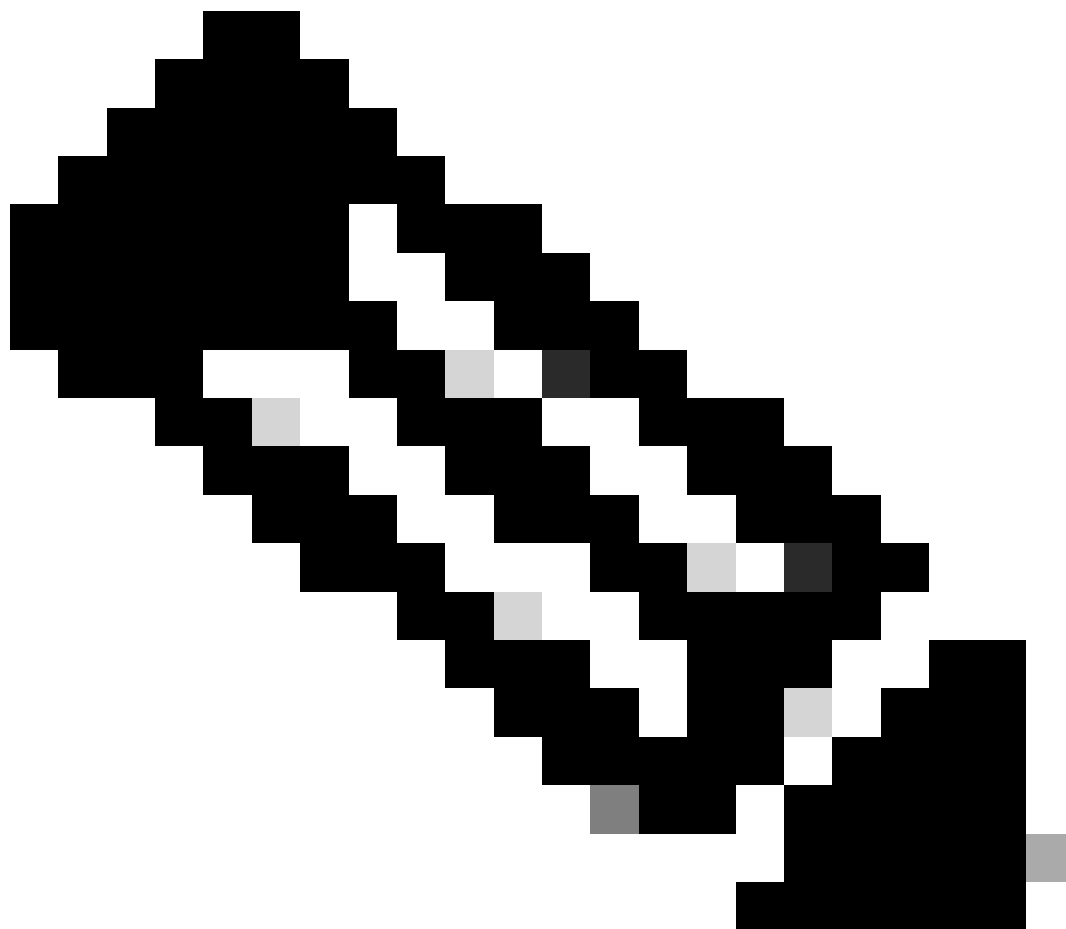
Afbeelding 6: PSN bewerken

Stap 4: Selecteer het gewenste Join Point voor het voorkeurspensioen.

Raadpleeg afbeelding 7:



