Configuration de l'agent d'ID passif du moteur Identity Services Engine basé sur EVT

Table des matières

- Introduction
- Conditions préalables
  - Exigences
  - Composants utilisés
- Informations générales
- Nécessité d'un nouveau protocole
  - Avantages de l'utilisation de MS-EVEN6
    - Haute disponibilité
    - Évolutivité
    - Architecture de configuration de test évolutif
    - Requête Événements historiques
    - Moins de frais de traitement
- Configurer
  - Diagramme de connectivité
  - Configurations
    - Configurer ISE pour l'agent PassiveID
    - Comprendre le fichier de configuration de PassiveID Agent
- Vérifier
  - Vérification des services PassiveID sur l'ISE
  - Vérification des services d'agent sur le serveur Windows
  - Paramètres requis au niveau du domaine Windows AD - Objets de stratégie de groupe

Introduction

Ce document décrit le nouvel agent ISE (Identity Services Engine) Passive Identity Connector (ISE-PIC) introduit dans la version ISE 3.0.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Administration des services d'identité Cisco
- MS-RPC, protocoles WMI
- Administration Active Directory

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Cisco Identity Services Engine version 3.0 et ultérieure
- Microsoft Windows Server 2016 Standard

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Informations générales

Cet article décrit également les avantages de l'agent ISE-PIC et la configuration de cet agent sur l'ISE. ISE Passive Identity Agent fait désormais partie intégrante de la solution Identity Firewall qui utilise également Cisco FirePower Management Center.

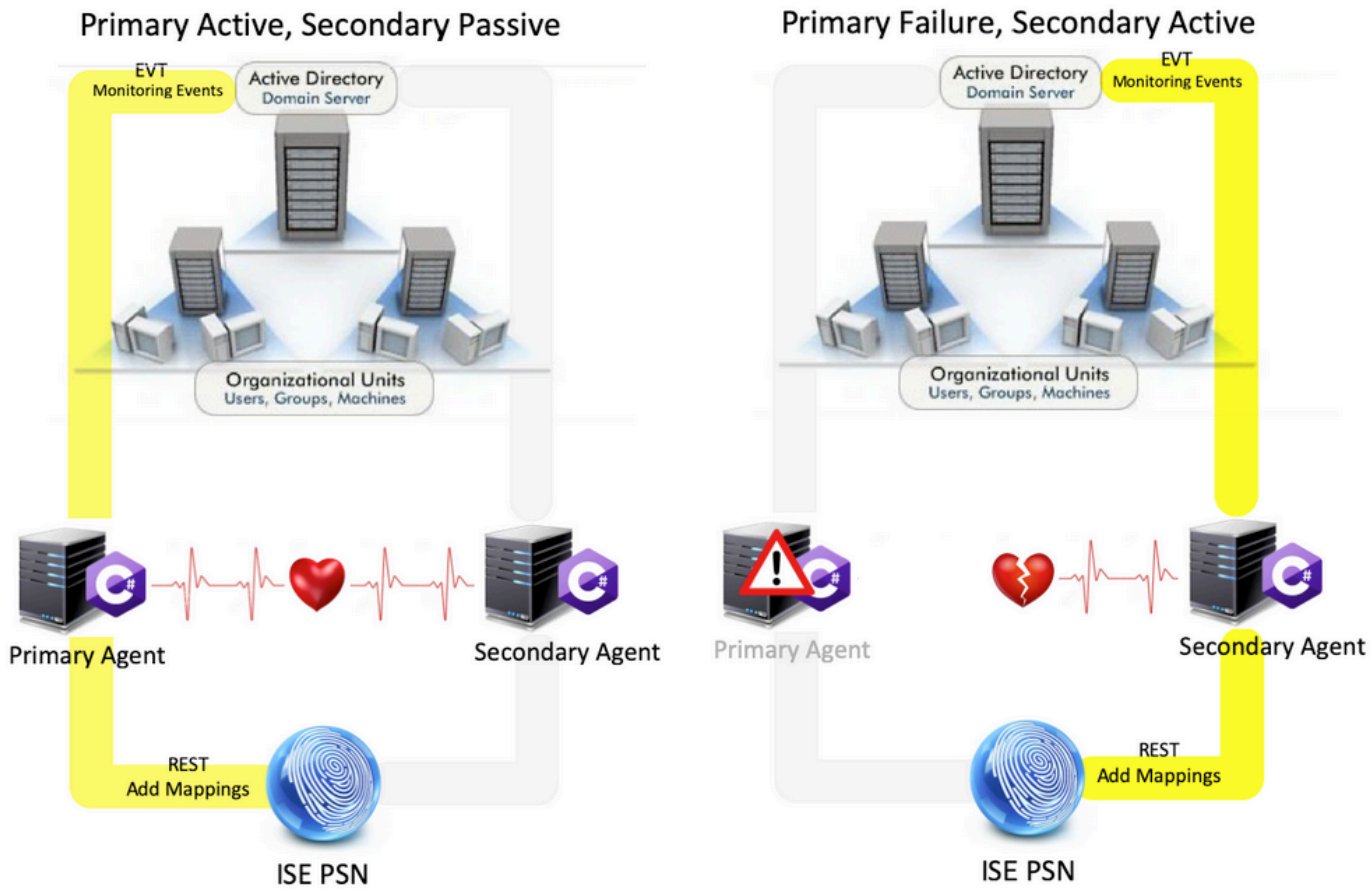
Nécessité d'un nouveau protocole

La fonctionnalité d'identité passive (ID passif) d'ISE présente un certain nombre de cas d'utilisation importants, notamment le pare-feu basé sur l'identité, EasyConnect, etc. Cette fonctionnalité dépend de la capacité à surveiller les utilisateurs qui se connectent aux contrôleurs de domaine Active Directory et à connaître leur nom d'utilisateur et leur adresse IP. Le principal protocole actuellement utilisé pour surveiller les contrôleurs de domaine est WMI. Cependant, il est difficile/invasif à configurer, a un impact sur les performances des clients et des serveurs, et a parfois une latence extrêmement importante pour voir les événements d'ouverture de session dans les déploiements à grande échelle. Après des recherches approfondies et d'autres moyens d'interroger les informations requises pour les services d'identité passifs, un protocole alternatif - connu sous le nom d'API d'évènement (EVT), qui est plus efficace dans la gestion de ce cas d'utilisation a été décidé. Il est parfois appelé MS-EVEN6, également connu sous le nom de protocole distant d'évènements, qui est le protocole RPC sous-jacent basé sur le câble.

Avantages de l'utilisation de MS-EVEN6

Haute disponibilité

L'agent d'origine n'avait pas d'option de haute disponibilité (HA) et s'il est nécessaire d'effectuer la maintenance sur le serveur sur lequel l'agent était en cours d'exécution ou a subi une panne, les événements de connexion seraient manqués et des fonctionnalités telles que le pare-feu basé sur l'identité verraient une perte de données pendant cette période. C'était l'une des principales préoccupations concernant l'utilisation de l'agent ISE PIC avant cette version. À partir de cette version, les agents peuvent travailler en haute disponibilité. ISE utilise le port UDP 9095 pour échanger des pulsations entre les agents afin de garantir la haute disponibilité. Plusieurs paires d'agents haute disponibilité peuvent être configurées pour surveiller différents contrôleurs de domaine.

