Configura agente ID passivo motore Identity Services basato su EVT

Sommario

Introduzione

Questo documento descrive il nuovo agente ISE Passive Identity Connector (ISE-PIC) introdotto nella versione ISE 3.0, i suoi vantaggi e la configurazione di questo agente sull'ISE. ISE Passive Identity Agent è diventato parte integrante della soluzione Identity Firewall utilizzando anche Cisco FirePower Management Center.

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.

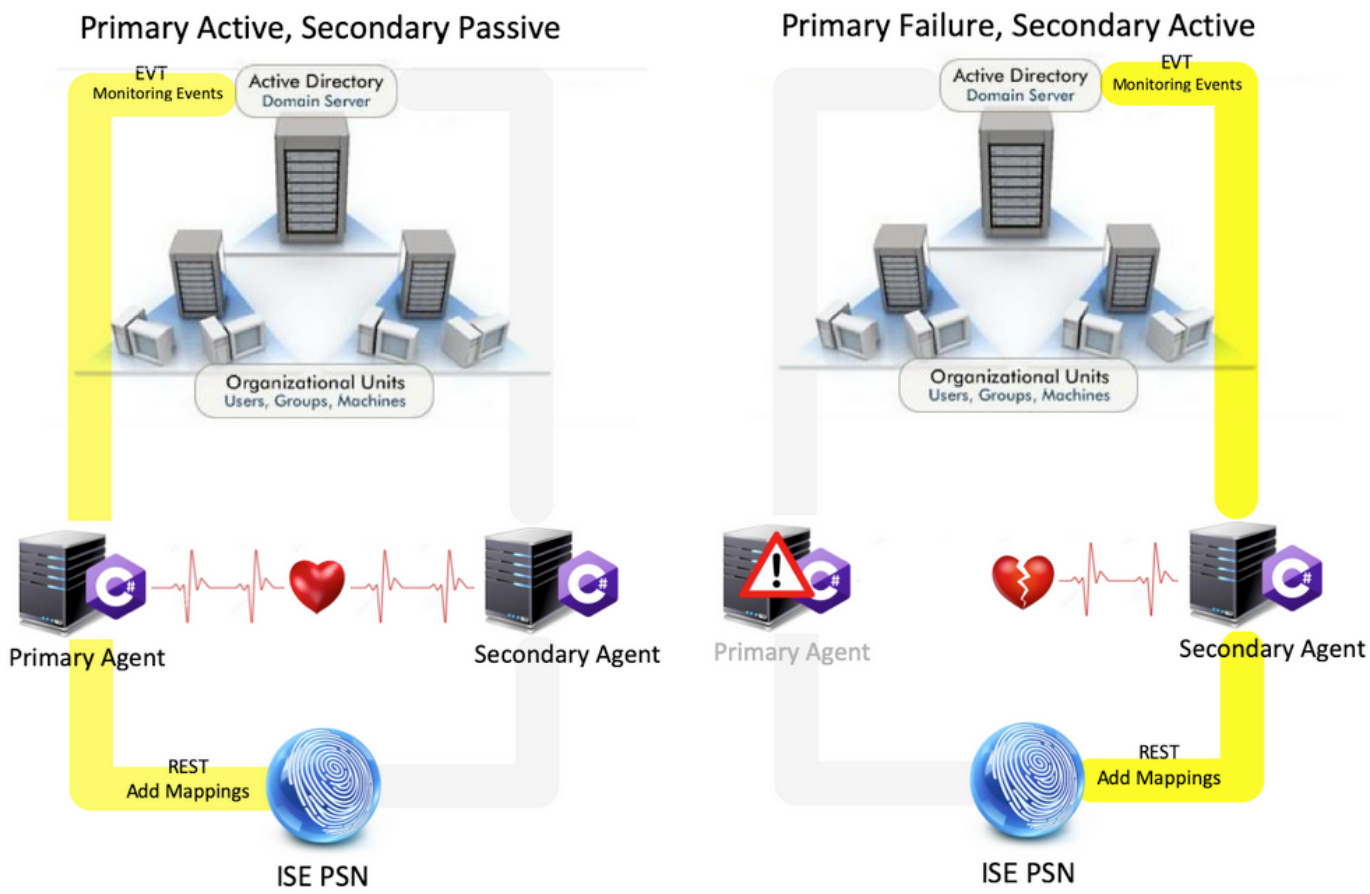
Necessità di un nuovo protocollo

La funzione di identità passiva (ID passivo) di ISE guida una serie di importanti scenari di utilizzo, tra cui Identity-Based Firewall, EasyConnect, ecc. Questa funzionalità dipende dalla possibilità di monitorare gli utenti che accedono ai controller di dominio Active Directory e di apprenderne 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 o API di gestione eventi, 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 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 perdere dati durante questo periodo. Questa è una delle principali preoccupazioni relative all'uso di ISE PIC Agent prima di questa release. ISE utilizza la porta UDP 9095 per lo scambio di heartbeat tra gli agenti.

