Comprendre la réservation de ressources à la demande pour AD sur le correctif 4 d'ISE 3.3

Table des matières

Introduction

Ce document décrit la réservation de ressources à la demande pour Active Directory sur ISE 3.3 Patch 4

Conditions préalables

Connaissances sur Cisco Identity Services Engine (ISE)

Connaissances sur Active Directory (AD)

Connaissances sur l'intégration ISE et AD

Composants requis

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes

- Correctif 4 de Cisco Identity Services Engine 3.3
- Microsoft Windows Active Directory 2016 ou version ultérieure

The information in this document was created from the devices in a specific lab environment. All of

the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Informations générales

Les authentifications AD sont parfois lentes et finissent par échouer. Les raisons possibles peuvent être le début de l'empilage de la file d'attente ADID ou l'épuisement de tous les threads du pool ADID.

Plus de détails sur ADID :

Un ADID, également appelé nom distinctif (DN), est une chaîne qui identifie de manière unique un objet dans l'annuaire Active Directory. Ils sont utilisés pour localiser et gérer des objets dans le domaine Active Directory. Les ADID sont essentiels à la gestion des comptes d'utilisateurs, des autorisations et d'autres ressources au sein d'un environnement Active Directory.

Un ADID type doit ressembler à ceci : CN=John Doe, OU=Sales, DC=example, DC=com ; where,

CN=John Doe : Représente le nom commun de l'utilisateur, John Doe.
OU=Ventes : Représente l'unité d'organisation (OU) à laquelle l'utilisateur appartient, dans ce cas, le service Ventes.
DC=exemple,DC=com : Représente les composants du domaine, à savoir example.com.

Exemple :

Reportez-vous à la photo 1 : Une configuration de point de jonction AD typique

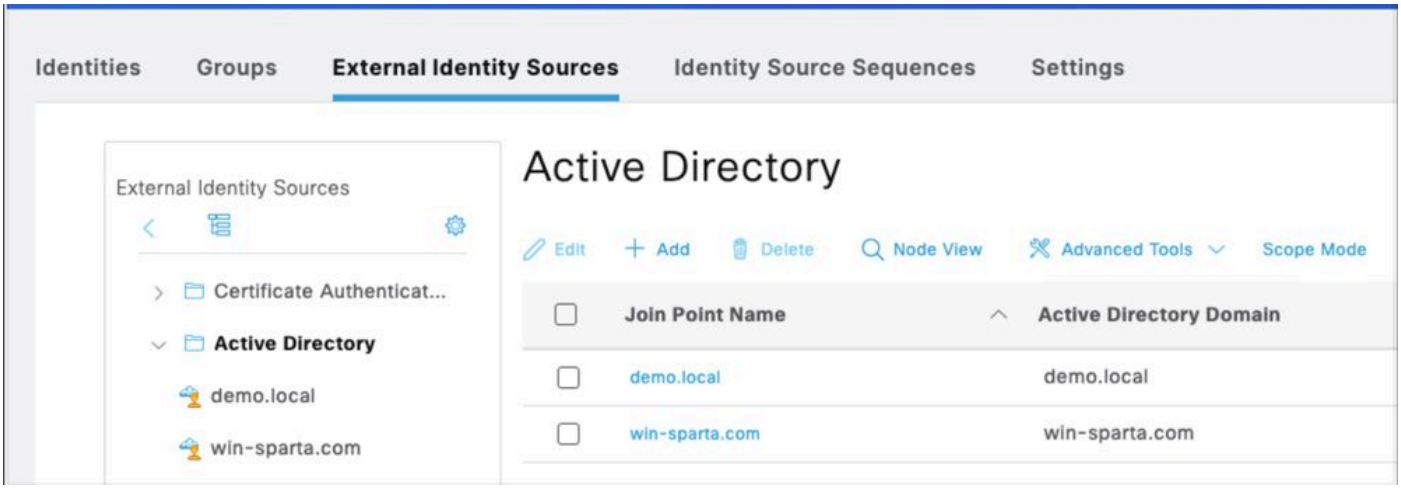


Image 1 : Points de jointure AD

Reportez-vous à la photo 2 : Diagramme de flux AD typique avec 2 points de jonction

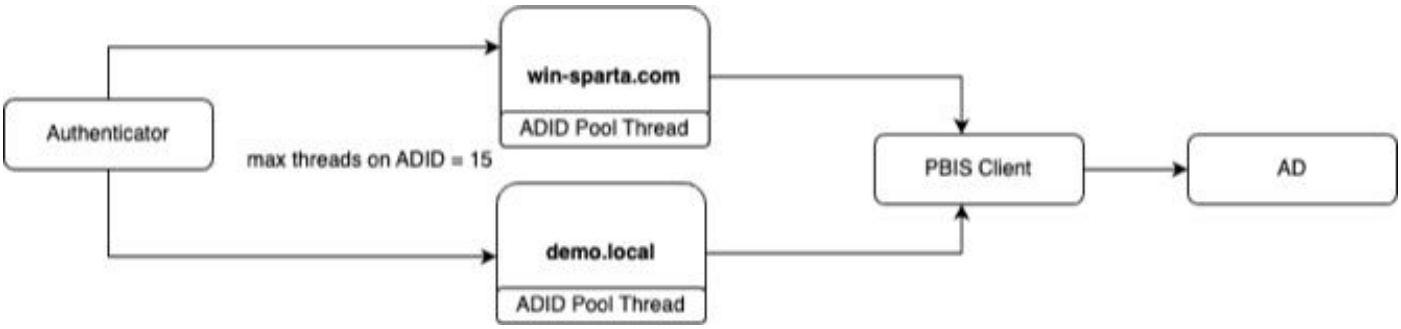


Image 2 : Diagramme de flux AD typique

Symptôme

Point de jonction lent sous le même pool de threads ADID

Problème

1. Quelles seraient les conséquences de la lenteur de l'un des points de jonction ? Par exemple, si 15 authentifications sont envoyées à ISE en même temps pour « demo.local » et que « demo.local » est anormalement lent, nous devons attendre la réponse de « demo.local » avant de traiter l'authentification win-sparta suivante.
2. Que se passe-t-il si les deux points de jointure partagent le même pool de threads ADID sous un point de jointure ?

