Verständnis von ISE-Services, Zweck und Fehlerbehebung

Inhalt

Einleitung

In diesem Dokument werden die ISE-Services, der Zweck und die Fehlerbehebung beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse der Cisco Identity Services Engine verfügen.

Verwendete Komponenten

Das Dokument ist nicht auf bestimmte Software- und Hardwareversionen der Cisco Identity Services Engine beschränkt.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Die Cisco Identity Services Engine (ISE) ist eine umfassende Lösung für erweiterte Netzwerksicherheit durch zentrales Richtlinienmanagement, Authentifizierung, Autorisierung und Abrechnung (AAA). Sie ermöglicht die Verwaltung des Netzwerkzugriffs für Benutzer, Geräte und Anwendungen und gewährleistet gleichzeitig Sicherheit, Compliance und ein nahtloses Anwendererlebnis.

Um diese Ziele zu erreichen, nutzt die Cisco ISE eine Reihe von Services, von denen jeder für spezifische Aufgaben verantwortlich ist, die das effiziente Funktionieren des Systems ermöglichen. Diese Services arbeiten zusammen, um einen sicheren Netzwerkzugriff, eine robuste Richtliniendurchsetzung, detaillierte Protokollierung, nahtlose Integration in externe Systeme und eine effiziente Erstellung von Geräteprofilen zu gewährleisten.

Jeder Service in der ISE spielt eine entscheidende Rolle bei der Aufrechterhaltung der Integrität und Verfügbarkeit der Lösung. Einige Dienste verarbeiten Kernfunktionen wie Datenbankmanagement und Authentifizierung, während andere erweiterte Funktionen wie die Erstellung von Geräteprofilen, die Zertifikatsverwaltung und die Überwachung ermöglichen.

Dieser Artikel bietet eine Übersicht über die verschiedenen Services der Cisco ISE und erläutert deren Zweck, Bedeutung und mögliche Schritte zur Fehlerbehebung, falls Probleme auftreten. Wenn Sie Administrator oder Netzwerksicherheitsexperte sind und diese Services kennen, können Sie einen reibungslosen und sicheren Betrieb Ihrer ISE-Bereitstellung sicherstellen.

Verständnis und Fehlerbehebung bei ISE-Services

Die im Screenshot erwähnten Services werden von der ISE zur Unterstützung ihrer Funktionalität genutzt. Überprüfen Sie den Status oder die in der ISE verfügbaren Services, indem Sie den Befehl show application status ise über die CLI des ISE-Knotens verwenden. Im Folgenden finden Sie eine Beispielausgabe, die den Status der auf der ISE verfügbaren Services anzeigt.

```
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
```

Die Services sind in der ISE verfügbar.

Sehen Sie sich nun die einzelnen Services genauer an.

Datenbank-Listener

Der Datenbank-Listener-Dienst ist eine wichtige Komponente, die bei der Verwaltung der Kommunikation zwischen der ISE und dem Datenbankserver hilft. Er überwacht und verarbeitet Anforderungen, die sich auf die Datenbank beziehen, und stellt sicher, dass das ISE-System in der zugrunde liegenden Datenbank lesen und schreiben kann.

Wichtige Informationen zum Datenbank-Listener-Dienst in der ISE

1. Kommunikationsschnittstelle: Sie fungiert als Kommunikationsbrücke zwischen der ISE und dem Datenbankserver und ermöglicht dem System das Abrufen und Speichern von Daten wie Benutzeranmeldeinformationen, Sitzungsinformationen, Netzwerkrichtlinien usw.

2. Unterstützung für externe Datenbanken: Die ISE kann so konfiguriert werden, dass sie eine externe Datenbank (z. B. Oracle oder Microsoft SQL Server) für die Benutzerauthentifizierung und die Richtlinienspeicherung verwendet. Der Database Listener Service stellt sicher, dass die ISE eine sichere und effiziente Verbindung mit dieser externen Datenbank herstellen und mit dieser interagieren kann.

3. Datenverarbeitung: Der Dienst hört Datenbankabfragen vom ISE-System ab und übersetzt sie dann in die entsprechenden Aktionen in der externen Datenbank. Er kann Anforderungen wie das Einfügen, Aktualisieren oder Löschen von Datensätzen sowie das Abrufen von Informationen aus der Datenbank verarbeiten.

4. Datenbankintegritätsüberwachung: Neben der Bereitstellung des Kommunikationskanals wird auch sichergestellt, dass die Verbindung zur externen Datenbank stabil und funktionsfähig ist. Wenn die Verbindung ausfällt, greift die ISE je nach Konfiguration auf den lokalen Speicher zurück oder wechselt in den heruntergestuften Modus.

Datenbankserver

Der Datenbankserver-Dienst ist für die Verwaltung der Speicherung und des Abrufs der vom System verwendeten Daten verantwortlich. Sie verarbeitet die Interaktion mit der zugrunde liegenden Datenbank, die die ISE zum Speichern von Konfigurationen, Richtlinieninformationen, Benutzerdaten, Authentifizierungsprotokollen, Geräteprofilen und anderen erforderlichen Informationen verwendet.

Wichtige Informationen zum Datenbankserverdienst in der ISE

1. Interne Datenspeicherung: Der Datenbankserver-Dienst verwaltet in erster Linie die interne eingebettete Datenbank, die von der ISE zum lokalen Speichern von Betriebsdaten verwendet wird. Dazu gehören Daten wie Authentifizierungs- und Autorisierungsdatensätze, Benutzerprofile, Netzwerkzugriffsrichtlinien, Geräte- und Endpunktinformationen sowie Sitzungsinformationen.

2. Eingebettete Datenbank: In den meisten Cisco ISE-Bereitstellungen verwendet das System eine eingebettete PostgreSQL-Datenbank für die lokale Speicherung. Der Datenbankserver-Dienst stellt sicher, dass diese Datenbank reibungslos funktioniert, und behandelt alle Abfragen,

Updates und Verwaltungsaufgaben im Zusammenhang mit den darin gespeicherten Daten.

3. Datenbankintegrität: Der Dienst stellt sicher, dass alle Transaktionen ordnungsgemäß verarbeitet werden und dass die Integrität der Datenbank gewahrt bleibt. Sie behandelt Aufgaben wie das Sperren von Datensätzen, das Verwalten von Datenbankverbindungen und das Ausführen von Datenbankabfragen.

Überprüfen und Problembehandlung, ob die Datenbanklistener- und Datenbankserverdienste initialisiert werden oder nicht ausgeführt werden

Der Datenbanklistener und der Datenbankserver sind wichtige Dienste, die zusammen ausgeführt werden müssen, damit alle anderen Dienste ordnungsgemäß funktionieren. Wenn diese Dienste nicht ausgeführt werden oder während der Initialisierung hängen bleiben, helfen diese Schritte zur Fehlerbehebung.

1. Starten Sie die ISE-Dienste mit den Befehlen application stop ise und application start ise neu.

2. Wenn es sich um einen VM-Knoten handelt, muss das Neustarten des Knotens von VM aus die Wiederherstellung der Services unterstützen.

3. Wenn der Knoten ein physischer Knoten ist, muss das Neustarten/Neuladen des Knotens vom CIMC bei der Wiederherstellung der Services helfen.

4. Wenn die Datenbank beschädigt ist, wenden Sie sich zur weiteren Fehlerbehebung an Cisco TAC.

Der Datenbank-Listener und der Datenbankserver werden in der Regel deaktiviert oder können nicht gestartet werden, wenn in der Datenbank eine Diskrepanz besteht oder die Datenbank nicht ordnungsgemäß initialisiert werden kann. In diesen Fällen muss das Zurücksetzen von Anwendungen mithilfe des Befehls application reset-config ise bei der Wiederherstellung und beim erneuten Starten der Datenbank helfen. Durch das Ausführen des Befehls application reset-config ise werden Konfigurationen und Zertifikate entfernt, die Details zu IP-Adresse und Domänenname bleiben jedoch erhalten. Es wird empfohlen, sich an das Cisco TAC zu wenden, um weitere Informationen zu erhalten und die möglichen Auswirkungen zu ermitteln, bevor Sie diesen Befehl auf einen Knoten in der Bereitstellung anwenden.

Anwendungsserver

Der Anwendungsserver ist eine Schlüsselkomponente für die Ausführung und Verwaltung der Kernfunktionen und -dienste der ISE-Plattform. Sie hostet die Geschäftslogik, Benutzeroberflächen und Services, die es der ISE ermöglichen, ihre Rolle bei der Netzwerkzugriffskontrolle, -authentifizierung, -autorisierung, -abrechnung und -richtlinienverwaltung auszuführen.

Wichtige Informationen zum Anwendungsserverdienst in der ISE

1. Benutzeroberfläche: Der Anwendungsserverdienst ist für das Rendern der webbasierten Benutzeroberfläche für die ISE zuständig. Dies ermöglicht Administratoren die Konfiguration und

Verwaltung von Richtlinien, die Anzeige von Protokollen und Berichten und die Interaktion mit anderen Funktionen der ISE.

2. Servicemanagement: Er ist für die verschiedenen Services verantwortlich, die von ISE bereitgestellt werden, einschließlich Richtlinienmanagement, Verwaltungsaufgaben und Kommunikation mit anderen ISE-Knoten in einer verteilten Bereitstellung.

3. Zentralisierte Verarbeitung: Der Anwendungsserverdienst spielt eine zentrale Rolle in der ISE-Architektur und stellt die Logik bereit, die Richtlinien, Authentifizierungsanforderungen und Daten von Netzwerkgeräten, Verzeichnissen und externen Diensten berücksichtigt.

Überprüfung für Anwendungsserver wird initialisiert oder wird nicht ausgeführt

Der Anwendungsserver ist von wenigen Webanwendungen wie Zertifikaten, Ressourcen, Bereitstellung und Lizenzierung abhängig. Wenn eine der Webanwendungen nicht initialisiert werden konnte, bleibt der Anwendungsserver im Initialisierungszustand stecken. Der Anwendungsserver benötigt abhängig von den Konfigurationsdaten auf dem Knoten etwa 15 bis 35 Minuten, um den Status **"Not running" (Nicht ausgeführt)** zu **erreichen** → **Initialisierung** → wird **gestartet**.

1. Stellen Sie sicher, dass das Administratorzertifikat der ISE gültig und in der Bereitstellung für alle Knoten aktiv ist.
2. Stellen Sie sicher, dass alle Knoten in der Bereitstellung mit dem primären Admin-Knoten synchronisiert sind.
3. Wenn es sich bei dem Knoten um eine VM handelt, stellen Sie sicher, dass die empfohlenen Ressourcen dem Knoten zugewiesen sind.

Überprüfen Sie den Status des Anwendungsservers mit dem Befehl **show application status ise** aus der CLI des ISE-Knotens. Die meisten Protokolle zum Anwendungsserver finden Sie unter

Catalina.Out- und Localhost.log-Dateien.

Wenn die genannten Bedingungen erfüllt sind und der Anwendungsserver im Initialisierungszustand verbleibt, sichern Sie das Supportpaket über die CLI/GUI der ISE. Stellen Sie die Dienste mithilfe der Befehle application stop ise und application start ise wieder her bzw. starten Sie die Anwendungen neu.

Profiler-Datenbank

Die Profiler-Datenbank ist eine spezielle Datenbank, in der Informationen über Netzwerkgeräte, Endpunkte und Geräteprofile gespeichert werden, die vom Profiler-Dienst erkannt werden. Der Profiler ist eine wichtige Komponente der ISE, die Netzwerkgeräte (z. B. Computer, Smartphones, Drucker, IoT-Geräte usw.) anhand von Netzwerkmerkmalen und -verhalten automatisch identifiziert und klassifiziert.

Wichtige Informationen zum Profiler-Datenbankdienst in der ISE

1. Erstellung von Geräteprofilen: Die Hauptfunktion des Profiler Database Service besteht darin, den Profilerstellungsprozess zu unterstützen. Die ISE speichert die während der Profilerstellung erfassten Informationen, z. B.:

- Gerätetyp (Beispiel: Smartphone, Laptop, Drucker, IoT-Gerät)

- Gerätebetriebssystem (Beispiel: Windows®, MacOS®, Cisco IOS®, Android®)
- Gerätehersteller
- Netzwerkverhalten oder -muster zur Klassifizierung von Geräten

2. Informationen zum Profiler: Es speichert Profiler-Attribute wie die Gerätehardware- und Softwareprofile, die verwendet werden, um Geräte vordefinierten Richtlinien zuzuordnen. Diese Informationen werden auch verwendet, um Geräte auf Basis ihres Profils dynamisch den richtigen Netzwerkzugriffsrichtlinien oder VLANs zuzuweisen.

3. Profilerstellungsprozess: Der Profilerstellungsprozess basiert in der Regel auf:

- Aktives Profiling: Die ISE fragt aktiv Geräte im Netzwerk nach Informationen ab.
- Passive Profilierung: Die ISE sammelt passiv Daten aus dem Netzwerkverkehr, z. B. DHCP-Anfragen, RADIUS-Attribute, HTTP-Header und andere Netzwerkprotokolle, um den Gerätetyp zu bestimmen.

Überprüfung und Fehlerbehebung bei ISE-Profiling-Services

1. Führen Sie in der ISE-CLI den Befehl show application status ise aus, um zu überprüfen, ob der Profiler-Datenbankdienst ausgeführt wird.

2. Navigieren Sie in der GUI des Knotens Primärer Admin zu Administration > Deployment > wählen Sie den Knoten aus. Klicken Sie auf Bearbeiten, und überprüfen Sie, ob Sitzungsdienste und Profilierungsdienste aktiviert sind.

3. Navigieren Sie nun zu Administration > Deployment > Select the node. Wechseln Sie zur Profiler-Konfiguration, und überprüfen Sie, ob erforderliche Tests zum Sichern der Endpunktdaten aktiviert sind.

4. Navigieren Sie zu Administration > System > Profiling, und überprüfen Sie die für CoA konfigurierten Profilereinstellungen.

5. Aus Kontextsicht > Endpunkte > Wählen Sie die Endpunkte aus, und überprüfen Sie die Attribute, die von verschiedenen Tests für Endpunkte gesammelt wurden.

Hilfreiche Fehlerbehebungen bei der Profilerstellung Probleme:

- Profiler (profiler.log)
- runtime-AAA (prrt-server.log)
- nsf (ise-psc.log)
- nsf-session (ise.psc.log)

ISE-Indizierungsmodul

Die Indexierungs-Engine ist ein Dienst für das effiziente Suchen, Indizieren und Abrufen von Daten, die in der ISE-Datenbank gespeichert sind. Sie verbessert die Leistung und Skalierbarkeit von ISE, insbesondere wenn es um die Verarbeitung großer Datenmengen und den schnellen Zugriff auf Informationen geht, die für Authentifizierungs-, Autorisierungs-, Überwachungs- und

Berichterstellungsaufgaben benötigt werden.

Wichtige Informationen zur ISE-Indizierungsengine in der ISE

1. Datenindizierung: Die ISE-Indizierungsengine erstellt Indizes für verschiedene Datentypen, die in der ISE gespeichert sind, wie z.B. Authentifizierungsprotokolle, Sitzungsprotokolle, Richtlinienzugriffe, Profilierungsdaten und Netzwerkzugriffsdatensätze. Die Indizierung hilft dabei, diese Daten so zu organisieren, dass das Suchen und Abfragen effizienter wird.

2. Protokollverwaltung und Berichterstellung: Dieser Service spielt eine entscheidende Rolle beim Protokollmanagement, da er die Leistung von Berichten und Protokollabfragen verbessert. Bei der Suche nach bestimmten Authentifizierungsereignissen ermöglicht die Indizierungs-Engine beispielsweise einen schnelleren Abruf der gewünschten Datensätze. Dies ist für die Sicherheitsüberwachung und Compliance-Berichte von entscheidender Bedeutung.

3. Datenabruf: Die Indizierungs-Engine muss außerdem sicherstellen, dass die ISE indizierte Daten bei Bedarf effizient aus der zugrunde liegenden Datenbank abrufen kann. So kann die ISE Anfragen über die Benutzeroberfläche, externe Tools oder APIs schnell beantworten.

