Comprendere i servizi, lo scopo e la risoluzione dei problemi ISE

Sommario

- Introduzione
- Prerequisiti
  - Requisiti
  - Componenti usati
- Premesse
- Descrizione e risoluzione dei problemi dei servizi ISE
  - Listener del database
    - Punti chiave del servizio di listener del database in ISE
  - Server di database
    - Punti chiave del servizio Database Server in ISE
    - Verificare e risolvere i problemi relativi all'inizializzazione o alla mancata esecuzione dei servizi del listener e del server di database
  - Server applicazioni
    - Punti chiave del servizio Application Server in ISE
    - Verifica per Application Server in corso di inizializzazione o non in esecuzione
  - Database profiler
    - Punti chiave del servizio database Profiler in ISE
    - Verifica e risoluzione dei problemi di ISE Profiling Services
  - ISE Indexing Engine
    - Verificare che il motore di indicizzazione ISE non sia in esecuzione o in fase di inizializzazione
  - Connettore AD
    - Funzioni principali del servizio AD Connector in ISE
  - Database sessione M&T
    - Funzioni principali del servizio di database delle sessioni M&T in ISE
    - Verifica e risoluzione dei problemi per il database delle sessioni M&T in ISE
  - Processore log M&T
    - Funzioni principali del servizio M&T Log Processor in ISE
    - Verifica e risoluzione dei problemi del servizio Processore di log M&T in ISE
  - Servizio Autorità di certificazione
    - Funzioni chiave del servizio Certification Authority in ISE
  - Servizio EST
    - Funzioni principali del servizio EST ad ISE
    - Verificare che l'Autorità di certificazione e il servizio EST non siano in esecuzione o in fase di inizializzazione
  - Servizio motore SXP
    - Funzioni principali del servizio SXP Engine in ISE
    - Verifica e risoluzione dei problemi per il servizio motore SXP a ISE
  - Servizio TC-NAC
    - Funzioni principali del servizio TC-NAC in ISE
    - Verifica e risoluzione dei problemi del servizio TC-NAC in ISE

- Servizio WMI PassiveID
  - Funzioni chiave del servizio WMI PassiveID in ISE
  - Verifica e risoluzione dei problemi del servizio WMI PassiveID
- Servizio syslog ID passivo
  - Funzioni chiave del servizio Syslog ID passivo
- Servizio API PassiveID
  - Funzioni chiave del servizio API ID passivo
- Servizio Agente ID passivo
  - Funzioni chiave del servizio Agente ID passivo
- Servizio endpoint ID passivo
  - Funzioni chiave di PassiveID Endpoint Service
- Servizio SPAN ID passivo
  - Funzioni chiave del servizio SPAN ID passivo
  - Verifica e risoluzione dei problemi per lo stack PassiveID (servizio SPAN PassiveID, servizio Syslog PassiveID, servizio Endpoint PassiveID, agente PassiveID, servizio API PassiveID)
- Server DHCP (dhcpd)
  - Funzioni principali del servizio Server DHCP (dhcpd) in ISE
  - Verifica e risoluzione dei problemi del server DHCP (dhcpd)
- Server DNS (denominato)
  - Funzioni chiave del servizio Server DNS (con nome) in ISE
  - Verifica e risoluzione dei problemi per il server DNS (denominato)
- ISE Messaging Service
  - Funzioni principali del servizio di messaggistica ISE
  - Verificare che il servizio di messaggistica ISE non sia in esecuzione o in fase di inizializzazione
- Servizio database ISE API Gateway
  - Funzioni chiave del servizio ISE API Gateway Database
  - Servizio ISE API Gateway
  - Funzioni chiave del servizio ISE API Gateway
  - Verifica e risoluzione dei problemi del servizio ISE API Gateway e del servizio ISE API Gateway Database
- Servizio ISE pxGrid Direct
  - Funzioni principali del servizio ISE pxGrid Direct
  - Verifica e risoluzione dei problemi del servizio ISEPxgrid Direct
- Servizio criteri di segmentazione
  - Funzioni chiave del servizio criteri di segmentazione
  - Verifica e risoluzione dei problemi del servizio criteri di segmentazione
- Servizio autenticazione REST
  - Funzioni chiave del servizio di autenticazione REST
  - Verifica e risoluzione dei problemi per autenticazione REST
- Connettore SSE
  - Funzioni principali del connettore SSE
  - Verifica e risoluzione dei problemi del connettore SSE
- Hermes (agente cloud pxGrid)
  - Caratteristiche e funzioni principali di Hermes (pxGrid Cloud Agent)
  - Verifica e risoluzione dei problemi di Hermes (agente cloud Pxgrid)
- McTrust (servizio di sincronizzazione Meraki)
  - Caratteristiche e funzioni principali di McTrust (Meraki Sync Service)
  - Verifica e risoluzione dei problemi di McTrust (servizio di sincronizzazione Meraki)
- ISE Node Exporter
  - Funzioni e caratteristiche principali di ISE Node Exporter

- ISE Prometheus Service
  - Caratteristiche e funzioni principali del servizio Prometeo di ISE
- ISE Grafana Service
  - Funzioni e caratteristiche principali di ISE Grafana Service
  - Verifica e risoluzione dei problemi di ISE Grafana Service, ISE Prometheus Service, ISE Node Exporter
- ISE NT LogAnalytics Elasticsearch
  - Funzioni e caratteristiche principali di ISE MNT LogAnalytics Elasticsearch
  - Verifica e risoluzione dei problemi di ISE M&T Log Analytics Elasticsearch
- ISE Logstash Service
  - Funzioni e caratteristiche principali del servizio ISE Logstash
  - Verifica e risoluzione dei problemi di ISE Logstash Service
- ISE Kibana Service
  - Caratteristiche e funzioni principali del servizio ISE Kibana
  - Verifica e risoluzione dei problemi del servizio ISE Kibana
- Servizio IPSec nativo ISE
  - Funzioni e caratteristiche principali del servizio IPSec nativo ISE
  - Verifica e risoluzione dei problemi del servizio IPSec nativo
- Profiler MFC
  - Funzioni e caratteristiche principali del servizio Profiler MFC ad ISE
  - Verifica e risoluzione dei problemi del servizio profiler MFC
- Punti chiave

Problemi standard ad ISE

- Verifica della media dei carichi elevati, problemi di utilizzo delle risorse (CPU / MEMORIA / DISCO), risorse insufficienti
- Verifica e risoluzione dei problemi di monitoraggio

Riferimento

Introduzione

Questo documento descrive i servizi, lo scopo e la risoluzione dei problemi di ISE.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza di Cisco Identity Services Engine.

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware specifiche di Cisco Identity Services Engine.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Cisco Identity Services Engine (ISE) è una soluzione completa progettata per fornire una sicurezza di rete avanzata tramite la gestione centralizzata delle policy, l'autenticazione, l'autorizzazione e l'accounting (AAA). Consente alle organizzazioni di gestire l'accesso alla rete per utenti, dispositivi e applicazioni, garantendo al contempo sicurezza, conformità e un'esperienza utente ottimale.

Per raggiungere questi obiettivi, Cisco ISE utilizza una serie di servizi, ognuno responsabile di attività specifiche che consentono al sistema di funzionare in modo efficiente. Questi servizi collaborano per garantire un accesso sicuro alla rete, l'applicazione efficace delle policy, la registrazione dettagliata, l'integrazione perfetta con i sistemi esterni e l'efficienza della profilatura dei dispositivi.

Ogni servizio di ISE svolge un ruolo fondamentale nel mantenimento dell'integrità e della disponibilità della soluzione. Alcuni servizi gestiscono funzioni di base, ad esempio la gestione e l'autenticazione del database, mentre altri attivano funzionalità avanzate quali la profilatura dei dispositivi, la gestione dei certificati e il monitoraggio.

In questo documento viene fornita una panoramica dei vari servizi di Cisco ISE, spiegandone lo scopo, l'importanza e le possibili procedure di risoluzione dei problemi in caso di problemi. La comprensione di questi servizi, che si tratti di un amministratore o di un professionista della sicurezza della rete, contribuisce a garantire un'implementazione efficiente e sicura di ISE.

Descrizione e risoluzione dei problemi dei servizi ISE

I servizi menzionati nello screenshot sono utilizzati da ISE per supportarne la funzionalità. Verificare lo stato o i servizi disponibili in ISE utilizzando il comando show application status ise dalla CLI del nodo ISE. Di seguito è riportato un esempio di output che mostra lo stato dei servizi disponibili sull'ISE.

```
honey/admin#show application status ise

ISE PROCESS NAME                       STATE            PROCESS ID
--------------------------------------------------------------------
Database Listener                      running          4101512
Database Server                        running          107 PROCESSES
Application Server                     running          4118209
Profiler Database                      running          4108739
ISE Indexing Engine                    running          4119606
AD Connector                           running          4121671
M&T Session Database                   running          4114154
M&T Log Processor                      running          4118388
Certificate Authority Service          running          4121560
EST Service                            running          61939
SXP Engine Service                     disabled
TC-NAC Service                         disabled
PassiveID WMI Service                  disabled
PassiveID Syslog Service               disabled
PassiveID API Service                  disabled
PassiveID Agent Service                disabled
PassiveID Endpoint Service             disabled
PassiveID SPAN Service                 disabled
DHCP Server (dhcpd)                    disabled
DNS Server (named)                     disabled
ISE Messaging Service                  running          4105571
ISE API Gateway Database Service       running          4107770
ISE API Gateway Service                running          4113275
ISE pxGrid Direct Service              running          36228
Segmentation Policy Service            disabled
REST Auth Service                      disabled
SSE Connector                          disabled
Hermes (pxGrid Cloud Agent)            disabled
McTrust (Meraki Sync Service)          disabled
ISE Node Exporter                      running          4122893
ISE Prometheus Service                 running          4124896
ISE Grafana Service                    running          4128455
ISE MNT LogAnalytics Elasticsearch     running          4130784
ISE Logstash Service                   running          4135868
ISE Kibana Service                     running          4137540
ISE Native IPSec Service               running          4142286
MFC Profiler                           running          52667
```

Servizi disponibili ad ISE.

A questo punto è possibile esaminare ogni servizio in modo più dettagliato.

Listener del database

Il servizio Database Listener è un componente critico che consente di gestire la comunicazione tra ISE e il server di database. Ascolta ed elabora le richieste relative al database, assicurandosi che il sistema ISE sia in grado di leggere e scrivere nel database sottostante.

Punti chiave del servizio di listener del database in ISE

1. Interfaccia di comunicazione: Funge da ponte di comunicazione tra ISE e il server di database, consentendo al sistema di recuperare e memorizzare dati come le credenziali utente, le informazioni sulla sessione, i criteri di rete e altro ancora.

2. Supporto database esterno: È possibile configurare ISE in modo che utilizzi un database esterno, ad esempio Oracle o Microsoft SQL Server, per l'autenticazione degli utenti e la memorizzazione delle policy. Il servizio di listener del database garantisce che ISE sia in grado di connettersi e interagire con il database esterno in modo sicuro ed efficiente.

3. Gestione dei dati: Il servizio resta in ascolto delle query del database dal sistema ISE e le traduce nelle azioni appropriate sul database esterno. Può gestire richieste quali l'inserimento, l'aggiornamento o l'eliminazione di record, nonché il recupero di informazioni dal database.

4. Monitoraggio dello stato del database: Oltre a fornire il canale di comunicazione, contribuisce anche a garantire che la connessione al database esterno sia stabile e funzionante. Se la connessione non riesce, ISE torna allo storage locale o entra in una modalità degradata a seconda della configurazione.

Server di database

Il servizio Database Server è responsabile della gestione dello storage e del recupero dei dati utilizzati dal sistema. Gestisce l'interazione con il database sottostante che ISE utilizza per archiviare la configurazione, le informazioni sulle policy, i dati utente, i log di autenticazione, i profili dei dispositivi e altre informazioni necessarie.

Punti chiave del servizio Database Server in ISE

1. Memorizzazione interna dei dati: Il servizio Database Server gestisce principalmente il database interno incorporato utilizzato da ISE per archiviare localmente i dati operativi. Sono inclusi dati quali i record di autenticazione e autorizzazione, i profili utente, i criteri di accesso alla rete, le informazioni su dispositivi ed endpoint e le informazioni sulla sessione.

2. Database incorporato: Nella maggior parte delle implementazioni Cisco ISE, il sistema usa un database PostgreSQL incorporato per l'archiviazione locale. Il servizio Database Server garantisce il corretto funzionamento del database e gestisce tutte le query, gli aggiornamenti e le attività di gestione relative ai dati archiviati al suo interno.

3. Integrità del database: Il servizio garantisce che tutte le transazioni vengano elaborate

correttamente e che venga mantenuta l'integrità del database. Gestisce attività quali il blocco dei record, la gestione delle connessioni al database e l'esecuzione di query sul database.

Verificare e risolvere i problemi relativi all'inizializzazione o alla mancata esecuzione dei servizi del listener e del server di database

Il listener del database e il server del database sono servizi essenziali che devono essere eseguiti insieme affinché tutti gli altri servizi funzionino correttamente. Se questi servizi non sono in esecuzione o sono bloccati durante l'inizializzazione, le operazioni di risoluzione dei problemi descritte di seguito consentono di eseguire il ripristino.

1. Riavviare i servizi ISE utilizzando i comandi application stop ise e application start ise.

2. Se si tratta di un nodo VM, il riavvio del nodo dalla VM deve facilitare il ripristino dei servizi.

3. Se il nodo è un nodo fisico, il riavvio/ricaricamento del nodo da CIMC deve facilitare il ripristino dei servizi.

4. Se il database è danneggiato, contattare Cisco TAC per ulteriori informazioni sulla risoluzione del problema.

Il listener del database e il server del database in genere non funzionano o non si avviano quando si verifica una discrepanza nel database o quando il database non può essere inizializzato correttamente. In questi casi, l'esecuzione del comando application reset-config ise per la reimpostazione dell'applicazione deve facilitare il ripristino e l'avvio del database. L'esecuzione del comando application reset-config ise rimuove le configurazioni e i certificati, ma i dettagli relativi all'indirizzo IP e al nome di dominio vengono mantenuti. Prima di applicare il comando su qualsiasi nodo della distribuzione, si consiglia di contattare Cisco TAC per ulteriori informazioni e per comprendere il potenziale impatto.

Server applicazioni

Application Server è un componente chiave responsabile dell'esecuzione e della gestione delle funzionalità e dei servizi principali della piattaforma ISE. Ospita la regola business, le interfacce utente e i servizi che consentono a ISE di svolgere il proprio ruolo nel controllo dell'accesso alla rete, nell'autenticazione, nell'autorizzazione, nella contabilità e nella gestione delle policy.