Reportez-vous à la photo 3 : Schéma du point de joint lent

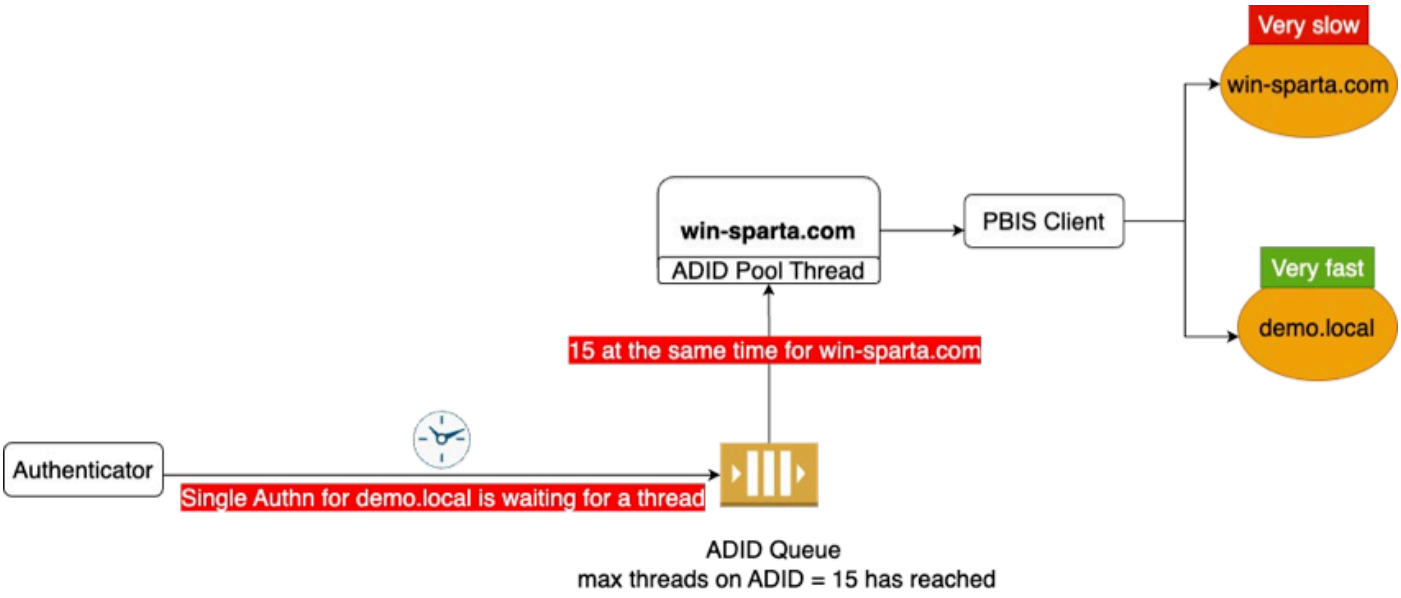
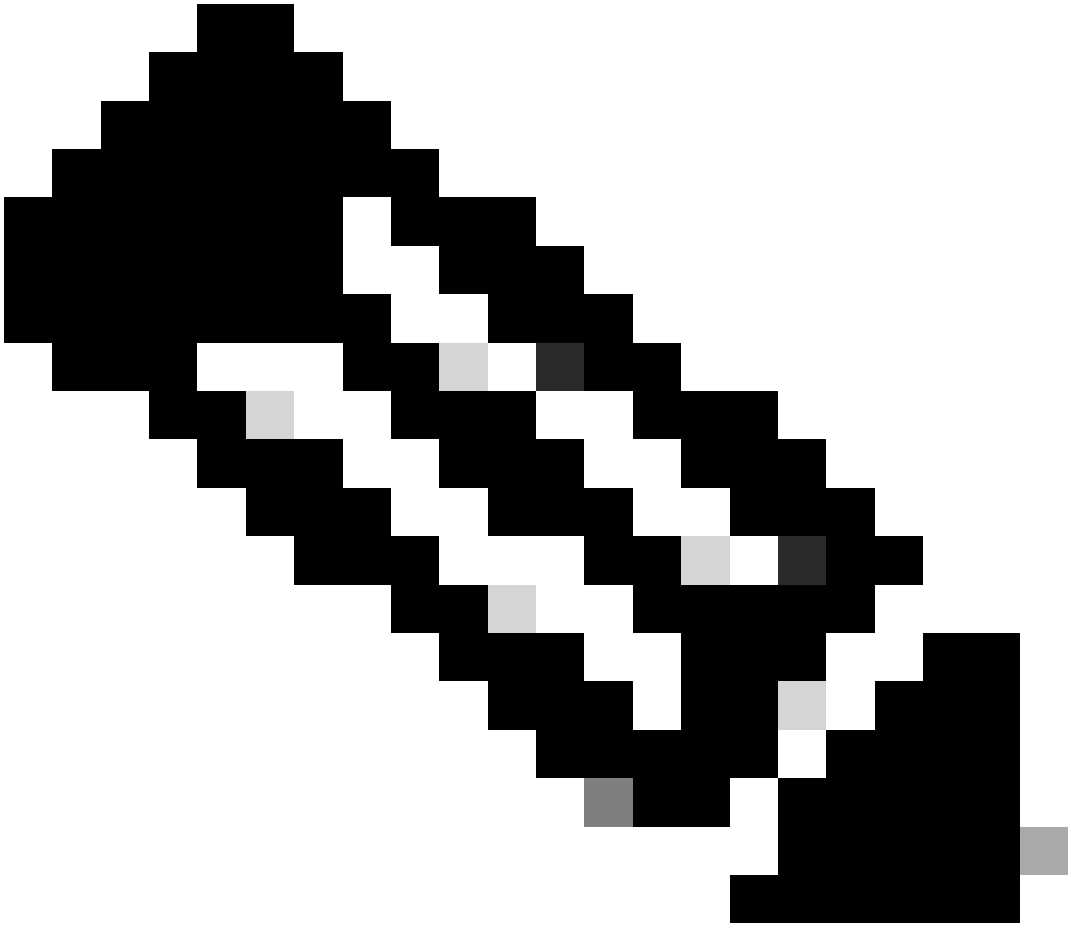


