Identidad de usuario de Firepower: Migración de agente de usuario a Identity Services Engine

Introducción

En futuras versiones, el agente de usuario Firepower ya no está disponible. Se sustituye por Identity Services Engine (ISE) o Identity Services Engine - Passive ID Connector (ISE-PIC). Si actualmente utiliza un agente de usuario y está considerando migrar a ISE, este documento proporciona consideraciones y estrategias para su migración.

Descripción general de la identidad del usuario

Actualmente existen dos métodos para extraer la información de identidad de usuario de las infraestructuras de identidad existentes: Integración de agente de usuario e ISE.

Agente de usuario

Agente de usuario es una aplicación instalada en una plataforma de Windows. Se basa en el protocolo Instrumental de administración de Windows (WMI) para acceder a los eventos de inicio de sesión de usuario (tipo de evento 4624) y, a continuación, guarda los datos en una base de datos local. Hay dos maneras en que el agente de usuario recupera los eventos de inicio de sesión: se actualizan en tiempo real a medida que el usuario inicia sesión (sólo Windows Server 2008 y 2012) o consulta de los datos para cada intervalo configurable. Del mismo modo, el agente de usuario envía los datos recibidos de Active Directory (AD) al Firepower Management Center (FMC) en tiempo real y envía lotes de datos de inicio de sesión a FMC de forma periódica.

Los tipos de inicios de sesión detectables por el Agente de usuario incluyen el inicio de sesión en un host directamente o a través de Escritorio remoto; inicio de sesión para compartir archivos; inicio de sesión en la cuenta del equipo. El agente de usuario no admite otros tipos de inicios de sesión como Citrix, inicios de sesión de red y inicios de sesión Kerberos.

El agente de usuario tiene una función opcional para detectar si el usuario asignado se ha desconectado. Si la comprobación de cierre de sesión está activada, comprueba periódicamente si el proceso "explorer.exe" se está ejecutando en cada extremo asignado. Si no puede detectar el proceso que se está ejecutando después de 72 horas, se elimina la asignación para este usuario.

Identity Services Engine

Identity Services Engine (ISE) es un servidor AAA robusto que gestiona las sesiones de inicio de sesión en la red del usuario. Dado que ISE se comunica directamente con dispositivos de red, como switches y controladores inalámbricos, tiene acceso a datos actualizados sobre las actividades del usuario, lo que lo convierte en un mejor origen de identidad que el agente de usuario. Cuando un usuario inicia sesión en un terminal, normalmente se conecta automáticamente a la red y, si la autenticación dot1x está habilitada para la red, ISE crea una sesión de autenticación para este usuario y la mantiene activa hasta que el usuario cierra la sesión de la red. Si ISE se integra con FMC, envía los datos de asignación de IP de usuario (junto

con otros datos recopilados por ISE) a FMC.

ISE se puede integrar con FMC a través de pxGrid. pxGrid es un protocolo diseñado para centralizar la distribución de información de sesión entre los servidores ISE y con otros productos. En esta integración, ISE actúa como un controlador pxGrid y FMC se suscribe al controlador para recibir datos de sesión (FMC no publica ningún dato en ISE excepto durante la remediación que se analiza más adelante) y pasa los datos a los sensores para lograr el reconocimiento de los usuarios.

Identity Services Engine Passive Identity Connector (ISE-PIC) es esencialmente una instancia de ISE con una licencia restringida. ISE-PIC no realiza ninguna autenticación, sino que actúa como centro central para diversas fuentes de identidad en la red, recopilando los datos de identidad y proporcionándolos a los suscriptores. ISE-PIC es similar al agente de usuario, ya que también utiliza WMI para recopilar eventos de inicio de sesión de AD, pero con funciones más sólidas conocidas como identidad pasiva. También se integra con FMC a través de pxGrid.

Consideraciones sobre la migración

Requisitos de licencia

El FMC no requiere licencias adicionales. Identity Services Engine requiere una licencia si aún no se ha implementado en la infraestructura. Consulte el documento Modelo de licencias de Cisco ISE para obtener más detalles. ISE Passive ID Connector es un conjunto de funciones que ya existe en la implementación completa de ISE, por lo que no se necesitan licencias adicionales si existe una implementación de ISE existente. Para una implementación nueva o independiente de ISE-PIC, consulte el documento Cisco ISE-PIC Licensing para obtener más detalles.

Certificado SSL

Aunque el agente de usuario no requiere Infraestructura de clave pública (PKI) para las comunicaciones con FMC y Active Directory, la integración de ISE o ISE-PIC requiere certificados SSL compartidos entre ISE y FMC únicamente con fines de autenticación. La integración admite certificados firmados y autofirmados por la Autoridad de Certificación, siempre que se agreguen a los certificados la EKU de "autenticación de servidor" y "autenticación de cliente" (uso de clave de extensión).