Punti chiave del servizio Application Server in ISE

1. Interfaccia utente: Application Server Service è responsabile del rendering dell'interfaccia utente basata sul Web (UI) per ISE. Questo consente agli amministratori di configurare e gestire le policy, visualizzare log e report e interagire con altre funzionalità di ISE.

2. Gestione dei servizi: È responsabile della gestione dei diversi servizi forniti da ISE, tra cui gestione delle policy, attività amministrative e comunicazione con altri nodi ISE in un'implementazione distribuita.

3. Elaborazione centralizzata: Il servizio Application Server svolge un ruolo centrale

nell'architettura ISE, fornendo la logica che interpreta le policy, le richieste di autenticazione e i dati provenienti da dispositivi di rete, directory e servizi esterni.

Verifica per Application Server in corso di inizializzazione o non in esecuzione

Il server applicazioni dipende da poche applicazioni Web, ad esempio certificati, risorse, distribuzione, licenze. Quando si verifica un errore di inizializzazione di una delle applicazioni Web, il server applicazioni rimane bloccato nello stato di inizializzazione. Il server applicazioni impiega da 15 a 35 minuti circa per passare da **Non in esecuzione** → **Inizializzazione** → **In esecuzione** a seconda dei dati di configurazione sul nodo.

1. Verificare che il certificato di amministrazione di ISE sia valido e attivo nella distribuzione per tutti i nodi.
2. Verificare che tutti i nodi nella distribuzione siano sincronizzati con il nodo Amministratore primario.
3. Se il nodo è una VM, verificare che le risorse consigliate siano allocate al nodo.

Verificare lo stato del server applicazioni utilizzando il comando **show application status ise** dalla CLI del nodo ISE. La maggior parte dei log relativi al server applicazioni sono disponibili in

File Catalina.Out e Localhost.log.

Se le condizioni indicate sono soddisfatte e il server applicazioni rimane bloccato nello stato di inizializzazione, proteggere il bundle di supporto dalla CLI / GUI di ISE. Ripristinare/riavviare i servizi utilizzando i comandi application stop ise e application start ise.

Database profiler

Database profiler è un database specializzato utilizzato per archiviare informazioni su dispositivi di rete, endpoint e profili di dispositivo individuati dal servizio Profiler. Il Profiler è un componente critico di ISE che identifica e classifica automaticamente i dispositivi di rete (come computer, smartphone, stampanti, dispositivi IoT e così via) in base alle caratteristiche e ai comportamenti della rete.

Punti chiave del servizio database Profiler in ISE

1. Creazione profilo dispositivo: La funzione principale del servizio di database del profiler è il supporto del processo di profiling. ISE utilizza questo servizio per archiviare le informazioni raccolte durante la profilatura, ad esempio:

- Tipo di dispositivo (ad esempio: smartphone, laptop, stampante, dispositivo IoT)
- Sistema operativo del dispositivo (ad esempio: Windows®, macOS®, Cisco IOS®, Android®
- Produttore dispositivo
- Comportamenti o modelli di rete che semplificano la classificazione dei dispositivi

2. Informazioni sul profiler: Memorizza attributi del profiler come i profili hardware e software dei dispositivi, che vengono utilizzati per abbinare i dispositivi ai criteri predefiniti. Queste informazioni vengono usate anche per assegnare dinamicamente i dispositivi alle policy di accesso alla rete o alle VLAN corrette in base al loro profilo.

3. Processo di profilatura: Il processo di creazione dei profili si basa in genere su:

- Profilatura attiva: ISE richiede attivamente informazioni ai dispositivi di rete.
- Profilatura passiva: ISE raccoglie passivamente dati dal traffico di rete, come richieste DHCP, attributi RADIUS, intestazioni HTTP e altri protocolli di rete, per determinare il tipo di dispositivo.

Verifica e risoluzione dei problemi di ISE Profiling Services

1. Dalla CLI di ISE, eseguire il comando show application status ise per verificare che il servizio del database del profiler sia in esecuzione.

2. Dalla GUI del nodo Amministratore principale, passare ad Amministrazione > Distribuzione > selezionare il nodo. Fare clic su Modifica e verificare che i servizi sessione e i servizi di profiling siano abilitati.

3. Passare a Amministrazione > Distribuzione > Selezionare il nodo. Passare alla configurazione del profiler e verificare se le richieste di verifica sono abilitate per la protezione dei dati degli endpoint.

4. Passare a Amministrazione > Sistema > Creazione profilo e verificare le impostazioni del profiler configurate per CoA.

5. Da Visibilità contesto > Endpoint > Selezionare gli endpoint e verificare gli attributi raccolti dalle diverse richieste per gli endpoint.

Debug utili per la risoluzione dei problemi di profilatura:

- profiler (profiler.log)
- runtime-AAA (prt-server.log)
- nsf (ise-psc.log)
- sessione nsf (ise.psc.log)

ISE Indexing Engine

Indexing Engine è un servizio responsabile dell'efficienza delle operazioni di ricerca, indicizzazione e recupero dei dati memorizzati nel database ISE. Migliora le prestazioni e la scalabilità di ISE, in particolare per quanto riguarda la gestione di grandi volumi di dati e l'accesso rapido alle informazioni necessarie per le attività di autenticazione, autorizzazione, monitoraggio e creazione di report.

Punti chiave del motore di indicizzazione ISE in ISE

1. Indicizzazione dei dati: Il motore di indicizzazione ISE crea indici per vari tipi di dati memorizzati in ISE, come log di autenticazione, log di sessione, accessi alle policy, dati di profilatura e record di accesso alla rete. L'indicizzazione consente di organizzare questi dati in modo da rendere più efficienti le operazioni di ricerca e di query.

2. Gestione dei registri e creazione di rapporti: Questo servizio svolge un ruolo critico nella gestione dei registri migliorando le prestazioni delle query di report e di registro. Ad esempio,

durante la ricerca di eventi di autenticazione specifici, il motore di indicizzazione consente il recupero più rapido dei record desiderati, fondamentale per il monitoraggio della sicurezza e il reporting di conformità.

3.Recupero dei dati: Il motore di indicizzazione è inoltre responsabile di garantire che ISE possa recuperare in modo efficiente i dati indicizzati dal database sottostante quando necessario. Ciò consente ad ISE di fornire risposte rapide alle richieste provenienti dall'interfaccia utente, da strumenti esterni o da API.

Verificare che il motore di indicizzazione ISE non sia in esecuzione o in fase di inizializzazione

1. Verificare che le ricerche DNS dirette e inverse funzionino per tutti i nodi del cluster tramite CLI utilizzando il comando **nslookup <FQDN / IP address of the ISE node >**.
2. Verificare che i certificati di amministratore ISE siano validi e attivi per tutti i nodi del cluster.
3. Verificare che NTP funzioni e sia sincronizzato con i nodi ISE tramite la CLI utilizzando il comando **show ntp**.

Il motore di indicizzazione viene utilizzato dal motore di visibilità del contesto e il motore di indicizzazione deve essere attivo e in esecuzione per consentire il funzionamento della visibilità del contesto. I log utili per la risoluzione dei problemi del motore di indicizzazione sono i file **ADE.log** che possono essere protetti dal bundle di supporto o gestiti dalla CLI usando il comando **show logging system ade/ADE.log tail** durante il problema.

Connettore AD

AD Connector (Active Directory Connector) è un servizio che consente l'integrazione di ISE con Microsoft Active Directory (AD), consentendo a ISE di autenticare, autorizzare e gestire gli utenti in base alle credenziali AD e all'appartenenza ai gruppi. Il connettore AD funge da ponte tra ISE e Active Directory, consentendo ad ISE di utilizzare AD per il controllo dell'accesso alla rete (NAC, Network Access Control) e l'applicazione delle policy.

Funzioni principali del servizio AD Connector in ISE

1. Integrazione con Active Directory: Il servizio AD Connector funge da ponte tra ISE e Active Directory. Consente ad ISE di connettersi in modo sicuro ad AD, rendendo possibile per ISE l'utilizzo di AD come archivio di identità centralizzato per l'autenticazione utente e l'applicazione delle policy.

2. Sincronizzazione: Il servizio AD Connector supporta la sincronizzazione dei dati di utenti e gruppi da Active Directory a ISE. Ciò garantisce che ISE disponga di informazioni aggiornate su utenti e gruppi, un elemento fondamentale per l'applicazione precisa della policy.

3. Comunicazioni sicure: Il servizio AD Connector stabilisce canali di comunicazione sicuri tra ISE e Active Directory, in genere utilizzando protocolli come LDAP su SSL (LDAPS) per garantire la privacy e l'integrità dei dati durante i processi di autenticazione e di query.

4. Supporto di più domini Active Directory: Il servizio può supportare connessioni a più domini Active Directory. Ciò è particolarmente utile in ambienti di grandi dimensioni o a più domini, dove ISE deve autenticare gli utenti da foreste o domini AD diversi.

5. Ricerca utenti e gruppi: Consente ad ISE di richiedere ad AD informazioni su utenti e gruppi. Possono includere dettagli quali i nomi utente, le appartenenze ai gruppi e altri attributi utente che possono essere utilizzati per applicare i criteri di accesso alla rete. Ad esempio, è possibile applicare criteri di accesso alla rete in base all'appartenenza a un gruppo AD di un utente (ad esempio: concedendo livelli di accesso diversi agli utenti di gruppi diversi).

1. Verificare che NTP sia sincronizzato con i nodi e che la differenza di tempo tra AD e ISE sia inferiore a 5 minuti.

2. Verificare se il server DNS è in grado di risolvere i nomi FQDN e i domini correlati ad Active Directory.

3. Passare a **Operazioni** > **Rapporti** > **Rapporti** > **Diagnostica** > **Operazioni connettore AD**, verificare gli eventi o i rapporti correlati ad AD.

I log utili per la risoluzione dei problemi sono **ad_agent.log** con i log di debug per il componente **runtime**.

Database sessione M&T

Il database delle sessioni di M&T (Monitoring and Troubleshooting Session Database) svolge un ruolo critico nell'archiviazione e nella gestione dei dati relativi alle sessioni per gli eventi di accesso alla rete. Il database delle sessioni M&T contiene informazioni sulle sessioni attive, tra cui le autenticazioni degli utenti, le connessioni dei dispositivi e gli eventi di accesso alla rete, che sono essenziali per il monitoraggio, la risoluzione dei problemi e l'analisi dell'attività di rete.

Funzioni principali del servizio di database delle sessioni M&T in ISE

1. Memorizzazione dei dati della sessione: Il servizio Database sessione M&T è responsabile dell'archiviazione e dell'indicizzazione dei dati relativi alle sessioni utente e dispositivo sulla rete. tra cui l'ora di inizio e di fine della sessione, i risultati dell'autenticazione, l'identità dell'utente o del dispositivo e i criteri associati (ad esempio le assegnazioni di ruoli o le assegnazioni VLAN). I dati includono inoltre informazioni di accounting RADIUS che descrivono in dettaglio il ciclo di vita della sessione, inclusa l'autenticazione iniziale e qualsiasi messaggio di accounting che tiene traccia degli eventi della sessione.

2. Dati storici e in tempo reale: Il servizio fornisce l'accesso ai dati delle sessioni in tempo reale (sessioni attive) e ai dati cronologici (sessioni passate). Ciò consente agli amministratori non solo di monitorare l'accesso continuo degli utenti, ma anche di esaminare i log delle sessioni precedenti per analizzare i problemi o convalidare gli eventi di accesso. Il monitoraggio in tempo reale delle sessioni permette di verificare che non vi siano dispositivi non autorizzati sulla rete.

3. Monitoraggio rafforzato: Informazioni dettagliate sull'attività di utenti e dispositivi, incluse le regole applicate alle relative sessioni, che consentono di rilevare potenziali problemi di sicurezza o accessi non autorizzati.

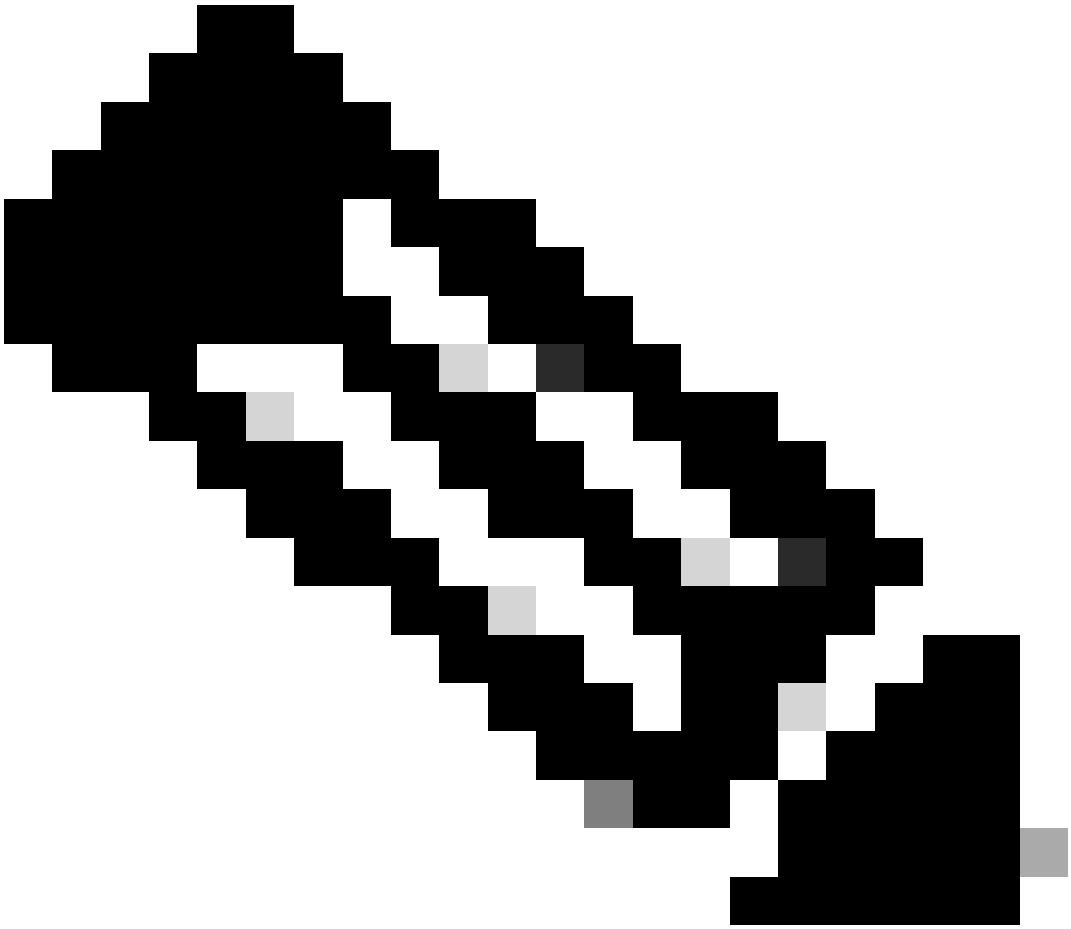
4. Revisione contabile e relazioni: Semplifica il controllo e la creazione di report sulla conformità archiviando la cronologia degli eventi di accesso alla rete e fornendo dati per la creazione di report normativi.

