

# يـلـع AD لـ بـلـطـالـا بـسـح دراومـلـا زجـح مـهـف ISE 3.3 4 حـيـحـصـت

## تـايـوتـحـمـلـا

---

[قـمـدقـمـلـا](#)

[قـيـسـاسـالـا تـابـلـطـمـلـا](#)

[قـبـولـطـمـلـا تـانـوكـمـلـا](#)

[قـيـسـاسـا تـامـولـعـم](#)

[ضـيـعـلـا](#)

[قـلـكـشـمـلـا](#)

[لـجـلـا](#)

[قـوطـخـب قـوطـخ نـيـوكـتـلـا](#)

[قـيـفـاضـالـيـصـافـت](#)

[اـمـحـالـصـاـوـعـاطـخـالـا فـاشـكـتـسـا](#)

[قـقـحـتـلـا](#)

[لـيـجـسـتـلـا](#)

[لـجـسـلـا تـاصـاصـق](#)

[قـعـئـاشـلـا قـلـئـسـالـا](#)

---

## قـمـدقـمـلـا

ISE 3.3 4 حـيـحـصـت يـلـع Active Directory لـ بـلـطـالـا بـسـح دراومـلـا زجـح لـوـح دـنـتـسـمـلـا اذـه فـصـي

## قـيـسـاسـالـا تـابـلـطـمـلـا

Cisco (ISE) نـم قـيـوـهـلـا تـامـدـخ كـرـحـم قـفـرـعـم

Active Directory (AD) يـف قـفـرـعـم

AD و (ISE) جـارـخـالـاـو لـاـخـدـالـا جـلـاعـم نـيـب لـمـا كـتـلـاب قـصـاخـالـا قـفـرـعـمـلـا

## قـبـولـطـمـلـا تـانـوكـمـلـا

قـيـلـالـلـا قـيـدـامـلـا تـانـوكـمـلـاـو جـمـارـبـلـا تـارـادـصـا يـلـا دـنـتـسـمـلـا اذـه يـف قـدـراولـا تـامـولـعـمـلـا دـنـتـسـت

- Cisco Identity Services Engine 3.3 Patch 4 جـمـانـرـبـلـا
- Microsoft Windows Active Directory 2016 و اـرـادـصـا و اـ

قـصـاخ قـيـلـمـعـم قـئـيـب يـف قـدـوجـومـلـا قـزـهـجـالـا نـم دـنـتـسـمـلـا اذـه يـف قـدـراولـا تـامـولـعـمـلـا عـاشـنـا مـت  
تـنـاك اذـا. (يـضـارـتـفـا) حـوسـمـم نـيـوكـتـب دـنـتـسـمـلـا اذـه يـف قـمـدـخـتـسـمـلـا قـزـهـجـالـا عـيـمـج تـأـدـب  
رـمـا يـال لـمـتـحـمـلـا رـيـثـاتـلـل كـمـهـف نـم دـكـأتـف ،لـيـغـشـتـلـا دـيـق كـتـكـبـش

## سياسات تامول عم

نوكت نأ نكمي. فاطملا ةيانهن يف لشفتو نايحألا ضعب يف ةئي طب AD ةقداصم نوكت ةفاك دافنتسا وأ مكارتل يف ءدبلا ADID راطتنا ةمئاق مايقي هه ةلمتحملا بابسألا ADID عمجت طبارت تارشؤم.

ADID لوح ليصافتلا نم ديزم:

لخاد انئاك ديرف لكشب فرعت ةلسلس نع ةرابع، (DN) زيمم مساب اضيأ فورعملا، ADID، Active Directory لاجم نمض اهترادإو تانئاكلا عقوم ديدحتل اهمادختسا متي. Active Directory ليلد نيمدختسملا تاباسح ةرادإل ةيمهألا غلاب ارمأ (ADID) ةيمقرلا ةزهجألا تافرعم دعت. Active Directory ةئيبي لخاد رخألا دراوملاو تانوذألاو.

لشلا اذهب ةيجذومنلا ADID ودبت نأ بجي: CN=John Doe, OU=Sales, DC=example, DC=com: ثيح،

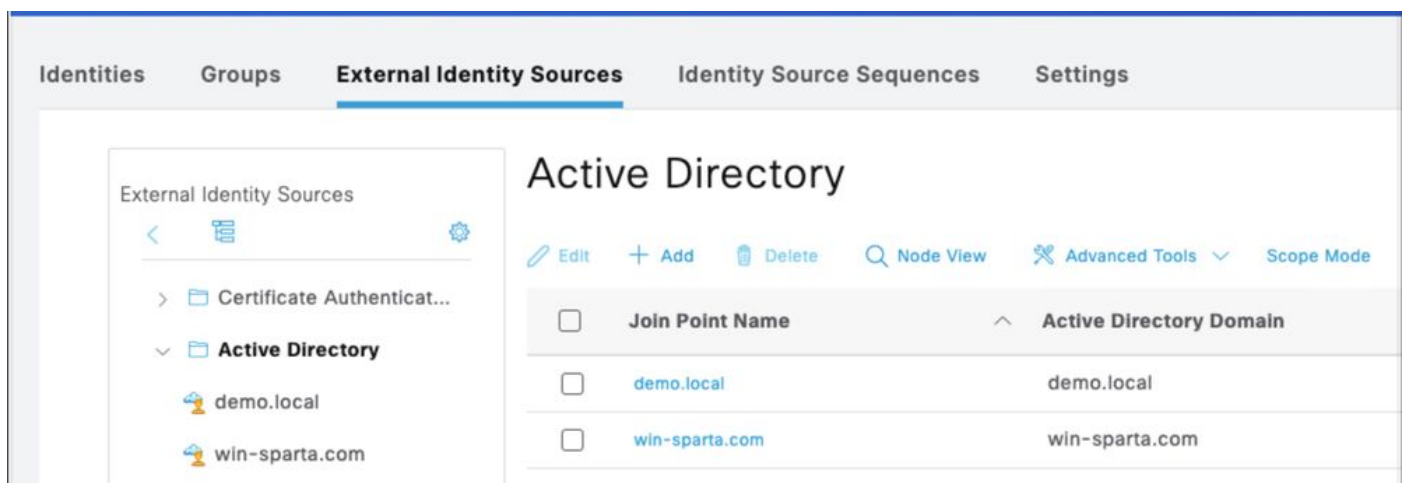
ود نوح، مدختسملا لئاشلا مسالا لثمي: ود نوح=ن.س.

