

Configurazione dell'agente ID passivo del motore dei servizi di identità basato su EVT

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[È necessario un nuovo protocollo](#)

[Vantaggi dell'utilizzo di MS-EVEN6](#)

[Alta disponibilità](#)

[Scalabilità](#)

[Architettura di impostazione del test di scalabilità](#)

[Query eventi cronologici](#)

[Minore sovraccarico di elaborazione](#)

[Configurazione](#)

[Diagramma connettività](#)

[Configurazioni](#)

[Configurazione di ISE per l'agente PassiveID](#)

[Informazioni sul file di configurazione di PassiveID Agent](#)

[Verifica](#)

[Verifica dei servizi PassiveID sull'ISE](#)

[Verifica servizi agente su Windows Server](#)

Introduzione

Questo documento descrive il nuovo agente ISE (Identity Services Engine) Passive Identity Connector (ISE-PIC) introdotto nella versione ISE 3.0.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco Identity Services Administration
- MS-RPC, protocolli WMI
- Amministrazione di Active Directory

Componenti usati

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

- Cisco Identity Services Engine versione 3.0 e successive
- Microsoft Windows Server 2016 Standard

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

Questo articolo descrive anche i vantaggi dell'agente ISE-PIC e la configurazione di tale agente sull'ISE. ISE Passive Identity Agent è diventato parte integrante della soluzione Identity Firewall che utilizza anche Cisco FirePower Management Center.

È necessario un nuovo protocollo

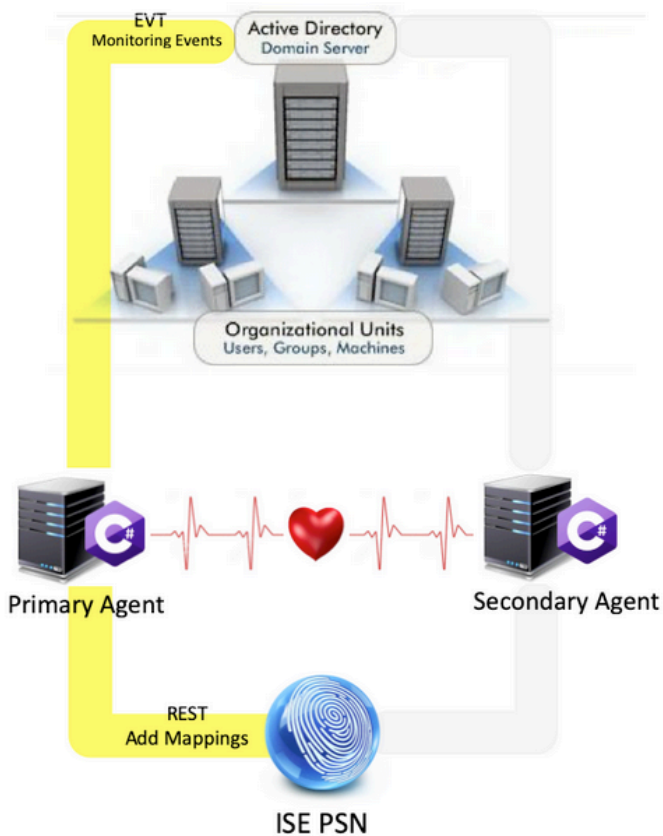
La funzione di identità passiva (ID passivo) di ISE guida una serie di importanti scenari di utilizzo, tra cui Identity-Based Firewall, EasyConnect, e così via. Questa funzionalità dipende dalla possibilità di monitorare gli utenti che accedono ai controller di dominio Active Directory e di conoscere il nome utente e l'indirizzo IP. Il protocollo principale attualmente utilizzato per monitorare i controller di dominio è WMI. Tuttavia, è difficile/invasivo da configurare, ha un impatto sulle prestazioni sia dei client che dei server e a volte ha una latenza estremamente ampia nel visualizzare gli eventi di accesso in installazioni scalabili. Dopo approfondite ricerche e metodi alternativi per il polling delle informazioni necessarie per i servizi di identità passiva, è stato deciso un protocollo alternativo, noto come EVT (Eventing API), più efficiente nella gestione di questo caso di utilizzo. È talvolta indicato come MS-EVEN6, noto anche come Eventing Remote Protocol, che è il protocollo RPC sottostante basato su connessioni in rete.