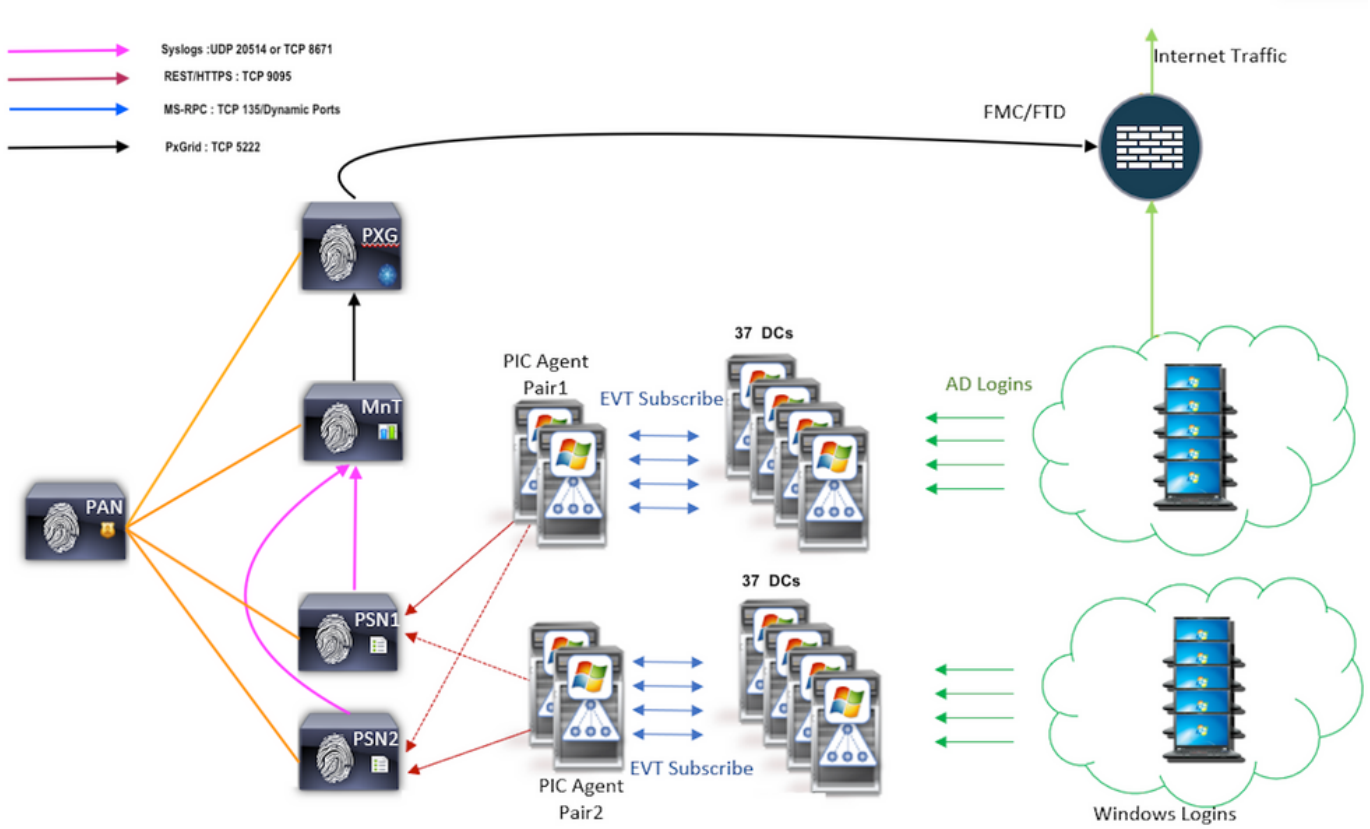


Scalabilità

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. Ecco 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 storici

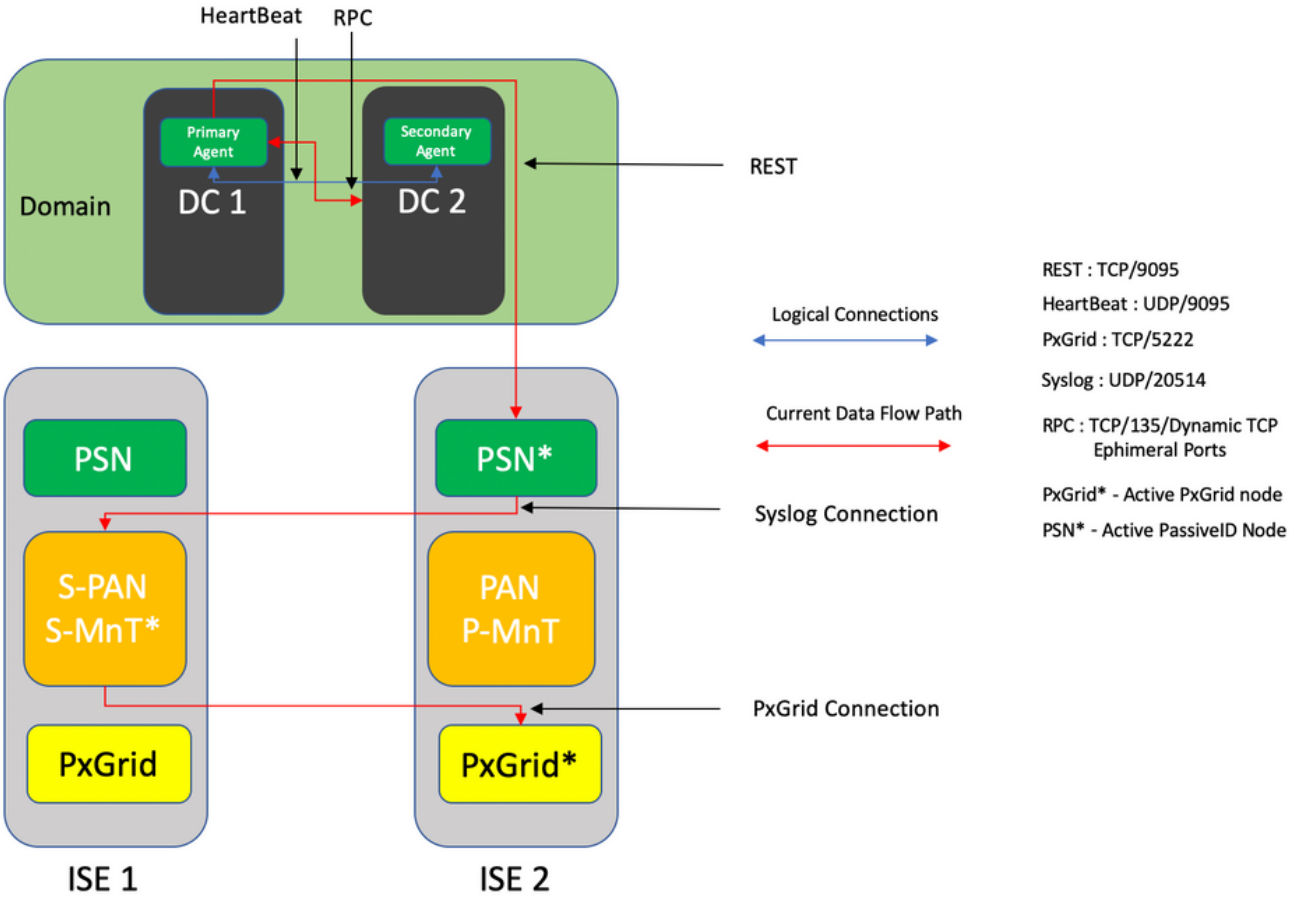
In caso di failover o in caso di riavvio del servizio per l'agente PIC, per assicurarsi che non vengano persi dati, gli eventi generati per il periodo di tempo passato vengono interrogati e inviati nuovamente ai nodi PSN. Per impostazione predefinita, ISE richiede 60 secondi di eventi passati dall'avvio 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 un numero di risorse così elevato come WMI. I test di scala hanno dimostrato che le prestazioni delle query con l'utilizzo dell'EVT sono notevolmente migliorate.

