瞭解ISE服務、用途和故障排除

目錄

簡介

本文檔介紹ISE服務、用途和故障排除。

必要條件

需求

思科建議您瞭解思科身份服務引擎。

採用元件

本檔案所述內容不限於任何特定思科身分識別服務引擎的軟體和硬體版本。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

思科身份服務引擎(ISE)是一個全面的解決方案，旨在通過集中式策略管理、身份驗證、授權和記帳(AAA)提供高級網路安全。　它使組織能夠管理使用者、裝置和應用程式的網路訪問，同時確保安全性、合規性和無縫的使用者體驗。

為了實現這些目標，思科ISE利用一系列服務，每個服務負責使系統高效運行的特定任務。這些服務協同工作，可確保安全的網路訪問、強大的策略實施、詳細的日誌記錄、與外部系統的無縫整合

以及高效的裝置分析。

ISE中的每項服務在維護解決方案的完整性和可用性方面起著至關重要的作用。有些服務處理核心功能，如資料庫管理和身份驗證，而有些服務則啟用高級功能，如裝置分析、證書管理和監控。

本文概述了思科ISE中的各種服務，解釋了它們的用途、重要性以及遇到問題的潛在故障排除步驟。無論您是管理員還是網路安全專業人員，瞭解這些服務都有助於確保您的ISE部署平穩安全運行。

瞭解ISE服務並對其進行故障排除

ISE利用螢幕截圖中提到的服務來支援其功能。通過ISE節點的CLI使用show application status ise命令驗證ISE中可用的狀態或服務。以下是顯示ISE上的狀態或可用服務的輸出示例。

```
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
```

ISE中提供的服務。

現在，詳細瞭解每項服務。

資料庫監聽程式

資料庫監聽程式服務是幫助管理ISE和資料庫伺服器之間通訊的關鍵元件。它偵聽和處理與資料庫相關的請求，確保ISE系統可以讀取和寫入其基礎資料庫。

關於ISE中的資料庫監聽程式服務的要點

1. 通訊介面:它充當ISE和資料庫伺服器之間的通訊橋樑，允許系統檢索和儲存使用者憑證、會話資訊、網路策略等資料。

2. 外部資料庫支援:可以將ISE配置為使用外部資料庫（如Oracle或Microsoft SQL Server）進行使用者身份驗證和策略儲存。資料庫監聽程式服務確保ISE可以安全高效地連線到此外部資料庫並與之互動。

3. 資料處理:服務偵聽來自ISE系統的資料庫查詢，然後將它們轉換為外部資料庫上的相應操作。它可以處理諸如插入、更新或刪除記錄之類的請求，以及從資料庫檢索資訊。

4. 資料庫運行狀況監控：除了提供通訊通道外，它還有助於確保與外部資料庫的連線穩定且可操作。如果連線失敗，ISE將返回到本地儲存或進入降級模式，具體取決於配置。

資料庫伺服器

資料庫伺服器服務負責管理系統使用的資料的儲存和檢索。它處理與ISE用來儲存配置、策略資訊、使用者資料、身份驗證日誌、裝置配置檔案和其他必要資訊的底層資料庫的互動。

關於ISE中資料庫伺服器服務的要點

1.內部資料儲存:資料庫伺服器服務主要管理ISE用來在本地儲存運算元據的內部嵌入式資料庫。其中包括身份驗證和授權記錄、使用者配置檔案、網路訪問策略、裝置和終端資訊、會話資訊等資料。

2.嵌入式資料庫:在大多數思科ISE部署中，系統使用嵌入式PostgreSQL資料庫進行本地儲存。資料庫伺服器服務確保此資料庫順利運行，並處理與儲存在其中的資料相關的所有查詢、更新和管理任務。