Vantaggi dell'utilizzo di MS-EVEN6

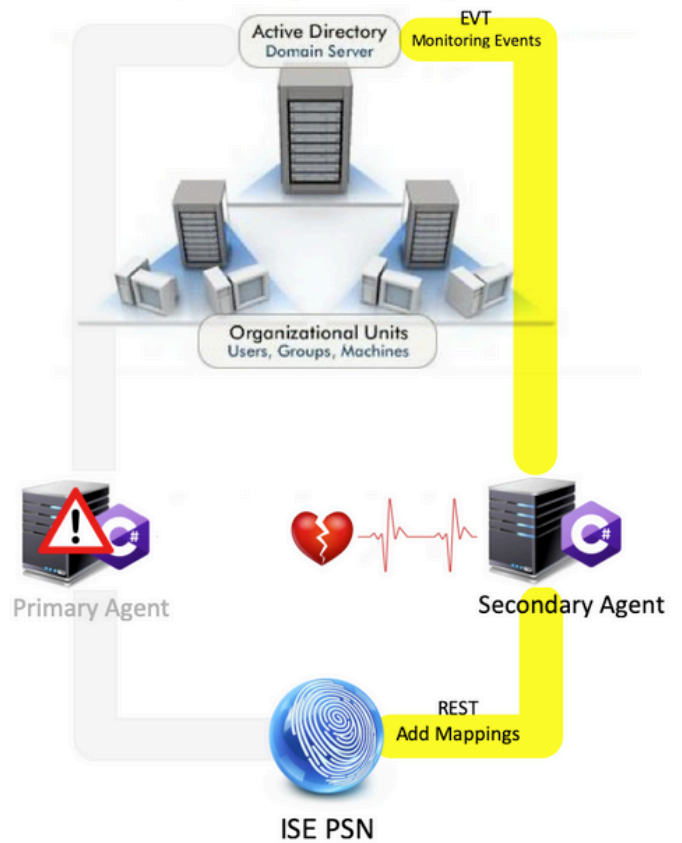
Alta disponibilità

L'agente originale non dispone di un'opzione di elevata disponibilità (HA) e se è necessario eseguire la manutenzione sul server in cui l'agente era in esecuzione o ha subito un'interruzione, gli eventi di accesso non verranno rilevati e funzionalità come il firewall basato su identità potrebbero causare la perdita di dati durante questo periodo. Questa è stata una delle principali preoccupazioni nell'uso di ISE PIC Agent prima di questa release. A partire da questa versione, gli agenti possono lavorare in alta disponibilità. ISE utilizza la porta UDP 9095 per lo scambio di heartbeat tra gli agenti al fine di garantire un'elevata disponibilità. È possibile configurare più coppie di agenti HA per il monitoraggio di controller di dominio diversi.

