

瞭解ISE 3.3補丁4上AD的按需資源保留

目錄

[簡介](#)

[前提條件](#)

[所需元件](#)

[背景資訊](#)

[症狀](#)

[問題](#)

[解決方案](#)

[逐步配置](#)

[其他詳細資訊](#)

[疑難排解](#)

[驗證](#)

[日誌記錄](#)

[日誌片段](#)

[常見問題](#)

簡介

本文檔介紹有關ISE 3.3補丁4上Active Directory的按需資源保留

前提條件

思科身份服務引擎(ISE)知識

Active Directory(AD)知識

有關ISE和AD整合的知識

所需元件

本文件中的資訊是以下列軟體和硬體版本為依據

- 思科身分識別服務引擎3.3補丁4
- Microsoft Windows Active Directory 2016或最新版本

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除 (預設) 的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

AD身份驗證有時很慢，最終會失敗。可能的原因可能是ADID隊列開始堆積或所有ADID池執行緒耗盡。

有關ADID的更多詳細資訊：

ADID(也稱為可分辨名稱(DN))是一個字串，用於唯一標識Active Directory目錄中的對象。它們用於查詢和管理Active Directory域中的對象。ADID對於管理Active Directory環境中的使用者帳戶、許可權和其他資源至關重要。

典型的ADID必須如下所示：CN=John Doe，OU=Sales，DC=example，DC=com;其中，

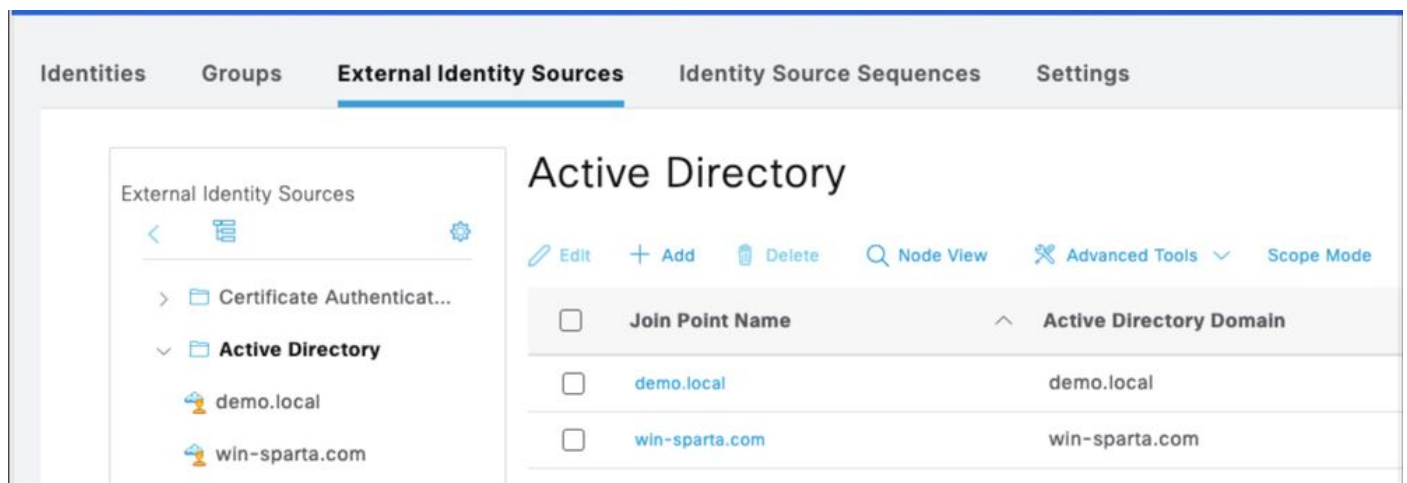
CN=John Doe:表示使用者的公用名John Doe。

OU=銷售：表示使用者所屬的組織單位(OU)，在本例中為銷售部門。

DC=example，DC=com:表示域元件，即example.com。

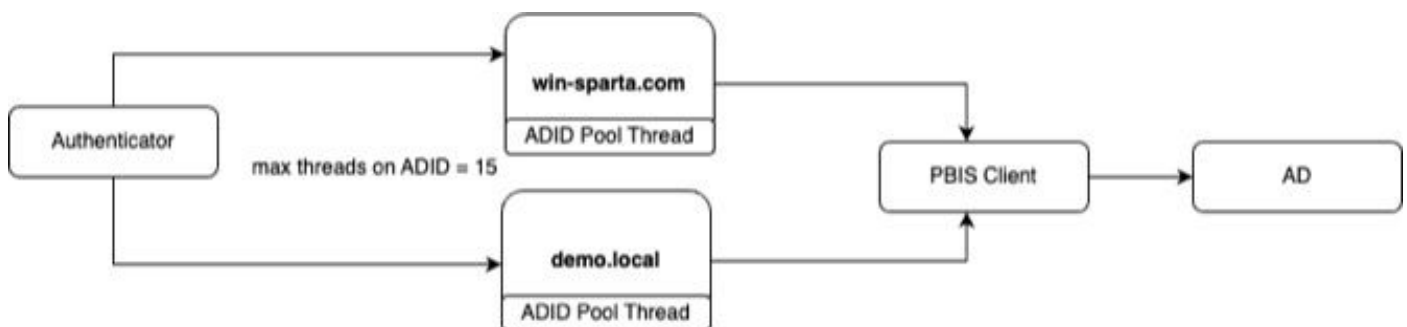
舉例來說：

請參閱圖片1:典型的AD連線點配置



圖片1:AD加入點

請參閱圖片2:具有2個連線點的典型AD流程圖



圖片2:典型的AD流程圖

症狀

同一ADID執行緒池下的慢加入點

問題

1. 其中一個連線點非常慢的後果是什麼？例如，如果「demo.local」和「demo.local」的15個身份驗證同時傳送到ISE的速度異常緩慢，我們將需要等待「demo.local」的響應，然後再處理後續的win-sparta身份驗證。
2. 如果兩個連線點在一個連線點下共用同一個ADID執行緒池會怎樣？