Vergewissern Sie sich, dass das ISE-Indizierungsmodul nicht ausgeführt oder initialisiert wird.

1. Überprüfen Sie mit dem Befehl **nslookup <FQDN / IP-Adresse des ISE-Knotens >, ob** die DNS-Vorwärts- und -Rückwärtssuche für alle Knoten im Cluster über die CLI funktioniert.
2. Überprüfen Sie, ob die ISE-Administratorzertifikate gültig und für alle Knoten im Cluster aktiv sind.
3. Überprüfen Sie mithilfe des Befehls **show ntp**, ob das NTP funktioniert und mit den ISE-Knoten über die CLI synchronisiert ist.

Die Indizierungs-Engine wird von der Kontexttransparenz verwendet, und die Indizierungs-Engine muss betriebsbereit sein, damit die Kontexttransparenz funktioniert. Nützliche Protokolle, die bei der Fehlerbehebung für die Indexierungs-Engine hilfreich sein könnten, sind **ADE.log**-Dateien, die mithilfe des Befehls **show logging system ade/ADE.log tail** vom Supportpaket gesichert oder über die CLI weitergeleitet werden können.

AD-Anschluss

AD Connector (Active Directory Connector) ist ein Dienst, mit dem die ISE in Microsoft Active Directory (AD) integriert werden kann, sodass die ISE Benutzer anhand ihrer AD-Anmeldeinformationen und Gruppenmitgliedschaften authentifizieren, autorisieren und verwalten kann. Der AD Connector fungiert als Brücke zwischen ISE und Active Directory und ermöglicht ISE die Nutzung von AD zur Netzwerkzugriffskontrolle (NAC) und Richtliniendurchsetzung.

Hauptfunktionen des AD Connector Service in der ISE

1. Integration in Active Directory: Der AD Connector-Dienst fungiert als Brücke zwischen ISE und Active Directory. Sie ermöglicht der ISE eine sichere Verbindung mit AD und ermöglicht ISE so, AD als zentralen Identitätsspeicher für die Benutzerauthentifizierung und Richtliniendurchsetzung zu verwenden.

2. Synchronisierung: Der AD Connector-Dienst unterstützt das Synchronisieren von Benutzer- und

Gruppendaten von Active Directory mit der ISE. So wird sichergestellt, dass die ISE über aktuelle Informationen zu Benutzern und Gruppen verfügt, was für eine genaue Durchsetzung der Richtlinien von entscheidender Bedeutung ist.

3. Sichere Kommunikation: Der AD Connector-Dienst stellt sichere Kommunikationskanäle zwischen ISE und Active Directory her und verwendet in der Regel Protokolle wie LDAP über SSL (LDAPS), um den Datenschutz und die Integrität während der Authentifizierungs- und Abfrageprozesse sicherzustellen.

4. Unterstützung mehrerer Active Directory-Domänen: Der Dienst kann Verbindungen zu mehreren Active Directory-Domänen unterstützen. Dies ist besonders in Umgebungen mit großen oder mehreren Domänen nützlich, in denen die ISE Benutzer aus verschiedenen AD-Gesamtstrukturen oder -Domänen authentifizieren muss.

5. Benutzer- und Gruppensuche: Mit dieser Funktion kann die ISE AD nach Benutzer- und Gruppeninformationen abfragen. Dazu können Details wie Benutzernamen, Gruppenmitgliedschaften und andere Benutzerattribute gehören, die zum Durchsetzen von Netzwerkzugriffsrichtlinien verwendet werden können. Netzwerkzugriffsrichtlinien können beispielsweise basierend auf einer AD-Gruppenmitgliedschaft des Benutzers angewendet werden (Beispiel: Gewährung unterschiedlicher Zugriffsebenen für Benutzer in verschiedenen Gruppen).

1. Stellen Sie sicher, dass das NTP mit den Knoten synchronisiert ist und die Zeitdifferenz zwischen AD und ISE weniger als 5 Minuten betragen muss.

2. Überprüfen Sie, ob der DNS-Server die FQDNs und Domänen auflösen kann, die mit dem AD in Verbindung stehen.

3. Navigieren Sie zu **Vorgänge** > **Berichte** > **Berichte** > **Diagnosen** > **AD-Connector-Vorgänge**, und überprüfen Sie die mit AD zusammenhängenden Ereignisse oder Berichte.

Nützliche Protokolle für die Fehlerbehebung sind **ad_agent.log** mit Debugprotokollen für die **Laufzeitkomponente**.

M&T-Sitzungsdatenbank

Die M&T-Sitzungsdatenbank (Monitoring und Troubleshooting Session Database) spielt eine wichtige Rolle beim Speichern und Verwalten von sitzungsbezogenen Daten für Netzwerkzugriffsereignisse. Die M&T Session Database enthält Informationen zu aktiven Sitzungen, einschließlich Benutzerauthentifizierungen, Geräteverbindungen und Netzwerkzugriffsereignissen, die für die Überwachung, Fehlerbehebung und Analyse von Netzwerkaktivitäten unerlässlich sind.

Schlüsselfunktionen des M&T Session Database Service in der ISE

1. Speicherung von Sitzungsdaten: Der M&T Session Database Service ist für das Speichern und Indizieren von Daten über Benutzer- und Gerätesitzungen im Netzwerk verantwortlich. Dazu gehören Start- und Endzeiten von Sitzungen, Authentifizierungsergebnisse, die Benutzer- oder Geräteidentität und die zugehörigen Richtlinien (z. B. Rollenzuweisungen oder VLAN-Zuweisungen). Die Daten enthalten außerdem RADIUS-Accounting-Informationen, die den Sitzungslebenszyklus detailliert beschreiben, einschließlich der Erstauthentifizierung und aller

Accounting-Meldungen, die Sitzungsereignisse verfolgen.

2. Echtzeit- und Verlaufsdaten: Der Service bietet Zugriff auf Echtzeit-Sitzungsdaten (aktive Sitzungen) und historische Sitzungsdaten (vergangene Sitzungen). So können Administratoren nicht nur den laufenden Benutzerzugriff überwachen, sondern auch auf vergangene Sitzungsprotokolle zurückblicken, um Probleme zu untersuchen oder Zugriffsereignisse zu validieren. Die Echtzeitüberwachung von Sitzungen stellt sicher, dass derzeit keine nicht autorisierten Geräte mit dem Netzwerk verbunden sind.

3. Verbesserte Überwachung: Bietet Einblicke in die Aktivitäten von Benutzern und Geräten, einschließlich der für ihre Sitzungen angewendeten Richtlinien, um potenzielle Sicherheitsbedenken oder nicht autorisierte Zugriffe zu erkennen.

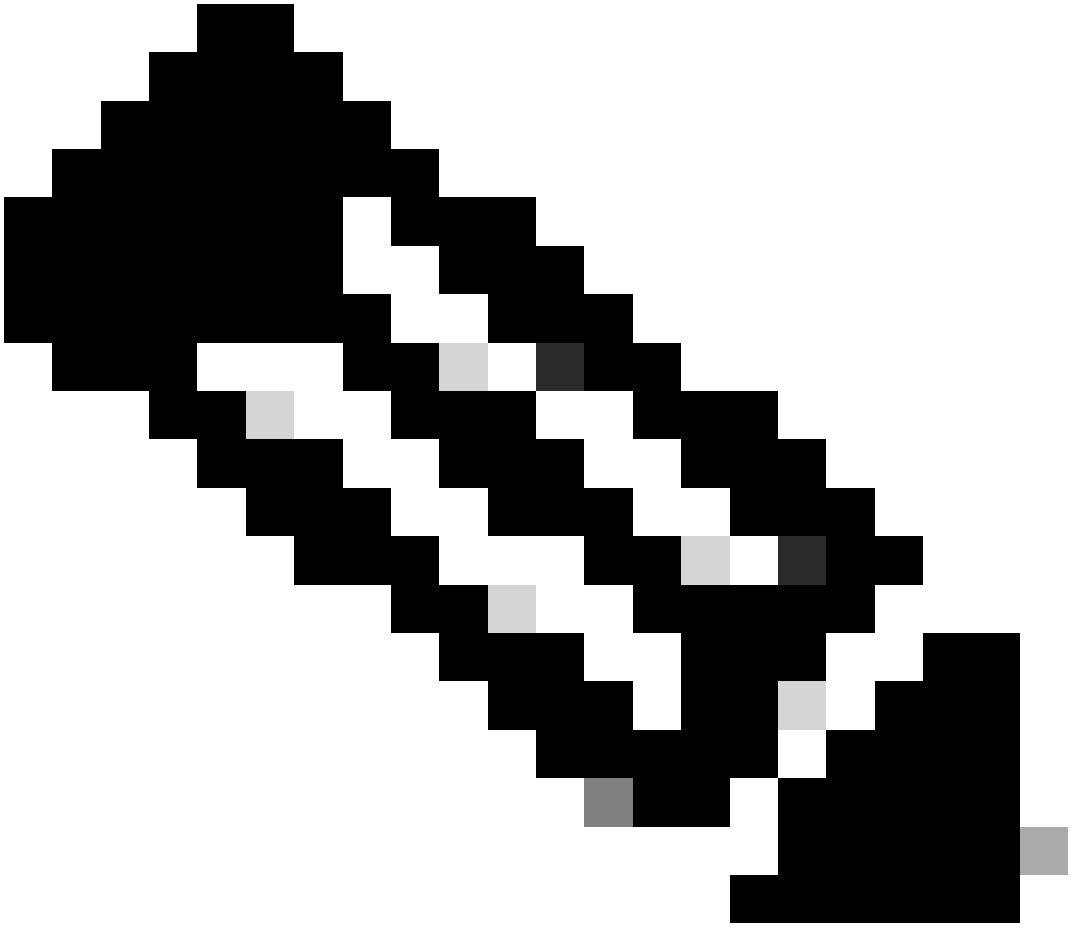
4. Abschlussprüfung und Berichterstattung: Erleichtert Compliance-Audits und Berichterstellung durch das Speichern eines Verlaufs von Netzwerkzugriffsereignissen und die Bereitstellung von Daten für die Erstellung von behördlichen Berichten.

Überprüfung und Fehlerbehebung für die M&T-Sitzungsdatenbank in der ISE

1. Überprüfen Sie, ob dem Knoten empfohlene Ressourcen zugewiesen sind.

2. Sicherer **Showtech-Support** von der ISE CLI zur weiteren Verifizierung des Problems.

3. Setzen Sie die M&T-Sitzungsdatenbank zurück, indem Sie den Befehl **application configure ise** über die ISE-CLI ausführen und Option **1** auswählen.



Anmerkung: Das Zurücksetzen der M&T-Datenbank muss erst nach der Überprüfung der potenziellen Auswirkungen auf die Bereitstellung erfolgen. Wenden Sie sich zur weiteren Überprüfung an das Cisco TAC.

Bekannte Fehler

Cisco Bug-ID： 32364

M&T-Protokollprozessor

Der M&T Log Processor (Monitoring and Troubleshooting Log Processor) ist eine Komponente, die für das Sammeln, Verarbeiten und Verwalten von Protokolldaten verantwortlich ist, die von verschiedenen Diensten innerhalb der ISE generiert werden. Es ist ein wichtiger Bestandteil des Monitoring und Troubleshooting (M&T)-Frameworks, das Administratoren bei der Überwachung und Fehlerbehebung von Netzwerkzugriffsereignissen, Authentifizierungsversuchen, der Richtliniendurchsetzung und anderen Aktivitäten innerhalb des ISE-Systems unterstützt. Der M&T Log Processor übernimmt speziell die Verarbeitung von Protokolleinträgen und stellt sicher, dass

die ISE die notwendigen Informationen für Reporting, Auditing und Fehlerbehebung speichern, analysieren und präsentieren kann.

Hauptfunktionen des M&T Log Processor Service in der ISE

1. Protokollerfassung und -verarbeitung: Der M&T Log Processor Service sammelt und verarbeitet Protokolle, die von verschiedenen ISE-Komponenten generiert werden, wie z. B. Authentifizierungsanforderungen, Autorisierungsentscheidungen, Abrechnungsmeldungen und Richtliniendurchsetzungsaktivitäten. Diese Protokolle enthalten detaillierte Informationen zu Benutzern, Geräten und Netzwerkzugriffsversuchen, z. B. Zeitstempel, Benutzer-IDs, Gerätetypen, angewendeten Richtlinien, Erfolg oder Misserfolg von Zugriffsanfragen und Fehlerursachen.

2. Berichterstattung und Einhaltung: Von diesem Dienst verarbeitete Protokolle sind für das Compliance-Reporting von entscheidender Bedeutung. Viele Vorschriften verlangen, dass Unternehmen Protokolle über Benutzerzugriffe und Sicherheitsereignisse aufbewahren. Der M&T Log Processor Service stellt sicher, dass alle relevanten Protokolle verarbeitet werden und für Audits zur Einhaltung gesetzlicher Vorschriften zur Verfügung stehen. Es unterstützt die Erstellung detaillierter Berichte auf der Grundlage von Protokolldaten, z. B. Benutzerzugriffsprotokolle, Erfolgs-/Fehlerquoten bei der Authentifizierung oder Protokolle zur Richtliniendurchsetzung.

Überprüfung und Fehlerbehebung des M&T Log Processor Service in der ISE

1. Stellen Sie sicher, dass der ISE-Knoten mit den empfohlenen Ressourcen gemäß Cisco Installationshandbuch bereitgestellt wird.

2. Führen Sie den Befehl **show logging system ade/ADE.log tail** über die ISE-CLI aus, um das Problem zu überprüfen und die entsprechenden Ausnahmen/Fehler anzuzeigen.

Bekannte Fehler

Cisco Bug-ID： 15130

Zertifizierungsstellendienst

Der CA-Dienst (Certificate Authority) ist eine wichtige Komponente für die Verwaltung digitaler Zertifikate zur Sicherung der Kommunikation und zur Authentifizierung von Geräten, Benutzern und Netzwerkdiensten. Digitale Zertifikate sind für den Aufbau vertrauenswürdiger Verbindungen und die Gewährleistung einer sicheren Kommunikation zwischen Clients (Computer, Smartphones, Netzwerkgeräte) und Netzwerkinfrastrukturkomponenten (Switches, Wireless Access Points, VPN-Gateways) unerlässlich. Der CA Service der Cisco ISE arbeitet mit X.509-Zertifikaten zusammen, die für verschiedene Zwecke der Netzwerksicherheit verwendet werden, darunter 802.1X-Authentifizierung, VPN-Zugriff, sichere Kommunikation und SSL/TLS-Verschlüsselung.

Schlüsselfunktionen des Zertifizierungsstellendienstes in der ISE

1. Zertifikatsverwaltung: Der Certificate Authority Service ist für die Erstellung, Ausstellung, Verwaltung und Verlängerung digitaler Zertifikate innerhalb der ISE zuständig. Diese Zertifikate werden für verschiedene Authentifizierungsprotokolle und Verschlüsselungszwecke im Netzwerk verwendet. Sie kann entweder als interne Zertifizierungsstelle fungieren oder in eine externe Zertifizierungsstelle integriert werden (Beispiel: Microsoft AD CS, öffentliche CAs wie VeriSign oder DigiCert), um Zertifikate auszustellen.

2. Ausstellung von Zertifikaten: In Umgebungen, die EAP-TLS oder ähnliche zertifikatbasierte Authentifizierungsmethoden erfordern, kann die ISE Zertifikate für Netzwerkzugriffsgeräte (Network Access Devices, NADs), Benutzer oder Endpunkte ausstellen. Die ISE kann automatisch Zertifikate für die Authentifizierung von Geräten und Benutzern generieren und bereitstellen oder Zertifikate von einer externen Zertifizierungsstelle anfordern.