Verifica e risoluzione dei problemi per il database delle sessioni M&T in ISE

1. Verificare se il nodo è allocato con le risorse consigliate.

2. **Visualizzazione** sicura **del supporto tecnico** dalla CLI di ISE per ulteriori verifiche del problema.

3. Reimpostare il database della sessione M&T eseguendo il comando **application configure ise** nella CLI di ISE e selezionare l'opzione **1**.



> Nota: La reimpostazione del database M&T deve essere eseguita solo dopo la verifica dell'impatto potenziale nella distribuzione. Contattare Cisco TAC per ulteriori verifiche.

Difetti noti

Cisco bug ID ·32364

Processore log M&T

M&T Log Processor (Monitoring and Troubleshooting Log Processor) è un componente responsabile della raccolta, dell'elaborazione e della gestione dei dati dei log generati da vari

servizi all'interno di ISE. È una parte chiave del framework M&T (Monitoring and Troubleshooting), che aiuta gli amministratori a monitorare e risolvere gli eventi di accesso alla rete, i tentativi di autenticazione, l'applicazione delle policy e altre attività all'interno del sistema ISE. M&T Log Processor gestisce in modo specifico l'elaborazione delle voci di log, garantendo che ISE sia in grado di archiviare, analizzare e presentare le informazioni necessarie per la creazione di report, il controllo e la risoluzione dei problemi.

Funzioni principali del servizio M&T Log Processor in ISE

1. Raccolta ed elaborazione dei registri: Il servizio M&T Log Processor raccoglie ed elabora i log generati da vari componenti ISE, quali richieste di autenticazione, decisioni di autorizzazione, messaggi di accounting e attività di applicazione delle policy. Questi registri includono informazioni dettagliate su utenti, dispositivi e tentativi di accesso alla rete, quali timestamp, ID utente, tipi di dispositivi, criteri applicati, esito positivo o negativo delle richieste di accesso e motivi degli errori.

2. Comunicazione e conformità: I registri elaborati da questo servizio sono fondamentali per la creazione di report di conformità. Molte normative richiedono alle organizzazioni di conservare i registri degli accessi degli utenti e degli eventi relativi alla sicurezza. Il servizio di elaborazione dei log M&T garantisce che tutti i log rilevanti vengano elaborati e siano disponibili per i controlli di conformità alle normative. Consente di generare report dettagliati basati sui dati di log, ad esempio i log degli accessi utente, le percentuali di autenticazione riuscita/non riuscita o i log di applicazione delle policy.

Verifica e risoluzione dei problemi del servizio Processore di log M&T in ISE

1. Verificare che il nodo ISE sia distribuito con le risorse consigliate, come indicato nella Guida all'installazione di Cisco.

2. Per verificare il problema, eseguire il comando **show logging system ade/ADE.log tail** tramite ISE CLI per individuare le eccezioni o gli errori rilevanti.

Difetti noti

Cisco ID bug ·15130

Servizio Autorità di certificazione

Il servizio CA (Certification Authority) è un componente critico che consente di gestire i certificati digitali per proteggere le comunicazioni e autenticare dispositivi, utenti e servizi di rete. I certificati digitali sono essenziali per stabilire connessioni attendibili e garantire una comunicazione sicura tra client (computer, smartphone, dispositivi di rete) e componenti dell'infrastruttura di rete (switch, punti di accesso wireless, gateway VPN). Il servizio CA di Cisco ISE funziona in tandem con i certificati X.509, che vengono utilizzati per diversi scopi nella sicurezza di rete, tra cui l'autenticazione 802.1X, l'accesso VPN, la comunicazione protetta e la crittografia SSL/TLS.

Funzioni chiave del servizio Certification Authority in ISE

1. Gestione dei certificati: Il Servizio Autorità di certificazione è responsabile della creazione, del

rilascio, della gestione e del rinnovo dei certificati digitali in ISE. Questi certificati vengono utilizzati per vari protocolli di autenticazione e scopi di crittografia in rete. Può fungere da autorità di certificazione interna o integrarsi con un'autorità di certificazione esterna (ad esempio: Servizi certificati Active Directory Microsoft, CA pubbliche quali VeriSign o DigiCert) per il rilascio di certificati.

2. Rilascio dei certificati: Per gli ambienti che richiedono EAP-TLS o metodi di autenticazione basati su certificati simili, ISE può rilasciare certificati per dispositivi di accesso alla rete (NAD), utenti o endpoint. ISE può generare e distribuire automaticamente certificati per l'autenticazione di dispositivi e utenti oppure può richiedere certificati a una CA esterna.

3. Registrazione certificato: Il servizio CA supporta la registrazione dei certificati per gli endpoint, ad esempio laptop, telefoni e altri dispositivi di rete, che devono essere autenticati in rete utilizzando i certificati. ISE utilizza protocolli come SCEP (Simple Certificate Enrollment Protocol) o ACME (Automated Certificate Management Environment) per facilitare la registrazione dei certificati per i dispositivi.

4. Rinnovo certificato: Il servizio automatizza il rinnovo dei certificati in scadenza per i dispositivi e gli utenti. Garantisce che i certificati siano sempre validi e aggiornati, impedendo interruzioni del servizio causate da certificati scaduti.

5. Integrazione con autorità di certificazione esterne: mentre ISE può agire come una propria CA, è più comune integrarsi con una CA esterna (ad esempio: Servizi certificati Microsoft Active Directory). Il Servizio CA può gestire l'interazione tra ISE e la CA esterna, richiedendo certificati per utenti, dispositivi e risorse di rete, se necessario.

Servizio EST

Enrollment over Secure Transport (EST) Service è un protocollo utilizzato per l'emissione sicura di certificati digitali a dispositivi di rete e utenti in un ambiente di autenticazione basato su certificati. EST è un protocollo di registrazione dei certificati che consente ai dispositivi di richiedere certificati a un'Autorità di certificazione (CA) in modo sicuro e automatico. Il servizio EST è particolarmente utile per l'autenticazione dei dispositivi, ad esempio in ambienti 802.1X, connessioni VPN o scenari BYOD (Bring Your Own Device), in cui i dispositivi devono eseguire l'autenticazione alla rete utilizzando i certificati.

Funzioni principali del servizio EST ad ISE

1.Registrazione certificato: Il servizio EST è responsabile dell'abilitazione della registrazione sicura dei certificati per i dispositivi (quali switch, punti di accesso o endpoint) che richiedono certificati ai fini dell'autenticazione. La registrazione viene eseguita tramite un trasporto protetto (in genere HTTPS), garantendo che il processo sia crittografato e protetto da accessi non autorizzati.

2. Revoca e rinnovo del certificato: Una volta registrati i certificati, anche il servizio EST svolge un ruolo nella gestione della revoca o del rinnovo dei certificati. Ad esempio, i dispositivi devono richiedere un nuovo certificato alla scadenza di quello corrente e EST può aiutare ad automatizzare questo processo.

3. Miglioramento del controllo dell'accesso alla rete: Consentendo ai dispositivi di eseguire l'autenticazione tramite certificati, il servizio EST rafforza la postura di sicurezza della rete, in particolare negli ambienti che utilizzano l'autenticazione 802.1X.

Verificare che l'Autorità di certificazione e il servizio EST non siano in esecuzione o in fase di inizializzazione

1. Passare a **Amministrazione > Sistema > Certificati > Autorità di certificazione > Impostazioni CA interne.** Verificare che lo stato di CA, EST e Risponditore OCSP sia Ordinato e abilitato.
2. I debug utili per la risoluzione dei problemi sono i file set, provisioning, ca-service e ca-service-cert. Fare riferimento ai file **toise-psc.log, catalina.out, caservice.log** e **error.log**.
3. Verificare che i certificati ISE Root CA e ISE Messaging siano validi nell'implementazione. Se è richiesto il rinnovo dell'autorità di certificazione radice ISE, selezionare **Amministrazione > Certificati > Richieste di firma del certificato > Genera richiesta di firma del certificato,** quindi selezionare Uso come **autorità di certificazione radice ISE.** Fare clic su renew **ISE Root CA**.

Servizio motore SXP

Il servizio motore SXP è responsabile della gestione e della semplificazione della comunicazione tra ISE e i dispositivi di rete mediante il codice di matricola (SGT) e il protocollo SXP (Security Group Exchange Protocol). Svolge un ruolo critico nel supporto dei criteri TrustSec, che vengono utilizzati per imporre il controllo dell'accesso alla rete in base al gruppo di sicurezza del dispositivo piuttosto che solo indirizzi IP o MAC. Il motore SXP di ISE viene utilizzato principalmente per lo scambio di informazioni sui gruppi di sicurezza, che aiutano a imporre i criteri in base all'identità, all'applicazione e alla posizione dell'utente o del dispositivo. Consente ai dispositivi di condividere i tag SGT (Security Group Tags), utilizzati per applicare i criteri di sicurezza ai dispositivi di rete, ad esempio router e switch.

Funzioni principali del servizio SXP Engine in ISE

1.Integrazione con TrustSec: SXP viene comunemente implementato in ambienti che utilizzano Cisco TrustSec, una soluzione che applica policy di sicurezza coerenti su reti cablate e wireless. SXP Engine facilita la comunicazione di SGT tra i dispositivi, consentendo l'applicazione dinamica delle policy in base al contesto di sicurezza di un dispositivo o utente.

2. Codici di matricola del gruppo di sicurezza (SGT): Il nucleo centrale dell'applicazione delle politiche di TrustSec è costituito dalle SGT. Questi tag vengono utilizzati per classificare il traffico di rete e il protocollo SXP consente di condividere la mappatura di questi tag con utenti o dispositivi specifici. Ciò consente un controllo granulare e basato su regole dell'accesso alla rete e del flusso del traffico.

Verifica e risoluzione dei problemi per il servizio motore SXP a ISE

1. Per impostazione predefinita, il servizio SXP Engine è disabilitato in ISE. Per abilitarlo, andare alla **GUI ISE > Amministrazione > Distribuzione, selezionare il nodo. Selezionare la casella Enable SXP Service** (Abilita servizio SXP), quindi scegliere l'interfaccia. Quindi, verificare lo stato del servizio SXP Engine dalla CLI di ISE usando il comando **show application status ise.**

2.In caso di problemi di comunicazione di rete, verificare che l'interfaccia assegnata al motore SXP abbia un indirizzo IP valido utilizzando il comando show interface nella CLI e verificare che la subnet IP sia consentita nella rete.

3. Controllare i registri RADIUS per verificare gli eventi di connessione SXP su ISE.

4.Abilitare il componente SXP sui nodi ISE per eseguire il debug e acquisire i registri e le eccezioni relativi a SXP.

Servizio TC-NAC

Il servizio TC-NAC (TrustSec Network Access Control) è un componente che facilita l'applicazione dei criteri TrustSec sui dispositivi di rete, garantendo che il controllo dell'accesso sia basato sui Security Group Tags (SGT) anziché sugli indirizzi IP o MAC tradizionali.

TrustSec è a sua volta un framework sviluppato da Cisco che consente l'applicazione di policy di sicurezza in tutta la rete in base a ruoli, utenti o contesti dei dispositivi, anziché utilizzare meccanismi legacy come VLAN o indirizzi IP. Fornisce un controllo dell'accesso alla rete più granulare e dinamico raggruppando i dispositivi in diversi gruppi di sicurezza e contrassegnandoli con SGT.

Funzioni principali del servizio TC-NAC in ISE

1. Integrazione con sistemi NAC di terze parti: Il servizio TC-NAC consente ad ISE di comunicare e interagire con soluzioni di terze parti per il controllo degli accessi alla rete. Questa funzionalità può essere utile per le organizzazioni che hanno già implementato l'infrastruttura NAC ma desiderano integrarla con Cisco ISE per migliorarne le funzionalità, applicare policy di sicurezza aggiuntive o sfruttare altre funzionalità di sicurezza della rete Cisco.

2. Garantire Un'Applicazione Ininterrotta Delle Politiche: Se integrata con soluzioni NAC di terze parti, ISE può assumere il controllo su alcuni aspetti dell'applicazione delle policy e del processo decisionale. Ciò consente una struttura di policy più unificata, garantendo che le policy applicate dai sistemi Cisco e non Cisco NAC siano coerenti sull'intera rete.

3. Supporto per sistemi NAC legacy: Il servizio TC-NAC aiuta le aziende che dispongono di sistemi NAC legacy a continuare a utilizzare tali sistemi adottando Cisco ISE per le funzionalità di sicurezza avanzate. ISE può integrarsi con le precedenti soluzioni NAC ed estenderne il ciclo di vita, fornendo in tandem il controllo dell'accesso, la sicurezza e l'applicazione della conformità.

4. Facilitare la comunicazione con i fornitori NAC di terze parti: Questo servizio consente ad ISE di facilitare la comunicazione con soluzioni NAC di terze parti che utilizzano protocolli o standard proprietari. ISE può interagire con i sistemi NAC di terze parti tramite protocolli standard (come RADIUS, TACACS+ o SNMP) o API personalizzate, a seconda della soluzione NAC utilizzata.

Verifica e risoluzione dei problemi del servizio TC-NAC in ISE

1. Verificare che il NAC incentrato sulle minacce sia abilitato selezionando **Amministrazione > Distribuzione > nodo PSN > Abilita NAC incentrato sulle minacce**.