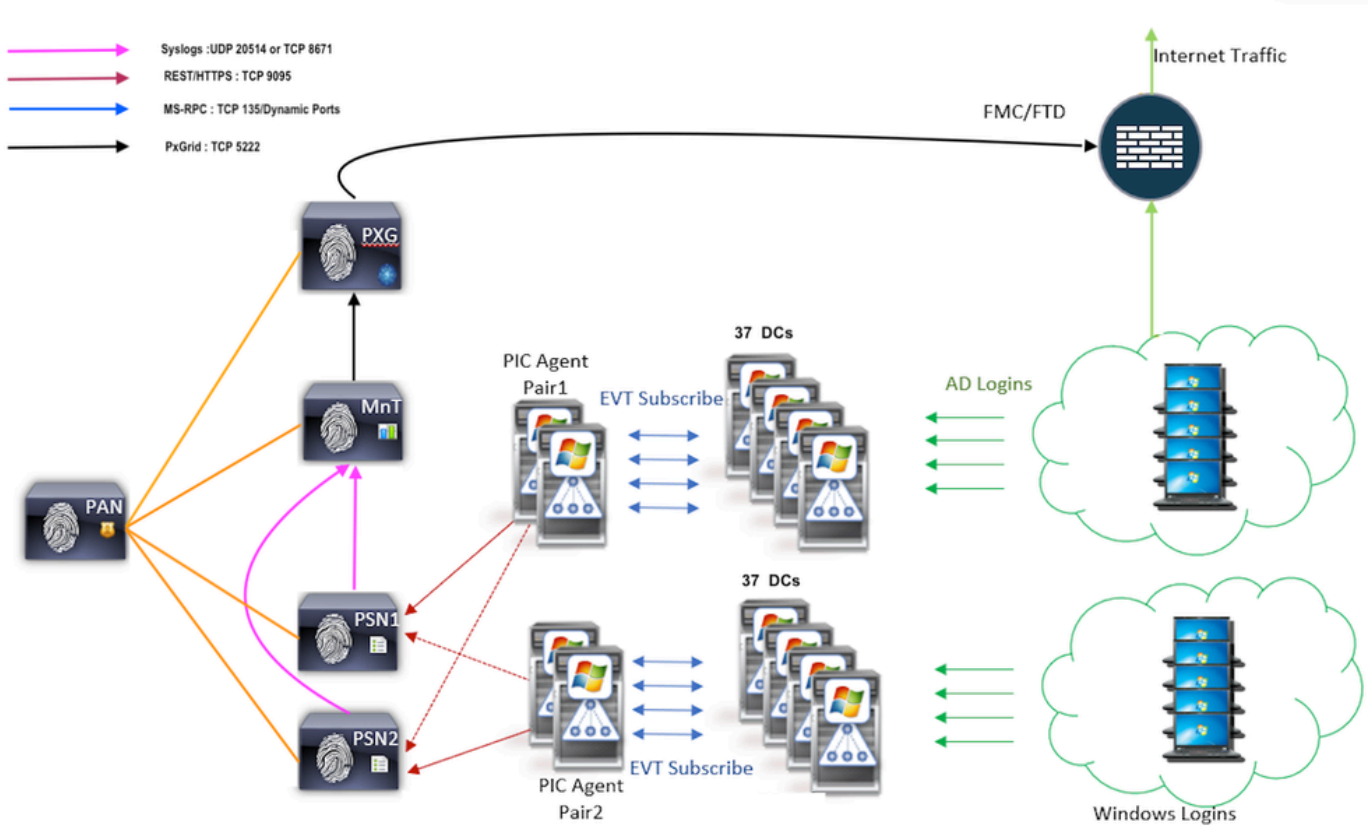


Évolutivité

Le nouvel agent offre une meilleure prise en charge avec des numéros d'échelle accrus pour un nombre de contrôleurs de domaine pris en charge et le nombre d'événements qu'il peut gérer. Voici les numéros d'échelle testés :

- Nombre maximal de contrôleurs de domaine surveillés (avec 2 paires d'agents) : 74
- Nombre maximal de mappages/événements testés : 292 000 (3 950 événements par data center)
- Nombre maximal de TPS testées : 500

Architecture de configuration de test évolutif



Requête Événements historiques

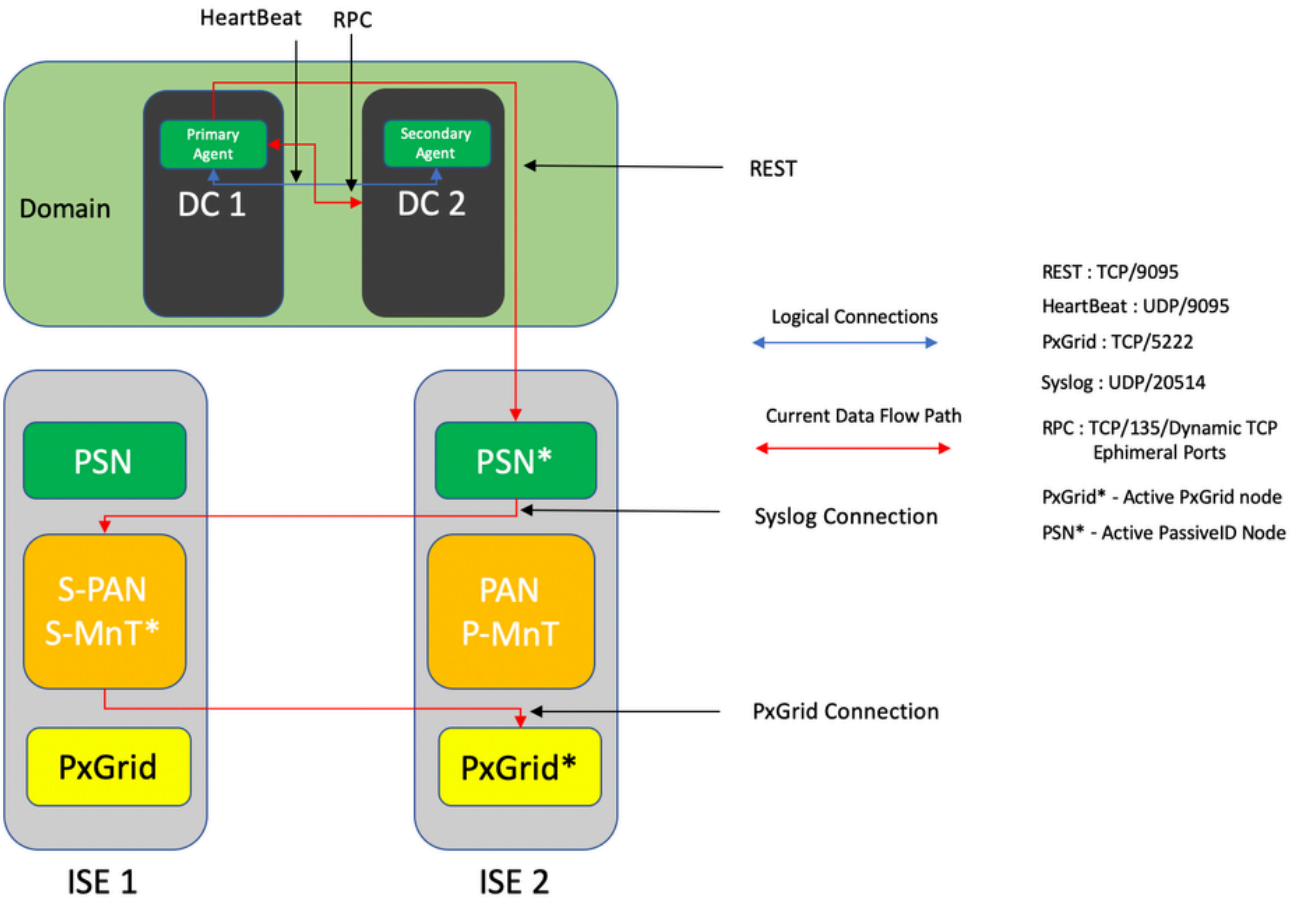
En cas de basculement, ou si un redémarrage de service est effectué pour le PIC-Agent, afin de s'assurer qu'aucune donnée n'est perdue, les événements qui sont générés dans le passé pendant une durée configurée sont interrogés et envoyés à nouveau aux noeuds PSN. Par défaut, 60 secondes d'événements passés depuis le début du service sont interrogées par l'ISE pour annuler toute perte de données pendant la perte de service.