مسق، ةلاحلا هذه يف، مدختسملا يمتني ثيح (OU) ةيميظنتلا ةدحولا لثمي: تاعيبملا OU=ن.س.

example.com. وه، لاجملا تانوكم لثمي: DC=example, DC=com.

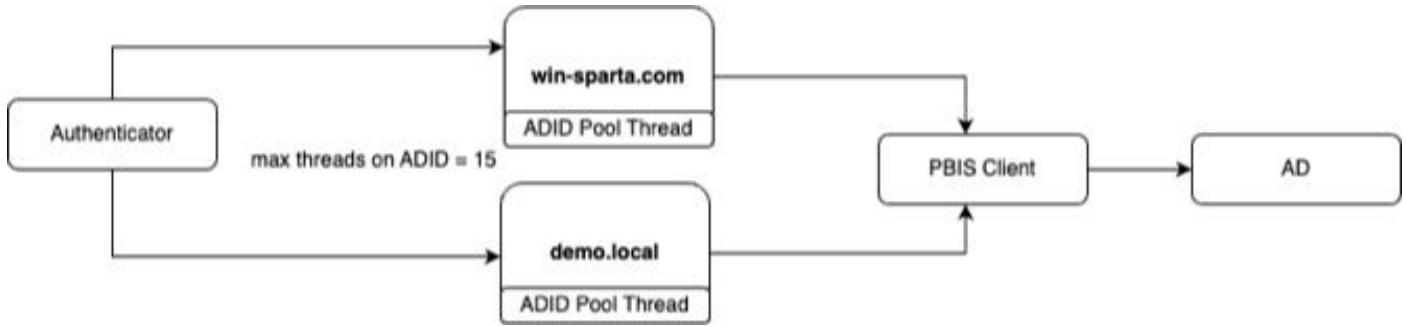
لثملا ليبس ىلع:

AD طبر ةطقنل ييجذومن نيوكت 1: ةروصلا ىلإ عجرا



تانالءالا طبر طاقن 1: ةروصلا

طبر يطقن عم ييجذومن AD قفدت ططخم 2: ةروصلا ىلإ عجرا



يُجذوم AD قفدت ططخم :ةيناثلا ةروصل

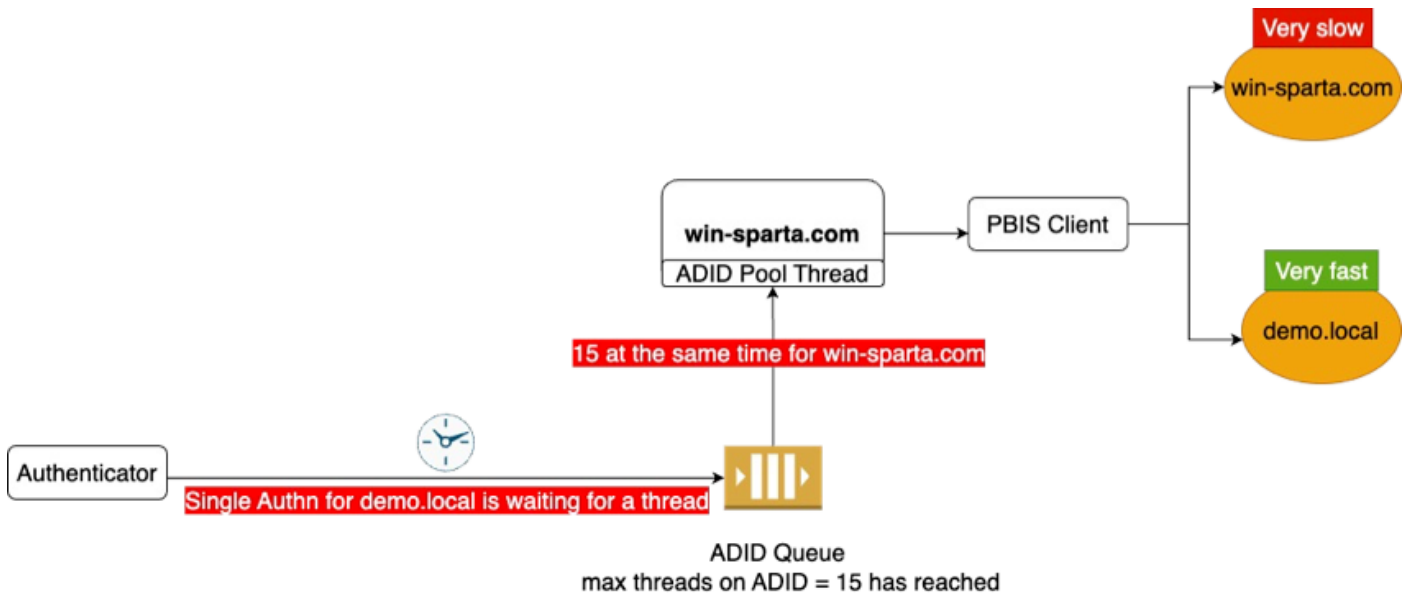
## ضرعلا

هسفن ADID طبارت رشؤم عمجت تحت ةئي طب طبر ةطقن

## ةلكشملا

- 15 لاسرا مت اذا ، لاثملا لئبس ىلع ؟ اء ةئي طب مامضنالا طاقن ىءح نوك بقاوع يه ام ريغ لكشب ائي طب "demo.local" ناك و "demo.local" ل تقولا سفن ي ISE ىل ةقداصم win-sparta ةقداصم ءءلام لبق "demo.local" نم ةباجتسال راطتنا انيلع نيعتيسف ، يداع ةءءالا win-sparta.
2. طبر ةطقن تحت ADID طبارت رشؤم عمجت سفن ناك راشت طبرلا يتطقن الك نأ ول اذا م ةءءاو ؟

ةئي طب لصفملا ةطقن قفدت ططخم :3 ةروصل ىل ءءرا



ىل الكشا نايرء :3 ةروصل

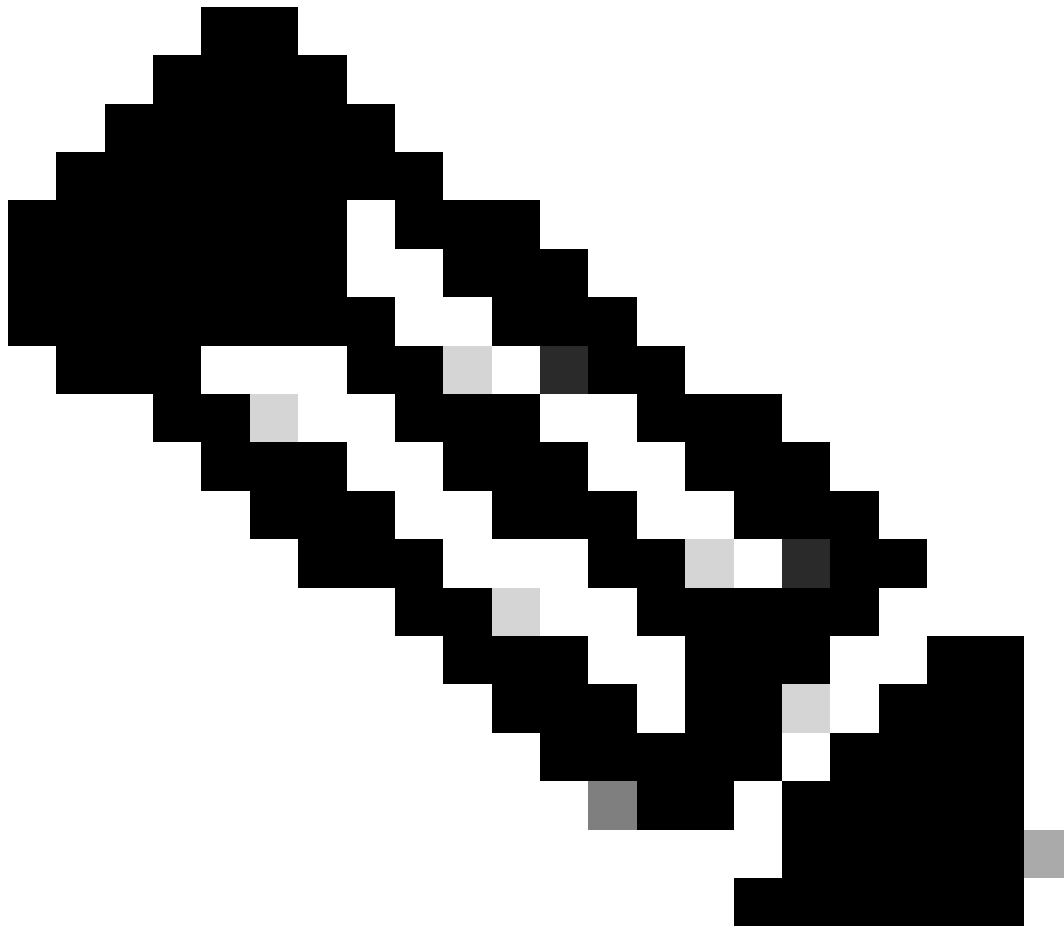


في win-sparta.com طاساوب 15 لا طبارتلا تارشؤم عي مج لغش متي ،انه :ةظالم  
local.يحيضوتلا ضرعلل طبارت رشؤم يا كرت نود تقولا سفن

