

ةي وهلا تامدخ كرحمل لماخ فرعم ليك ونيوكت EVT ىلا ةدنتسملا

تايوتحمل

[ةمدقملا](#)

[ةيساسألا تابلطتملا](#)

[تابلطتملا](#)

[ةمدختسملا تانوكملا](#)

[ةيساسأ تامولعم](#)

[ديدج لوكوتورب ىلا ةجالحلا](#)

[MS-EVEN6 مادختسا اياز](#)

[ةيلاعلا ةجاتالا](#)

[ريوطتلا ةيلباق](#)

[رابتخال دادعلا ةينب ريوطت](#)

[ةيخيبراتلا تادخال مالعتسا](#)

[لقأ ةجلاعم فيلاكت](#)

[نيوكتلا](#)

[لائصتاللي طيختملا مسرلا](#)

[تانيوكتلا](#)

[PassiveID ليكول ISE نيوكت](#)

[PassiveID ليكول نيوكت فلم مهف](#)

[ةحصلا نم ققحتلا](#)

[ISE ىلع PassiveID تامدخ نم ققحتلا](#)

[Windows مداخل ليكول تامدخ نم ققحتلا](#)

ةمدقملا

ةديدجال ةي وهلا تامدخ كرحمل (ISE-PIC) Passive Identity Connector ليكول دنتسملا اذه فصبي
ISE 3.0 رادصا يف هميدقت مت يذلا

ةيساسألا تابلطتملا

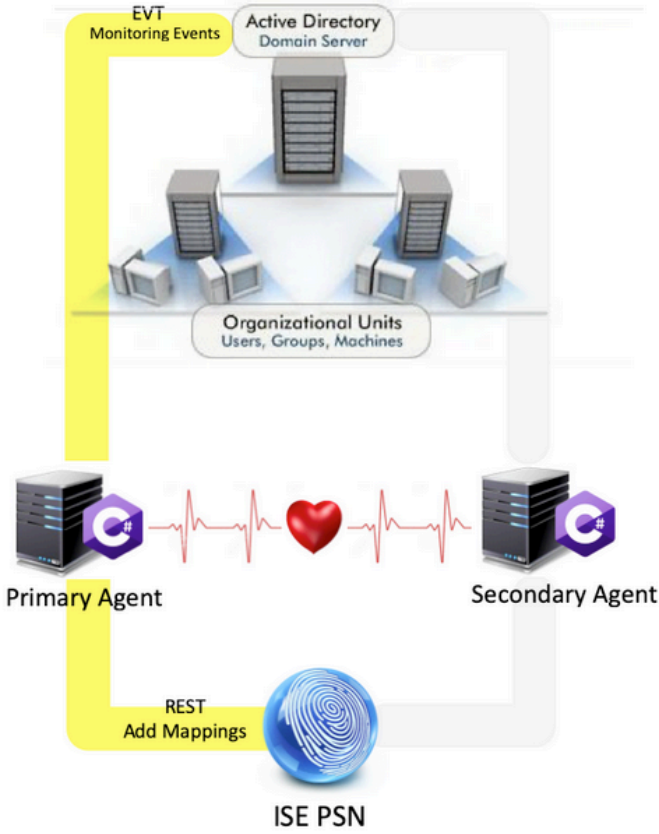
تابلطتملا

ةيلالتل عيضاوملاب ةفرعم لكي دل نوكت نأب Cisco ي صوت:

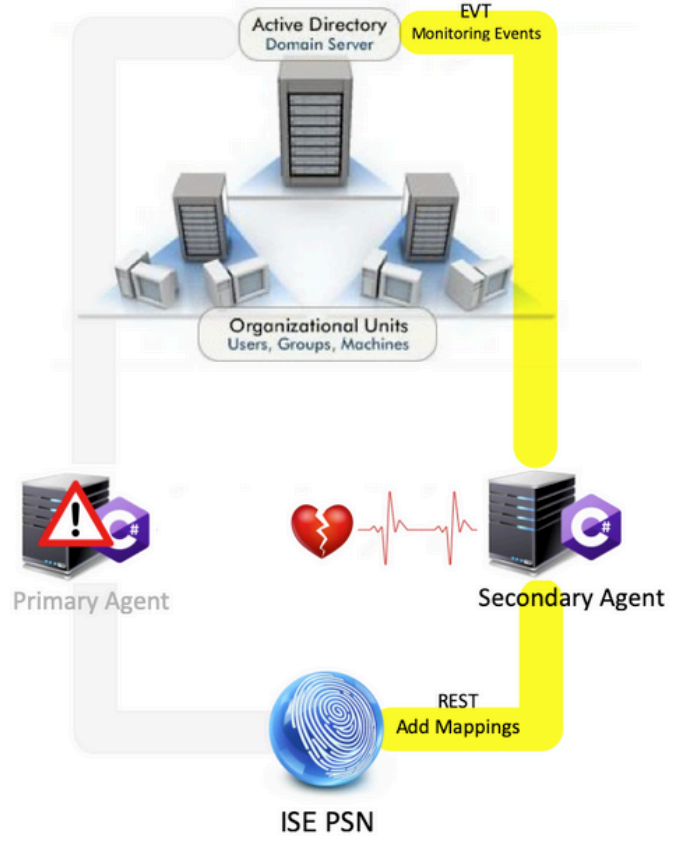
- Cisco نم ةي وهلا تامدخ ةرادا
- WMI و MS-RPC تالوكوتورب
- Active Directory ةرادا