Configurazione

Diagramma connettività

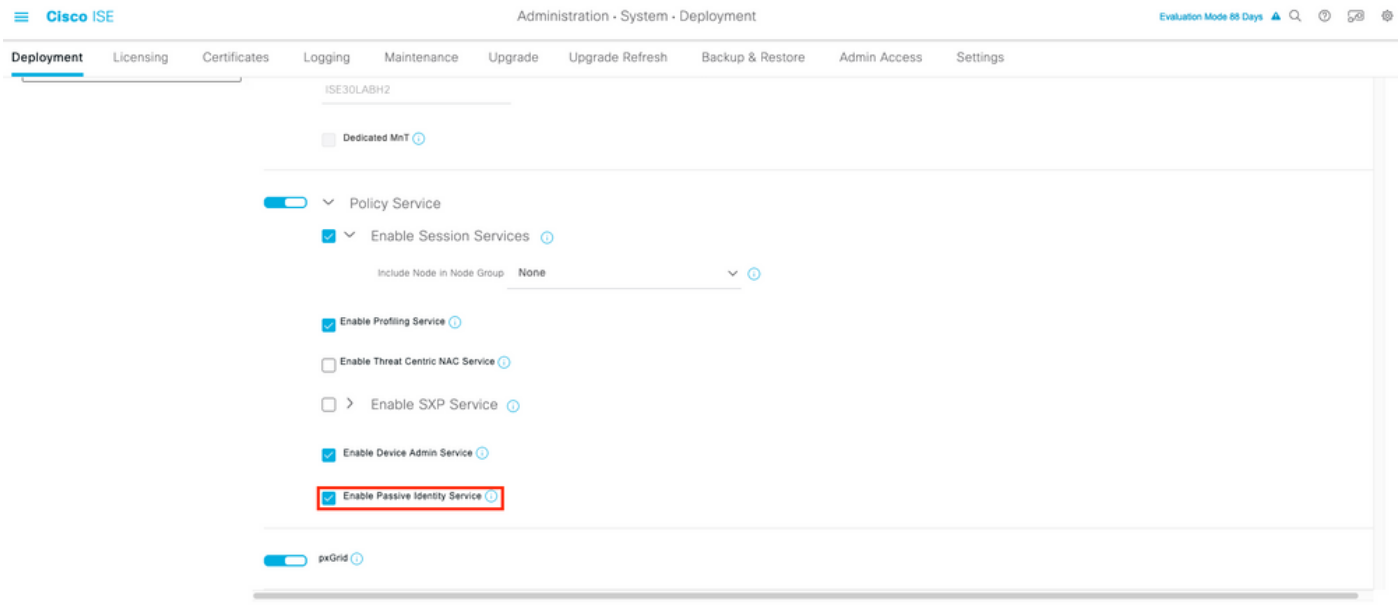


Configurazioni

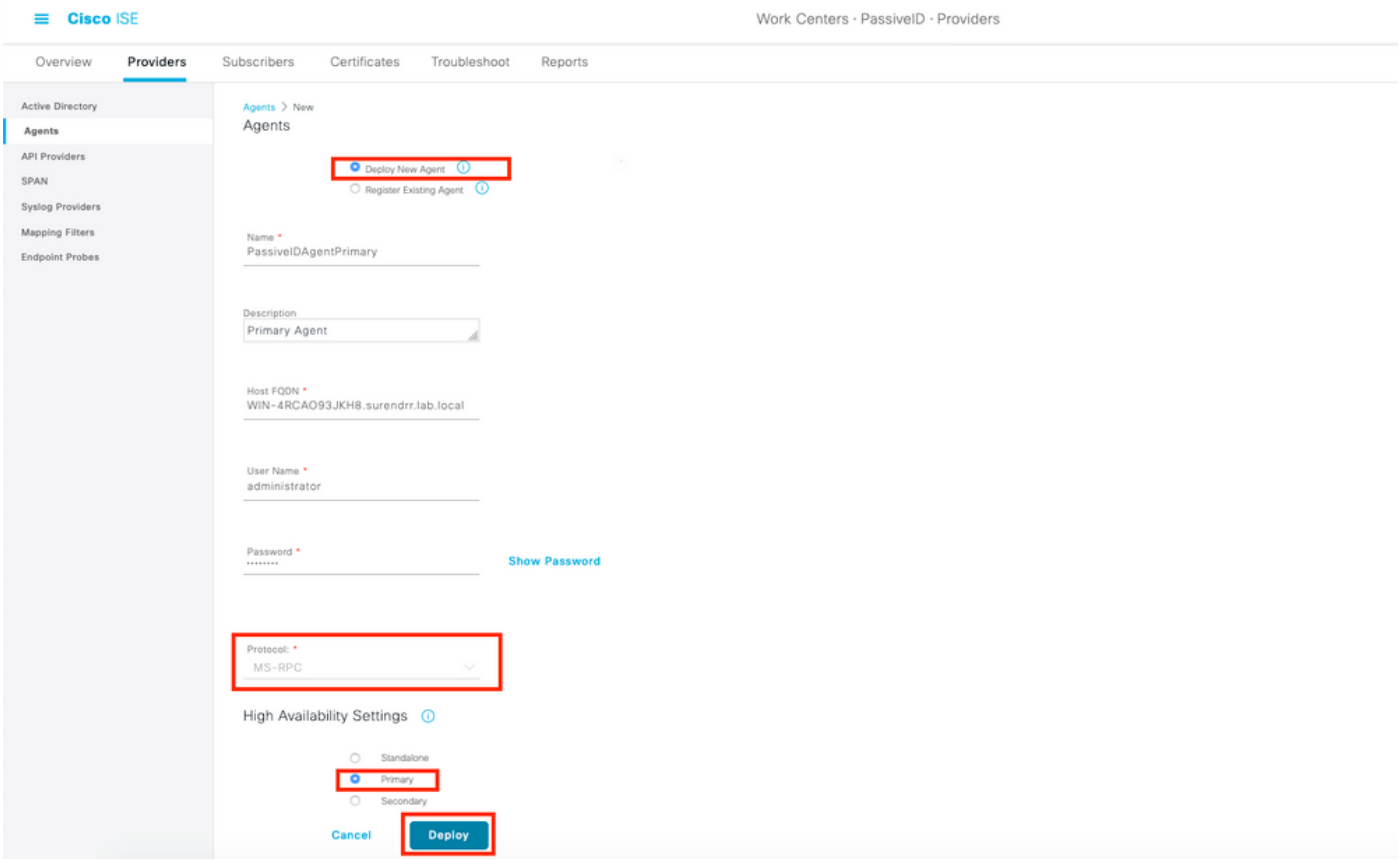
Configurazione di ISE per l'agente PassiveID

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:



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

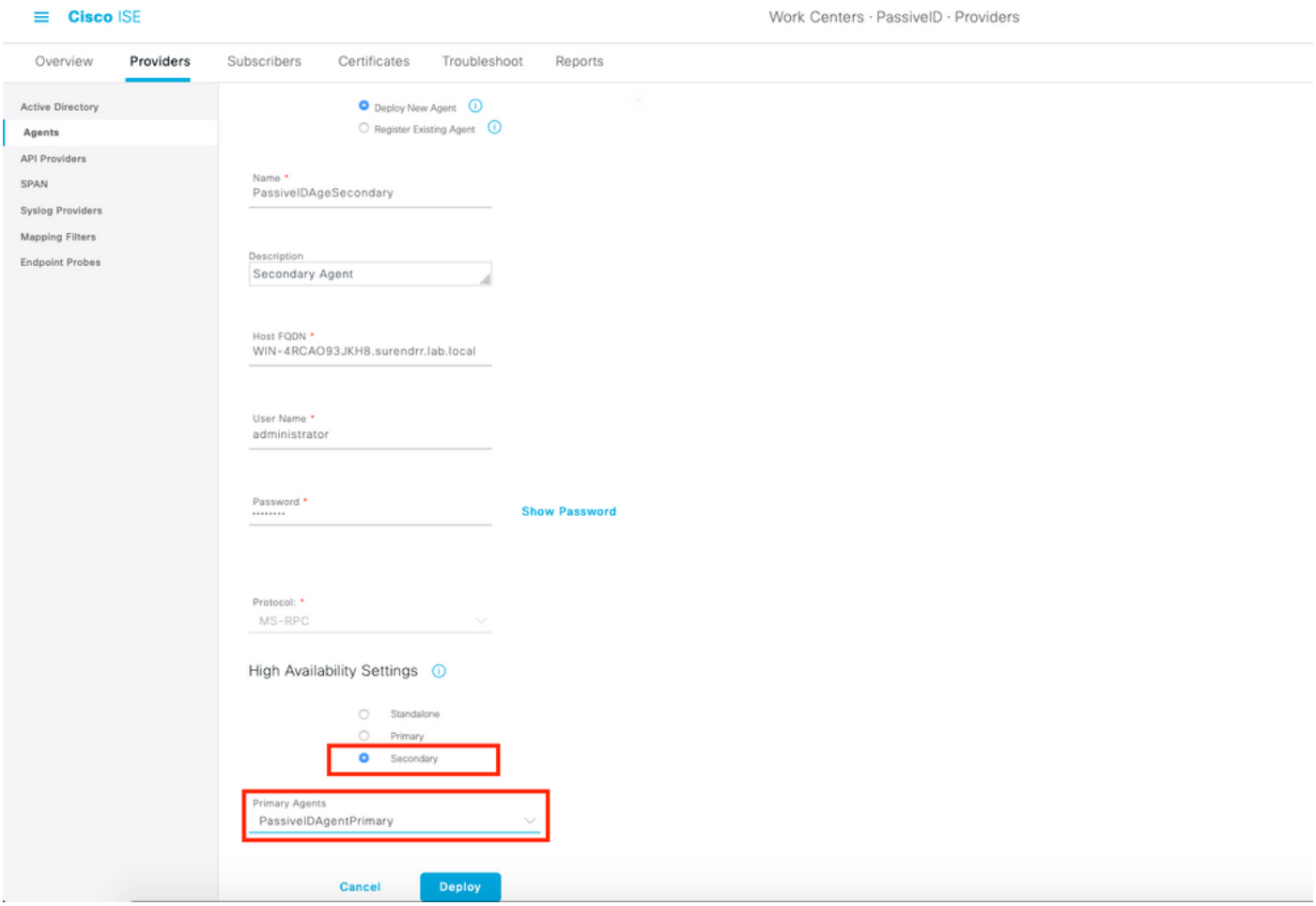


Nota: 1. Se l'agente deve essere installato da ISE sul controller di dominio, l'account utilizzato deve disporre di privilegi sufficienti per installare un programma ed eseguirlo sul server indicato nel campo FQDN host. L'FQDN host può essere quello di un server membro anziché di un controller di dominio.

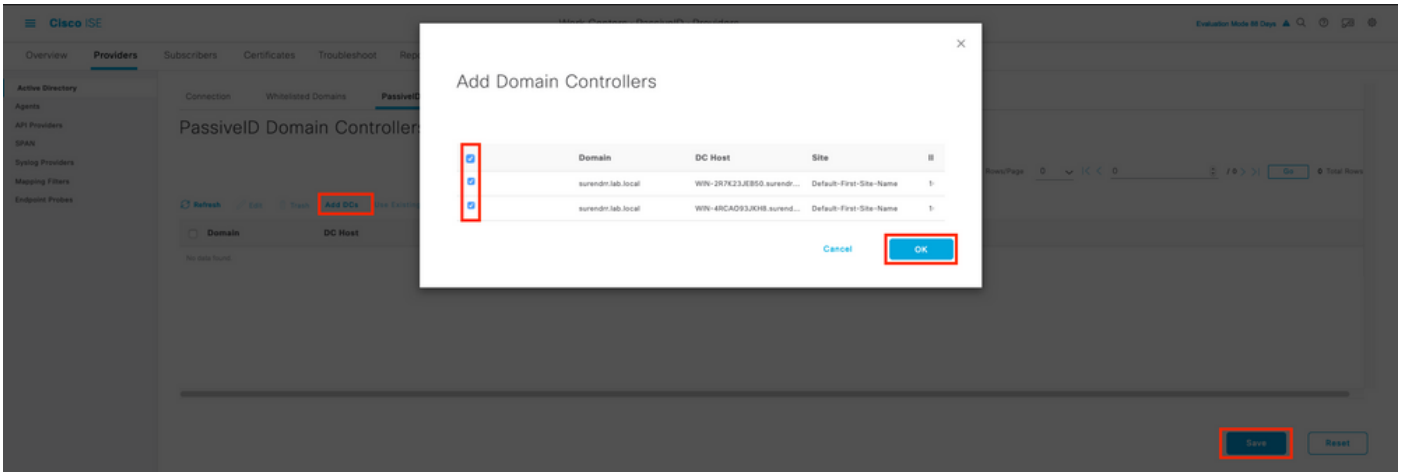