---

## لحل

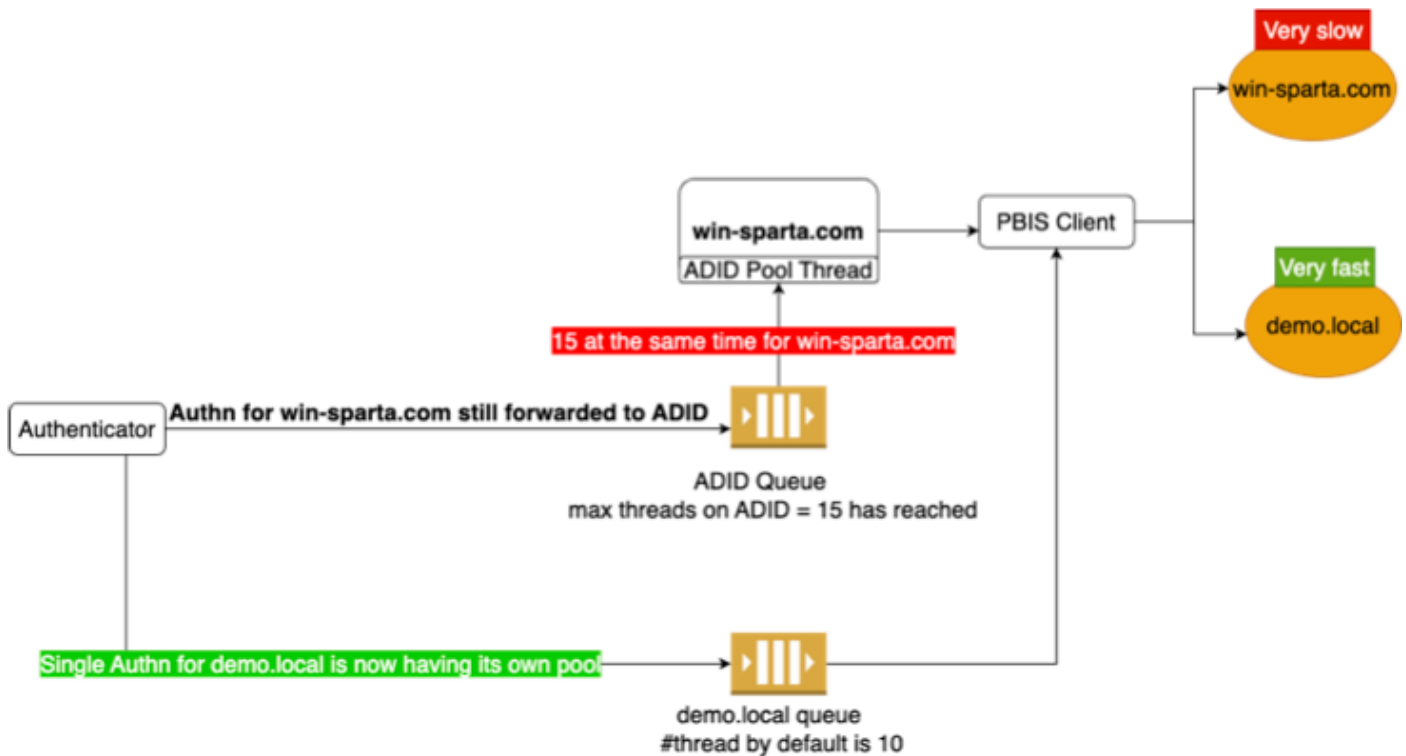
- AD طبر طاقن لكل كرتشم طبارت رشؤم عمجت وه يضارتفالا كولسلا
- .اهب ةصاخلا دراوملا ىلع لوصحلل طبرة طقن لك ميسقت نيلوؤسملل نكمي ،كلذ عمو



لكل طبارة تارشوم 10 يضارتهال نوكي AD، تايولوا بيترت قي بطت دن ع:ة طحال م  
طبارتهال تارشوم عمجت.