ةمدختسملا تانوكملا

Primary Active, Secondary Passive



Primary Failure, Secondary Active

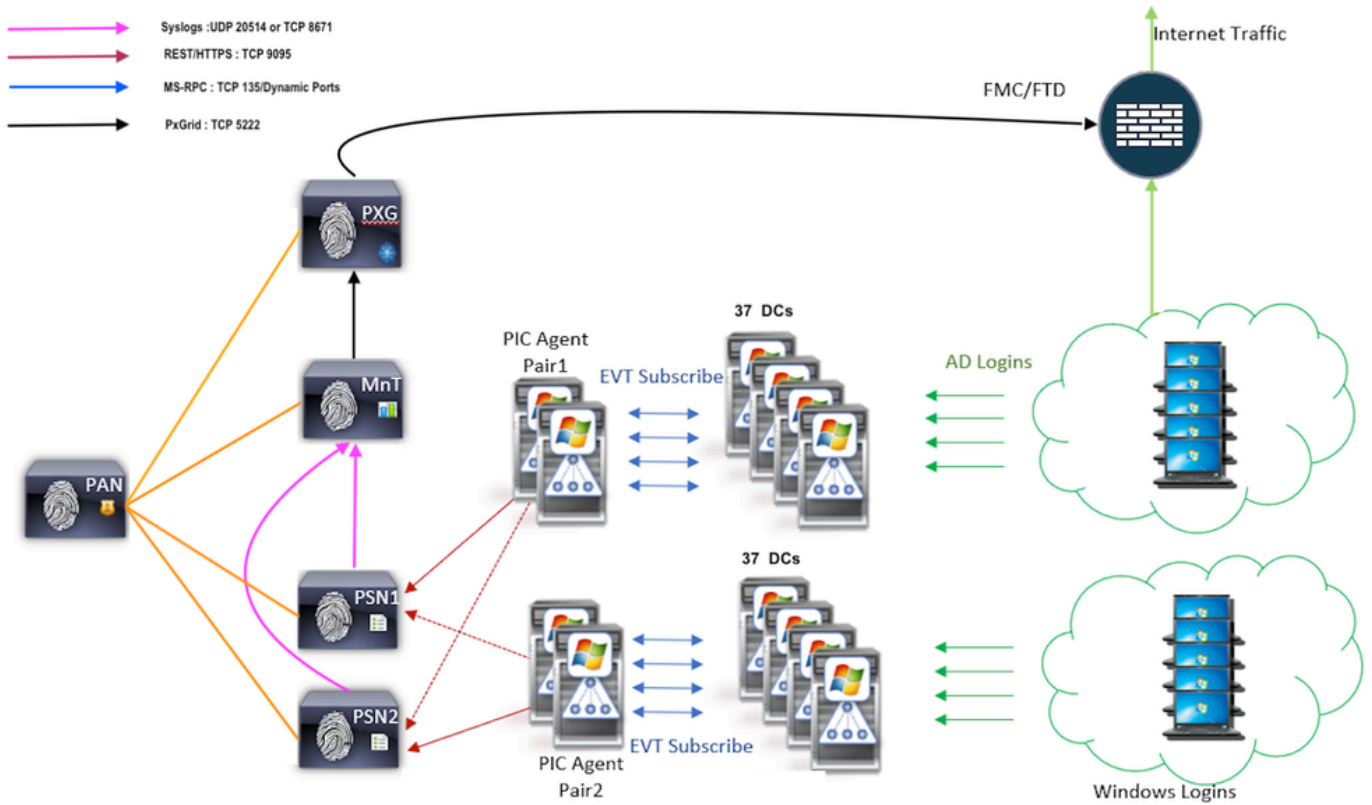


ريوطت الة لباق

تادحو نم موعدم ددعل سايقم ال ماقراً ةدايز عم لصفأ امعد ديدجل لايكوال جم انرب ال رفوي : اهرابتخا مت يتل سايقم ال ماقراً يه اه . اهتجل عام نكمي يتل اذحال ددعو لاجم لبا م كحت ال

- 74 : (جم انرب ال نم نيچوز عم) اهدصر مت يتل لاجم لبا م كحت ال تادحو ددعل ىصق ال دحل
- راي ت لك ل اذحو 3950) 292 000 : اهرابتخا مت يتل اذحال/ات اني يتل ددعل ىصق ال دحل (رم تسم)
- 500 : ةر بتخم ال جت نم ل ذفان مل ىصق ال دحل

