On-Demand-Ressourcenreservierung für AD auf ISE 3.3, Patch 4

Inhalt

Einleitung

Dieses Dokument beschreibt die On-Demand-Ressourcenreservierung für Active Directory auf der ISE 3.3 Patch 4.

Voraussetzungen

Kenntnisse zur Cisco Identity Services Engine (ISE)

Kenntnisse über Active Directory (AD)

Kenntnisse über ISE und AD-Integration

Erforderliche Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen

- Patch 4 der Cisco Identity Services Engine 3.3
- Microsoft Windows Active Directory 2016 oder neueste

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten

Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

AD-Authentifizierungen sind manchmal langsam und schlagen schließlich fehl. Mögliche Gründe können die ADID-Warteschlange sein, die mit dem Stapeln beginnt, oder alle ADID-Pool-Threads, die erschöpft sind.

Weitere Informationen zu ADID:

Eine ADID, auch Distinguished Name (DN) genannt, ist eine Zeichenfolge, die ein Objekt innerhalb des Active Directory-Verzeichnisses eindeutig identifiziert. Sie werden verwendet, um Objekte in der Active Directory-Domäne zu suchen und zu verwalten. ADIDs sind für die Verwaltung von Benutzerkonten, Berechtigungen und anderen Ressourcen in einer Active Directory-Umgebung von entscheidender Bedeutung.

Eine typische ADID muss wie folgt aussehen: CN=Max Mustermann,OU=Vertrieb,DC=Beispiel,DC=com; Dabei gilt,

CN=Karl Müller: Stellt den allgemeinen Benutzernamen John Doe dar.
OU = Vertrieb: Stellt die Organisationseinheit dar, zu der der Benutzer gehört, in diesem Fall die Vertriebsabteilung.
DC=Beispiel,DC=com: Stellt die Domänenkomponenten dar, nämlich example.com.

Beispiele:

Siehe Bild 1: Eine typische AD-Join-Point-Konfiguration

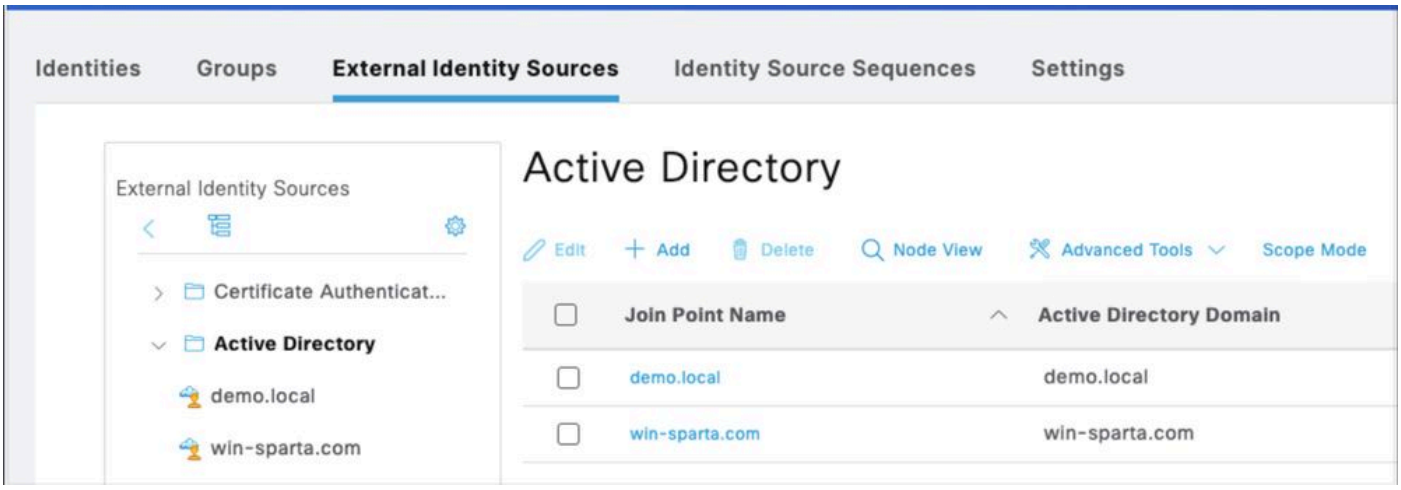


Abbildung 1: AD-Verknüpfungspunkte

Siehe Bild 2: Ein typisches AD-Flussdiagramm mit 2 Verbindungspunkten

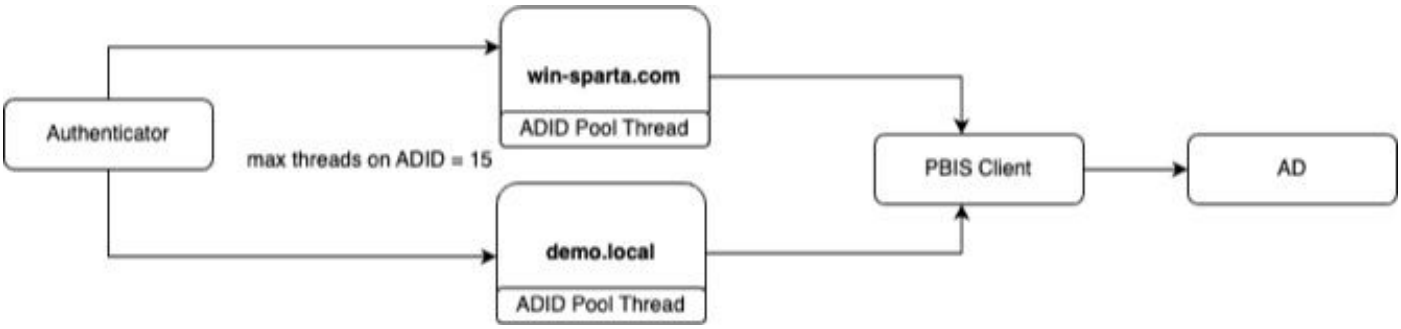


Abbildung 2: Ein typisches AD-Flussdiagramm

Symptom

Langsamer Verbindungspunkt unter demselben ADID-Thread-Pool

Problem

1. Welche Folgen hätte es, wenn einer der Verbindungspunkte sehr langsam wäre? Wenn beispielsweise 15 Authentifizierungen gleichzeitig für "demo.local" und "demo.local" an die ISE gesendet werden, was ungewöhnlich langsam ist, müssen wir auf die Antwort von "demo.local" warten, bevor wir die anschließende win-sparta-Authentifizierung handhaben können.
2. Was ist, wenn beide Verknüpfungspunkte denselben ADID-Thread-Pool unter einem Verknüpfungspunkt teilen?