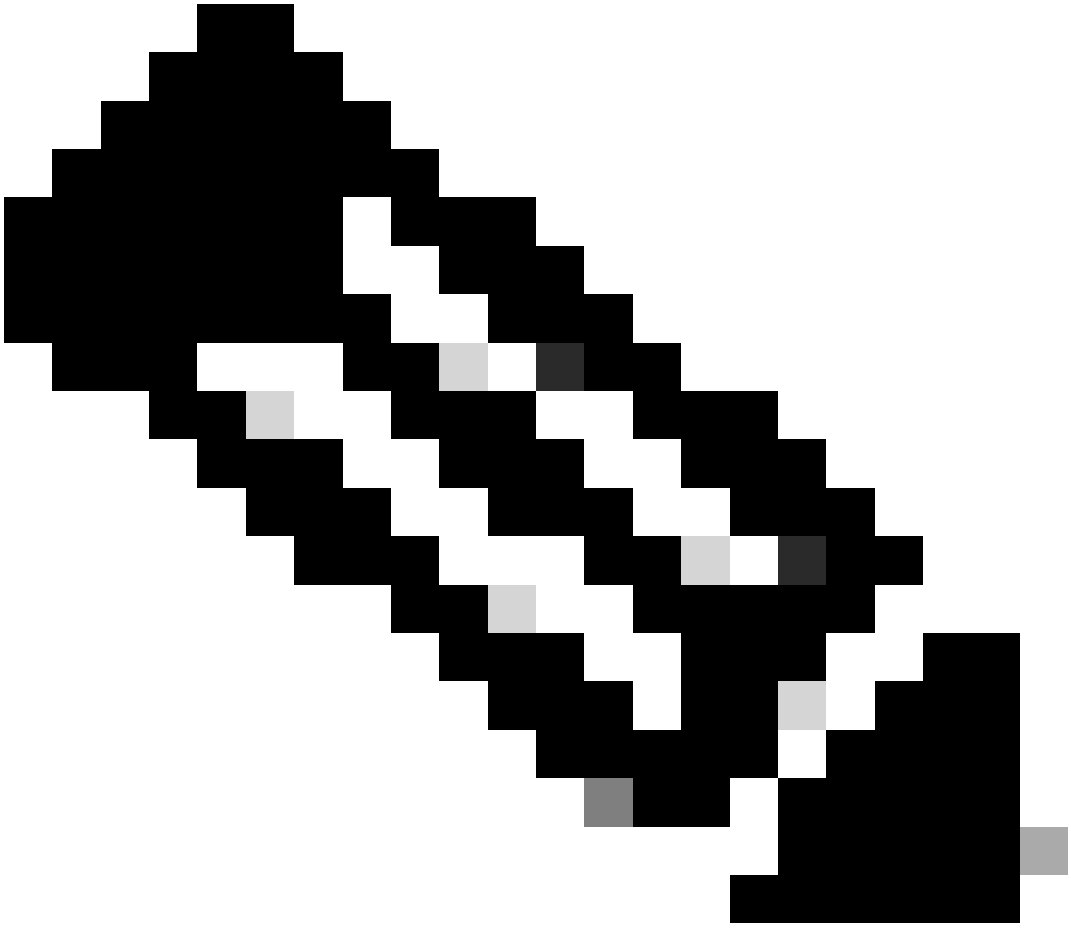
Image 3 : Flux problématique



Remarque : Ici, les 15 threads sont occupés par win-sparta.com en même temps, ne laissant aucun thread pour demo.local

Solution

- Le comportement par défaut est un pool de threads commun pour tous les points de jointure Active Directory
- Cependant, les administrateurs peuvent segmenter chaque point de jointure pour disposer de leurs propres ressources.



Remarque : Lorsque la hiérarchisation AD est appliquée, la valeur par défaut est 10 threads par pool de threads.

Reportez-vous à la photo 4 : Organigramme du point de jonction réservé à la demande

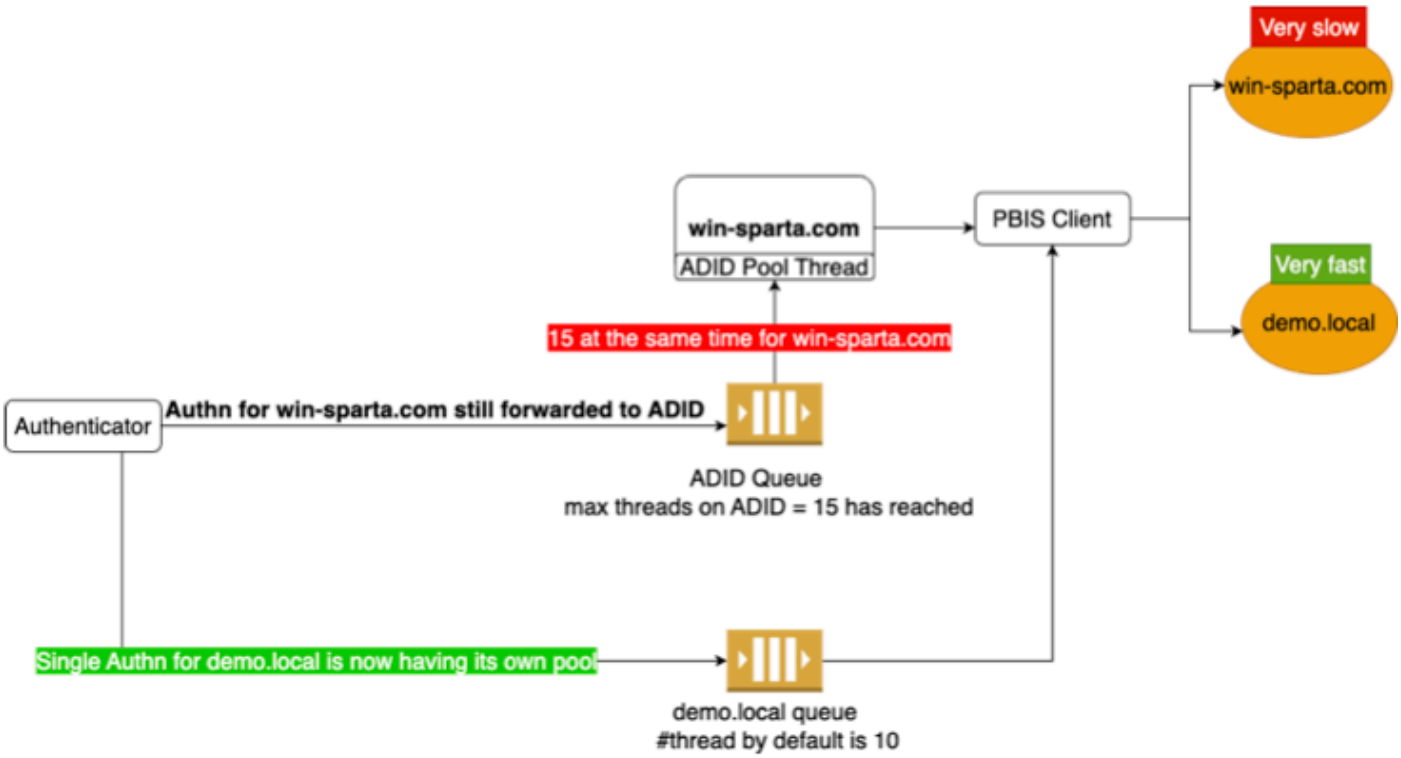


Image 4 : Flux de solution

Configuration pas à pas

Étape 1 : Créez deux points de jointure AD distincts. Voici par exemple ce que nous avons : demo.local et win-sparta.com

Étape2: Créer une hiérarchisation de point de connexion après la création du point de connexion AD.