رابتخال دادع اة ن ب ريوطت



ةيخيرات ال اادخال الالعتسا

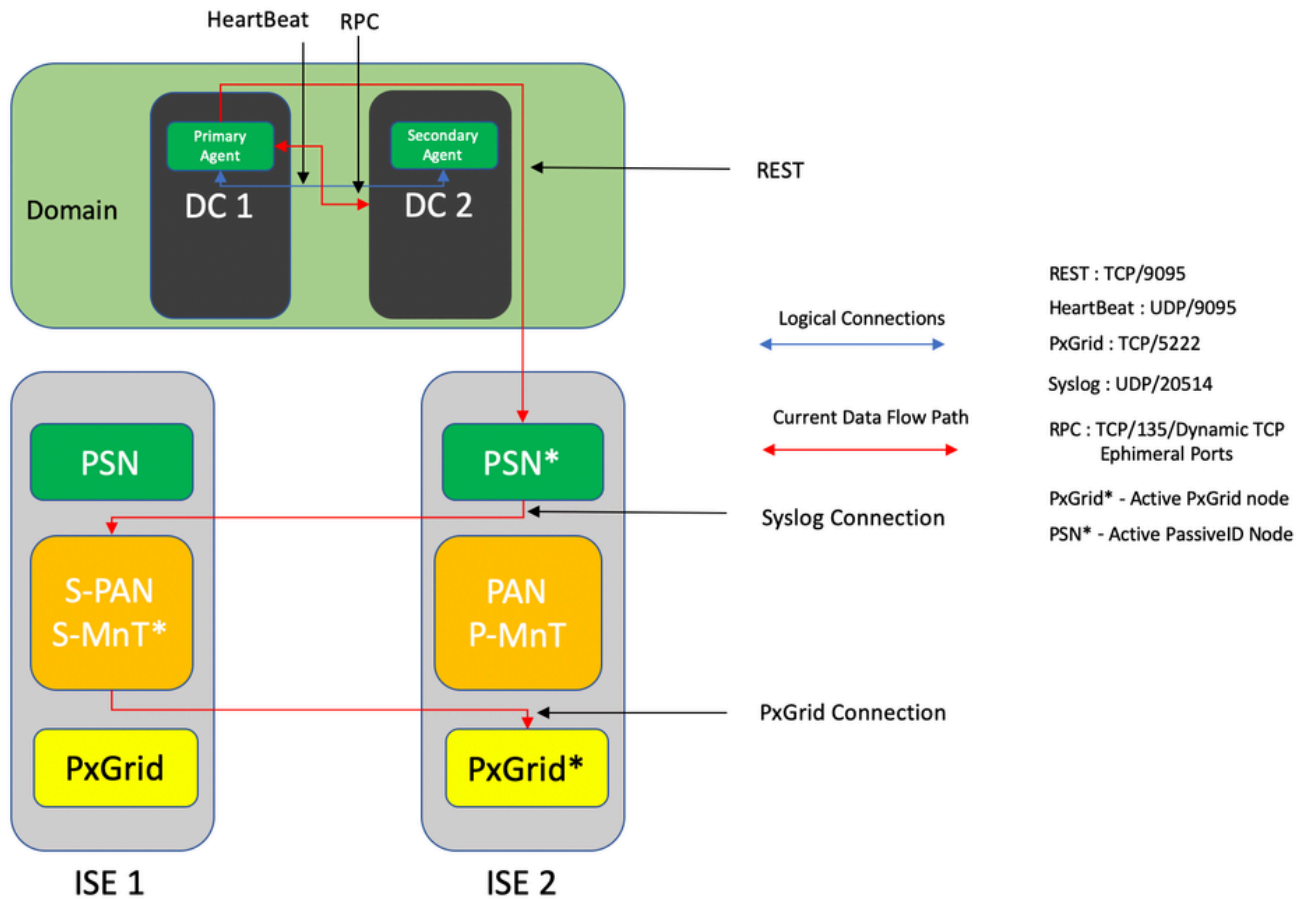
دق ف مدع نامضل ، PIC ليلكول ةمدخال ليلغشت ةداع اارج اءلا ف و ا ، لش فال زواجت ةلا ف ي مت ةينمز ةرتفل يضا ملال ف اه و اشن ن مت ي ال اادخال الالعتسا الال متي ، تانا ي ةي ا نع ISE ن مالعتسا الال متي ، يضا رتفا لكش بو . ير ا ةرم PSN دق الال اسرا واه نيوك ت تانا ي بلل دق ف ا ض فرل ةي نا ت 60 ةمي ق ب ةمدخال ادب ذنم عقت ي الال ةق با الال اادخال الال ةمدخال نادق ف انا ت ا .

لقا ةعلا م في لالت

لالمال الال ن ماض ف ثكم لكش ب (CPU) ةيزك رمال ةعلا م الال ةدحو مدختست ي الال WMI س كع الال عو تره ظا و . WMI لثم دراوم الال نم ديدع الال ك لهتست الال EVT ةينقت ن ا ف ، ةري ب الال و ا ةري ب الال EVT. ةينقت مادختسا ب تاراس ف الال الال ار ي ثك ان سحم اءا سا ي ق الال تارا ب ت ا خ ا .