2. Se il problema riguarda la scheda SourceFire FireAMP, verificare se è consentita la **porta 443** nella rete.

3. Verificare i dettagli della sessione dell'endpoint da **Operations > Threat-Centric NAC Live Logs.**

Allarmi attivati dal NAC incentrato sulla minaccia:

- Scheda non raggiungibile (ID syslog: 91002): Indica che non è possibile raggiungere la scheda.
- Connessione scheda non riuscita (ID syslog: 91018): Indica che la scheda è raggiungibile ma la connessione tra la scheda e il server di origine non è attiva.
- Scheda arrestata a causa di un errore (ID syslog: 91006): Questo allarme viene attivato se la scheda di rete non si trova nello stato desiderato. Se viene visualizzato questo avviso, controllare la configurazione della scheda e la connettività del server. Per ulteriori informazioni, consultare i registri dell'adattatore.
- Errore scheda (ID syslog: 91009): Indica che l'adattatore Qualys non è in grado di stabilire una connessione o scaricare informazioni dal sito Qualys.

Debug utili per la risoluzione dei problemi del TC-NAC:

- va-runtime (varuntime.log)
- va-service (varuntime.log e vaaggregation.log)
- TC-NAC (ise-psc.log)
- anc (ise-psc.log)

Servizio WMI PassiveID

Il servizio WMI PassiveID è un servizio che consente ad ISE di eseguire la profilatura dei dispositivi utilizzando Strumentazione gestione Windows (WMI) come meccanismo passivo per l'identificazione e la profilatura degli endpoint nella rete. Svolge un ruolo cruciale nella profilatura dei dispositivi, in particolare negli ambienti in cui i dispositivi che eseguono il sistema operativo Windows devono essere identificati con precisione per il controllo dell'accesso alla rete e l'applicazione delle policy.

Funzioni chiave del servizio WMI PassiveID in ISE

1. Raccolta identità dispositivo: Il servizio WMI PassiveID consente ad ISE di raccogliere passivamente informazioni sull'identità dai dispositivi Windows tramite Strumentazione gestione Windows (WMI). Raccoglie dettagli di sistema quali il nome host del dispositivo, la versione del sistema operativo e altri attributi rilevanti senza richiedere la partecipazione attiva del dispositivo.

2. Integrazione con ISE Policy: Le informazioni raccolte dal servizio WMI PassiveID sono integrate nel framework della policy ISE. Consente l'applicazione dinamica di regole basate su attributi dei dispositivi quali tipo, sistema operativo e conformità agli standard di sicurezza.

Verifica e risoluzione dei problemi del servizio WMI PassiveID

Una fonte estremamente sicura e precisa, nonché la più comune, da cui ricevere informazioni sugli utenti. In qualità di probe, AD utilizza la tecnologia WMI per fornire identità utente autenticate. Inoltre, AD stesso, anziché la probe, funge da sistema di origine (un provider) da cui anche altri probe recuperano i dati utente.

Debug e informazioni utili necessari per la risoluzione dei problemi. Impostare questi attributi sul livello di debug per i problemi relativi a WMI PassiveID:

- ID passivo (passiveid*)
- registrazione in fase di esecuzione (prrt-server.log)
- Active Directory (ad)_agent.log) - Livello di traccia
- collector (collector.log) (su PassiveID, nodi MnT e su nodo pxGrid attivo se le sessioni sono pubblicate)
- pxGrid (pxgrid/) (sul nodo MnT secondario e sul nodo pxGrid attivo se le sessioni sono pubblicate)

Informazioni necessarie per la risoluzione dei problemi relativi a WMI PassiveID:

1. Che funzionasse prima? Qualsiasi modifica apportata di recente. (come per l'aggiornamento, installazione di patch su ISE/aggiornamento su CD)
2. La connessione di test funziona correttamente (prima dell'integrazione, verificare la connessione di test)
3. Dettagli sul nome utente utilizzato per l'aggiunta ad AD e sul nome utente utilizzato per WMI (account amministratore o non amministratore)
4. Verificare se sono registrati gli eventi (4768, 4770) nel controller di dominio. (Registro visualizzatore eventi dal controller di dominio)
5. Registri acquisiti: Impostare il livello di debug per la registrazione in fase di esecuzione e l'ID passivo, quindi configurare wmi per il controller di dominio specifico, AD - livello di traccia con timestamp.

Servizio syslog ID passivo

Il servizio Syslog ID passivo è un servizio che consente alla funzionalità di profiling ID passivo di raccogliere ed elaborare messaggi syslog da dispositivi di rete nell'ambiente. Questi messaggi syslog contengono informazioni importanti sugli endpoint connessi alla rete e ISE li utilizza per profilare questi dispositivi per il controllo dell'accesso alla rete e l'applicazione delle policy.

Funzioni chiave del servizio Syslog ID passivo

1. Autenticazione passiva: Il servizio Syslog ID passivo consente a Cisco ISE di autenticare passivamente utenti e dispositivi raccogliendo messaggi syslog da dispositivi di rete (come switch o router) che indicano l'attività di utenti e dispositivi. Ciò è utile in situazioni in cui i metodi di autenticazione attivi tradizionali, come 802.1X, non sono adatti o fattibili.

2. Registrazione degli eventi: Il servizio Syslog ID passivo si basa sul protocollo syslog per ricevere i log dai dispositivi di rete che registrano l'accesso e il comportamento degli utenti sulla rete. Le informazioni contenute in questi log possono includere cose come i tentativi di login del

dispositivo, i punti di accesso e i dettagli dell'interfaccia, che aiutano ISE a identificare passivamente il dispositivo o l'utente.

Servizio API PassiveID

Il servizio API PassiveID è un servizio che consente l'integrazione con i sistemi che richiedono informazioni sull'identità dei dispositivi o degli utenti connessi alla rete. Viene in genere utilizzato in ambienti in cui gli amministratori di rete desiderano eseguire azioni e policy basate sull'identità senza richiedere protocolli di autenticazione di rete attivi, ad esempio 802.1X per ogni dispositivo.

Funzioni chiave del servizio API ID passivo

1. Integrazione con i sistemi esterni: L'API ID passivo consente ad ISE di ricevere informazioni sull'identità da sistemi o dispositivi di rete di terze parti (come switch, router, firewall o qualsiasi sistema in grado di generare eventi relativi all'identità). Questi sistemi esterni possono inviare informazioni come messaggi syslog, log di autenticazione o altri dati che possono aiutare ISE a identificare passivamente un utente o un dispositivo.

2. Autenticazione passiva: Il servizio API ID passivo viene utilizzato per autenticare utenti e dispositivi in modo passivo raccogliendo dati di identità senza richiedere l'autenticazione attiva (ad esempio: nessuna necessità di autenticazione 802.1X, MAB o Web). Ad esempio, può acquisire informazioni da dispositivi di rete, registri di Active Directory o appliance di sicurezza e utilizzarle per identificare l'utente o il dispositivo.

3. Mappatura delle informazioni sull'identità: L'API ID passivo può essere utilizzata per mappare i dati di identità a criteri di sicurezza specifici. Queste informazioni vengono utilizzate per assegnare dinamicamente i tag o i ruoli dei gruppi di sicurezza a utenti e dispositivi, influendo quindi sull'applicazione dei controlli di accesso alla rete, ad esempio i criteri di segmentazione e firewall.

Servizio Agente ID passivo

Il servizio Agente ID passivo è un servizio che consente la profilatura dei dispositivi tramite l'utilizzo di Agenti ID passivi installati sugli endpoint (ad esempio computer, laptop, dispositivi mobili e così via). L'agente PassiveID consente ad ISE di raccogliere informazioni di profiling sui dispositivi della rete ascoltando il traffico proveniente dagli endpoint, senza bisogno di scansioni attive o interazioni dirette con i dispositivi.

Funzioni chiave del servizio Agente ID passivo

1. Identificazione passiva dell'utente e del dispositivo: Il servizio Passive ID Agent è responsabile della raccolta passiva delle informazioni sull'identità, in genere da dispositivi di rete o endpoint, e dell'invio di questi dati ad ISE. Questo servizio consente ad ISE di autenticare e identificare utenti e dispositivi in base alle loro attività o caratteristiche, senza bisogno di un'autenticazione attiva da parte del dispositivo (ad esempio: senza credenziali 802.1X fornite).

2. Integrazione con altri componenti Cisco: L'agente ID passivo lavora a stretto contatto con i dispositivi di rete Cisco, come switch, controller wireless e punti di accesso, per raccogliere

informazioni relative all'identità dal traffico di rete, dai log di syslog o da altri sistemi di gestione. Può inoltre essere integrato con Cisco TrustSec e Cisco Identity Services per mappare questi dati a tag Security Group (SGT) specifici o ad altri criteri basati sull'identità.

3. Controllo degli accessi contestuale alla rete: L'agente ID passivo invia queste informazioni a Cisco ISE, che quindi applica le policy di controllo dell'accesso appropriate in base all'identità e al contesto dell'utente o del dispositivo. Ciò può includere:

- Controllo degli accessi basato sui ruoli.
- Assegnazione VLAN dinamica.
- Segmentazione della rete.
- Applicazione dei criteri di sicurezza in base al ruolo utente o alla postura di sicurezza del dispositivo.

Servizio endpoint ID passivo

Il servizio Endpoint PassiveID è un servizio responsabile dell'identificazione e della profilatura degli endpoint (dispositivi) sulla rete basata sulla tecnologia PassiveID. Questo servizio aiuta ISE a raccogliere, elaborare e classificare le informazioni sui dispositivi che si connettono alla rete, senza richiedere l'interazione attiva con gli endpoint stessi. Il servizio Endpoint ID passivo svolge un ruolo critico nella creazione di profili, nel controllo dell'accesso alla rete e nell'applicazione dei criteri di sicurezza.

Funzioni chiave di PassiveID Endpoint Service

1. Identificazione passiva dell'utente e del dispositivo: Il servizio PassiveID Endpoint consente a Cisco ISE di identificare e autenticare i dispositivi sulla rete in modo passivo, utilizzando le informazioni tratte dalle attività di rete o dai log di sistema. Ciò include l'identificazione di utenti e dispositivi in base al comportamento o alle caratteristiche della rete, ad esempio indirizzo MAC, indirizzo IP o informazioni di accesso da un archivio identità esterno come Active Directory (AD).

2. Raccolta dei dati dagli endpoint: Il servizio endpoint raccoglie vari tipi di dati specifici dell'endpoint da origini diverse:

- Informazioni di accesso utente da archivi identità esterni come Active Directory o altre directory.
- Caratteristiche del dispositivo quali indirizzi IP, indirizzi MAC e tipo di dispositivo (ad esempio: se il dispositivo è un PC Windows, un telefono cellulare o un dispositivo IoT).
- Attività della rete dell'endpoint, ad esempio richieste DHCP, richieste ARP e altre comunicazioni a livello di rete.

Servizio SPAN ID passivo

Il servizio SPAN PassiveID è un servizio che sfrutta il mirroring delle porte SPAN (Switched Port Analyzer) sui dispositivi di rete per acquisire e analizzare il traffico di rete per la profilatura degli endpoint. Questo servizio aiuta ISE a raccogliere passivamente informazioni sugli endpoint (dispositivi) sulla rete analizzandone i modelli di comunicazione senza richiedere sonde attive o

agenti installati sui dispositivi stessi.

Funzioni chiave del servizio SPAN ID passivo

1. Raccolta passiva delle identità dal traffico SPAN: Il servizio SPAN PassiveID consente ad ISE di raccogliere dati di identità in base al traffico di rete di cui viene eseguito il mirroring o la copia tramite una porta SPAN su uno switch. Una porta SPAN viene in genere utilizzata per il monitoraggio della rete mediante il mirroring del traffico di rete da altre porte o VLAN. L'acquisizione di questo traffico consente ad ISE di raccogliere passivamente informazioni sull'identità, quali:

- Indirizzi MAC dei dispositivi.
- Indirizzi IP associati ai dispositivi.
- Richieste DHCP o altre informazioni relative all'identità provenienti dal traffico acquisito.
- Registri di autenticazione da dispositivi di rete, quali switch o controller wireless.

2. Acquisizione delle informazioni sull'identità di utenti e dispositivi: Il servizio SPAN ascolta essenzialmente il traffico che attraversa la rete e identifica le informazioni sull'identità delle chiavi provenienti dai pacchetti di rete senza dover interagire direttamente con i dispositivi. Ciò può includere dati quali:

- Identità utente quando vengono autenticati tramite protocolli quali EAP (Extensible Authentication Protocol).
- Identità dei dispositivi basate su indirizzi MAC e indirizzi IP.
- Ruoli e comportamenti dei dispositivi in base ai modelli di traffico e agli eventi osservati.

Verifica e risoluzione dei problemi per lo stack PassiveID (servizio SPAN PassiveID, servizio Syslog PassiveID, servizio Endpoint PassiveID, agente PassiveID, servizio API PassiveID)

1. Lo stack PassiveID è un elenco di provider e tutti i servizi nello stack PassiveID sono disabilitati per impostazione predefinita. Selezionare ISE GUI > Administration > Deployment > Select the node, Enable Passive Identity Service (Abilita servizio di identità passiva), quindi fare clic su Save (Salva). Per verificare lo stato del servizio dello stack di ID passivi, accedere alla CLI del nodo ISE ed eseguire il comando show application status ise.

2. In caso di problemi con l'agente ID passivo, verificare se l'FQDN dell'agente è risolvibile dal nodo ISE. Per eseguire questa operazione, accedere alla CLI di ISE ed eseguire il comando nslookup < FQDN dell'agente configurato >.

3. Verificare che il motore di indicizzazione ISE sia attivo e che le ricerche DNS inverse e inoltrate vengano risolte dal DNS o dal server dei nomi configurato in ISE.

4. Per garantire una comunicazione senza problemi con i provider di syslog, controllare che le porte UDP 40514 e TCP 11468 siano aperte nella rete.

5. Per configurare il provider SPAN su un nodo, verificare che il servizio ISE Passive Identity sia abilitato. Verificare che l'interfaccia che si desidera configurare sul provider SPAN sia disponibile in ISE, utilizzando il comando show interface dalla CLI di ISE.

Per controllare i registri, in base al provider di ID passivo, è necessario esaminare passiveid-syslog.log, passiveid-agent.log, passiveid-api.log, passiveid-endpoint.log, passiveid-span.log. I registri citati possono essere protetti dal bundle di supporto del nodo ISE.

Server DHCP (dhcpd)

Il servizio Server DHCP (dhcpd) è un servizio che fornisce funzionalità DHCP (Dynamic Host Configuration Protocol) ai dispositivi di rete. Viene utilizzato principalmente per assegnare indirizzi IP alle periferiche (endpoint) che tentano di connettersi alla rete. Ad ISE, il server DHCP svolge un ruolo cruciale nel fornire gli indirizzi IP agli endpoint che li richiedono quando si connettono alla rete. Il servizio può inoltre fornire informazioni di configurazione aggiuntive, ad esempio server DNS, gateway predefinito e altre impostazioni di rete.

