

ISE 3.3パッチ4でのADのオンデマンドリソース予約について

内容

[はじめに](#)

[前提条件](#)

[必要なコンポーネント](#)

[背景説明](#)

[症状](#)

[問題](#)

[解決方法](#)

[ステップバイステップ設定](#)

[その他の詳細事項](#)

[トラブルシューティング](#)

[検証](#)

[Logging](#)

[ログのスニペット](#)

[FAQ](#)

はじめに

このドキュメントでは、ISE 3.3パッチ4のActive Directoryのオンデマンドリソース予約(ODR)について説明します。

前提条件

Cisco Identity Services Engine(ISE)に関する知識

Active Directory(AD)の知識

ISEとADの統合に関する知識

必要なコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco Identity Services Engine 3.3パッチ4
- Microsoft Windows Active Directory 2016または最新

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな (デフォルト) 設定で作業を開始していま

す。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

AD認証は低速で、最終的には失敗する場合があります。考えられる理由は、ADIDキューが積み重なり始めるか、すべてのADIDプールスレッドが使い果たされていることです。

ADIDの詳細：

ADIDは、識別名(DN)とも呼ばれ、Active Directoryディレクトリ内のオブジェクトを一意に識別する文字列です。Active Directoryドメイン内のオブジェクトを検索および管理するために使用されます。ADIDは、Active Directory環境内のユーザーアカウント、アクセス許可、およびその他のリソースを管理するために重要です。

一般的なADIDは次のようになります。CN=John Doe,OU=Sales,DC=example,DC=com; where,

- CN=John Doe：ユーザの共通名John Doeを表します。
- OU=Sales：ユーザが属する組織単位(OU) (この場合は営業部門) を表します。
- DC=example,DC=com：ドメインコンポーネント(example.com)を表します。

例：

図1：一般的なAD参加ポイント設定を参照してください。

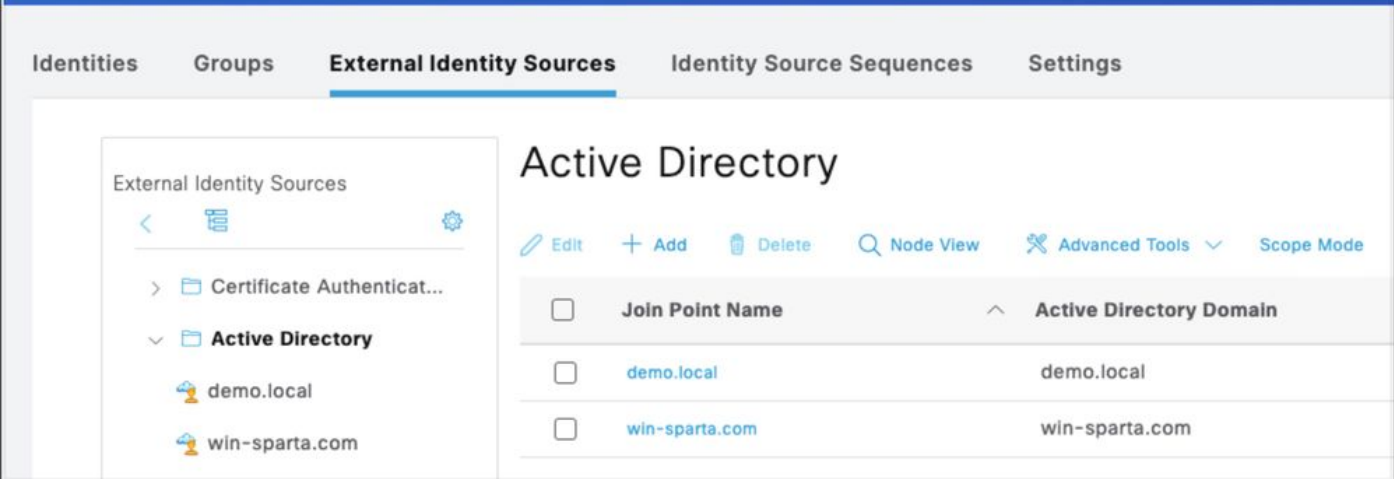


図1:AD参加ポイント

図2「2つの接続ポイントを持つ一般的なADフロー図」を参照してください。

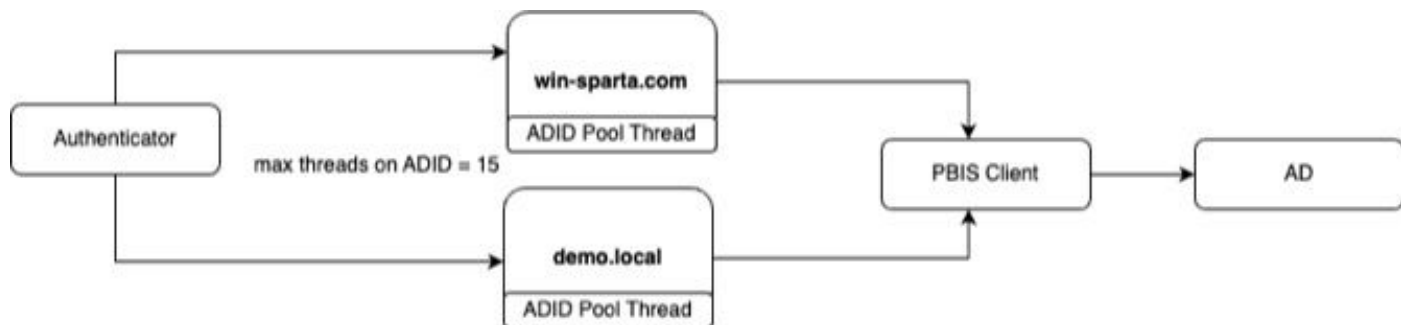


図2：一般的なADフロー図

症状

同じADIDスレッドプールの低速な結合ポイント

問題

1. 結合ポイントの1つが非常に遅いと、どのような結果になるか？たとえば、「demo.local」と「demo.local」に対する15の認証が同時にISEに送信されると、通常は遅くなります。後続のwin-sparta認証を処理する前に、「demo.local」からの応答を待つ必要があります。
2. 両方の結合ポイントが1つの結合ポイントで同じADIDスレッドプールを共有する場合はどうすればいいですか。