نيوك الال

لاص الال ي طي طخت الال مسر الال



تاني وكتال

PassiveID ليكول ISE ني وكت

ةدحاو ةسايس ةمدخ ةدقع ىلع Passive Identity تامدخ ني كمت بجي، PassiveID تامدخ ني وكتال يف لمعت يتال ةلماخل ةي وهال تامدخ لى صقأ دحك ني تدقع مادختسا نكمي. لقألا ىلع (PSN) نكمي و Active Directory لاجم ىل ISE مامضنا اضيأ بجي. يطايت حال/طشنال لى غشتال عضو مت "ءالكو" ةطساوب لاجملا اذ ه يف ةدوجوملا هذ لاجملا اب مكحتال تادحو ةبقارم طقف [Active Directory](#) لمالك لى لى عجر، Active Directory لاجم ىل ISE لى مامضنال ل ISE ىلع مهنى وكت

وه امك ةلماخل ةي وهال تامدخ ني كمت ل ريرحت > [PSN رتخأ] > رشن > ماظن > ةرادا ىل لقتنا انه حضورم:

Cisco ISE Administration - System - Deployment

Deployment Licensing Certificates Logging Maintenance Upgrade Upgrade Refresh Backup & Restore Admin Access Settings

ISE30LABH2

Dedicated MnT

Policy Service

Enable Session Services

Include Node in Node Group: None

Enable Profiling Service

Enable Threat Centric NAC Service

Enable SXP Service

Enable Device Admin Service

Enable Passive Identity Service

pxGrid

وه امك دي ج ليك ورش نل ة فاضا > ءالك و > تار فوم > PassiveID > لم عل ا زكارم لى ل ل قتنا
انه حضورم:

Cisco ISE Work Centers - PassiveID - Providers

Overview Providers Subscribers Certificates Troubleshoot Reports

Active Directory

Agents

API Providers

SPAN

Syslog Providers

Mapping Filters

Endpoint Probes

Agents > New Agents

Deploy New Agent

Register Existing Agent

Name *
PassiveIDAgentPrimary

Description
Primary Agent

Host FQDN *
WIN-4RCAO93JKH8.surendrr.lab.local

User Name *
administrator

Password *
..... Show Password

Protocol *
MS-RPC

High Availability Settings

Standalone

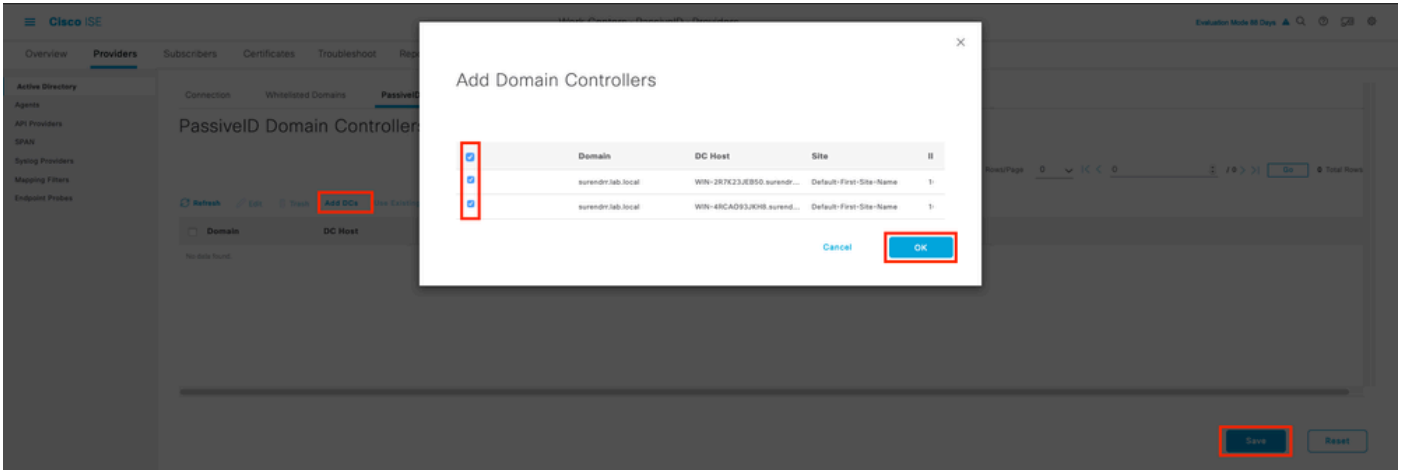
Primary

Secondary

Cancel Deploy

ل ا ج م ل ا ب م ك ح ت ل ة د ح و لى ل ع ISE ة ط س ا و ب لى م ع ل ا تى ب ث ت م تى س ن ا ك ا ذ ا 1. ة ظ ح ا ل م
ه ل ي غ ش ت و ج م ا ن ر ب تى ب ث ت ل ة ف ا ك ت ا ز ا ي ت م ا ا ن ه م د خ ت س م ل ا ب ا س ح ل ل ن و ك ي ن ا ب ج ي ف
ن ا ن ك م ي (FQDN). "ف ي ض م ل ل ل م ا ك ل ا ب ل ه و م ل ا ل ا ج م ل ا م س ا" ل ق ح ي ف ر و ك ذ م ل ا م د ا خ ل ل لى ل ع
ل ا ج م ل ا ب م ك ح ت ة د ح و ن م ا ل د ب و ض ع م د ا خ و ه ا ن ه ف ي ض م ل ا ل FQDN ن و ك ي

2. م س R P C م ع ISE، ن م ة ق ب ا س ر ش ن ة ل م ع ن م و ا، ا ي و د ي ل ع ف ل ا ب لى م ع تى ب ث ت م ت ا ذ ا.