Funzioni principali del servizio Server DHCP (dhcpd) in ISE

1. Allocazione dinamica degli indirizzi IP: Il servizio dhcpd di ISE funziona come server DHCP, che fornisce l'allocazione degli indirizzi IP ai dispositivi che richiedono un indirizzo IP quando si connettono alla rete. Questo è importante negli scenari in cui i dispositivi si uniscono alla rete in modo dinamico, ad esempio in ambienti BYOD (Bring Your Own Device) o quando i dispositivi vengono configurati per ottenere automaticamente i propri indirizzi IP.

2. DHCP basato sul profilo: Il servizio dhcpd può allocare gli indirizzi IP in base al profilo del dispositivo. Se il profilo del dispositivo è stato eseguito da ISE (ad esempio: determinando se si tratta di uno smartphone, un laptop, un dispositivo IoT), può assegnare un indirizzo IP appropriato o applicare altre impostazioni in base al tipo di dispositivo o ruolo.

3. Supporto dell'inoltro DHCP: ISE può funzionare come agente di inoltro DHCP, inoltrando le richieste DHCP dai dispositivi a un server DHCP esterno se ISE non gestisce l'assegnazione effettiva dell'indirizzo IP. In questo caso, il servizio dhcpd può inoltrare le richieste dei dispositivi a un server DHCP centrale, mentre ISE continua ad applicare le policy di rete e i controlli degli accessi.

Verifica e risoluzione dei problemi del server DHCP (dhcpd)

1. Contattare Cisco TAC per verificare se il pacchetto del server DHCP è installato sull'ISE.

2. Accedere alla radice di **ISE > rpm -qi dhcp**.

Server DNS (denominato)

Il servizio Server DNS (denominato) è un servizio che consente a ISE di fungere da server DNS (Domain Name System) o da risolutore DNS. È principalmente responsabile della risoluzione dei nomi di dominio in indirizzi IP e viceversa, facilitando la comunicazione tra i dispositivi nella rete.

Funzioni chiave del servizio Server DNS (con nome) in ISE

1. Risoluzione DNS per la comunicazione ISE: Il servizio denominato in ISE aiuta a risolvere i

nomi di dominio in indirizzi IP. Ciò è particolarmente importante quando ISE deve connettersi ad altri dispositivi di rete o servizi esterni (come server Radius, Active Directory o server NTP esterni) usando nomi di dominio anziché indirizzi IP.

- Ad esempio, quando ISE deve raggiungere un server Radius o un servizio di directory esterno (come Active Directory), deve risolvere il nome di dominio del server in un indirizzo IP.
- ISE esegue query sul server DNS configurato nel sistema per risolvere i nomi di dominio, garantendo una comunicazione ottimale.

2. Risoluzione DNS per i servizi esterni: Il servizio DNS consente ad ISE di connettersi a servizi esterni che richiedono nomi di dominio. Ad esempio, ISE deve risolvere i nomi dei servizi esterni, come:

- Servizi basati su cloud.
- Server NTP (Network Time Protocol).
- CA o server LDAP.

3. Server DNS multidominio e ridondanti: È possibile configurare ISE in modo che utilizzi più server DNS per la ridondanza. Nel caso in cui un server DNS diventi non disponibile, ISE può eseguire il fallback su un altro server DNS per garantire un funzionamento continuo e la risoluzione DNS.

Verifica e risoluzione dei problemi per il server DNS (denominato)

1. Dalla CLI del nodo ISE, verificare la raggiungibilità al server dei nomi o al server DNS della distribuzione usando il comando **ping <IP del server DNS / server dei nomi>**.

2. Verificare la risoluzione DNS degli FQDN ISE utilizzando il comando **nslookup <FQDN / indirizzo IP dei nodi ISE>** dalla CLI di ISE.

ISE Messaging Service

Il servizio di messaggistica ISE è un componente che semplifica la comunicazione asincrona tra i vari servizi e componenti del sistema ISE. Svolge un ruolo cruciale nell'architettura di sistema complessiva di ISE, consentendo a diverse parti della piattaforma di inviare e ricevere messaggi, gestire attività e sincronizzare attività.

Funzioni principali del servizio di messaggistica ISE

1. Comunicazione interprocesso (IPC): Il servizio di messaggistica ISE svolge un ruolo chiave nell'attivazione della comunicazione interprocesso (IPC) tra diversi servizi ISE. Assicura che i diversi moduli e servizi ISE, come l'autenticazione, l'autorizzazione e l'applicazione delle policy, possano scambiare dati e istruzioni in modo coordinato.

2. Supporto per ambienti distribuiti: In implementazioni ISE più grandi o distribuite (ad esempio in configurazioni a più nodi o ad alta disponibilità), il servizio di messaggistica agevola la comunicazione tra i vari nodi ISE. Ciò garantisce che i dati, come le richieste di autenticazione, le

sessioni utente e gli aggiornamenti delle policy, siano sincronizzati correttamente sui diversi nodi del sistema ISE.

3. Sincronizzazione criteri e configurazione: Il servizio di messaggistica è coinvolto nella sincronizzazione di configurazioni e policy tra i nodi ISE. Quando vengono apportate modifiche alla configurazione di un nodo primario, il servizio garantisce che tali modifiche vengano propagate ai nodi secondari o di backup del sistema. Ciò è essenziale per mantenere la coerenza e garantire che le policy di accesso alla rete applicate in diverse posizioni o nodi ISE distribuiti rimangano sincronizzate.

Verificare che il servizio di messaggistica ISE non sia in esecuzione o in fase di inizializzazione

1. Verificare che la porta TCP 8671 non sia bloccata nel firewall, in quanto questa porta è utilizzata per la comunicazione tra i nodi tra i dispositivi ISE.

2. Verificare la presenza di errori nel collegamento alla coda e, in caso affermativo, rinnovare i certificati ISE Messaging e ISE Root CA in quanto gli errori del collegamento alla coda si verificherebbero in genere a causa di problemi di danneggiamento del certificato interno. Per risolvere gli errori di collegamento alla coda, rinnovare il certificato ISE Messaging e ISE Root CA facendo riferimento all'articolo : ISE- Queue Link Error

3. Da GUI -> Amministrazione -> Certificati -> Selezionare ISE Messaging Certificate. Fare clic su Visualizza per verificare lo stato del certificato.

I log utili per risolvere i problemi del servizio di messaggistica ISE sono ade.log, disponibile nel bundle di supporto, che può essere scaricato dalla CLI usando il comando show logging system ade/ADE.log tail durante il problema.

4. Se il log ADE.log mostra rabbitmq: connessione rifiutata errori, contattare Cisco TAC per rimuovere il blocco per il modulo Rabbitmq da ISE Root.

Servizio database ISE API Gateway

Il servizio ISE API Gateway Database è un componente responsabile della gestione e dell'elaborazione dei dati relativi alle richieste API e alle risposte nel sistema ISE. Agisce da intermediario che connette il gateway API ISE al database ISE, garantendo che le applicazioni personalizzate possano aggiornare o modificare i dati anche all'interno di ISE (ad esempio, regolando i criteri di accesso o aggiungendo/rimuovendo utenti) tramite chiamate API gestite dal servizio.

Funzioni chiave del servizio ISE API Gateway Database

1. Accesso API ai dati ISE: Il servizio ISE API Gateway Database funge da bridge, consentendo alle applicazioni esterne di interagire con il database ISE tramite le API RESTful di ISE. Queste API possono essere utilizzate per recuperare o modificare i dati memorizzati nel database ISE, ad esempio:

- Registri di autenticazione utente.
- Criteri di accesso alla rete.

- Informazioni sul profilo del dispositivo.
- Configurazione e impostazioni del sistema.

2. Abilitazione delle integrazioni di sistemi esterni: Questo servizio svolge un ruolo fondamentale nell'integrazione di ISE con sistemi esterni, tra cui:

- Server di autenticazione esterni (LDAP, Active Directory, RADIUS).
- Sistemi di gestione della rete (NMS).
- Soluzioni SIEM (Security Information and Event Management).
- Applicazioni o servizi personalizzati che devono interagire con i dati ISE.

Fornendo l'accesso alle API, il servizio API Gateway Database consente a questi sistemi esterni di interrogare i dati ISE, inviare aggiornamenti ad ISE o attivare azioni specifiche all'interno di ISE in risposta a eventi esterni.

3. Supporto della comunicazione API RESTful: ISE espone le API RESTful progettate per funzionare su HTTP/HTTPS. Il servizio di database gateway API è responsabile della gestione del flusso di richieste e risposte API, garantendo che le richieste vengano autenticate, elaborate e che vengano restituiti i dati appropriati dal database ISE.

Servizio ISE API Gateway

Il servizio ISE API Gateway è un componente cruciale che fornisce all'API RESTful l'accesso a servizi, dati e funzionalità ISE. Opera come ponte tra ISE e i sistemi esterni, consentendo a questi sistemi di interagire a livello di programmazione con il controllo degli accessi alla rete, l'applicazione di policy, l'autenticazione e altri servizi ISE. API Gateway consente ad applicazioni di terze parti, sistemi di gestione della rete e applicazioni personalizzate di interagire con Cisco ISE senza dover intervenire manualmente o accedere direttamente all'interfaccia utente ISE.

Funzioni chiave del servizio ISE API Gateway

1. Abilitazione dell'accesso API ad ISE: Il servizio ISE API Gateway consente ai sistemi esterni di accedere e interagire in modo sicuro con i dati e le policy Cisco ISE usando le API RESTful. Fornisce accesso a livello di programmazione a funzionalità ISE, quali autenticazione, applicazione di policy, gestione di sessione e altro ancora.

2. Controllo programmatico: Il servizio API Gateway consente il controllo a livello di programmazione delle funzioni ISE. Gli amministratori e gli sviluppatori possono utilizzare le API per:

- Recuperare o modificare i criteri di rete.
- Eseguire query o gestire le sessioni utente e i registri di autenticazione.
- Creare e gestire le regole di controllo di accesso alla rete.
- Accedere o aggiornare i profili dispositivo.

Questo controllo può essere utilizzato per l'automazione o l'orchestrazione personalizzata del flusso di lavoro, ad esempio per la regolazione dinamica delle policy di accesso alla rete in base ai dati in tempo reale o per l'integrazione di ISE in una più ampia piattaforma di automazione della

sicurezza.

3. Monitoraggio e relazioni: Il servizio API Gateway consente ai sistemi esterni di raccogliere dati dai log ISE operativi, dalla cronologia delle sessioni e dai dettagli sull'applicazione delle policy. Questa operazione è importante per:

- Creazione di report sulla conformità.
- Monitoraggio della sicurezza.
- Risposta alla richiesta di assistenza.

Le chiamate API possono essere utilizzate per eseguire il pull di registri, informazioni di audit ed eventi, consentendo ai team preposti alla sicurezza di monitorare le attività ISE da un dashboard o da uno strumento di reporting centralizzato.

Verifica e risoluzione dei problemi del servizio ISE API Gateway e del servizio ISE API Gateway Database

1. Verificare se il certificato amministratore del nodo ISE è attivo e valido. Passare a Amministrazione > Certificati > Selezionare il nodo > Seleziona certificato amministratore. Fare clic su Visualizza per verificare lo stato del certificato di amministrazione del nodo ISE.

2. Impostare i componenti ise-api-gateway, api-gateway e apiservice di cui eseguire il debug. I log possono essere dettagliati utilizzando i seguenti comandi:

- show logging application ise-psc.log tail
- show logging application api-gateway.log tail

Servizio ISE pxGrid Direct

Il servizio ISE pxGrid Direct è un componente critico che supporta la funzionalità pxGrid (Platform Exchange Grid) in ISE. pxGrid è una tecnologia Cisco che semplifica la condivisione e l'integrazione sicura, standardizzata e scalabile dei dati tra le soluzioni di sicurezza di rete Cisco e applicazioni, servizi e dispositivi di terze parti. Il servizio ISE pxGrid Direct consente la comunicazione diretta tra ISE e altri sistemi compatibili con pxGrid senza la necessità di dispositivi o servizi intermedi.

Funzioni principali del servizio ISE pxGrid Direct

1. Integrazione diretta con sistemi di terze parti: Il servizio ISE pxGrid Direct consente l'integrazione diretta di ISE con sistemi di sicurezza di rete di terze parti, come firewall, router, soluzioni NAC, piattaforme SIEM e altre appliance di sicurezza. Consente a questi sistemi di scambiare informazioni relative agli eventi di accesso alla rete, agli incidenti relativi alla sicurezza e ai dati contestuali della rete.

2. Condivisione del contesto: Una delle funzioni principali di pxGrid è la condivisione delle informazioni contestuali (come identità dei dispositivi, ruoli utente, postura di sicurezza e informazioni di accesso alla rete). Con il servizio pxGrid Direct, ISE può condividere direttamente questo contesto con altri dispositivi o applicazioni senza affidarsi a metodi tradizionali come

RADIUS o TACACS+.

3. Comunicazione semplificata: Utilizzando pxGrid, ISE può comunicare e scambiare informazioni con soluzioni di terze parti utilizzando un protocollo standardizzato. Ciò semplifica il processo di integrazione, poiché i sistemi non richiedono integrazioni personalizzate per ogni singola soluzione di terze parti.

4. Sicurezza e conformità migliorate: Il servizio pxGrid Direct migliora inoltre la postura di sicurezza e la conformità garantendo che tutti i sistemi nell'ecosistema di rete abbiano accesso agli stessi dati contestuali in tempo reale su utenti, dispositivi e policy di sicurezza. Ciò garantisce un'applicazione più coordinata delle policy di sicurezza di rete in tutto l'ambiente.

Verifica e risoluzione dei problemi del servizio ISEPxgrid Direct

1. Contattare Cisco TAC per verificare se **edda*.lock*** è presente nella cartella /tmp. In caso affermativo, Cisco TAC rimuove il blocco e riavvia il servizio Pxgrid Direct dalla radice.

2. Impostare il componente **PxGrid Direct** per il debug nel nodo ISE per la risoluzione dei problemi. I registri possono essere protetti tramite il pacchetto di supporto ISE o l'interfaccia CLI ISE utilizzando questi comandi:

show logging applicazione pxgriddirect-service.log

show logging applicazione pxgriddirect-connector.log

I log menzionati forniscono informazioni sui dati dell'endpoint recuperati e ricevuti da Cisco ISE, insieme allo stato di connettività di Pxgrid Connector.