3.資料庫完整性:該服務確保所有事務都得到正確處理，並確保資料庫的完整性。它處理鎖定記錄、管理資料庫連線和執行資料庫查詢等任務。

驗證資料庫監聽程式和資料庫伺服器服務是否正在初始化或未運行，並對其進行故障排除

資料庫監聽程式和資料庫伺服器是必須同時運行才能使所有其他服務正常運行的基本服務。如果這些服務未在運行或在初始化期間停滯，則這些故障排除步驟可幫助進行恢復。

1.使用application stop ise和application start ise 命令重新啟動ISE服務。

2.如果這是一個VM節點，從VM重新啟動該節點必須有助於恢復服務。

3.如果節點是物理節點，從CIMC重新啟動/重新載入節點必須有助於恢復服務。

4.如果資料庫損毀，請聯絡Cisco TAC進行進一步的疑難排解。

當資料庫中存在差異或資料庫無法正確初始化時，資料庫監聽程式和資料庫伺服器通常關閉或無法啟動。在這些情況下，使用application reset-config ise命令執行應用程式重置必須有助於資料庫的恢復和全新啟動。運行application reset-config ise命令將刪除配置和證書，但保留IP地址和域名詳細資訊。建議在將此命令應用於部署中的任何節點之前，與Cisco TAC聯絡以瞭解更多資訊並瞭解潛在影響。

應用伺服器

應用伺服器是負責運行和管理ISE平台核心功能和服務的關鍵元件。它承載業務邏輯、使用者介面和服務，允許ISE在網路訪問控制、身份驗證、授權、記賬和策略管理中執行其角色。

關於ISE中應用伺服器服務的要點

1.使用者介面(UI):應用伺服器服務負責呈現基於Web的ISE使用者介面(UI)。這允許管理員配置和管理策略、檢視日誌和報告，以及與ISE的其他功能互動。

2.服務管理:它負責處理ISE提供的不同服務，包括策略管理、管理任務以及分散式部署中與其他ISE節點的通訊。

3.集中處理:應用伺服器服務在ISE架構中扮演著中心角色，提供能夠理解策略、身份驗證請求以及來自網路裝置、目錄和外部服務的資料的邏輯。

應用程式伺服器正在初始化或未運行的驗證

應用程式伺服器依賴於少量的Web應用程式，如證書、資源、部署、許可。當任何Web應用程式初始化失敗時，應用程式伺服器將停滯在初始化狀態。根據節點上的配置資料，應用程式伺服器從**未運行到初始→運行→態需要**大約15到35分鐘。

1. 確保ISE的管理員證書在所有節點的部署中有效且處於活動狀態。
2. 確保部署中的所有節點都與主管理節點同步。
3. 如果該節點是VM，請確保將建議的資源分配給該節點。

在ISE節點的CLI中使用**show application status ise**命令驗證應用伺服器的狀態。大部分與應用伺服器相關的日誌位於

Catalina.Out和Localhost.log檔案。

如果滿足上述條件，並且應用伺服器仍停滯在初始化狀態，請從ISE的CLI/GUI保護支援捆綁包。使用application stop ise和application start ise 命令恢復/重新啟動服務。

Profiler資料庫

Profiler資料庫是一個專用資料庫，用於儲存有關Profiler服務發現的網路裝置、終端和裝置配置檔案的資訊。Profiler是ISE的關鍵元件，它根據網路特徵和行為自動識別和分類網路裝置（如電腦、智慧手機、印表機、IoT裝置等）。

有關ISE中的Profiler資料庫服務的要點

1.裝置分析:Profiler資料庫服務的主要功能是支援分析過程。ISE使用此服務來儲存分析過程中收集的資訊，例如：

- 裝置型別(例如：智慧手機、筆記型電腦、印表機、物聯網裝置)
- 裝置作業系統(例如：Windows®、macOS®、Cisco IOS®、Android®)
- 裝置製造商
- 有助於對裝置進行分類的網路行為或模式

2. Profiler資訊:它儲存分析器屬性，如用於使裝置與預定義策略相匹配的裝置硬體和軟體配置檔案。此資訊還用於根據裝置的配置檔案將裝置動態分配到正確的網路訪問策略或VLAN。

3.分析過程:分析過程通常基於：

- 活動分析:ISE主動查詢網路上的裝置以獲取資訊。
- 被動分析:ISE被動地從網路流量（例如DHCP請求、RADIUS屬性、HTTP報頭和其他網路協定）收集資料以確定裝置型別。