> لمعل زكارم ىلإ لقتنا ،مهنم شادحأل دادرتسال مه مادختسا نكمي نىذلا ءال كولا ديدحتل
PassiveID > [طبرلا ةطقن ىلع رقنا] > Active Directory > تامدخال ىرفوم > PassiveID
م ث ،لېك ورتخأ .رورملا ةملكو مدختسملا مسال خدأ .رىرت قوف رقناو لاجم لاب مكحتل تادحو
نىوكتل لامكإل PassiveID بىوبتلل ةمالع ىف ظفح قوف رقنا .ةشاشلا ظفح



Edit Item

Host FQDN

WIN-4CP5CGGV2UI.surendrr.lab.local

Description

User Name*

administrator

Password

.....

Show Password

Protocol


Agent

Agent*

PassiveIDAgentPrimary

Cancel

Save

 3.0 رادصالا ىتح مسقلا اذه يف انه رابتخاو نيوكت تاراىخ كانه نوكي نأ نكمي :ةظالم Patch 4.

PassiveID ليوكت فلم مهف

ف C:\Program files (x86)\Cisco\Cisco ISE PassiveID Agent\PICAgent.exe.config في PassiveID لماع نيوكت فلم دجاوتي انه حضوم ىوتحم ىلع نيوكتال فلم يوتحي .

```
<?xml version="1.0" encoding="utf-8"?>
```

```
<نيوكتال>
```

```
<configSections>
```

```
<section name="log4net" type="log4net.config.log4NetConfigurationSectionHandler, log4net"/>
```

```
</configSections>
```

```
<log4net>
```

```

<root>
<level value="debug" /> <!-- اري دحت ، اطخ ، حداف ، لي غشت ال فاق ي : لي جشت ال تا يوت سم -->
<!-- all ، اء اطخ ال ج ح ص ت ، تام ول عم
لم اع ل ا ه ع ي م ج ت م ت ي ت ال ال ج س ل ال ص ا خ ال " ل ج س ل " يوت سم ن ي ي ع ت ي ل ع ا ذ ه ل م ع ي -->
PassiveID ي ل ع ه ل ي غ ش ت م ت ي ي ذ ل ا م دا خ ال ي ل ع -->
<appender-ref ref="RollingFileAppender" />
</root>
<Appender name="RollingFileAppender" type="log4net.Appender.RollingFileAppender">
<file value="CiscoSEPICAgent.log" /> <!-- ا ذ ه ل ي د ع ت ب م ق ت ال -->
<appendToFile value="true" />
<rollingStyle value="size" />
<maxSizeRollBackup value="5" /> <!-- ا ذ ه ط ب ض ي -->
<!-- ا ه ر ي و د ت ل ب ق ا ه و ا ش ن | م ت ي ي ت ال
م ت ي ل ج س ف ل م ل ك ل م ج ح ي ص ق ا ا ذ ه ط ب ض ي -->
<maximumFileSize value="10 م ت ي ا ب ا غ ي م" /> <!-- ا ذ ه ط ب ض ي -->
<!-- ه و ا ش ن |
<staticLogFileName value="true" />
<!-- ط ي ط خ ت ال ع و ن
<conversionPattern value="%date %level - %message%new line" />
</ط ي ط خ ت ال />
</ق ح ل م ل />
</log4net>
<!-- ا ذ ه ط ب ض ي
<supportedRuntime version="v4.0"/>
<supportedRuntime version="v2.0.50727"/>
</startup>
<appSettings>
<add key="heartbeatFrequency" value="400" /> <!-- ا ذ ه د د ح ي
