

# Comprendere la prenotazione di risorse su richiesta per AD su patch 4 ISE 3.3

## Sommario

---

[Introduzione](#)

[Prerequisiti](#)

[Componenti richiesti](#)

[Premesse](#)

[Sintomo](#)

[Problema](#)

[Soluzione](#)

[Configurazione dettagliata](#)

[Ulteriori dettagli](#)

[Risoluzione dei problemi](#)

[Verifica](#)

[Registrazione](#)

[Registra frammenti](#)

[Domande frequenti](#)

---

## Introduzione

In questo documento viene descritto come prenotare le risorse su richiesta per Active Directory in ISE 3.3 Patch 4

## Prerequisiti

Conoscenza di Cisco Identity Services Engine (ISE)

Informazioni su Active Directory (AD)

Conoscenze sull'integrazione di ISE e AD

## Componenti richiesti

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware

- Patch 4 per Cisco Identity Services Engine 3.3
- Microsoft Windows Active Directory 2016 o versione successiva

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata

ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

## Premesse

Le autenticazioni AD sono talvolta lente e possono fallire. Possibili cause: la coda ADID sta iniziando l'accumulo o tutti i thread del pool ADID si stanno esaurendo.

Maggiori dettagli su ADID:

Un ADID, noto anche come nome distinto (DN), è una stringa che identifica in modo univoco un oggetto nella directory di Active Directory. Vengono utilizzati per individuare e gestire gli oggetti all'interno del dominio di Active Directory. Gli ADID sono fondamentali per la gestione degli account utente, delle autorizzazioni e di altre risorse in un ambiente Active Directory.

Un ADID tipico deve avere il seguente aspetto: CN=Mario Rossi,OU=Vendite,DC=esempio,DC=com; dove,

CN=Mario Rossi: Rappresenta il nome comune dell'utente, John Doe.

OU=Vendite: Rappresenta l'unità organizzativa a cui appartiene l'utente, in questo caso il reparto vendite.

DC=esempio,DC=com: Rappresenta i componenti del dominio, ovvero example.com.

Ad esempio:

Per ulteriori informazioni, fare riferimento alla figura 1: Una configurazione tipica dei punti di join AD

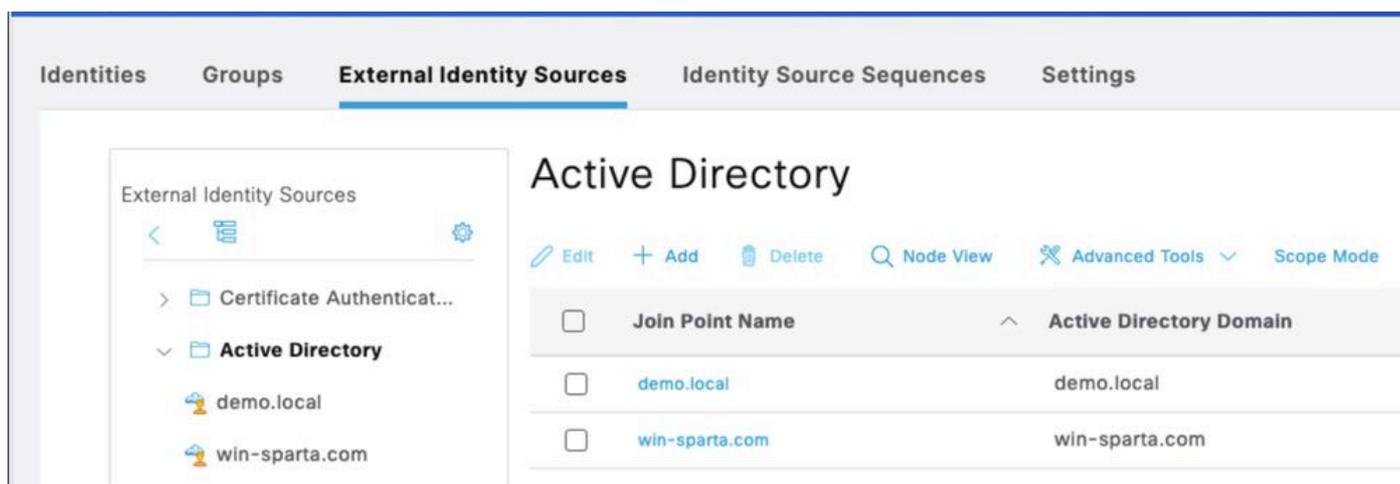


Immagine 1: Punti di join AD

Per ulteriori informazioni, fare riferimento alla figura 2: Un tipico diagramma di flusso AD con 2 punti di join