図3「遅いジョイント点のフロー図」を参照してください。

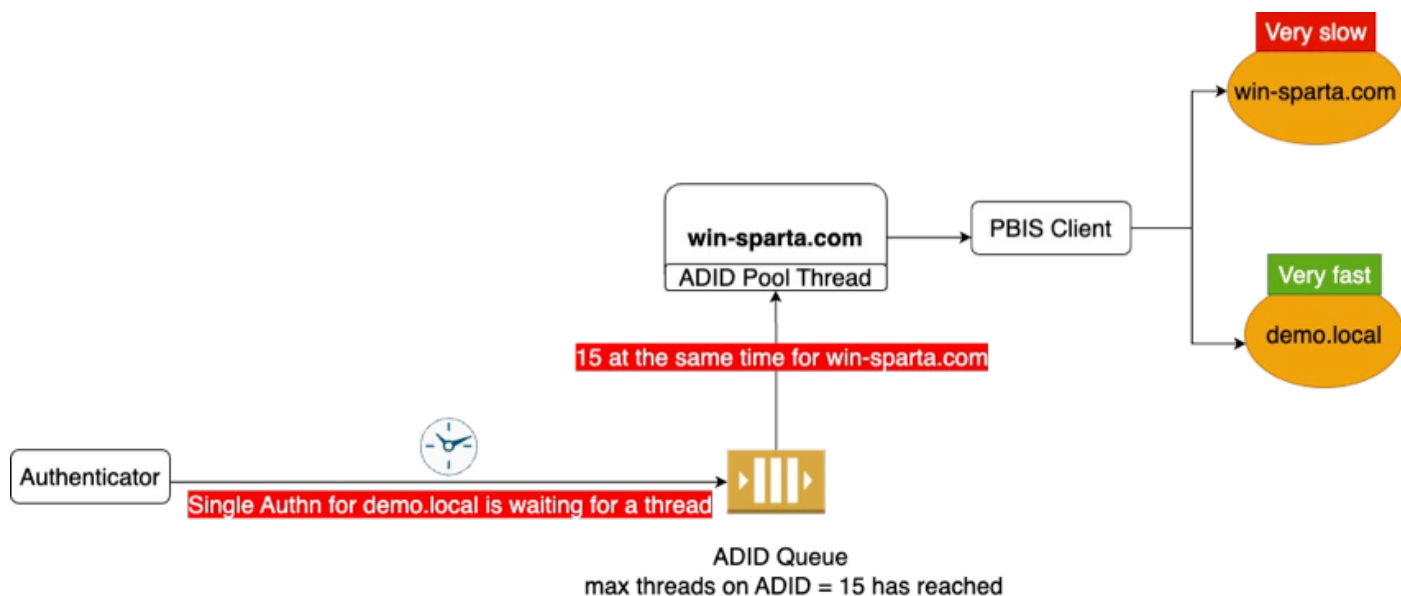
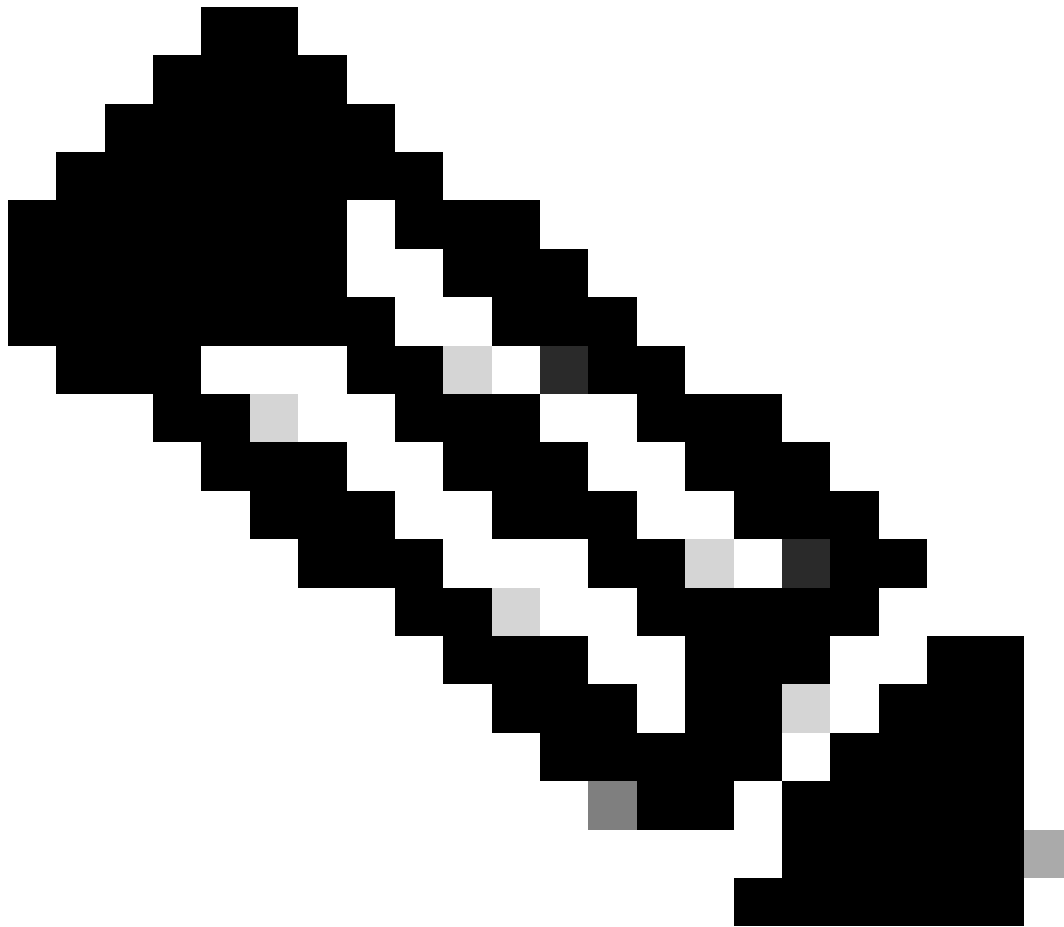


