Identiteit gebruiker Firepower: Migratie van gebruikersagent naar Identity Services Engine

Inleiding

In toekomstige versies is de Firepower User Agent niet langer beschikbaar. Deze wordt vervangen door de Identity Services Engine (ISE) of Identity Services Engine - Passive ID-connector (ISE-PIC). Als u momenteel gebruikersagent gebruikt en wilt migreren naar ISE, dan biedt dit document overwegingen en strategieën voor uw migratie.

Overzicht van identiteit gebruiker

Er zijn momenteel twee methoden om de identiteit van de gebruiker uit de bestaande identiteitsinfrastructuur te halen: Gebruikersagent en ISE-integratie.

gebruikersagent

Gebruikersagent is een toepassing die op een Windows-platform is geïnstalleerd. Het is gebaseerd op het protocol van Windows Management Instrumentation (WMI) om toegang te krijgen tot een aanmelding door gebruiker (eventtype 4624) en slaat de gegevens vervolgens op in een lokale database. Er zijn twee manieren waarop Gebruiker Agent de openingsgebeurtenissen herstelt: in real-time bijgewerkt als gebruiker inlogt (alleen Windows Server 2008 en 2012), of de gegevens voor elk configureerbare interval opvragen. Op dezelfde manier stuurt Gebruikersagent gegevens die van Active Directory (AD) zijn ontvangen naar het FireSIGHT Management Center (FMC) in real-time en stuurt u regelmatig batches met aanmeldingsgegevens naar het FMC.

Typen logins die door een gebruikersagent kunnen worden gedetecteerd, zijn inloggen in een host rechtstreeks of via een afstandsbediening; inloggen voor het delen van bestanden; aanmelding van computeraccount. Andere typen logins zoals Citrix, netwerklogons en Kerberos-logins worden niet ondersteund door gebruikersagent.

Gebruiker Agent heeft een optionele functie om te detecteren of de in kaart gebrachte gebruiker is uitgeschakeld. Als de controle op het licht is ingeschakeld, controleert het periodiek of het proces "explorer.exe" op elk in kaart gebracht eindpunt wordt uitgevoerd. Als u het actieve proces niet kunt detecteren, wordt de mapping voor deze gebruiker na 72 uur verwijderd.

Identity Services Engine

Identity Services Engine (ISE) is een robuuste AAA-server die de netwerkinlogsessies van de gebruiker beheert. Aangezien ISE direct met netwerkapparaten zoals switches en draadloze controllers communiceert, heeft het toegang tot actuele gegevens over de activiteiten van de gebruiker. Hierdoor is het een betere identiteitsbron dan de gebruikersagent. Wanneer een gebruiker op een eindpunt inlogt, sluit het zich automatisch aan op het netwerk, en als punt1x authenticatie voor het netwerk wordt toegelaten, creëert ISE een authenticatiesessie voor deze gebruiker en houdt het in leven tot de gebruiker van het netwerk aflogt. Als ISE met FMC is geïntegreerd, stuurt het de gebruiker-IP mapping (samen met andere gegevens die door ISE worden verzameld) naar FMC.

ISE kan via pxGrid met FMC worden geïntegreerd. pxGrid is een protocol dat is ontworpen om de distributie van sessieinformatie tussen ISE-servers en met andere producten te centraliseren. In deze integratie treedt ISE op als een PxGrid-controller en FMC abonneert op de controller om sessiegegevens te ontvangen (FMC publiceert geen gegevens aan ISE, behalve tijdens herstelwerkzaamheden die later worden besproken) en geeft de gegevens door aan sensoren om gebruikersbewustzijn te bereiken.

Identity Services Engine Passive Identity Connector (ISE-PIC) is in wezen een geval van ISE met een beperkte licentie. ISE-PIC voert geen authenticatie uit, maar fungeert in plaats daarvan als een centraal knooppunt voor verschillende identiteitsbronnen in het netwerk, waarbij de identiteitsgegevens worden verzameld en aan abonnees worden verstrekt. ISE-PIC is vergelijkbaar met User Agent in die ook WMI gebruikt om inloggebeurtenissen van AD te verzamelen, maar met robuustere functies die bekend zijn als Passive Identity. Het wordt ook geïntegreerd met FMC via pxGrid.

Migratieoverwegingen

Licentie-vereisten

Het FMC heeft geen extra licenties nodig. Voor Identity Services Engine is een licentie vereist indien deze nog niet in de infrastructuur is ingezet. Raadpleeg het Cisco ISE Licensing Model-document voor meer informatie. ISE Passive ID Connector is een functieset die al in volledige ISE-implementatie bestaat, daarom zijn er geen extra licenties vereist als er een bestaande ISE-implementatie is. Raadpleeg voor een nieuwe of afzonderlijke implementatie van ISE-PIC het Cisco ISE-PIC Licensing document voor meer informatie.

SSL-certificaat

Hoewel User Agent geen Public Key Infrastructure (PKI) nodig heeft voor communicatie met FMC en Active Directory, vereist ISE of ISE-PIC integratie alleen SSL-certificaten die door ISE en FMC worden gedeeld voor verificatiedoeleinden. De integratie ondersteunt de door de certificeringsinstantie ondertekende en zelf ondertekende certificaten, op voorwaarde dat zowel de "Server Authentication"- als de "Client Authentication" EKU (Exmission Key Gebruik) aan de certificaten worden toegevoegd.