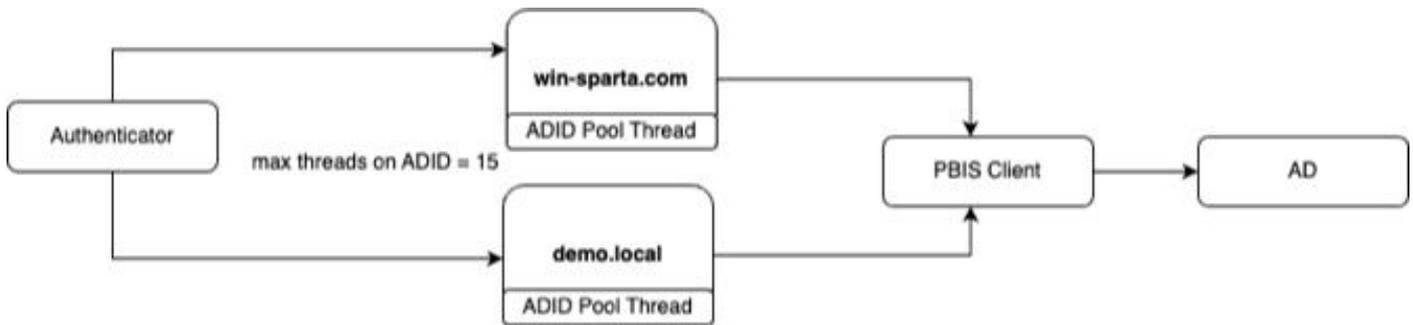


Immagine 2: Un tipico diagramma di flusso di AD

## Sintomo

Punto di join lento nello stesso pool di thread ADID

## Problema

1. Quali sarebbero le conseguenze di un rallentamento di uno dei punti di unione? Ad esempio, se 15 autenticazioni vengono inviate ad ISE contemporaneamente per "demo.local" e "demo.local" è insolitamente lento, dovremo attendere la risposta da "demo.local" prima di gestire la successiva autenticazione win-sparta.
2. Cosa succede se entrambi i punti di join condividono lo stesso pool di thread ADID sotto un punto di join?

Per ulteriori informazioni, fare riferimento alla figura 3: Diagramma di flusso del punto a giunto lento

