Migrate from User Agent to Identity Services Engine

Contents

Introduction

Background Information

User Identity Overview

- User Agent
- Identity Services Engine
- Identity Services Engine - Passive Identity Connector (ISE-PIC)

Migration Considerations

- Licensing Requirements
- SSL Certificate
- Identity Source Coverage
- User Agent End of Life
- Compatibility

Migration Strategy

- Preparing for Migration
- Cutover Process

Related Information

Introduction

This document describes how to migrate from User Agent to Identity Services Engine (ISE) for Firepower User Agent.

Background Information

In future releases, the Firepower User Agent is no longer available. It is replaced by the ISE or Identity Services Engine - Passive ID Connector (ISE-PIC). If you currently use User Agent and are considering migrating to ISE, this document provides considerations and strategies for your migration.

User Identity Overview

There are currently two methods to extract User Identity information from existing identity infrastructures: User Agent and ISE integration.

User Agent

User Agent is an application installed on a Windows platform. It relies on the Windows Management Instrumentation (WMI) protocol in order to access the user logon events (event type 4624) and then saves the data to a local database. There are two ways User Agent retrieves the logon events: updated in real-time as the user logs in (Windows Server 2008 and 2012 only) or polling the data for every configurable interval.

Similarly, the User Agent sends data received from Active Directory (AD) to the Firepower Management Center (FMC) in real-time and sends batches of logon data to FMC regularly.

Types of logins detectable by the User Agent include login to a host directly or via Remote Desktop; file-sharing login; and computer account login. Other types of logins such as Citrix, network logons, and Kerberos logins are not supported by User Agent.

User Agent has an optional feature to detect if the mapped user has logged off. If the logoff check is enabled, it periodically checks if the explorer.exe process is running on each mapped endpoint. If it cannot detect the process running, then, after 72 hours the mapping for this user is removed.

Identity Services Engine

ISE is a robust AAA server that manages the network login sessions of the user. Since ISE communicates directly with network devices such as switches and wireless controllers, it has access to up-to-date data regarding the activities of the user, making it a better identity source than the User Agent. When a user logs on to an endpoint, it usually automatically connects to the network, and if **dot1x** authentication is enabled for the network, ISE creates an authentication session for these users and keeps it alive until the user logs off the network. If ISE is integrated with FMC, it forwards the user-IP mapping (along with other data collected by ISE) data to FMC.

ISE can be integrated with FMC via pxGrid. pxGrid is a protocol designed to centralize the distribution of session information among ISE servers and with other products. In this integration, ISE acts as a pxGrid Controller and FMC subscribes to the controller in order to receive session data (FMC does not publish any data to ISE except during remediation which is discussed later) and passes the data to the sensors in order to achieve user awareness.

Identity Services Engine - Passive Identity Connector (ISE-PIC)

Identity Services Engine - Passive Identity Connector (ISE-PIC) is essentially an instance of ISE with a restricted license. ISE-PIC does not perform any authentication, but instead acts as a central hub for various identity sources in the network, collecting the identity data and providing them to subscribers. ISE-PIC is similar to User Agent in the way that it also uses WMI in order to gather login events from the AD but with more robust features known as Passive Identity. It is also integrated with FMC via pxGrid.

Migration Considerations

Licensing Requirements

The FMC does not require additional licenses. ISE requires a license if it is not already deployed in the infrastructure. Refer to the Cisco ISE Licensing Model document for details. ISE-PIC is a feature set already existing in full ISE deployment, therefore no additional licenses are required if there is an existing ISE deployment. For a new or separate deployment of ISE-PIC, refer to the Cisco ISE-PIC Licensing document for details.

SSL Certificate

While User Agent does not require Publick Key Infrastructure (PKI) for communications with FMC and AD, ISE or ISE-PIC integration requires SSL certificates shared between ISE and FMC for authentication purposes only. The integration supports Certificate Authority-signed and self-signed certificates, provided that both Server Authentication and Client Authentication Extention Key Usage (EKU) are added to the certificates.