3. Zertifikatregistrierung: Der Zertifizierungsstellendienst unterstützt die Zertifikatregistrierung für Endgeräte wie Laptops, Telefone und andere Netzwerkgeräte, die sich mithilfe von Zertifikaten beim Netzwerk authentifizieren müssen. Die ISE verwendet Protokolle wie SCEP (Simple Certificate Enrollment Protocol) oder ACME (Automated Certificate Management Environment), um die Zertifikatregistrierung für Geräte zu vereinfachen.

4. Erneuerung des Zertifikats: Der Service automatisiert die Verlängerung ablaufender Zertifikate für Geräte und Benutzer. Sie stellt sicher, dass Zertifikate immer gültig und aktuell sind, und verhindert Service-Unterbrechungen, die durch abgelaufene Zertifikate verursacht werden.

5. Integration in externe Zertifizierungsstellen: Die ISE kann zwar als eigene Zertifizierungsstelle fungieren, die Integration in eine externe Zertifizierungsstelle ist jedoch weit verbreiteter (Beispiel: Microsoft Active Directory-Zertifikatdienste). Der CA Service kann die Interaktion zwischen der ISE und der externen CA verwalten und bei Bedarf Zertifikate für Benutzer, Geräte und Netzwerkressourcen anfordern.

EST-Dienst

Der Enrollment over Secure Transport (EST) Service ist ein Protokoll, das zur sicheren Ausgabe digitaler Zertifikate an Netzwerkgeräte und Benutzer in einer zertifikatbasierten Authentifizierungsumgebung verwendet wird. EST ist ein Protokoll zur Zertifikatsregistrierung, mit dem Geräte Zertifikate von einer Zertifizierungsstelle (Certificate Authority, CA) sicher und automatisiert anfordern können. Der EST-Service ist insbesondere für die Geräteauthentifizierung nützlich, z. B. in 802.1X-Umgebungen, VPN-Verbindungen oder BYOD-Szenarien (Bring Your Own Device), bei denen sich Geräte mithilfe von Zertifikaten im Netzwerk authentifizieren müssen.

Wichtigste Funktionen des EST-Service in der ISE

1.Zertifikatregistrierung: Der EST-Dienst ist für die Aktivierung der sicheren Zertifikatregistrierung für Geräte (z. B. Switches, Access Points oder Endgeräte) verantwortlich, die Zertifikate für Authentifizierungszwecke benötigen. Die Registrierung erfolgt über eine sichere Verbindung (in der Regel HTTPS), die sicherstellt, dass der Prozess verschlüsselt ist und vor unberechtigtem Zugriff geschützt ist.

2. Widerruf und Verlängerung von Zertifikaten: Nach der Registrierung von Zertifikaten spielt der EST-Dienst auch eine Rolle bei der Verwaltung des Widerrufs oder der Verlängerung von Zertifikaten. Beispielsweise müssen Geräte nach Ablauf des aktuellen Zertifikats ein neues Zertifikat anfordern. EST kann dabei helfen, diesen Prozess zu automatisieren.

3. Verbesserte Netzwerkzugriffskontrolle: Da Geräte sich mithilfe von Zertifikaten authentifizieren können, stärkt der EST-Dienst den Sicherheitsstatus des Netzwerks, insbesondere in Umgebungen, in denen eine 802.1X-Authentifizierung verwendet wird.

Überprüfen, ob die Zertifizierungsstelle und der EST-Dienst nicht ausgeführt/initialisiert werden

1. Navigieren Sie zu **Administration > System > Certificates > Certificate Authority > Internal CA settings.** Stellen Sie sicher, dass CA-, EST- und OCSP-Responder-Status sortiert und aktiviert ist.
2. Hilfreiche Debugging-Programme, die bei der Fehlerbehebung helfen können, sind Test , Provisioning , ca-service und ca-service-cert. Siehe **toise-psc.log , catalina.out , caservice.log** und **error.log**.
3. Überprüfen, ob die ISE-Stammzertifizierungsstelle und die ISE-Messaging-Zertifikate in der Bereitstellung gültig sind Wenn eine Verlängerung der ISE-Stammzertifizierungsstelle erforderlich ist, navigieren Sie zu **Administration > Certificates > Certificate Signing Requests > Generate Certificate Signing Request, und** wählen Sie usage as **ISE Root CA aus.** Klicken Sie auf **ISE-Stammzertifizierungsstelle** erneuern.

SXP-Moduldienst

Der SXP Engine Service ist für das Management und die Vereinfachung der Kommunikation zwischen der ISE und Netzwerkgeräten unter Verwendung des Security Group Tag (SGT) und des Security Group Exchange Protocol (SXP) zuständig. Sie spielt eine entscheidende Rolle bei der Unterstützung von TrustSec-Richtlinien, die dazu dienen, die Netzwerkzugriffskontrolle auf der Basis der Sicherheitsgruppe des Geräts und nicht nur von IP-Adressen oder MAC-Adressen durchzusetzen. Die SXP-Engine in ISE wird hauptsächlich für den Austausch von Sicherheitsgruppendaten verwendet, was bei der Durchsetzung von Richtlinien basierend auf Benutzer- oder Geräteidentität, Anwendung und Standort hilft. Sie ermöglicht Geräten die gemeinsame Nutzung von Sicherheitsgruppentags (SGTs), die zum Durchsetzen von Sicherheitsrichtlinien für Netzwerkgeräte wie Router und Switches verwendet werden.

Hauptfunktionen des SXP Engine Service in der ISE

1.Integration mit TrustSec: SXP wird in der Regel in Umgebungen bereitgestellt, die Cisco TrustSec nutzen, eine Lösung, die konsistente Sicherheitsrichtlinien in kabelgebundenen und Wireless-Netzwerken durchsetzt. Die SXP Engine vereinfacht die Kommunikation von SGTs zwischen Geräten und ermöglicht eine dynamische Richtliniendurchsetzung basierend auf dem Sicherheitskontext eines Geräts oder Benutzers.

2. Sicherheitsgruppentags (SGTs): Der Kern der Richtliniendurchsetzung bei TrustSec sind SGTs. Diese Tags werden zur Klassifizierung des Netzwerkverkehrs verwendet. Das SXP-Protokoll unterstützt die gemeinsame Nutzung der Zuordnung dieser Tags zu bestimmten Benutzern oder Geräten. Dies ermöglicht eine präzise, richtliniengesteuerte Kontrolle des Netzwerkzugriffs und des Datenverkehrs.

Überprüfung und Fehlerbehebung für den SXP Engine Service in der ISE

1. Standardmäßig ist der SXP Engine-Service in ISE deaktiviert. Um sie zu aktivieren, gehen Sie zu **ISE GUI > Administration > Deployment, wählen Sie den Knoten.** Aktivieren Sie das Kontrollkästchen **Enable SXP Service**, und wählen Sie die Schnittstelle aus. Überprüfen Sie dann den Status des SXP Engine-Service über die ISE-CLI mit dem Befehl **show application status ise.**

2. Falls Probleme bei der Netzwerkkommunikation auftreten, überprüfen Sie, ob die der SXP-Engine zugewiesene Schnittstelle über eine gültige IP-Adresse verfügt, indem Sie den Befehl show interface in der CLI verwenden. Stellen Sie sicher, dass das IP-Subnetz im Netzwerk zugelassen ist.

3. Überprüfen Sie die RADIUS-Live-Protokolle, um die SXP-Verbindungsereignisse auf der ISE zu überprüfen.

4.Aktivieren Sie die SXP-Komponente auf den ISE-Knoten, um relevante Protokolle und Ausnahmen im Zusammenhang mit SXP zu debuggen und zu erfassen.

TC-NAC-Dienst

Der TC-NAC Service (TrustSec Network Access Control) ist eine Komponente, die die Durchsetzung von TrustSec-Richtlinien auf Netzwerkgeräten erleichtert und sicherstellt, dass die Zugriffskontrolle auf Sicherheitsgruppentags (SGTs) und nicht auf herkömmlichen IP- oder MAC-Adressen basiert.

TrustSec wiederum ist ein von Cisco entwickeltes Framework, das die Durchsetzung von Sicherheitsrichtlinien im gesamten Netzwerk auf Basis von Geräterollen, Benutzern oder Kontexten ermöglicht, anstatt veraltete Mechanismen wie VLANs oder IP-Adressen zu verwenden. Sie ermöglicht eine präzisere und dynamischere Netzwerkzugriffskontrolle, indem Geräte in verschiedene Sicherheitsgruppen gruppiert und mit SGTs versehen werden.

Hauptfunktionen des TC-NAC Service in der ISE

1. Integration mit NAC-Systemen von Drittanbietern: Der TC-NAC Service ermöglicht der ISE die Kommunikation und Interaktion mit Netzwerkzugriffskontrolllösungen von Drittanbietern. Dies kann für Organisationen nützlich sein, die bereits über eine NAC-Infrastruktur verfügen, diese aber in die Cisco ISE integrieren möchten, um die Funktionalität zu verbessern, zusätzliche Sicherheitsrichtlinien zu nutzen oder andere Netzwerksicherheitsfunktionen von Cisco zu nutzen.

2. Nahtlose Richtliniendurchsetzung: Bei Integration mit NAC-Lösungen von Drittanbietern kann die ISE bestimmte Aspekte der Richtliniendurchsetzung und Entscheidungsfindung übernehmen. Dadurch wird ein einheitlicheres Richtlinien-Framework geschaffen, das sicherstellt, dass die von Cisco NAC- und anderen Systemen angewendeten Richtlinien im gesamten Netzwerk konsistent sind.

3. Unterstützung für ältere NAC-Systeme: Der TC-NAC Service unterstützt Unternehmen mit vorhandenen NAC-Altsystemen dabei, diese Systeme weiterhin zu verwenden und gleichzeitig die

Cisco ISE für die verbesserten Sicherheitsfunktionen einzusetzen. Die ISE kann in ältere NAC-Lösungen integriert werden und deren Lebenszyklus verlängern. Sie bietet Zugriffskontrolle, Sicherheit und Compliance-Durchsetzung gleichzeitig.

4. Vereinfachung der NAC-Anbieterkommunikation mit Drittanbietern: Dieser Service ermöglicht der ISE die Kommunikation mit NAC-Lösungen von Drittanbietern, die proprietäre Protokolle oder Standards verwenden. Die ISE kann mit NAC-Systemen von Drittanbietern über Standardprotokolle (wie RADIUS, TACACS+ oder SNMP) oder benutzerdefinierte APIs interagieren, je nach verwendeter NAC-Lösung.

Überprüfung und Fehlerbehebung des TC-NAC-Service in der ISE

1. Überprüfen Sie, ob Threat Centric NAC aktiviert ist, indem Sie zu **Administration > Deployment > PSN node > Enable Threat Centric NAC** navigieren.

2. Wenn das Problem beim SourceFire FireAMP-Adapter liegt, überprüfen Sie, ob **Port 443** in Ihrem Netzwerk zulässig ist.

3. Überprüfen Sie die Sitzungsdetails für den Endpunkt unter **Operations > Threat-Centric NAC Live Logs (Vorgänge > Bedrohungsorientierte NAC-Live-Protokolle).**

Durch Threat Centric NAC ausgelöste Alarme:

- Adapter nicht erreichbar (Syslog-ID: 91002): Zeigt an, dass der Adapter nicht erreicht werden kann.
- Adapterverbindung fehlgeschlagen (Syslog-ID: 91018): Zeigt an, dass der Adapter erreichbar ist, die Verbindung zwischen dem Adapter und dem Quellserver jedoch nicht hergestellt wurde.
- Adapter aufgrund eines Fehlers angehalten (Syslog-ID: 91006): Dieser Alarm wird ausgelöst, wenn sich der Adapter nicht im gewünschten Zustand befindet. Wenn dieser Alarm angezeigt wird, überprüfen Sie die Adapterkonfiguration und die Serververbindung. Weitere Informationen finden Sie in den Adapterprotokollen.
- Adapterfehler (Syslog-ID: 91009): Zeigt an, dass der Qualys-Adapter keine Verbindung mit der Qualys-Site herstellen oder Informationen von dieser Site herunterladen kann.

Hilfreiche Fehlerbehebungen für TC-NAC-Probleme:

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

PassiveID-WMI-Dienst

Der PassiveID-WMI-Dienst ist ein Dienst, mit dem die ISE die Erstellung von Geräteprofilen mithilfe von Windows Management Instrumentation (WMI) als passiven Mechanismus zur

Identifizierung und Profilierung von Endpunkten im Netzwerk durchführen kann. Sie spielt eine entscheidende Rolle bei der Erstellung von Geräteprofilen, insbesondere in Umgebungen, in denen Geräte mit Windows OS für die Netzwerkzugriffskontrolle und Richtliniendurchsetzung genau identifiziert werden müssen.

Hauptfunktionen des PassiveID-WMI-Dienstes in der ISE

1. Geräteidentitätserfassung: Der WMI-Dienst PassiveID ermöglicht der ISE die passive Erfassung von Identitätsinformationen von Windows-Geräten mithilfe von Windows Management Instrumentation (WMI). Es erfasst Systemdetails, wie den Hostnamen des Geräts, die Betriebssystemversion und andere relevante Attribute, ohne dass das Gerät aktiv daran teilnehmen muss.

2. Integration in die ISE-Richtlinie: Die vom PassiveID-WMI-Dienst erfassten Informationen sind in das ISE-Richtlinien-Framework integriert. Sie hilft bei der dynamischen Anwendung von Richtlinien, die auf Geräteattributen wie Typ, Betriebssystem und Einhaltung von Sicherheitsstandards basieren.

PassiveID WMI-Dienst überprüfen und Fehlerbehebung durchführen

Eine äußerst sichere und präzise Quelle sowie die gängigste, von der Benutzerinformationen empfangen werden können. Als Probe arbeitet AD mit der WMI-Technologie, um authentifizierte Benutzeridentitäten bereitzustellen. Außerdem fungiert AD selbst, anstatt der Probe, als Quellsystem (ein Anbieter), von dem andere Proben ebenfalls Benutzerdaten abrufen.

Hilfreiche Debugging-Informationen und Informationen, die für die Fehlerbehebung erforderlich sind. Legen Sie diese Attribute auf die Debugging-Ebene für PassiveID-WMI-Probleme fest:

- PassiveID (Passiveid*)
- Runtime-logging (prrt-server.log)
- Active Directory (ad)_agent.log - Ablaufverfolgungsebene
- Collector (collection.log) (auf PassiveID-, MnT-Knoten und auf aktivem pxGrid-Knoten, wenn Sitzungen veröffentlicht werden)
- pxGrid (pxgrid/) (auf sekundärem MnT und aktivem pxGrid-Knoten, wenn die Sitzungen veröffentlicht werden)

Für die Fehlerbehebung von PassiveID WMI erforderliche Informationen:

1. Ob es vorher funktioniert hat? Alle kürzlich vorgenommenen Änderungen (Wie Upgrade, Patch-Installation auf ISE/Upgrade auf RZ)
2. Funktioniert die Testverbindung ordnungsgemäß (vor der Integration auf Testverbindung überprüfen)
3. Details zum Benutzernamen, der für den Beitritt zu AD verwendet wird, und zum Benutzernamen, der für WMI verwendet wird (unabhängig davon, ob es sich um ein Administratorkonto oder ein anderes Konto handelt)
4. Überprüft, ob die Ereignisse (4768, 4770) im Rechenzentrum protokolliert werden. (Ereignisanzeige-Protokoll von Rechenzentrum)

5. Erfassungsprotokolle: Legen Sie die Debug-Ebene für passive ID und Laufzeitprotokollierung fest, und führen Sie dann die Konfiguration wmi für diesen DC, AD - die Ablaufverfolgungsebene mit Zeitstempel aus.

PassiveID-Syslog-Dienst

Der PassiveID Syslog Service ist ein Dienst, mit dem die PassiveID-Profilierungsfunktion Syslog-Meldungen von Netzwerkgeräten in der Umgebung sammeln und verarbeiten kann. Diese Syslog-Meldungen enthalten wichtige Informationen über die mit dem Netzwerk verbundenen Endpunkte, die von der ISE zur Profilerstellung dieser Geräte für die Netzwerkzugriffskontrolle und Richtliniendurchsetzung verwendet werden.