Reportez-vous à la photo 5 :

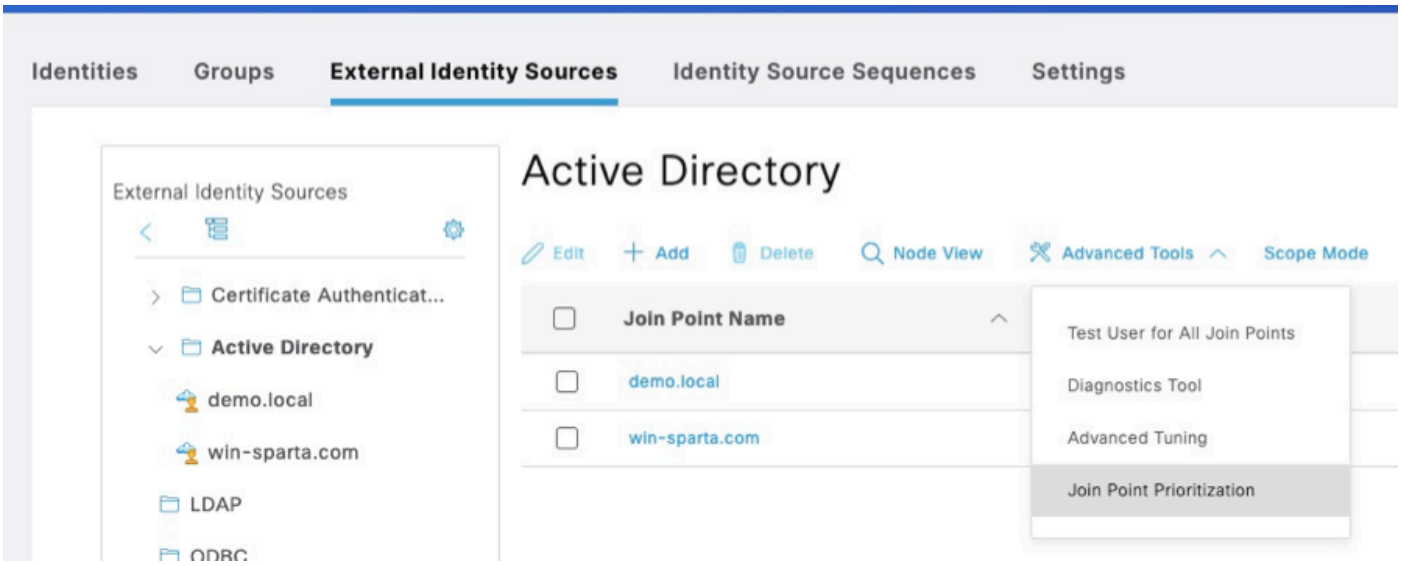


Image 5 : Hiérarchisation des points de jonction

Étape 3 : Sous Hiérarchisation des points de jonction, sélectionnez le PSN pour lequel vous

préférez réserver des ressources AD dédiées. Cliquez sur Edit.

Reportez-vous à la photo 6 :

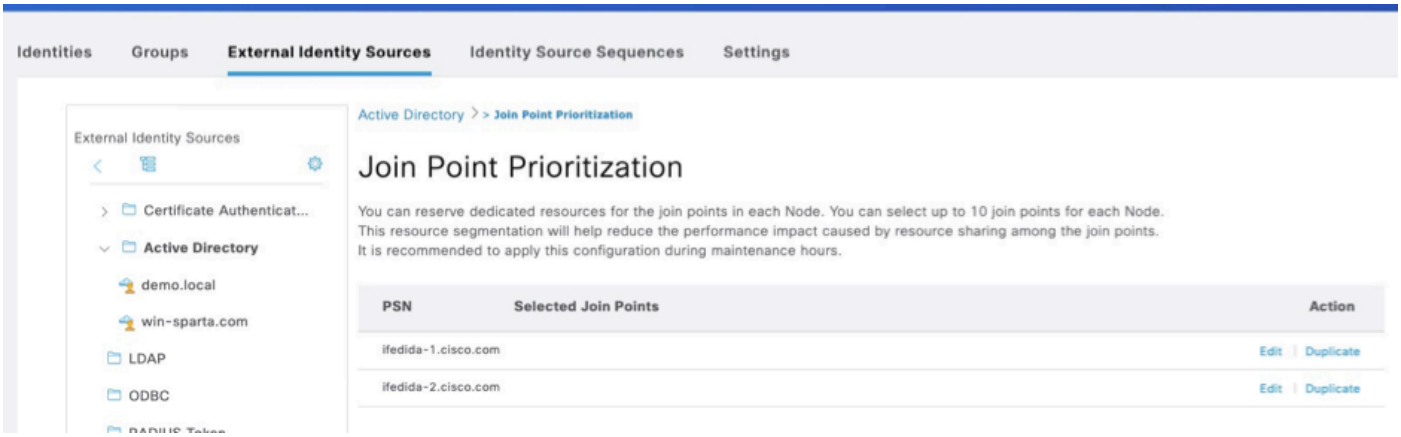


Image 6 : Modifier PSN

Étape 4 : Sélectionnez le point de jonction préféré pour le PSN préféré.

Reportez-vous à la photo 7 :