Primary Active, Secondary Passive



Primary Failure, Secondary Active

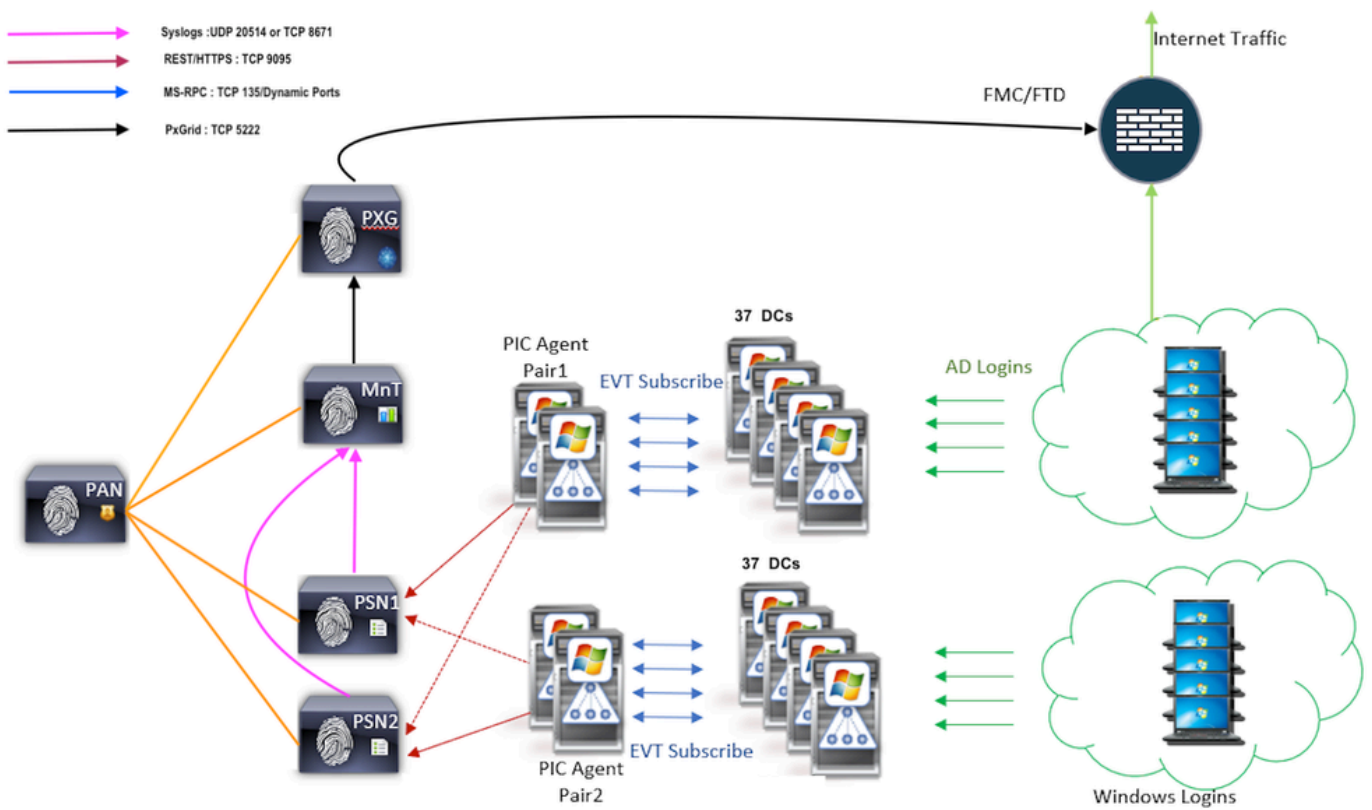


Scalabilità

Il nuovo agente fornisce un supporto migliore con numeri di scala maggiori per un numero supportato di controller di dominio e il numero di eventi che può gestire. Questi sono i numeri della scala che sono stati testati :

- Numero massimo di controller di dominio monitorati (con 2 coppie di agenti): 74
- Numero massimo di mapping/eventi testati: 292.000 (3.950 eventi per DC)
- TPS massimo testato: 500

Architettura di impostazione del test di scalabilità



Query eventi cronologici

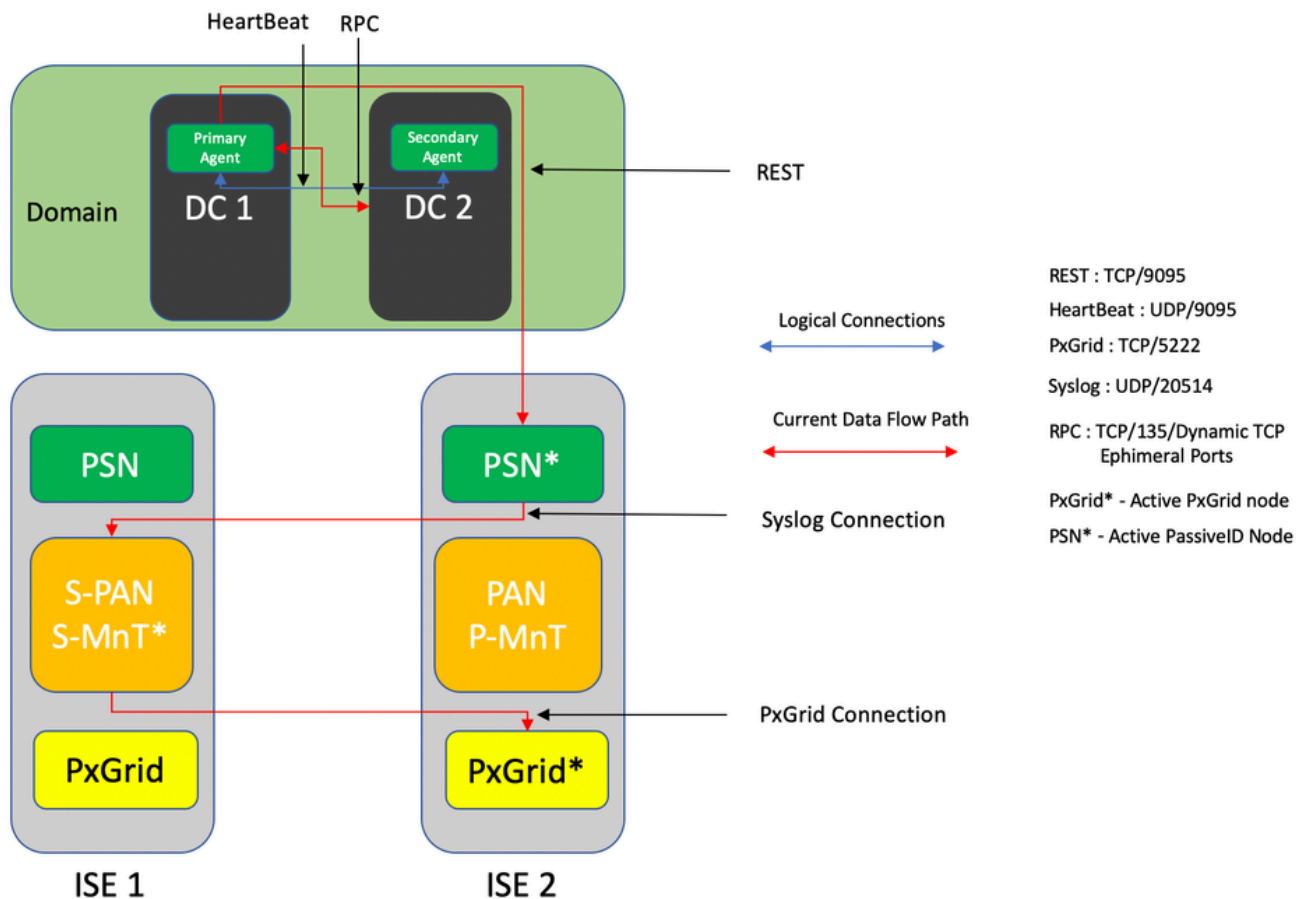
In caso di failover o nel caso in cui venga eseguito il riavvio del servizio per l'agente PIC, per assicurarsi che non vengano persi dati, gli eventi generati in precedenza per un periodo di tempo configurato vengono interrogati e inviati di nuovo ai nodi PSN. Per impostazione predefinita, ISE richiede 60 secondi di eventi passati dall'avvio del servizio per evitare qualsiasi perdita di dati durante la perdita del servizio.