---

بلطال بسح ةزوجم لاة كترشم لاة طقنللا قفدت ططخم: 4 ةروصلال ال عجرا



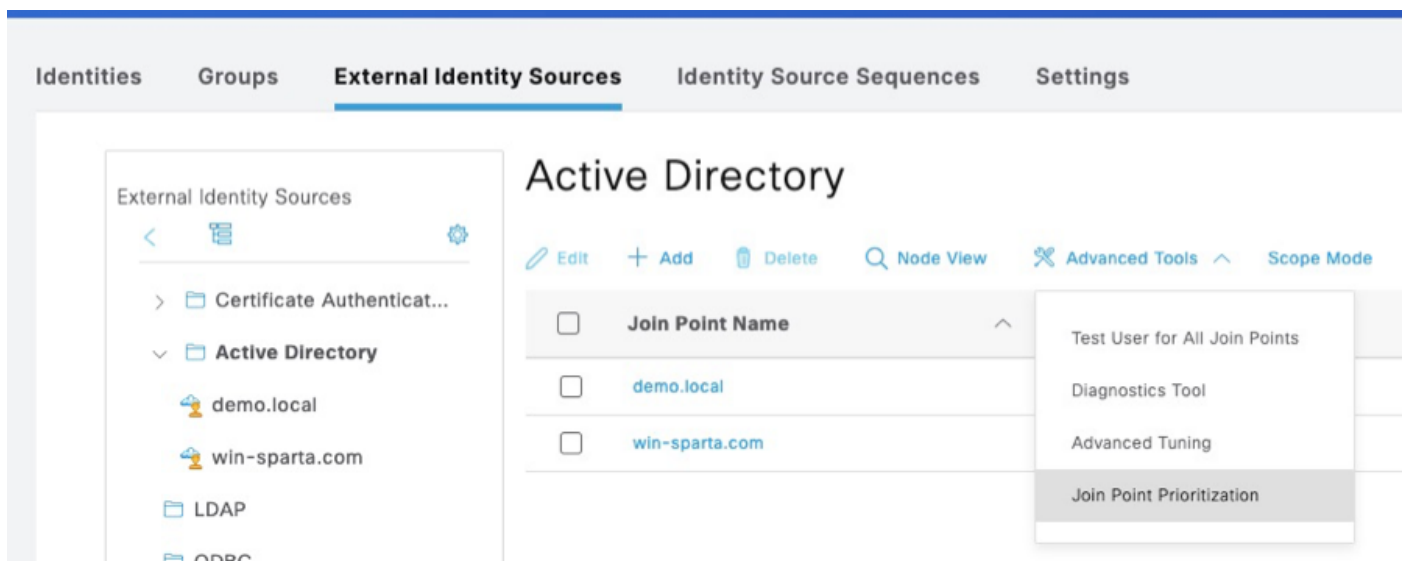
الحل قفدت 4: ةروصل

## ةوطخب ةوطخ نيوكتل

win-sparta.com و demo.local ةببرجت ةخسن :اني دل ال ثم انه .ني تل لصفنم AD طبر ي تطقن ءاشن : 1 ةوطخل

AD طبر ةطقن ءاشن دع ب طبرل ةطقن تايولوا ببرت ءاشن : 2 ةوطخل

5: ةروصل الى عجرا



طبرل ةطقن تايولوا ببرت 5: ةروصل

ةصصخم ال AD دراوم زج لصفن يذل ال PSN دح ،طبرل ةطقن تايولوا ببرت تحت : 3 ةوطخل ريرجت قوف رقنا .هل

## 6: ةروصل الى عرجا

The screenshot shows the 'Join Point Prioritization' configuration page. The left sidebar lists 'External Identity Sources' with 'Active Directory' expanded, showing 'demo.local' and 'win-sparta.com'. The main content area has a breadcrumb 'Active Directory > > Join Point Prioritization' and a title 'Join Point Prioritization'. Below the title is a descriptive text: '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.' Below this is a table with columns 'PSN', 'Selected Join Points', and 'Action'.

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

PSN ري رحت 6: ةروصل الى

ل. لضمفم الى PSN ل ةلضمفم الى طبرل ةطقن ددح 4: ةوطخل

## 7: ةروصل الى عرجا

The screenshot shows a 'Selected Join Points' dialog box. It has a title bar with a close button. The main text says: 'Please select the list of Join Points for the chosen Node. Note that only up to 10 Join Points can be selected. Node: ifedida-1.cisco.com'. Below this are two boxes: 'Available' containing 'win-sparta.com' and 'Selected' containing 'demo.local'. Between the boxes are two arrows: a right-pointing arrow and a left-pointing arrow. At the bottom are 'Cancel' and 'Apply' buttons.

ةددحم الى طبرل ةطقن 7: ةروصل الى



تارشمۇم عمجت تايولوالا بېتتت ي ف ةنمضم ريغ طبر طاقن يا مدختست :ةظحال م  
طبارت رشؤم 15 غلبې ىصقا دح هل يذلاو ،ةكرتشملا طبارتلا

تايولوالا ديدحت نم ءاهتئالا مت :5 ةوطخال

8: ةروصلا ىلا عجرا

IdentitiesGroups**External Identity Sources**Identity Source SequencesSettings

External Identity Sources

<

>

Certificate Authenticat...