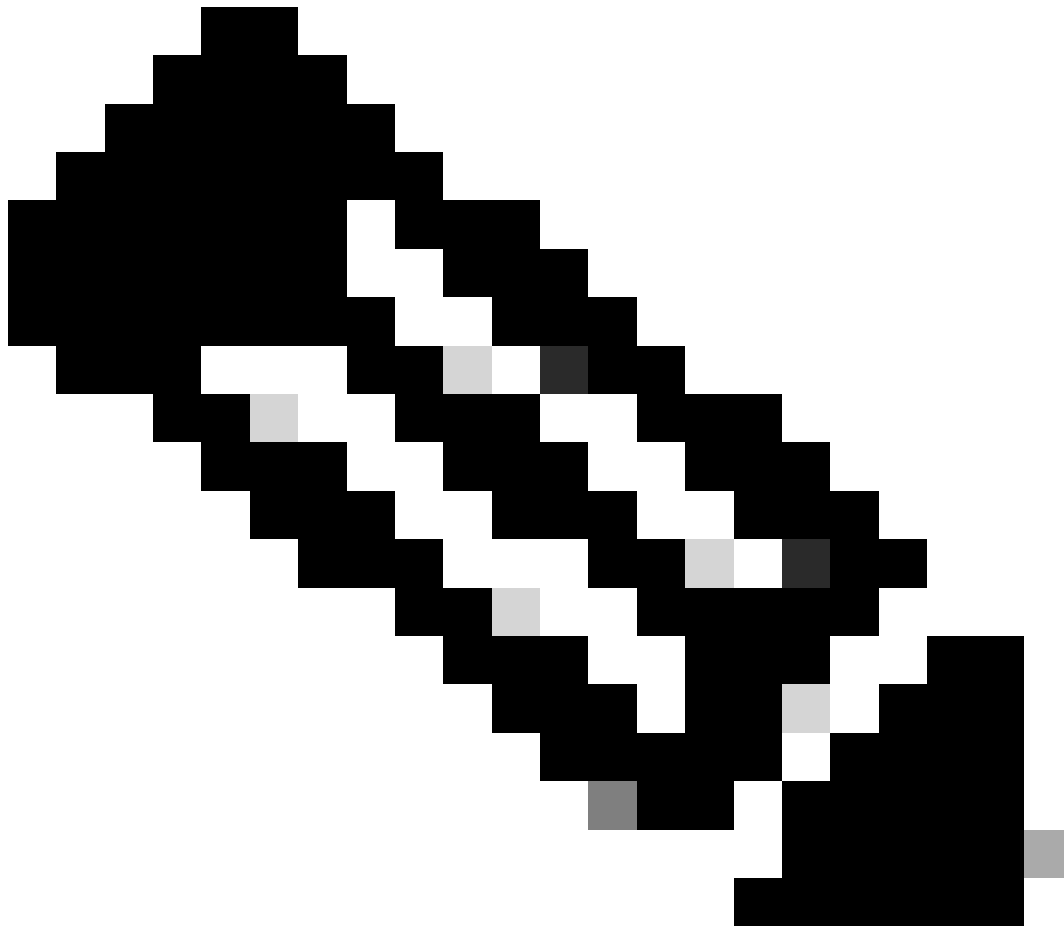
図3：問題のあるフロー



注：ここでは、同時に15個のスレッドすべてがwin-sparta.comによって占有され、demo.localのスレッドは残りません。

解決方法

- デフォルトの動作は、すべてのAD参加ポイントに共通のスレッドプールです
- ただし、管理者は各参加ポイントをセグメント化して独自のリソースを持つことができます。