Siehe Bild 3: Flussdiagramm des langsamen Gelenkpunktes

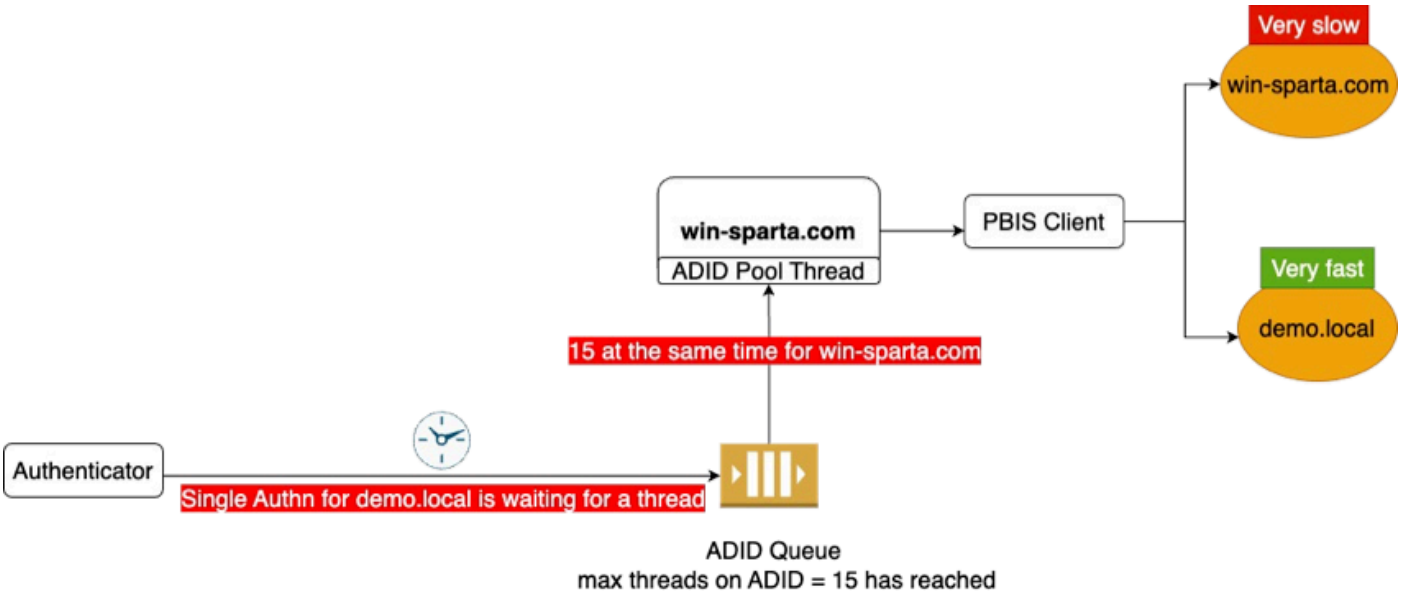
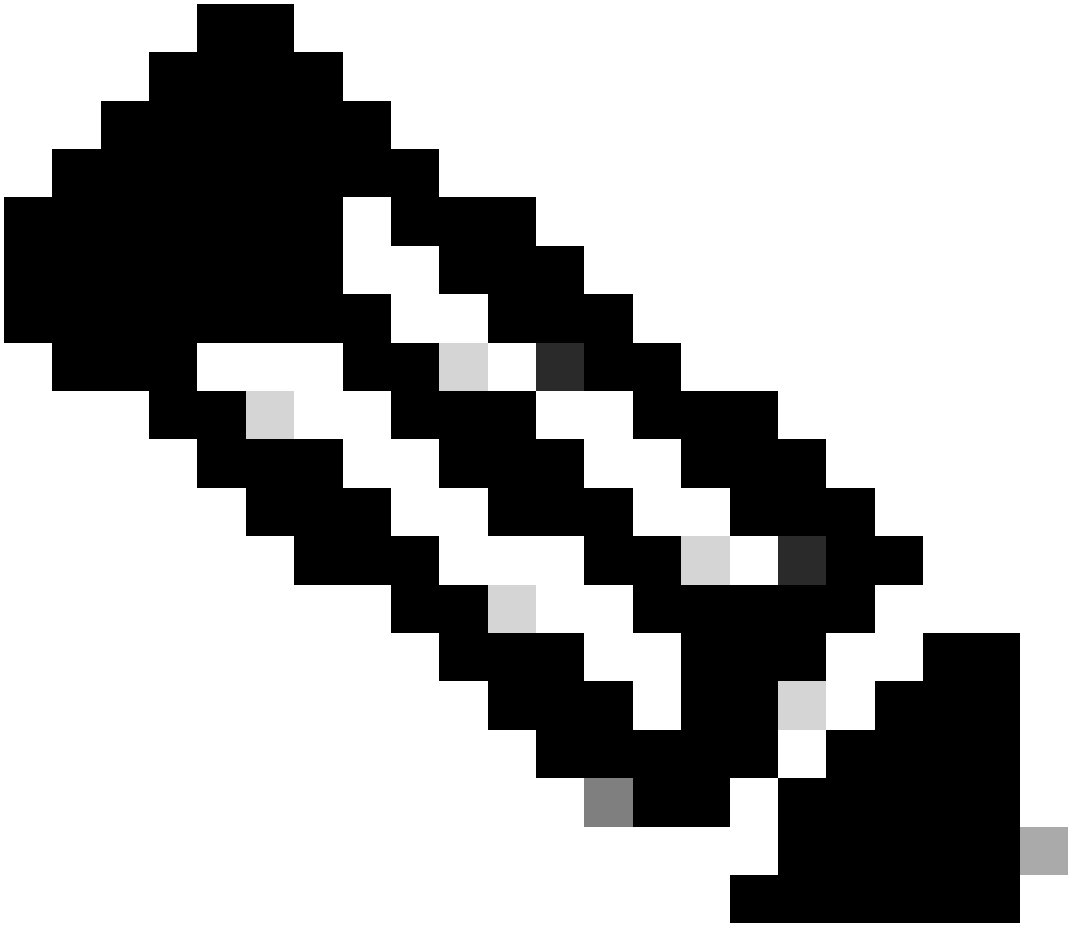