▼

Active Directory

demo.local

win-sparta.com

LDAP

ODBC

RADIUS Token

RSA SecurID

SAML Id Providers

Social Login

REST

Active Directory > > Join Point Prioritization

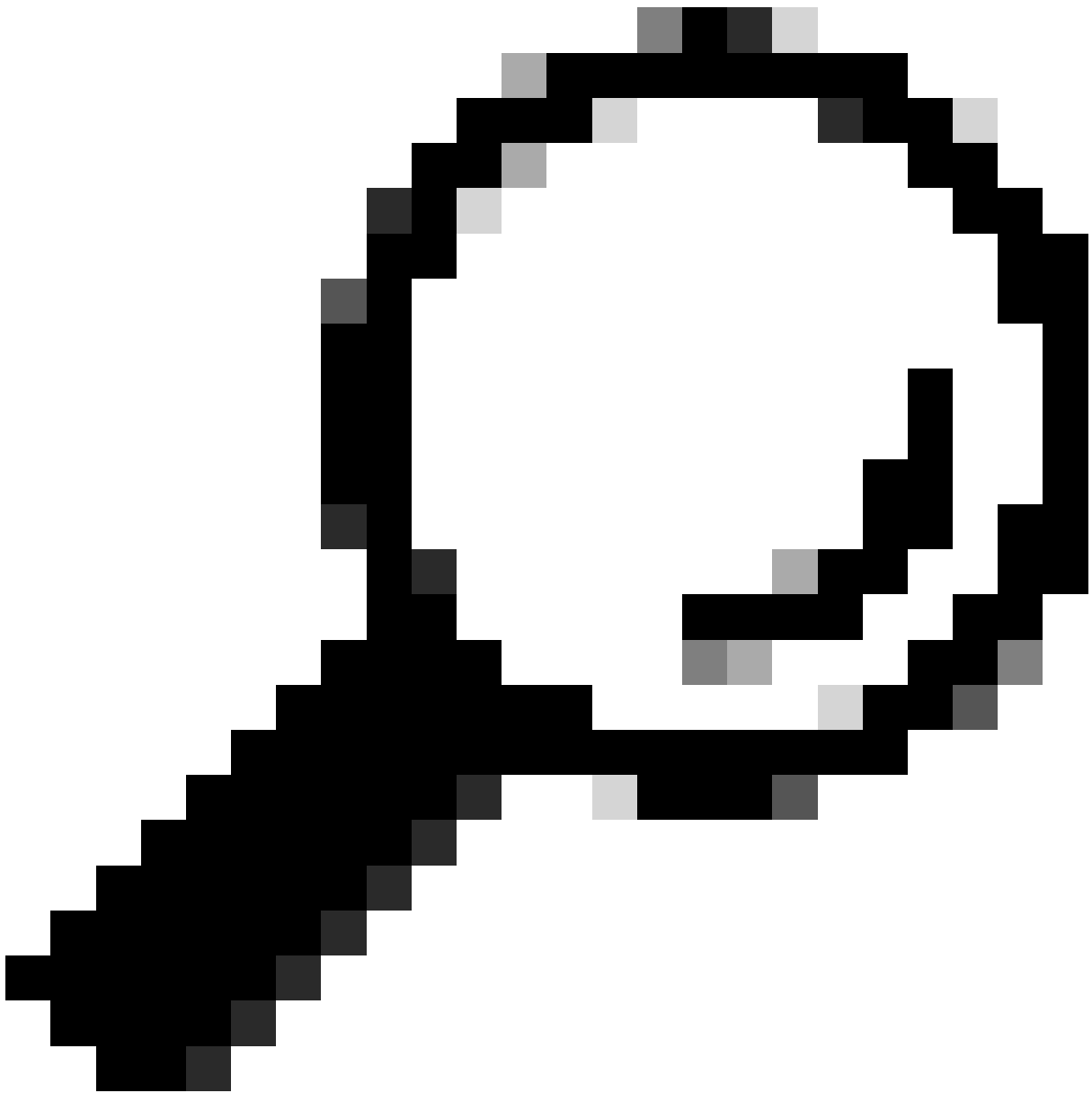
## Join Point Prioritization

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> |

تايولوالا بيترت نيوكت :8 ةروصلال

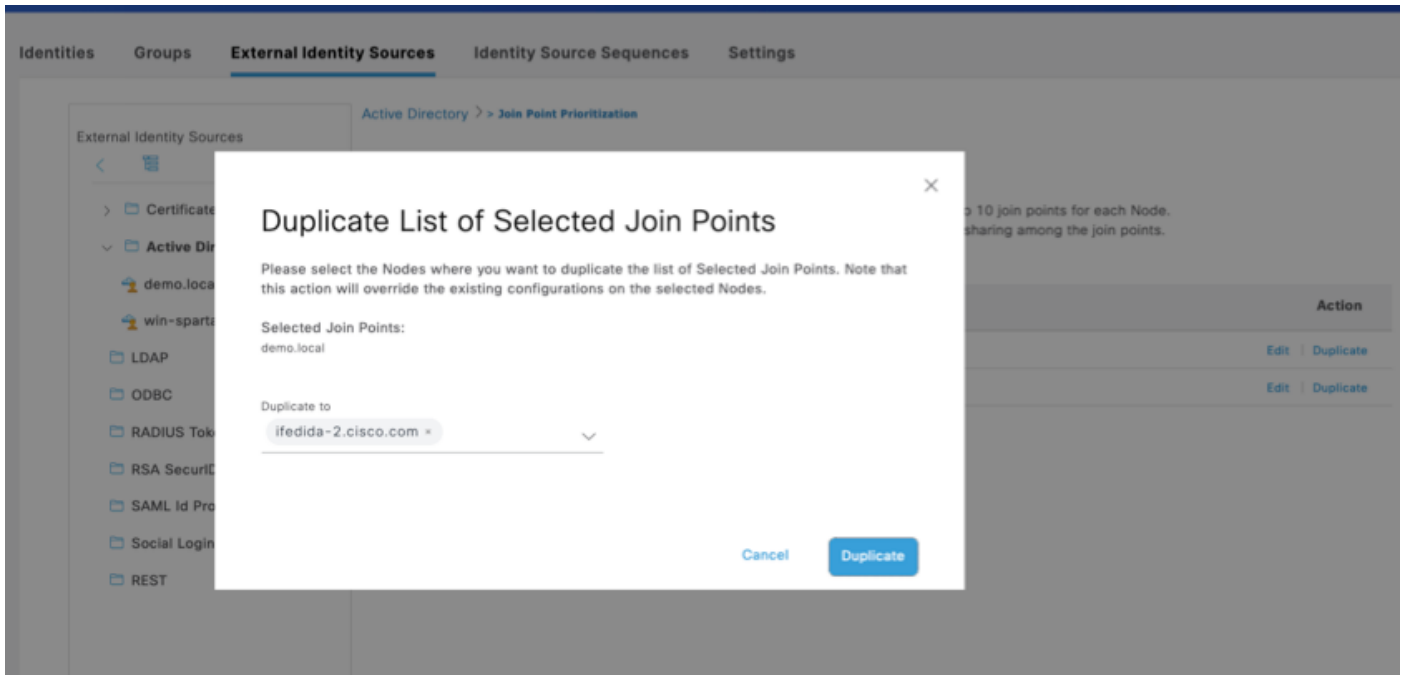
ةيفاضا ليصافت



عيطتسې تنأ، رخآ PSNs ىلإ دادعإ ةيلمع هسفن لا رركي نأ تنأ ديرې نإ: حيملت  
مئيس يتلا طبرلا ةطقن رتخاو، بولطم لا PSN دح. راخ ةفعاضم لا تلمعتسا  
يلصلأا تايولوألا بيترت عم اهراركت