Minore sovraccarico di elaborazione

A differenza di WMI, che richiede un utilizzo intensivo della CPU in caso di carico elevato o su larga scala, EVT non utilizza molte risorse come WMI. I test di scala hanno dimostrato che le prestazioni delle query con l'utilizzo dell'EVT sono state notevolmente migliorate.

Configurazione

Diagramma connettività



Configurazioni

Configurazione di ISE per l'agente PassiveID


Per configurare i servizi PassiveID, è necessario che i servizi Passive Identity siano abilitati in almeno un nodo PSN (Policy Service Node). Per i servizi di identità passiva che funzionano in modalità attiva/standby è possibile utilizzare un massimo di due nodi. Anche ISE deve essere aggiunto a un dominio Active Directory e solo i controller di dominio presenti nel dominio possono essere monitorati dagli agenti configurati sull'ISE. Per aggiungere ISE a un dominio Active Directory, consultare la [Guida all'integrazione di Active Directory](#).

Passare a Amministrazione > Sistema > Distribuzione > [Scegliere un PSN] > Modifica per abilitare i servizi di identità passiva, come mostrato di seguito:


The screenshot shows the Cisco ISE Administration interface for System Deployment. The 'Deployment' tab is active. Under the 'Policy Service' section, the 'Enable Passive Identity Service' checkbox is checked and highlighted with a red box. Other services like 'Enable Session Services', 'Enable Profiling Service', and 'Enable Device Admin Service' are also checked. The 'pxGrid' toggle is also visible.

Passare a Centri di lavoro > ID passivo > Provider > Agenti > Aggiungi per distribuire un nuovo agente come mostrato di seguito:

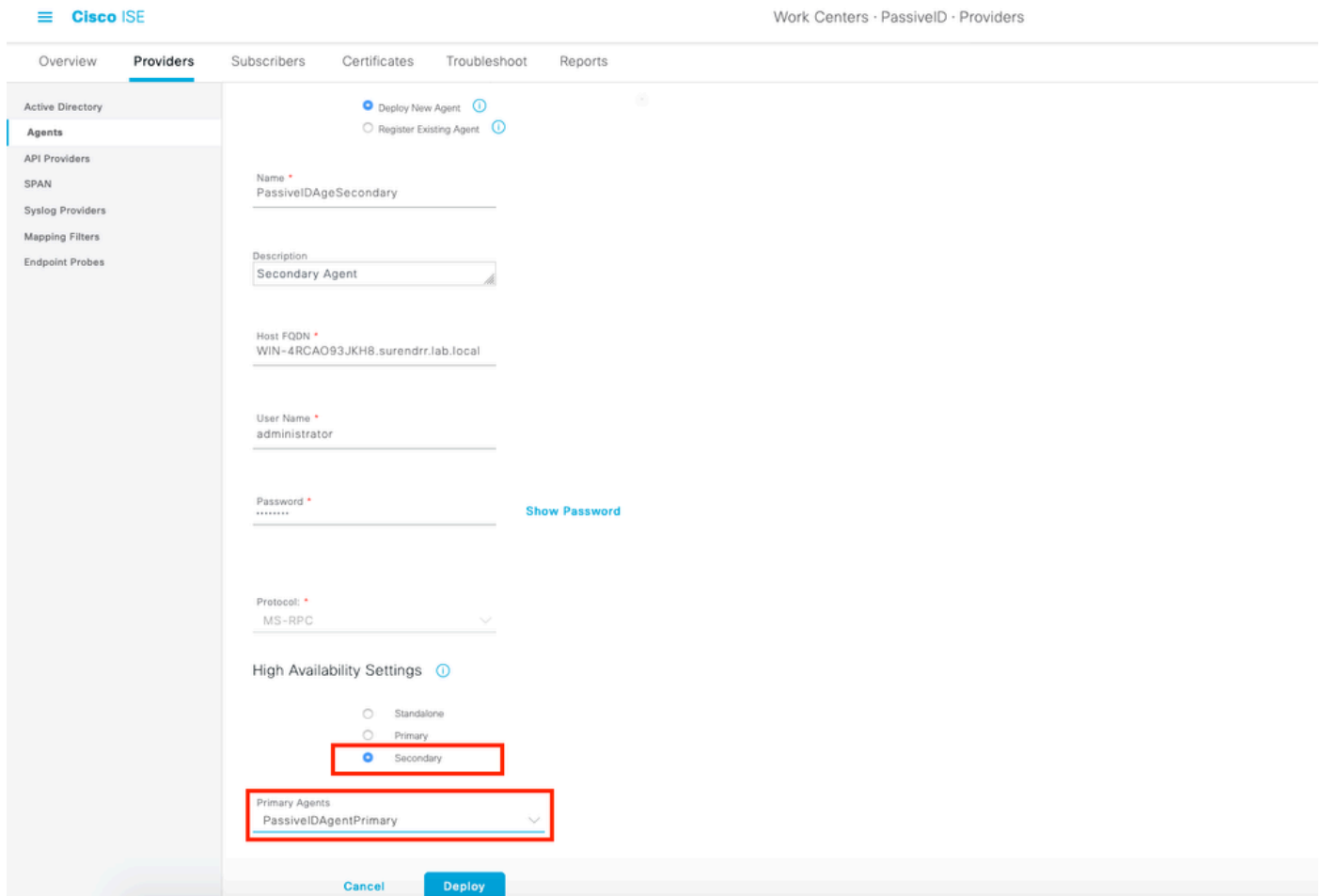
The screenshot shows the Cisco ISE Administration interface for Work Centers - PassiveID - Providers. The 'Agents > New' page is open. The 'Deploy New Agent' button is highlighted with a red box. The 'Name' field contains 'PassiveIDAgentPrimary'. The 'Description' field contains 'Primary Agent'. The 'Host FQDN' field contains 'WIN-4RCAO93JKH8.surendrr.lab.local'. The 'User Name' field contains 'administrator'. The 'Password' field is masked with dots. The 'Protocol' dropdown menu is set to 'MS-RPC' and is highlighted with a red box. Under 'High Availability Settings', the 'Primary' radio button is selected and highlighted with a red box. The 'Deploy' button is also highlighted with a red box.