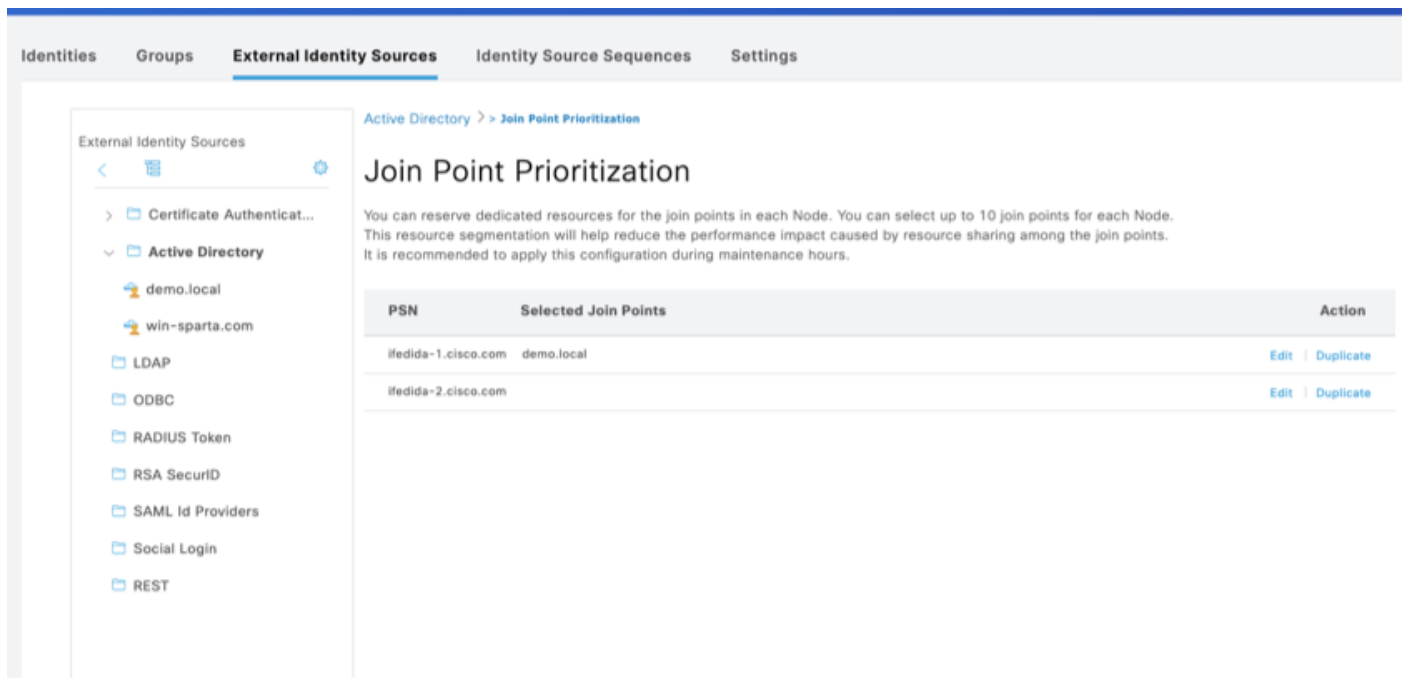
Afbeelding 7: Geselecteerd Join Point



Opmerking: Alle join points die niet in de prioritering zijn opgenomen, maken gebruik van de Common Thread-pool, die een maximum van 15 threads heeft.