---

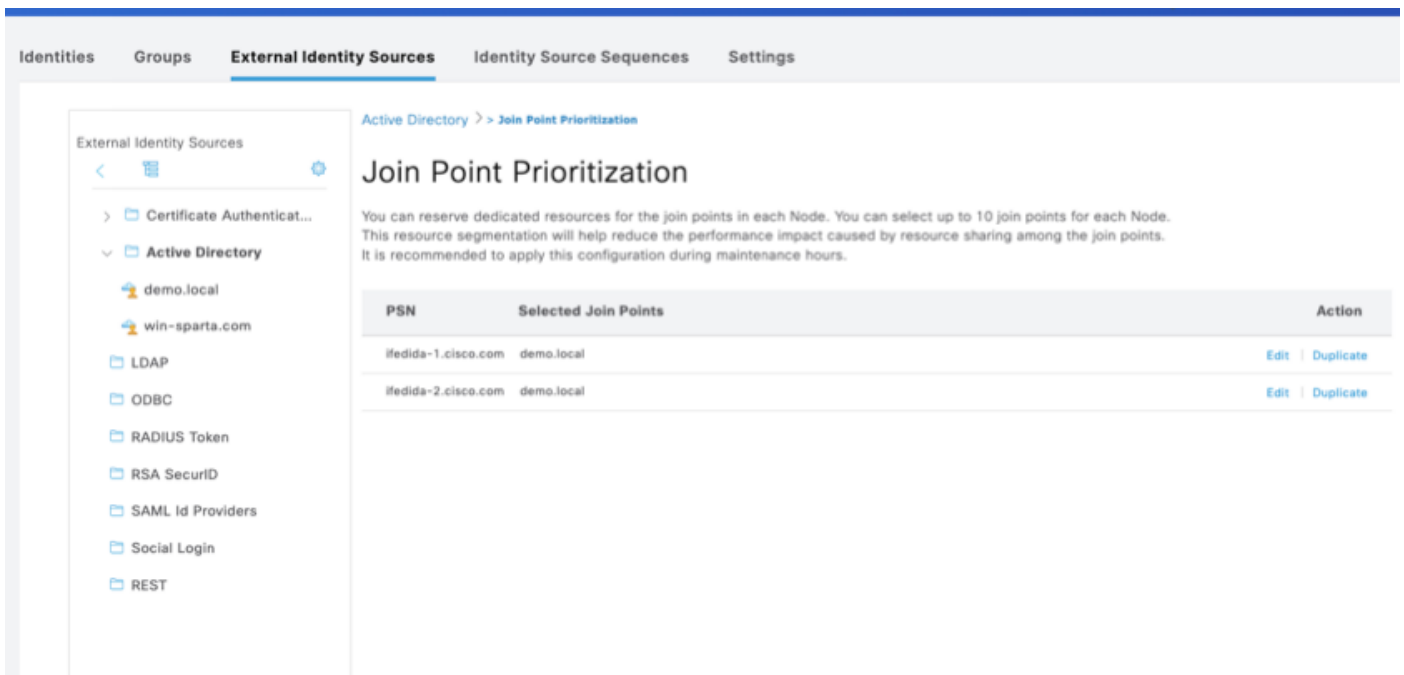
ن: ويكتلا حيملت: 9 ةروصلا ىلإ عجرا



تايولولأل بيترت نيوكت راركت 9: ةروصل

راركتل دعب ةيئاهنل ةمئاقلا 6: ةوطخل

10: ةروصلال ىلإ عجرا



تايولولأل بيترت دعب ةيئاهنل ةمئاقلا: ةرشلال ةروصل

اهحالصلإو ءاطخلأل فاشكتسا

ققحتل

رييغت > تاقىققتل > ريراققتل > تايلمعلا: ىلإ لقتنا. نيوكتل تارييغت نم ققحت نيوكتل قىققت

11: ةروصلال ىلإ عجرا

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 |

قيقتال ريرقت نيوكت: 11 ةروصلال

لجستال

- AAA لىغشتال تقو تالچسل ءاطخأل حىحصت ىوتسم نيكم تب مق
  - prrt-server.log لىلحت
- 12: ةروصلال ىلإ عجرا

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

حىحصتال لچس نيوكت: 12 ةروصلال

لچسل تاصاصق

prrt-server.log [debug]: لىضارتال لچسلال:

طبارتال تارشؤم عمجت ،0x7fecd2ccc700،DEBUG،135،2024-08-23 07:16:48،EventHandler،  
win- : ايلخاد نيحزانال ىلإ ADIDS لوصو : ةصصخمل لىضارتال  
sparta.com\_wxETIH16Pk\_106

prrt-server.log [INFO]: ةصصخمل دراومال نييعت دنع:

- ActiveDirectoryIDStore،2024-09-08 16:52:01.048،INFO، 0x7f2452ccf700، تارشؤم عمجت  
ADThreadPool0 ىلإ IDP : win-sparta.com\_wxETIH16Pk\_106 : صصخمل طبارتال
- ActiveDirectoryIDStore،2024-09-08 16:57:11.258،INFO، 0x7f2452ccf700، تارشؤم عمجت  
ADThreadPool1 ىلإ IDP : demo.local\_6EcNs6UzwX\_89 : صصخمل طبارتال

prrt-server.log [INFO]:

- ةصصخمل دراومال ددحن نأ لبق:
  - EventHandler، 2024-09-02 08:45:54،673،INFO،0x7fafb793c700،م ت ريرمت،  
ADIDStore=لالتال طبارتال رشؤم عمجت مسا ةمئاق مچ

1.EventDispatcher.cpp:757=راطتال

• دراومال صي صختب انمق نأ دعب :

- EventHandler،2024-09-02 08:45:54.673،INFO، 0x7f4867ff9700، ري رمت مت  
ةمئاق مچج ،ADThreadPool=يالاتل طبارتل تارشؤم عمجت مسال  
1.EventDispatcher.cpp:841=راطتال

"ADThreadPool": ل طبارتل تارشؤم عمجت مادختسا بقعتل

ADThreadPool=يالاتل طبارتل تارشؤم عمجت مسال يلاتل تارح ري رمتب ماق ،0x7f57792f7700،  
(دعجرت يلاتل تارحسلا نم ليلق ددع) StackID:0x7f57a4f761c0

2. 0x7f57732c7700،Stack: 0x7f57a4f761c0 ءادتسا ActiveDirectoryIDStore:  
MethodCaller<ActiveDirectoryIDStore و PlainAuthenticateAndQueryEvent>

3. 0x7f57732c7700،cntx=0000210117،sesn=ifedida-  
1/51586362/5273.CPMSSessionID=c0A3143000000800018958،user=ABCD،CallStationID[CID=[CN0  
ب.م] 956: ءادتسا مت CAD\_PAPAuthenticate (ABCD)

4. 0x7f57732c7700،cntx=000210117،sesn=ifedida-  
1/51586362/5273.CPMSSessionID=c0A314300000080018958،user=،الاصتال StationID=[CAD]  
1026: حجن CAD\_PAPAuthenticate (ABCD)

5. 0x7f57732c7700، ري رمت مت Main=يالاتل طبارتل تارشؤم عمجت مسال يلاتل تارح ري رمت مت

## ةعئاشال ةلئسال

ISE؟ اهمعدي نأ نكمي يلاتل AD Join طاقن ددع مك :لاؤس

.دحاو ISE رشن يلع Active Directory طبر ةطقن 50 يلاتل لصي ام نيوكت كنكمي :ةباجال

بسح تايولوالا بيترت مادختسا يننكمي له ،ةددعتم AD طبر طاقن يدل ناك اذا :لاؤس  
بطلال

معن :ةباجال

؟دحاو لاجمل تايولوالا بيترت نودب يضارتفال طبارتل تارشؤم مچج وه ام :لاؤس

طبارت تارشؤم 15 :ةباجال

نأ ،رابتعالا يفعض ؟باسحال ءارج متي فيك ،تايولوالا بيترت نيوكتب تمق اذا :لاؤس  
ريغ domain1.com عم domain2.com و domain3.com و domain1.com - طبرال طاقن 3 ويراني  
تايولوالا ددحتل هنيوكت متي domain2.com و domain3.com و تايولوالا ددحتل نوكم

تارشؤم مدختسي domain1.com ناف ،ةيولوالا ددحتل 1 لاجمل نيوكت متي مل اذا :ةباجال  
نيوكت متي هنأل ارطن ،كلذ عمو .تقولاسفن يفي كلذل لك - ةرفوتمال ةعئاشال 15 طبارتل  
طبارت تارشؤم 10 نامدختسي امهناف ،ةيولوالا ددحت مادختساب domain2.com و domain3.com  
ةعئاشال طبارت تارشؤم 15 عمجت نم ناديفتسي/ناعبتي الويضارتفا لكشب امهنم لك

ةمچرتل هذه ل و ح

ةيلآل ا تاي ن ق ت ل ا ن م ة و م ج م ا د خ ت س ا ب د ن ت س م ل ا ا ذ ه Cisco ت م چ ر ت م ل ا ع ل ا ا ح ن ا ع م ج ي ف ن ي م د خ ت س م ل ل م ع د ي و ت ح م م ي د ق ت ل ة ي ر ش ب ل ا و ا م ك ة ق ي ق د ن و ك ت ن ل ة ي ل آ ة م چ ر ت ل ض ف ا ن ا ة ط ح ا ل م ي ج ر ي . ة ص ا خ ل ا م ه ت غ ل ب Cisco ي ل خ ت . ف ر ت ح م م چ ر ت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة م چ ر ت ل ا ع م ل ا ح ل ا و ه ي ل ا ا م ا د ع و ج ر ل ا ب ي ص و ت و ت ا م چ ر ت ل ا ه ذ ه ة ق د ن ع ا ه ت ي ل و ئ س م Systems ( ر ف و ت م ط ب ا ر ل ا ) ي ل ص ا ل ا ي ز ي ل ج ن ا ل ا د ن ت س م ل ا