 Nota: Se l'agente deve essere installato da ISE sul controller di dominio, l'account utilizzato deve disporre di privilegi sufficienti per installare un programma ed eseguirlo sul server indicato nel campo Nome di dominio completo (FQDN) host. Il nome di dominio completo (FQDN) dell'host può essere quello di un server membro anziché di un controller di dominio.

2. Se un agente è già installato manualmente o da una precedente distribuzione ISE, con

 MSRPC, le autorizzazioni e le configurazioni necessarie sul lato Active Directory o Windows sono inferiori rispetto a WMI, l'altro protocollo (e l'unico disponibile prima della versione 3.0) utilizzato dagli agenti PIC. L'account utente utilizzato in questo caso può essere un account di dominio normale che fa parte del gruppo Lettori registro eventi. Scegliere Registra agente esistente e utilizzare i dettagli dell'account per registrare l'agente installato manualmente nei controller di dominio.

Al termine di una distribuzione corretta, configurare un altro agente su un server diverso e aggiungerlo come agente secondario e quindi il relativo peer primario, come illustrato in questa immagine.

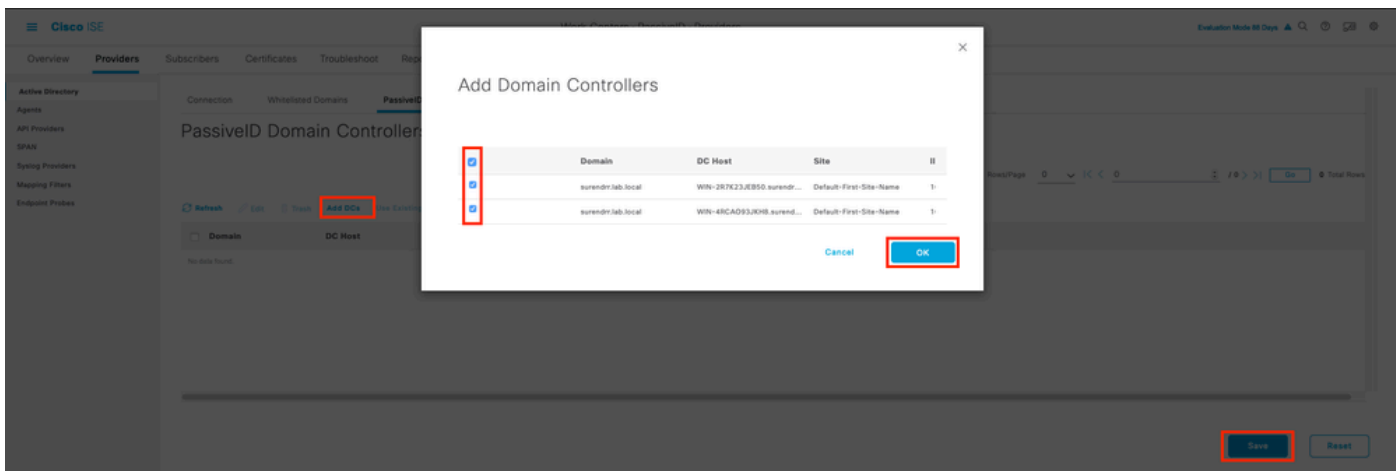


The screenshot shows the Cisco ISE configuration interface for a Secondary Agent. The page is titled "Work Centers · PassivelD · Providers" and has a navigation menu with "Providers" selected. The configuration form includes the following fields and options:

- Agents:** Deploy New Agent, Register Existing Agent
- Name:** PassivelDAgeSecondary
- Description:** Secondary Agent
- Host FQDN:** WIN-4RCAO93JKH8.surendrr.lab.local
- User Name:** administrator
- Password:** [Redacted] [Show Password](#)
- Protocol:** MS-RPC
- High Availability Settings:** Standalone, Primary, Secondary
- Primary Agents:** PassivelDAgentPrimary

Buttons for "Cancel" and "Deploy" are visible at the bottom of the form.