Dekking van identiteitsbron

Gebruiker Agent beschrijft alleen inloggebeurtenissen van Windows bureaubladen, met een op opiniepeiling gebaseerde detectie van uitlogingen. ISE-PIC heeft betrekking op Windows-desktopinloggen plus extra identiteitsbronnen zoals AD-agent, Kerberos SPAN, Syslog Parser en Terminal Services Agent (TSA). Full ISE heeft alle dekking van ISE-PIC plus netwerkauthenticatie van niet-Windows werkstations en mobiele apparaten onder andere eigenschappen.

	gebruikersagent	ISE-PIC	ISE
Logboek actieve directory	Ja	Ja	Ja
Netwerkaanmelding	Nee	Nee	Ja
Endpoint Probe	Ja	Ja	Ja
InfoBlox/IPAM's	Nee	Ja	Ja
LDAP	Nee	Ja	Ja
Secure-webgateways	Nee	Ja	Ja

REST API-bronnen	Nee	Ja	Ja
Syslog Parser	Nee	Ja	Ja
Netwerkafstand	Nee	Ja	Ja

Eindtijd van gebruikersagent

De laatste versie van Firepower to support User Agent is 6.6, wat een waarschuwing bevat dat Gebruikersagent moet worden uitgeschakeld voordat de upgrade naar latere releases wordt uitgevoerd. Als een upgrade naar een versie van meer dan 6.6 nodig is, moet de migratie van gebruikersagent naar ISE of ISE-PIC vóór de upgrade voltooid zijn. Raadpleeg de gebruikershandleiding bij de configuratie van de agent voor meer informatie.

Compatibiliteit

Controleer de compatibiliteitsgids voor FirePOWER-producten om er zeker van te zijn dat de softwareversies die bij de integratie betrokken zijn, compatibel zijn. Houd er rekening mee dat voor toekomstige FirePOWER-releases ondersteuning voor latere ISE-versies specifieke patchniveaus nodig kan zijn.

Migratiestrategie

De migratie van Gebruiker Agent naar ISE of ISE-PIC vereist zorgvuldige planning, uitvoering en testen om een vlotte overgang van de gebruiker identiteitsbron voor FMC te verzekeren en om elke impact op gebruikersverkeer te vermijden. In dit deel worden de beste praktijken en aanbevelingen voor deze activiteit beschreven.

Voorbereiden op migratie

De volgende stappen kunnen worden gezet voordat u de tekst van gebruikersagent naar ISE Integration doorsnijdt.

Stap 1. Configureer ISE of ISE-PIC om PassiveID in te schakelen en stel een WMI-verbinding in met actieve map. Raadpleeg de ISE-PIC beheergids.

Stap 2. Bereid het identiteitsbewijs van het FMC voor. Het kan een door het VCC afgegeven zelfgetekend certificaat zijn of een op het VCC gegenereerd certificaataanvraag (CSR), die door een particuliere of openbare certificeringsinstantie (CA) moet worden ondertekend. Het zelf ondertekende certificaat of het wortelcertificaat van de CA moet op ISE zijn geïnstalleerd. Raadpleeg de ISE- en FMC-integratiegids voor meer informatie.

Stap 3. Installeer het CA-basiscertificaat dat aan de hand van het ISE-certificaat (of het PxGrid-certificaat indien zelf ondertekend) op FMC is ondertekend. Raadpleeg de ISE- en FMC-integratiegids voor meer informatie.

keuzeproces

De FMC-ISE-integratie kan niet worden geconfigureerd zonder de configuratie van gebruikersagent op FMC uit te schakelen, omdat de twee configuraties elkaar uitsluiten. Dit zou de gebruikers tijdens de verandering kunnen beïnvloeden. Deze stappen worden aanbevolen tijdens het onderhoudsvenster.

Stap 1. Schakel FMC-ISE-integratie in en na. Raadpleeg de ISE- en FMC-integratiegids voor meer informatie.

Stap 2. Zorg ervoor dat gebruikersactiviteiten aan FMC worden gerapporteerd door te navigeren naar **Analyse > Gebruiker > Gebruiker > Gebruiker Activiteiten** op FMC.

Stap 3. Controleer dat user-IP mapping en user-group mapping beschikbaar zijn op beheerde apparaten op
Analyse > Verbonden > Evenementen > Tabelweergave van verbindingsgebeurtenissen.

Stap 4. Wijzig het beleid voor toegangscontrole om de actie tijdelijk te wijzigen om de bewaking te **controleren** op regels die verkeer blokkeren, afhankelijk van de gebruikersnaam of de conditie van de gebruikersgroep. Voor regels die verkeer op Initiator gebruiker of groep toestaan, maak een dubbele regel die het verkeer zonder gebruikerscriteria toestaat en blokkeer dan de originele regel. Het doel van deze stap is ervoor te zorgen dat bedrijfskritisch verkeer niet wordt beïnvloed tijdens de testfase na het onderhoudsvenster.

Stap 5. Na het onderhoudsvenster, tijdens normale openingstijden, observeer de verbindingsgebeurtenissen op FMC om de gebruiker-IP-mapping te controleren. Merk op dat de verbindingsgebeurtenissen gebruikersinformatie tonen slechts als er een toegelaten regel is die gebruikersgegevens vereist. Daarom wordt in de vorige fase gesuggereerd om de actie te volgen.

Stap 6. Zodra de gewenste staat is bereikt, draait u simpelweg de wijzigingen in het toegangscontrolebeleid om en zet u de beleidsuitvoering naar beheerde apparaten aan.

Aanvullende informatie

- Videolessen: Gebruiker Agent-overgang naar ISE-PIC
- Cisco ISE 2.4 Admin Guide: Licentie
- Identity Services Engine Passive Identity Connector (ISE-PIC) installatie en beheerdershandleiding, release 2.2
- Configuratiehandleiding voor gebruikersagent
- Cisco-compatibiliteitsgids
- Configuratie ISE 2.4 en FMC 6.2.3 pxGrid-integratie