注:AD優先順位付けが適用される場合、デフォルトはスレッドプールあたり10スレッドです。

図4「オンデマンド予約ジョイントポイントのフロー図」を参照してください。

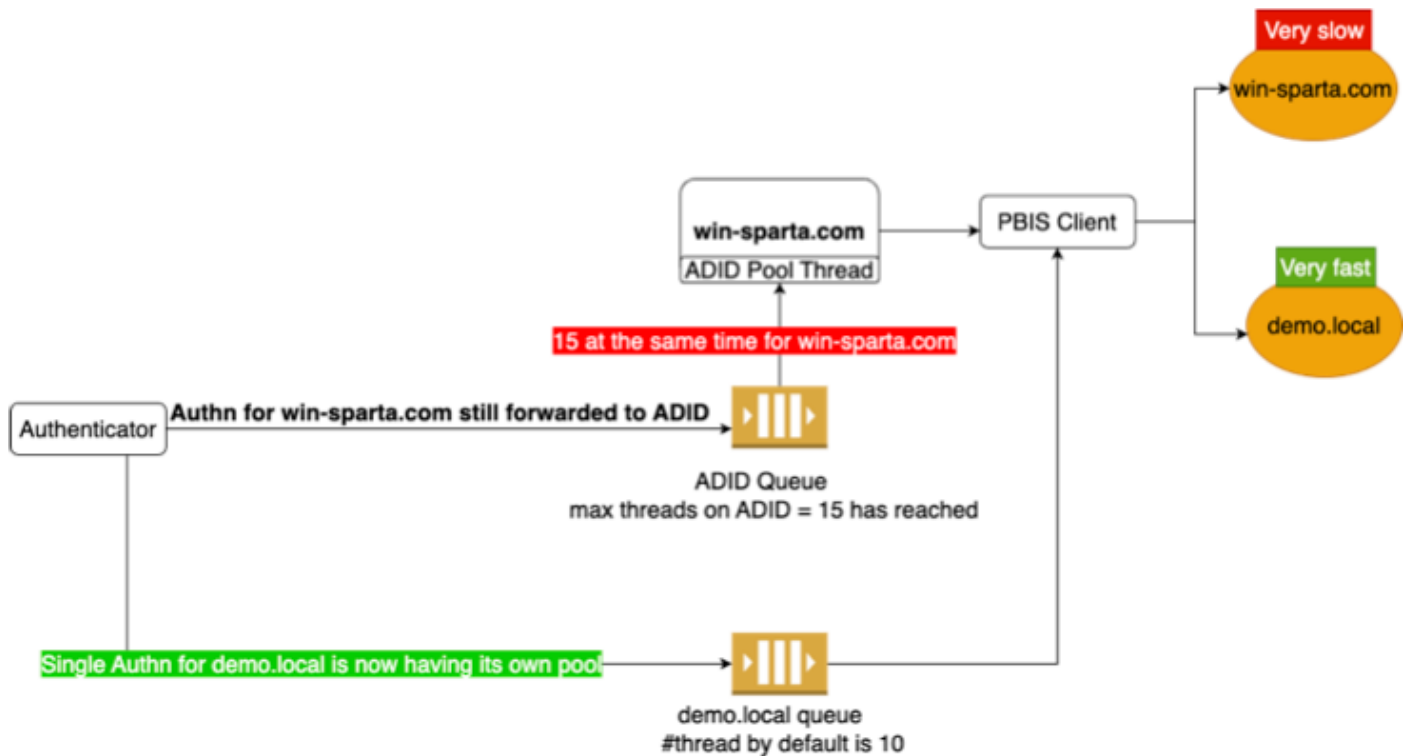


図4：ソリューションフロー

ステップバイステップ設定

手順1:2つの個別のAD結合ポイントを作成します。たとえば、demo.localとwin-sparta.comがあります。

手順2:AD参加ポイントの作成後に、参加ポイントの優先順位付けを作成します。

詳細については、図5:

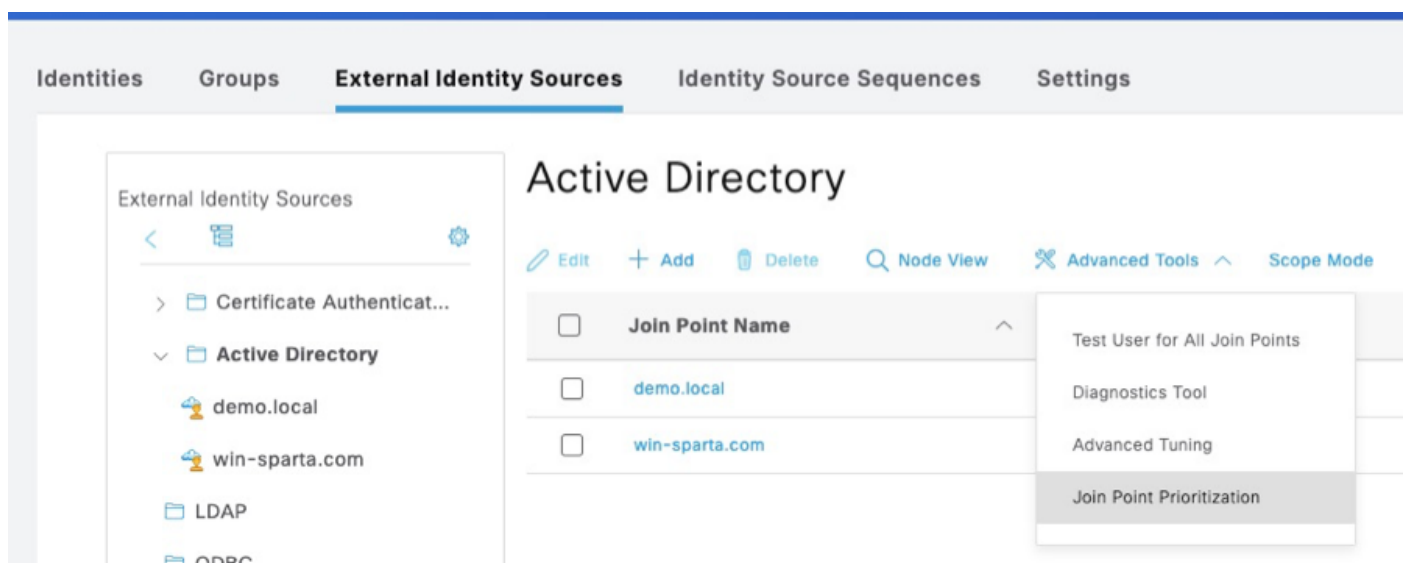


図5：参加ポイントの優先順位付け

ステップ3:Join Point Prioritizationで、専用ADリソースを予約するPSNを選択します。[Edit] をクリックします。

詳細については、図6:

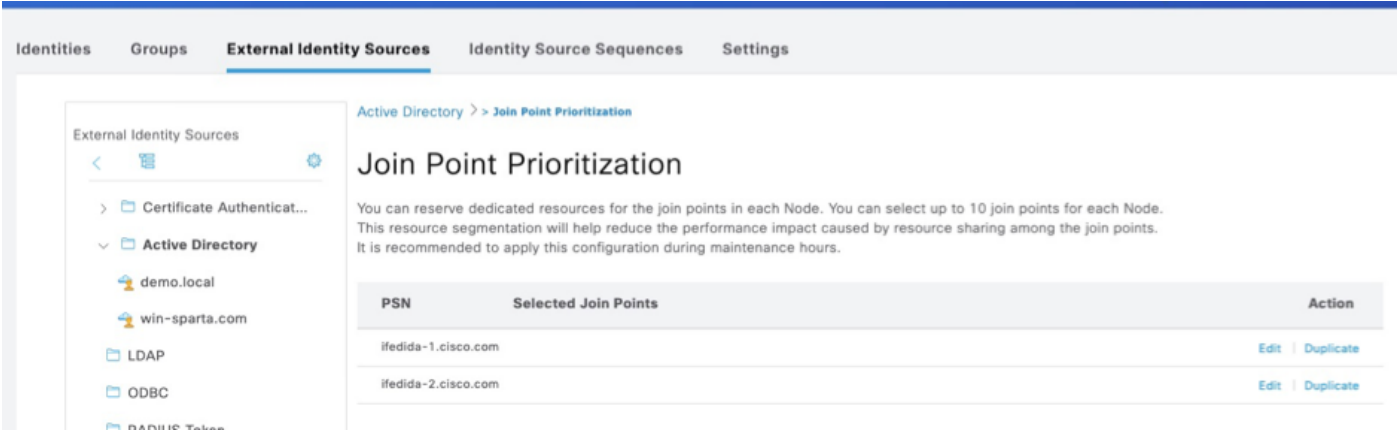


図6: PSNの編集

ステップ4：優先PSNの優先接続点を選択します。

詳細については、図7:

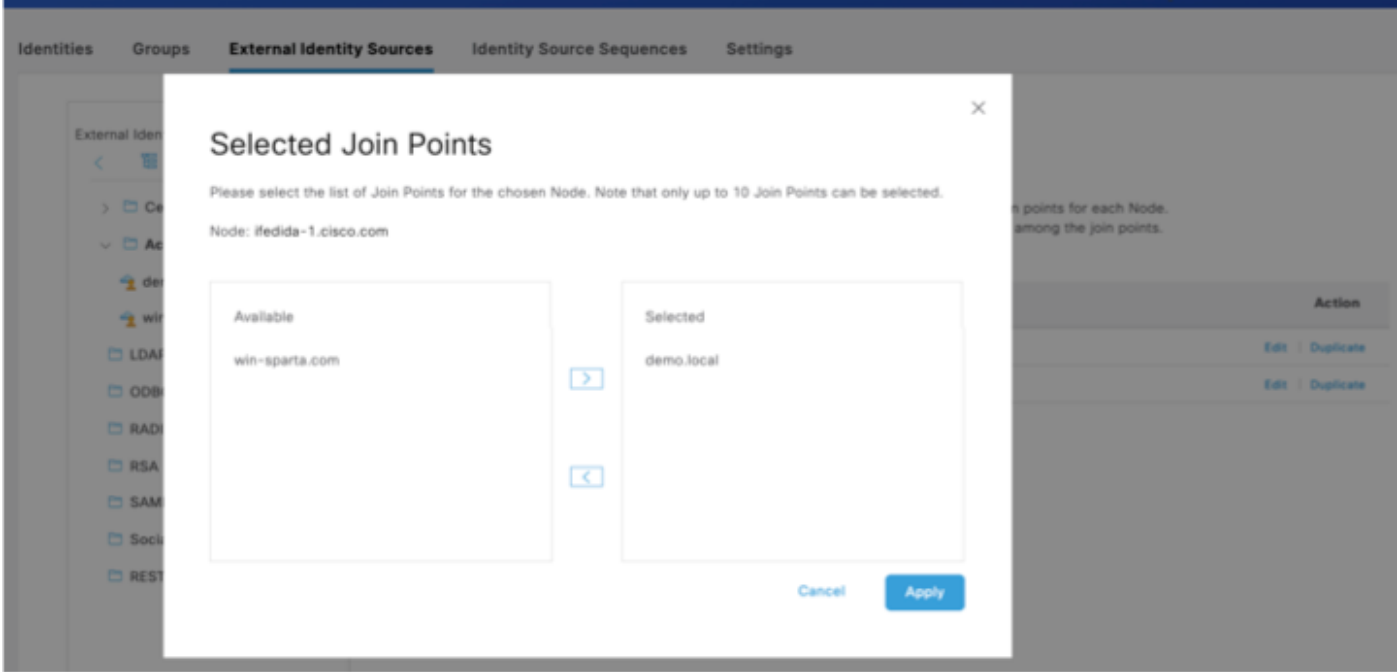
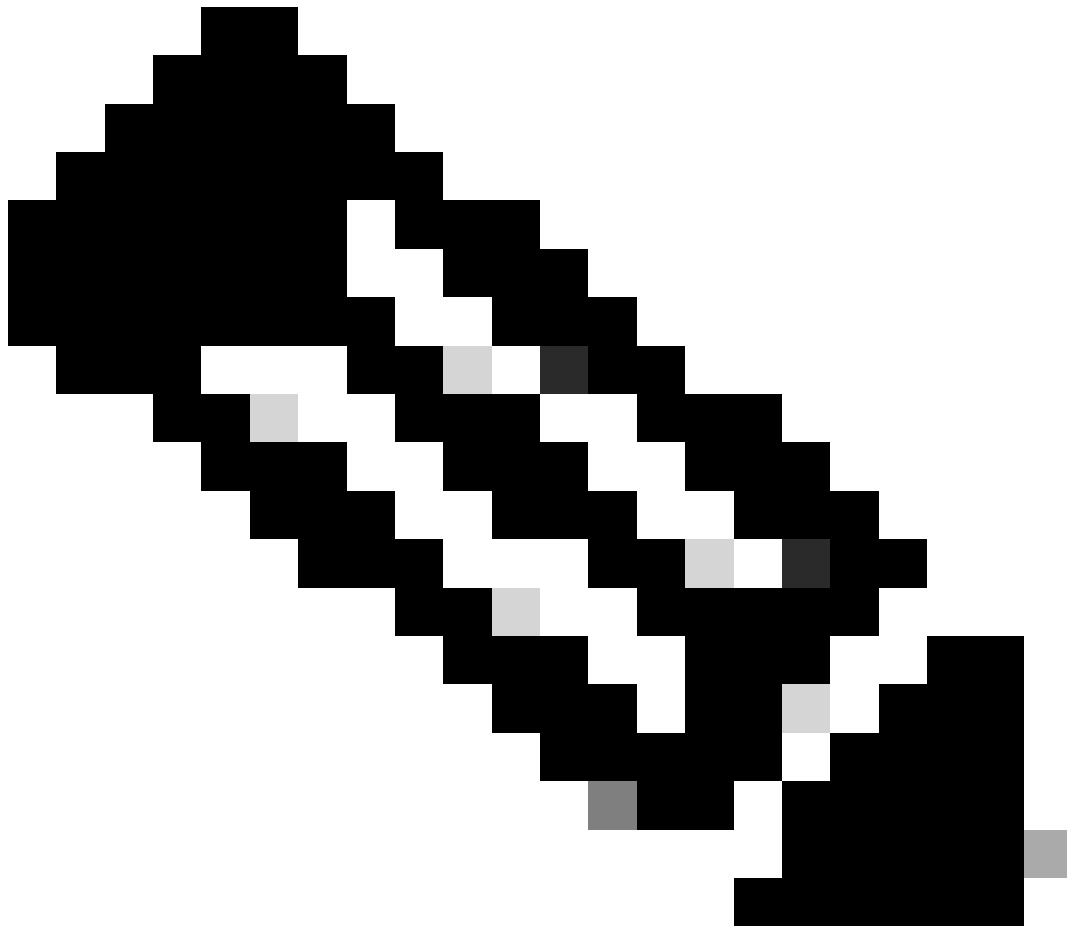