驗證ISE分析服務並對其進行故障排除

1.從ISE CLI運行show application status ise命令以驗證profiler資料庫服務正在運行。

2.從主管理節點的GUI導航到管理>部署>選擇節點。按一下Edit並驗證session services 和profiling services 是否已啟用。

3.現在，導航到管理>部署>選擇節點。移動到Profiler配置，並驗證是否已啟用保護端點資料所需的探測器。

4.導航到Administration > System > Profiling，然後驗證為CoA配置的分析器設定。

5.從上下文可視性>端點 >選擇端點並驗證由不同端點探測功能收集的屬性。

用於排除分析問題的有用調試：

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

ISE索引引擎

索引引擎是一項服務，負責高效地搜尋、索引和檢索ISE資料庫中儲存的資料。它增強了ISE的效能和可擴充性，尤其是在處理大量資料並提供對身份驗證、授權、監控和報告任務所需資訊的快速訪問方面。

關於ISE中的ISE索引引擎的要點

1.資料索引:ISE索引引擎為ISE中儲存的各種型別的資料建立索引，如身份驗證日誌、會話日誌、策

略命中、分析資料和網路訪問記錄。索引有助於以一種使搜尋和查詢更加高效的方式組織此資料。

2.日誌管理和報告:此服務通過提高報告和日誌查詢的效能，在日誌管理中扮演著關鍵角色。例如，在搜尋特定的身份驗證事件時，索引引擎可以更快地檢索所需的記錄，這對於安全監視和法規遵從性報告至關重要。

3.資料檢索:索引引擎還負責確保ISE能夠在需要時從其基礎資料庫中高效地檢索索引資料。這允許ISE對來自使用者介面、外部工具或API的查詢提供快速響應。

驗證ISE索引引擎未運行或未初始化

1. 使用**nslookup <FQDN / IP address of the ISE node >** 命令，通過CLI驗證正向和反向DNS查詢是否工作正常或群集中的所有節點。
2. 驗證ISE管理員證書對於群集中的所有節點是否有效且處於活動狀態。
3. 使用**show ntp** 命令，通過CLI驗證NTP是否工作並與ISE節點同步。

索引引擎由上下文可視性使用，並且需要啟動並運行索引引擎才能使上下文可視性工作。有助於索引引擎故障排除的有用日誌包括**ADE.log**檔案，可以在問題發生期間使用**show logging system ade/ADE.log tail** 命令從支援捆綁包保護這些檔案，或通過CLI對其進行跟蹤。

AD聯結器

AD聯結器(Active Directory Connector)是一種允許ISE與Microsoft Active Directory(AD)整合的服務，使ISE能夠根據使用者的AD憑證和組成員身份對使用者進行身份驗證、授權和管理。AD聯結器充當ISE和Active Directory之間的橋樑，允許ISE利用AD進行網路訪問控制(NAC)和策略實施。

ISE中AD聯結器服務的關鍵功能

1.與Active Directory整合:AD聯結器服務充當ISE和Active Directory之間的橋樑。它允許ISE安全連線到AD，使ISE能夠利用AD作為集中身份庫進行使用者身份驗證和策略實施。

2. 同步:AD聯結器服務支援將使用者和組資料從Active Directory同步到ISE。這可以確保ISE擁有有關使用者和組的最新資訊，這些資訊對於準確策略實施至關重要。

3.安全通訊:AD聯結器服務在ISE和Active Directory之間建立安全通訊通道，通常使用協定(如LDAP over SSL(LDAPS))以確保身份驗證和查詢過程中的資料隱私和完整性。

4.多個Active Directory域支援:該服務可以支援到多個Active Directory域的連線。這在大型或多域環境中尤其有用，因為在這種環境中，ISE需要驗證來自不同AD林或域的使用者。

5.使用者和組查詢:它使ISE能夠查詢AD中的使用者和組資訊。這可能包括使用者名稱、組成員身份和其他可用於實施網路訪問策略的使用者屬性等詳細資訊。例如，可以基於使用者AD組成員身份應用網路訪問策略(例如：向不同組中的使用者授予不同的訪問級別)。