2. Se un agente è già installato manualmente o da una precedente distribuzione ISE, con MSRPC, le autorizzazioni e le configurazioni necessarie sul lato Active Directory o Windows sono inferiori rispetto a WMI, l'altro protocollo (e l'unico disponibile prima della 3.0) utilizzato dagli agenti PIC. L'account 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.

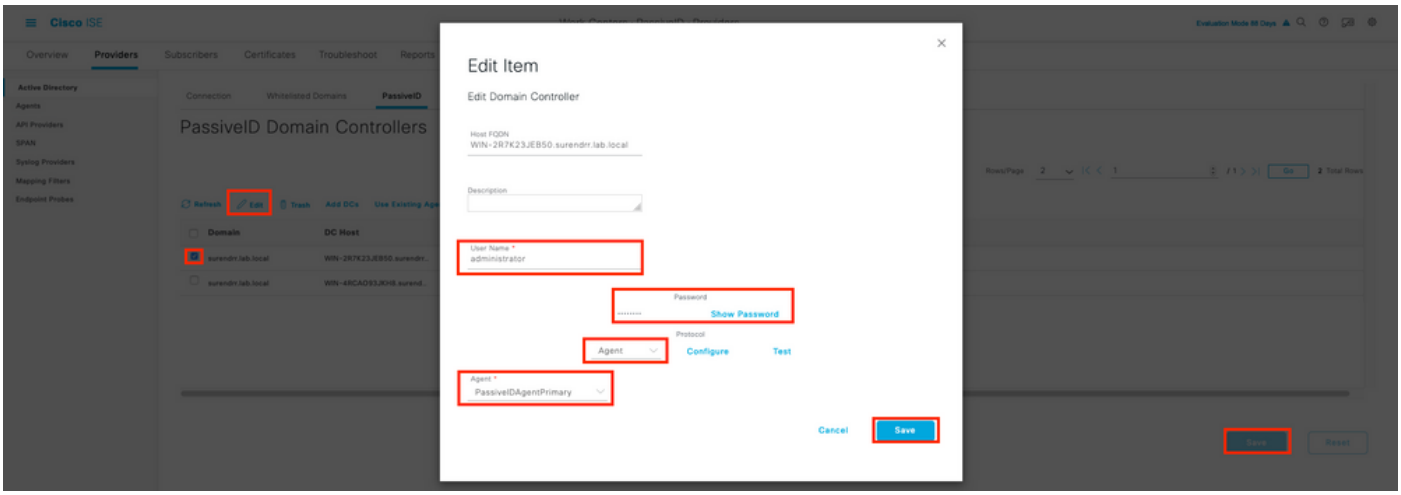
Al termine di una distribuzione corretta, configurare un altro agente su un server diverso e aggiungerlo come agente secondario e quindi come peer primario, come illustrato in questa immagine.