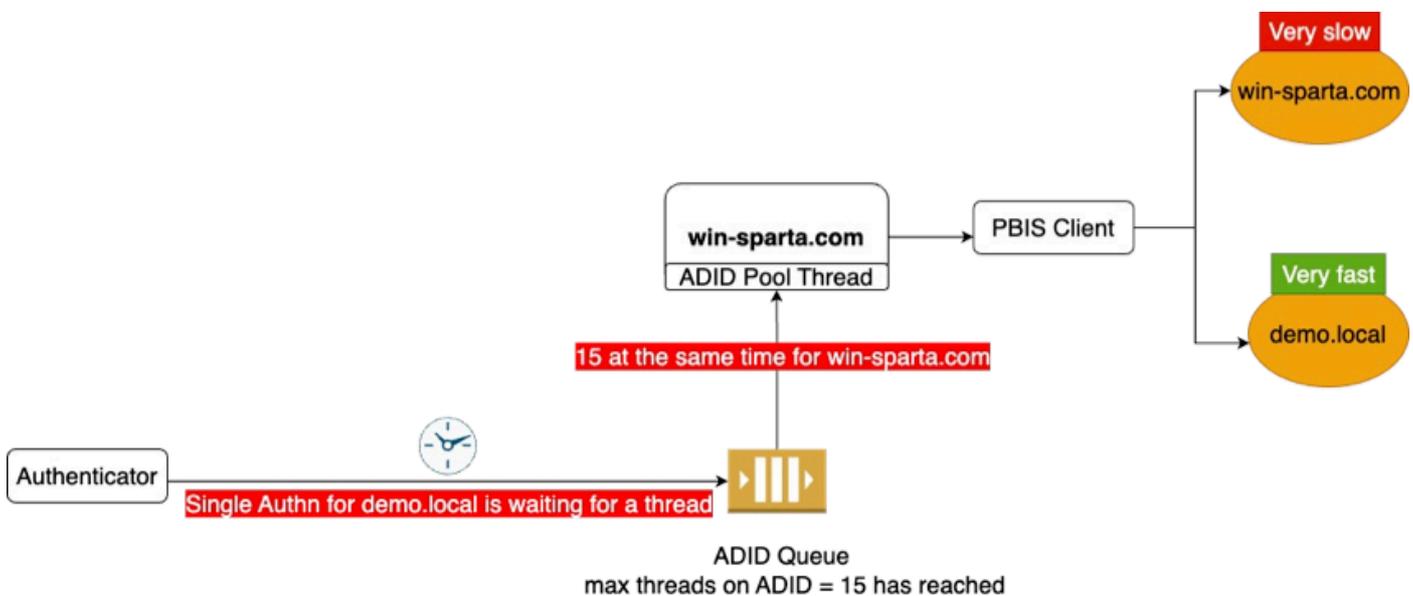


Immagine 3: Flusso problematico

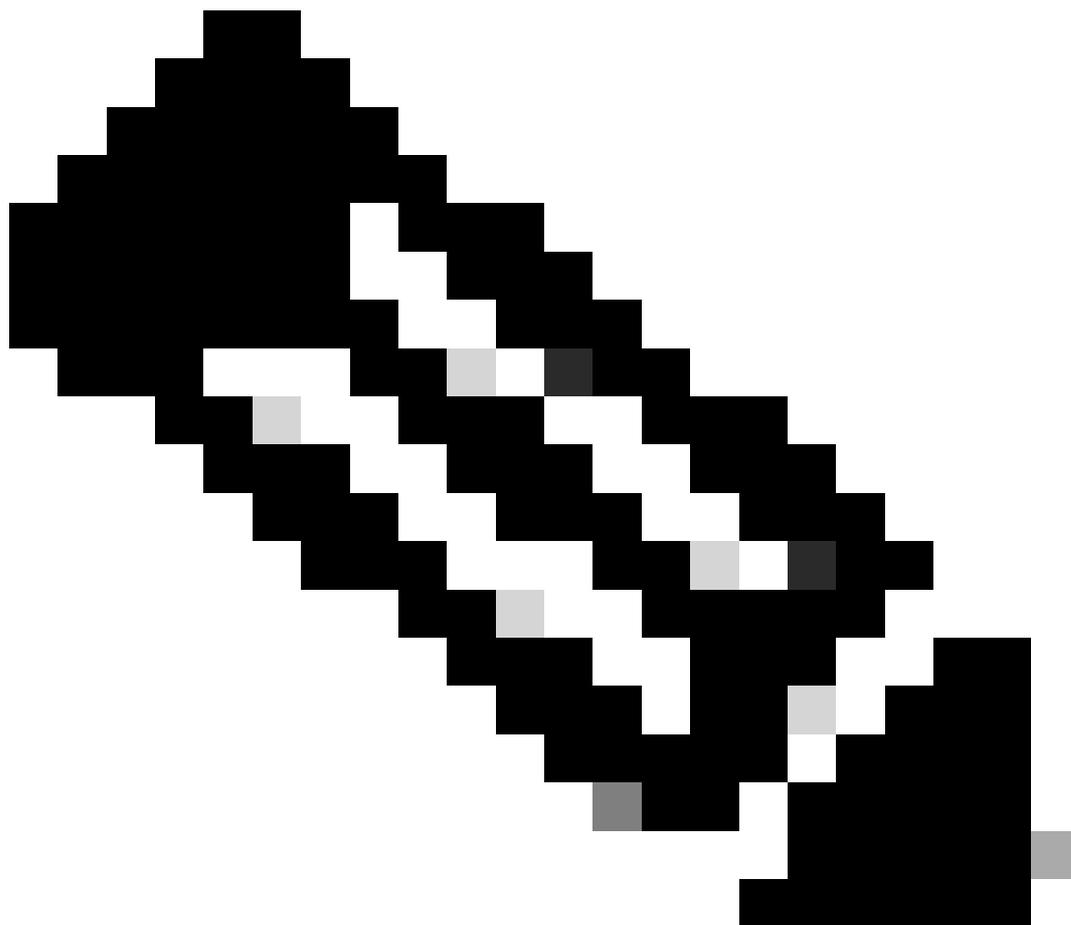


Nota: Qui, tutti i 15 Thread sono occupati da win-sparta.com allo stesso tempo senza lasciare alcun thread per demo.local

---

## Soluzione

- Il comportamento predefinito è un pool di thread comune per tutti i punti di join AD
- Tuttavia, gli amministratori possono segmentare ogni punto di join in modo che disponga di risorse proprie.



Nota: Quando viene applicata la definizione di priorità di Active Directory, l'impostazione predefinita è 10 thread per pool di thread.

---

Per ulteriori informazioni, fare riferimento alla figura 4: Diagramma di flusso del punto congiunto prenotato su richiesta



Immagine 4: Flusso della soluzione

## Configurazione dettagliata

Fase 1: Creare 2 punti di join AD separati. Di seguito sono riportati alcuni esempi: demo.local e win-sparta.com

Fase 2: Creare la definizione di priorità per i punti di join dopo la creazione dei punti di join AD.

Per ulteriori informazioni, fare riferimento alla figura 5:

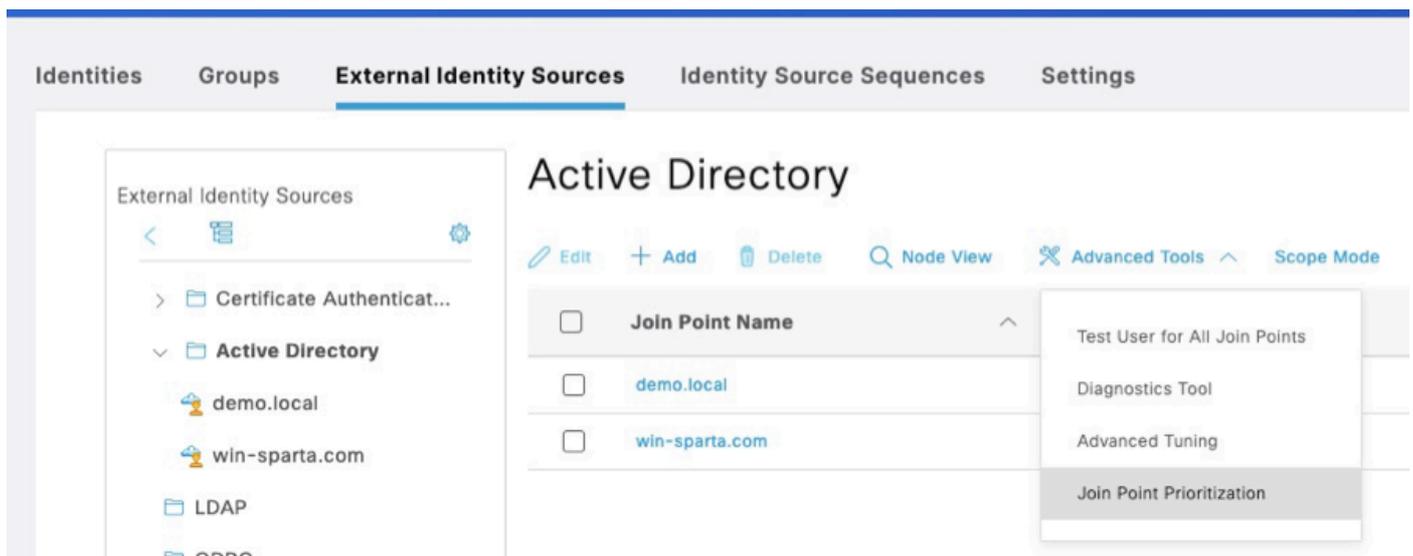


Immagine 5: Assegnazione di priorità ai punti di join

Fase 3: In Assegnazione di priorità ai punti di join selezionare il numero PSN che si desidera riservare alle risorse AD dedicate. Fare clic su Edit (Modifica).