Schlüsselfunktionen des Passiv-ID-Syslog-Service

1. Passive Authentifizierung: Der Passive ID Syslog-Service ermöglicht der Cisco ISE die passive Authentifizierung von Benutzern und Geräten, indem Syslog-Meldungen von Netzwerkgeräten (wie Switches oder Routern) gesammelt werden, die auf Benutzer- und Gerätaktivität hinweisen. Dies ist in Situationen nützlich, in denen herkömmliche aktive Authentifizierungsmethoden wie 802.1X nicht geeignet oder durchführbar sind.

2. Ereignisprotokollierung: Der passive ID-Syslog-Dienst nutzt das Syslog-Protokoll, um Protokolle von Netzwerkgeräten zu empfangen, die den Benutzerzugriff und das Verhalten im Netzwerk nachverfolgen. Die in diesen Protokollen enthaltenen Informationen können z. B. Anmeldeversuche von Geräten, Access Points und Schnittstellendetails umfassen, anhand derer die ISE das Gerät oder den Benutzer passiv identifizieren kann.

PassiveID API-Dienst

Der PassiveID API Service ermöglicht die Integration mit Systemen, die Informationen über die Identität von Geräten oder Benutzern benötigen, die mit dem Netzwerk verbunden sind. Es wird in der Regel in Umgebungen eingesetzt, in denen Netzwerkadministratoren identitätsbasierte Richtlinien und Aktionen durchführen möchten, ohne dass für jedes Gerät aktive Netzwerkauthentifizierungsprotokolle wie 802.1x erforderlich sind.

Hauptfunktionen des Passive ID API Service

1. Integration in externe Systeme: Über die Passive ID-API kann die ISE Identitätsinformationen von Systemen oder Netzwerkgeräten von Drittanbietern (wie Switches, Routern, Firewalls oder anderen Systemen, die identitätsbezogene Ereignisse generieren können) empfangen. Diese externen Systeme können Informationen wie Syslog-Meldungen, Authentifizierungsprotokolle oder andere relevante Daten senden, die der ISE helfen, Benutzer oder Geräte passiv zu identifizieren.

2. Passive Authentifizierung: Der API-Dienst für passive IDs dient zur passiven Authentifizierung von Benutzern und Geräten, indem Identitätsdaten ohne aktive Authentifizierung erfasst werden (Beispiel: 802.1X-, MAB- oder Web-Authentifizierung ist nicht erforderlich). So können beispielsweise Informationen von Netzwerkgeräten, Active Directory-Protokollen oder Sicherheitsanwendungen erfasst und zur Identifizierung von Benutzern oder Geräten verwendet

werden.

3. Zuordnen von Identitätsinformationen: Die Passive ID-API kann verwendet werden, um Identitätsdaten bestimmten Sicherheitsrichtlinien zuzuordnen. Diese Informationen werden verwendet, um Benutzern und Geräten dynamisch Sicherheitsgruppen-Tags (SGTs) oder Rollen zuzuweisen, was sich dann auf die Durchsetzung von Netzwerkzugriffskontrollen (wie Segmentierung und Firewall-Richtlinien) auswirkt.

PassiveID-Agent-Dienst

Der PassiveID Agent Service ermöglicht die Erstellung von Geräteprofilen mithilfe von PassiveID Agents, die auf Endgeräten (z. B. Computern, Laptops, Mobilgeräten usw.) installiert sind. Mit dem Passive ID Agent kann die ISE Profilierungsinformationen über Geräte im Netzwerk sammeln, indem sie den Datenverkehr von Endpunkten abhört, ohne dass aktive Scans oder direkte Interaktionen mit den Geräten erforderlich sind.

Schlüsselfunktionen des Dienstes für passive ID-Agenten

1. Passive Benutzer- und Geräteerkennung: Der passive ID-Agent-Dienst sammelt Identitätsdaten passiv, in der Regel von Netzwerkgeräten oder Endgeräten, und sendet diese Daten an die ISE. Mit diesem Service kann die ISE Benutzer und Geräte anhand ihrer Aktivitäten oder Merkmale authentifizieren und identifizieren, ohne dass eine aktive Authentifizierung durch das Gerät erforderlich ist (Beispiel: ohne Bereitstellung von 802.1X-Anmeldedaten).

2. Integration in andere Cisco Komponenten: Der passive ID-Agent arbeitet eng mit Netzwerkgeräten von Cisco wie Switches, Wireless-Controllern und Access Points zusammen, um identitätsbezogene Informationen aus dem Netzwerkverkehr, Syslog-Protokollen oder anderen Managementsystemen zu erfassen. Die Lösung kann auch in Cisco TrustSec und Cisco Identity Services integriert werden, um diese Daten spezifischen Security Group Tags (SGTs) oder anderen identitätsbasierten Richtlinien zuzuordnen.

3. Kontextabhängige Netzwerkzugriffskontrolle: Der passive ID-Agent sendet diese Informationen an die Cisco ISE, die dann die entsprechenden Zugriffskontrollrichtlinien auf Basis der Identität und des Kontexts des Benutzers oder Geräts anwendet. Dies kann Folgendes umfassen:

- Rollenbasierte Zugriffskontrolle
- Dynamische VLAN-Zuordnung
- Netzwerksegmentierung:
- Durchsetzung von Sicherheitsrichtlinien auf Basis der Benutzerrolle oder des Sicherheitsstatus des Geräts

PassiveID-Endpunktdienst

Der PassiveID Endpoint Service ist ein Dienst, der für die Identifizierung und Profilerstellung von Endpunkten (Geräten) im Netzwerk auf Basis der PassiveID-Technologie verantwortlich ist. Dieser Service unterstützt die ISE bei der Erfassung, Verarbeitung und Klassifizierung von Informationen über Geräte, die eine Verbindung mit dem Netzwerk herstellen, ohne dass eine aktive Interaktion

mit den Endgeräten erforderlich ist. Der Passive ID-Endpunktdienst spielt eine entscheidende Rolle bei der Profilerstellung, der Netzwerkzugriffskontrolle und der Durchsetzung von Sicherheitsrichtlinien.

Hauptfunktionen des PassiveID-Endpunktdiensts

1. Passive Benutzer- und Geräteerkennung: Der Passive ID Endpoint Service ermöglicht es der Cisco ISE, Geräte im Netzwerk passiv zu identifizieren und zu authentifizieren, indem Informationen aus Netzwerkaktivitäten oder Systemprotokollen genutzt werden. Dies umfasst die Identifizierung von Benutzern und Geräten anhand ihres Netzwerkverhaltens oder ihrer Eigenschaften, z. B. MAC-Adresse, IP-Adresse oder Anmeldeinformationen aus einem externen Identitätsspeicher wie Active Directory (AD).

2. Datenerfassung von Endpunkten: Der Endpoint Service sammelt verschiedene Arten endpunktspezifischer Daten aus verschiedenen Quellen:

- Benutzeranmeldeinformationen aus externen Identitätsspeichern wie Active Directory oder anderen Verzeichnissen.
- Gerätemerkmale wie IP-Adressen, MAC-Adressen und Gerätetyp (Beispiel: ob es sich um einen Windows-PC, ein Mobiltelefon oder ein IoT-Gerät handelt).
- Netzwerkaktivitäten von Endpunkten wie DHCP-Anfragen, ARP-Anfragen und andere Kommunikationen auf Netzwerkebene.

PassiveID-SPAN-Dienst

Der PassiveID SPAN-Service nutzt SPAN-Port-Spiegelung (Switched Port Analyzer) auf Netzwerkgeräten, um den Netzwerkverkehr für die Erstellung von Endgeräteprofilen zu erfassen und zu analysieren. Dieser Service unterstützt die ISE bei der passiven Erfassung von Informationen über Endgeräte (Geräte) im Netzwerk. Dabei werden die Kommunikationsmuster im Netzwerk analysiert, ohne dass aktive Diagnosetools oder Agenten auf den Geräten selbst installiert werden müssen.

Hauptfunktionen des PassiveID SPAN-Service

1. Passive Identitätserfassung aus SPAN-Datenverkehr: Der PassiveID SPAN-Service ermöglicht der ISE die Erfassung von Identitätsdaten auf Basis des Netzwerkverkehrs, der über einen SPAN-Port an einem Switch gespiegelt oder kopiert wird. Ein SPAN-Port wird normalerweise für die Netzwerküberwachung verwendet, indem der Netzwerkverkehr von anderen Ports oder VLANs gespiegelt wird. Durch die Erfassung dieses Datenverkehrs kann die ISE beispielsweise folgende Identitätsinformationen passiv erfassen:

- MAC-Adressen von Geräten
- Mit Geräten verknüpfte IP-Adressen
- DHCP-Anfragen oder andere identitätsbezogene Informationen vom erfassten Datenverkehr.
- Authentifizierungsprotokolle von Netzwerkgeräten wie Switches oder Wireless Controllern

2. Erfassung von Informationen zur Benutzer- und Geräteidentität: Der SPAN-Service hört den

Datenverkehr im Netzwerk ab und identifiziert wichtige Identitätsinformationen aus den Netzwerkpaketen, ohne direkt mit den Geräten interagieren zu müssen. Dies kann Daten wie die folgenden umfassen:

- Benutzeridentitäten bei der Authentifizierung über Protokolle wie EAP (Extensible Authentication Protocol).
- Geräteidentitäten basierend auf MAC- und IP-Adressen.
- Geräterollen und -verhalten basierend auf den beobachteten Datenverkehrsmustern und -ereignissen

Überprüfung und Fehlerbehebung für den PassiveID-Stack (PassiveID SPAN-Service, PassiveID Syslog-Service, PassiveID Endpoint-Service, PassiveID Agent, PassiveID API-Service)

1. Der PassiveID-Stapel ist eine Liste von Anbietern, und alle Dienste im PassiveID-Stapel sind standardmäßig deaktiviert. Navigieren Sie zu ISE GUI > Administration > Deployment > Wählen Sie den Knoten, Enable Passive Identity Service, und klicken Sie auf Save. Um den Status des PassiveID-Stapeldiensts zu überprüfen, melden Sie sich bei der CLI des ISE-Knotens an, und führen Sie den Befehl show application status ise aus.

2. Wenn Probleme mit dem passiven ID-Agenten auftreten, überprüfen Sie, ob der FQDN des Agenten vom ISE-Knoten aus auflösbar ist. Melden Sie sich dazu bei der ISE-CLI an, und führen Sie den Befehl nslookup < FQDN of Agent configured > aus.

3. Stellen Sie sicher, dass die ISE-Indizierungsengine aktiv ist und sowohl umgekehrte als auch weitergeleitete DNS-Lookups durch den DNS- oder Namensserver aufgelöst werden, der in der ISE konfiguriert ist.

4. Um eine nahtlose Kommunikation mit den Syslog-Anbietern zu gewährleisten, überprüfen Sie, ob UDP-Port 40514 und TCP-Port 11468 in Ihrem Netzwerk offen sind.

5. Um den SPAN-Anbieter auf einem Knoten zu konfigurieren, stellen Sie sicher, dass der passive ISE-Identitätsdienst aktiviert ist. Überprüfen Sie mithilfe des Befehls show interface in der ISE-CLI, ob die Schnittstelle, die Sie für den SPAN-Provider konfigurieren möchten, in der ISE verfügbar ist.

Um die Protokolle anhand des Anbieters der passiven ID zu überprüfen, müssen Sie Folgendes überprüfen: passiveid-syslog, passiveid-agent.log, passiveid-api.log, passiveid-endpoint.log, passiveid-span.log. Die genannten Protokolle können vom Support-Paket des ISE-Knotens gesichert werden.

DHCP-Server (DHCP)

Der DHCP-Server-Dienst (dhcpd) ist ein Dienst, der Netzwerkgeräten DHCP-Funktionen (Dynamic Host Configuration Protocol) bereitstellt. Es wird hauptsächlich verwendet, um Geräten (Endpunkten), die eine Verbindung mit dem Netzwerk herstellen möchten, IP-Adressen zuzuweisen. In der ISE spielt der DHCP-Server eine entscheidende Rolle bei der Bereitstellung von IP-Adressen für Endpunkte, die diese bei der Verbindung mit dem Netzwerk anfordern. Der Service kann außerdem zusätzliche Konfigurationsinformationen bereitstellen, z. B. DNS-Server,

Standard-Gateway und andere Netzwerkeinstellungen.

Wichtigste Funktionen des DHCP-Server-Dienstes (dhcpd) in der ISE

1. Dynamische IP-Adresszuweisung: Der dhcpd-Dienst in der ISE fungiert als DHCP-Server, der Geräten, die eine IP-Adresse anfordern, wenn sie eine Verbindung mit dem Netzwerk herstellen, eine IP-Adressenzuweisung bereitstellt. Dies ist in Szenarien wichtig, in denen Geräte dem Netzwerk dynamisch beitreten, z. B. in BYOD-Umgebungen (Bring Your Own Device) oder wenn Geräte so konfiguriert sind, dass sie ihre IP-Adressen automatisch beziehen.

2. Profilbasiertes DHCP: Der dhcpd-Dienst kann IP-Adressen basierend auf dem Profil des Geräts zuweisen. Wenn die ISE ein Profil für das Gerät erstellt hat (Beispiel: ob es sich um ein Smartphone, einen Laptop oder ein IoT-Gerät handelt), kann es je nach Gerätetyp oder Rolle eine geeignete IP-Adresse zuweisen oder andere Einstellungen übernehmen.

3. Unterstützung für DHCP-Relay: Die ISE kann als DHCP-Relay-Agent fungieren und DHCP-Anfragen von Geräten an einen externen DHCP-Server weiterleiten, wenn die ISE die tatsächliche IP-Adresszuweisung nicht verarbeitet. In diesem Fall kann der dhcpd-Dienst Anfragen von Geräten an einen zentralen DHCP-Server weiterleiten, während die ISE weiterhin Netzwerkrichtlinien und Zugriffskontrollen anwendet.

Überprüfung und Fehlerbehebung beim DHCP-Server (DHCP)

1. Wenden Sie sich an das Cisco TAC, um zu überprüfen, ob das DHCP-Serverpaket auf der ISE installiert ist.

2. Melden Sie sich beim Stamm der **ISE an > rpm -qi dhcp**.

DNS-Server (benannt)

Der DNS-Server-Dienst (mit dem Namen) ist ein Dienst, mit dem die ISE als DNS-Server (Domain Name System) oder DNS-Resolver fungieren kann. Er ist in erster Linie für die Auflösung von Domänennamen in IP-Adressen und umgekehrt zuständig und erleichtert so die Kommunikation zwischen Geräten im Netzwerk.

Wichtigste Funktionen des DNS-Server-Dienstes (benannter Dienst) in der ISE

1. DNS-Auflösung für ISE-Kommunikation: Der benannte Service in der ISE hilft, Domänennamen in IP-Adressen aufzulösen. Dies ist besonders dann wichtig, wenn die ISE eine Verbindung zu anderen Netzwerkgeräten oder externen Services (wie Radius-Servern, Active Directory oder externen NTP-Servern) herstellen muss, indem Domänennamen anstelle von IP-Adressen verwendet werden.

- Wenn die ISE beispielsweise einen Radius-Server oder einen externen Verzeichnisdienst (wie Active Directory) erreichen muss, muss sie den Domänennamen dieses Servers in eine IP-Adresse auflösen.
- Die ISE fragt den auf dem System konfigurierten DNS-Server ab, um diese Domänennamen aufzulösen und eine reibungslose Kommunikation sicherzustellen.

2. DNS-Auflösung für externe Dienste: Der DNS-Dienst ermöglicht der ISE die Verbindung mit externen Diensten, die Domänennamen erfordern. ISE muss beispielsweise die Namen externer Services wie die folgenden auflösen:

- Cloud-basierte Services:
- NTP-Server (Network Time Protocol)
- Zertifizierungsstellen (Certificate Authorities, CAs) oder LDAP-Server.