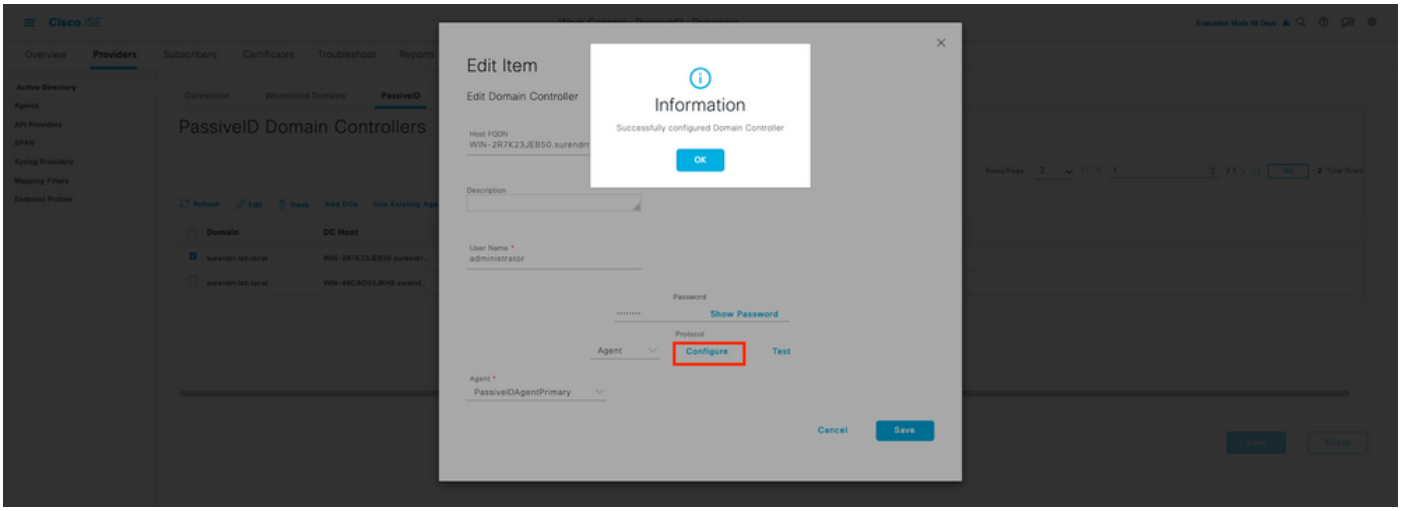
Per monitorare i controller di dominio tramite gli agenti, selezionare **Centri di lavoro > ID passivo > Provider > Active Directory > [Fare clic sul punto di join] > ID passivo** . Fare clic su **Add DCs** (Aggiungi controller di dominio) e scegliere i controller di dominio da cui recuperare gli eventi/mapping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

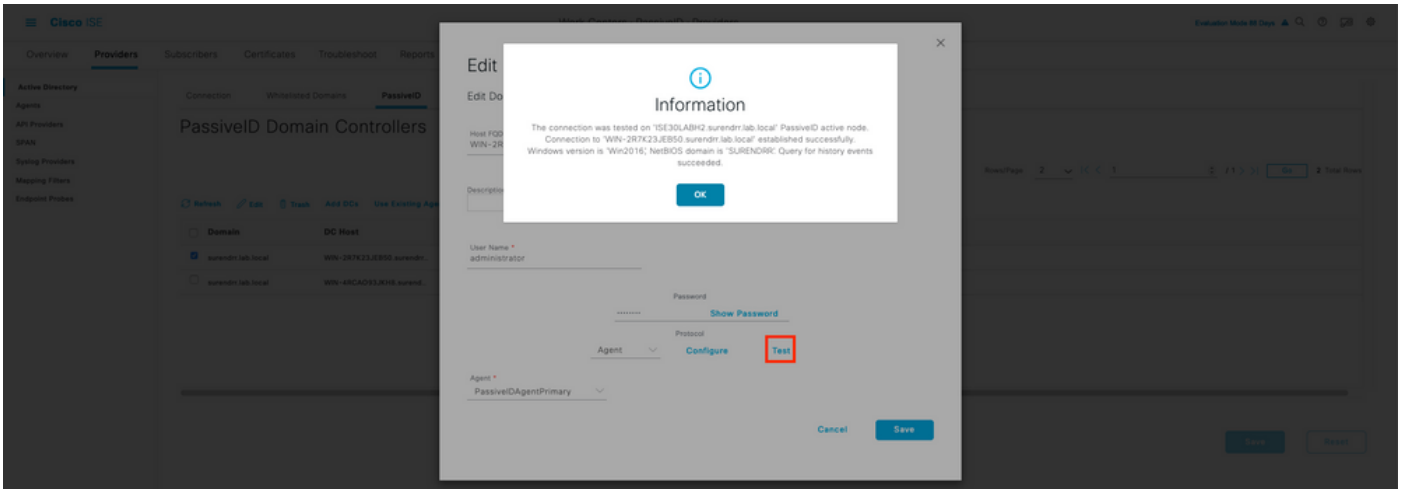


Per specificare gli agenti da utilizzare per recuperare gli eventi da, selezionare **Centri di lavoro > ID passivo > Provider > Active Directory > [Fare clic sul punto di join] > ID passivo. Scegliere i controller di dominio e fare clic su Modifica**. Immettere il *nome utente* e la *password*. Scegliere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