ا ه ن ي و ك ت م ت ا ذ ا ي و ن ا ث ل ل م ا ع ل ا و ي س ا س ا ل ل ي م ع ل ن ي ب ا ه ل ي غ ش ت م ت ي ي ت ال ا ي ن ا ث ي ل ل م
I S E ي ل ع ج و ز ي ف -->
<add key="heartbeatThreshold" value="1000"/> <!-- ا ذ ه د د ح ي
ا ذ ه د م ل ل ي ص ق ا ل ا ذ ه د د ح ي
ك ل ذ د ع ب م ت ي ي ت ال ب ل ق ل ا ت ا ر ق ن ا ه ل ج ا ن م ل ي م ع ل ر ط ت ن ي ي ت ال ي ل ل م ل ي ن ا و ث ل ل ا ب ا ي ن م ز ل
ر خ ا ل ل ي م ع ل ي ل ع ل ف س ا م ا ل ع ع و
<add key="showHeartbeats" value="false" /> <!-- ا ذ ه د د ح ي
ل ن ا س ر ض ر ع ل "true" ي ل ا م ي ق ل ا ر ي ي غ ت ب م ق -->
<!-- ل ج س ل ف ل م ي ف ب ل ق ل ا ض ب ن
<add key="maxRestThreads" value="200" /> <!-- ا ذ ه د د ح ي
R E S T ط ب ا ر ت ت ا ر ش و م د د ع ل ي ص ق ا ل ا ذ ه د د ح ي
ن م ه ب ح ص ن ي م ل ا م و ي ت ح ا م ي ق ل ا ه ذ ه ر ي غ ت ال I S E . ل ا ش ا د ا ل ل ا س ر ا ل ا ه ج ا ت ن | ن ك م ي ي ت ال
C i s c o T A C . -->
<add key="mappingTransport" value="rest" /> <!-- ا ذ ه د د ح ي
ل ا س ر ا ل م د خ ت س م ل ا ط ي س و ل ا ع و ن
<!-- ا ذ ه ر ي غ ت ال I S E . ي ل ا ت ا ن ي ي ع ت ال
<add key="maxHistorySeconds" value="60" /> <!-- ا ذ ه د د ح ي
ي ت ال ي ض ا م ل ا ي ف ي ن ا و ث ل ل ا ب ا ذ ه د د ح ي
<!-- ا ذ ه د د ح ي
<add key="restTimeout" value="5000" /> <!-- ا ذ ه د د ح ي
I S E ي ل ا R E S T ا ع ا د ت س ا ل ا ه م ل ا م ي ق د د ح ي
<!-- ا ذ ه د د ح ي
<add key="showTPS" value="false" /> <!-- ا ذ ه د د ح ي
T P S ض ر ع ل "true" ي ل ا م ي ق ل ا ه ذ ه ر ي ي غ ت ب م ق -->
<!-- I S E ي ل ا ا ه ل ا س ر ا و ا ه ل ا ب ق ت س ا م ت ي ي ت ال ا ش ا د ا ل ل
<add key="showPOST" value="false" /> <!-- ا ذ ه د د ح ي
ا ش ا د ا ل ا ع ا ب ط ل "true" ي ل ا م ي ق ل ا ه ذ ه ر ي ي غ ت ب م ق -->
<!-- I S E ي ل ا ا ه ل ا س ر ا م ت ي ي ت ال

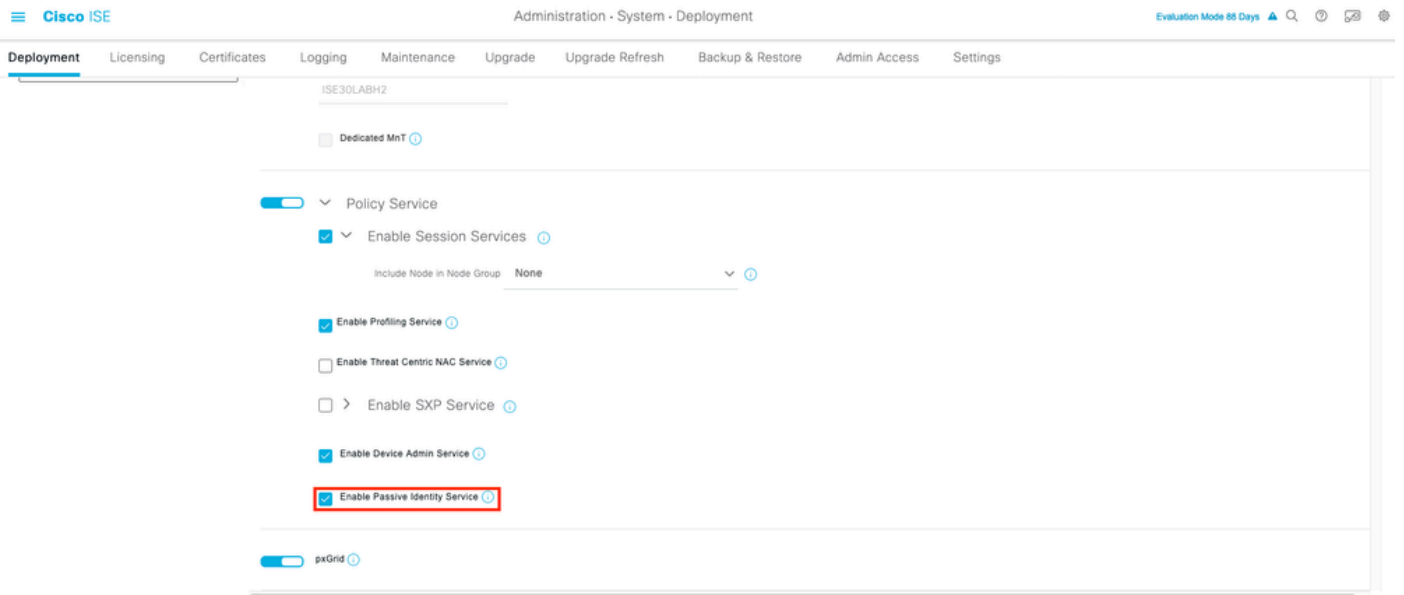
```

```
<add key="nodeFailOverTimeSpan" value="5000" /> <!-- ددحي طارش دحل ايتلا ةيناث يلل ملاب دحل طارش ددحي -->
يتلا ةيناث يلل ملاب دحل طارش ددحي
PSN PassiveID ةدق ب لاصتالا يف ثدحت نأ نكمي يتلا ءاطخألا ددح باسح اهلالخ متي
--> لش فل ايطختل ةطشنلا
<add key="nodeFailOverMaxErrors" value="5" /> <!-- ددحي دحل ايتلا ةيناث يلل ملاب دحل طارش ددحي -->
حومس مل ايطخألا ددحل ايتلا ةيناث يلل ملاب دحل طارش ددحي
PSN PassiveID ةدق ب لاصتالا يف ثدحت نأ نكمي يتلا ءاطخألا ددح باسح اهلالخ متي
--> دادعتسالا عضو يف
</appSettings>
</configuration>
```