3. Domänenübergreifende und redundante DNS-Server: Die ISE kann zur Redundanz für die Verwendung mehrerer DNS-Server konfiguriert werden. Falls ein DNS-Server nicht mehr verfügbar ist, kann die ISE auf einen anderen DNS-Server zurückgreifen, um einen unterbrechungsfreien Betrieb und eine kontinuierliche DNS-Auflösung zu gewährleisten.

Überprüfung und Fehlerbehebung für DNS-Server (benannt)

1. Überprüfen Sie über die CLI des ISE-Knotens mit dem Befehl **ping <IP des DNS-Servers / Namensserver>,** ob der Namensserver oder der DNS-Server der Bereitstellung erreichbar ist.

2. Überprüfen Sie die DNS-Auflösung von ISE FQDNs mithilfe des Befehls **nslookup <FQDN / IP address of ISE nodes>** über die ISE CLI.

ISE-Messaging-Service

Der ISE Messaging Service ist eine Komponente, die die asynchrone Kommunikation zwischen verschiedenen Diensten und Komponenten innerhalb des ISE-Systems ermöglicht. Es spielt eine entscheidende Rolle in der Gesamtsystemarchitektur der ISE und ermöglicht den verschiedenen Teilen der Plattform das Senden und Empfangen von Nachrichten, das Verwalten von Aufgaben und das Synchronisieren von Aktivitäten.

Wichtigste Funktionen des ISE Messaging Service

1. Inter-Process Communication (IPC): Der ISE Messaging Service spielt eine Schlüsselrolle bei der Ermöglichung der prozessübergreifenden Kommunikation (IPC) zwischen verschiedenen ISE-Services. Sie stellt sicher, dass verschiedene ISE-Module und -Services wie Authentifizierung, Autorisierung und Richtliniendurchsetzung Daten und Anweisungen koordiniert austauschen können.

2. Verteilte Umgebungsunterstützung: In größeren oder verteilten ISE-Bereitstellungen (z. B. in Konfigurationen mit mehreren Knoten oder mit hoher Verfügbarkeit) erleichtert der Messaging Service die Kommunikation zwischen den verschiedenen ISE-Knoten. Dadurch wird sichergestellt, dass Daten wie Authentifizierungsanforderungen, Benutzersitzungen und Richtlinienaktualisierungen korrekt über verschiedene Knoten innerhalb des ISE-Systems synchronisiert werden.

3. Synchronisierung von Richtlinien und Konfiguration: Der Messaging Service ist an der Synchronisierung von Konfigurationen und Richtlinien zwischen ISE-Knoten beteiligt. Wenn Konfigurationsänderungen an einem primären Knoten vorgenommen werden, stellt der Service

sicher, dass diese Änderungen an sekundäre oder Backup-Knoten im System weitergeleitet werden. Dies ist wichtig, um die Konsistenz zu gewährleisten und sicherzustellen, dass die Netzwerkzugriffsrichtlinien, die auf verschiedene Standorte oder verteilte ISE-Knoten angewendet werden, synchronisiert bleiben.

Vergewissern Sie sich, dass der ISE Messaging Service nicht ausgeführt wird oder initialisiert wird.

1. Stellen Sie sicher, dass der Port TCP 8671 in der Firewall nicht blockiert ist, da dieser Port für die Kommunikation zwischen ISE-Geräten zwischen Knoten verwendet wird.

2. Überprüfen Sie die ISE-Nachrichten und ISE-Root-Zertifizierungsstellenzertifikate auf Fehler bei der Warteschlangenverbindung, und erneuern Sie ggf. die ISE-Nachrichten, da Fehler bei der Warteschlangenverbindung aufgrund der Beschädigung des internen Zertifikats auftreten würden. Erneuern Sie zur Behebung von Warteschlangenverbindungsfehlern das ISE Messaging- und ISE Root CA-Zertifikat. Verwenden Sie hierzu den folgenden Artikel: ISE - Queue Link Error

3. Aus GUI -> Administration -> Certificates -> Select ISE Messaging Certificate. Klicken Sie auf View, um den Status des Zertifikats zu überprüfen.

Nützliche Protokolle für die Fehlerbehebung beim ISE Messaging Service werden erstellt.log, das im Supportpaket verfügbar ist oder über die CLI mit dem Befehl show logging system ade/ADE.log tail während des Problems aufgerufen werden kann.

4. Wenn die ADE.log-log-Anzeige rabbitmq: Verbindung verweigert Fehler, wenden Sie sich an Cisco TAC, um die Sperre für Rabbitmq-Modul von ISE Root zu entfernen.

ISE API-Gateway-Datenbankdienst

Der ISE API Gateway Database Service ist eine Komponente, die für das Management und die Verarbeitung von Daten im Zusammenhang mit API-Anfragen und -Antworten innerhalb des ISE-Systems verantwortlich ist. Sie fungiert als Vermittler, der das ISE API-Gateway mit der ISE-Datenbank verbindet, um sicherzustellen, dass benutzerdefinierte Anwendungen Daten auch innerhalb der ISE aktualisieren oder ändern können (z. B. durch Anpassung von Zugriffsrichtlinien oder Hinzufügen/Entfernen von Benutzern). Dies geschieht über API-Aufrufe, die vom Dienst verwaltet werden.

Hauptfunktionen des ISE API Gateway Database Service (ISE-API-Gateway)

1. API-Zugriff auf ISE-Daten: Der ISE API Gateway Database Service fungiert als Bridge und ermöglicht externen Anwendungen die Interaktion mit der ISE-Datenbank über die ISE RESTful-APIs. Diese APIs können zum Abrufen oder Ändern von Daten verwendet werden, die in der ISE-Datenbank gespeichert sind. Beispiele:

- Benutzerauthentifizierungsprotokolle
- Netzwerkzugriffsrichtlinien.
- Erstellung von Geräteprofilen.

- Systemkonfiguration und -einstellungen

2. Externe Systemintegrationen aktivieren: Dieser Service spielt eine entscheidende Rolle bei der Integration der ISE in externe Systeme wie:

- Externe Authentifizierungsserver (LDAP, Active Directory, RADIUS).
- Netzwerkmanagementsysteme (NMS).
- Security Information and Event Management (SIEM)-Lösungen
- Individuelle Anwendungen oder Services, die mit ISE-Daten interagieren müssen.

Durch die Bereitstellung des API-Zugriffs ermöglicht der API Gateway Database Service diesen externen Systemen die Abfrage von ISE-Daten, das Senden von Updates an die ISE oder das Auslösen bestimmter Aktionen innerhalb der ISE als Reaktion auf externe Ereignisse.

3. Unterstützung der RESTful API-Kommunikation: Die ISE stellt RESTful-APIs bereit, die für die Verwendung über HTTP/HTTPS konzipiert sind. Der API Gateway Database Service verwaltet den Fluss der API-Anfragen und -Antworten und stellt sicher, dass die Anfragen authentifiziert und verarbeitet werden und dass entsprechende Daten aus der ISE-Datenbank als Antwort zurückgegeben werden.

ISE API-Gateway-Service

Der ISE API Gateway Service ist eine wichtige Komponente, die RESTful API-Zugriff auf ISE-Services, -Daten und -Funktionen bietet. Sie fungiert als Brücke zwischen der ISE und externen Systemen, sodass diese Systeme programmgesteuert mit der ISE-Netzwerkzugriffskontrolle, Richtliniendurchsetzung, Authentifizierung und anderen Services interagieren können. Das API-Gateway ermöglicht die Interaktion von Drittanbieteranwendungen, Netzwerkmanagementsystemen und benutzerdefinierten Anwendungen mit der Cisco ISE, ohne dass manuelle Eingriffe oder direkter Zugriff auf die ISE-Benutzeroberfläche erforderlich sind.

Wichtigste Funktionen des ISE API Gateway Service

1. API-Zugriff auf ISE aktivieren: Der ISE API Gateway Service ermöglicht externen Systemen den sicheren Zugriff auf und die Interaktion mit Cisco ISE-Daten und -Richtlinien über RESTful-APIs. Dies ermöglicht den programmgesteuerten Zugriff auf ISE-Funktionen wie Authentifizierung, Richtliniendurchsetzung, Sitzungsmanagement und vieles mehr.

2. Programmgesteuerte Kontrolle: Der API Gateway Service ermöglicht die programmgesteuerte Steuerung von ISE-Funktionen. Administratoren und Entwickler können APIs verwenden, um:

- Abrufen oder Ändern von Netzwerkrichtlinien.
- Abfragen oder Verwalten von Benutzersitzungen und Authentifizierungsprotokollen
- Erstellen und verwalten Sie Regeln für die Netzwerkzugriffskontrolle.
- Auf Geräteprofile zugreifen oder diese aktualisieren.

Diese Kontrolle kann für die Automatisierung oder die individuelle Workflow-Orchestrierung genutzt werden, z. B. für die dynamische Anpassung von Netzwerkzugriffsrichtlinien auf Basis von Echtzeitdaten oder die Integration der ISE in eine breitere Plattform zur

Sicherheitsautomatisierung.

3. Überwachung und Berichterstattung: Der API Gateway Service ermöglicht externen Systemen die Erfassung von Daten aus betrieblichen ISE-Protokollen, dem Sitzungsverlauf und den Details zur Richtliniendurchsetzung. Dies ist wichtig für:

- Compliance-Berichte.
- Sicherheitsüberwachung.
- Reaktion auf Vorfälle:

Über API-Aufrufe können Protokolle, Audit-Informationen und Ereignisse abgerufen werden, sodass Sicherheitsteams ISE-Aktivitäten über ein zentrales Dashboard oder ein zentrales Reporting-Tool überwachen können.

Überprüfung und Fehlerbehebung des ISE API Gateway Service und des ISE API Gateway Database Service

1. Überprüfen Sie, ob das Administratorzertifikat des ISE-Knotens aktiv und gültig ist. Navigieren Sie zu Administration > Certificates > Select the node > Select Admin Certificate. Klicken Sie auf Anzeigen, um den Status des Admin-Zertifikats des ISE-Knotens zu überprüfen.

2. Legen Sie ise-api-gateway, api-gateway, apiservice Komponenten zu debuggen und die Protokolle können mit den folgenden Befehlen verfolgt werden:

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

ISE pxGrid Direct-Service

Der ISE pxGrid Direct Service ist eine wichtige Komponente, die die pxGrid-Funktion (Platform Exchange Grid) in der ISE unterstützt. pxGrid ist eine Cisco Technologie, die eine sichere, standardisierte und skalierbare Datenfreigabe und Integration zwischen Cisco Netzwerksicherheitslösungen und Anwendungen, Services und Geräten von Drittanbietern ermöglicht. Der ISE pxGrid Direct Service ermöglicht die direkte Kommunikation zwischen der ISE und anderen pxGrid-kompatiblen Systemen, ohne dass zwischengeschaltete Geräte oder Dienste erforderlich sind.

Wichtigste Funktionen des ISE pxGrid Direct Service

1. Direkte Integration in Systeme von Drittanbietern: Der ISE pxGrid Direct Service ermöglicht der ISE die direkte Integration in Netzwerksicherheitssysteme von Drittanbietern, wie Firewalls, Router, NAC-Lösungen, SIEM-Plattformen und andere Sicherheitsanwendungen. Sie ermöglicht diesen Systemen den Austausch von Informationen über Netzwerkzugriffsereignisse, Sicherheitsvorfälle und kontextbezogene Netzwerkdaten.

2. Kontextfreigabe: Eine der Hauptfunktionen von pxGrid ist die Freigabe von Kontextinformationen (wie Geräteidentitäten, Benutzerrollen, Sicherheitsstatus und Netzwerkzugriffsinformationen). Mit dem pxGrid Direct Service kann die ISE diesen Kontext direkt

mit anderen Geräten oder Anwendungen teilen, ohne sich auf traditionelle Methoden wie RADIUS oder TACACS+ verlassen zu müssen.

3. Vereinfachte Kommunikation: Mit pxGrid kann die ISE über ein standardisiertes Protokoll mit Drittanbieterlösungen kommunizieren und Informationen austauschen. Dies vereinfacht den Integrationsprozess, da die Systeme nicht für jede einzelne Drittanbieterlösung einzeln integriert werden müssen.

4. Verbesserte Sicherheit und Compliance: Der pxGrid Direct Service verbessert zudem den Sicherheitsstatus und die Compliance, indem er sicherstellt, dass alle Systeme im Netzwerk auf dieselben kontextbezogenen Echtzeitdaten über Benutzer, Geräte und Sicherheitsrichtlinien zugreifen können. Dadurch wird eine besser koordinierte Durchsetzung von Netzwerksicherheitsrichtlinien in der gesamten Umgebung gewährleistet.

Überprüfen und Fehlerbehebung beim ISEPxgrid Direct Service

1. Wenden Sie sich an das Cisco TAC, um zu überprüfen, ob **edda*.lock*** im Ordner /tmp vorhanden ist. Wenn ja, entfernt Cisco TAC die Sperre und startet den Pxgrid Direct Service vom Root neu.

2. Legen Sie die **PxGrid Direct**-Komponente für das Debuggen im ISE-Knoten zur Fehlerbehebung fest. Die Protokolle können mithilfe der folgenden Befehle über das ISE-Supportpaket oder die ISE-CLI gesichert werden:

show logging-Anwendung pxgriddirect-service.log

show logging-Anwendung pxgriddirect-connector.log

Die genannten Protokolle enthalten Informationen zu den von der Cisco ISE abgerufenen und empfangenen Endpunktdaten sowie zum Verbindungsstatus des Pxgrid Connector.

Segmentierungsrichtliniendienst

Der Segmentation Policy Service ist eine Schlüsselkomponente für die Durchsetzung von Netzwerksegmentierungsrichtlinien auf Basis der Benutzeridentität, des Gerätestatus oder anderer kontextbezogener Informationen. Sie ermöglicht die Kontrolle des Zugriffs von Benutzern und Geräten auf bestimmte Netzwerksegmente und stellt sicher, dass nur autorisierte Benutzer oder Geräte auf bestimmte Teile des Netzwerks zugreifen können. Die Segmentierung des Netzwerks ist von entscheidender Bedeutung, um die Angriffsfläche des Netzwerks zu verkleinern, die laterale Bewegung von Bedrohungen zu verhindern und die Einhaltung von Vorschriften sicherzustellen. Der Segmentation Policy Service der ISE dient dazu, diese Netzwerksegmentierungsregeln dynamisch und flexibel im gesamten Netzwerk durchzusetzen.

Hauptfunktionen des Segmentierungsrichtliniendiensts

1. Netzwerksegmente definieren: Der Segmentation Policy Service in der ISE ermöglicht es Administratoren, verschiedene Netzwerksegmente (Subnetze oder VLANs) basierend auf den Eigenschaften von Benutzern oder Geräten zu definieren. Beispiele:

- Geräte mit unterschiedlichen Sicherheitsstufen können unterschiedlichen Segmenten zugeordnet werden (z.B.: vertrauenswürdigen Geräten in einem VLAN und nicht vertrauenswürdigen Geräten in einem anderen).
- Benutzer aus verschiedenen Abteilungen oder Rollen können verschiedenen Netzwerksegmenten zugewiesen werden, um die geringsten Berechtigungen durchzusetzen und den Zugriff auf vertrauliche Ressourcen zu beschränken.

2. Dynamische Segmentierung: Dieser Service ermöglicht eine dynamische Netzwerksegmentierung, d. h. die Netzwerksegmente oder VLANs können sich je nach den Echtzeitbedingungen ändern. Beispiele:

- Ein Benutzer kann einem bestimmten VLAN basierend auf seiner Rolle oder seinem Gerätezustand zugewiesen werden.
- Ein Gerät, das als nicht konform eingestuft wird oder auf dem ein veraltetes Betriebssystem ausgeführt wird, kann in ein Quarantäne- oder Gast-VLAN verschoben werden, bis eine Wiederherstellung erfolgt ist.