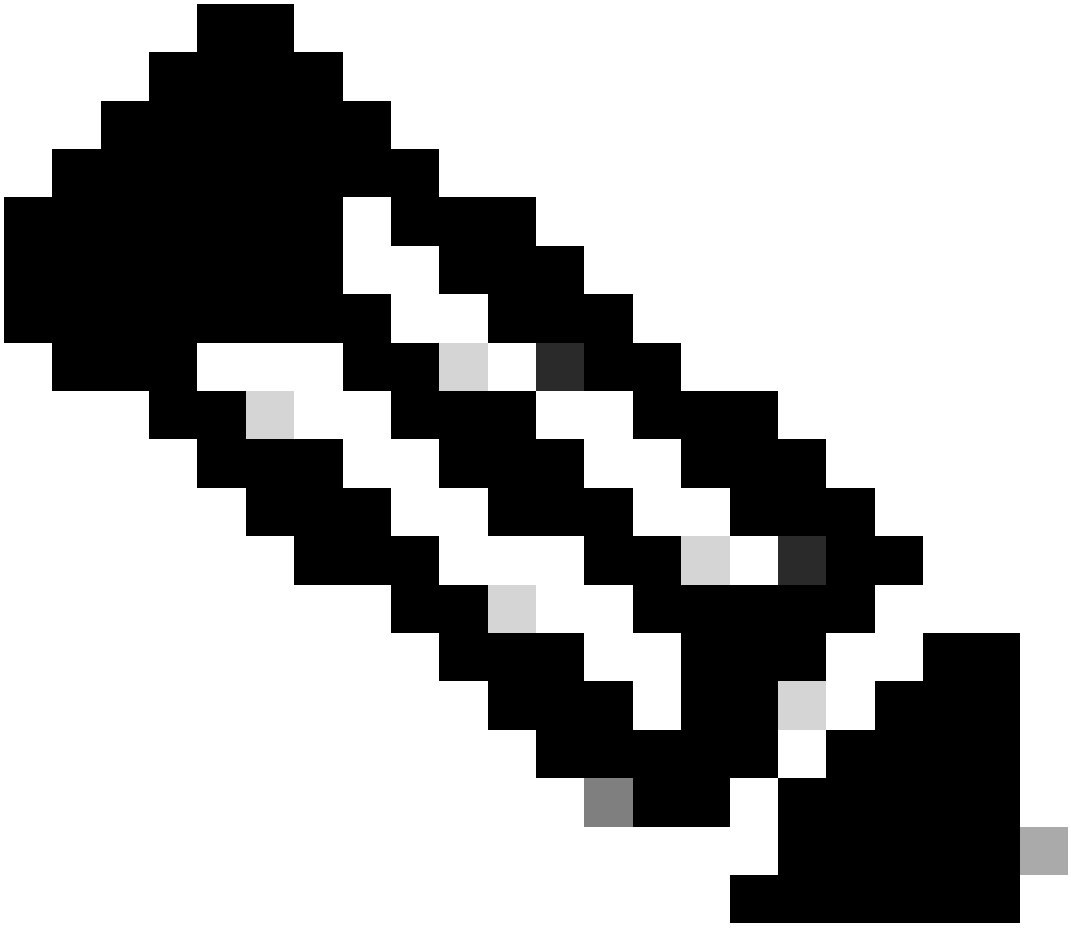
Abbildung 3: Problematische Strömung



Anmerkung: Hier werden alle 15 Threads gleichzeitig von win-sparta.com belegt, sodass kein Thread für demo.local übrig bleibt

Lösung

- Das Standardverhalten ist ein gemeinsamer Threadpool für alle AD-Verknüpfungspunkte.
- Administratoren können jedoch jeden Verknüpfungspunkt segmentieren, um über eigene Ressourcen zu verfügen.



Anmerkung: Bei Anwendung der AD-Priorisierung lautet der Standardwert 10 Threads pro Threadpool.

Siehe Bild 4: Flussdiagramm des On-Demand-reservierten Gelenkpunkts

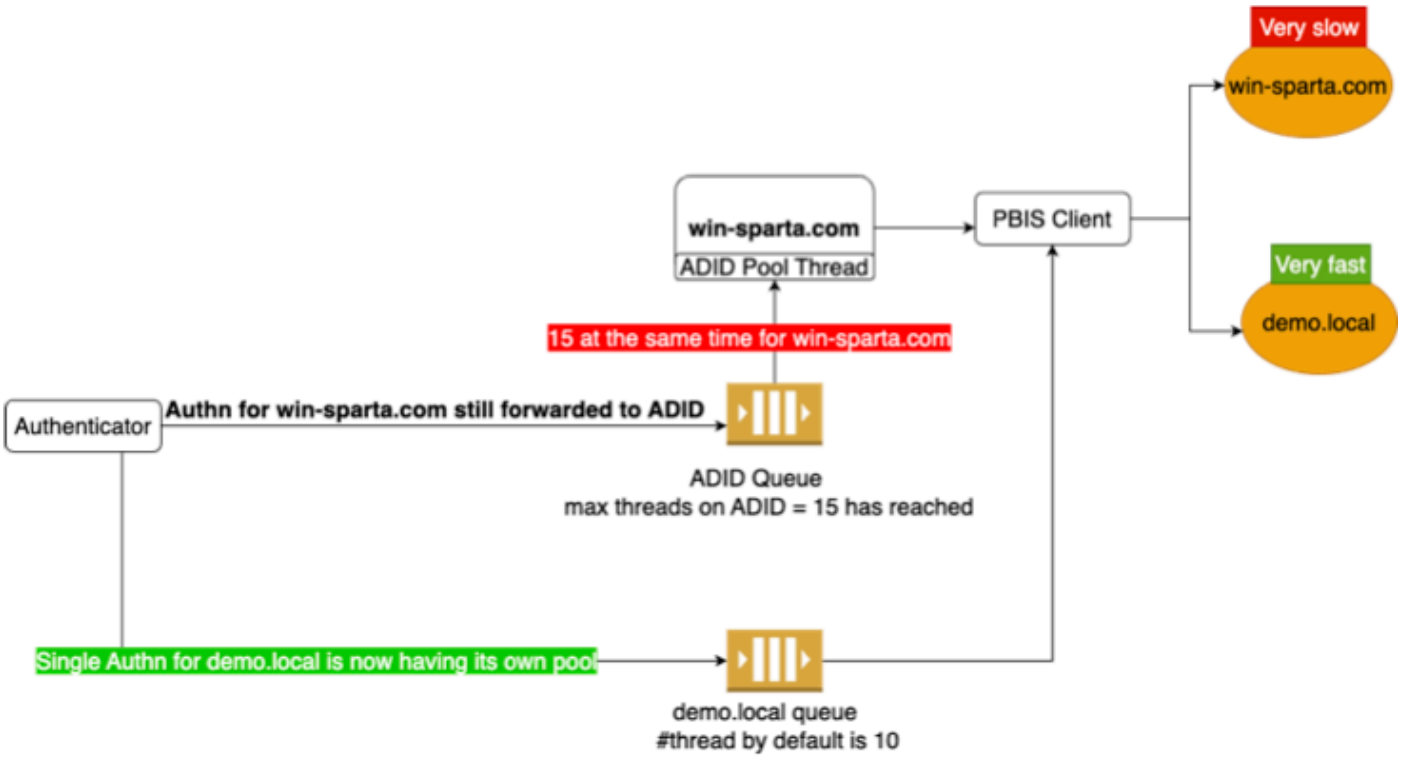


Abbildung 4: Lösungsablauf

Schrittweise Konfiguration

Schritt 1: Erstellen Sie zwei separate AD-Verknüpfungspunkte. Hier haben wir zum Beispiel: demo.local und win-sparta.com