請參閱圖3:慢節點流程圖

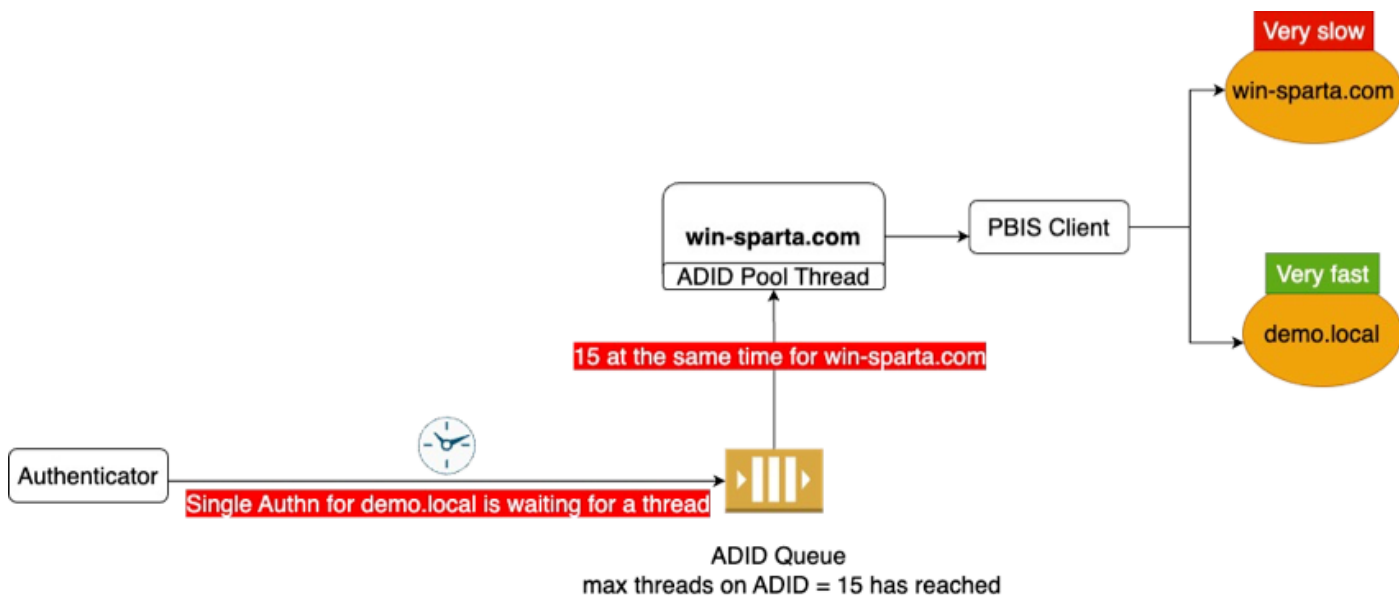


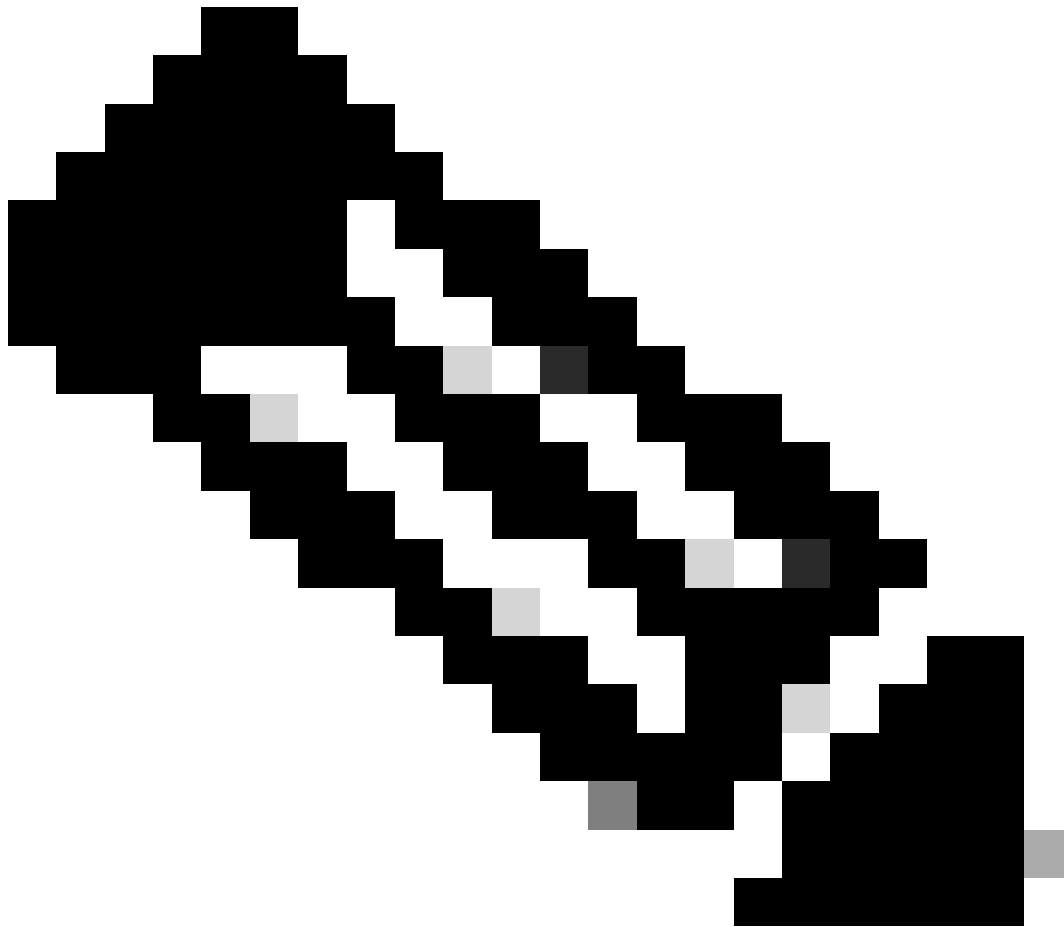
圖3:有問題的流



附註：這裡，所有15個執行緒同時由win-sparta.com佔用，沒有執行緒用於demo.local

解決方案

- 預設行為是所有AD連線點的公共執行緒池