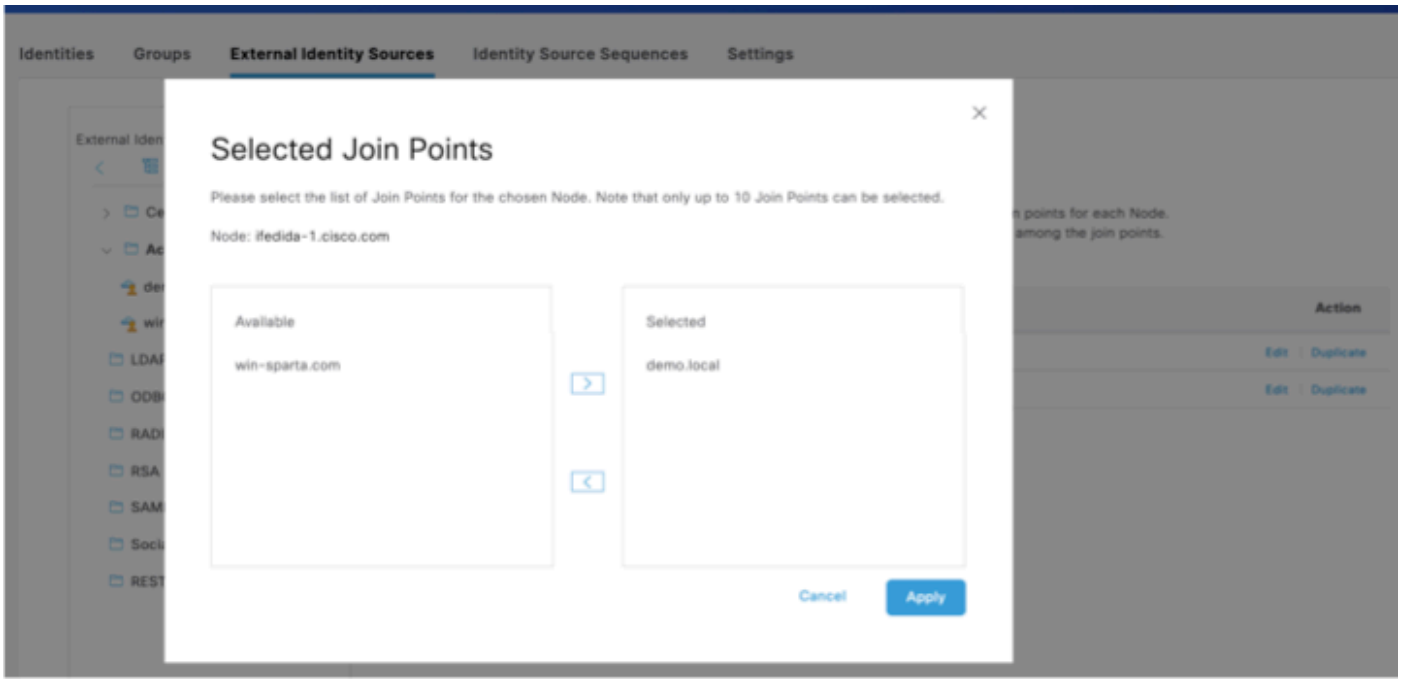
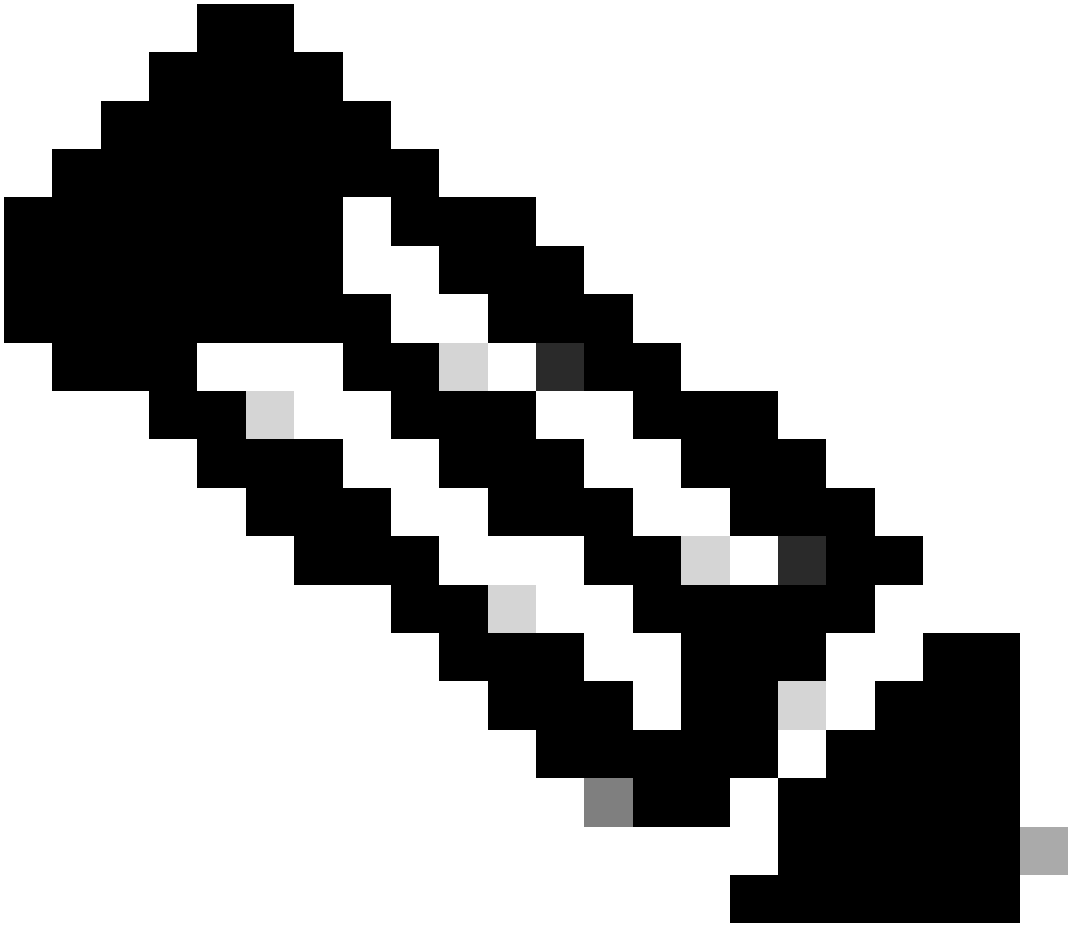


Image 7 : Point de jonction sélectionné



Remarque : Tous les points de jointure non inclus dans la hiérarchisation utilisent le pool de threads communs, qui a une limite maximale de 15 threads.

Étape 5 : La hiérarchisation est finalisée

Reportez-vous à la photo 8 :