Per monitorare i controller di dominio che utilizzano gli agenti, selezionare Centri di lavoro > ID passivo > Provider > Active Directory > [Fare clic sul punto di join] > ID passivo . Fare clic su Aggiungi controller di dominio e scegliere i controller di dominio da cui recuperare gli eventi/mapping IP utente, fare clic su OK e quindi su Salva per salvare le modifiche, come mostrato nell'immagine.



Per specificare gli agenti da cui recuperare gli eventi, selezionare Centri di lavoro > ID passivo > Provider > Active Directory > [Fare clic sul punto di join] > ID passivo. Scegliere i controller di dominio e fare clic su Modifica. Immettere il nome utente e la password. Scegliere Agente, quindi Salva la finestra di dialogo. Fare clic su Save (Salva) nella scheda PassiveID per completare la configurazione.



Edit Item

Host FQDN
WIN-4CP5CGGV2UI.surendrr.lab.local

Description

User Name*
administrator

Password
.....


Show Password

Protocol
Agent

Agent*
PassiveIDAgentPrimary

Cancel

Save

 Nota: in questa sezione sono disponibili le opzioni Configura e Prova fino alla versione 3.0 Patch 4.

Informazioni sul file di configurazione di PassiveID Agent

Il file di configurazione dell'agente PassiveID si trova in C:\Program Files (x86)\Cisco\Cisco ISE PassiveID Agent\PICAgent.exe.config . Il file di configurazione contiene quanto riportato di seguito:

```
<?xml version="1.0" encoding="utf-8"?>
<configurazione>
<SezioniConfigurazione>
<section name="log4net" type="log4net.Config.Log4NetConfigurationSectionHandler, log4net"/>
</configSezioni>
```