図7：選択した結合点



注：優先順位付けに含まれない結合ポイントは、最大15スレッドの共通スレッドプールを利用します。

ステップ5：優先順位付けの最終決定

詳細については、図8:

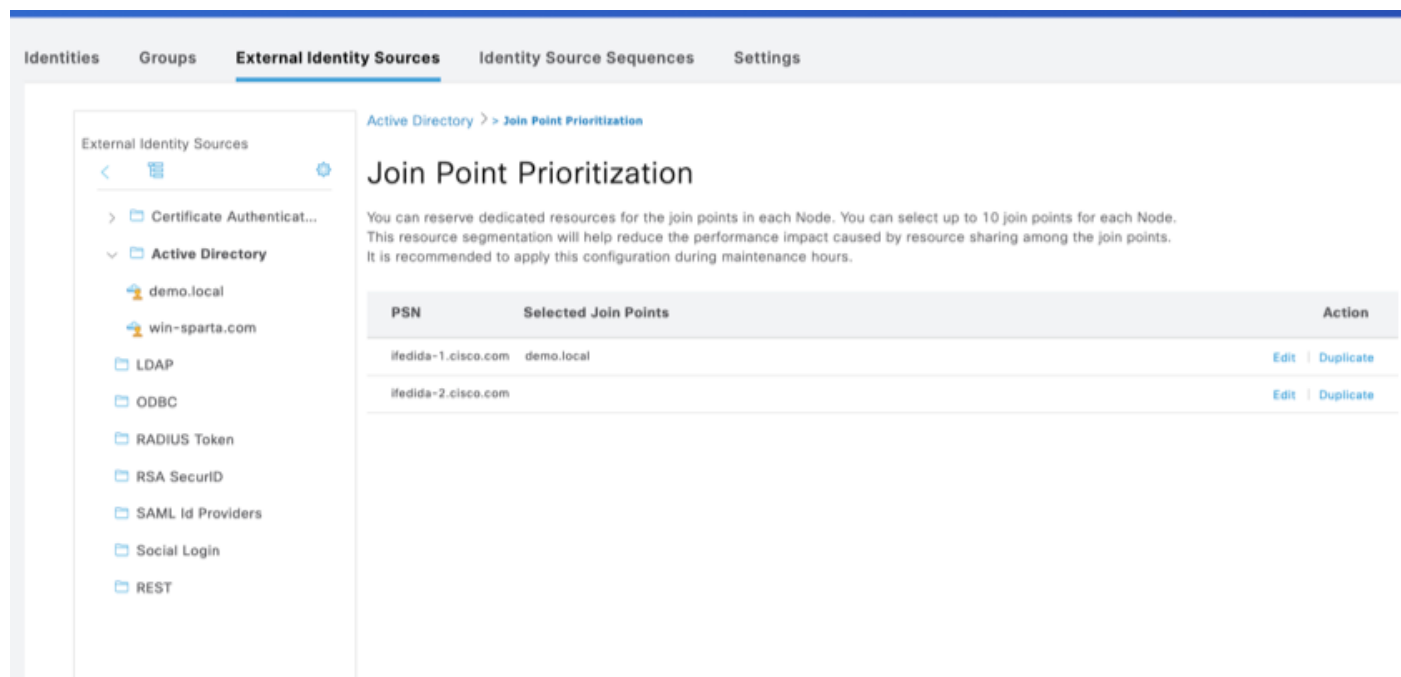
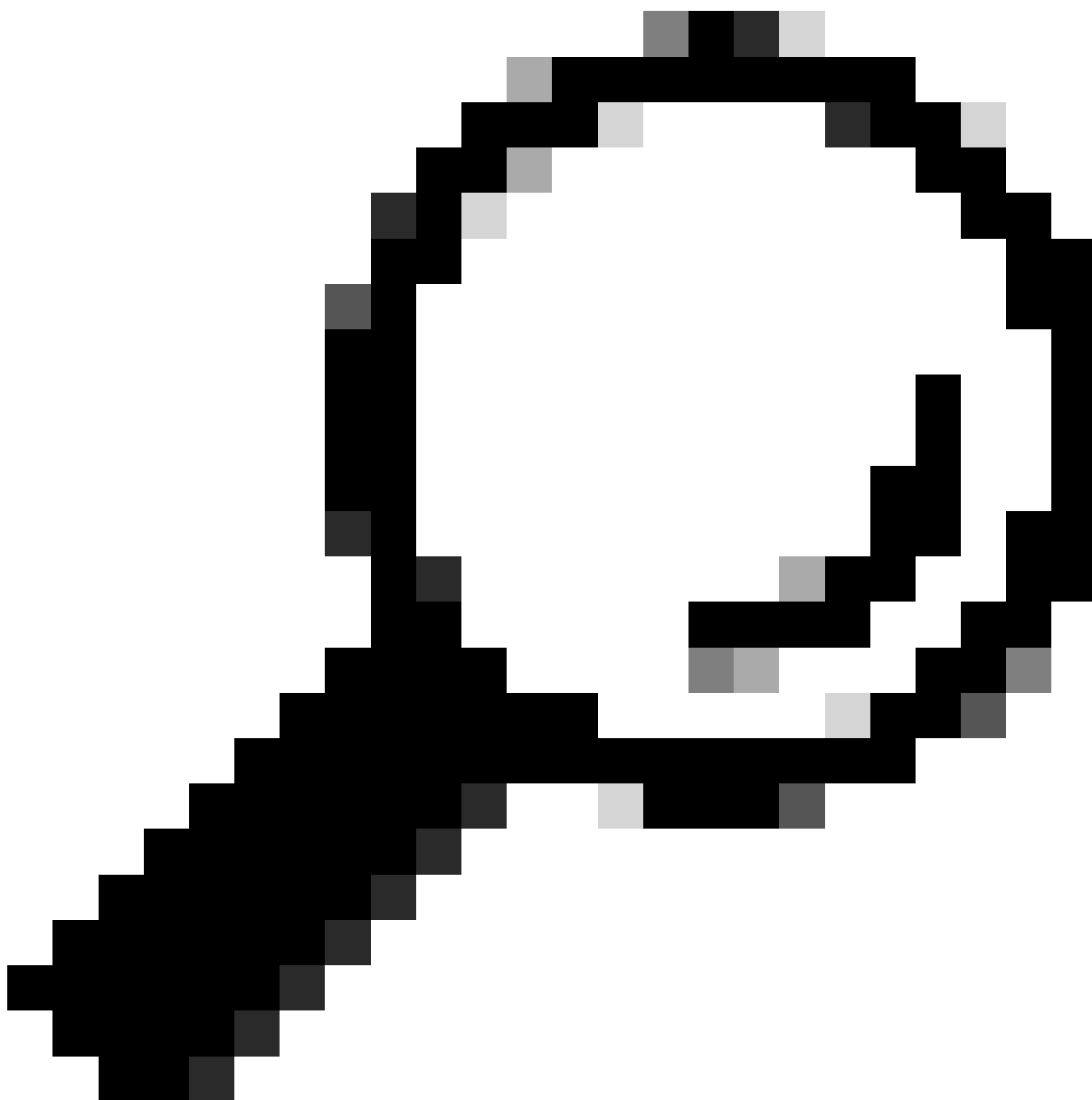