Moins de frais de traitement

Contrairement à WMI, qui sollicite énormément le processeur à grande échelle ou à forte charge, EVT ne consomme pas autant de ressources que WMI. Les tests d'échelle ont montré une performance nettement améliorée des requêtes avec l'utilisation de l'EVT.

Configurer

Diagramme de connectivité

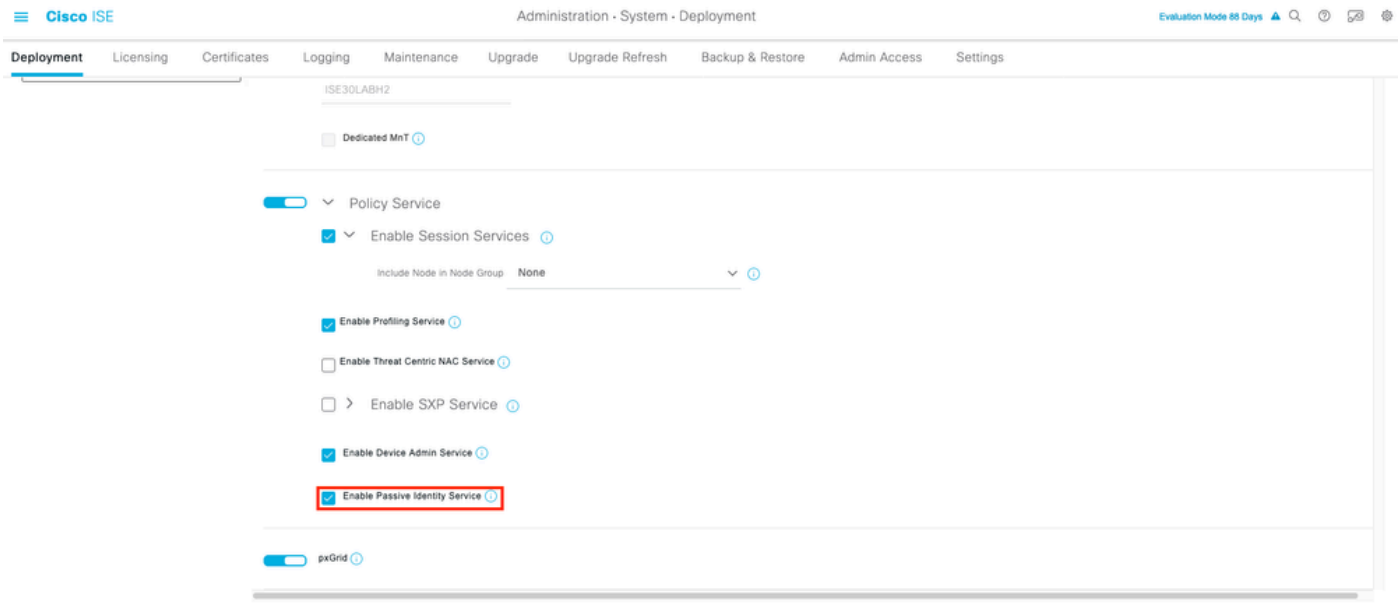


Configurations

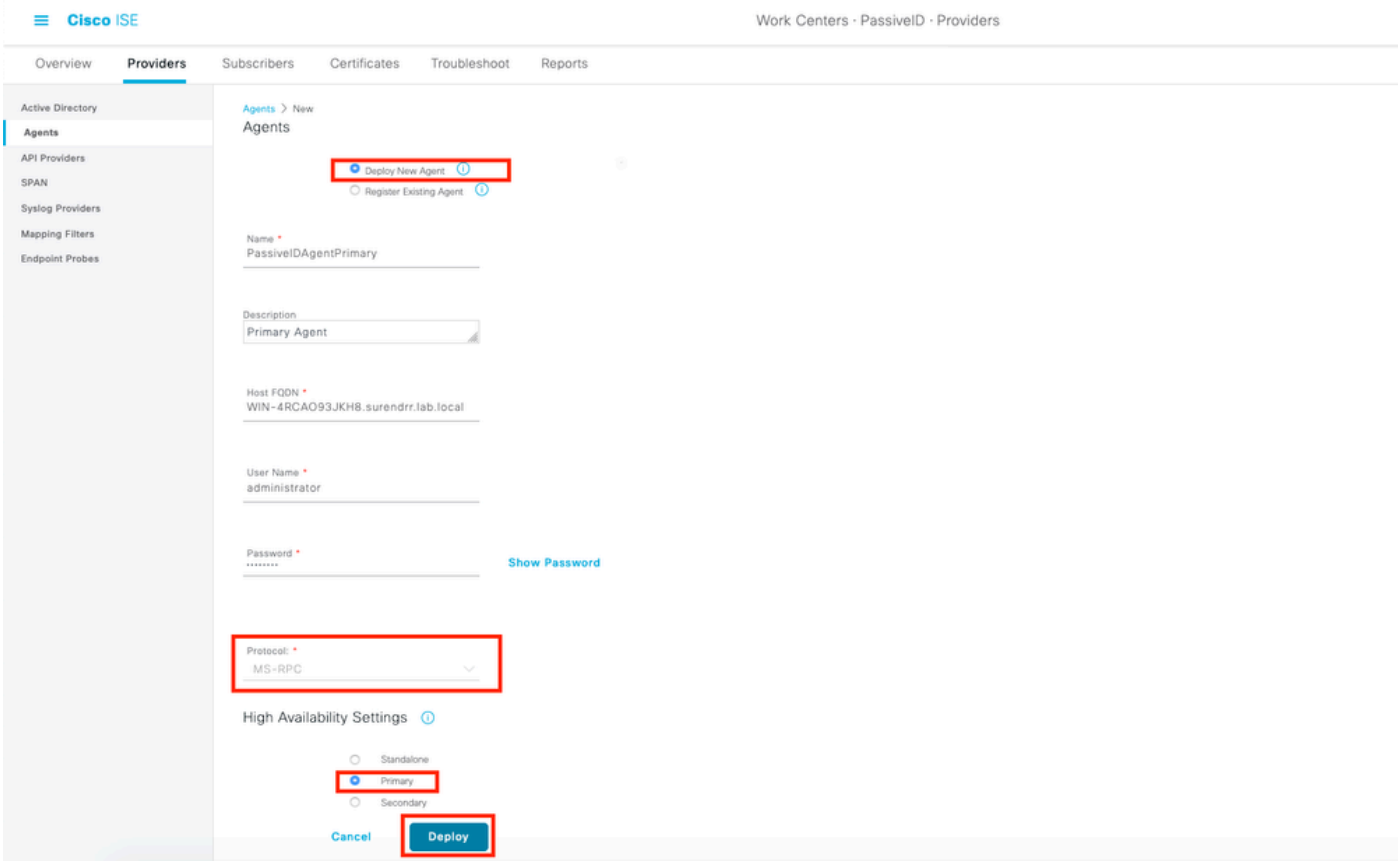
Configurer ISE pour l'agent PassiveID

Afin de configurer les services PassiveID, vous devez avoir activé les services d'identité passive sur au moins un noeud de service de stratégie (PSN). Un maximum de deux noeuds peuvent être utilisés pour les services d'identité passifs qui fonctionnent en mode actif/veille. ISE doit également être joint à un domaine Active Directory et seuls les contrôleurs de domaine présents