1.驗證NTP是否與節點同步，以及AD和ISE之間的時間差是否必須小於5分鐘。

2.驗證DNS伺服器是否可以解析與AD相關的FQDN和域。

3.定位至**「工序」>「報表」>「報表」>「診斷」>「AD聯結器工序」**,驗證與AD相關的事件或報表。

用於故障排除的有用日誌是**ad_agent.log**，其中包含運行時元件的調試日誌。

M&T會話資料庫

M&T會話資料庫（監控和故障排除會話資料庫）在儲存和管理網路訪問事件的會話相關資料方面起著重要作用。M&T會話資料庫儲存有關活動會話的資訊，包括使用者身份驗證、裝置連線和網路訪問事件，這對於監控、故障排除和分析網路活動至關重要。

ISE中M&T會話資料庫服務的關鍵功能

1.會話資料儲存:M&T Session Database服務負責儲存和索引網路上有關使用者和裝置會話的資料。這包括會話開始和結束時間、身份驗證結果、使用者或裝置身份以及關聯的策略（如角色分配或VLAN分配）。 資料還包括詳細說明會話生命週期的RADIUS記帳資訊，包括初始身份驗證和跟蹤會話事件的任何記帳消息。

2.即時和歷史資料:該服務提供對即時會話資料（活動會話）和歷史會話資料（過去會話）的訪問。這使管理員不僅能夠監控持續的使用者訪問，而且能夠檢視過去的會話日誌，以調查問題或驗證訪問事件。即時會話監控有助於確保網路中當前沒有未經授權的裝置。

3.加強監測:提供對使用者和裝置活動的深入瞭解，包括應用於其會話的策略，有助於檢測潛在的安全問題或未經授權的訪問。

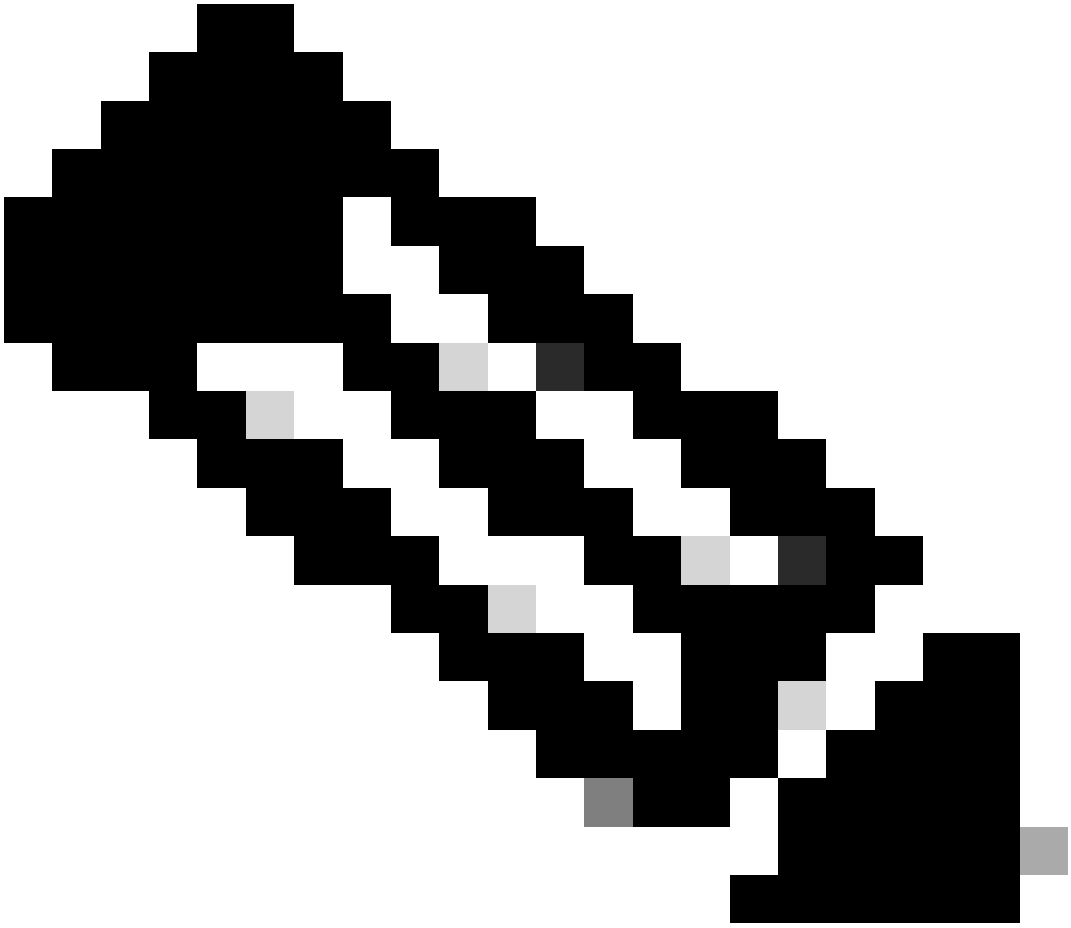
4.審計和報告:通過儲存網路訪問事件的歷史記錄和為管理報告提供資料，促進合規性稽核和報告。