3. Richtlinienbasierte Durchsetzung: Der Segmentierungsrichtliniendienst verwendet Richtlinien, um zu entscheiden, in welchem Segment ein Gerät oder ein Benutzer platziert werden muss. Diese Strategien können verschiedene Faktoren berücksichtigen, wie z.B.:

- Benutzeridentität: Basierend auf Benutzerrolle oder Attributen.
- Gerätestatus: Der Status oder Compliance-Status des Geräts (Beispiel: Wird die neueste Antivirensoftware ausgeführt?)
- Ort: Der physische Standort des Benutzers oder Geräts im Netzwerk (Beispiel: Büro, Gastbereich, Remote-Zugriff).
- Zugriffszeit: Die Uhrzeit oder der Wochentag, an dem bzw. an dem die Zugriffsanforderung erfolgt.

4. Durchsetzung von Sicherheitsrichtlinien: Der Segmentation Policy Service stellt sicher, dass Sicherheitsrichtlinien konsistent auf allen Netzwerkgeräten (wie Switches, Routern, Firewalls) durchgesetzt werden, indem Branchenstandards wie RADIUS und VLAN-Zuweisung genutzt werden. So kann die Cisco ISE mit Geräten in der Netzwerkinfrastruktur kommunizieren, um die erforderlichen Segmentierungsrichtlinien durchzusetzen.

Service für die Überprüfung und Fehlerbehebung von Segmentierungsrichtlinien

1. Überprüfen Sie, ob die Segmentierung ordnungsgemäß konfiguriert ist, indem Sie zu Work Centers > TrustSec > Overview > Dashboard navigieren.

2. Work Centers > TrustSec > Reports (Berichte) wählen Sie TrustSec Reports (TrustSec-Berichte) aus, um den Service-Status und die Berichte der Segmentierungsrichtlinie zu überprüfen.

REST-Authentifizierungsdienst

Der REST-Auth-Dienst stellt Authentifizierungsfunktionen mithilfe von RESTful-APIs bereit. Externe Anwendungen und Systeme können Benutzer oder Geräte authentifizieren, indem sie mit

der ISE über HTTP(S) unter Verwendung von Standard-REST-Protokollen interagieren. Dieser Service ermöglicht die nahtlose Integration der Cisco ISE-Authentifizierungsfunktionen in Anwendungen oder Systeme von Drittanbietern, die Benutzer oder Geräte authentifizieren müssen, jedoch nicht die herkömmlichen Methoden (wie RADIUS oder TACACS+) verwenden können.

Schlüsselfunktionen des REST-Authentifizierungsdienstes

1. RESTful-Authentifizierung: Der REST-Auth-Dienst ermöglicht Authentifizierungsanforderungen über das REST-API-Protokoll. Dies ermöglicht externe Systeme (Beispiel: Anwendungen, Netzwerkgeräte oder -dienste von Drittanbietern), um Benutzer oder Geräte mithilfe der ISE als Authentifizierungsserver zu authentifizieren, allerdings über RESTful-Webdienstaufrufe anstelle von herkömmlichen Authentifizierungsprotokollen wie RADIUS oder TACACS+.

2. Integration in externe Anwendungen: Dieser Dienst wurde für externe Anwendungen entwickelt, die Benutzer oder Geräte authentifizieren müssen, aber keine herkömmlichen Authentifizierungsmethoden (wie RADIUS oder TACACS+) verwenden. Stattdessen können sie über REST-APIs mit der ISE interagieren, wodurch die Integration der ISE-Authentifizierung in webbasierte oder Cloud-native Anwendungen vereinfacht wird.

3. Flexible und skalierbare Authentifizierung: Der REST Auth Service bietet eine skalierbare Authentifizierungsmethode, die nicht auf Netzwerkgeräte oder Lösungen vor Ort beschränkt ist. Sie kann von Cloud-Services, mobilen Anwendungen und anderen webbasierten Plattformen verwendet werden, die Benutzer oder Geräte authentifizieren müssen, indem sie die ISE nach Anmeldeinformationen und Richtlinien abfragen.

4. Einfach anzuwenden: Die REST-API bietet eine standardisierte Schnittstelle, die im Vergleich zu herkömmlichen Methoden einfacher in moderne Software und Anwendungen zu integrieren ist. Es bietet Antworten im JSON-Format und verwendet HTTP-Methoden wie GET, POST, PUT und DELETE, wodurch es für Webentwickler und Systeme, die ISE für die Authentifizierung integrieren, leichter zugänglich wird.

Überprüfung und Fehlerbehebung für REST Auth

1. Um Probleme im Zusammenhang mit Open API zu beheben, legen Sie die apisservice-Komponente auf debug fest.

2. Um Probleme im Zusammenhang mit ERS API zu beheben, legen Sie ers-Komponente auf debug fest.

Wenn die GUI-Seite des API-Service: https://{iseip}:{port}/api/swagger-ui/index.html oder https://{iseip}:9060/ers/sdk ist verfügbar. Der API-Dienst funktioniert wie erwartet.

Weitere Informationen zur API finden Sie in der API-Dokumentation.

SSE-Connector

Der SSE Connector (Secure Software-Defined Edge Connector) ist ein Service, der die ISE in die

Cisco Secure Software-Defined Access (SD-Access)-Lösung integriert. Der SSE Connector ermöglicht der ISE die sichere Kommunikation mit dem Cisco DNA Center und ermöglicht automatisierte Netzwerkrichtlinien, Segmentierung und Sicherheitsmanagement am Edge in einer SD-Zugriffsumgebung.

Wichtigste Funktionen des SSE-Connectors

1. Integration in Sicherheitssysteme von Drittanbietern: Der SSE Connector erleichtert die Integration der Cisco ISE in Sicherheitssysteme von Drittanbietern wie Firewalls, Intrusion Prevention Systems (IPS), Network Access Control (NAC)-Lösungen und Security Information and Event Management (SIEM)-Systeme. Sie ermöglicht diesen externen Systemen das sichere Senden und Empfangen von Daten von der ISE, was für eine dynamischere Richtliniendurchsetzung verwendet werden kann.

2. Echtzeit-Bedrohungsinformationen: Durch die Verbindung der ISE mit anderen Sicherheitssystemen ermöglicht der SSE Connector den Austausch von Echtzeit-Bedrohungsinformationen. Zu diesen Informationen können verdächtige Aktivitäten, kompromittierte Endgeräte oder von anderen Sicherheitssystemen erkannte schädliche Verhaltensweisen gehören, sodass die ISE Zugriffsrichtlinien dynamisch an die aktuellen Bedrohungsstufen oder den Gerätestatus anpassen kann.

3. Automatisierte Problembehebung: Die durch den SSE Connector ermöglichte Integration kann automatisierte Problembehebungs-Workflows unterstützen. Wenn ein System beispielsweise durch eine externe Sicherheits-Appliance als kompromittiert gekennzeichnet wird, kann die ISE automatisch Richtlinien durchsetzen, die den Netzwerkzugriff blockieren, oder den Endpunkt zur weiteren Untersuchung an ein Problembehebungs-Netzwerksegment umleiten.

Überprüfung und Fehlerbehebung des SSE-Steckverbinders

1. Der SSE-Connector ist nur aktiviert, wenn der PassiveID-Dienst in der ISE aktiviert ist.

2. Die sse-connector (connector.log)-Komponente im debug bietet weitere Informationen zu SSE Connector-bezogenen Meldungen.

Hermes (pxGrid Cloud-Agent)

Hermes (pxGrid Cloud Agent) ist eine Komponente, die die Integration zwischen der ISE und dem pxGrid (Platform Exchange Grid)-Ökosystem in einer Cloud-Umgebung vereinfacht. Hermes ist der Cloud-basierte Agent für die Kommunikation zwischen der ISE und Cloud-basierten Services oder Plattformen. Er unterstützt das pxGrid-Framework für den Austausch von Kontextinformationen zwischen verschiedenen Netzwerk- und Sicherheitssystemen.

Wichtigste Funktionen von Hermes (pxGrid Cloud Agent)

1. Cloud-to-On-Premises-Integration: Hermes (pxGrid Cloud Agent) wurde entwickelt, um die nahtlose Integration zwischen Cloud-basierten Services und der standortbasierten ISE-Infrastruktur zu erleichtern. Sie erweitert die Leistungsfähigkeit von pxGrid über herkömmliche

standortbasierte Netzwerkumgebungen hinaus und ermöglicht einen sicheren Datenaustausch sowie die Durchsetzung von Richtlinien über Cloud-basierte Anwendungen und Services hinweg.

2. pxGrid-Netzwerkunterstützung: pxGrid ist eine Cisco Plattform für den sicheren Austausch von Kontext und Informationen über Netzwerksicherheitslösungen hinweg. Hermes fungiert als Cloud-Agent für pxGrid und ermöglicht die sichere Kommunikation in Echtzeit zwischen der ISE und verschiedenen Cloud-basierten Services. Dank dieser Integration können Netzwerksicherheitsrichtlinien sowohl in standortbasierten als auch in Cloud-Umgebungen konsistent sein, was das Management und die Durchsetzung von Sicherheitsrichtlinien vereinfacht.

3. Cloud-basierte Endgeräte-Transparenz: Einer der Hauptvorteile von Hermes ist die Transparenz von Cloud-basierten Endgeräten, ähnlich wie die ISE die Transparenz von Endgeräten vor Ort ermöglicht. Es kann Daten über Geräte und Benutzer in der Cloud sammeln, z. B. über deren Compliance-Status, Sicherheitsstatus und Identitätsdaten. So kann die ISE Netzwerkzugriffsrichtlinien für Cloud-Endgeräte ebenso durchsetzen wie für Geräte vor Ort.

4. Nahtlose Erweiterung der ISE auf Cloud-Umgebungen: Einer der Hauptvorteile von Hermes ist die nahtlose Verbindung zwischen der ISE-Umgebung vor Ort und der wachsenden Anzahl Cloud-nativer Anwendungen. So können ISE-Sicherheitsrichtlinien, Authentifizierungsverfahren und Zugriffskontrollen einfacher auf Cloud-Services ausgedehnt werden, ohne dass die vorhandene Infrastruktur komplett überholt werden muss.

Hermes überprüfen und Fehlerbehebung durchführen (PXGrid Cloud Agent)

1. Standardmäßig ist der Hermes-Service deaktiviert. Wenn Sie ISE mit der Cisco PxGrid-Cloud verbinden, wird der Hermes-Service aktiviert. Wenn der Hermes-Service in der ISE deaktiviert ist, überprüfen Sie, ob die Option Pxgrid Cloud in der **ISE-GUI > Administration > Deployment** aktiviert ist, **und wählen Sie ISE-Knoten aus**. Bearbeiten **Sie PXGrid Cloud.**

2. Nützliche Debugs für die Behebung von Problemen im Zusammenhang mit der Pxgrid-Cloud sind **hermes.log** und **pxcloud.log**. Diese Debugs sind nur auf Pxgrid-Knoten verfügbar, auf denen Pxgrid Cloud aktiviert ist.

McTrust (Meraki Sync Service)

McTrust (Meraki Sync Service) ist ein Service, der die Integration zwischen Cisco ISE und Cisco Meraki-Systemen ermöglicht, insbesondere zum Synchronisieren und Verwalten von Netzwerkgeräten und Zugriffsrichtlinien. Der McTrust-Service dient zur Synchronisierung von Benutzer- und Geräteinformationen zwischen der Cloud-basierten Netzwerkinfrastruktur von Meraki und den standortbasierten Identitäts- und Richtlinienmanagementsystemen der ISE.

Wichtigste Funktionen von McTrust (Meraki Sync Service)

1. Nahtlose Integration in Meraki Geräte: McTrust ermöglicht der ISE die Synchronisierung und Integration mit den Cloud-basierten Geräten von Meraki. Dazu gehören Geräte wie Meraki Access Points, Switches und Security-Appliances, die in das Meraki-Portfolio integriert sind. Sie ermöglicht der ISE die direkte Kommunikation mit der Meraki-Infrastruktur und vereinfacht die

Anwendung von Richtlinien für die Netzwerkzugriffskontrolle auf von Meraki verwaltete Geräte.

2. Automatisierte Gerätesynchronisierung: Der Meraki Sync Service synchronisiert automatisch ISE-Richtlinien mit Meraki-Netzwerkgeräten. Das bedeutet, dass alle Änderungen, die an den Richtlinien für die Netzwerkzugriffskontrolle in der ISE vorgenommen werden, automatisch auch von Meraki Geräten übernommen werden, ohne dass manuelle Eingriffe erforderlich sind. Dies erleichtert Administratoren die Verwaltung des Netzwerkzugriffs über Meraki- und ISE-Plattformen hinweg.

3. Richtliniendurchsetzung für von Meraki verwaltete Geräte: Mit McTrust kann die ISE Netzwerkzugriffsrichtlinien auf Meraki-Geräten basierend auf Authentifizierung und Gerätestatus durchsetzen. Sie kann Meraki-Netzwerkelementen dynamisch Richtlinien zuweisen, z. B. die Anpassung von VLAN-Zuweisungen, die Anwendung von Zugriffskontrolllisten (ACLs) oder die Beschränkung des Zugriffs auf bestimmte Netzwerkressourcen, je nach Sicherheitsstatus des Geräts oder des Benutzers, der den Zugriff anfordert.

4. Meraki Dashboard-Integration: McTrust integriert die ISE direkt in das Meraki Dashboard und bietet so eine einheitliche Management-Oberfläche. Durch diese Integration können Administratoren Netzwerkrichtlinien und Zugriffskontrollregeln für Meraki-Geräte und ISE-verwaltete Ressourcen über die Cloud-verwaltete Meraki-Schnittstelle anzeigen und verwalten.

Überprüfen und Fehlerbehebung bei McTrust (Meraki Sync Service)

1. Melden Sie sich bei der ISE-GUI an -> Work Centers -> TrustSec -> Integrations -> Sync status. Überprüfen Sie alle festgestellten Probleme/Fehler.

2. Stellen Sie sicher, dass alle Administratorzertifikate der ISE-Knoten aktiv und gültig sind.

Nützliches Debugging zur Fehlerbehebung des Meraki Sync Service ist meraki-connector.log.

ISE Node Exporter

Der ISE Node Exporter-Service ist eine Komponente für die Überwachung und Erfassung von Leistungsmetriken aus dem ISE-System, insbesondere aus den ISE-Knoten (ob es sich um Administrationsknoten, Überwachungsknoten oder Richtliniendienstknoten handelt).

Wichtigste Funktionen von ISE Node Exporter

1.Metrik-Export: Der ISE Node Exporter stellt eine Reihe leistungsbezogener Kennzahlen bereit, z. B. CPU-Auslastung, Arbeitsspeichernutzung, Festplattenauslastung, Netzwerkstatistiken, Systemauslastung und andere Kennzahlen auf Betriebssystemebene. Diese Metriken werden dann zur Überwachung des Status und der Leistung des ISE-Knotens verwendet und können in einem Überwachungs-Dashboard wie Grafana visualisiert werden.

2. Systemzustandsüberwachung: Durch den Export der Leistungsdaten an Prometheus ermöglicht der ISE Node Exporter eine kontinuierliche Überwachung des Zustands und Betriebsstatus des ISE-Knotens. Administratoren können Warnungen auf der Grundlage vordefinierter Schwellenwerte erstellen, um sie über Leistungsverschlechterungen oder Systemprobleme zu

informieren.

3. Integration von Prometheus: Der ISE Node Exporter wird in der Regel in Verbindung mit Prometheus verwendet, einem Open-Source-Überwachungs- und Warn-Toolkit, das auf Zuverlässigkeit und Skalierbarkeit ausgelegt ist. Der Node Exporter stellt Kennzahlen auf Systemebene bereit, die von Prometheus erfasst und gespeichert werden können, um Zeitreihendaten zu erfassen und zu speichern.

ISE-Prometheus-Service

Der ISE Prometheus Service ist ein Service, der Prometheus mit der ISE integriert, um die Überwachung und Erfassung von Leistungsmetriken aus dem ISE-System zu ermöglichen. Prometheus ist ein Open-Source-Überwachungs- und Warnungs-Toolkit zur Erfassung, Speicherung und Analyse von Zeitreihendaten. Der ISE Prometheus Service ermöglicht es der ISE, ihre internen Metriken für Überwachungszwecke an Prometheus weiterzugeben.