Identity Source Coverage

User Agent covers only Windows login events from Windows Desktops, with polling-based logout detection. ISE-PIC covers Windows Desktop login plus additional identity sources such as AD Agent, Kerberos SPAN, Syslog Parser, and Terminal Services Agent (TSA). Full ISE has the coverage of all ISE-PICs plus network authentication from non-Windows workstations and mobile devices among other features.

	User Agent	ISE-PIC	ISE
Active Directory Desktop Logon	Yes	Yes	Yes
Network Logon	No	No	Yes
Endpoint Probe	Yes	Yes	Yes
InfoBlox/IPAMs	No	Yes	Yes
LDAP	No	Yes	Yes
Secure Web Gateways	No	Yes	Yes
REST API Sources	No	Yes	Yes
Syslog Parser	No	Yes	Yes
Network Span	No	Yes	Yes

User Agent End of Life

The last version of Firepower to support User Agent is 6.6, which provides a warning that User Agent must be disabled prior to upgrading to later releases. If an upgrade to a version later than 6.6 is necessary, migration from User Agent to ISE or ISE-PIC must be completed prior to the upgrade. Refer to the User Agent Configuration Guide for further details.

Compatibility

Review the Firepower product compatibility guide in order to ensure the software versions involved in the integration are compatible. Note that for future Firepower releases, support for later ISE versions requires specific patch levels.

Migration Strategy

Migration from User Agent to ISE or ISE-PIC requires careful planning, execution, and testing in order to ensure a smooth transition of user identity source for FMC and avoid any impact on user traffic. This section provides the best practices and recommendations for this activity.

Preparing for Migration

These steps can be accomplished before cutting over from User Agent to ISE Integration:

Step 1. Configure ISE or ISE-PIC to enable PassiveID, and establish WMI connection with Active Directory. Refer to the ISE-PIC Administration Guide.

Step 2. Prepare the identity certificate of the FMC. It can be either a self-signed certificate issued by the FMC or a Certificate Signing Request (CSR) generated on the FMC, to be signed by a private or public Certificate Authority (CA). The self-signed certificate or the root certificate of the CA must be installed on ISE. Refer to the ISE And FMC Integration Guide for further details.

Step 3. Install the CA root certificate that signed the pxGrid certificate of the ISE (or the pxGrid certificate if self-signed) on FMC. Refer to the ISE And FMC Integration Guide for further details.

Cutover Process

FMC-ISE integration cannot be configured without disabling the User Agent configuration on FMC since the two configurations are mutually exclusive. This can potentially affect the users during the change. These steps are recommended to be performed during the maintenance window.

Step 1. Enable and verify FMC-ISE integration. Refer to the ISE And FMC Integration Guide for details.

Step 2. Ensure user activities are reported to the FMC by navigating to Analysis > User > User Activities page on FMC.

Step 3. Review that user-IP mapping and user-group mapping are available on managed devices from Analysis > Connections > Events > Table View of Connection Events.

Step 4. Modify the Access Control Policy in order to temporarily change the action to **Monitor** to any rules that block traffic depending on the username or user group condition. For rules that allow traffic based on initiator user or group, make a duplicate rule that allows the traffic without user criteria, and then disable the original rule. The purpose of this step is to ensure that business-critical traffic is not impacted during the testing stage after the maintenance window.

Step 5. After the maintenance window, during normal business hours, observe the Connection Events on FMC in order to monitor the user-IP mapping. Note that the connection events show user information only if there is an enabled rule that requires user data. This is why the monitor action is suggested in the earlier step.

Step 6. Once the desired state is achieved, simply revert the changes done to the Access Control Policies and push policy deployment to the managed devices.

Related Information

- Video Tutorial: User-Agent Transition to ISE-PIC
- Cisco ISE 2.4 Admin Guide: Licensing

- User Agent Configuration Guide
- Cisco Firepower Compatibility Guide
- Configure ISE 2.4 and FMC 6.2.3 pxGrid Integration
- Cisco Technical Support & Downloads