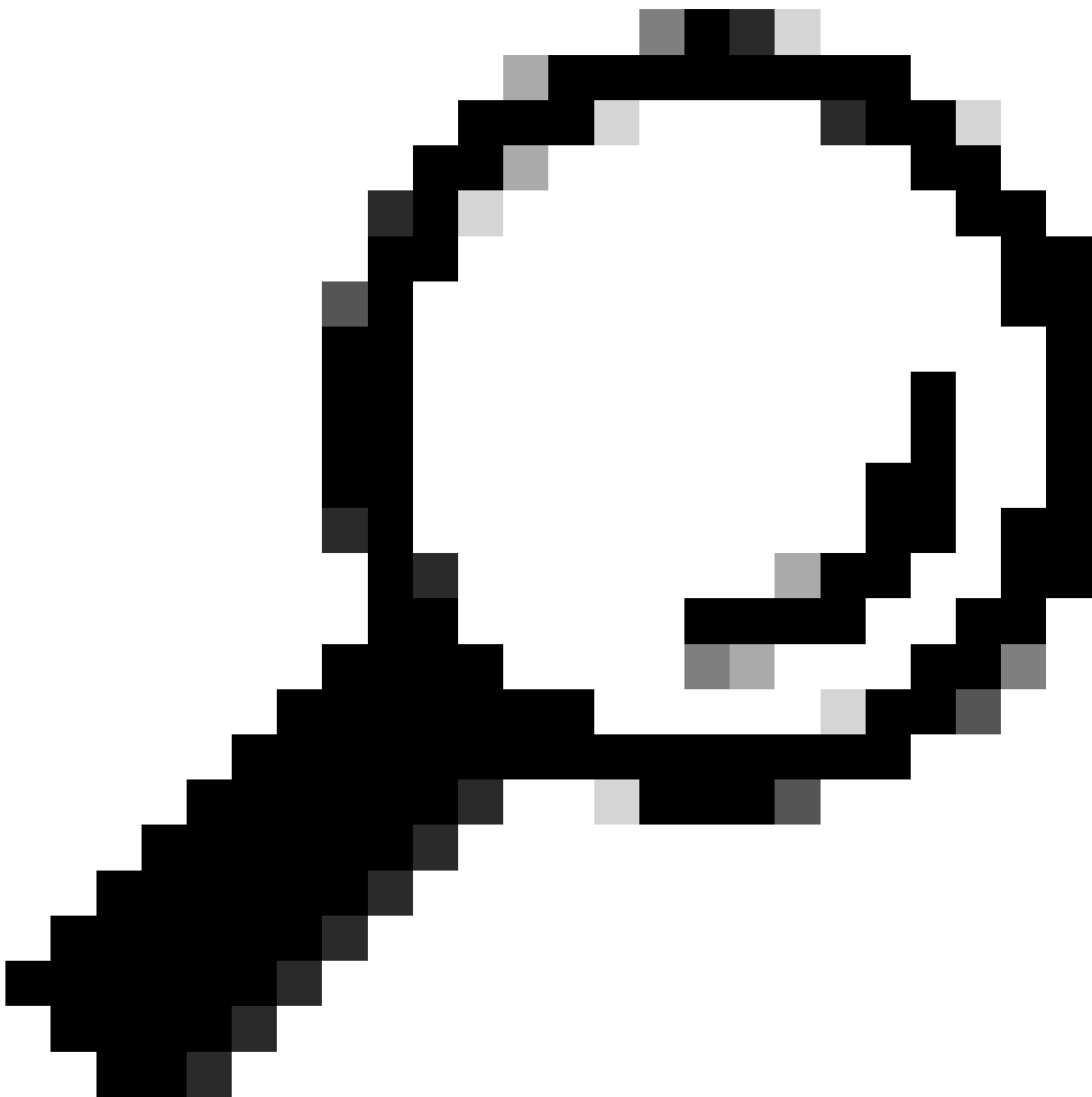
Stap 5: Prioritering is voltooid

Raadpleeg Illustratie 8:



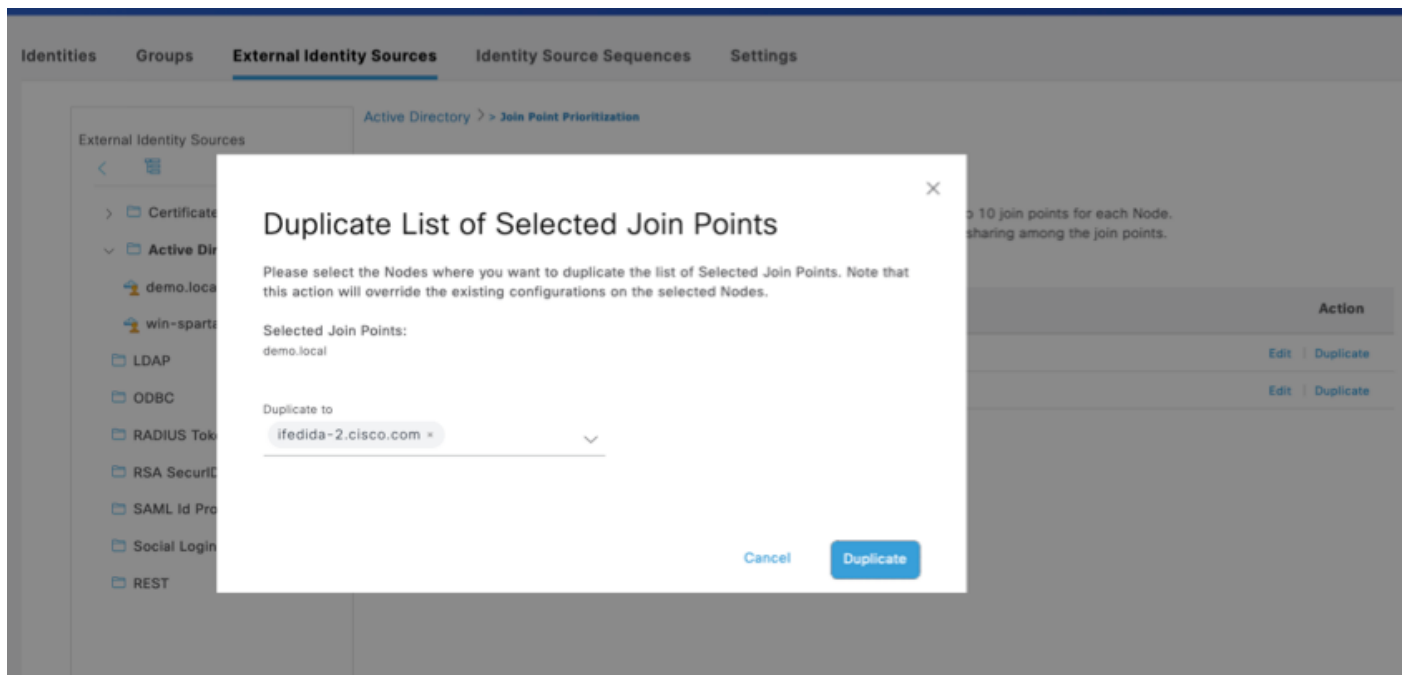
Afbeelding 8: Prioritering configuratie

Aanvullende gegevens



Tip: Als u dezelfde instellingen wilt herhalen voor andere PSN's, kunt u de optie Dupliceren gebruiken. Selecteer het gewenste PSN en kies het Join Point dat moet worden gedupliceerd, samen met de oorspronkelijke Prioritatie.

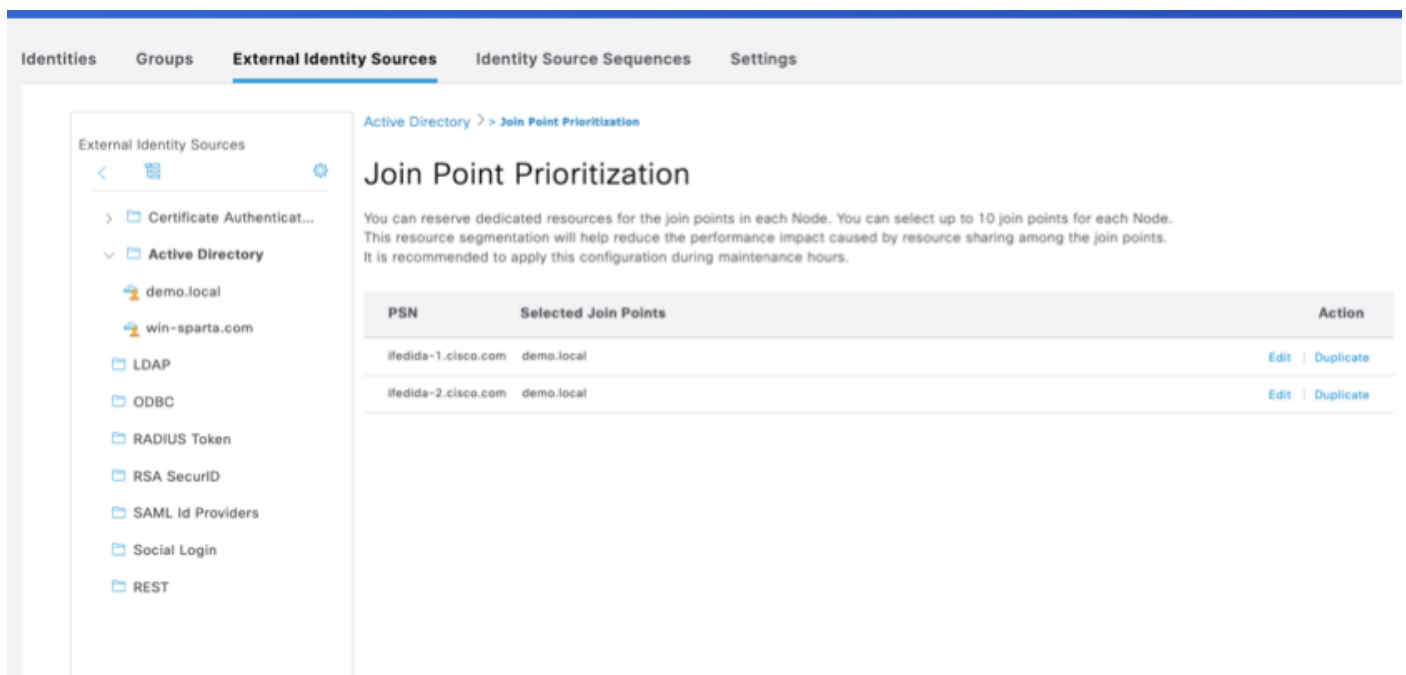
Raadpleeg afbeelding 9: Configuratie-tip:



Beeld 9: Dubbele prioriteitsconfiguratie

Stap 6: Definitieve lijst na duplicatie

Raadpleeg afbeelding 10:



Afbeelding 10: Definitieve lijst na prioritering

Probleemoplossing

Verificatie

Controleer de wijzigingen in de configuratie. Navigeren naar: Operations > Rapporten > Audits > Change Configuration Audit

Raadpleeg afbeelding 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

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

Afbeelding 11: Auditrapport Config

Logboekregistratie

- Debug niveau inschakelen voor runtime-AAA-logbestanden.
 - Prt-server.log analyseren
- Raadpleeg afbeelding 12:

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

Afbeelding 12: Debug Log Config

Logfragmenten

prtr-server.log [DEBUG]: Standaard log:

EventHandler,2024-08-23 07:16:48,135,DEBUG,0x7fecd2cc700,Toegewezen standaard thread pool : Verder opslaan in IDP: win-sparta.com_wxETIH16Pk_106

prtr-server.log [INFO]: Wanneer we speciale bronnen instellen:

- ActiveDirectoryIDStore,2024-09-08 16:52:01,048,INFO,0x7f2452cf700,Toegewezen thread pool : ADThreadPool0 naar IDP : win-sparta.com_wxETIH16Pk_106
- ActiveDirectoryIDStore,2024-09-08 16:57:11,258,INFO,0x7f2452cf700,Toegewezen thread pool : ADThreadPool1 naar IDP : demo.local_6ecNs6UZWX_89

prtr-server.log [INFO]:

- Voordat we de beschikbare middelen hebben ingesteld:
 - EventHandler, 2024-09-02 08:45:54,673,INFO,0x7f 793c700, gebeurtenis doorgegeven aan de volgende thread pool naam=ADIDStore, wachtrij grootte=1,EventDispatcher.cpp:757

- Nadat we de beschikbare middelen hebben ingesteld:
 - EventHandler,2024-09-02 08:45:54,673,INFO, 0x7f4867ff9700,Genoemde gebeurtenis aan de volgende naam van de draadpool=ADThreadPool0, wachtrijs grootte=1,EventDispatcher.cpp:841

Gebruik van "ADThreadPool0" volgen:

1. 0x7f57792f7700, gebeurtenis doorgegeven aan de volgende thread pool name=ADThreadPool0 (een paar logs terug StackID:0x7f57a4f761c0)
2. 0x7f57732c7700,Stapel: 0x7f57a4f761c0 ActiveDirectoryIDS bellen: MethodeCaller<ActiveDirectoryIDSSStore, PlainAuthenticate en QueryEvent>
3. 0x7f57732c7700,cntx=0000210117,sen=ifedida-1/515863662/5273,CPMSessionID=C0A31430000000800018958,user=abcd,CallingStationID=[CAD] 956: CAD_PAPAuthenticate (abcd)
4. 0x7f57732c7700,cntx=0000210117,sen=ifedida-1/515863662/5273,CPMSessionID=C0A31430000000800018958,user=abcd,CallingStationID=[CAD] 1026: CAD_PAPAuthenticate (abcd) geslaagd
5. 0x7f57732c7700, gebeurtenis doorgegeven aan de volgende thread pool name=Main

FAQ

Vraag: Hoeveel AD Join points kan ISE ondersteunen?

Antwoord: U kunt maximaal 50 Active Directory-samenvoegingspunten configureren op één ISE-implementatie.

Vraag: Als ik meerdere AD Join Points heb, kan ik dan nog steeds On-Demand prioritering gebruiken?

Antwoord: Ja

Vraag: Wat is de standaarddraadgrootte zonder prioritering voor een enkel domein?

Antwoord: 15 threads

Vraag: Als ik prioritering configureer, hoe wordt de berekening uitgevoerd? Overweeg bijvoorbeeld een 3 Join Point-scenario - domain1.com, domain2.com en domain3.com met domain1.com is niet geconfigureerd voor prioritering en domain2.com en domain3.com en zijn geconfigureerd voor prioritering.

Antwoord: Als domain1 niet is geconfigureerd voor prioritering, maakt domain1.com gebruik van de 15 gemeenschappelijke threads die beschikbaar zijn - allemaal tegelijk. Aangezien domain2.com en domain3.com echter zijn geconfigureerd met prioritering, gebruiken ze standaard 10 threads en gebruiken ze de gebruikelijke 15 threads pool niet.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.