Cobertura de origen de identidad

El agente de usuario sólo cubre los eventos de inicio de sesión de Windows desde los escritorios de Windows, con detección de cierre de sesión basada en sondeos. ISE-PIC incluye el inicio de sesión en Windows Desktop, además de orígenes de identidad adicionales como AD Agent, Kerberos SPAN, Syslog Parser y Terminal Services Agent (TSA). El ISE completo cuenta con toda la cobertura de ISE-PIC, además de autenticación de red desde estaciones de trabajo y dispositivos móviles que no son de Windows, entre otras funciones.

	Agente de usuario	ISE-PIC	ISE
Inicio de sesión en Active Directory Desktop	Yes	Yes	Yes
Inicio de sesión de red	No	No	Yes
Sonda de terminal	Yes	Yes	Yes
InfoBlox/IPAM	No	Yes	Yes

LDAP	No	Yes	Yes
Gateways web seguros	No	Yes	Yes
Fuentes de API REST	No	Yes	Yes
Syslog Parser	No	Yes	Yes
Extensión de red	No	Yes	Yes

Fin de vida útil del agente de usuario

La última versión de Firepower para admitir el agente de usuario es la 6.6, que proporciona una advertencia de que el agente de usuario debe desactivarse antes de actualizar a versiones posteriores. Si es necesaria una actualización a una versión superior a 6.6, la migración de User Agent a ISE o ISE-PIC debe completarse antes de la actualización. Consulte la guía de configuración del agente de usuario para obtener más detalles.

Compatibilidad

Revise la guía de compatibilidad de productos Firepower para asegurarse de que las versiones de software involucradas en la integración sean compatibles. Tenga en cuenta que para futuras versiones de Firepower, el soporte para versiones posteriores de ISE puede requerir niveles de parches específicos.

Estrategia de migración

La migración de un agente de usuario a ISE o ISE-PIC requiere una cuidadosa planificación, ejecución y prueba para garantizar una transición fluida del origen de identidad del usuario para FMC y evitar cualquier impacto en el tráfico de los usuarios. Esta sección proporciona las mejores prácticas y recomendaciones para esta actividad.

Preparación para la migración

Los siguientes pasos se pueden realizar antes de pasar de User Agent a ISE Integration.

Paso 1. Configure ISE o ISE-PIC para habilitar PassiveID y establecer la conexión WMI con Active Directory. Consulte la Guía de Administración de ISE-PIC.

Paso 2. Preparar el certificado de identidad de FMC. Puede ser un certificado autofirmado emitido por FMC o una solicitud de firma de certificado (CSR) generada en el FMC, que debe ser firmado por una autoridad de certificación privada o pública (CA). El certificado autofirmado o el certificado raíz de la CA se deben instalar en ISE. Consulte la Guía de integración de ISE y FMC para obtener más detalles.

Paso 3. Instale el certificado raíz de CA que firmó el certificado pxGrid de ISE (o el certificado pxGrid si se firma automáticamente) en FMC. Consulte la Guía de integración de ISE y FMC para obtener más detalles.

Proceso de transición

La integración de FMC-ISE no se puede configurar sin deshabilitar la configuración del agente de usuario en FMC, ya que las dos configuraciones son mutuamente excluyentes. Esto podría afectar potencialmente a los usuarios durante el cambio. Se recomienda realizar estos pasos

durante la ventana de mantenimiento.

Paso 1. Habilite y verifique la integración de FMC-ISE. Consulte la Guía de integración de ISE y FMC para obtener más detalles.

Paso 2. Asegúrese de que las actividades de usuario se informen a FMC que navegan a la página **Análisis > Usuario > Actividades de usuario** en FMC.

Paso 3. Revise que la asignación de IP de usuario y la asignación de grupo de usuarios están disponibles en los dispositivos administrados en **Análisis > Conexiones > Eventos > Vista de tabla de eventos de conexión**.

Paso 4. Modifique la política de control de acceso para cambiar temporalmente la acción a **Monitor** a cualquier regla que bloquee el tráfico dependiendo de la condición de nombre de usuario o grupo de usuarios. Para las reglas que permiten el tráfico basado en el usuario o grupo iniciador, realice una regla duplicada que permita el tráfico sin criterios de usuario y luego inhabilite la regla original. El objetivo de este paso es garantizar que el tráfico empresarial crítico no se vea afectado durante la fase de prueba después de la ventana de mantenimiento.

Paso 5. Después de la ventana de mantenimiento, durante el horario laboral normal, observe los eventos de conexión en FMC para monitorear la asignación de IP de usuario. Tenga en cuenta que los eventos de conexión sólo muestran información del usuario si hay una regla habilitada que requiere datos del usuario. De ahí que en el paso anterior se sugiera la acción de supervisión.

Paso 6. Una vez alcanzado el estado deseado, simplemente revierta los cambios realizados en las Políticas de control de acceso e impulse la implementación de políticas a los dispositivos administrados.

Información adicional

- Tutorial de vídeo: Transición de agente de usuario a ISE-PIC
- Guía de administración de Cisco ISE 2.4: Licencias
- Guía de instalación y administrador de Identity Connector pasivo (ISE-PIC) de Identity Services Engine, versión 2.2
- Guía de configuración del agente de usuario
- Guía de compatibilidad de Cisco Firepower
- Configuración de la integración de ISE 2.4 y FMC 6.2.3 pxGrid