ةحصلا نم ققحتلا

ISE لىل PassiveID تامدخ نم ققحتلا

1. عضو مت امك (GUI) ةيموسرلا مدختس ملة ةهجاو لىل PassiveID ةمدخ نيكم نم ققحت. (CLI) رمأوالا رطس ةهجاو لىل show application status رمأالا نم ليغشتلا ديقي لىل ةمالع ISE. ةصاخلا



<#root>

```
ISE PROCESS NAME STATE PROCESS ID
```

```
-----
Database Listener running 129052
Database Server running 108 PROCESSES
Application Server running 9830
Profiler Database running 5127
ISE Indexing Engine running 13361
AD Connector running 20609
M&T Session Database running 4915
M&T Log Processor running 10041
Certificate Authority Service running 15493
EST Service running 41658
SXP Engine Service disabled
Docker Daemon running 815
```

TC-NAC Service disabled
pxGrid Infrastructure Service disabled
pxGrid Publisher Subscriber Service disabled
pxGrid Connection Manager disabled
pxGrid Controller disabled

PassiveID WMI Service running

15951

PassiveID Syslog Service running

16531

PassiveID API Service running

17093

PassiveID Agent Service running

17830

PassiveID Endpoint Service running

18281

PassiveID SPAN Service running

20253

DHCP Server (dhcpd) disabled
DNS Server (named) disabled
ISE Messaging Service running 1472
ISE API Gateway Database Service running 4026
ISE API Gateway Service running 7661
Segmentation Policy Service disabled
REST Auth Service disabled
SSE Connector disabled

2. زكارم في لاجم لآب مكحتل تادحوب الصتم ISE Active Directory رفوم ناك اذام ققحت.
لمعلا > PassiveID > تامدخل رفوم > Active Directory > Connection.

ISE Node	ISE Node R...	Status	Domain Controller	Site
ISE30LABH1.suresndr.lab.local	PRIMARY	Operational	WIN-257X218950.suresndr.l...	Default-Free-Site-Name
ISE30LABH2.suresndr.lab.local	SECONDARY	Operational	WIN-4KCA093.KH8.suresndr.l...	Default-Free-Site-Name

3. في ليكول ةطساوب اهتبقارم متي ةبولطملا لاجم لآب مكحتل تادحوت ناك اذام ققحت.
لمعلا > PassiveID > تامدخل رفوم > Active Directory > PassiveID.

Cisco ISE Work Centers - PassiveID - Providers

Overview Providers Subscribers Certificates Troubleshoot Reports

Active Directory Agents API Providers SPAN Styling Providers Mapping Filters Endpoint Probes

Connection Whitelisted Domains **PassiveID** Groups Attributes Advanced Settings

PassiveID Domain Controllers

Rows/Page 2 < 1 > 1 > Go 2 Total Rows

Refresh Edit Trash Add DCs Use Existing Agent Config WMI Add Agent

Domain	DC Host	Site	IP Address	Monitor Using
<input type="checkbox"/> surendr.lab.local	WIN-2R7K23JE850.surendr...	Default-First-Site-Name	10.127.196.85	PassiveIDAgentPrimary
<input type="checkbox"/> surendr.lab.local	WIN-4RCAD93JKH8.surend...	Default-First-Site-Name	10.127.196.85	PassiveIDAgentPrimary

4. لي غشت الل دي ق اهت بقارم متي يت الل لاجم لاب مكحت الل تادحو ة لاج تناك اذ اام ق قحت .
 PassiveID > لمعل زكارم في تامولعمل ة حول لي عل رضخا ة مالع عضوم ت ، لاثملا لي بس
 تامولعمل ة حول > ة مالع ة رظن .