驗證ISE中的M&T會話資料庫並排除故障

1.驗證是否為該節點分配了建議的資源。

2.從ISE CLI**獲取安全show技術支援**，以進一步驗證問題。

3.通過**ISE CLI中運行application configure ise** 命令並選擇選項**1**，重置M&T會話資料庫。



附註：只有在驗證部署中的潛在影響之後，才能重置M&T資料庫。請與Cisco TAC聯絡以進行進一步驗證。

已知瑕疵

[思科錯誤ID ·32364]

M&T日誌處理器

M&T Log Processor(Monitoring and Troubleshooting Log Processor)是一個負責收集、處理和管理ISE內各種服務生成的日誌資料的元件。它是監控和故障排除(M&T)框架的關鍵部分，可幫助管理員監控和排除ISE系統中的網路訪問事件、身份驗證嘗試、策略實施和其他活動故障。M&T日誌處理器專門處理日誌條目的處理，確保ISE可以儲存、分析和提供報告、稽核和故障排除所需的資訊。

ISE中M&T日誌處理器服務的主要功能

1.日誌收集和處理:M&T日誌處理器服務收集和處理由各種ISE元件生成的日誌，例如身份驗證請求

、授權決策、記帳消息和策略實施活動。這些日誌包含有關使用者、裝置和網路訪問嘗試的詳細資訊，例如時間戳、使用者ID、裝置型別、應用的策略、訪問請求成功或失敗以及失敗原因。

2.報告和合規性:此服務處理的日誌對於合規性報告至關重要。許多法規要求組織保留使用者訪問和安全事件日誌。M&T日誌處理器服務確保所有相關日誌都得到處理，並可用於合規性稽核。它有助於根據日誌資料（如使用者訪問日誌、身份驗證成功/失敗率或策略實施日誌）生成詳細報告。

驗證ISE中的M&T日誌處理器服務並對其進行故障排除

1.確保根據《思科安裝指南》使用建議的資源部署ISE節點。

2.要驗證問題，請通過ISE CLI運行**show logging system ade/ADE.log tail**命令檢視相關異常/錯誤。

已知瑕疵

思科錯誤ID ·15130

證書頒發機構服務

證書頒發機構(CA)服務是一個關鍵元件，可幫助管理數位證書以保護通訊以及驗證裝置、使用者和網路服務。數位證書對於建立可信連線並確保客戶端（電腦、智慧手機、網路裝置）和網路基礎設施元件（交換機、無線接入點、VPN網關）之間的安全通訊至關重要。 思科ISE中的CA服務與X.509證書配合使用，這些證書用於多種網路安全用途，包括802.1X身份驗證、VPN訪問、安全通訊和SSL/TLS加密。

ISE中證書頒發機構服務的關鍵功能

1.證書管理:證書頒發機構服務負責處理ISE內數位證書的建立、頒發、管理和續訂。這些憑證用於網路中的各種驗證通訊協定與加密目的。它可以充當內部證書頒發機構，也可以與外部CA整合(例如：Microsoft AD CS、VeriSign或DigiCert等公共CA來頒發證書。