- 但是，管理員可以對每個連線點進行分段，使其具有自己的資源。



附註：應用AD優先順序時，預設情況下每個執行緒池有10個執行緒。

請參閱圖4:按需預留節點流程圖



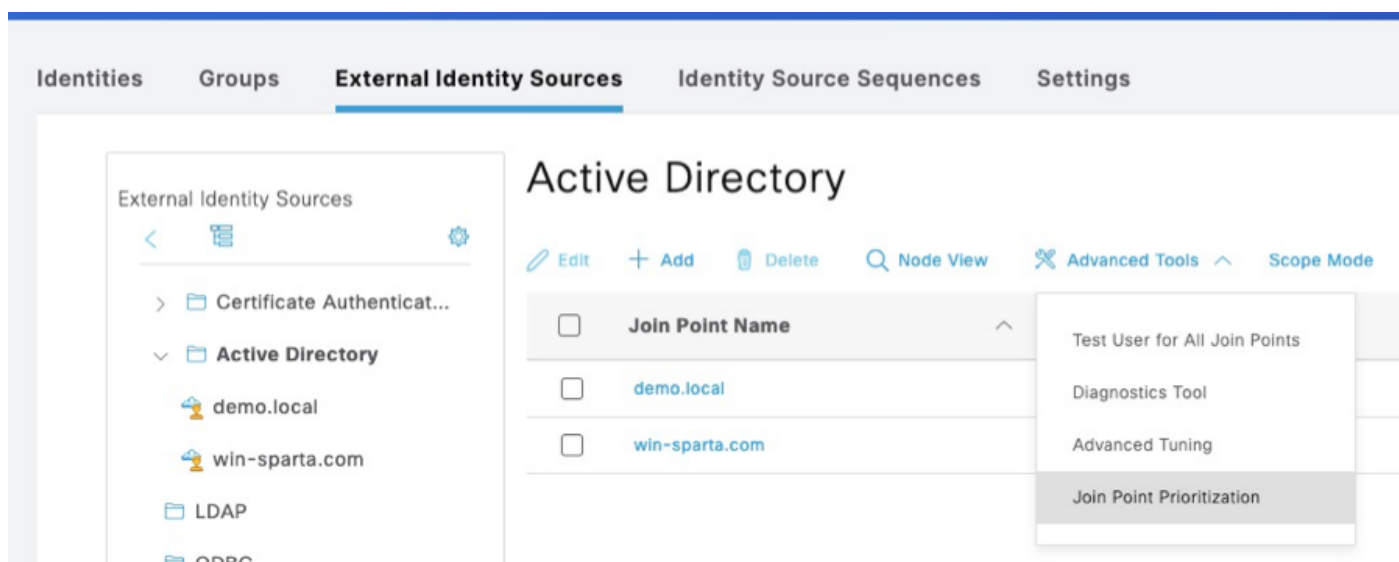
圖片4:解決方案流

逐步配置

第1步：建立2個單獨的AD連線點。例如：demo.local和win-sparta.com