Servizio criteri di segmentazione

Il servizio criteri di segmentazione è un componente chiave responsabile dell'applicazione dei criteri di segmentazione della rete in base all'identità dell'utente, alla postura del dispositivo o ad altre informazioni contestuali. Aiuta a controllare l'accesso di utenti e dispositivi a segmenti di rete specifici, garantendo che solo gli utenti autorizzati o i dispositivi conformi possano accedere a determinate parti della rete. La segmentazione della rete è essenziale per ridurre la superficie di attacco della rete, prevenire lo spostamento laterale delle minacce e garantire la conformità alle normative. Il servizio Segmentation Policy di ISE viene usato per applicare queste regole di segmentazione della rete in modo dinamico e flessibile attraverso la rete.

Funzioni chiave del servizio criteri di segmentazione

1. Definizione dei segmenti di rete: Il servizio Segmentation Policy Service di ISE consente agli amministratori di definire vari segmenti di rete (subnet o VLAN) in base alle caratteristiche di utenti o dispositivi. Ad esempio:

- Dispositivi con posture di sicurezza diverse possono essere assegnati a segmenti diversi (ad esempio: dispositivi attendibili in una VLAN e dispositivi non attendibili in un'altra).
- Gli utenti di diversi reparti o ruoli possono essere assegnati a segmenti di rete diversi per applicare privilegi minimi e limitare l'accesso alle risorse riservate.

2. Segmentazione dinamica: Questo servizio consente la segmentazione dinamica della rete, ovvero i segmenti di rete o le VLAN possono variare in base alle condizioni in tempo reale. Ad esempio:

- È possibile assegnare un utente a una VLAN specifica in base al ruolo o allo stato di integrità del dispositivo.
- Un dispositivo ritenuto non conforme o con un sistema operativo non aggiornato può essere spostato in una VLAN di quarantena o guest finché non viene risolto.

3. Applicazione basata su politiche: Il servizio criteri di segmentazione utilizza i criteri per decidere in quale segmento deve essere posizionato un dispositivo o un utente. Tali politiche possono tener conto di vari fattori, quali:

- Identità utente: In base al ruolo o agli attributi utente.
- Postura dispositivo: Lo stato di salute o di conformità del dispositivo (ad esempio: è in esecuzione il software antivirus più recente?).
- Percorso: La posizione fisica dell'utente o del dispositivo nella rete (ad esempio: ufficio, area guest, accesso remoto).
- Ora di accesso: Ora del giorno o della settimana in cui viene effettuata la richiesta di accesso.

4. Applicazione delle politiche di sicurezza: Il servizio di policy di segmentazione garantisce l'applicazione coerente delle policy di sicurezza su tutti i dispositivi di rete (come switch, router, firewall) utilizzando standard di settore come RADIUS e assegnazione di VLAN. Questo consente a Cisco ISE di comunicare con i dispositivi dell'infrastruttura di rete per applicare le policy di segmentazione richieste.

Verifica e risoluzione dei problemi del servizio criteri di segmentazione

1. Verificare che la segmentazione sia configurata correttamente passando a Centri di lavoro > TrustSec > Panoramica > Dashboard.

2. Centri di lavoro > TrustSec > Rapporti, selezionare Rapporti TrustSec per verificare lo stato e i rapporti del servizio criteri di segmentazione.

Servizio autenticazione REST

Il servizio di autenticazione REST è un servizio che fornisce funzionalità di autenticazione tramite API RESTful. Permette ad applicazioni e sistemi esterni di autenticare utenti o dispositivi interagendo con ISE su HTTP(S) utilizzando i protocolli REST standard. Questo servizio consente l'integrazione perfetta della funzionalità di autenticazione Cisco ISE con applicazioni o sistemi di terze parti che devono autenticare utenti o dispositivi, ma non possono utilizzare i metodi tradizionali (come RADIUS o TACACS+).

Funzioni chiave del servizio di autenticazione REST

1. Autenticazione RESTful: Il servizio di autenticazione REST abilita le richieste di autenticazione

tramite il protocollo API REST. Ciò consente di utilizzare sistemi esterni (ad esempio: applicazioni, dispositivi di rete di terze parti o servizi) per autenticare gli utenti o i dispositivi che usano ISE come server di autenticazione, ma tramite chiamate al servizio Web RESTful anziché tramite protocolli di autenticazione tradizionali come RADIUS o TACACS+.

2. Integrazione con applicazioni esterne: Questo servizio è progettato per applicazioni esterne che richiedono l'autenticazione di utenti o dispositivi, ma non utilizzano metodi di autenticazione tradizionali (come RADIUS o TACACS+). Possono invece interagire con ISE tramite API REST, semplificando l'integrazione dell'autenticazione ISE in applicazioni basate sul Web o native per il cloud.

3. Autenticazione flessibile e scalabile: Il servizio di autenticazione REST fornisce un metodo di autenticazione scalabile che non è limitato ai soli dispositivi di rete o alle soluzioni locali. Può essere utilizzato da servizi cloud, applicazioni mobili e altre piattaforme basate sul Web che devono autenticare utenti o dispositivi interrogando ISE per le credenziali e le policy.

4. Facile da applicare: L'API REST offre un'interfaccia standardizzata, che è più facile da applicare e integrare con software e applicazioni moderni rispetto ai metodi tradizionali. Fornisce risposte in formato JSON e utilizza metodi HTTP come GET, POST, PUT e DELETE, rendendolo più accessibile per gli sviluppatori Web e i sistemi che integrano ISE per l'autenticazione.

Verifica e risoluzione dei problemi per autenticazione REST

1. Per risolvere i problemi relativi ad Open API, impostare il componente apiservice su debug.

2. Per risolvere i problemi relativi all'API ERS, impostare il componente ers su debug.

Se la pagina dell'interfaccia utente del servizio API: https://{iseip}:{port}/api/swagger-ui/index.html o https://{iseip}:9060/ers/sdk è accessibile. Il servizio API funziona come previsto.

Per ulteriori informazioni sull'API, consultare la documentazione dell'API.

Connettore SSE

Il connettore SSE (Secure Software-Defined Edge Connector) è un servizio che integra ISE con la soluzione Cisco Secure Software-Defined Access (SD-Access). Il connettore SSE consente ad ISE di comunicare in modo sicuro con Cisco DNA Center, abilitando policy di rete automatizzate, segmentazione e gestione della sicurezza dei bordi in un ambiente SD-Access.

Funzioni principali del connettore SSE

1. Integrazione con sistemi di sicurezza di terze parti: Il connettore SSE semplifica l'integrazione di Cisco ISE con sistemi di sicurezza di terze parti come firewall, sistemi di prevenzione delle intrusioni (IPS), soluzioni di controllo dell'accesso alla rete (NAC) e sistemi SIEM (Security Information and Event Management). Consente a questi sistemi esterni di inviare o ricevere dati da ISE in modo sicuro, che può essere utilizzato per un'applicazione più dinamica delle policy.

2. Intelligenza delle minacce in tempo reale: Collegando ISE ad altri sistemi di sicurezza, il

connettore SSE permette lo scambio di informazioni in tempo reale sulle minacce. Queste informazioni possono includere attività sospette, endpoint compromessi o comportamenti dannosi rilevati da altri sistemi di sicurezza, consentendo all'ISE di regolare dinamicamente le policy di accesso in base ai livelli di minaccia correnti o allo stato dei dispositivi.

3. Risanamento automatico: L'integrazione attivata da SSE Connector può supportare flussi di lavoro di risoluzione automatizzata. Ad esempio, se un sistema è contrassegnato come compromesso da un'appliance di sicurezza esterna, ISE può applicare automaticamente policy che bloccano l'accesso alla rete o reindirizzare l'endpoint a un segmento di rete di monitoraggio e aggiornamento per ulteriori indagini.

Verifica e risoluzione dei problemi del connettore SSE

1. Il connettore SSE è abilitato solo quando il servizio PassiveID è abilitato in ISE.

2. Il componente sse-connector (connector.log) nel debug fornisce ulteriori informazioni sui messaggi relativi al connettore SSE.

Hermes (agente cloud pxGrid)

Hermes (pxGrid Cloud Agent) è un componente che facilita l'integrazione tra ISE e l'ecosistema pxGrid (Platform Exchange Grid) in un ambiente cloud. Hermes è l'agente basato su cloud utilizzato per abilitare la comunicazione tra ISE e le piattaforme o i servizi basati su cloud, supportando il framework pxGrid per la condivisione di informazioni contestuali tra diversi sistemi di rete e sicurezza.

Caratteristiche e funzioni principali di Hermes (pxGrid Cloud Agent)

1. Integrazione da cloud a locale: Hermes (pxGrid Cloud Agent) è progettato per facilitare l'integrazione tra i servizi basati su cloud e l'infrastruttura ISE locale. Estende la potenza di pxGrid oltre i tradizionali ambienti di rete locali, consentendo lo scambio sicuro dei dati e l'applicazione delle policy su applicazioni e servizi basati su cloud.

2. Supporto dell'ecosistema pxGrid: pxGrid è una piattaforma Cisco per la condivisione sicura del contesto e delle informazioni attraverso le soluzioni di sicurezza di rete. Hermes agisce come agente cloud per pxGrid, consentendo una comunicazione sicura in tempo reale tra ISE e i vari servizi basati su cloud. Questa integrazione consente l'uniformità dei criteri di sicurezza di rete sia negli ambienti locali che in quelli cloud, semplificando la gestione e l'applicazione della sicurezza.

3. Visibilità degli endpoint basata su cloud: Uno dei vantaggi principali di Hermes è la visibilità sugli endpoint basati su cloud, analogamente a quanto offerto da ISE sugli endpoint locali. Può raccogliere dati su dispositivi e utenti nel cloud, ad esempio la postura di conformità, lo stato di sicurezza e le informazioni sull'identità. Ciò consente ad ISE di applicare policy di accesso alla rete sugli endpoint cloud come farebbe per i dispositivi locali.

4. Estensione perfetta di ISE agli ambienti cloud: Uno dei vantaggi principali di Hermes è che fornisce un ponte senza interruzioni tra l'ambiente ISE locale e il crescente numero di applicazioni

native cloud. In questo modo è più facile estendere le policy di sicurezza ISE, i metodi di autenticazione e i controlli di accesso ai servizi cloud senza richiedere una revisione completa dell'infrastruttura esistente.

Verifica e risoluzione dei problemi di Hermes (agente cloud Pxgrid)

1. Per impostazione predefinita, il servizio Hermes è disabilitato. La connessione di ISE al cloud Cisco PxGrid abilita il servizio Hermes. Quindi, se il servizio Hermes è disabilitato in ISE, verificare se l'opzione Pxgrid Cloud è abilitata da **ISE GUI > Amministrazione > Distribuzione, selezionare il nodo ISE**. Modifica , **abilita Pxgrid Cloud.**

2. I debug utili per la risoluzione dei problemi relativi al cloud Pxgrid sono **hermes.log** e **pxcloud.log**. Questi debug sono disponibili solo nel nodo Pxgrid in cui è abilitato Pxgrid Cloud.

McTrust (servizio di sincronizzazione Meraki)

McTrust (Meraki Sync Service) è un servizio che consente l'integrazione tra i sistemi Cisco ISE e Cisco Meraki, in particolare per la sincronizzazione e la gestione dei dispositivi di rete e delle policy di accesso. Il servizio McTrust funge da connettore per la sincronizzazione delle informazioni su dispositivi e utenti tra l'infrastruttura di rete gestita dal cloud di Meraki e i sistemi di gestione delle identità e delle policy ISE on-premises.

Caratteristiche e funzioni principali di McTrust (Meraki Sync Service)

1. Integrazione perfetta con i dispositivi Meraki: McTrust consente ad ISE di sincronizzarsi e integrarsi con i dispositivi gestiti dal cloud di Meraki. Tra questi vi sono dispositivi come access point Meraki, switch e appliance di sicurezza che fanno parte della linea di prodotti Meraki. Permette ad ISE di comunicare direttamente con l'infrastruttura di Meraki, semplificando l'applicazione di policy di controllo dell'accesso alla rete ai dispositivi gestiti da Meraki.

2. Sincronizzazione automatica dei dispositivi: Il servizio di sincronizzazione Meraki sincronizza automaticamente le policy ISE con i dispositivi di rete Meraki. Ciò significa che qualsiasi modifica apportata alle policy di controllo dell'accesso alla rete in ISE viene automaticamente riflessa nei dispositivi Meraki, senza richiedere un intervento manuale. Ciò semplifica la gestione dell'accesso alla rete da parte degli amministratori sia sulle piattaforme Meraki che ISE.

3. Applicazione delle policy per i dispositivi gestiti con Meraki: McTrust consente ad ISE di applicare policy di accesso alla rete sui dispositivi Meraki basate sull'autenticazione e la postura. Può assegnare dinamicamente policy agli elementi della rete Meraki, come regolare le assegnazioni delle VLAN, applicare gli Access Control Lists (ACL), o limitare l'accesso a certe risorse di rete, a seconda della postura di sicurezza del dispositivo o dell'utente che richiede l'accesso.

4. Integrazione con Meraki Dashboard: McTrust integra ISE direttamente con Meraki Dashboard, fornendo un'interfaccia di gestione unificata. Grazie a questa integrazione, gli amministratori possono visualizzare e gestire le policy di rete e le regole di controllo dell'accesso sia per i dispositivi Meraki che per le risorse gestite da ISE, il tutto dall'interfaccia gestita dal cloud Meraki.

Verifica e risoluzione dei problemi di McTrust (servizio di sincronizzazione Meraki)

1. Accedere alla GUI di ISE -> Work Centres -> TrustSec -> Integrations -> Sync status. Verificare eventuali problemi/errori rilevati.

2. Verificare che tutti i certificati di amministratore dei nodi ISE siano attivi e validi.

Il comando meraki-connector.log è utile per risolvere i problemi del servizio di sincronizzazione Meraki.

ISE Node Exporter

Il servizio ISE Node Exporter è un componente utilizzato per il monitoraggio e la raccolta delle metriche delle prestazioni dal sistema ISE, in particolare dai nodi ISE (nodi di amministrazione, nodi di monitoraggio o nodi di servizio delle policy).

Funzioni e caratteristiche principali di ISE Node Exporter

1.Esportazione delle metriche: ISE Node Exporter fornisce una vasta gamma di metriche relative alle prestazioni, quali l'utilizzo della CPU, della memoria, del disco, delle statistiche di rete, del carico del sistema e altre metriche a livello di sistema operativo. Queste metriche vengono quindi utilizzate per il monitoraggio dello stato e delle prestazioni del nodo ISE e possono essere visualizzate in un dashboard di monitoraggio come Grafana.

