# Identité utilisateur Firepower : Migration de l'agent utilisateur vers Identity Services Engine

## Introduction

Dans les versions futures, Firepower User Agent n'est plus disponible. Il est remplacé par ISE (Identity Services Engine) ou ISE-PIC (Identity Services Engine - Passive ID Connector). Si vous utilisez actuellement User Agent et envisagez de migrer vers ISE, ce document fournit des considérations et des stratégies pour votre migration.

## Présentation de l'identité utilisateur

Il existe actuellement deux méthodes pour extraire les informations d'identité utilisateur de l'infrastructure d'identité existante : Intégration de User Agent et ISE.

### Agent utilisateur

Agent utilisateur est une application installée sur une plate-forme Windows. Il utilise le protocole WMI (Windows Management Instrumentation) pour accéder aux événements d'ouverture de session utilisateur (type d'événement 4624), puis enregistre les données dans une base de données locale. Il existe deux méthodes pour récupérer les événements de connexion : mis à jour en temps réel lorsque l'utilisateur se connecte (Windows Server 2008 et 2012 uniquement) ou interroge les données pour chaque intervalle configurable. De même, l'agent utilisateur envoie en temps réel les données reçues d'Active Directory (AD) au Firepower Management Center (FMC) et envoie régulièrement des lots de données d'ouverture de session à FMC.

Les types de connexion détectables par l'agent utilisateur incluent la connexion à un hôte directement ou via le Bureau à distance ; connexion au partage de fichiers ; connexion au compte d'ordinateur. D'autres types de connexion tels que Citrix, les connexions réseau et les connexions Kerberos ne sont pas pris en charge par l'agent utilisateur.

L'Agent utilisateur dispose d'une fonctionnalité facultative permettant de détecter si l'utilisateur mappé s'est déconnecté. Si la vérification de déconnexion est activée, elle vérifie périodiquement si le processus « explorer.exe » est exécuté sur chaque point de terminaison mappé. Si vous ne parvenez pas à détecter le processus en cours d'exécution après 72 heures, le mappage de cet utilisateur est supprimé.

### Plateforme de services d'identité

Identity Services Engine (ISE) est un serveur AAA robuste qui gère les sessions de connexion réseau de l'utilisateur. Comme ISE communique directement avec des périphériques réseau tels que des commutateurs et des contrôleurs sans fil, il a accès à des données à jour concernant les activités de l'utilisateur, ce qui en fait une meilleure source d'identité que l'Agent utilisateur. Lorsqu'un utilisateur se connecte à un point d'extrémité, il se connecte généralement automatiquement au réseau et si l'authentification dot1x est activée pour le réseau, ISE crée une session d'authentification pour cet utilisateur et le maintient actif jusqu'à ce que l'utilisateur se déconnecte du réseau. Si ISE est intégré à FMC, il transmet les données de mappage utilisateur-

IP (ainsi que d'autres données collectées par ISE) à FMC.

ISE peut être intégré à FMC via pxGrid. pxGrid est un protocole conçu pour centraliser la distribution des informations de session entre les serveurs ISE et avec d'autres produits. Dans cette intégration, ISE agit en tant que contrôleur pxGrid et FMC s'abonne au contrôleur pour recevoir des données de session (FMC ne publie aucune donnée à ISE, sauf lors de la correction qui sera abordée plus loin) et transmet les données aux capteurs afin de sensibiliser l'utilisateur.

**Identity Services Engine Passive Identity Connector (ISE-PIC)** est essentiellement une instance d'ISE avec une licence restreinte. ISE-PIC n'effectue aucune authentification, mais agit plutôt comme un concentrateur central pour les différentes sources d'identité du réseau, collectant les données d'identité et les fournissant aux abonnés. ISE-PIC est similaire à User Agent en ce sens qu'il utilise également WMI pour collecter les événements de connexion à partir d'AD, mais avec des fonctionnalités plus robustes appelées Passive Identity. Il est également intégré à FMC via pxGrid.

# Considérations relatives à la migration

## Exigences de licence

Le FMC ne nécessite pas de licences supplémentaires. Identity Services Engine nécessite une licence si elle n'est pas déjà déployée dans l'infrastructure. Pour plus d'informations, reportez-vous au document Cisco ISE Licensing Model. ISE Passive ID Connector est un ensemble de fonctionnalités déjà existant dans le déploiement ISE complet. Par conséquent, aucune licence supplémentaire n'est requise s'il existe un déploiement ISE existant. Pour un nouveau déploiement ou un déploiement distinct d'ISE-PIC, reportez-vous au document Cisco ISE-PIC Licensing pour plus de détails.

## Certificat SSL

Bien que l'agent utilisateur ne nécessite pas d'infrastructure à clé publique (PKI) pour les communications avec FMC et Active Directory, l'intégration ISE ou ISE-PIC nécessite des certificats SSL partagés entre ISE et FMC à des fins d'authentification uniquement. L'intégration prend en charge les certificats signés et auto-signés par l'autorité de certification, à condition que l'EKU « Authentification du serveur » et « Authentification du client » (Extention Key Usage) soient ajoutés aux certificats.