dans ce domaine peuvent être surveillés par des agents configurés sur ISE. Afin de joindre ISE à un domaine Active Directory, référez-vous au Guide d'intégration d'Active Directory.

Accédez à Administration > System > Deployment > [Choisir un PSN] > Edit pour activer les services d'identité passifs comme indiqué ici :



Accédez à Work Centers > PassiveID > Providers > Agents > Add pour déployer un nouvel agent comme indiqué ici :

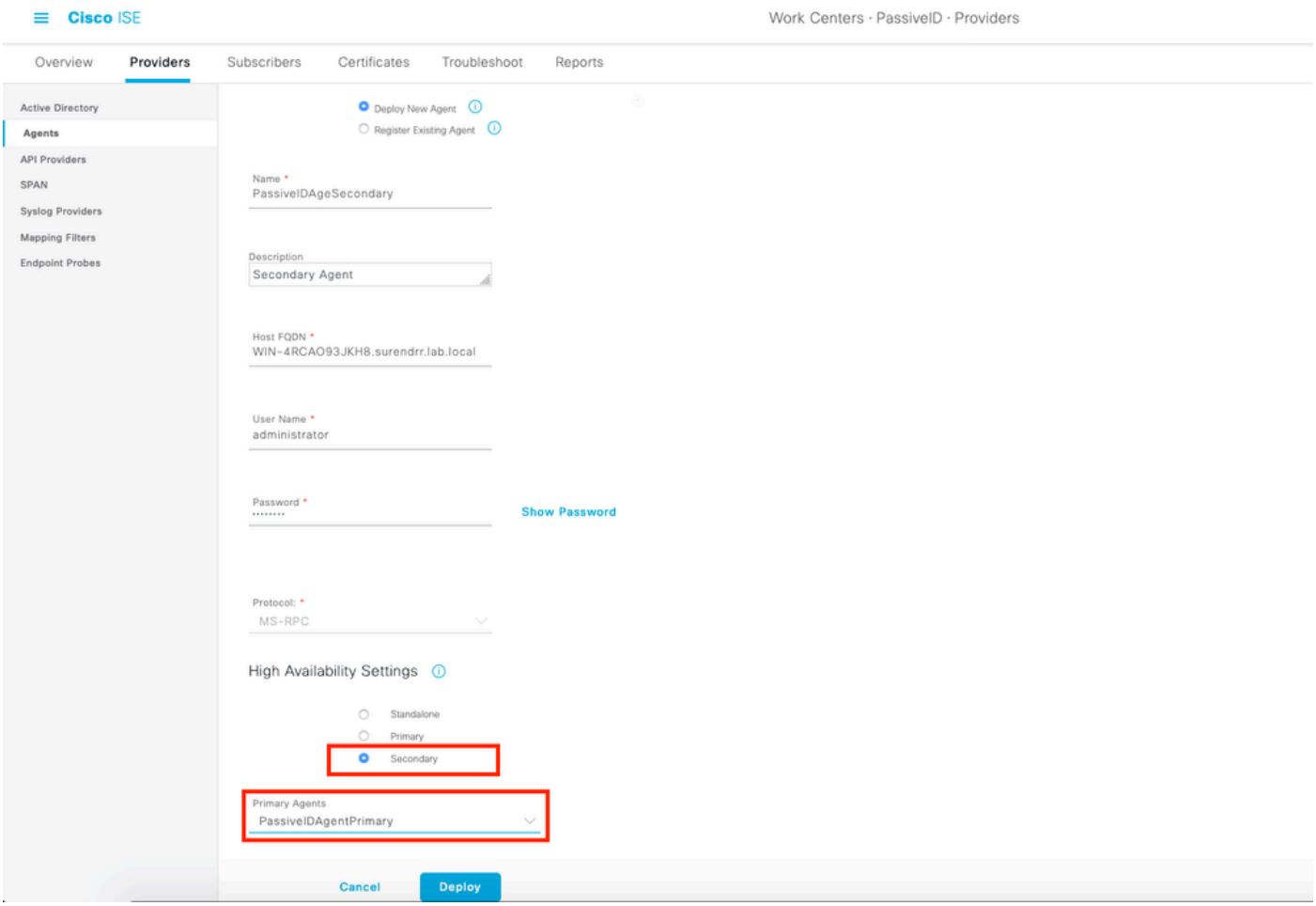


Remarque : 1. Si l'agent doit être installé par ISE sur le contrôleur de domaine, le compte utilisé ici doit disposer de privilèges suffisants pour installer un programme et l'exécuter sur le serveur mentionné dans le champ Nom de domaine complet de l'hôte (FQDN). Le nom de domaine complet de l'hôte peut être celui d'un serveur membre plutôt que celui d'un