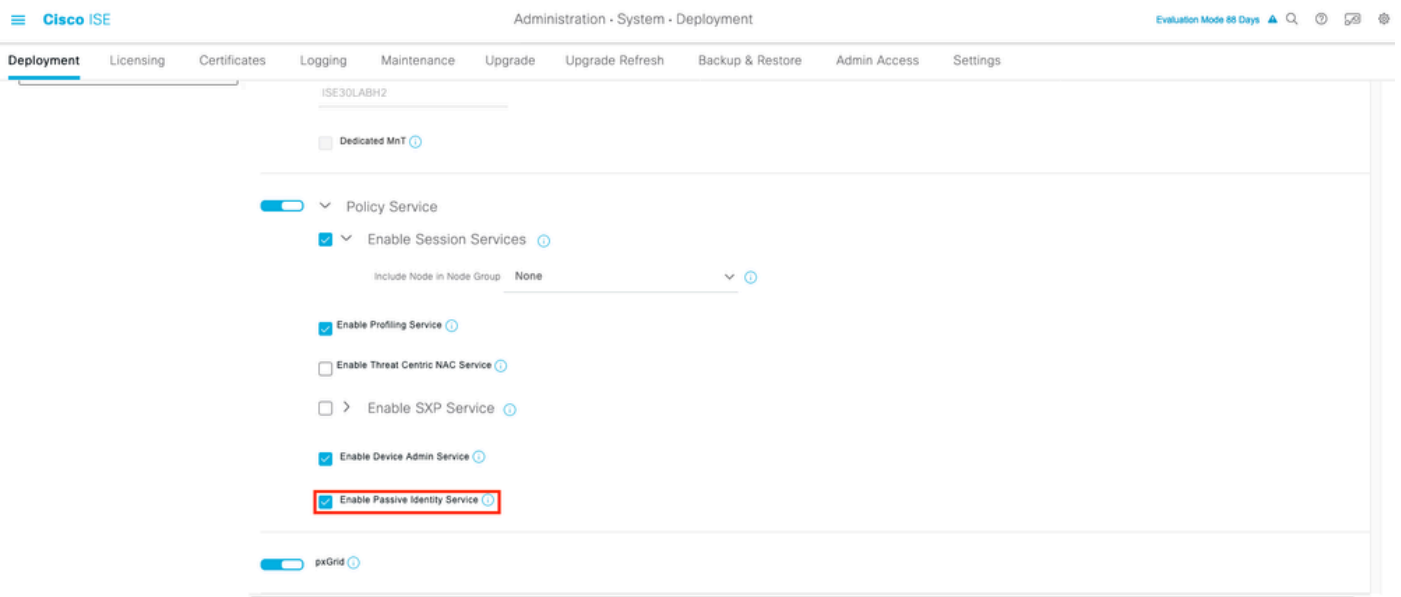
```
<log4net>
<radice>
<level value="DEBUG" /> <!-- Livelli di registrazione: OFF, FATAL, ERROR, WARN, INFO,
DEBUG, ALL -->
<!-- imposta il livello di log dei log raccolti per l'agente PassiveID sul server in cui viene eseguito. -
->
<appender-ref ref="RollingFileAppender" />
</root>
<appender name="RollingFileAppender" type="log4net.Appender.RollingFileAppender">
<file value="CiscoISEPICAgent.log" /> <!-- Non modificare -->
<appendToFile value="true" />
<rollingStyle value="Size" />
<maxSizeRollBackups value="5" /> <!-- Questo numero imposta il numero massimo di file di log
generati prima del rollover -->
<maximumFileSize value="10MB" /> <!-- Imposta le dimensioni massime di ogni file di log
generato -->
<staticLogFileName value="true" />
<layout type="log4net.Layout.PatternLayout">
<conversionPattern value="%date %level - %message%newline" />
</layout>
</appender>
</log4net>
<avvio>
<supportedRuntime version="v4.0"/>
<supportedRuntime version="v2.0.50727"/>
</avvio>
<impostazioniApp>
<add key="heartbeatFrequency" value="400" /> <!-- Questo numero definisce la frequenza del
battito cardiaco in millisecondi tra l'agente primario e l'agente secondario se configurato in una
coppia sull'ISE -->
<add key="heartbeatThreshold" value="1000"/> <!-- Questo numero definisce la durata massima
in millisecondi per cui l'agente attende gli heartbeat, dopo la quale l'altro agente viene
contrassegnato -->
<add key="showHeartbeats" value="false" /> <!-- Modificare il valore su "true" per visualizzare i
messaggi di heartbeat nel file di log -->
<add key="maxRestThreads" value="200" /> <!-- Definisce il numero massimo di thread REST
che possono essere generati per inviare gli eventi all'ISE. Non modificare questo valore fino a
quando non indicato da Cisco TAC. -->
<add key="mappingTransport" value="rest" /> <!-- Definisce il tipo di supporto utilizzato per
inviare i mapping all'ISE. Non modificare questo valore -->
<add key="maxHistorySeconds" value="60" /> <!-- Definisce la durata in secondi nel passato per
cui è necessario recuperare gli eventi cronologici in caso di riavvio del servizio -->
<add key="restTimeout" value="5000" /> <!-- Definisce il valore di timeout per una chiamata
REST all'ISE -->
<add key="showTPS" value="false" /> <!-- Modificare questo valore in "true" per visualizzare i
TPS degli eventi ricevuti e inviati all'ISE -->
```

```
<add key="showPOSTS" value="false" /> <!-- Modificare questo valore in "true" per stampare gli
eventi inviati all'ISE -->
<add key="nodeFailoverTimeSpan" value="5000" /> <!-- Definisce la condizione per la soglia in
millisecondi entro la quale viene conteggiato per il failover il numero di errori che possono
verificarsi nella comunicazione con il nodo PSN ID passivo attivo -->
<add key="nodeFailoverMaxErrors" value="5" /> <!-- Definisce il numero massimo di errori
tollerati nel nodo specificatoFailoverTimeSpan prima del failover sul nodo PSN PassiveID in
standby -->
</appSettings>
</configuration>
```

Verifica

Verifica dei servizi PassiveID sull'ISE

1. Verificare se il servizio PassiveID è abilitato sulla GUI e se è stato contrassegnato anche come in esecuzione dal comando show application status ise sulla CLI di ISE.



<#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. Verificare se il provider ISE Active Directory è connesso ai controller di dominio nei centri di lavoro > ID passivo > Provider > Active Directory > Connessione.

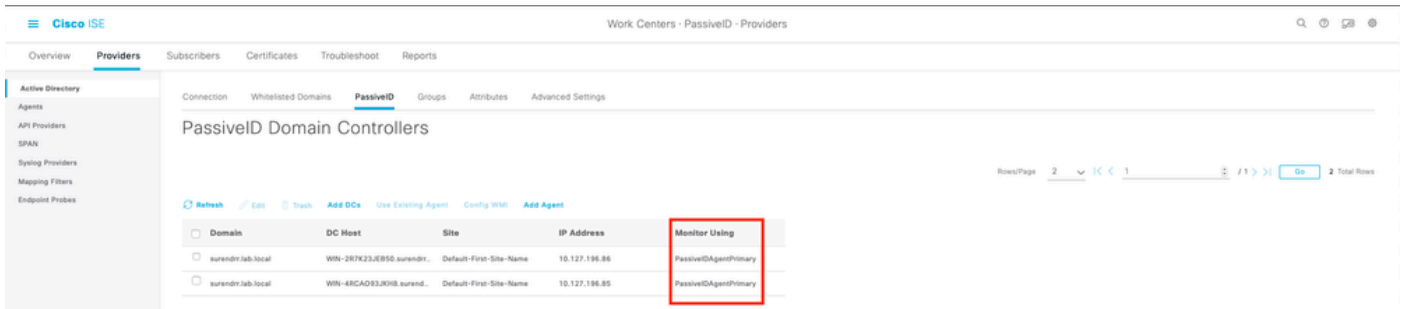
The screenshot shows the Cisco ISE Work Centers interface for PassiveID Providers. The 'Providers' tab is active, and the 'Active Directory' sub-tab is selected. The 'Connection' section shows the following details:

- Join Point Name: PassiveID-AD
- Active Directory Domain: surendr.lab.local

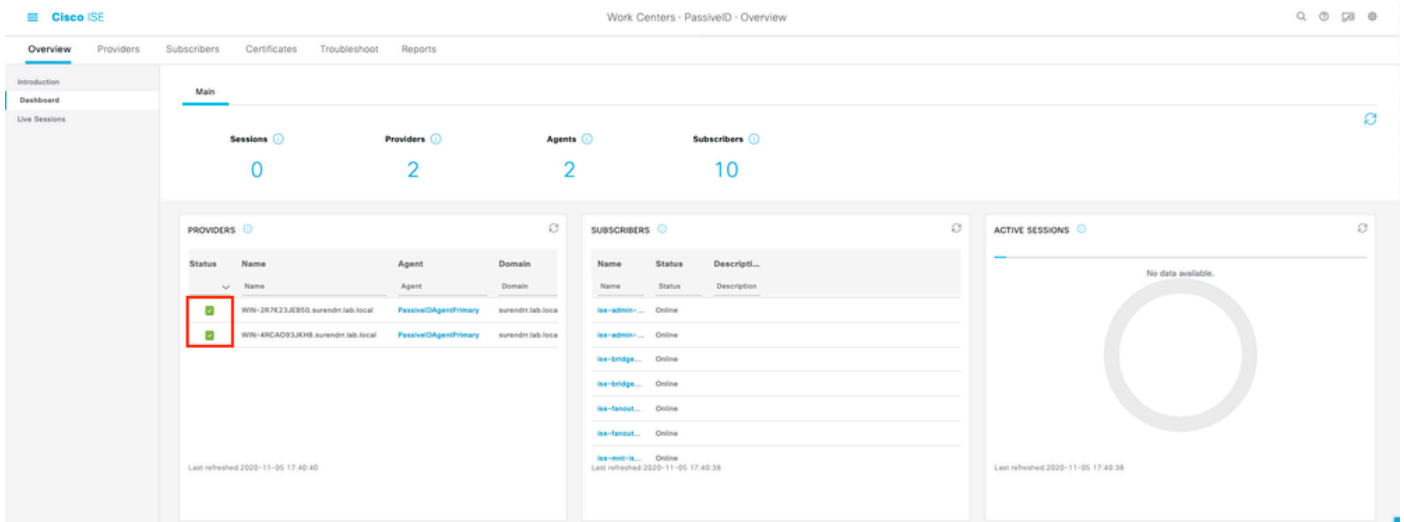
Below the connection details is a table of ISE nodes:

ISE Node	ISE Node R...	Status	Domain Controller	Site
ISE3LAB1.suendr.lab.local	PRIMARY	Operational	WIN-257X21J950.suendr.l...	Default-Frai-Site-Name
ISE3LAB2.suendr.lab.local	SECONDARY	Operational	WIN-4KCA093JRH8.suendr.l...	Default-Frai-Site-Name

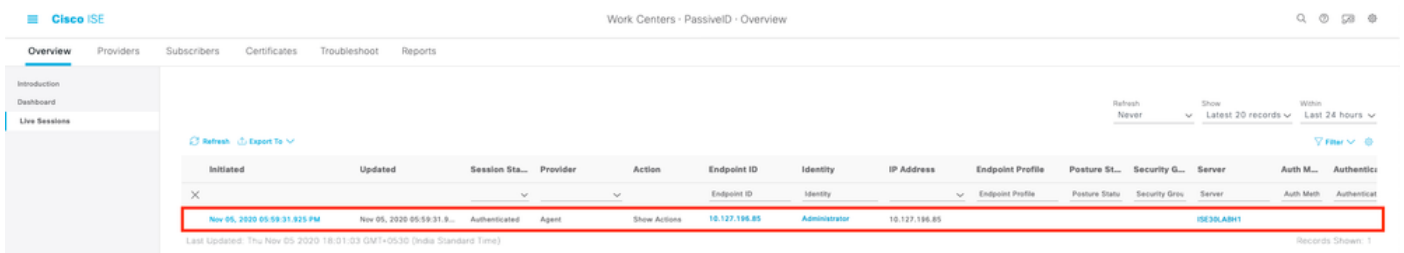
3. Verificare se i controller di dominio richiesti sono controllati dall'agente in Centri di lavoro > ID passivo > Provider > Active Directory > ID passivo.



4. Verificare se lo stato dei controller di dominio monitorati è attivo. Ad esempio, contrassegnato in verde sul dashboard in Centri di lavoro > ID passivo > Panoramica > Dashboard.



5. Verificare che le sessioni attive vengano popolate quando viene registrato un accesso Windows nel controller di dominio in Centri di lavoro > ID passivo > Panoramica > Sessioni attive.



Verifica servizi agente su Windows Server

1. Verificare il servizio ISEPICAgent sul server in cui è installato l'agente PIC.

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\$SQLEXPRESS	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](#)

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).