Cisco ISE Work Centers - PassiveID - Overview

Overview Providers Subscribers Certificates Troubleshoot Reports

Introduction Dashboard Live Sessions

Main

Sessions 0 Providers 2 Agents 2 Subscribers 10

PROVIDERS

Status	Name	Agent	Domain
<input checked="" type="checkbox"/>	WIN-2R7K23JE850.surendr.lab.local	PassiveIDAgentPrimary	surendr.lab.local
<input checked="" type="checkbox"/>	WIN-4RCAD93JKH8.surendr.lab.local	PassiveIDAgentPrimary	surendr.lab.local

Subscribers

Name	Status	Description
ise-admin...	Online	
ise-admin...	Online	
ise-bridge...	Online	
ise-bridge...	Online	
ise-fanout...	Online	
ise-fanout...	Online	
ise-fanout...	Online	
ise-ns...	Online	

ACTIVE SESSIONS

No data available.

Last refreshed 2020-11-05 17:40:40

Last refreshed 2020-11-05 17:40:38

5. ة دحو لي ل Windows لي لوخد لي ج ست دنع Live لمعل تاسلج ل ة بيت نم ق قحت .
 Live. لمعل تاسلج > ة مالع ة رظن > PassiveID > لمعل زكارم في لاجم لاب مكحت الل

Cisco ISE Work Centers - PassiveID - Overview

Overview Providers Subscribers Certificates Troubleshoot Reports

Introduction Dashboard Live Sessions

Refresh Show Latest 20 records Within Last 24 hours

Refresh Export To

Initiated	Updated	Session Sta...	Provider	Action	Endpoint ID	Identity	IP Address	Endpoint Profile	Posture St...	Security G...	Server	Auth M...	Authentic...
X					Endpoint ID	Identity		Endpoint Profile	Posture Status	Security Gros	Server	Auth Meth	Authentic
Nov 05, 2020 05:59:31.925 PM	Nov 05, 2020 05:59:31.9...	Authenticated	Agent	Show Actions	10.127.196.85	Administrator	10.127.196.85				ISE3LABH1		

Last Updated: Thu, Nov 05, 2020 18:01:03 GMT+05:30 (India Standard Time)

Records Shown: 1
























Windows م داخ لي ل ة كول تامدخ نم ق قحت الل

1. PIC لي كو ت بيت مت شي م داخ الل لي ل ISEPICAgent ة مدخ نم ق قحت .

Task Manager

File Options View

Processes Performance Users Details **Services**

Name	PID	Description	Status	Group
 ISEPIAgent	9392	Cisco ISE PassiveID Agent	Running	
 WSearch		Windows Search	Stopped	
 wmiApSrv		WMI Performance Adapter	Stopped	
 WinDefend	3052	Windows Defender Service	Running	
 WIDWriter	2044	Windows Internal Database VSS Writer	Running	
 WdNisSvc		Windows Defender Network Inspecti...	Stopped	
 VSS		Volume Shadow Copy	Stopped	
 VMwareCAFManagementA...		VMware CAF Management Agent Se...	Stopped	
 VMwareCAFCommAmqpLi...		VMware CAF AMQP Communicatio...	Stopped	
 vmvss		VMware Snapshot Provider	Stopped	
 VMTools	2484	VMware Tools	Running	
 VGAuthService	2480	VMware Alias Manager and Ticket S...	Running	
 vds	4236	Virtual Disk	Running	
 VaultSvc	724	Credential Manager	Running	
 UIODetect		Interactive Services Detection	Stopped	
 UevAgentService		User Experience Virtualization Service	Stopped	
 TrustedInstaller		Windows Modules Installer	Stopped	
 TieringEngineService		Storage Tiers Management	Stopped	
 SQLWriter	3148	SQL Server VSS Writer	Running	
 SQLTELEMETRY\$SQLEXPRES...	4884	SQL Server CEIP service (SQLEXPRESS)	Running	
 SQLBrowser		SQL Server Browser	Stopped	
 SQLAgent\$SQLEXPRESS		SQL Server Agent (SQLEXPRESS)	Stopped	
 snpsvc		Software Protection	Stopped	

 Fewer details |  Open Services

ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن م ة و مچ م ادخت ساب دن تسمل اذ ه Cisco ت مچرت
ملاعلاء نأ عي مچ ي ف ن ي م دخت سمل ل معد ي و تح م مي دقت ل ة ي رش ب ل و
امك ة ق ي قد ن و ك ت ن ل ة ي ل ة مچرت ل ض ف أ ن ة ظ حال م ي ج ر ي . ة ص ا خ ل م ه ت غ ل ب
Cisco ي ل خ ت . ف ر ت ح م مچرت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة مچرت ل ا ع م ل ا ح ل ا و ه
ي ل ا م ا د ع و ج ر ل ا ب ي ص و ت و ت ا مچرت ل ا ه ذ ه ة ق د ن ع ا ه ت ي ل و ئ س م Cisco
Systems (ر ف و ت م ط ب ا ر ل ا) ي ل ص أ ل ا ي ز ي ل ج ن ا ل ا دن تسمل ا