2. Monitoraggio dello stato del sistema: Esportando i dati sulle prestazioni in Prometheus, ISE Node Exporter permette di monitorare continuamente lo stato operativo e di salute del nodo ISE. Gli amministratori possono creare avvisi in base a soglie predefinite per notificare il peggioramento delle prestazioni o problemi di sistema.

3. Integrazione di Prometheus: ISE Node Exporter viene normalmente utilizzata insieme a Prometheus, un toolkit per il monitoraggio e gli avvisi open-source progettato per garantire affidabilità e scalabilità. Node Exporter espone metriche a livello di sistema che possono essere scartate da Prometheus per raccogliere e memorizzare dati di serie temporali.

ISE Prometheus Service

ISE Prometheus è un servizio che integra Prometheus con ISE per consentire il monitoraggio e la raccolta di metriche delle prestazioni dal sistema ISE. Prometheus è un toolkit open-source per il monitoraggio e l'avviso utilizzato per raccogliere, memorizzare e analizzare i dati delle serie temporali. Grazie al servizio ISE Prometheus, ISE può esporre le proprie metriche interne a Prometheus a scopo di monitoraggio.

Caratteristiche e funzioni principali del servizio Prometeo di ISE

1. Raccolta delle metriche per il monitoraggio: Il servizio ISE Prometheus è progettato per esportare varie metriche operative e di prestazioni relative al sistema ISE. Queste metriche in genere includono, tra l'altro, l'utilizzo della CPU e il carico del sistema, l'utilizzo della memoria,

l'utilizzo del disco e le prestazioni di I/O, le statistiche di rete, le statistiche delle richieste di autenticazione, le statistiche di applicazione dei criteri, lo stato del sistema e i dati relativi al tempo di attività

2. Integrazione di Prometheus: Il servizio Prometheus permette ad ISE di esporre i dati in un formato compatibile con Prometheus, che raccoglie questi dati a intervalli regolari. Prometheus archivia i dati in un database time-series, consentendo di tenere traccia delle tendenze e delle prestazioni storiche del sistema ISE.

3. Visualizzazione e reporting con Grafana: Il servizio Prometheus di ISE si integra perfettamente con Grafana, un popolare strumento di visualizzazione open-source. Dopo aver esportato le metriche in Prometheus, gli amministratori possono utilizzare dashboard Grafana per visualizzare i dati in tempo reale. Ciò consente di identificare facilmente i colli di bottiglia prestazionali, le tendenze del sistema e i potenziali problemi nell'implementazione di ISE.

ISE Grafana Service

Il servizio ISE Grafana fornisce la visualizzazione delle metriche delle prestazioni del sistema tramite Grafana, una piattaforma open source per il monitoraggio e la visualizzazione dei dati. Si integra con Prometheus per visualizzare i dati storici e in tempo reale raccolti da ISE, consentendo agli amministratori di creare dashboard interattivi che forniscono informazioni sullo stato, le prestazioni e l'utilizzo del sistema ISE.

Funzioni e caratteristiche principali di ISE Grafana Service

1. Dashboard personalizzabili: Grafana è altamente personalizzabile, consentendo agli amministratori di creare e modificare dashboard in base alle loro specifiche esigenze di monitoraggio. È possibile creare query personalizzate per estrarre punti dati specifici da Prometheus e visualizzare tali query in vari formati, ad esempio grafici, tabelle, heatmap e così via.

2. Monitoraggio centralizzato per implementazioni ISE distribuite: Per le implementazioni ISE distribuite, in cui più nodi ISE vengono distribuiti in diverse sedi, Grafana fornisce una vista centralizzata di tutte le metriche di sistema raccolte da ciascun nodo. Ciò consente agli amministratori di monitorare le prestazioni dell'intera implementazione ISE da un'unica postazione.

3. Dati storici e analisi delle tendenze: Con i dati memorizzati in Prometheus, Grafana consente l'analisi cronologica della metrica del sistema, consentendo agli amministratori di tenere traccia delle tendenze nel tempo. Ad esempio, possono monitorare le variazioni dell'utilizzo della CPU nell'ultimo mese o le fluttuazioni delle percentuali di riuscita dell'autenticazione. Questi dati cronologici sono importanti per la pianificazione della capacità, l'analisi delle tendenze e l'identificazione di problemi a lungo termine.

Verifica e risoluzione dei problemi di ISE Grafana Service, ISE Prometheus Service, ISE Node Exporter

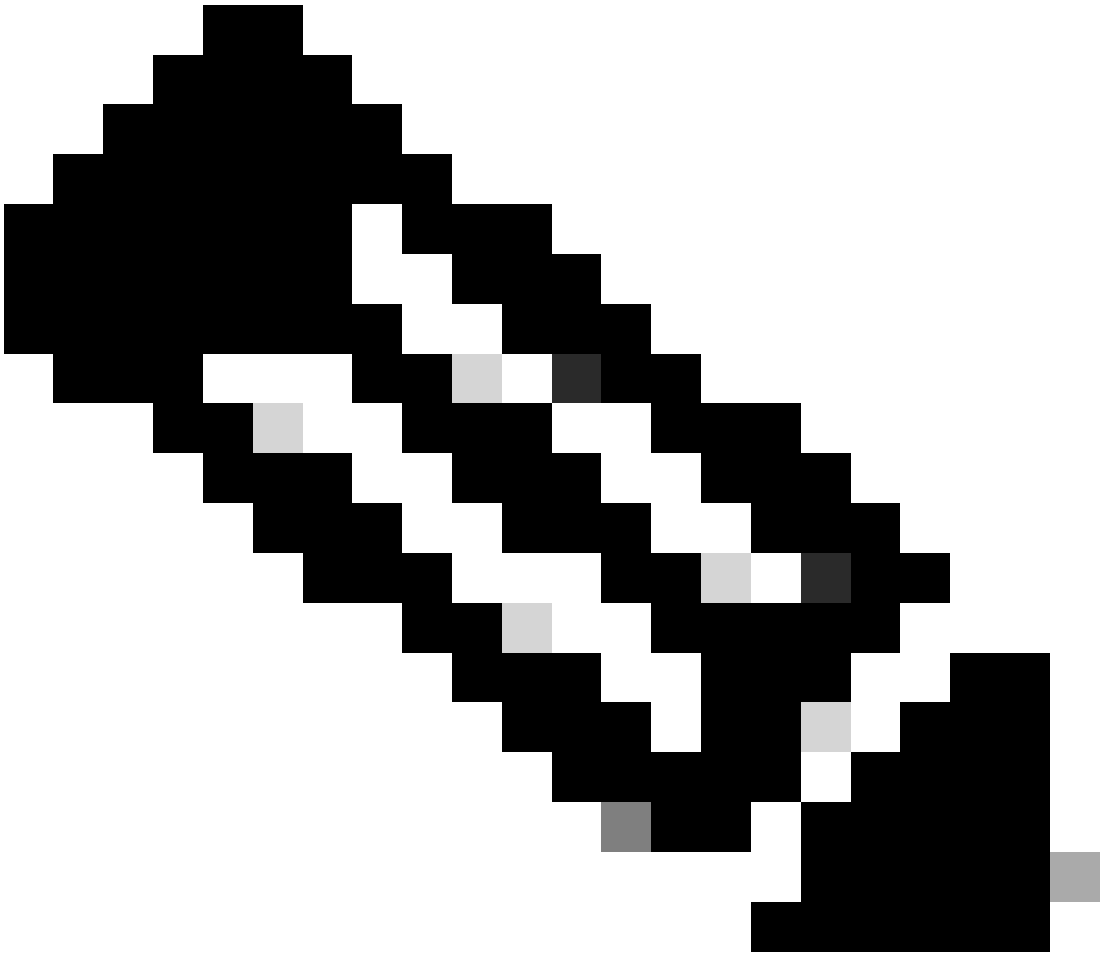
1. ISE Grafana Service, ISE Prometheus Service e ISE Node Exporter operano insieme e sono chiamati Grafana Stack Services. Non sono disponibili debug specifici da abilitare per la

risoluzione dei problemi relativi a questi servizi. Tuttavia, questi comandi facilitano la risoluzione dei problemi.

show logging application ise-prometheus/prometheus.log

show logging application ise-node-exporter/node-exporter.log

show logging application ise-grafana/grafana.log



Nota: Quando il monitoraggio è abilitato, ISE Node Exporter, ISE Prometheus Service e ISE Grafana Service devono essere in esecuzione e l'interruzione di uno di questi servizi può causare problemi durante la raccolta dei dati.

ISE NT LogAnalytics Elasticsearch

ISE MNT LogAnalytics Elasticsearch è un componente che integra Elasticsearch con le funzionalità di monitoraggio e risoluzione dei problemi (MNT) di ISE. Viene utilizzato per l'aggregazione, la ricerca e l'analisi dei log relativi ai log e agli eventi ISE. Elasticsearch è un

motore di ricerca e analisi distribuito e ampiamente utilizzato e, se integrato con ISE, migliora la capacità del sistema di archiviare, analizzare e visualizzare i dati di log generati dai componenti ISE.

Funzioni e caratteristiche principali di ISE MNT LogAnalytics Elasticsearch

1. Archiviazione e indicizzazione dei registri: Il servizio Elasticsearch di ISE è responsabile dell'archiviazione e dell'indicizzazione dei dati di registro generati da ISE. Elasticsearch è un motore di ricerca e analisi distribuito e consente di archiviare i log ISE in modo da eseguire ricerche, eseguire query e recuperare eventi, errori o attività di sistema specifiche in modo rapido.

2. Integrazione con Log Analytics: ISE NT LogAnalytics Elasticsearch lavora in abbinamento a Log Analytics per fornire una soluzione di registrazione completa. Consente ad ISE di raccogliere dati di log relativi all'autenticazione, all'applicazione delle policy, alle operazioni di sistema e ad altre attività. Questi dati vengono archiviati in Elasticsearch, che semplifica l'esecuzione di analisi dettagliate e la comprensione del comportamento di ISE.

3. Registrazione centralizzata: Integrandosi con Elasticsearch, ISE offre una soluzione di registrazione centralizzata, fondamentale per gli ambienti che richiedono una raccolta di log distribuiti. Ciò consente agli amministratori di visualizzare e analizzare i log di più nodi ISE in un'unica interfaccia unificata, semplificando la risoluzione dei problemi e il monitoraggio delle prestazioni ISE.

4. Analisi dei log e risoluzione dei problemi: Il servizio ISE MNT LogAnalytics Elasticsearch aiuta gli amministratori ad analizzare il comportamento del sistema e a risolvere i problemi rendendo i dati dei log facilmente accessibili. Se ad esempio si verifica un picco improvviso di errori di autenticazione o un'interruzione imprevista del sistema, Elasticsearch consente di eseguire rapidamente query sui dati di registro per identificare la causa principale.

Verifica e risoluzione dei problemi di ISE M&T Log Analytics Elasticsearch

1. La disabilitazione e la riabilitazione del servizio di analisi dei log ad ISE deve essere di aiuto. Passare a Operazioni > Sistema 360 > Impostazioni > Analisi log (disabilita e abilita usando l'opzione di attivazione/disattivazione).

2. Il riavvio di M&T Log Analytics da ISE Root risolve il problema. Per eseguire questa azione, contattare Cisco TAC.

Difetti noti

Cisco bug ID ·66198

ISE Logstash Service

ISE Logstash Service è un componente che integra Logstash, una pipeline di elaborazione dati open-source, con ISE per la raccolta, la trasformazione e l'inoltro dei log. Logstash funge da agente di raccolta e inoltro dei log, consentendo l'elaborazione e l'invio dei log ISE ad altri sistemi per l'analisi, l'archiviazione e il monitoraggio. Logstash è un potente strumento open source che raccoglie, analizza e inoltra log o altri dati da diverse origini a una posizione centrale per lo

storage, l'analisi e la visualizzazione. Nel contesto di ISE, ISE Logstash Service viene utilizzato per elaborare e inoltrare i log in formato strutturato a un sistema di log centralizzato, dove possono essere ulteriormente analizzati, monitorati e visualizzati.

Funzioni e caratteristiche principali del servizio ISE Logstash

1. Raccolta e inoltro dei registri: La funzione principale di ISE Logstash Service è raccogliere dati di log da vari componenti ISE (ad esempio, log di autenticazione, log di sistema, log di applicazione delle policy e così via) e inoltrarli a una posizione centrale (in genere Elasticsearch o un altro sistema di gestione dei log) per la memorizzazione e l'analisi.

2. Analisi dei registri: Logstash può analizzare i log raccolti in formati strutturati. Elabora i dati non elaborati del registro ed estrae informazioni significative da esso, trasformando le voci del registro in un formato più facile da interrogare e analizzare. Ciò può comportare il filtraggio, l'analisi e l'arricchimento dei dati prima di inoltrarli a Elasticsearch o ad altri sistemi.

Verifica e risoluzione dei problemi di ISE Logstash Service

1. Nessun debug specifico da abilitare. Tuttavia, **show logging application ise-logstash/logstash.log** fornisce informazioni dettagliate sullo stato del servizio.

2. La disabilitazione e la riabilitazione del servizio di analisi dei registri in ISE deve essere di aiuto. Passare a **Operazioni > Sistema 360 > Impostazioni > Analisi log** (disabilitare e abilitare utilizzando l'opzione di attivazione/disattivazione).

Difetti noti relativi al servizio Logstash

Cisco bug ID ·74832

Cisco ID bug ·58596

ISE Kibana Service

ISE Kibana Service è un componente che integra Kibana, uno strumento di visualizzazione dei dati open-source, con l'infrastruttura di registrazione e monitoraggio ISE. Kibana lavora in tandem con Elasticsearch (che archivia e indicizza i dati di log) per fornire una piattaforma potente per la visualizzazione, la ricerca e l'analisi dei log ISE e delle metriche delle prestazioni.

Caratteristiche e funzioni principali del servizio ISE Kibana

1. Visualizzazione dei dati: Il servizio ISE Kibana consente agli amministratori di creare rappresentazioni visive dei dati di registro raccolti da ISE. Ciò può includere:

- Grafici e tabelle per le tendenze relative all'autenticazione, all'applicazione delle policy, all'attività degli utenti e all'integrità del sistema.
- Grafici a torta, a linee e a barre per tenere traccia di metriche specifiche quali il numero di accessi non riusciti, la durata della sessione o gli errori nel tempo.