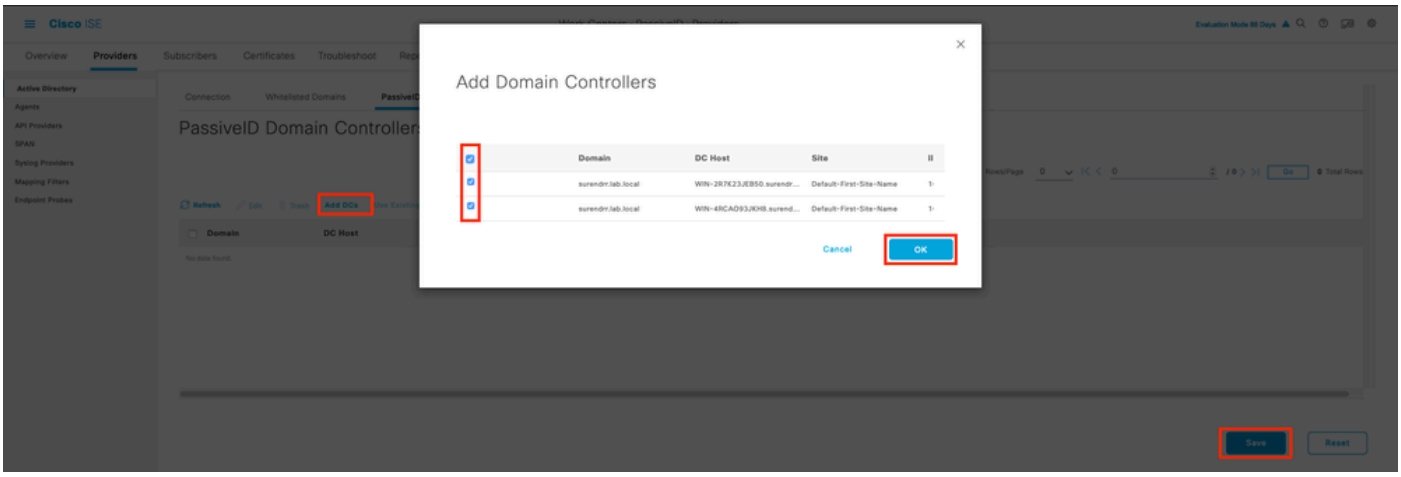
contrôleur de domaine.

2. Si un agent est déjà installé manuellement, ou à partir d'un déploiement précédent de l'ISE, avec MSRPC, les autorisations et configurations requises côté Active Directory ou Windows sont moins nombreuses que WMI, l'autre protocole (et le seul disponible avant la version 3.0) utilisé par les agents PIC. Le compte d'utilisateur utilisé dans ce cas peut être un compte de domaine normal qui fait partie du groupe Lecteurs du journal des événements. Choisissez Register Existing Agent et utilisez ces détails de compte pour enregistrer l'agent qui est installé manuellement sur les contrôleurs de domaine.

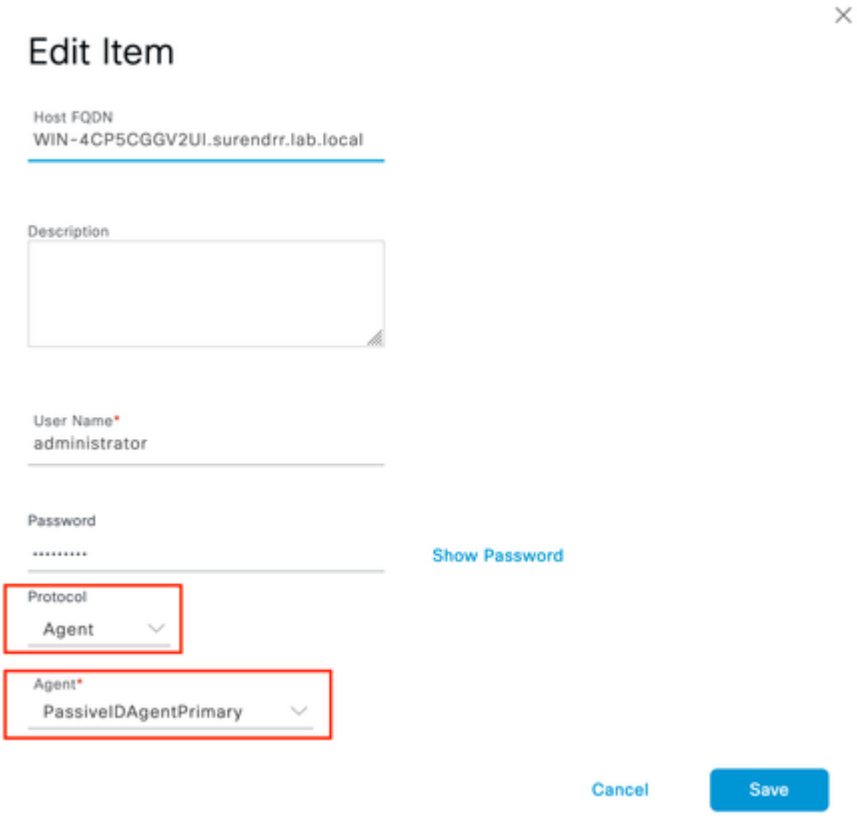
Après un déploiement réussi, configurez un autre agent sur un autre serveur et ajoutez-le en tant qu'agent secondaire, puis en tant qu'homologue principal, comme illustré dans cette image.



Afin de surveiller les contrôleurs de domaine qui utilisent les agents, naviguez vers Work Centers > PassiveID > Providers > Active Directory > [Cliquez sur le point de jonction] > PassiveID . Cliquez sur Add DCs et choisissez les contrôleurs de domaine à partir desquels le mappage/les événements User-IP sont récupérés, cliquez sur OK, puis cliquez sur Save pour enregistrer les modifications, comme illustré dans cette image.



Afin de spécifier les agents qui peuvent être utilisés pour récupérer les événements de, naviguez à Work Centers > PassiveID > Providers > Active Directory > [Cliquez sur le point de jonction] > PassiveID. Sélectionnez les contrôleurs de domaine et cliquez sur Modifier. Entrez un nom d'utilisateur et un mot de passe. Choisissez Agent, puis Enregistrer la boîte de dialogue. Cliquez sur Save dans l'onglet PassiveID pour terminer la configuration.



Surveillance d'un contrôleur de domaine

Remarque : Cette section peut contenir des options de configuration et de test jusqu'à la version 3.0 du patch 4.