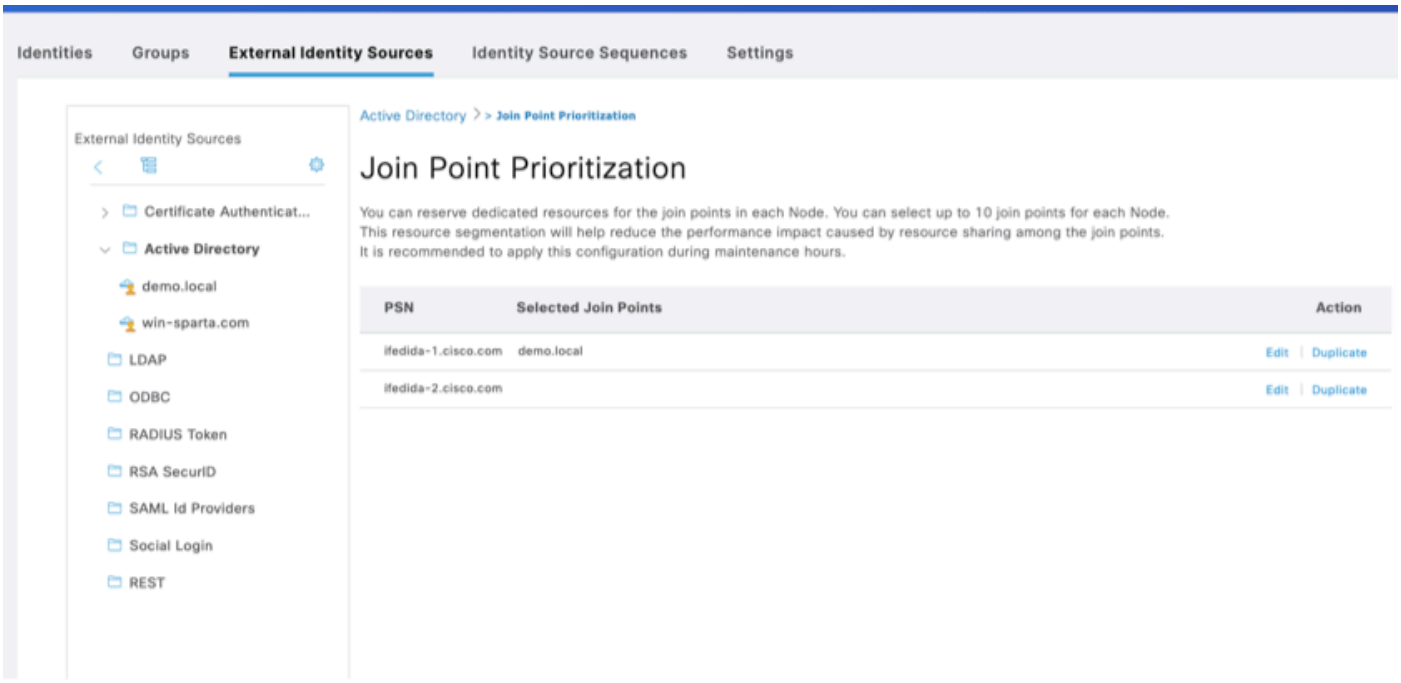
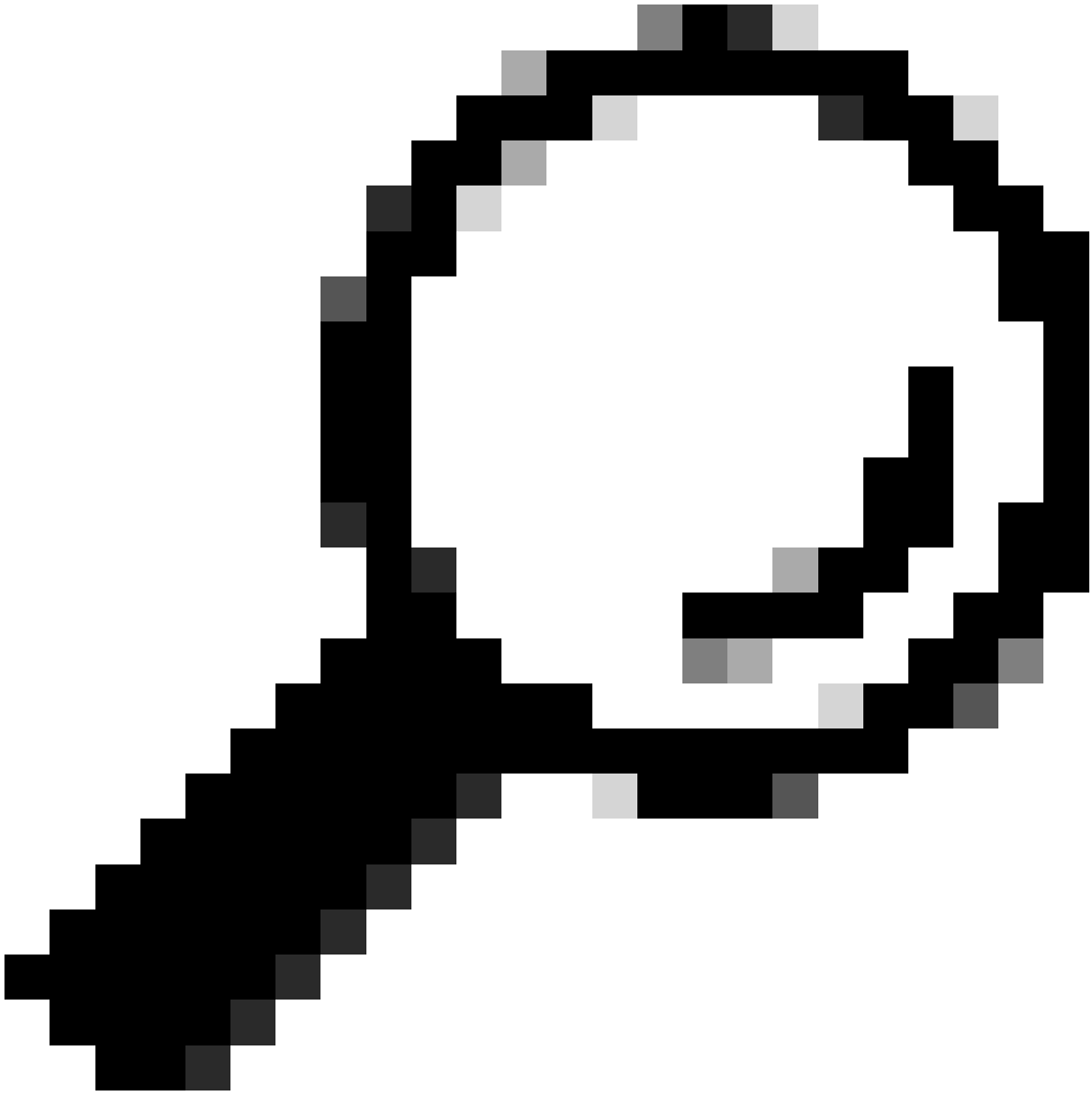


Image 8 : Configuration des priorités

Détails supplémentaires



Conseil : Si vous souhaitez répliquer les mêmes paramètres sur d'autres PSN, vous pouvez utiliser l'option Dupliquer. Sélectionnez le PSN souhaité, puis choisissez le point de jonction à dupliquer avec la hiérarchisation d'origine.