Wichtigste Funktionen des ISE Prometheus Service

1. Metrik-Erfassung für die Überwachung: Der ISE Prometheus Service wurde entwickelt, um verschiedene Betriebs- und Leistungsmetriken für das ISE-System zu exportieren. Zu diesen Metriken gehören in der Regel, jedoch nicht beschränkt auf CPU-Nutzung und Systemlast, Arbeitsspeichernutzung, Festplattennutzung und E/A-Leistung, Netzwerkstatistiken, Statistiken zu Authentifizierungsanforderungen, Statistik zur Richtliniendurchsetzung, Systemzustand- und Betriebsbereitschaftsdaten

2. Integration von Prometheus: Der Prometheus Service ermöglicht es der ISE, Daten in einem mit Prometheus kompatiblen Format verfügbar zu machen, das diese Daten in regelmäßigen Abständen scannt. Anschließend speichert Prometheus die Daten in einer Zeitreihendatenbank, sodass Trends und Leistungsverläufe des ISE-Systems nachverfolgt werden können.

3. Visualisierung und Reporting mit Grafana: Der Prometheus Service in der ISE lässt sich nahtlos in Grafana integrieren, ein beliebtes Open-Source-Visualisierungstool. Nach dem Exportieren der Kennzahlen nach Prometheus können Administratoren die Daten in Echtzeit über Grafana-Dashboards visualisieren. Dies ermöglicht die einfache Identifizierung von Performance-Engpässen, Systemtrends und potenziellen Problemen bei der ISE-Bereitstellung.

ISE Grafana-Service

Der ISE Grafana Service ist ein Service, der mithilfe von Grafana, einer Open-Source-Plattform für Überwachung und Datenvisualisierung, eine Visualisierung der Systemleistungsmetriken ermöglicht. Durch die Integration mit Prometheus können Echtzeit- und Verlaufsdaten angezeigt werden, die von der ISE gesammelt wurden. So können Administratoren interaktive Dashboards erstellen, die Einblicke in die Integrität, Leistung und Nutzung des ISE-Systems liefern.

Wichtigste Funktionen des ISE Grafana Service

1. Anpassbare Dashboards: Grafana ist umfassend anpassbar, sodass Administratoren

Dashboards entsprechend ihren spezifischen Überwachungsanforderungen erstellen und ändern können. Benutzerdefinierte Abfragen können erstellt werden, um bestimmte Datenpunkte aus Prometheus zu extrahieren, und diese Abfragen können in verschiedenen Formaten wie Diagrammen, Tabellen, Heatmaps und mehr visualisiert werden.

2. Zentralisierte Überwachung für verteilte ISE-Bereitstellungen: Für verteilte ISE-Bereitstellungen, bei denen mehrere ISE-Knoten an verschiedenen Standorten bereitgestellt werden, bietet Grafana eine zentrale Ansicht aller Systemmetriken, die von jedem Knoten erfasst werden. So können Administratoren die Leistung der gesamten ISE-Bereitstellung von einem zentralen Punkt aus überwachen.

3. Historische Daten und Trendanalyse: Mithilfe der in Prometheus gespeicherten Daten ermöglicht Grafana eine Verlaufsanalyse von Systemmetriken, sodass Administratoren Trends im Zeitverlauf verfolgen können. So können sie beispielsweise beobachten, wie sich die CPU-Auslastung im letzten Monat verändert hat oder wie sich die Erfolgsraten bei der Authentifizierung verändert haben. Diese Verlaufsdaten sind für die Kapazitätsplanung, Trendanalysen und die Identifizierung langfristiger Probleme hilfreich.

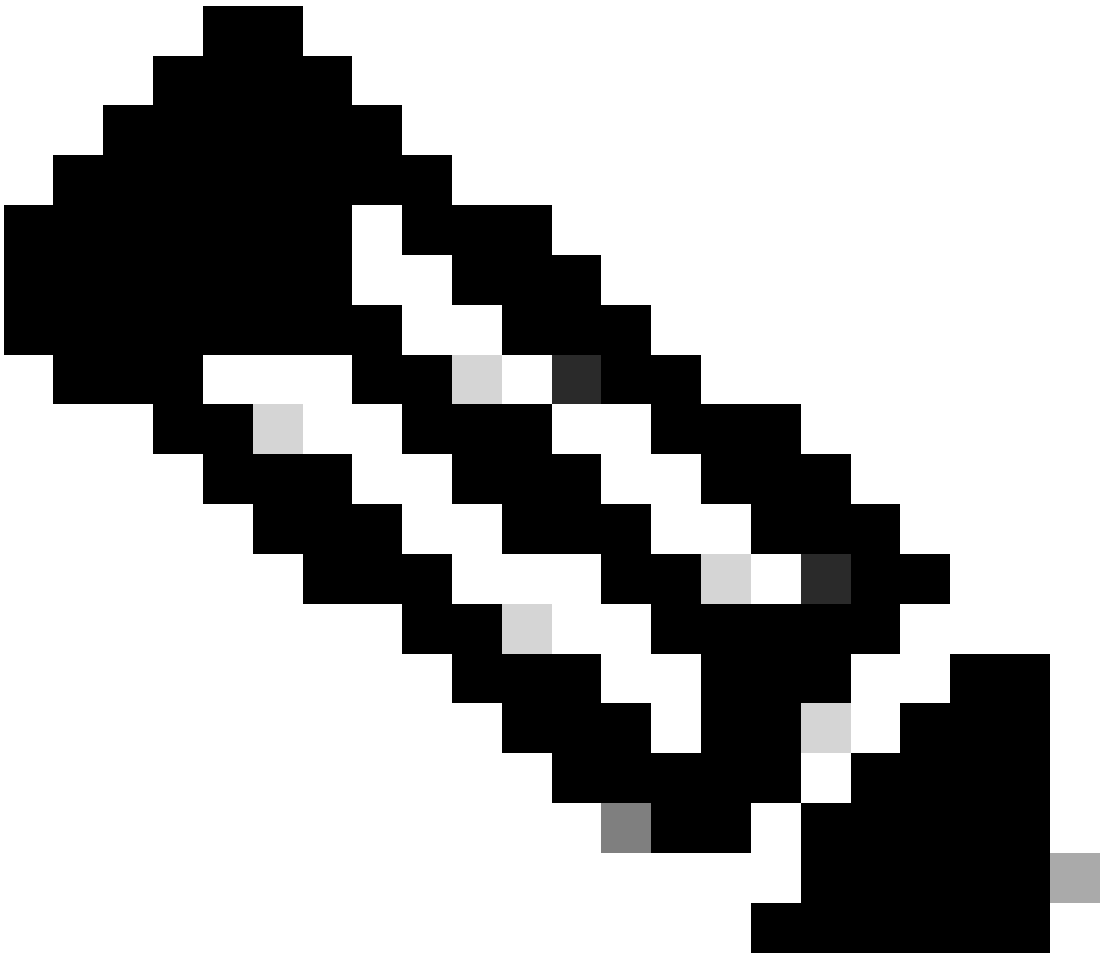
Überprüfen und Fehlerbehebung bei ISE Grafana Service, ISE Prometheus Service, ISE Node Exporter

1. ISE Grafana Service, ISE Prometheus Service und ISE Node Exporter Service arbeiten zusammen und werden als Grafana Stack Services bezeichnet. Es gibt keine speziellen Debugs, die zur Fehlerbehebung für diese Dienste aktiviert werden können. Diese Befehle sind jedoch bei der Fehlerbehebung hilfreich.

show logging-Anwendung ise-prometheus/prometheus.log

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

show logging-Anwendung ise-grafana/grafana.log



Anmerkung: Wenn die Überwachung aktiviert ist, müssen ISE Node Exporter, ISE Prometheus Service und ISE Grafana Service ausgeführt werden, und eine Unterbrechung dieser Services verursacht Probleme bei der Datenerfassung.

ISE MNT LogAnalytics ElasticSearch

ISE MNT LogAnalytics Elasticsearch ist eine Komponente, die Elasticsearch mit ISE Monitoring and Troubleshooting (MNT)-Funktionen integriert. Sie wird für die Protokollaggregation, Suche und Analyse von ISE-Protokollen und -Ereignissen verwendet. Elasticsearch ist eine weit verbreitete Such- und Analysefunktion, die bei der Integration in die ISE die Speicherung, Analyse und Visualisierung von Protokolldaten, die von ISE-Komponenten generiert werden, optimiert.

Wichtigste Funktionen von ISE MNT LogAnalytics Elasticsearch

1. Protokollspeicherung und -indizierung: Der Elasticsearch-Service in der ISE ist für die Speicherung und Indizierung der von der ISE generierten Protokolldaten verantwortlich. Elasticsearch ist eine verteilte Such- und Analysefunktion, mit der ISE-Protokolle so gespeichert werden können, dass bestimmte Ereignisse, Fehler oder Systemaktivitäten schnell durchsucht,

abgefragt und abgerufen werden können.

2. Integration mit Log Analytics: ISE MNT LogAnalytics Elasticsearch bietet zusammen mit Log Analytics eine umfassende Protokollierungslösung. Sie ermöglicht der ISE die Erfassung von Protokolldaten zur Authentifizierung, Richtliniendurchsetzung, zu Systemvorgängen und anderen Aktivitäten. Diese Daten werden in Elasticsearch gespeichert, was die Durchführung detaillierter Analysen und die Gewinnung von Einblicken in das ISE-Verhalten vereinfacht.

3. Zentrale Protokollierung: Durch die Integration mit Elasticsearch bietet die ISE eine zentralisierte Protokollierungslösung, die für Umgebungen, in denen verteilte Protokollerfassung erforderlich ist, von entscheidender Bedeutung ist. Auf diese Weise können Administratoren Protokolle mehrerer ISE-Knoten über eine zentrale, einheitliche Schnittstelle anzeigen und analysieren, was die Fehlerbehebung und Überwachung der ISE-Leistung vereinfacht.

4. Protokollanalyse und Fehlerbehebung: Der ISE MNT LogAnalytics Elasticsearch-Service unterstützt Administratoren bei der Analyse des Systemverhaltens und der Fehlerbehebung, indem er den einfachen Zugriff auf Protokolldaten ermöglicht. Wenn es beispielsweise zu einem plötzlichen Anstieg von Authentifizierungsfehlern oder einem unerwarteten Systemausfall kommt, ermöglicht Elasticsearch die schnelle Abfrage von Protokolldaten, um die Ursache zu identifizieren.

Überprüfung und Fehlerbehebung bei ISE M&T LogAnalytics Elasticsearch

1. Deaktivieren und erneutes Aktivieren des Protokollanalysediensts in der ISE muss hilfreich sein. Navigieren Sie zu Operations > System 360 > Settings > Log analytics (deaktivieren und aktivieren Sie diese Option mit einem Knebel).

2. Durch den Neustart von M&T LogAnalytics vom ISE-Root wird das Problem behoben. Wenden Sie sich an Cisco TAC, um diese Aktion durchzuführen.

Bekannte Fehler

Cisco Bug-ID・ 66198

ISE-Protokolldienst

Der ISE Logstash Service ist eine Komponente, die Logstash, eine Open-Source-Datenverarbeitungspipeline, mit der ISE für die Protokollsammlung, -umwandlung und -weiterleitung integriert. Logstash fungiert als Protokollsammler und -weiterleitung, sodass ISE-Protokolle verarbeitet und zur Analyse, Speicherung und Überwachung an andere Systeme gesendet werden können. Logstash ist ein leistungsstarkes Open-Source-Tool, das Protokolle oder andere Daten aus verschiedenen Quellen sammelt, analysiert und an einen zentralen Ort weiterleitet, wo sie gespeichert, analysiert und visualisiert werden können. Im Kontext der ISE dient der ISE Logstash Service dazu, Protokolle in einem strukturierten Format zu verarbeiten und an ein zentrales Protokollierungssystem weiterzuleiten, wo sie weiter analysiert, überwacht und visualisiert werden können.

Wichtigste Funktionen des ISE Logstash Service

1. Protokollerfassung und -weiterleitung: Die Hauptfunktion des ISE-Logstash-Service besteht darin, Protokolldaten von verschiedenen ISE-Komponenten (wie Authentifizierungsprotokolle, Systemprotokolle, Protokolle zur Richtliniendurchsetzung usw.) zu sammeln und zur Speicherung und Analyse an einen zentralen Ort (in der Regel Elasticsearch oder ein anderes Protokollmanagementsystem) weiterzuleiten.

2. Protokoll-Analyse: Logstash kann die gesammelten Logs in strukturierten Formaten analysieren. Es verarbeitet unformatierte Protokolldaten und extrahiert aussagekräftige Informationen daraus, wobei die Protokolleinträge in ein Format umgewandelt werden, das einfacher abzufragen und zu analysieren ist. Hierzu können die Daten gefiltert, analysiert und angereichert werden, bevor sie an Elasticsearch oder andere Systeme weitergeleitet werden.

Überprüfung und Fehlerbehebung des ISE Logstash Service

1. Keine bestimmten Debugs aktiviert. Die **Protokollanwendung "show logging" ise-logstash/logstash.log** bietet jedoch Einblicke in den Service-Status.

2. Deaktivieren und erneutes Aktivieren des Log Analytics Service in der ISE muss helfen. Navigieren Sie zu **Operations > System 360 > Settings > Log analytics** (deaktivieren und aktivieren Sie diese Option mit einem Knebel).

Bekannte Fehler im Zusammenhang mit dem Logstash-Service

Cisco Bug-ID・ 74832

Cisco Bug-ID・ 58596

ISE Kibana-Service

Der ISE Kibana Service ist eine Komponente, die Kibana, ein Open-Source-Datenvisualisierungstool, mit der ISE-Protokollierungs- und Überwachungsinfrastruktur integriert. Kibana arbeitet mit Elasticsearch (das Protokolldaten speichert und indiziert) zusammen, um eine leistungsstarke Plattform für die Visualisierung, Suche und Analyse von ISE-Protokollen und Leistungsmetriken bereitzustellen.

Wichtigste Merkmale und Funktionen des ISE Kibana Service

1. Datenvisualisierung: Mit dem ISE Kibana Service können Administratoren visuelle Darstellungen der von der ISE gesammelten Protokolldaten erstellen. Dies kann Folgendes umfassen:

- Diagramme, Diagramme und Tabellen für Trends in den Bereichen Authentifizierung, Richtliniendurchsetzung, Benutzeraktivität und Systemzustand.
- Tortendiagramme, Liniendiagramme und Balkendiagramme, um bestimmte Metriken wie die Anzahl der fehlgeschlagenen Anmeldungen, die Sitzungsdauer oder Fehler im Zeitverlauf zu

verfolgen.