Verifica e risoluzione dei problemi del servizio ISE Kibana

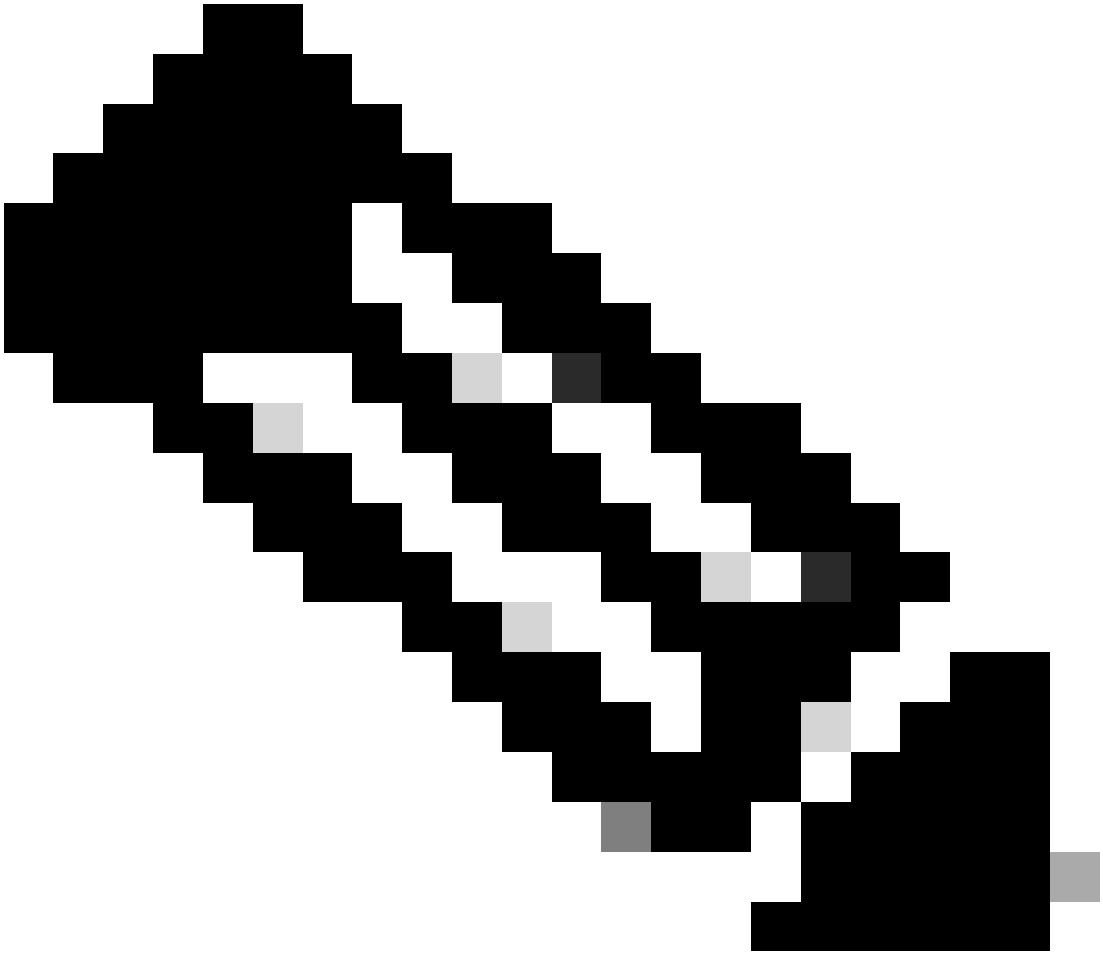
1. Se il servizio Kibana di ISE non è in esecuzione, disabilitare e riabilitare l'analisi dei log in ISE, selezionare Operations > System 360 > Settings, Log analytics (disabilitare e abilitare usando l'opzione di attivazione/disattivazione).

2. In molti scenari, può esistere una voce duplicata nella cartella /etc/hosts che deve causare un problema. Contattare TAC per rimuovere la voce duplicata.

Difetti noti relativi alla questione Kibana

Cisco bug ID ·78050

Cisco ID bug ·59848



Nota: Quando Log Analytics è abilitato, ISE NT Log Analytics Elasticsearch, ISE Logstash Service, ISE Kibana Service devono essere in esecuzione e l'interruzione di uno di questi servizi può causare problemi durante la raccolta dei dati.

Servizio IPSec nativo ISE

Il servizio IPSec nativo di ISE fa riferimento al supporto integrato per IPSec (Internet Protocol Security), che fornisce una comunicazione sicura tra i nodi ISE o tra ISE e altri dispositivi di rete. IPSec è una suite di protocolli utilizzati per proteggere le comunicazioni di rete tramite l'autenticazione e la crittografia di ogni pacchetto IP in una sessione di comunicazione.Il servizio IPSec nativo fa parte della più ampia struttura di gestione della sicurezza e dell'accesso alla rete. Offre funzionalità per gestire e gestire le connessioni VPN IPsec, garantendo la sicurezza dei dati trasmessi tra il sistema ISE e gli endpoint remoti. Ciò potrebbe comportare interazioni con dispositivi client, dispositivi di accesso alla rete (come router o firewall) o anche altri nodi ISE, dove la crittografia IPsec e il tunneling sono necessari per proteggere le informazioni riservate.

Funzioni e caratteristiche principali del servizio IPSec nativo ISE

1. Comunicazioni protette tramite IPsec: La funzione principale del servizio IPSec nativo ISE è quella di stabilire e mantenere canali di comunicazione protetti con IPsec. Ciò comporta l'uso di meccanismi di crittografia e autenticazione per garantire che i dati trasmessi tra ISE e altri dispositivi siano protetti da intercettazioni, manomissioni e accessi non autorizzati.

2. Connettività VPN IPsec: Il servizio IPSec nativo ISE semplifica le connessioni VPN che utilizzano il protocollo IPsec per fornire un tunnel protetto e crittografato per la trasmissione dei dati. Questa caratteristica è particolarmente utile per gli utenti remoti, le filiali o altri luoghi che hanno la necessità di accedere in modo sicuro all'ambiente ISE su reti non attendibili (ad esempio, Internet).

3. Supporto per VPN ad accesso remoto: Il servizio IPSec nativo può essere utilizzato nelle configurazioni VPN ad accesso remoto, in cui gli utenti o i dispositivi che si trovano fuori sede (ad esempio, dipendenti remoti o filiali) si connettono in modo sicuro al sistema ISE tramite tunnel IPsec. Questo servizio garantisce che tutto il traffico di accesso remoto venga crittografato e autenticato prima di raggiungere l'ambiente ISE.

4.Compatibilità client VPN IPsec: Il servizio IPSec nativo ISE garantisce la compatibilità con i client VPN IPsec. Supporta configurazioni client comuni, consentendo ai dispositivi di connettersi in modo sicuro alla rete senza esporre a rischi i dati sensibili.

Verifica e risoluzione dei problemi del servizio IPSec nativo

1. Nessun debug specifico da abilitare per il servizio IPSec nativo. Verificare i log utilizzando il comando show logging application strongswan/charon.log tail dalla CLI di ISE.

2. Se si riscontrano problemi per il tunnel, verificare lo stato di attivazione del tunnel tramite GUI > Amministrazione > Sistema > Impostazioni > Protocolli > IPSec > IPSec nativo.

Profiler MFC

Il profiler MFC è un componente specializzato utilizzato per la profilatura di dispositivi ed endpoint di rete. La creazione di profili è una parte chiave del controllo degli accessi alla rete, in quanto

consente ad ISE di identificare i dispositivi sulla rete, classificarli e applicare policy di rete appropriate in base al tipo di dispositivo e al comportamento.

Funzioni e caratteristiche principali del servizio Profiler MFC ad ISE

1. Profilatura del traffico: Il servizio MFC Profiler in ISE è responsabile della raccolta e della creazione del profilo dei dati sul traffico. Controlla il comportamento degli endpoint sulla rete, inclusi i tipi di applicazioni utilizzate, i servizi a cui si accede e i modelli di traffico esposti dai dispositivi. Questi dati consentono di creare un profilo per ogni endpoint.

2. Profilatura degli endpoint: Il servizio MFC Profiler consente ad ISE di identificare e classificare gli endpoint in base al loro comportamento. Ad esempio, rileva se un endpoint è una stampante, un computer o un dispositivo mobile in base ai modelli di traffico. Ciò consente di applicare policy più specifiche per diversi tipi di dispositivi, migliorando la sicurezza e l'efficienza operativa.

Verifica e risoluzione dei problemi del servizio profiler MFC

1. Passare a ISE GUI -> Administration -> Profiling -> MFC profiling and AI rules, verificare se il servizio è abilitato.

2. Se il servizio è abilitato ma è visualizzato come disabilitato / non in esecuzione tramite il comando show application status ise nella CLI di ISE. Disabilitare e riabilitare il servizio di profilatura MFC in ISE facendo riferimento al punto 1.

Debug utili per la risoluzione dei problemi: Componente del profiler MFC nel debug. I log possono essere verificati dal bundle di supporto o dalla coda dei log usando il comando show logging application ise-pi-profiler.log tail dalla CLI di ISE.

Errore noto del profiler MFC che indica che il profiler non è in esecuzione anziché disabilitato:

Cisco bug ID ·72853

Punti chiave

1. Per ripristinare i servizi, riavviare i servizi utilizzando i comandi application stop ise e application start ise tramite la CLI di ISE.

2. In caso di problemi, accertarsi che esista un bundle di supporto da acquisire dalla CLI di ISE GUI / ISE per un'ulteriore verifica del problema. Link di riferimento per la creazione di ISE Support bundle tramite GUI e CLI: Collect Support Bundle on the Identity Services Engine

3. Se i problemi sono correlati alle risorse, alla media del carico, all'utilizzo del disco e così via, è obbligatorio raccogliere i dump di thread e di heap per l'analisi.

4. Prima di eseguire il ricaricamento del nodo, contattare Cisco TAC e fornire registri protetti per un'ulteriore analisi.

Problemi standard ad ISE

A parte i problemi con i servizi ISE, queste sono alcune delle preoccupazioni trovate nei nodi ISE insieme alle operazioni di risoluzione dei problemi di base richieste.

Verifica del carico medio elevato, problemi di utilizzo delle risorse (CPU / MEMORIA / DISCO), risorse insufficienti

1. Verificare che le risorse consigliate da Cisco siano allocate al nodo utilizzando il comando show inventory dalla CLI di ISE.

2. Dalla CLI del nodo ISE, eseguire il comando tech top per verificare l'utilizzo delle risorse di ISE.

3. Verificare l'utilizzo del disco utilizzando il comando show disk dalla CLI di ISE.

4. Eliminare gli endpoint inattivi, cancellare il disco locale del nodo ed eseguire le operazioni di pulizia dell'aggiornamento.

Se il problema persiste, contattare Cisco TAC e fornire il bundle di supporto protetto, il dump dell'heap e il dump del thread dal nodo in cui si è verificato il problema.

Per proteggere il dump dell'heap, accedere alla CLI del nodo ISE, eseguire il comando **application configure ise**. Selezionare **l'opzione 2.**

Per proteggere il dump del thread, accedere alla CLI del nodo ISE, eseguire il comando **application configure ise**, selezionare l'**opzione 23.** Il dump del thread è incluso nel bundle di supporto o può essere aggiornato tramite ISE CLI utilizzando il comando **show logging application appserver/catalina.out**.

Verifica e risoluzione dei problemi di monitoraggio

La funzione di monitoraggio e risoluzione dei problemi (MnT) di ISE è uno dei principali elementi dell'architettura ISE che fornisce funzionalità di monitoraggio, reporting e avviso.

ISE visualizza le informazioni di monitoraggio in molti luoghi, tra cui:

- Home page Cisco ISE
- Viste Visibilità contesto
- Registri e sessioni Live RADIUS
- Ricerca globale
- Registri in tempo reale NAC incentrati sulle minacce
- Registri TACACS Live

Problemi generali osservati nella categoria Monitoraggio e risoluzione dei problemi:

1. Registri Radius/TACACS Live non disponibili
2. Sessioni live non disponibili
3. Riepilogo stato non disponibile
4. Problemi di prestazioni (elevata CPU/memoria) rilevati sui nodi MnT

Debug da abilitare sui nodi MnT per ridurre il problema:

1. Cisco-mnt
2. Collector
3. Cpm-mnt
4. registrazione in fase di esecuzione

Oltre ai componenti menzionati nel debug, queste informazioni possono essere utili per la risoluzione dei problemi:

1. Le sessioni in tempo reale sono interessate o sono limitate ai registri in tempo reale?
2. I registri Radius o TACACS sono interessati o sono interessati da entrambi?
3. L'utilizzo della CPU o lo spazio di swap sui nodi MnT è elevato?
4. Quanti file di buffer vengono visualizzati sui nodi MnT? I file di buffer sono disponibili in: /opt/CSCOcpm/mnt/data/collector.
5. Le prenotazioni di memoria e CPU sono abilitate, in caso contrario abilitarle.
6. Il database MnT/config/session è stato reimpostato negli ultimi tempi?
7. I syslog vengono inviati dai nodi PSN ai nodi MnT?

Se si utilizzano i servizi Syslog per MnT, queste informazioni sono necessarie ai fini della risoluzione dei problemi:

1. Si sta utilizzando una destinazione syslog sicura. In caso contrario, disabilitarla in quanto causa deadlock nei thread che impediscono il funzionamento dell'agente di raccolta?
2. Se si utilizza una destinazione syslog protetta, verificare che il mapping dei certificati sia impostato correttamente in Amministrazione->Registrazione->Destinazioni di registrazione remota->Agente di raccolta syslog protetto 1 e 2
3. Verificare che le categorie di registrazione siano impostate correttamente (si consiglia di rimuovere le categorie di registrazione inutilizzate/indesiderate - in questo modo si riduce il carico sui nodi MnT) e che le destinazioni di registrazione siano configurate correttamente.
4. Controllare i file awrrep*.html dal bundle di supporto per comprendere e ottenere un suggerimento su quale componente invia syslog più frequenti. Ad esempio, se le tabelle TACACS vengono visualizzate con query di inserimento o aggiornamento, è possibile controllare i log di raccolta per stabilire la correlazione e capire quali syslog vengono inviati più frequentemente

Se il problema è relativo alle prestazioni sul nodo MnT, sono necessarie le seguenti informazioni:

1. top output tecnico dalla CLI ISE del nodo MnT.

2. Se la CPU è alta, è presente anche un elevato utilizzo della memoria o dello spazio di swap?

3. Pacchetto di supporto con dump heap e dump thread protetti.

Riferimento

- Guida dell'amministratore di Cisco Identity Services Engine, versione 3.3
- Risoluzione dei problemi e abilitazione dei debug su ISE

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).