Per ulteriori informazioni, fare riferimento alla figura 6:

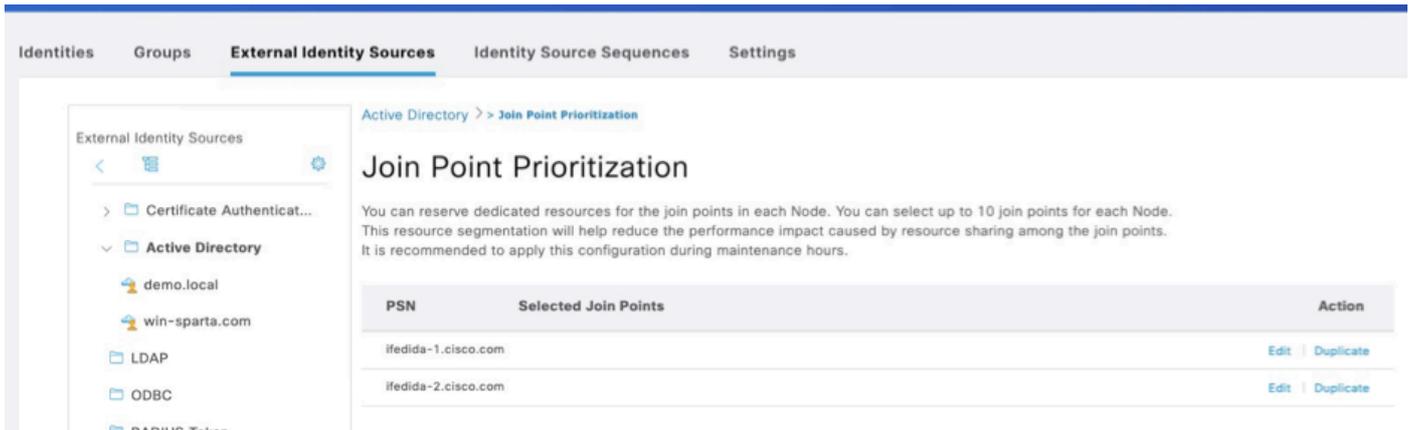


Immagine 6: Modifica PSN

Fase 4: Selezionare il punto di join preferito per il PSN preferito.

Per ulteriori informazioni, fare riferimento alla figura 7:

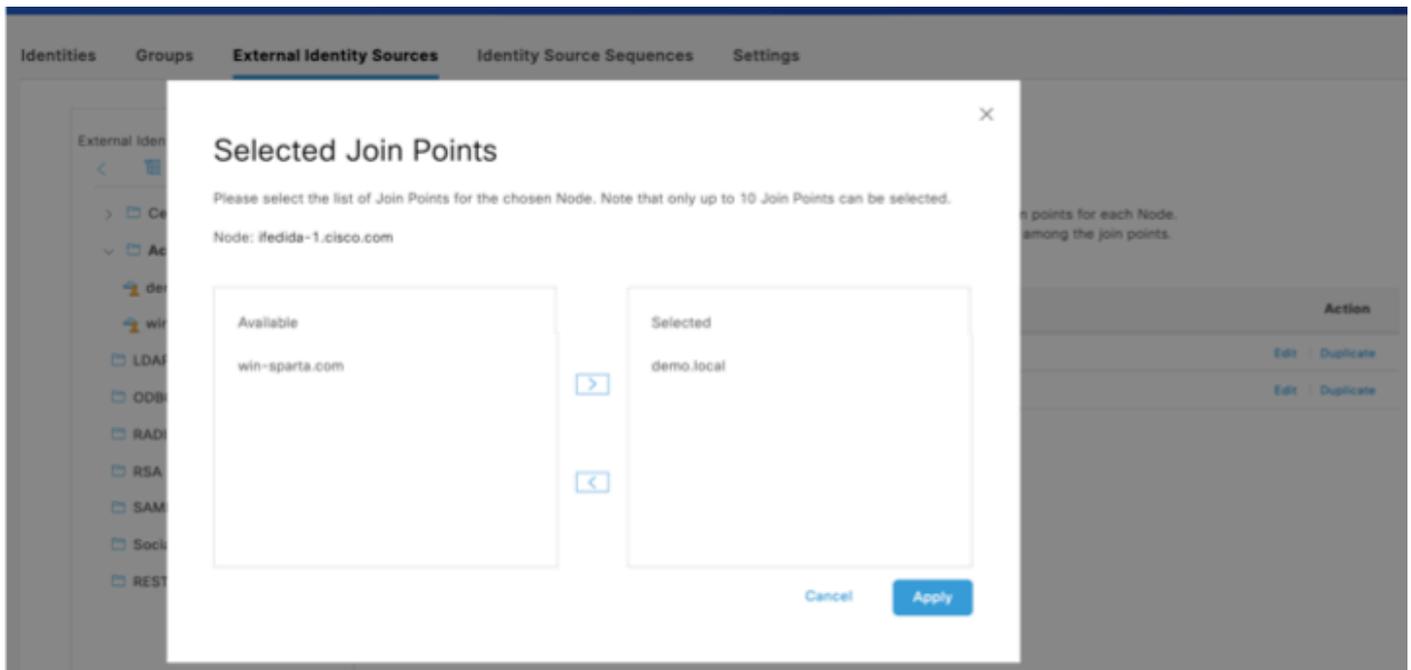
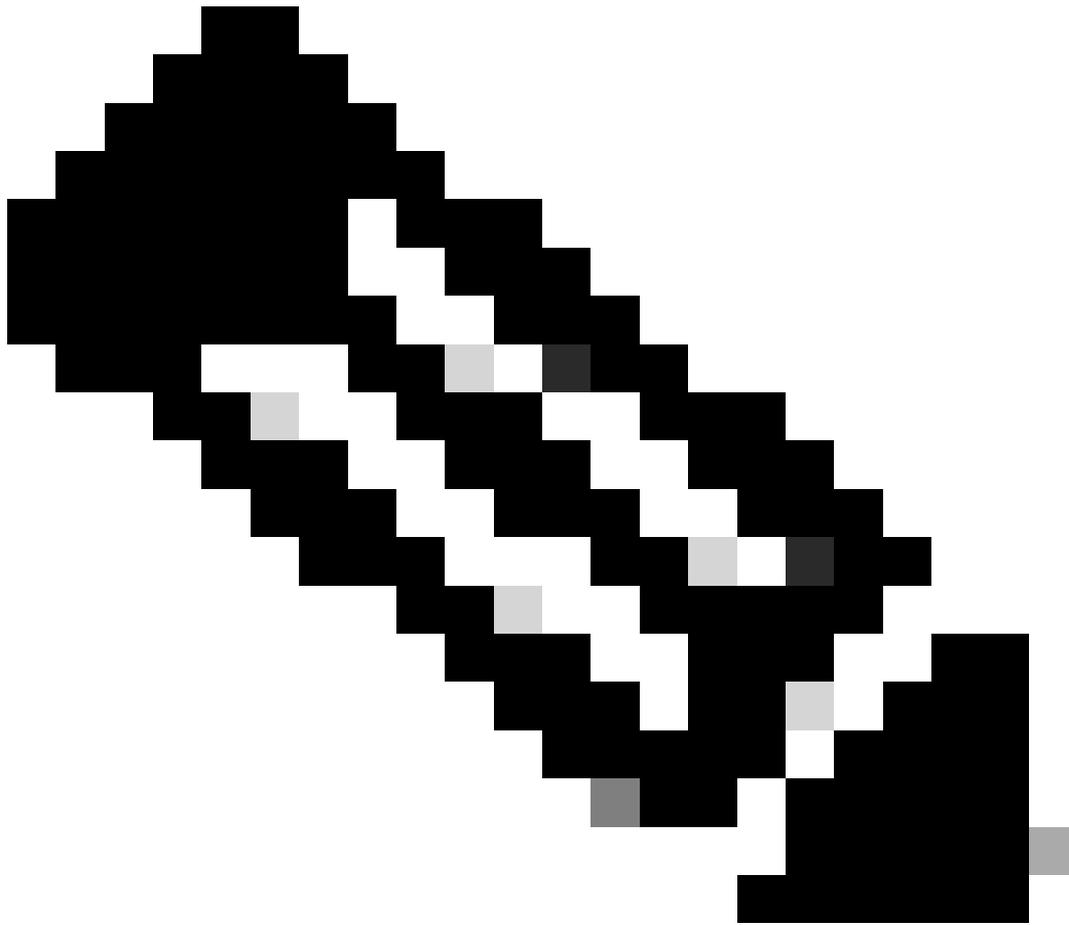


Immagine 7: Punto di join selezionato



Nota: I punti di join non inclusi nella definizione di priorità utilizzano il pool di thread comuni, che ha un limite massimo di 15 thread.

---

Fase 5: Assegnazione di priorità completata

Per ulteriori informazioni, fare riferimento alla figura 8:

Identities   Groups   **External Identity Sources**   Identity Source Sequences   Settings

External Identity Sources

- > Certificate Authentikat...
- ▼ **Active Directory**
  - demo.local
  - win-sparta.com
- LDAP
- ODBC
- RADIUS Token
- RSA SecurID
- SAML Id Providers
- Social Login
- REST