Comprendre le fichier de configuration de PassiveID Agent

Le fichier de configuration de l'agent PassiveID se trouve à l'adresse suivante : C:\Program Files (x86)\Cisco\Cisco ISE PassiveID Agent\PICAgent.exe.config. Le contenu du fichier de configuration est le suivant :

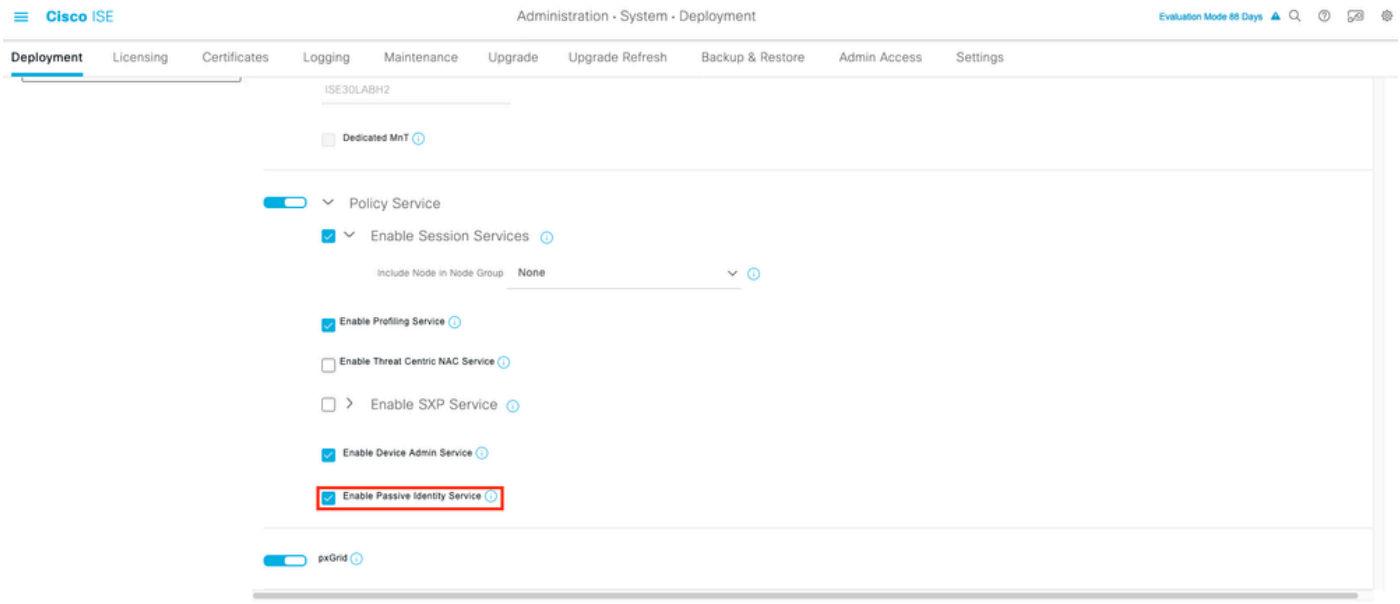
```
< ? xml version="1.0" encoding="utf-8"?>
<configuration>
<configSections>
<section name="log4net" type="log4net.Config.Log4NetConfigurationSectionHandler, log4net"/>
</configSections>
<log4net>
<racine>
<level value="DEBUG" /> <!— Niveaux de journalisation : DÉSACTIVÉ, FATAL, ERREUR, AVERTIR, INFOS, DÉBOGAGE, TOUT —>
<!— Définit le niveau des journaux collectés pour l'agent PassiveID sur le serveur sur lequel il s'exécute. —>
<appender-ref="RollingFileAppender" />
</root>
<appender name="RollingFileAppender" type="log4net.Appender.RollingFileAppender">
<file value="CiscoISEPICAgent.log" /> <!— Ne modifiez pas ce —>
<appendToFile value="true" />
<rollingStyle value="Size" />
<maxSizeRollBackups value="5" /> <!— Ce nombre définit le nombre maximal de fichiers journaux qui sont générés avant qu'ils ne soient transférés —>
<maximumFileSize value="10MB" /> <!— Définit la taille maximale de chaque fichier journal généré —>
<staticLogFileName value="true" />
<layout type="log4net.Layout.PatternLayout">
<conversionPattern value="%date %level - %message%newline" />
</layout>
</appender>
</log4net>
<démarrage>
<supportedRuntime version="v4.0"/>
<supportedRuntime version="v2.0.50727"/>
</startup>
<appSettings>
<add key="heartbeatFrequency" value="400" /> <!— Ce nombre définit la fréquence de battement du coeur en millisecondes qui s'exécute entre l'agent principal et l'agent secondaire s'il est configuré dans une paire sur l'ISE —>
<add key="heartbeatThreshold" value="1000"/> <!— Ce nombre définit la durée maximale, en millisecondes, pendant laquelle l'agent attend des pulsations, après quoi l'autre agent est déconnecté —>
```

<add key="showHeartbeats" value="false" /> <!— Remplacez la valeur par "true" pour afficher les messages de pulsation dans le fichier journal —>
<add key="maxRestThreads" value="200" /> <!— Définit le nombre maximal de threads REST pouvant être générés pour envoyer les événements à l'ISE. Ne modifiez pas cette valeur tant que le TAC Cisco ne vous le conseille pas. —>
<add key="mappingTransport" value="rest" /> <!— Définit le type de support utilisé pour envoyer les mappages à l'ISE. Ne modifiez pas cette valeur —>
<add key="maxHistorySeconds" value="60" /> <!— Définit la durée en secondes passée pendant laquelle les événements historiques doivent être récupérés en cas de redémarrage du service —>
<add key="restTimeout" value="5000" /> <!— Définit la valeur du délai d'attente pour un appel REST à l'ISE —>
<add key="showTPS" value="false" /> <!— Remplacez cette valeur par "true" pour afficher le TPS des événements reçus et envoyés à l'ISE —>
<add key="showPOSTS" value="false" /> <!— Remplacez cette valeur par « true » pour imprimer les événements envoyés à l'ISE —>
<add key="nodeFailoverTimeSpan" value="5000" /> <!— Définit la condition pour le seuil en millisecondes dans lequel le nombre d'erreurs qui peuvent se produire en communication avec le noeud PSN PassiveID actif est compté pour le basculement —>
<add key="nodeFailoverMaxErrors" value="5" /> <!— Définit le nombre maximal d'erreurs tolérées dans le nodeFailoverTimeSpan spécifié avant le basculement vers le noeud PSN PassiveID de secours —>
</appSettings>
</configuration>

Vérifier

Vérification des services PassiveID sur l'ISE

1. Vérifiez si le service PassiveID est activé sur l'interface graphique utilisateur et également marqué comme étant en cours d'exécution à partir de la commande show application status ise sur l'interface de ligne de commande de l'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