第2步：建立AD加入點後建立加入點優先順序。

請參閱圖5:



圖片5:加入點優先排序

第3步：在加入點優先順序下，選擇您希望保留專用AD資源的PSN。按一下「編輯」。

請參閱圖6:

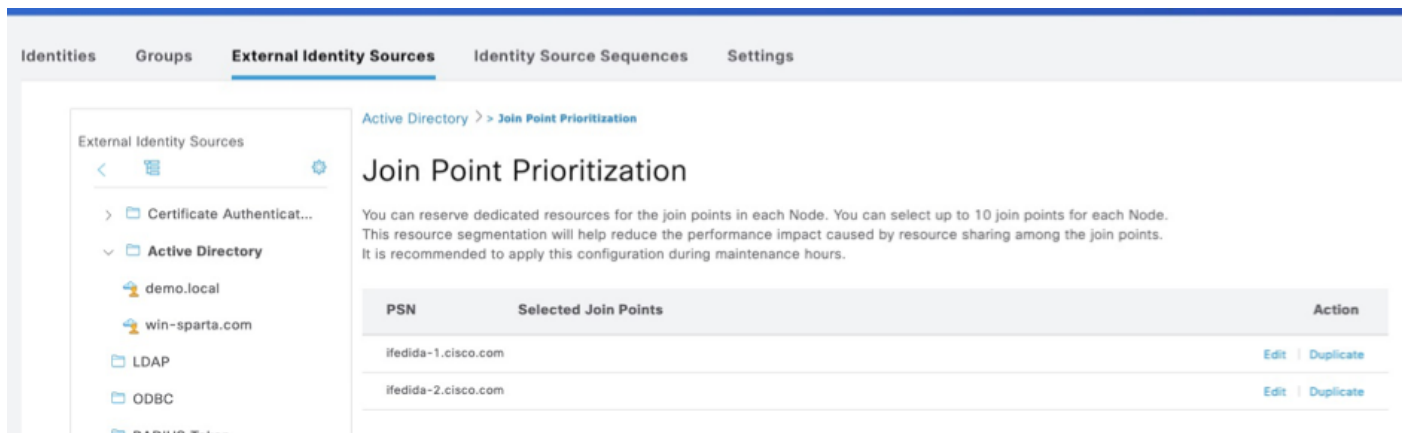


圖6:編輯PSN

第4步：選擇首選PSN的首選連線點。

請參閱圖7:

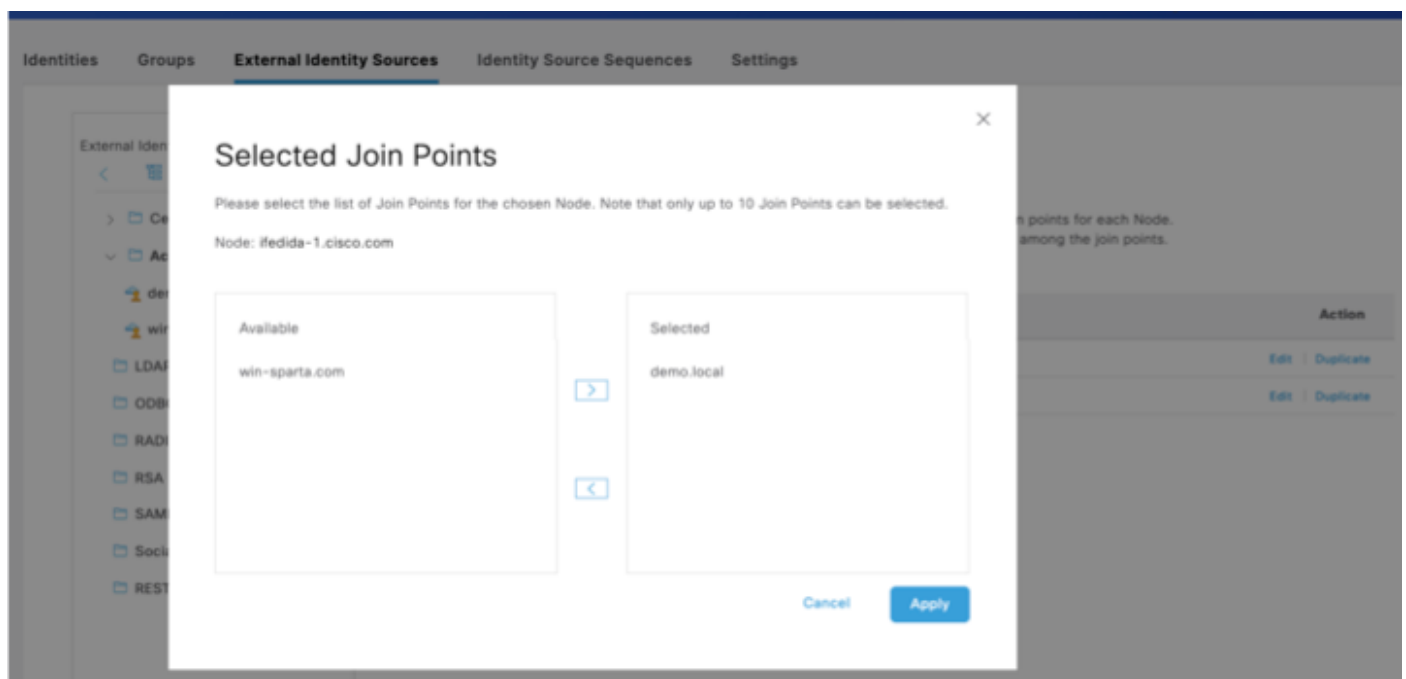
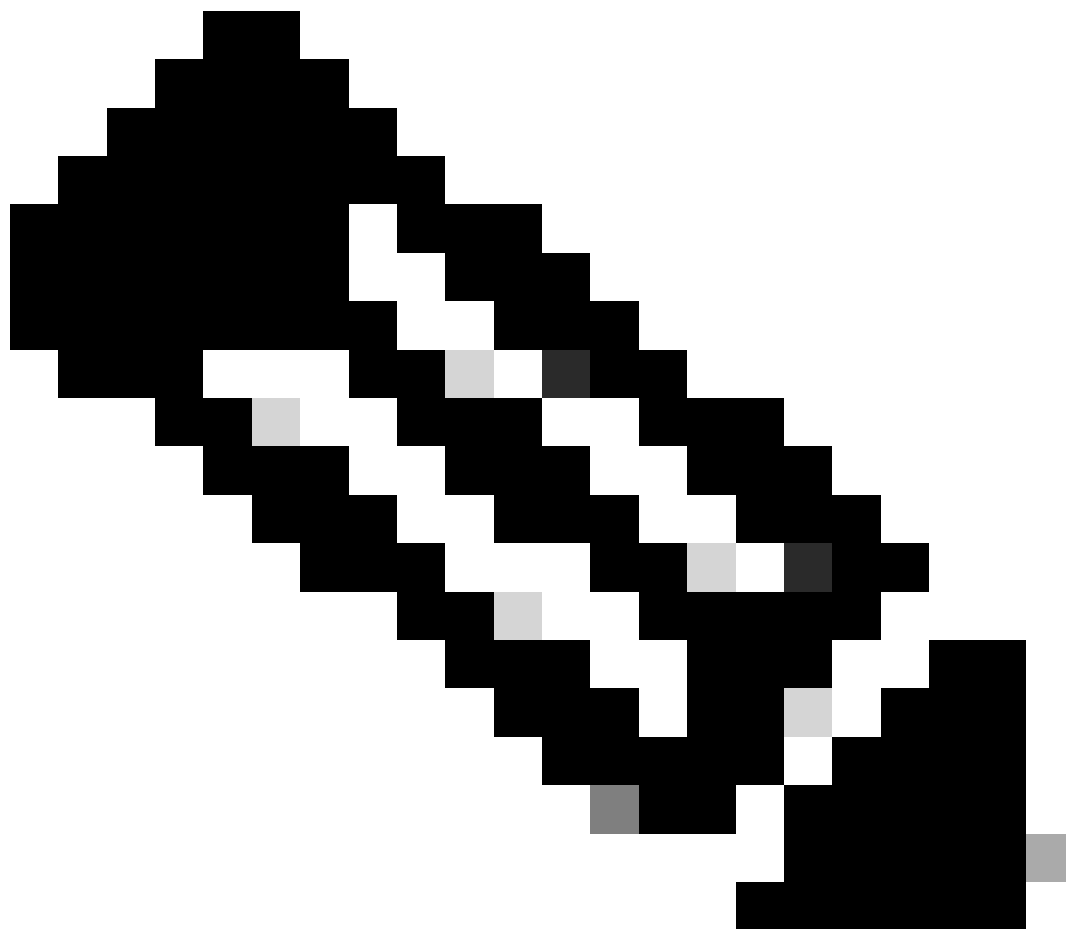


圖7:選定的加入點



附註：未包括在優先順序中的任何加入點都使用公共執行緒池，該池最多限制為15個執行緒。

第5步：已完成優先排序

請參閱圖8:

IdentitiesGroupsExternal Identity SourcesIdentity Source SequencesSettings

External Identity Sources

<📁⚙️

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

Active Directory > > Join Point Prioritization

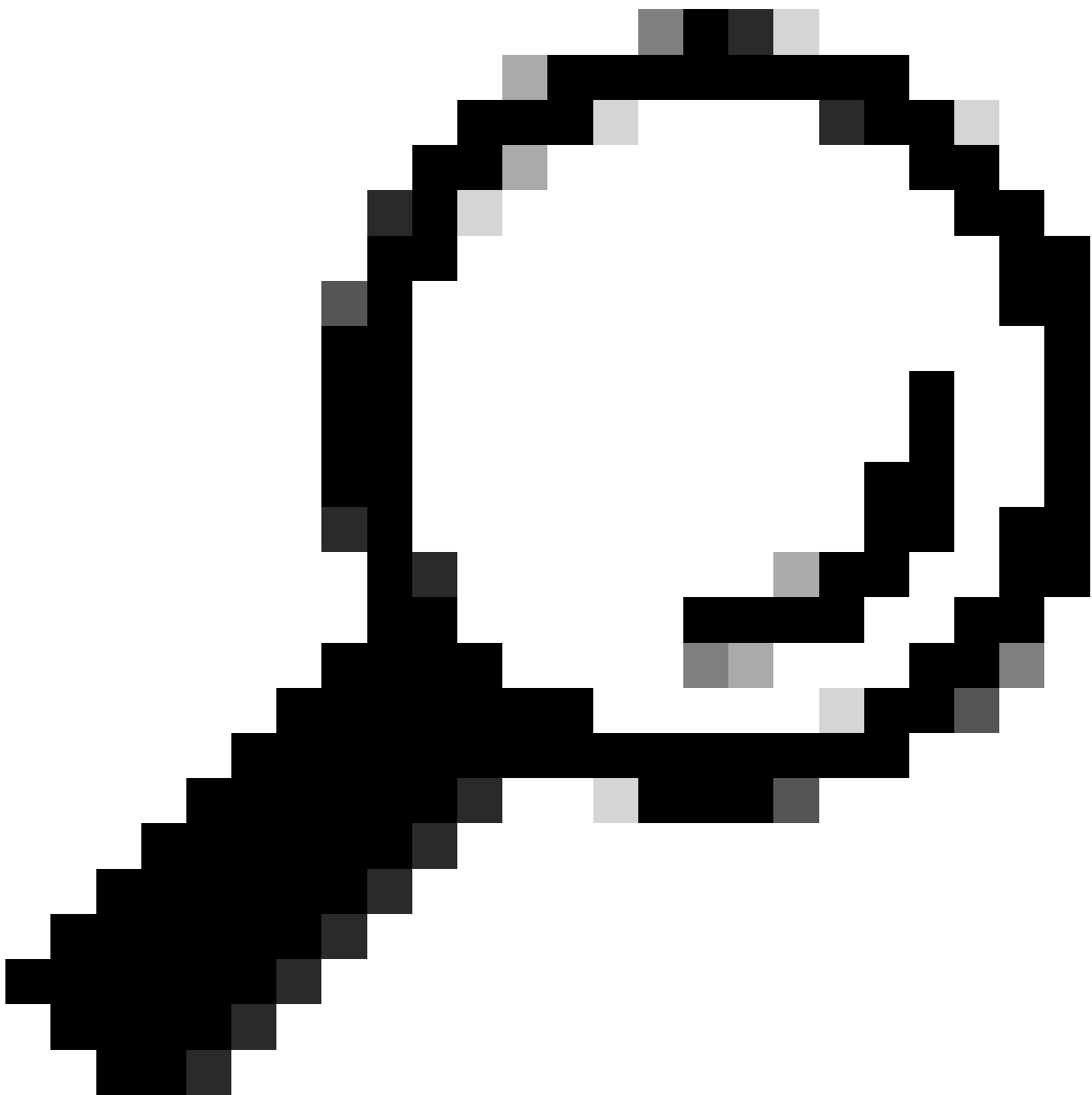
Join Point Prioritization

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	Edit Duplicate
ifedida-2.cisco.com		Edit Duplicate