Active Directory > Join Point Prioritization

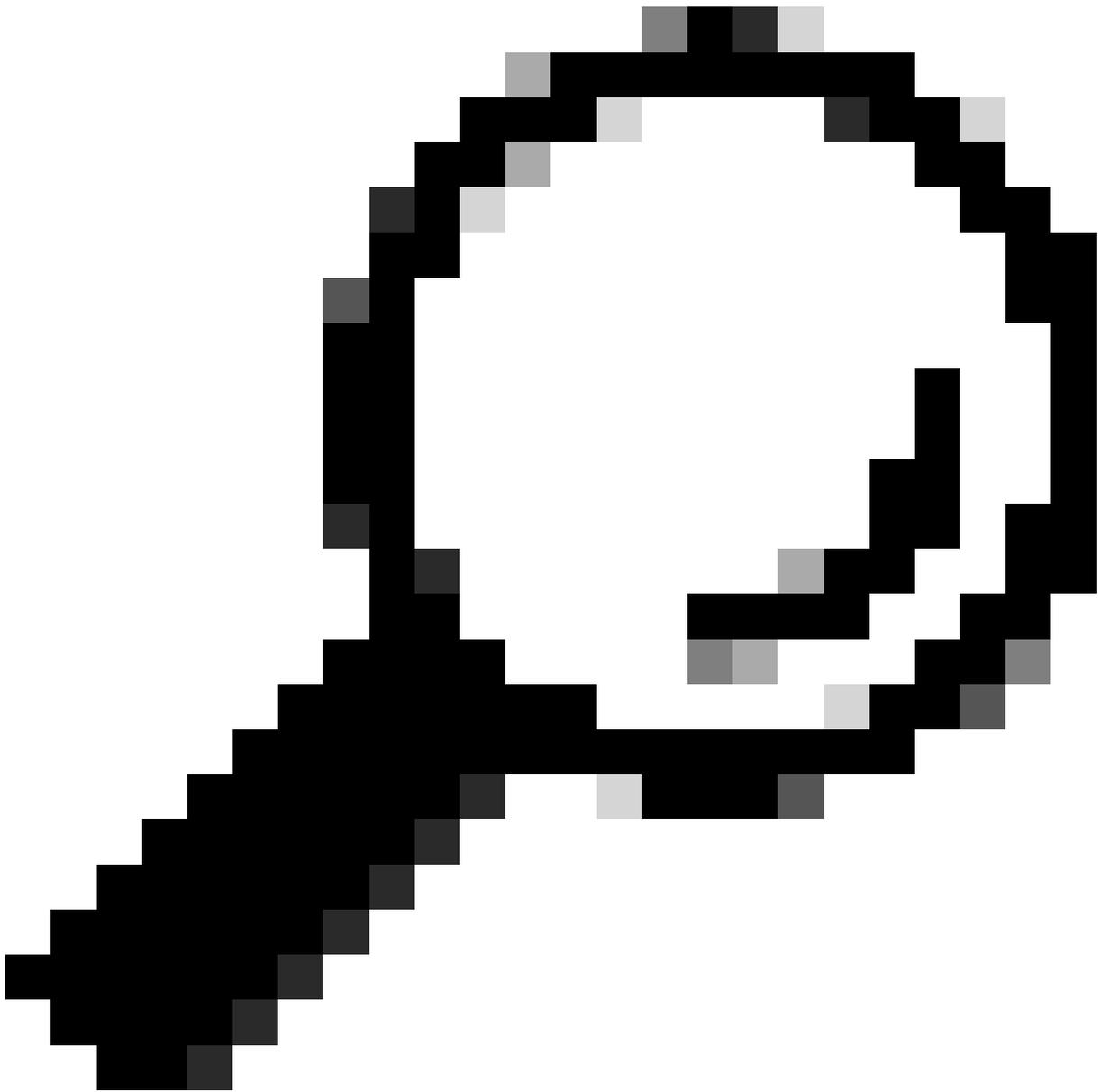
## Join Point Prioritization

You can reserve dedicated resources for the join points in each Node. You can select up to 10 join points for each Node. This resource segmentation will help reduce the performance impact caused by resource sharing among the join points. It is recommended to apply this configuration during maintenance hours.

PSN	Selected Join Points	Action
ifedida-1.cisco.com	demo.local	<a href="#">Edit</a>   <a href="#">Duplicate</a>
ifedida-2.cisco.com		<a href="#">Edit</a>   <a href="#">Duplicate</a>

Immagine 8: Configurazione assegnazione priorità

Ulteriori dettagli



Suggerimento: Se si desidera replicare le stesse impostazioni in altri nomi PSN, è possibile utilizzare l'opzione Duplica. Selezionare il PSN desiderato e scegliere il punto di join da duplicare insieme alla definizione di priorità originale.

---

Per ulteriori informazioni, fare riferimento alla figura 9: Suggerimento:

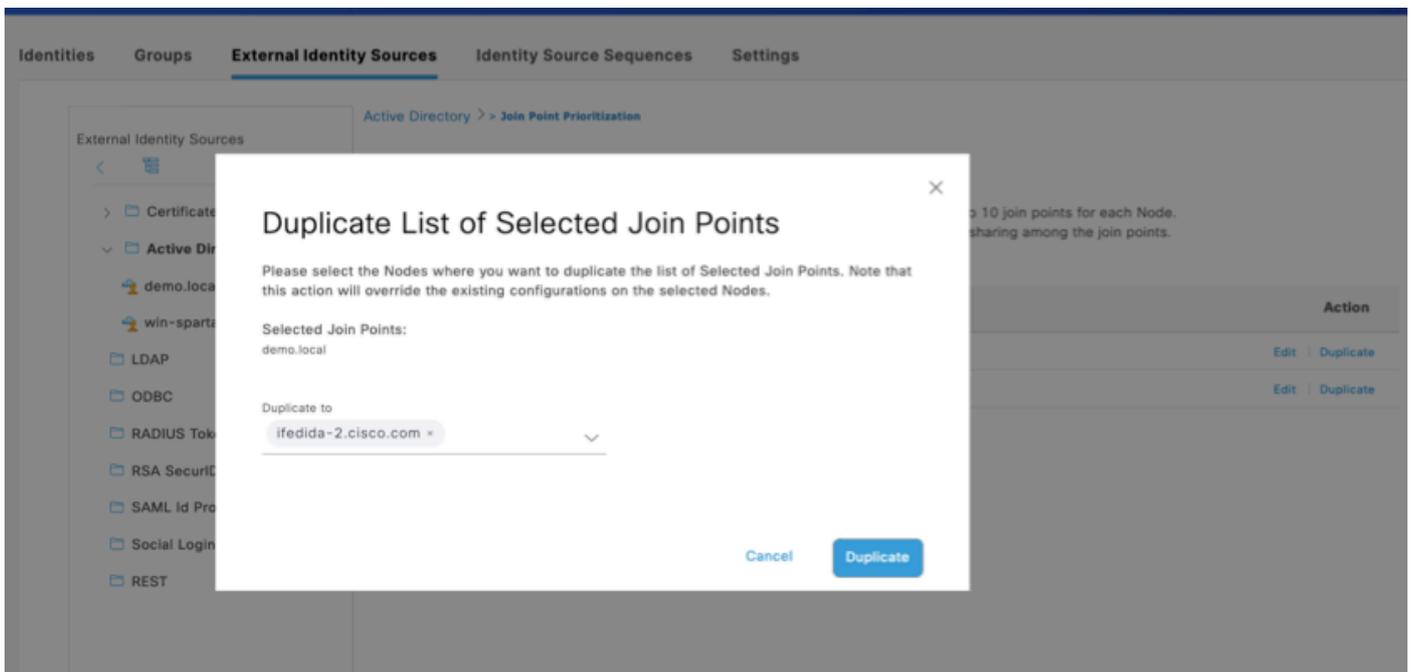


Immagine 9: Configurazione di assegnazione priorità duplicata

## Passaggio 6: Elenco finale dopo la duplicazione

Per ulteriori informazioni, fare riferimento alla figura 10:

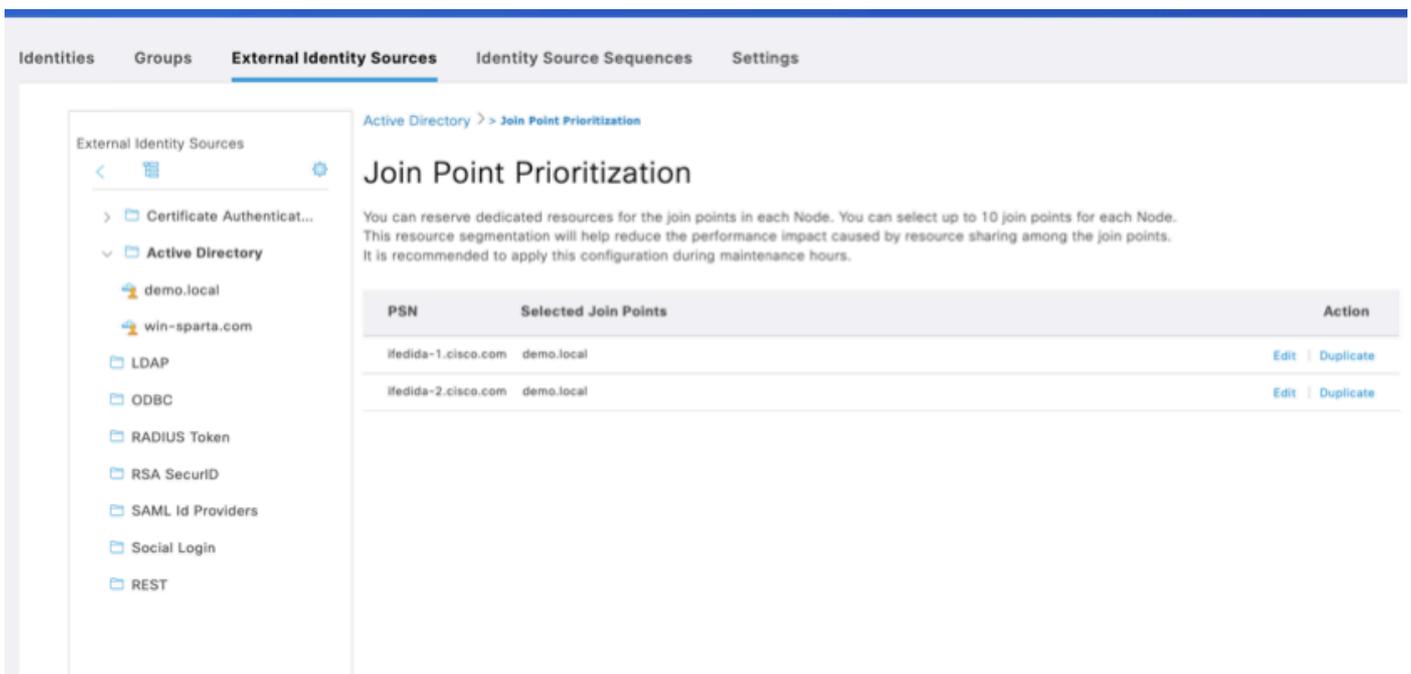


Immagine 10: Elenco finale dopo la definizione di priorità

# Risoluzione dei problemi

## Verifica

Verificare le modifiche alla configurazione. Accedere a: Operazioni > Report > Audit > Modifica audit configurazione

Per ulteriori informazioni, fare riferimento alla figura 11:

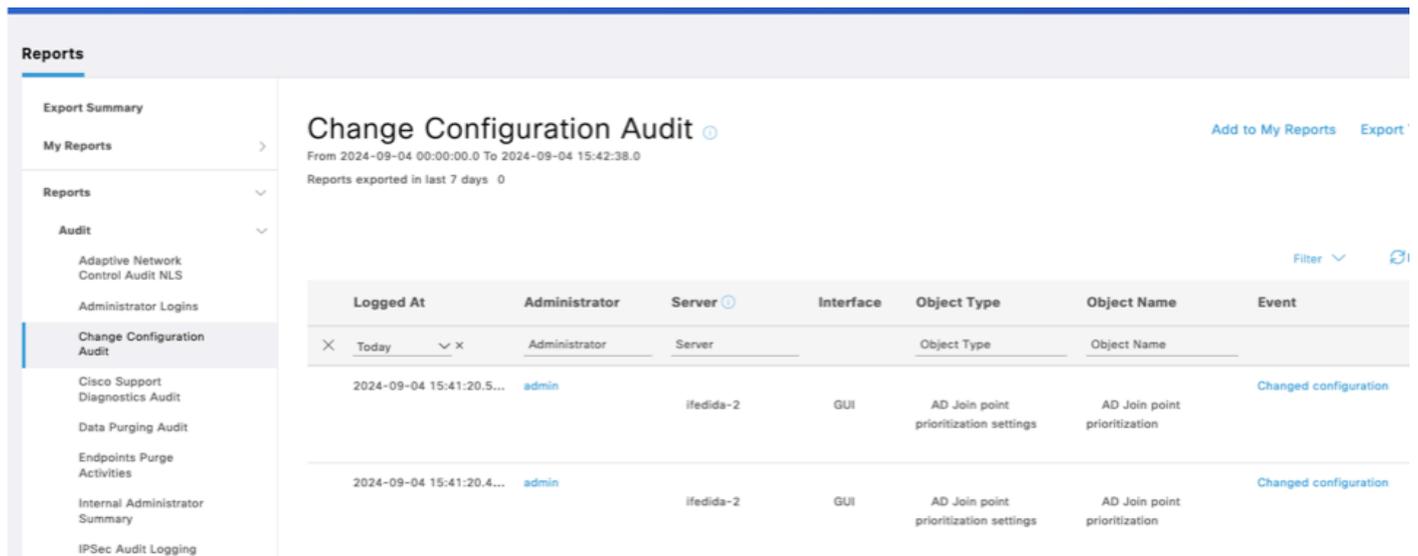


Immagine 11: Configura report di audit

## Registrazione

- Abilitare il livello di debug per i log AAA di runtime.
- Analizza prrt-server.log

Per ulteriori informazioni, fare riferimento alla figura 12:



Immagine 12: Configurazione registro di debug

## Registra frammenti

port-server.log [DEBUG]: Registro predefinito:

EventHandler,2024-08-23 07:16:48,135,DEBUG,0x7fec2ccc700,Pool di thread predefinito allocato: ADIDStore su IDP: win-sparta.com\_wxETIH16Pk\_106

prrt-server.log [INFO]: quando si impostano le risorse dedicate:

- ActiveDirectoryIDStore,2024-09-08 16:52:01,048,INFO ,0x7f2452ccf700,Pool di thread allocato: ADThreadPool0 in IDP: win-sparta.com\_wxETIH16Pk\_106
- ActiveDirectoryIDStore,2024-09-08 16:57:11,258,INFO ,0x7f2452ccf700,Pool di thread allocato: ADThreadPool1 su IDP: demo.local\_6EcNs6UzwX\_89

port-server.log [INFORMAZIONI]:

- Prima di impostare le risorse dedicate:
  - EventHandler, 2024-09-02 08:45:54,673,INFO,0x7fafb793c700,Evento passato al successivo pool di thread name=ADIDStore, queue size=1,EventDispatcher.cpp:757
- Dopo aver impostato le risorse dedicate:

- EventHandler,2024-09-02 08:45:54,673,INFO ,0x7f4867ff9700,Evento passato al successivo nome pool di thread=ADThreadPool0, dimensioni coda=1,EventDispatcher.cpp:841

Per tenere traccia dell'utilizzo del pool di thread di "ADThreadPool0":

1. 0x7f57792f7700,Evento passato al successivo pool di thread name=ADThreadPool0 (pochi log indietro StackID:0x7f57a4f761c0)
2. 0x7f57732c7700,Stack: 0x7f57a4f761c0 Chiamata ad ActiveDirectoryIDStore: MethodCaller<ActiveDirectoryIDStore, PlainAuthenticateAndQueryEvent>
3. 0x7f57732c7700,cntx=0000210117,ssen=ifedida-1/515863662/5273,CPMSessionID=C0A314300000080018958,user=abcd,CallingStationID=[CAD] 956: CAD\_PAPAuthenticate (abcd) chiamato
4. 0x7f57732c7700,cntx=0000210117,ssen=ifedida-1/515863662/5273,CPMSessionID=C0A314300000080018958,user=abcd,CallingStationID=[CAD] 1026: CAD\_PAPAuthenticate (abcd) completato
5. 0x7f57732c7700,Evento passato al successivo pool di thread name=Main

## Domande frequenti

Domanda: Quanti AD Join Point può supportare ISE?

Risposta. È possibile configurare fino a 50 punti di join di Active Directory su una singola implementazione ISE.

Domanda: Se si dispone di più punti di accesso ad Active Directory, è ancora possibile utilizzare l'assegnazione di priorità su richiesta?

Risposta. Sì

Domanda: Quali sono le dimensioni predefinite del thread senza definizione di priorità per un singolo dominio?

Risposta. 15 thread

Domanda: Se si configura l'assegnazione di priorità, come viene eseguito il calcolo? Si consideri uno scenario con 3 punti di join: domain1.com, domain2.com e domain3.com con domain1.com non è configurato per Prioritization e domain2.com e domain3.com sono configurati per Prioritization.

Risposta. Se domain1 non è configurato per la definizione di priorità, domain1.com utilizza i comuni 15 thread disponibili, tutti contemporaneamente. Tuttavia, poiché domain2.com e domain3.com sono configurati con Prioritization, utilizzano 10 thread ciascuno per impostazione predefinita e non seguono/utilizzano il pool comune di 15 thread.

## Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).