Schritt 2: Erstellen einer Join Point-Priorisierung nach der AD-Join Point-Erstellung

Siehe Bild 5:

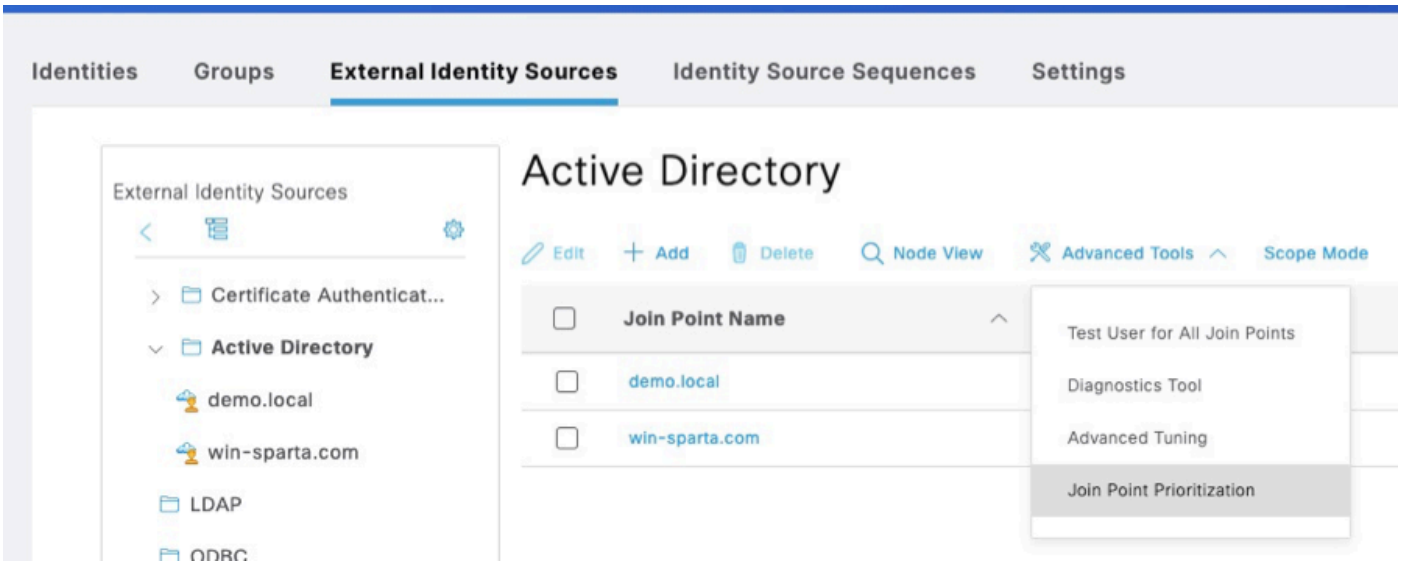


Abbildung 5: Join Point-Priorisierung

Schritt 3: Wählen Sie unter Join Point Prioritization (Join-Point-Priorisierung) den PSN aus, den Sie für die Reservierung dedizierter AD-Ressourcen bevorzugen. Klicken Sie auf Bearbeiten.

Siehe Bild 6:

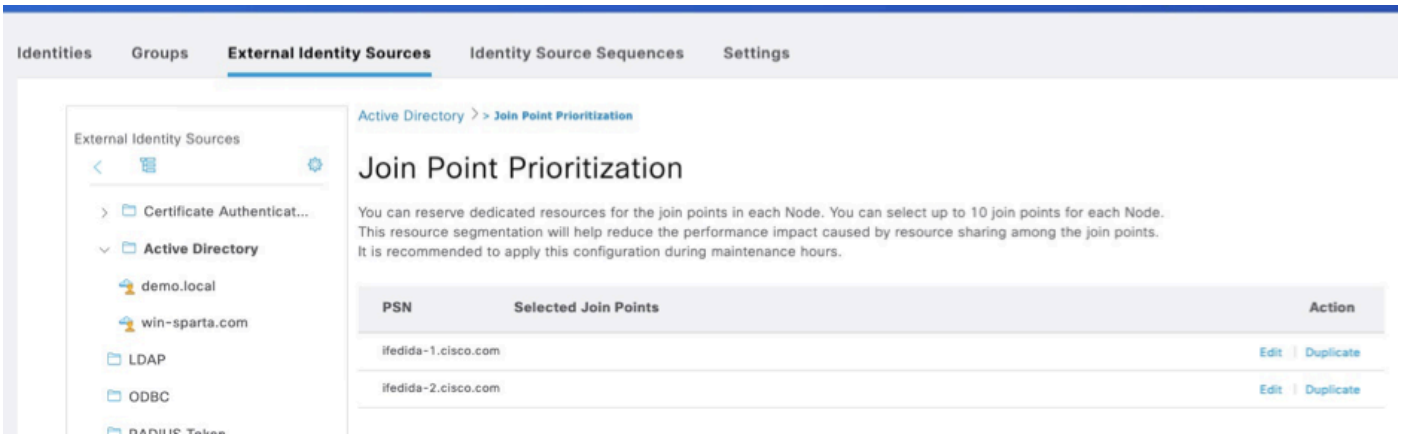


Abbildung 6: PSN bearbeiten

Schritt 4: Wählen Sie den bevorzugten Verbindungspunkt für das bevorzugte PSN aus.

Siehe Bild 7:

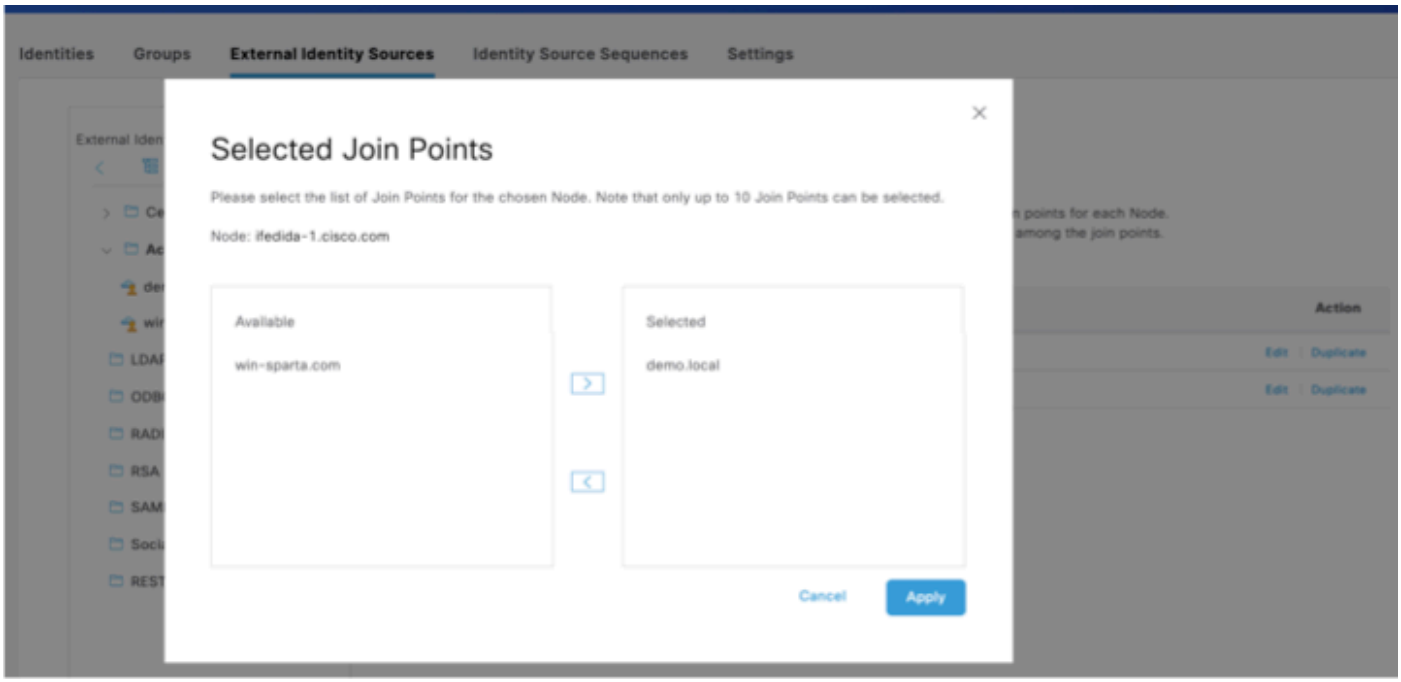
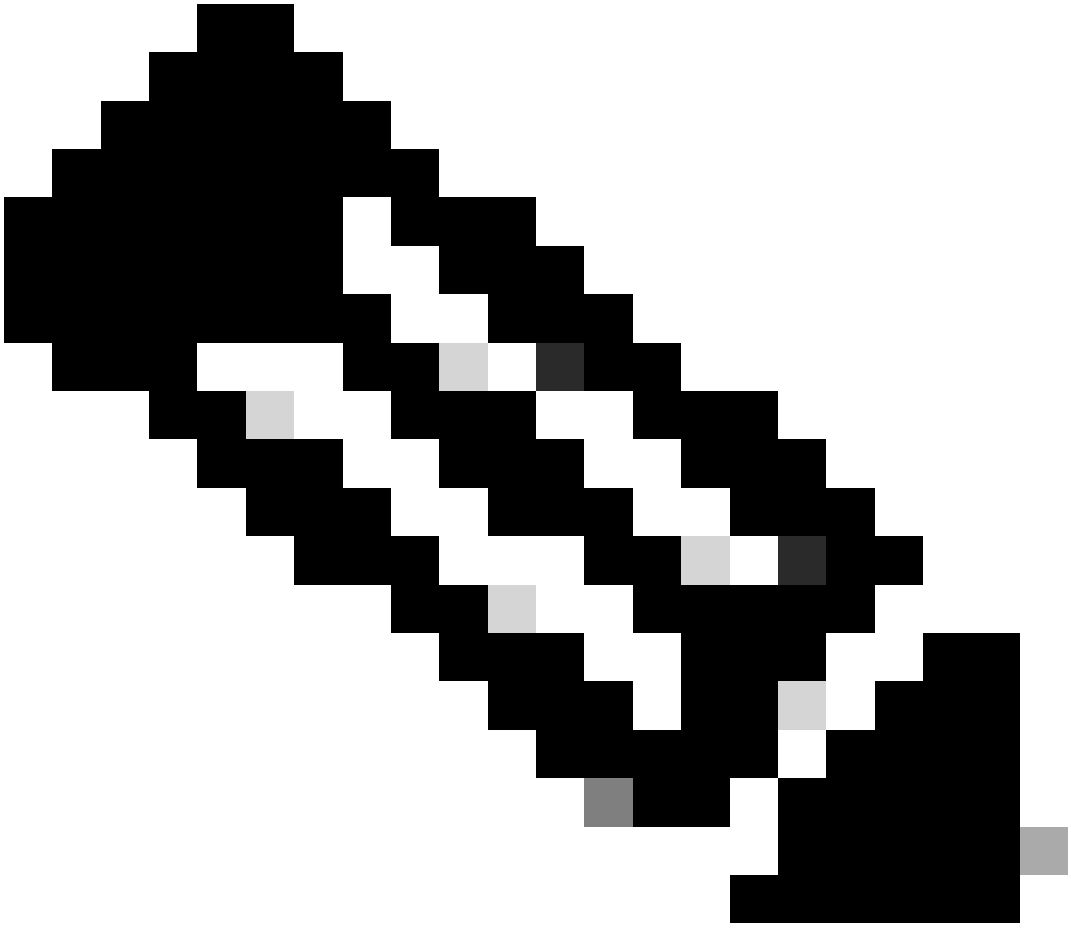


Abbildung 7: Ausgewählter Verbindungspunkt



Anmerkung: Alle Join-Punkte, die nicht in der Priorisierung enthalten sind, verwenden den gemeinsamen Thread-Pool, der maximal 15 Threads hat.

Schritt 5: Priorisierung abgeschlossen

Siehe Bild 8:

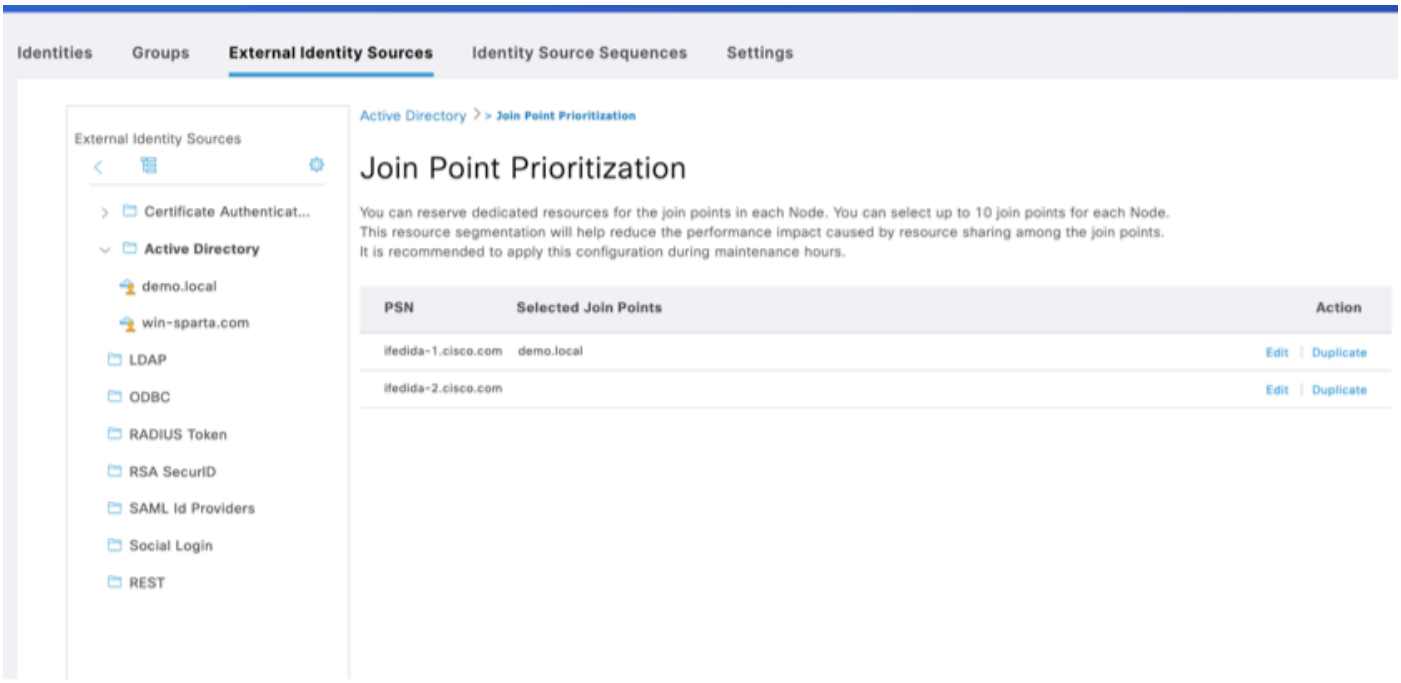
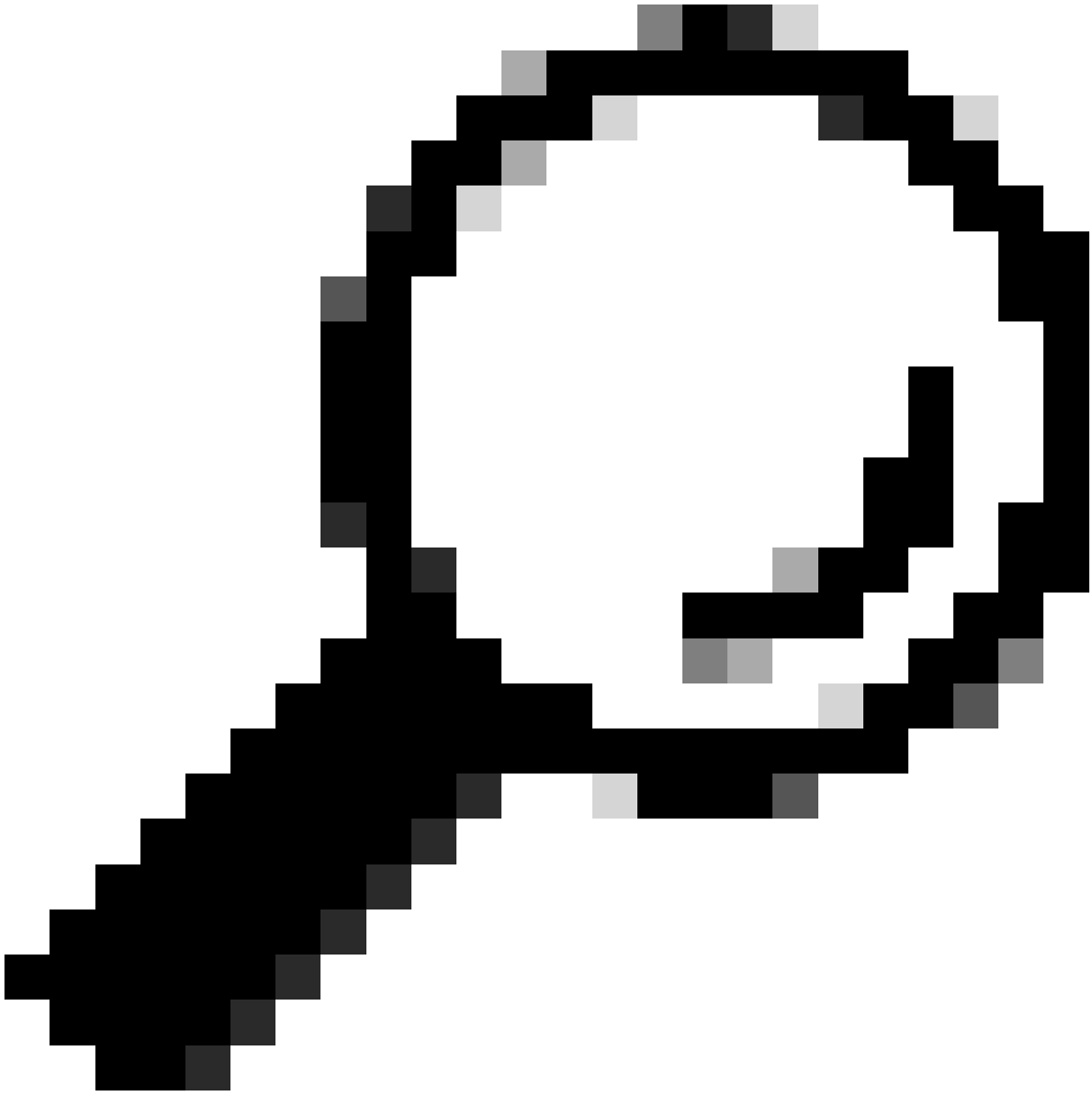


Abbildung 8: Konfiguration zur Priorisierung

Weitere Details



Tipp: Wenn Sie dieselben Einstellungen auf andere PSNs replizieren möchten, können Sie die Option Duplizieren verwenden. Wählen Sie die gewünschte PSN aus, und wählen Sie den zu duplizierenden Verknüpfungspunkt zusammen mit der ursprünglichen Priorisierung aus.