圖8:優先順序配置

其他詳細資訊



提示：如果要將相同的設定複製到其他PSN，可以使用Duplicate選項。選擇所需的PSN，然後選擇要與原始優先順序一起複製的加入點。

請參閱圖9:配置提示：

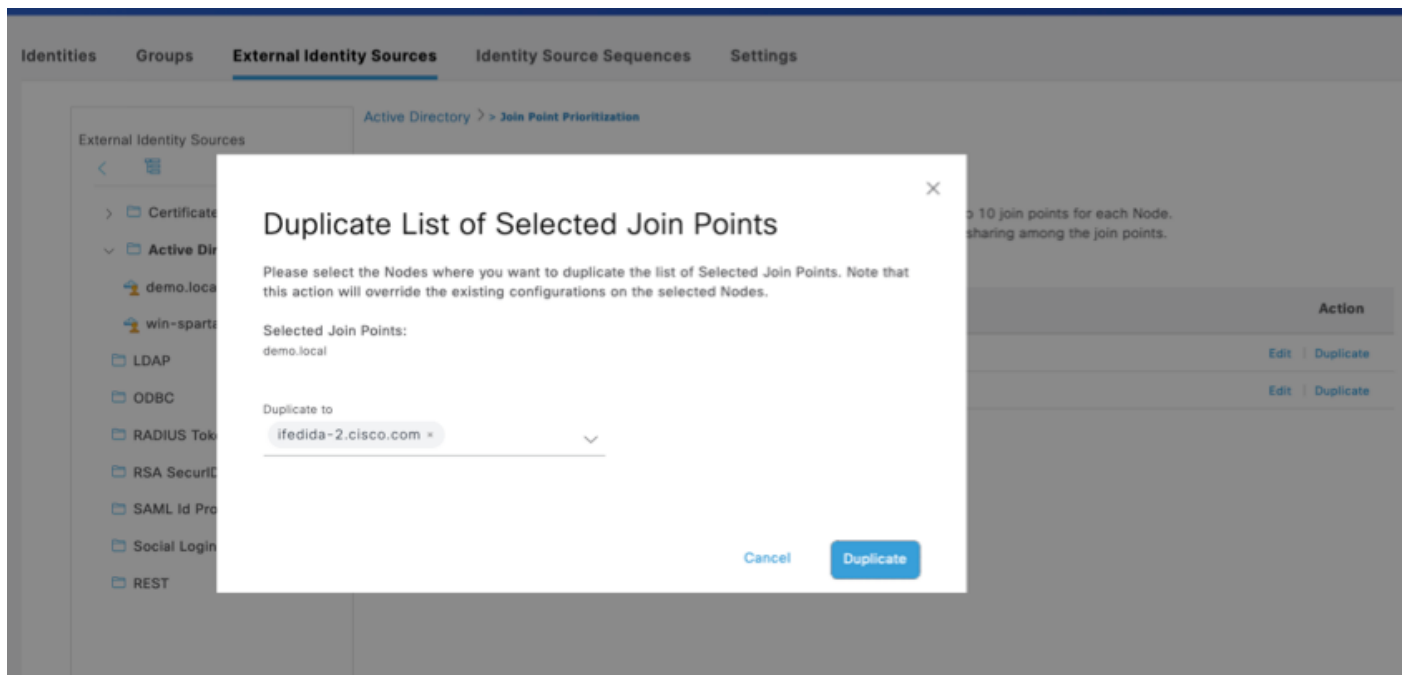
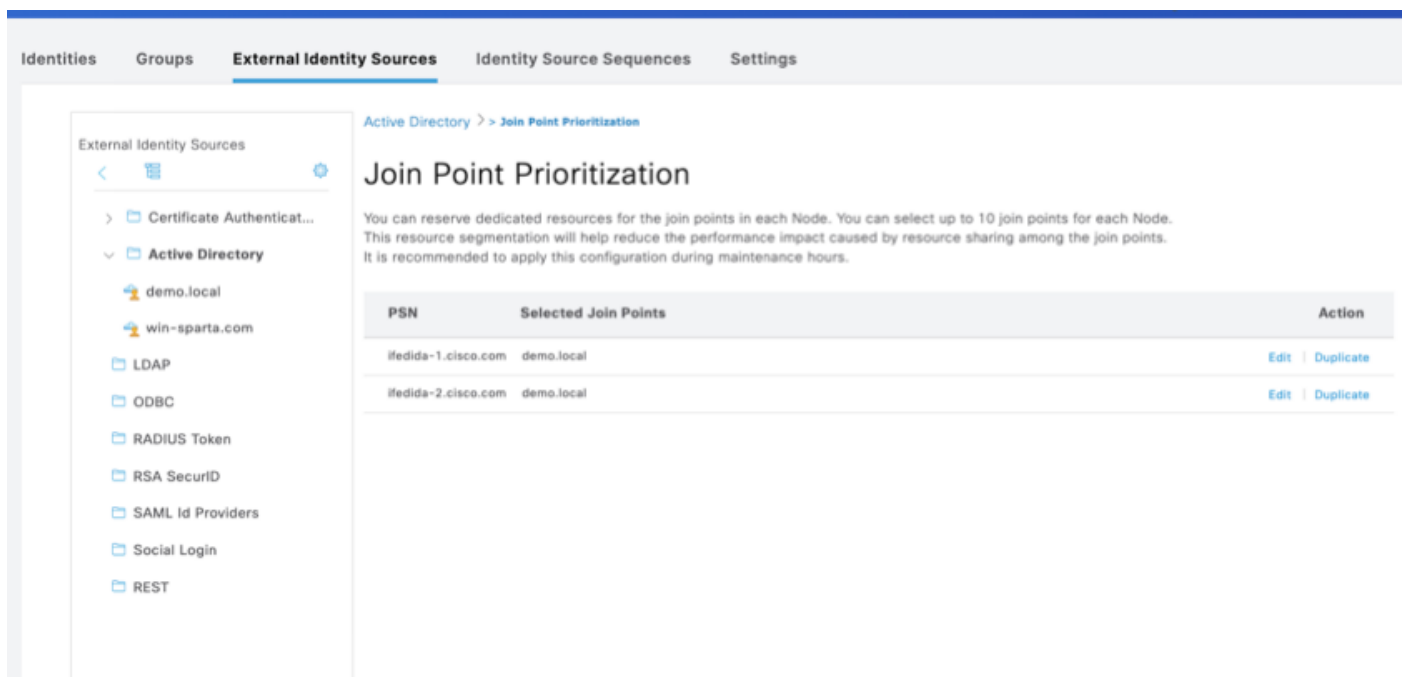