## Couverture de la source d'identité

L'agent utilisateur ne couvre que les événements de connexion Windows des bureaux Windows, avec détection de déconnexion basée sur l'interrogation. ISE-PIC couvre la connexion au bureau Windows ainsi que des sources d'identité supplémentaires telles que AD Agent, Kerberos SPAN, Syslog Parser et Terminal Services Agent (TSA). L'ISE complète offre la couverture de l'ISE-PIC ainsi que l'authentification réseau des postes de travail et des appareils mobiles non Windows, entre autres fonctionnalités.

| | Agent utilisateur | ISE-PIC | ISE |
|---|---|---|---|
| **Connexion à Active Directory Desktop** | Oui | Oui | Oui |
| **Connexion réseau** | Non | Non | Oui |
| **Sonde de point de** | Oui | Oui | Oui |

| | | | |
|---|---|---|---|
| terminaison | | | |
| InfoBlox/IPAM | Non | Oui | Oui |
| LDAP | Non | Oui | Oui |
| Passerelles Web sécurisées | Non | Oui | Oui |
| Sources de l'API REST | Non | Oui | Oui |
| Analyseur Syslog | Non | Oui | Oui |
| Portée du réseau | Non | Oui | Oui |

### Fin de vie de l'agent utilisateur

La dernière version de Firepower pour prendre en charge User Agent est la version 6.6, qui fournit un avertissement indiquant que User Agent doit être désactivé avant la mise à niveau vers les versions ultérieures. Si une mise à niveau vers une version supérieure à 6.6 est nécessaire, la migration de User Agent vers ISE ou ISE-PIC doit être effectuée avant la mise à niveau. Pour plus d'informations, reportez-vous au Guide de configuration de l'agent utilisateur.

### Compatibilité

Veuillez consulter le guide de compatibilité des produits Firepower pour vous assurer que les versions logicielles impliquées dans l'intégration sont compatibles. Veuillez noter que pour les versions futures de Firepower, la prise en charge des versions ISE ultérieures peut nécessiter des niveaux de correctifs spécifiques.

## Stratégie de migration

La migration de User Agent vers ISE ou ISE-PIC nécessite une planification, une exécution et des tests minutieux pour garantir une transition en douceur de la source d'identité utilisateur pour FMC et éviter tout impact sur le trafic utilisateur. Cette section présente les meilleures pratiques et les recommandations pour cet exercice.

### Préparation de la migration

Les étapes suivantes peuvent être effectuées avant de passer de l'Agent utilisateur à l'Intégration ISE.

Étape 1. Configurez ISE ou ISE-PIC pour activer PassiveID et établissez une connexion WMI avec Active Directory. Reportez-vous au Guide d'administration ISE-PIC.

Étape 2. Préparez le certificat d'identité de FMC. Il peut s'agir d'un certificat auto-signé émis par FMC ou d'une demande de signature de certificat (CSR) générée sur le FMC, à signer par une autorité de certification privée ou publique. Le certificat auto-signé ou le certificat racine de l'autorité de certification doit être installé sur ISE. Pour plus d'informations, reportez-vous au Guide d'intégration ISE et FMC.

Étape 3. Installez le certificat racine de l'autorité de certification qui a signé le certificat pxGrid de l'ISE (ou le certificat pxGrid s'il est autosigné) sur FMC. Pour plus d'informations, reportez-vous au Guide d'intégration ISE et FMC.

### Processus de basculement

L'intégration FMC-ISE ne peut pas être configurée sans désactiver la configuration de l'agent utilisateur sur FMC, car les deux configurations s'excluent mutuellement. Cela pourrait affecter les utilisateurs pendant la modification. Il est recommandé d'effectuer ces étapes pendant la période de maintenance.

Étape 1. Activez et vérifiez l'intégration FMC-ISE. Pour plus d'informations, reportez-vous au guide d'intégration ISE et FMC.

Étape 2. Assurez-vous que les activités des utilisateurs sont signalées à FMC en naviguant jusqu'à la page **Analyse > Utilisateur > Activités des utilisateurs** sur FMC.

Étape 3. Vérifier que le mappage utilisateur-IP et le mappage de groupe d'utilisateurs sont disponibles sur les périphériques gérés sur
**Analysis > Connections > Events > Table View of Connection Events**.

Étape 4. Modifiez la stratégie de contrôle d'accès pour modifier temporairement l'action **Surveillance** en toute règle qui bloque le trafic en fonction du nom d'utilisateur ou de la condition de groupe d'utilisateurs. Pour les règles qui autorisent le trafic en fonction de l'utilisateur ou du groupe initiateur, créez une règle en double qui autorise le trafic sans critères utilisateur, puis désactivez la règle d'origine. Cette étape a pour but de s'assurer que le trafic stratégique n'est pas affecté pendant l'étape de test après la fenêtre de maintenance.

Étape 5. Après la fenêtre de maintenance, pendant les heures de bureau normales, observez les événements de connexion sur FMC pour surveiller le mappage utilisateur-IP. Notez que les événements de connexion n'affichent les informations utilisateur que s'il existe une règle activée qui nécessite des données utilisateur. D'où la raison pour laquelle l'action de surveillance est suggérée dans l'étape précédente.

Étape 6. Une fois l'état souhaité atteint, il vous suffit de rétablir les modifications apportées aux politiques de contrôle d'accès et de pousser le déploiement des politiques vers les périphériques gérés.

# Additional Information

- Didacticiel vidéo : Transition de l'agent utilisateur vers ISE-PIC
- Guide d'administration de Cisco ISE 2.4 : Licence
- Guide d'installation et d'administration d'ISE-PIC (Identity Services Engine Passive Identity Connector), version 2.2
- Guide de configuration de l'agent utilisateur
- Guide de compatibilité Cisco Firepower
- Configuration de l'intégration ISE 2.4 et FMC 6.2.3 pxGrid