Reportez-vous à l'image 9 : Conseil de configuration :

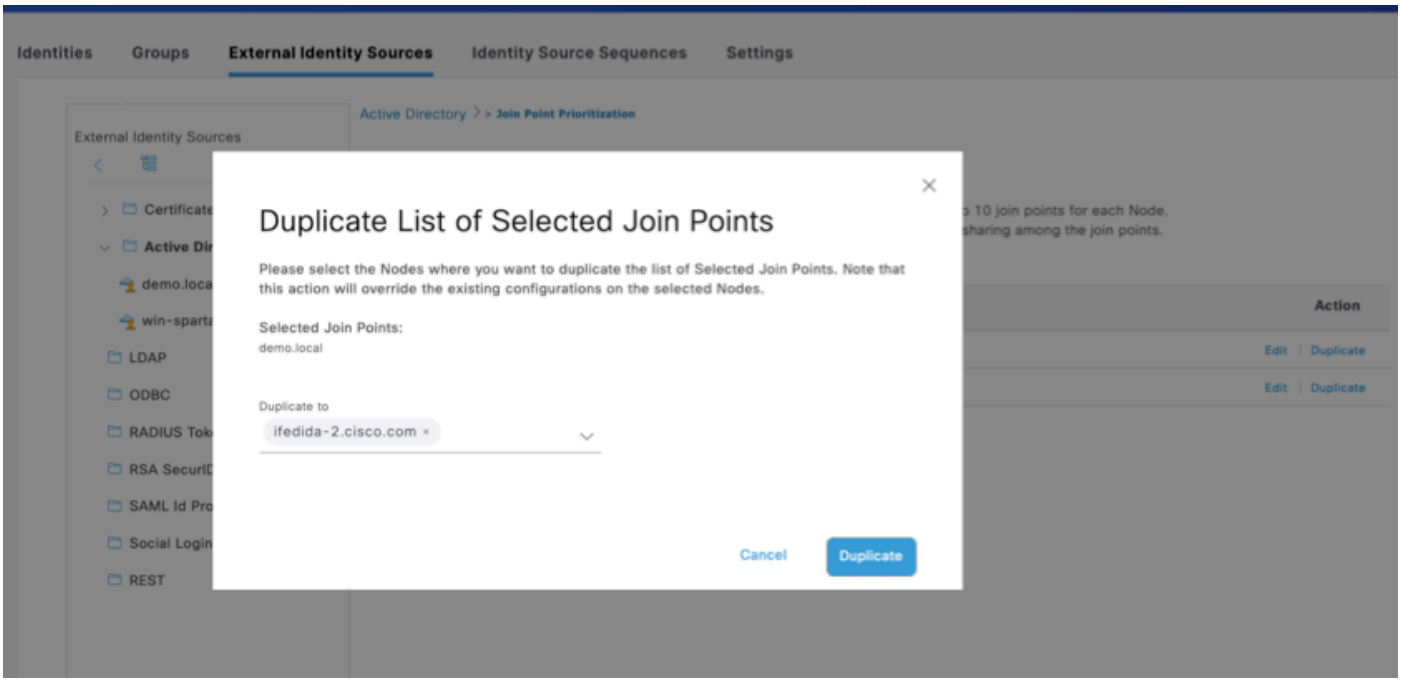


Image 9 : Duplication de la configuration de priorité

Étape 6 : liste définitive après duplication

Reportez-vous à la photo 10 :

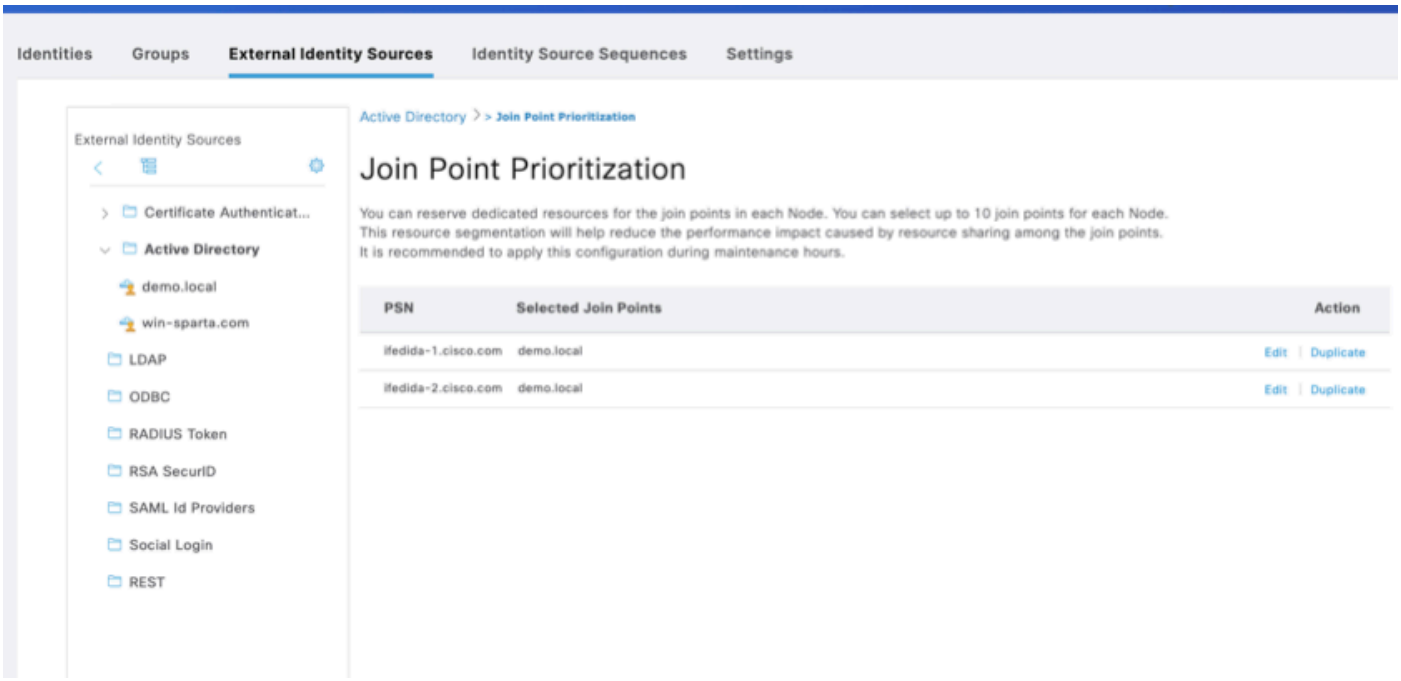


Image 10 : liste définitive après hiérarchisation

Dépannage

Vérification

Vérifiez les modifications de configuration. Naviguez jusqu’à l’adresse : Opérations > Rapports > Audits > Modifier l'audit de configuration

