Identità utente Firepower: Migrazione da agente utente a Identity Services Engine

Introduzione

Nelle versioni future, Firepower User Agent non è più disponibile. Viene sostituita da Identity Services Engine (ISE) o Identity Services Engine - Passive ID Connector (ISE-PIC). Se al momento si utilizza User Agent e si intende migrare ad ISE, questo documento fornisce considerazioni e strategie per la migrazione.

Panoramica sull'identità dell'utente

Esistono attualmente due metodi per estrarre le informazioni sull'identità dell'utente dall'infrastruttura delle identità esistente: User Agent e integrazione ISE.

Agente utente

Agente utente è un'applicazione installata su una piattaforma Windows. Si basa sul protocollo Strumentazione gestione Windows (WMI) per accedere agli eventi di accesso dell'utente (tipo di evento 4624) e quindi salva i dati in un database locale. Esistono due modi per recuperare gli eventi di accesso: aggiornato in tempo reale all'accesso dell'utente (solo Windows Server 2008 e 2012) o durante il polling dei dati per ogni intervallo configurabile. Analogamente, l'agente utente invia i dati ricevuti da Active Directory (AD) al centro di gestione Firepower (FMC) in tempo reale e invia regolarmente batch di dati di accesso al centro.

I tipi di login rilevabili dall'agente utente includono il login a un host direttamente o tramite Desktop remoto; accesso con condivisione dei file; account computer. Altri tipi di accesso, ad esempio Citrix, gli accessi di rete e Kerberos, non sono supportati dall'agente utente.

Agente utente dispone di una funzionalità facoltativa per rilevare se l'utente mappato si è disconnesso. Se il controllo della disconnessione è abilitato, controlla periodicamente se il processo "explorer.exe" è in esecuzione su ciascun endpoint mappato. Se non è possibile rilevare il processo in esecuzione dopo 72 ore, il mapping per questo utente viene rimosso.

Identity Services Engine

Identity Services Engine (ISE) è un solido server AAA che gestisce le sessioni di accesso alla rete dell'utente. Poiché ISE comunica direttamente con dispositivi di rete quali switch e controller wireless, ha accesso a dati aggiornati sulle attività degli utenti, rendendola una fonte di identità migliore rispetto all'agente utente. Quando un utente accede a un endpoint, in genere si connette automaticamente alla rete e, se l'autenticazione dot1x è abilitata per la rete, ISE crea una sessione di autenticazione per questo utente e la mantiene attiva fino a quando l'utente non si disconnette dalla rete. Se ISE è integrato con FMC, inoltra i dati della mappatura IP utente (insieme ad altri dati raccolti da ISE) al FMC.

ISE può essere integrato con FMC tramite pxGrid. pxGrid è un protocollo progettato per centralizzare la distribuzione delle informazioni sulla sessione tra i server ISE e con altri prodotti.

In questa integrazione, ISE agisce come un pxGrid Controller e FMC si iscrive al controller per ricevere i dati della sessione (FMC non pubblica alcun dato ad ISE se non durante le riparazioni che saranno discusse in seguito) e passa i dati ai sensori per ottenere la consapevolezza dell'utente.

Identity Services Engine Passive Identity Connector (ISE-PIC) è essenzialmente un'istanza di ISE con una licenza limitata. ISE-PIC non esegue l'autenticazione, ma funge da hub centrale per le diverse origini di identità della rete, raccogliendo i dati di identità e fornendoli agli utenti. ISE-PIC è simile a User Agent in quanto utilizza anche WMI per raccogliere gli eventi di accesso da AD, ma con funzionalità più affidabili note come identità passiva. È anche integrato con FMC tramite pxGrid.

Considerazioni sulla migrazione

Requisiti delle licenze

Il CCP non richiede licenze aggiuntive. Identity Services Engine richiede una licenza se non è già implementato nell'infrastruttura. Per ulteriori informazioni, consultare il documento Cisco ISE Licensing Model. ISE Passive ID Connector è un set di funzionalità già esistente nella distribuzione completa di ISE, quindi non sono necessarie licenze aggiuntive se è presente una distribuzione di ISE. Per un'implementazione nuova o separata di ISE-PIC, consultare il documento sulle licenze Cisco ISE-PIC per ulteriori informazioni.

Certificato SSL

Mentre l'agente utente non richiede l'infrastruttura PKI (Public Key Infrastructure) per le comunicazioni con FMC e Active Directory, l'integrazione ISE o ISE-PIC richiede certificati SSL condivisi tra ISE e FMC solo a scopo di autenticazione. L'integrazione supporta i certificati autofirmati e firmati da Autorità di certificazione, a condizione che ai certificati vengano aggiunti sia l'utilizzo chiavi di estensione che l'utilizzo chiavi di autenticazione client.

Copertura origine identità

L'agente utente copre solo gli eventi di accesso a Windows dai desktop di Windows, con rilevamento della disconnessione basata su polling. ISE-PIC riguarda l'accesso a Windows Desktop e altre origini di identità, quali AD Agent, Kerberos SPAN, Syslog Parser e Terminal Services Agent (TSA). Full ISE offre tutto il supporto di ISE-PIC, oltre all'autenticazione di rete da workstation non Windows e dispositivi mobili, oltre ad altre funzioni.