Èpossibile verificare la corretta applicazione della configurazione utilizzando i pulsanti **Configure** e **Test**, come mostrato nelle immagini seguenti:





Informazioni sul file di configurazione di PassiveID Agent

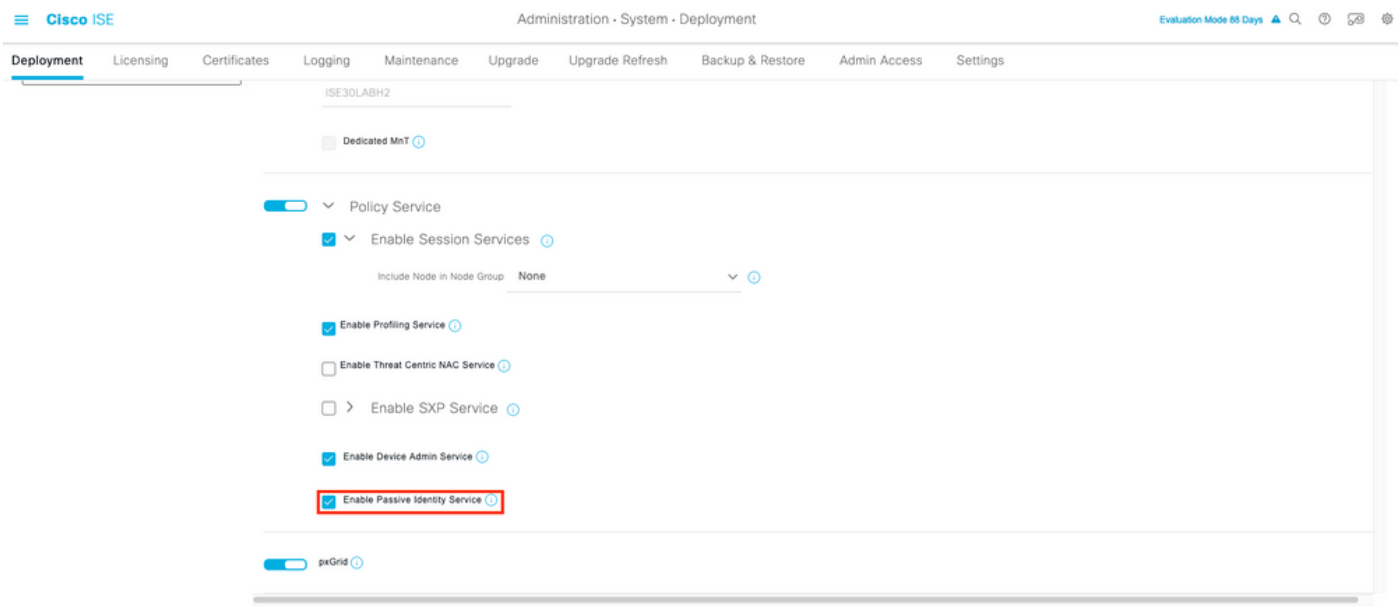
Il file di configurazione dell'agente PassiveID si trova in **C:\Program Files (x86)\Cisco\Cisco ISE**

PassiveID Agent\PICAgent.exe.config . Il contenuto del file di configurazione è indicato di seguito:

Verifica

Verifica dei servizi PassiveID sull'ISE

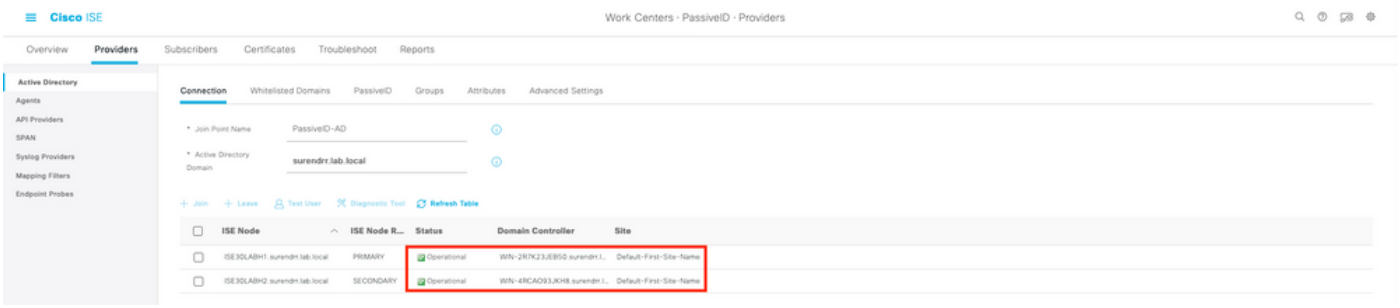
1. Verificare che il servizio PassiveID sia abilitato sulla GUI e sia anche contrassegnato come in esecuzione dal comando **show application status ise** sulla CLI di ISE.