Reportez-vous à la photo 11 :

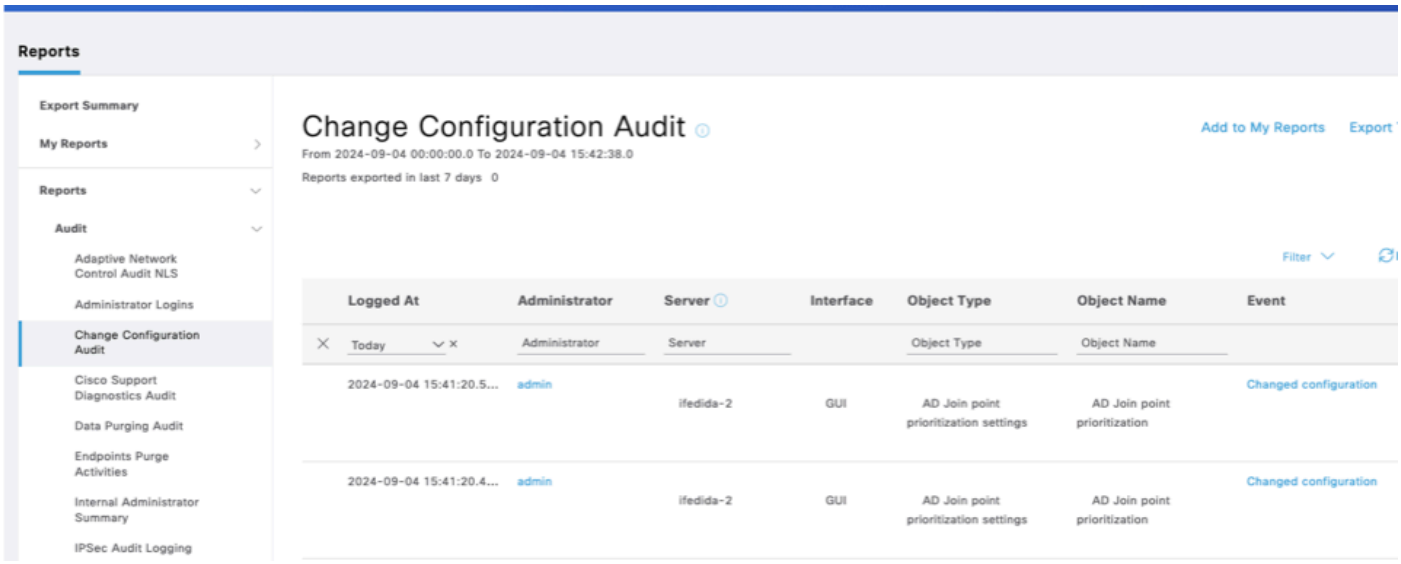


Image 11 : Rapport d'audit de configuration

Journalisation

- Activez le niveau de débogage pour les journaux d'exécution AAA.
- Analyser le fichier prt-server.log
  Reportez-vous à la photo 12 :

Image 12 : Configuration du journal de débogage

Extraits de journal

prrt-server.log [DEBUG] : journal par défaut :

EventHandler,2024-08-23 07:16:48,135,DEBUG,0x7fecd2ccc700, pool de threads par défaut alloués : ADIDStore vers IDP : win-sparta.com_wxETlH16Pk_106

prrt-server.log [INFO] : Lorsque nous définissons des ressources dédiées :

- ActiveDirectoryIDStore,2024-09-08 16:52:01,048,INFO,0x7f2452ccf700,Pool de threads alloués : ADThreadPool0 vers IDP : win-sparta.com_wxETlH16Pk_106
- ActiveDirectoryIDStore,2024-09-08 16:57:11,258,INFO,0x7f2452ccf700,Pool de threads alloués : ADThreadPool1 vers IDP : demo.local_6EcNs6UzwX_89

prt-server.log [INFO] :

- Avant de définir des ressources dédiées :
  - EventHandler, 2024-09-02 08:45:54,673,INFO,0x7fafb793c700,Événement transmis au pool de threads suivant nom=ADIDStore, taille de file d'attente=1,EventDispatcher.cpp:757

- Après avoir défini les ressources dédiées :
    - EventHandler,2024-09-02 08:45:54,673,INFO ,0x7f4867ff9700,Événement transmis au pool de threads suivant nom=ADThreadPool0, taille de file d'attente=1,EventDispatcher.cpp : 841

Pour suivre l'utilisation du pool de threads de « ADThreadPool0 » :

1. 0x7f57792f7700,Événement transmis au pool de threads suivant name=ADThreadPool0 (quelques journaux reviennent à StackID : 0x7f57a4f761c0)

2. 0x7f57732c7700, pile : 0x7f57a4f761c0 Appel d'ActiveDirectoryIDStore : Méthode MethodCaller<ActiveDirectoryIDStore, PlainAuthenticateAndQueryEvent>

3. 0x7f57732c7700, cntx=0000210117, sen=ifedida-1/515863662/5273, CPMSessionID=C0A314300000000800018958, user=abcd, CallingStationID=[CAD] 956 : CAD_PAPAuthenticate (abcd) appelé

4. 0x7f57732c7700, cntx=0000210117, sen=ifedida-1/515863662/5273, CPMSessionID=C0A314300000000800018958, user=abcd, CallingStationID=[CAD] 1026 : CAD_PAPAuthenticate (abcd) réussi

5. 0x7f57732c7700,Événement transmis au pool de threads suivant name=Main

Forum aux questions

Question : Combien de points de connexion AD ISE peut-il prendre en charge ?

Réponse : Vous pouvez configurer jusqu'à 50 points de jonction Active Directory sur un déploiement ISE unique.

Question : Si j'ai plusieurs points de connexion AD, puis-je toujours utiliser la hiérarchisation à la demande ?

Réponse : Oui

Question : Quelle est la taille de thread par défaut sans hiérarchisation pour un seul domaine ?

Réponse : 15 threads

Question : Si je configure la hiérarchisation, comment le calcul est-il effectué ? Considérez qu'un scénario à 3 points de jonction - domain1.com, domain2.com et domain3.com avec domain1.com n'est pas configuré pour la hiérarchisation et domain2.com et domain3.com sont configurés pour la hiérarchisation.

Réponse : Si domain1 n'est pas configuré pour la hiérarchisation, domain1.com utilise les 15 threads communs disponibles, tous en même temps. Cependant, puisque domain2.com et domain3.com sont configurés avec la hiérarchisation, ils utilisent 10 threads chacun par défaut et ne suivent pas/utilisent le pool commun de 15 threads.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.