二、發證:對於需要EAP-TLS或類似基於證書的身份驗證方法的環境，ISE可以為網路訪問裝置(NAD)、使用者或終端頒發證書。ISE可以自動生成和部署用於驗證裝置和使用者的證書，也可以從外部CA請求證書。

3.證書註冊:CA服務支援終端（例如筆記型電腦、電話和其他網路裝置）的證書註冊，這些終端需要使用證書向網路進行身份驗證。ISE使用SCEP（簡單證書註冊協定）或ACME（自動證書管理環境）等協定來簡化裝置的證書註冊。

4.證書續訂:該服務可自動為裝置和使用者續訂即將到期的證書。它確保證書始終保持有效且為最新，防止證書過期導致服務中斷。

5.與外部證書頒發機構整合：雖然ISE可以充當自己的CA，但更常見的是與外部CA整合(例如：Microsoft Active Directory證書服務)。 CA服務可以管理ISE和外部CA之間的互動，根據需要請求使用者、裝置和網路資源的證書。

EST服務

通過安全傳輸(EST)註冊服務是一種協定，用於在基於證書的身份驗證環境中向網路裝置和使用者安全地頒發數位證書。EST是一種證書註冊協定，允許裝置以安全且自動的方式向證書頒發機構(CA)請求證書。EST服務對於裝置身份驗證尤其有用，例如802.1X環境、VPN連線或BYOD（自帶裝置）場景，在這些場景中，裝置需要使用證書向網路進行身份驗證。

ISE中EST服務的主要功能

1.證書註冊:EST服務負責為需要證書進行身份驗證的裝置（如交換機、接入點或終端）啟用安全證書註冊。註冊通過安全傳輸（通常為HTTPS）完成，確保該進程經過加密並保護免受未經授權的訪問。

2.憑證撤銷及續期:註冊證書後，EST服務還負責管理證書撤銷或續訂。例如，裝置需要在當前證書過期時請求新證書，EST可以幫助自動完成此過程。

3.改進網路訪問控制:通過使裝置能夠使用證書進行身份驗證，EST服務增強了網路的安全狀態，特別是在使用802.1X身份驗證的環境中。

驗證證書頒發機構和EST服務未運行/正在初始化

1. 導覽至**Administration > System > Certificates > Certificate Authority > Internal CA settings**。確保CA、EST和OCSP響應程式狀態已排序並啟用。
2. 有助於進行故障排除的有用調試有set、provisioning、ca-service和ca-service-cert。 請參閱**toise-psc.log**、**catalina.out**、**caservice.log**和**error.log**檔案。
3. 驗證ISE根CA和ISE消息證書在部署中有效。如果需要續訂ISE根CA，**請導航到管理>證書>證書簽名請求>生成證書簽名請求**，選擇使用作為ISE根CA。**按一下**renew ISE Root CA。

SXP引擎服務

SXP引擎服務負責使用安全組標籤(SGT)和安全組交換協定(SXP)管理和促進ISE與網路裝置之間的通訊。 它在支援TrustSec策略方面發揮著關鍵作用，TrustSec策略用於根據裝置的安全組（而不僅僅是IP地址或MAC地址）實施網路訪問控制。ISE中的SXP引擎主要用於交換安全組資訊，這有助於根據使用者或裝置身份、應用程式和位置實施策略。它使裝置能夠共用安全組標籤(SGT)，用於跨網路裝置（如路由器和交換機）實施安全策略。

ISE中SXP引擎服務的主要功能

1.與TrustSec整合:SXP通常部署在利用Cisco TrustSec的環境中，Cisco TrustSec解決方案可在有線和無線網路中實施一致的安全策略。SXP引擎便於裝置之間的SGT通訊，允許基於裝置或使用者的安全上下文的動態策略實施。

2.安全組標籤(SGT):TrustSec的政策執行核心圍繞SGT。這些標籤用於分類網路流量，而SXP協定可幫助共用這些標籤到特定使用者或裝置的對映。這允許對網路訪問和流量進行精細的、策略驅動的控制。