Siehe Bild 9: Konfigurationstipp:

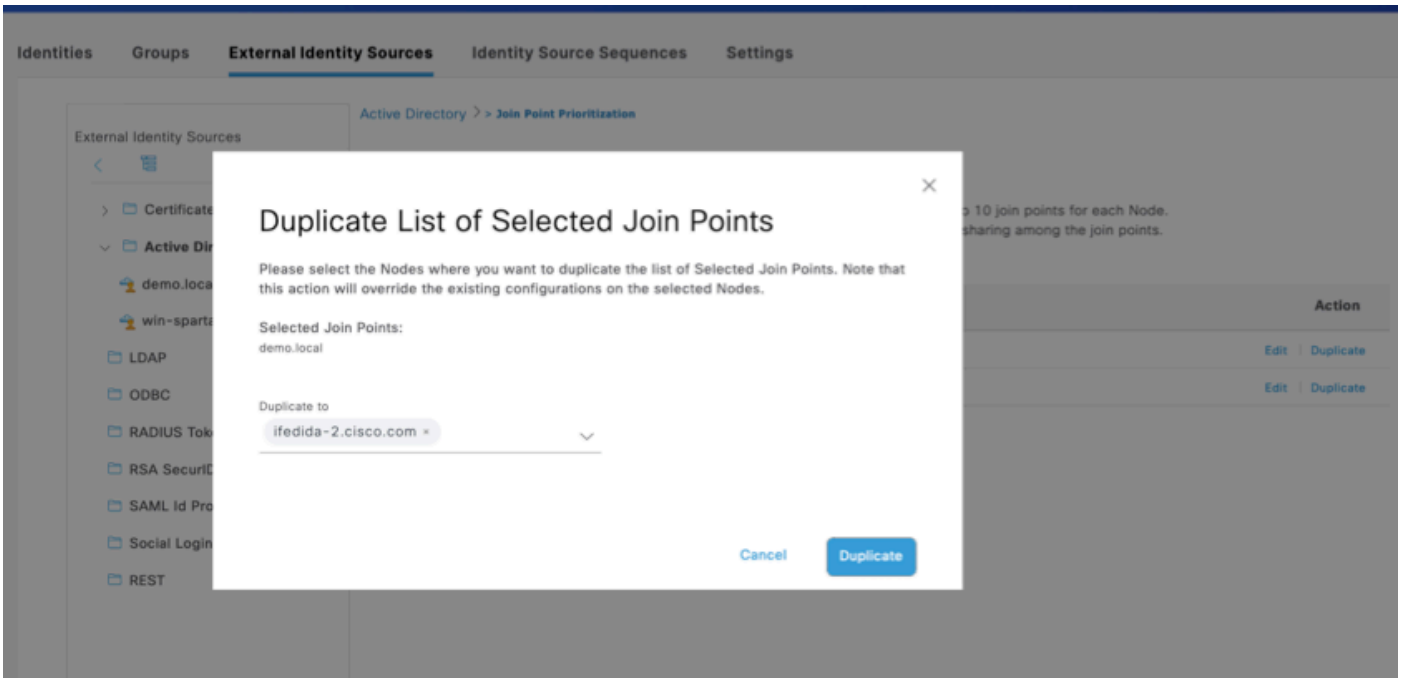


Bild 9: Konfiguration für Priorisierung duplizieren

Schritt 6: Endgültige Liste nach der Duplizierung

Siehe Bild 10:

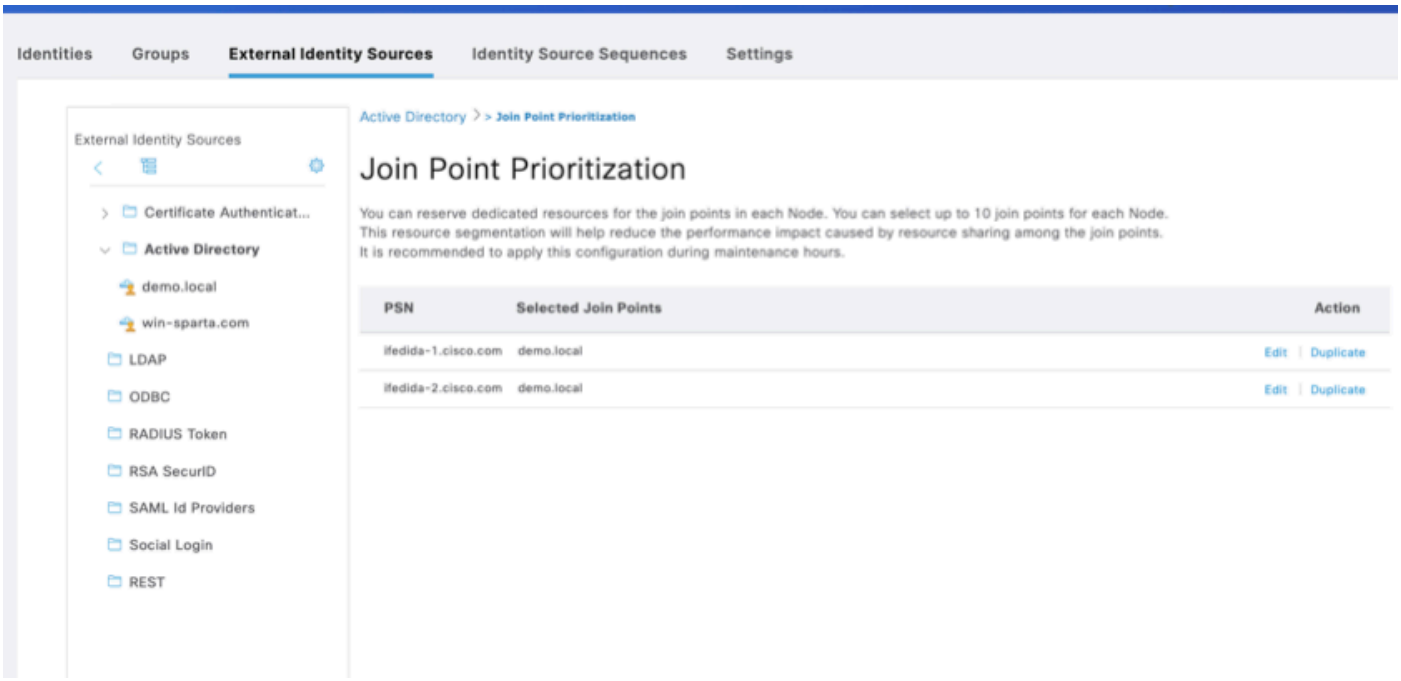


Bild 10: Endgültige Liste nach Priorisierung

Fehlerbehebung

Verifizierung

Überprüfen der Konfigurationsänderungen Navigieren Sie zu: Betrieb > Berichte > Audits > Konfigurationsprüfung ändern

Siehe Bild 11:

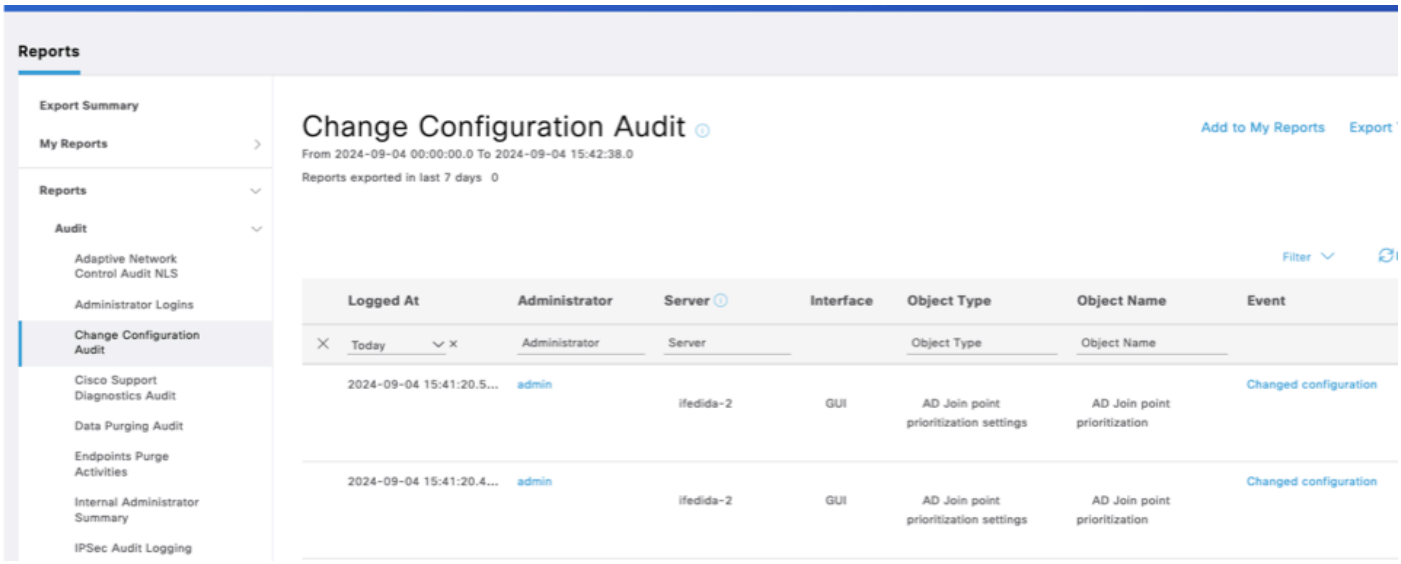


Bild 11: Konfigurationsauditbericht

Protokollieren

- Debug-Ebene für AAA-Laufzeitprotokolle aktivieren.
- prrt-server.log analysieren
  Siehe Bild 12:

Bild 12: Konfiguration des Debug-Protokolls

Ausschnitte protokollieren

prt-server.log [DEBUG]: Standard-Protokoll:

EventHandler, 2024-08-23 07:16:48,135,DEBUG,0x7fecd2ccc700,Zugewiesener Standard-Threadpool: ADIDStore für IDP: win-sparta.com_wxETlH16Pk_106

prrt-server.log [INFO]: Wenn wir dedizierte Ressourcen festlegen:

- ActiveDirectoryIDStore, 2024-09-08 16:52:01,048,INFO ,0x7f2452ccf700,Zugewiesener Threadpool : ADThreadPool0 an IDP: win-sparta.com_wxETlH16Pk_106
- ActiveDirectoryIDStore, 2024-09-08 16:57:11,258,INFO ,0x7f2452ccf700,Zugewiesener Threadpool : ADThreadPool1 an IDP: demo.local_6EcNs6UzwX_89

prrt-server.log [INFO]:

- Bevor wir dedizierte Ressourcen festgelegt haben:
  - EventHandler, 2024-09-02 08:45:54,673,INFO,0x7fafb793c700,Übergegebenes Ereignis an den nächsten Threadpoolnamen=ADIDStore, Warteschlangengröße=1,EventDispatcher.cpp:7 57

- Nachdem wir dedizierte Ressourcen festgelegt haben:
    - EventHandler, 2024-09-02 08:45:54,673,INFO ,0x7f4867ff9700,Übergegebenes Ereignis an den nächsten Threadpoolnamen=ADThreadPool0, Warteschlangengröße=1,EventDispatcher.cc S. 841

So verfolgen Sie die Verwendung von "ADThreadPool0" im Threadpool:

1. 0x7f57792f7700,Übergegebenes Ereignis an den nächsten Threadpoolnamen=ADThreadPool0 (wenige Protokolle zurück StackID:0x7f57a4f761c0)

2. 0x7f57732c7700,Stack: 0x7f57a4f761c0 ActiveDirectoryIDStore aufrufen: MethodCaller<ActiveDirectoryIDStore, PlainAuthenticateAndQueryEvent>

3. 0x7f57732c7700,cntx=0000210117,sesn=ifedida-1/515863662/5273,CPMSessionID=C0A31430000000800018958,user=abcd,CallingStationID=[CAD] 956: CAD_PAPAuthenticate (abcd) aufgerufen

4. 0x7f57732c7700,cntx=000210117,sen=ifedida-1/515863662/5273,CPMSession ID=C0A31430000000800018958,user=abcd,CallingStationID=[CAD] 1026: CAD_PAPAuthenticate (abcd) erfolgreich

5. 0x7f57732c7700,Übergegebenes Ereignis an den nächsten Threadpoolnamen=Main

Häufig gestellte Fragen

Frage: Wie viele AD-Join-Points unterstützt die ISE?

Antwort: Sie können bis zu 50 Active Directory-Verknüpfungspunkte in einer einzelnen ISE-Bereitstellung konfigurieren.

Frage: Wenn ich mehrere AD-Join-Punkte habe, kann ich dann weiterhin die On-Demand-Priorisierung verwenden?

Antwort: Ja

Frage: Wie groß ist der Standard-Thread ohne Priorisierung für eine einzelne Domäne?

Antwort: 15 Threads

Frage: Wie erfolgt die Berechnung, wenn ich die Priorisierung konfiguriere? Ein Szenario mit drei Join Points - domain1.com, domain2.com und domain3.com mit domain1.com ist nicht für die Priorisierung konfiguriert, domain2.com und domain3.com für die Priorisierung.

Antwort: Wenn Domäne1 nicht für die Priorisierung konfiguriert ist, verwendet domain1.com die allgemeinen 15 verfügbaren Threads - alle gleichzeitig. Da domain2.com und domain3.com jedoch mit Priorisierung konfiguriert sind, verwenden sie standardmäßig jeweils 10 Threads und nicht den gemeinsamen 15 Threadpool.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.