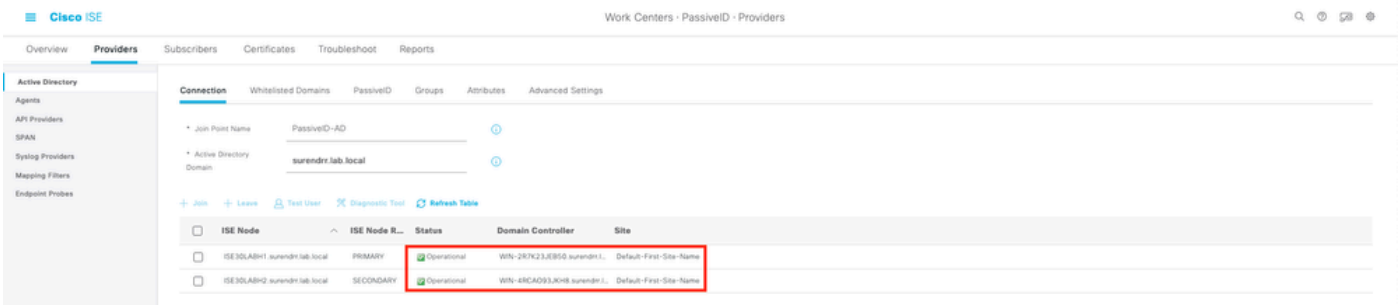
PassiveID Endpoint Service running

18281

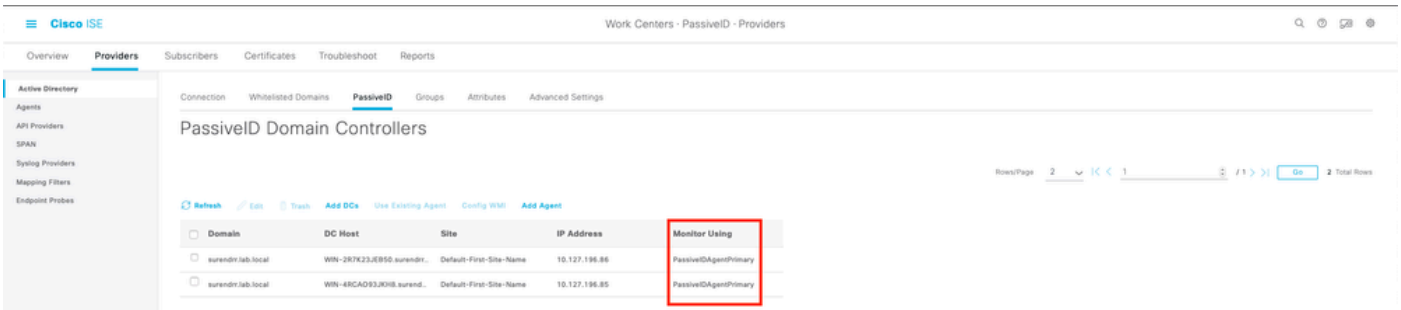
PassiveID SPAN Service running

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

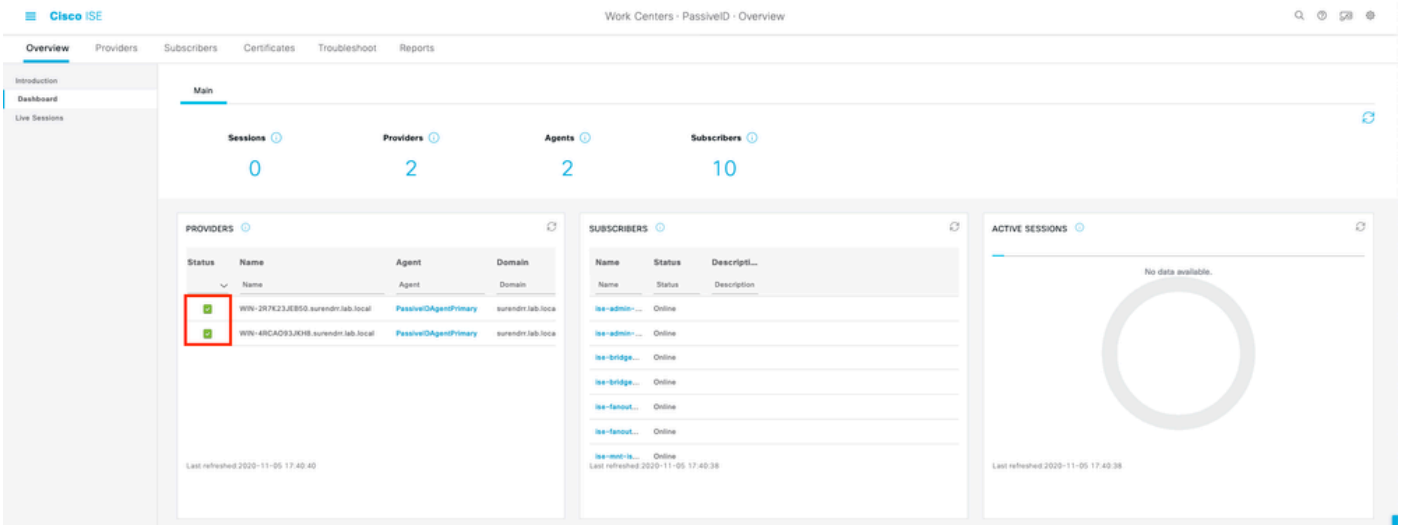
2. Vérifiez si le fournisseur ISE Active Directory est connecté aux contrôleurs de domaine dans Work Centers > PassiveID > Providers > Active Directory > Connection.



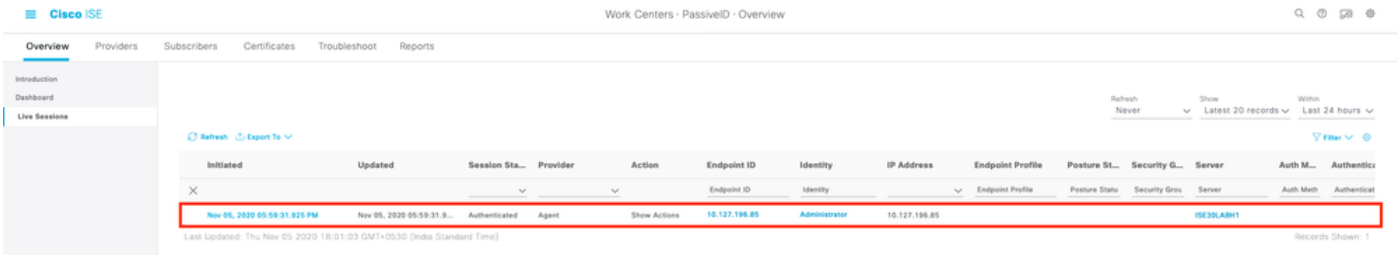
3. Vérifiez si les contrôleurs de domaine requis sont surveillés par Agent at Work Centers > PassiveID > Providers > Active Directory > PassiveID.



4. Vérifiez si l'état des contrôleurs de domaine surveillés est actif. Par exemple, marqué en vert sur le tableau de bord dans Centres de travail > ID passif > Vue d'ensemble > Tableau de bord.