圖9:重複的優先順序配置

第6步：複製後最終清單

請參閱圖片10:



圖片10:確定優先順序後的最終清單

疑難排解

驗證

驗證配置更改。導覽至：操作>報告>稽核>更改配置稽核

請參閱圖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

圖片 11:配置審計報告

日誌記錄

- 為運行時AAA日誌啟用調試級別。
 - 分析prrt-server.log
- 請參閱圖12:

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

圖片 12:調試日誌配置

日誌片段

prrt-server.log [DEBUG]:默認日誌：

EventHandler，2024-08-23 07:16:48,135,DEBUG，0x7fecd2ccc700，分配的默認線程池：新增至IDP:win-sparta.com_wxETIH16Pk_106

prrt-server.log [INFO]：設置專用資源時:

- ActiveDirectoryIDStore，2024-09-08 16:52:01,048,INFO，0x7f2452ccf700，分配的執行緒池：ADThreadPool0到IDP :win-sparta.com_wxETIH16Pk_106
- ActiveDirectoryIDStore，2024-09-08 16:57:11,258,INFO，0x7f2452ccf700，分配的執行緒池：ADThreadPool1到IDP :demo.local_6EcNs6UzwX_89

prrt-server.log [INFO]:

- 在設置專用資源之前：
 - EventHandler，2024-09-02 08:45:54,673,INFO，0x7fafb793c700，將事件傳遞到下一個執行緒池名稱=ADIDStore，隊列大小=1,EventDispatcher.cpp:757
- 在設置專用資源之後：

- EventHandler , 2024-09-02 08:45:54,673,INFO , 0x7f4867ff9700 , 將事件傳遞到下一個執行緒池name=ADThreadPool0 , 隊列大小=1,EventDispatcher.cpp:841

跟蹤"ADThreadPool0"的執行緒池使用情況：

1. 0x7f57792f7700 , 將事件傳遞到下一個執行緒池名稱= ADThreadPool0 (少數日誌返回 StackID:0x7f57a4f761c0)
2. 0x7f57732c7700 , 堆疊：0x7f57a4f761c0呼叫ActiveDirectoryIDStore:方法 MethodCaller<ActiveDirectoryIDStore , PlainAuthenticateAndQueryEvent>
3. 0x7f57732c7700,cntx=0000210117,sesn=ifedida-1/515863662/5273,CPMSessionID=C0A31430000000800018958,user=abcd , CallingStationID=[CAD] 956:已呼叫CAD_PAPAuthenticate(abcd)
4. 0x7f57732c7700,cntx=000210117,sesn=ifedida-1/515863662/5273,CPMSessionID=C0A31430000000800018958,user=abcd,CallingStationID=[CAD] 1026:CAD_PAPAuthenticate(abcd)成功
5. 0x7f57732c7700 , 將事件傳遞到下一個執行緒池名稱=Main

常見問題

問題：ISE可以支援多少個AD加入點？

答案：您可以在單個ISE部署上配置最多50個Active Directory加入點。

問題：如果我有多個AD加入點，是否仍可使用按需優先順序排序？

答案：是

問題：對於單個域，沒有優先順序的預設執行緒大小是多少？

答案：15個執行緒

問題：如果配置優先順序，如何進行計算？考慮一下，未針對優先順序配置3個加入點方案 — domain1.com、domain2.com和domain3.com domain1.com，以及domain2.com和domain3.com針對優先順序配置。

答案：如果未將domain1配置為優先排序，則domain1.com會同時使用常用的15個執行緒。但是，由於domain2.com和domain3.com配置了優先順序，因此它們預設使用10個執行緒，並且不遵循/利用公共的15個執行緒池。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。