Überprüfung und Fehlerbehebung des ISE Kibana-Service

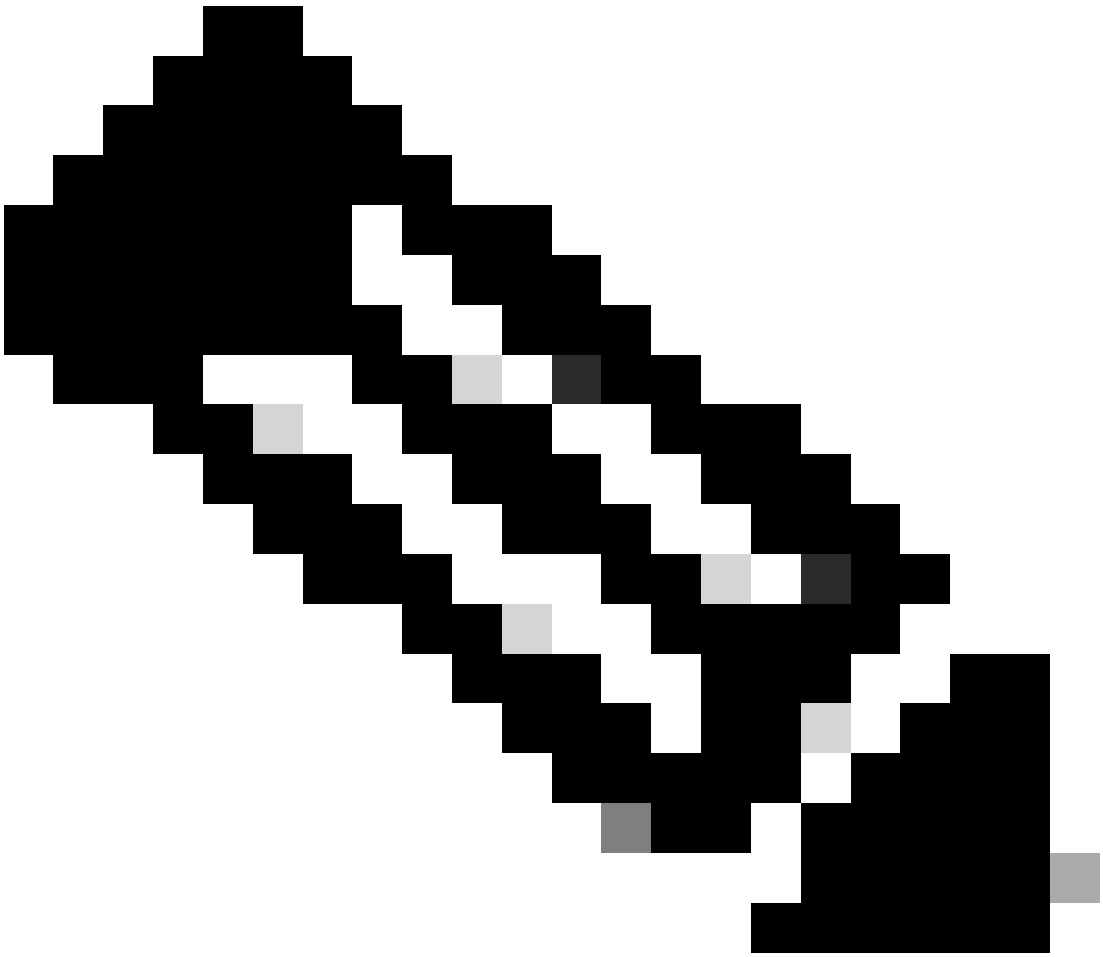
1. Wenn der ISE-Kibana-Dienst nicht ausgeführt wird, müssen Sie die Protokollanalyse in ISE deaktivieren und erneut aktivieren. Navigieren Sie dazu zu Operations > System 360 > Settings, Log analytics (Deaktivieren und Aktivieren mit der Option toggle).

2. In vielen Szenarien kann es einen doppelten Eintrag im Ordner /etc/hosts geben, der ein Problem verursachen muss. Wenden Sie sich an das TAC, um die doppelte Eingabe zu entfernen.

Bekannte Mängel im Zusammenhang mit dem Kibana-Problem

Cisco Bug-ID・ 78050

Cisco Bug-ID・ 59848



Anmerkung: Wenn die Protokollanalyse aktiviert ist, müssen ISE MNT LogAnalytics Elasticsearch, ISE Logstash Service und ISE Kibana Service ausgeführt werden, und eine Unterbrechung dieser Services kann während der Datenerfassung zu Problemen führen.

ISE Nativer IPSec-Dienst

Der ISE Native IPSec Service bezieht sich auf die integrierte Unterstützung von IPSec (Internet Protocol Security), die eine sichere Kommunikation zwischen ISE-Knoten oder zwischen ISE und anderen Netzwerkgeräten ermöglicht. IPSec ist eine Protokollfamilie zur Sicherung der Netzwerkkommunikation durch Authentifizierung und Verschlüsselung jedes IP-Pakets in einer Kommunikationssitzung.Der Native IPSec-Dienst ist Teil des umfassenderen Sicherheits- und Netzwerkzugriffsverwaltungsrahmens. Es bietet Funktionen zur Handhabung und Verwaltung von IPsec-VPN-Verbindungen und stellt sicher, dass die zwischen dem ISE-System und den Remote-Endpunkten übertragenen Daten sicher sind. Dies kann Interaktionen mit Client-Geräten, Netzwerkzugriffsgeräten (wie Routern oder Firewalls) oder sogar anderen ISE-Knoten umfassen, bei denen IPsec-Verschlüsselung und -Tunneling zum Sichern vertraulicher Informationen erforderlich sind.

Wichtigste Funktionen des nativen ISE IPSec-Service

1. Sichere Kommunikation über IPsec: Die Hauptfunktion des ISE Native IPSec Service besteht darin, sichere Kommunikationskanäle über IPsec einzurichten und aufrechtzuerhalten. Hierzu werden Verschlüsselungs- und Authentifizierungsmechanismen verwendet, um sicherzustellen, dass die zwischen der ISE und anderen Geräten übertragenen Daten vor Abfangen, Manipulation und nicht autorisiertem Zugriff geschützt sind.

2. IPsec-VPN-Verbindungen: Der ISE Native IPSec Service unterstützt VPN-Verbindungen, die das IPsec-Protokoll verwenden, um einen sicheren, verschlüsselten Tunnel für die Datenübertragung bereitzustellen. Dies ist besonders für Mitarbeiter an Remote-Standorten, Zweigstellen oder anderen Standorten nützlich, die über nicht vertrauenswürdige Netzwerke (z. B. das Internet) sicher auf die ISE-Umgebung zugreifen müssen.

3. Unterstützung für Remote Access VPN: Der Native IPSec-Dienst kann in VPN-Konfigurationen für den Remote-Zugriff eingebunden werden, bei denen sich Benutzer oder Geräte an einem externen Standort (z. B. Mitarbeiter an entfernten Standorten oder Zweigstellen) über IPsec-Tunnel sicher mit dem ISE-System verbinden. Dieser Service stellt sicher, dass der gesamte Remote-Zugriffsverkehr verschlüsselt und authentifiziert wird, bevor er die ISE-Umgebung erreicht.

4.IPsec-VPN-Client-Kompatibilität: Der ISE Native IPSec-Dienst stellt die Kompatibilität mit IPsec-VPN-Clients sicher. Sie unterstützt gängige Client-Konfigurationen, sodass Geräte sicher mit dem Netzwerk verbunden werden können, ohne dass vertrauliche Daten Risiken ausgesetzt sind.

Systemeigenen IPSec-Dienst überprüfen und Fehler beheben

1. Für den Native IPSec-Dienst sind keine speziellen Debugs verfügbar. Überprüfen Sie die Protokolle mit dem Befehl show logging application strongswan/charon.log tail über die ISE-CLI.

2. Wenn bei einem Tunnel Probleme auftreten, überprüfen Sie den Status des Tunnelaufbaus über GUI > Administration > System > Settings > Protocols > IPSec > Native IPSec.

MFC-Profiler

Der MFC Profiler ist eine spezielle Komponente für die Profilerstellung von Netzwerkgeräten und Endgeräten. Die Profilerstellung ist ein wichtiger Bestandteil der Netzwerkzugriffskontrolle, da die ISE so Geräte im Netzwerk identifizieren, klassifizieren und je nach Gerätetyp und -verhalten die entsprechenden Netzwerkrichtlinien anwenden kann.

Wichtigste Funktionen des MFC Profiler Service in der ISE

1. Datenverkehrsprofile: Der MFC Profiler-Service in der ISE ist für die Erfassung und Profilerstellung der Datenverkehrsdaten zuständig. Es überwacht das Verhalten von Endgeräten im Netzwerk, einschließlich der verwendeten Anwendungstypen, der aufgerufenen Services und der von den Geräten angezeigten Datenverkehrsmuster. Diese Daten helfen bei der Erstellung eines Profils für jeden Endpunkt.

2. Endgeräteprofilierung: Der MFC Profiler-Service ermöglicht der ISE die Identifizierung und Kategorisierung von Endpunkten basierend auf deren Verhalten. Basierend auf Datenverkehrsmustern erkennt es beispielsweise, ob es sich bei einem Endgerät um einen Drucker, einen Computer oder ein Mobilgerät handelt. So können spezifischere Richtlinien für verschiedene Gerätetypen durchgesetzt und die Sicherheit und Betriebseffizienz verbessert werden.

MFC-Profiler-Service überprüfen und Fehlerbehebung durchführen

1. Navigieren Sie zu ISE GUI -> Administration -> Profiling -> MFC profiling and AI rules, und überprüfen Sie, ob der Service aktiviert ist.

2. Wenn der Dienst aktiviert ist, aber als deaktiviert angezeigt wird/nicht ausgeführt wird, wird er über den Befehl show application status ise in der ISE-CLI ausgeführt. Deaktivieren und reaktivieren Sie den MFC-Profilerstellungsdienst in der ISE, indem Sie auf Schritt 1 verweisen.

Hilfreiche Fehlerbehebungsfunktionen: MFC-Profiler-Komponente im Debugging. Die Protokolle konnten mithilfe des Befehls show logging application ise-pi-profiler.log tail über die ISE-CLI aus dem Support-Paket verifiziert oder an die Protokolle weitergeleitet werden.

Bekannter Fehler für MFC-Profiler, der anzeigt, dass der Status nicht ausgeführt wird, anstatt deaktiviert zu sein:

Cisco Bug-ID・ 72853

Wichtigste Punkte

1. Starten Sie die Dienste mithilfe der Befehle application stop ise und application start ise über die ISE-CLI neu, um die Dienste wiederherzustellen.

2. Wenn ein Problem auftritt, stellen Sie sicher, dass ein Support-Paket von der ISE-GUI/ISE-CLI erfasst wird, um das Problem weiter zu überprüfen. Referenzlink für die Erstellung des ISE-Supportpakets über die GUI und CLI: Collect Support Bundle on the Identity Services Engine

3. Wenn sich die Probleme auf Ressourcen, den Lastdurchschnitt, die Festplattennutzung usw. beziehen, müssen Thread Dump und Heap Dump für die Analyse gesammelt werden.

4. Wenden Sie sich vor dem erneuten Laden des Knotens an das Cisco TAC, und stellen Sie sichere Protokolle für die weitere Analyse bereit.

Standardisierte Bedenken in der ISE

Abgesehen von den Problemen mit ISE-Services gibt es bei ISE-Knoten einige Probleme, die zusammen mit grundlegenden Schritten zur Fehlerbehebung behoben werden müssen.

Überprüfung auf durchschnittlich hohe Auslastung, Probleme bei der Ressourcennutzung (CPU / ARBEITSSPEICHER / DATENTRÄGER), unzureichende Ressourcen

1. Überprüfen Sie, ob die von Cisco empfohlenen Ressourcen dem Knoten mithilfe des Befehls show Inventory über die ISE-CLI zugewiesen wurden.

2. Führen Sie über die CLI des ISE-Knotens den Befehl tech top aus, um die Ressourcennutzung der ISE zu überprüfen.

3. Überprüfen Sie die Datenträgerauslastung mit dem Befehl show disk über die ISE-CLI.

4. Löschen Sie die inaktiven Endpunkte, löschen Sie die lokale Festplatte des Knotens, und führen Sie Upgrade-Bereinigungen durch.

Wenn das Problem weiterhin besteht, wenden Sie sich an das Cisco TAC, und stellen Sie das sichere Support-Paket, den Heap-Dump und den Thread-Dump für den Knoten bereit, bei dem das Problem auftritt.

Um das Heap-Dump zu sichern, melden Sie sich bei der CLI des ISE-Knotens an, und führen Sie den Befehl **application configure ise** aus. Wählen Sie Option 22 aus.

Um den Thread-Dump zu sichern, melden Sie sich bei der CLI des ISE-Knotens an, führen den Befehl **application configure ise** aus, wählen Sie **Option 23. Der** Thread-Dump ist im Supportpaket enthalten oder kann über die ISE-CLI mit dem Befehl **show logging application appserver/catalina.out** überwacht werden.

Überprüfen und Beheben von Überwachungsproblemen

Die Überwachungs- und Fehlerbehebungsfunktion (Monitoring and Troubleshooting, MnT) der ISE ist eine der Hauptkomponenten der ISE-Architektur und bietet Überwachungs-, Berichterstellungs- und Benachrichtigungsfunktionen.

Die ISE zeigt Überwachungsinformationen an zahlreichen Stellen an, darunter:

- Cisco ISE-Startseite

- Sichtbarkeitsansichten
- RADIUS Live-Protokolle und -Sitzungen
- Globale Suche
- Bedrohungsorientierte NAC Live-Protokolle
- TACACS-Live-Protokolle

Allgemeine Probleme, die in der Kategorie Überwachung und Fehlerbehebung beobachtet wurden:

1. Radius-/TACACS-Live-Protokolle nicht verfügbar
2. Live-Sitzungen nicht verfügbar
3. Statuszusammenfassung nicht verfügbar
4. Performance-Probleme (hohe CPU/Speicher) bei MnT-Knoten

Debugs, die auf den MnT-Knoten aktiviert werden sollen, um das Problem einzugrenzen:

1. Cisco-mnt
2. Collector
3. CPM-mnt
4. Laufzeitprotokollierung

Zusätzlich zu den beim Debuggen erwähnten Komponenten können diese Informationen bei der Fehlerbehebung hilfreich sein:

1. Sind auch Live-Sitzungen betroffen oder nur Live-Protokolle?
2. Sind Radius- oder TACACS-Protokolle betroffen oder beide?
3. Sehen Sie eine hohe CPU-Auslastung oder eine hohe Auslagerungsauslastung auf MnT-Knoten?
4. Wie viele Pufferdateien sehen Sie auf den MnT-Knoten. Pufferdateien finden Sie unter: /opt/CSCOcpm/mnt/data/collector
5. Sind Speicher- und CPU-Reservierungen aktiviert, falls nicht, aktivieren Sie diese bitte.
6. Wurde das Zurücksetzen der MnT/config/session-DB in letzter Zeit durchgeführt?
7. Werden Syslogs von PSNs an MnT-Knoten gesendet?

Wenn Sie Syslog-Dienste für MnT verwenden, sind diese Informationen zur Fehlerbehebung erforderlich:

1. Verwenden Sie ein sicheres Syslog-Ziel? Wenn nicht, deaktivieren Sie es, da es bekanntermaßen Deadlocks in Threads verursacht, die dazu führen, dass der Collector nicht mehr funktioniert.
2. Verwenden Sie ein sicheres Syslog-Ziel? Stellen Sie sicher, dass die Zertifikatzuordnung unter Administration->Logging->Remote logging Targets->Secure Syslog Collector 1 und 2 richtig festgelegt ist.
3. Überprüfen Sie, ob die Protokollierungskategorien ordnungsgemäß festgelegt sind (empfohlen zum Entfernen nicht verwendeter/unerwünschter Protokollierungskategorien - dadurch wird die Last für MnT-Knoten reduziert), und stellen Sie fest, dass die Protokollierungsziele ordnungsgemäß konfiguriert sind.
4. Überprüfen Sie die awrrep*.html-Dateien aus dem Supportpaket, um zu verstehen, welche

Komponente häufigere Syslogs sendet. Wenn beispielsweise TACACS-Tabellen mit Einfüge- oder Aktualisierungsabfragen angezeigt werden, können wir die Collector-Protokolle überprüfen, um eine Korrelation herzustellen, um zu ermitteln, welche Syslogs häufiger gesendet werden.

Wenn das Problem mit der Leistung auf dem MnT-Knoten zusammenhängt, benötigen wir folgende Informationen:

1. tech top output aus der ISE CLI des MnT-Knotens.

2. Wenn die CPU hoch ist, sehen Sie auch eine hohe Arbeitsspeicher- oder Auslastung des Auslagerungsbereichs?

3. Stützpaket mit Heap Dump und Thread Dump gesichert.

Referenz

- Administratorleitfaden für die Cisco Identity Services Engine, Version 3.3
- Fehlerbehebung und Aktivieren von Debuggen auf der ISE

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.