図8：優先順位付けの設定

その他の詳細事項



ヒント：同じ設定を他のPSNに複製する場合は、[複製]オプションを使用できます。目的のPSNを選択し、元の優先順位付けとともに複製する結合ポイントを選択します。

「図9：設定のヒント：

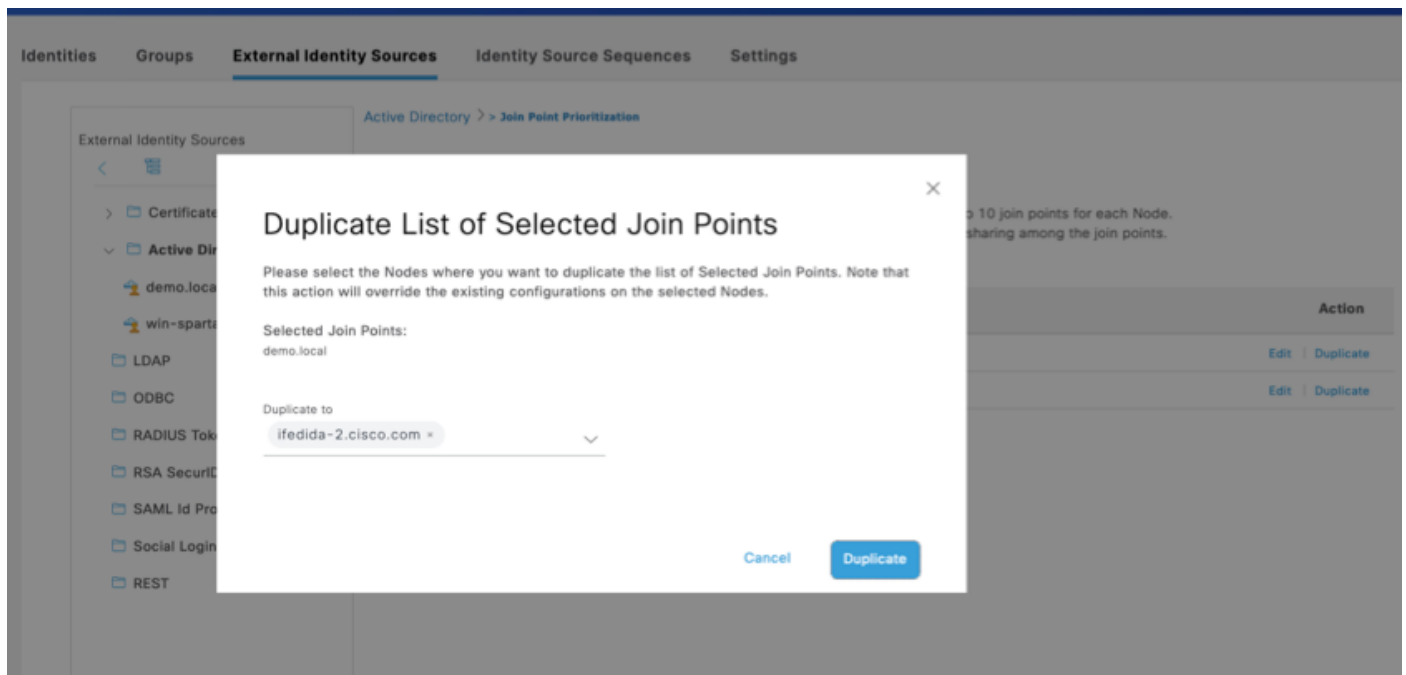


図9：優先順位付け構成の複製

ステップ6：複製後の最終リスト

詳細については、図10:

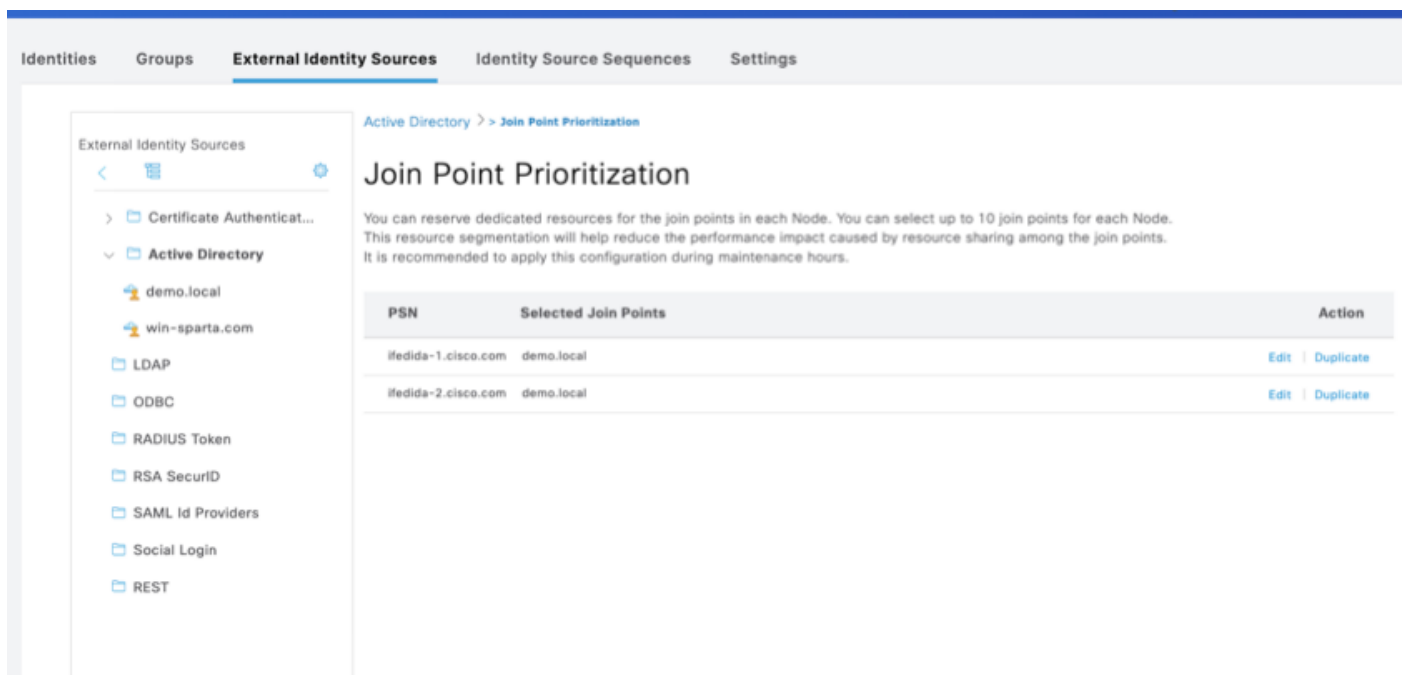


図10：プライオリティ設定後の最終リスト

トラブルシューティング

検証

設定変更を確認します。「工程」>「レポート」>「監査」>「構成監査の変更」にナビゲートします。

詳細については、図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

図11:Config Audit Report

Logging

- ランタイムAAAログのデバッグレベルを有効にします。
 - prrt-server.logの分析
- 詳細については、図12:

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

図12：デバッグログの設定

ログのスニペット

prrt-server.log [DEBUG]:デフォルトログ：

EventHandler,2024-08-23 07:16:48,135,DEBUG,0x7fecd2ccc700 , 割り当てられたデフォルトスレッドプール：AIDStore to IDP：win-sparta.com_wxETIH16Pk_106

prrt-server.log [INFO]:専用リソースを設定する場合

- ActiveDirectoryIDStore,2024-09-08 16:52:01,048,INFO,0x7f2452ccf700 , 割り当てスレッドプール：ADThreadPool0からIDP:win-sparta.com_wxETIH16Pk_106
- ActiveDirectoryIDStore,2024-09-08 16:57:11,258,INFO,0x7f2452ccf700 , 割り当て済みスレッドプール：ADThreadPool1からIDP:demo.local_6EcNs6UzwX_89

prrt-server.log [情報]:

- 専用リソースを設定する前に:
 - EventHandler, 2024-09-02 08:45:54,673,INFO,0x7fafb793c700,Passed event to the next thread pool name=ADIDStore, queue size=1,EventDispatcher.cpp:757
- 専用リソースを設定した後:

- EventHandler,2024-09-02 08:45:54,673,INFO,0x7f4867ff9700,Passed event to the next thread pool name=ADThreadPool0, queue size=1,EventDispatcher.cpp:841

「ADThreadPool0」のスレッドプール使用状況を追跡するには：

1. 0x7f57792f7700イベントが次のスレッドプール名=ADThreadPool0に渡されました
(StackID:0x7f57a4f761c0にいくつかのログが戻されます)
2. 0x7f57732c7700、スタック：0x7f57a4f761c0がActiveDirectoryIDStore: Method
MethodCaller<ActiveDirectoryIDStore, PlainAuthenticateAndQueryEvent>を呼び出しています
3. 0x7f57732c7700,cntx=0000210117,sesn=ifedida-
1/515863662/5273,CPMSessionID=C0A31430000000800018958,user=abcd,CallingStationID=[CAD]
956: CAD_PAPAuthenticate (abcd)が呼び出されました
4. 0x7f57732c7700,cntx=0000210117,sesn=ifedida-1/515863662
/5273,CPMSessionID=C0A31430000000800018958,user=abcd,CallingStationID=[CAD] 1026:
CAD_PAPAuthenticate (abcd)成功
5. 0x7f57732c7700、イベントを次のスレッドプールname=Mainに渡しました

FAQ

質問：ISEでサポートできるAD参加ポイントはいくつですか。

正解：1つのISE導入で最大50のActive Directory参加ポイントを設定できます。

質問：複数のAD参加ポイントがある場合でも、オンデマンドの優先順位付けを使用できますか。

正解：はい

質問：単一ドメインの優先順位付けのないデフォルトのスレッドサイズはいくつですか。

正解：15スレッド

質問：優先順位付けを設定する場合、どのように計算が行われますか。3つの参加ポイント
(domain1.com、domain2.com、およびdomain3.comとdomain1.com)が優先順位付けに設定され
ておらず、domain2.comとdomain3.comが優先順位付けに設定されているとします。

正解：domain1がプライオリティ設定に設定されていない場合、domain1.comは使用可能な共通
の15スレッドをすべて同時に使用します。ただし、domain2.comとdomain3.comには優先順位付
けが設定されているため、デフォルトではそれぞれ10のスレッドが使用され、共通の15スレッド
プールに従って使用されることはありません。

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。