	Agente utente	ISE-PIC	ISE
Accesso a Active Directory Desktop	Sì	Sì	Sì
Accesso alla rete	No	No	Sì
Probe dell'endpoint	Sì	Sì	Sì
InfoBlox/Gestione indirizzi IP	No	Sì	Sì
LDAP	No	Sì	Sì
Gateway Web protetti	No	Sì	Sì
Origini API REST	No	Sì	Sì
Parser syslog	No	Sì	Sì

Span di rete	No	Sì	Sì

Fine del ciclo di vita agente utente

L'ultima versione di Firepower per il supporto dell'agente utente è 6.6, che indica che l'agente utente deve essere disabilitato prima di eseguire l'aggiornamento a versioni più recenti. Se è necessario un aggiornamento a una versione superiore alla 6.6, è necessario completare la migrazione da User Agent ad ISE o ISE-PIC prima dell'aggiornamento. Per ulteriori informazioni, consultare la Guida alla configurazione dell'agente utente.

Compatibilità

Consultare la guida alla compatibilità dei prodotti Firepower per assicurarsi che le versioni software coinvolte nell'integrazione siano compatibili. Per le future versioni di Firepower, il supporto per le versioni ISE più recenti potrebbe richiedere livelli di patch specifici.

Strategia di migrazione

La migrazione da User Agent ad ISE o ISE-PIC richiede un'attenta pianificazione, esecuzione e test per garantire una transizione senza problemi dell'origine dell'identità utente per FMC ed evitare qualsiasi impatto sul traffico degli utenti. In questa sezione vengono illustrate le procedure ottimali e i suggerimenti per l'attività.

Preparazione per la migrazione

I passaggi successivi possono essere eseguiti prima del passaggio da User Agent a ISE Integration.

Passaggio 1. Configurare ISE o ISE-PIC per abilitare PassiveID e stabilire una connessione WMI con Active Directory. Fare riferimento alla Guida all'amministrazione di ISE-PIC.

Passaggio 2. Preparare il certificato di identità del CCP. Può trattarsi di un certificato autofirmato rilasciato dal CCP o di una richiesta di firma del certificato (CSR) generata dal CCP e firmata da un'autorità di certificazione (CA) pubblica o privata. Il certificato autofirmato o il certificato radice della CA deve essere installato su ISE. Per ulteriori informazioni, consultare la guida all'integrazione di ISE e FMC.

Passaggio 3. Installare il certificato radice CA che ha firmato il certificato pxGrid di ISE (o il certificato pxGrid se autofirmato) su FMC. Per ulteriori informazioni, consultare la guida all'integrazione di ISE e FMC.

Processo di copertura

Impossibile configurare l'integrazione FMC-ISE senza disabilitare la configurazione dell'agente utente in FMC perché le due configurazioni si escludono a vicenda. Ciò potrebbe influire sugli utenti durante la modifica. Queste operazioni sono consigliate durante la finestra di manutenzione.

Passaggio 1. Abilitare e verificare l'integrazione FMC-ISE. Per ulteriori informazioni, consultare la Guida all'integrazione di ISE e FMC.

Passaggio 2. Verificare che le attività utente vengano segnalate al CCP passando alla pagina **Analisi > Utente >** Attività **utente** nel CCP.

Passaggio 3. Verificare che il mapping utente-IP e il mapping utente-gruppo siano disponibili nei dispositivi gestiti su
Analisi > Connessioni > Eventi > Visualizzazione tabella degli eventi di connessione.

Passaggio 4. Modificare i criteri di controllo dell'accesso per modificare temporaneamente l'azione da **Monitorare** a qualsiasi regola che blocchi il traffico a seconda della condizione del nome utente o del gruppo di utenti. Per le regole che consentono il traffico in base all'utente o al gruppo iniziatore, creare una regola duplicata che consenta il traffico senza criteri utente e quindi disattivare la regola originale. Lo scopo di questa fase è garantire che il traffico business critical non venga influenzato durante la fase di test successiva alla finestra di manutenzione.

Passaggio 5. Dopo la finestra di manutenzione, durante il normale orario di lavoro, osservare gli eventi di connessione su FMC per monitorare il mapping utente-IP. Si noti che gli eventi di connessione visualizzano le informazioni utente solo se è presente una regola attivata che richiede dati utente. Per questo motivo l'azione di monitoraggio è suggerita nel passaggio precedente.

Passaggio 6. Una volta raggiunto lo stato desiderato, è sufficiente annullare le modifiche apportate ai criteri di controllo di accesso e inviare la distribuzione dei criteri ai dispositivi gestiti.

Ulteriori informazioni

- Esercitazione video: Transizione di User Agent ad ISE-PIC
- Guida per l'amministratore di Cisco ISE 2.4: Licenze
- Guida all'installazione e amministrazione di Identity Services Engine Passive Identity Connector (ISE-PIC), versione 2.2
- Guida alla configurazione dell'agente utente
- Guida alla compatibilità di Cisco Firepower
- Configurazione dell'integrazione di ISE 2.4 e FMC 6.2.3 pxGrid