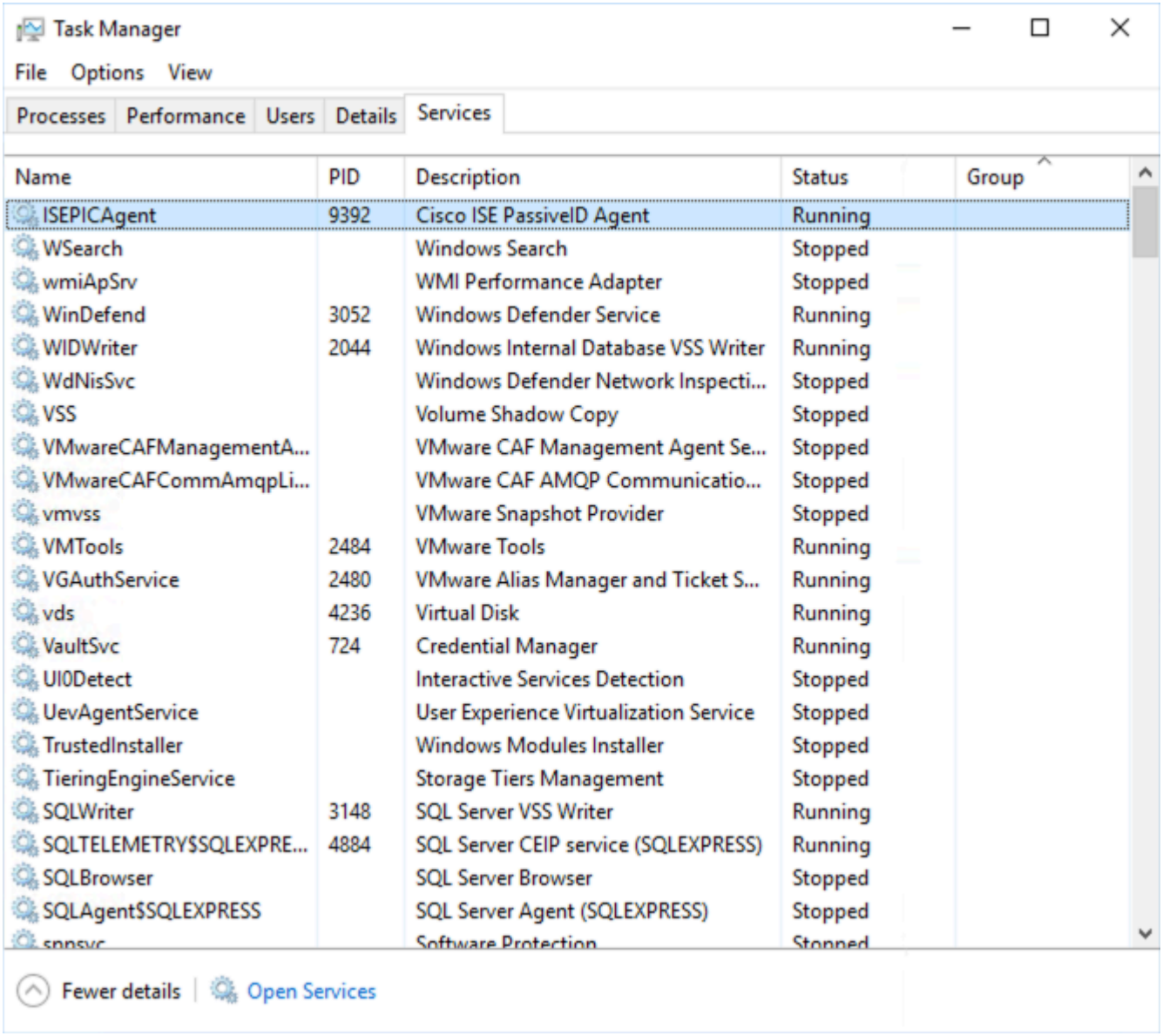


5. Vérifiez que les sessions en direct sont remplies lorsqu'une ouverture de session Windows est enregistrée sur le contrôleur de domaine dans Work Centers > PassiveID > Overview > Live Sessions.



Vérification des services d'agent sur le serveur Windows

1. Vérifiez le service ISEPICAgent sur le serveur sur lequel l'agent PIC est installé.

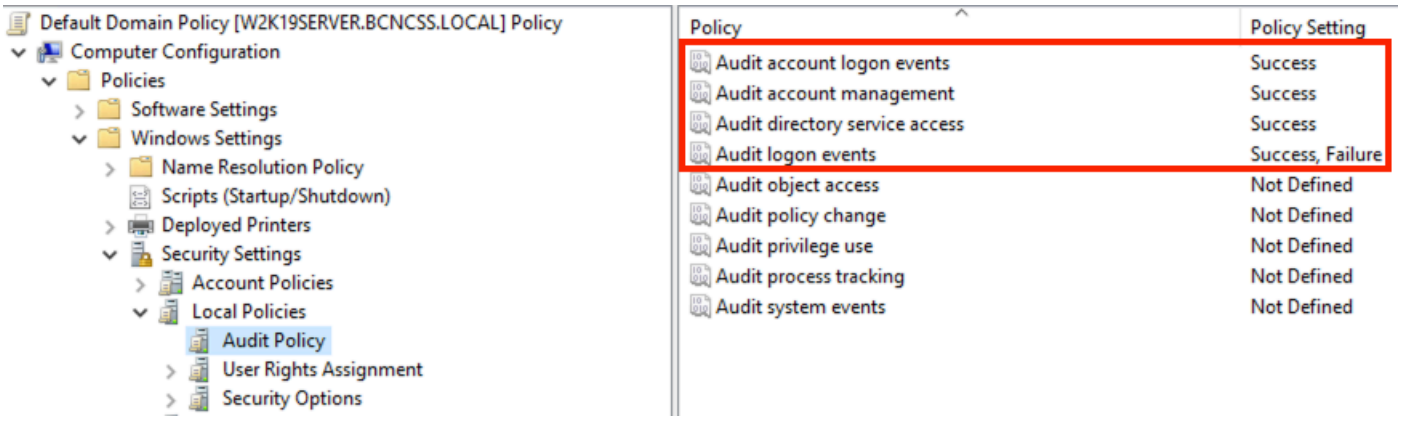


Paramètres requis au niveau du domaine Windows AD - Objets de stratégie de groupe

1. Pour que l'agent ISE PIC puisse lire les entrées des événements de connexion et de déconnexion des utilisateurs, le compte utilisé peut être un compte de service (sans expiration du mot de passe) et peut être un compte de domaine normal et membre du groupe Lecteurs de journaux d'événements

2.- Dans la stratégie de domaine, vérifiez que les paramètres suivants sont définis :

Stratégie de domaine par défaut (ou celle que le client utilise pour ses ordinateurs de domaine) > Paramètres Windows > Paramètres de sécurité > Stratégies locales > Stratégie d'audit et activez les entrées suivantes :



Certains clients se fient à la configuration avancée des stratégies d'audit au lieu d'utiliser les anciennes stratégies locales

.

Si c'est le cas, définissez des stratégies d'audit avancées : Dans l'Éditeur de gestion des stratégies de groupe. Développez Configuration ordinateur → Naviguer vers Stratégies → Naviguer vers Paramètres Windows → Naviguer vers Paramètres de sécurité → Naviguer vers Configuration avancée des stratégies d'audit → Naviguer vers Stratégies d'audit. Définissez les stratégies d'audit suivantes :

Gestion des comptes

· Vérification Gestion des comptes informatiques : Succès

· Gestion du groupe de distribution de la vérification : Succès

· Gestion du groupe de sécurité de la vérification : Succès

· Vérification de la gestion des comptes utilisateurs : Succès

Accès DS

· Accès au service de répertoire de vérification : Succès

Connexion/Déconnexion

· Déconnexion de la vérification : Succès

L'entrée Session au niveau du PIC ISE peut être vue immédiatement, juste après la connexion de l'utilisateur.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.