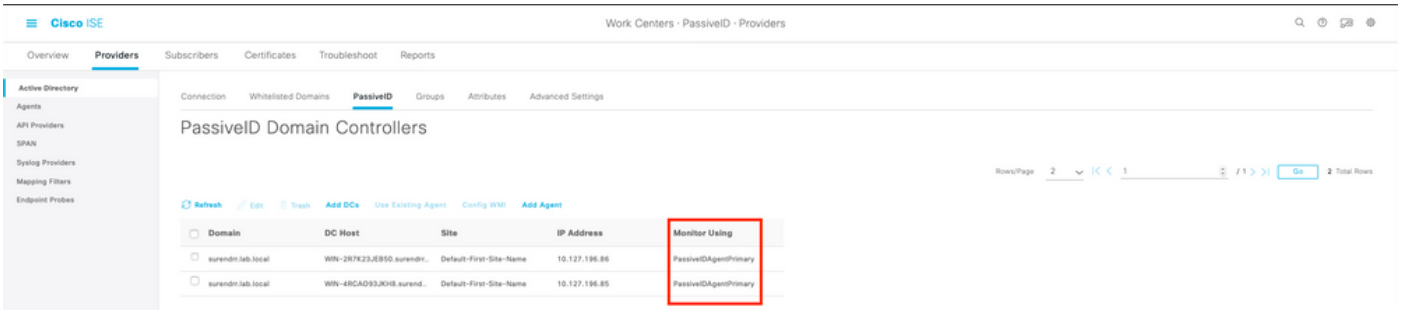

```
ISE PROCESS NAME STATE PROCESS ID
--------------------------------------------------------------------
Database Listener running 129052
Database Server running 108 PROCESSES
Application Server running 9830
Profiler Database running 5127
ISE Indexing Engine running 13361
AD Connector running 20609
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
```

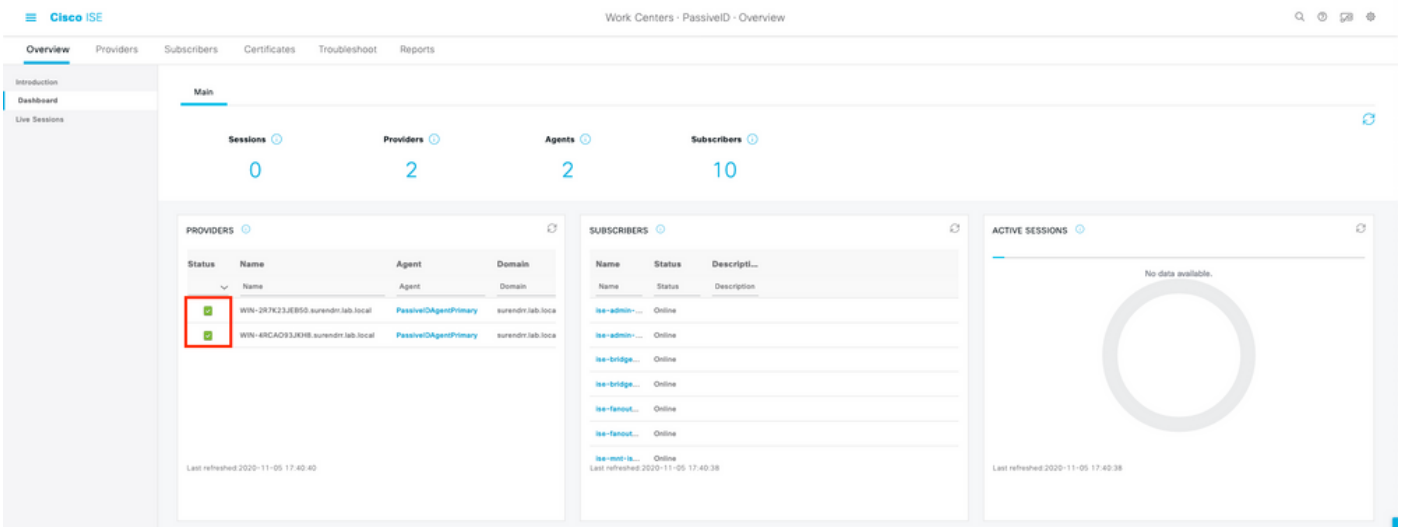
2. Verificare se il provider ISE Active Directory è connesso ai controller di dominio nei **centri di lavoro > ID passivo > Provider > Active Directory > Connessione**.



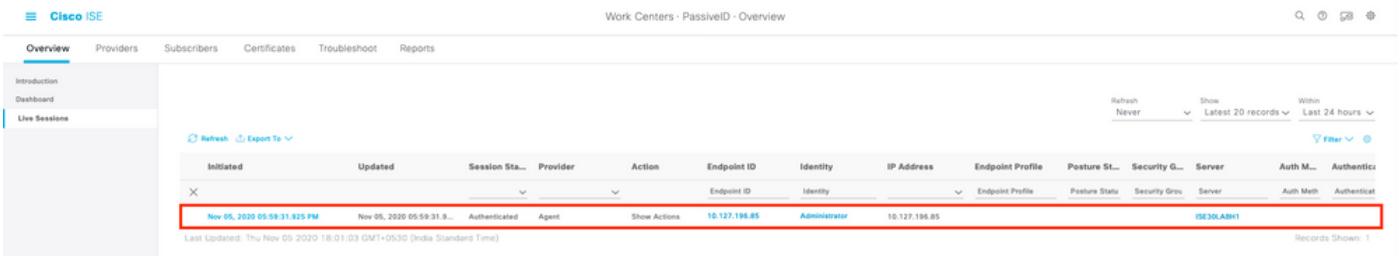
3. Verificare se i controller di dominio richiesti sono controllati dall'**agente in Centri di lavoro > ID passivo > Provider > Active Directory > ID passivo**.



4. Verificare se lo stato dei controller di dominio monitorati è attivo, ovvero 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.