ISE中SXP引擎服務的驗證和故障排除

1.預設情況下，ISE中禁用SXP引擎服務。要啟用它，請轉到**ISE GUI > Administration > Deployment，選**

擇節點。選中Enable SXP Service框，然後選擇介面。然後，使用**show application status ise** 命令從ISE CLI驗證SXP引擎服務的狀態。

2.如果存在網路通訊問題，通過在CLI中使用show　interface命令驗證分配給SXP引擎的介面具有有效的IP地址，並確保網路中允許IP子網。

3.檢查RADIUS即時日誌以驗證ISE上的SXP連線事件。

4.啟用ISE節點上的SXP元件以調試和捕獲與SXP相關的日誌和異常。

TC-NAC服務

TC-NAC服務（TrustSec網路訪問控制）是一個促進在網路裝置上實施TrustSec策略的元件，確保訪問控制基於安全組標籤(SGT)而不是傳統IP或MAC地址。

TrustSec則是由思科開發的一個框架，它根據裝置角色、使用者或情景實現跨網路的安全策略實施，而不是使用VLAN或IP地址等傳統機制。它通過將裝置分為不同的安全組並使用SGT標籤，提供更加精細和動態的網路訪問控制。

ISE中TC-NAC服務的主要功能

1.與第三方NAC系統整合:TC-NAC服務使ISE能夠與第三方網路訪問控制解決方案進行通訊和互動。對於已部署現有NAC基礎設施但希望將其與思科ISE整合以改善功能、利用其他安全策略或利用思科其他網路安全功能的組織，這非常有用。

2.提供無縫的策略實施:當與第三方NAC解決方案整合時，ISE可以接管策略實施和決策的某些方面。這樣可以建立更統一的策略框架，確保思科和非Cisco　NAC系統應用的策略在整個網路中保持一致。

3.支援傳統NAC系統:TC-NAC服務幫助具有傳統NAC系統的組織，允許它們繼續使用這些系統，同時採用思科ISE增強安全功能。ISE可以與舊式NAC解決方案整合並延長其生命週期，同時提供訪問控制、安全性和合規性實施。

4.促進第三方NAC供應商通訊:此服務允許ISE促進與使用專有協定或標準的第三方NAC解決方案的通訊。ISE可以通過行業標準協定（如RADIUS、TACACS+或SNMP）或自定義API與第三方NAC系統互動，具體取決於所用的NAC解決方案。

驗證ISE中的TC-NAC服務並對其進行故障排除

1.導航到**管理>部署> PSN節點>**啟用以威脅為中心的**NAC**，以驗證是否已啟用以威脅為中心的NAC。

2.如果SourceFire FireAMP介面卡出現問題，請驗證您的網路**中是否**允許埠443。

3.從**操作** > **以威脅**為中心的**NAC即時日誌驗證終端會話詳細資訊**。

由以威脅為中心的NAC觸發的警報：

- 介面卡無法訪問(系統日誌ID:91002):表示無法訪問介面卡。

- 介面卡連線失敗(系統日誌ID:91018):表示介面卡可訪問，但介面卡和源伺服器之間的連線已關閉。

- 介面卡由於錯誤而停止(系統日誌ID:91006):如果介面卡未處於所需狀態，將觸發此警報。如果顯示此警報，請檢查介面卡配置和伺服器連線。有關詳細資訊，請參閱介面卡日誌。

- 介面卡錯誤(系統日誌ID:91009):表示Qualys介面卡無法與Qualys站點建立連線或從Qualys站點下載資訊。

用於診斷TC-NAC問題的有用調試：

- va-runtime(varuntime.log)
- va-service（varuntime.log和vaggregation.log）
- TC-NAC(ise-psc.log)
- anc(ise-psc.log)

PassiveID WMI服務

PassiveID WMI服務是允許ISE使用Windows Management Instrumentation(WMI)作為被動機制執行裝置分析的服務，用於識別和分析網路中的端點。它在裝置分析方面發揮著關鍵作用，尤其是在需要準確識別運行Windows OS的裝置以進行網路訪問控制和策略實施的環境中。

ISE中PassiveID WMI服務的關鍵功能

1.裝置身份收集:PassiveID WMI服務允許ISE使用Windows Management Instrumentation(WMI)從Windows裝置被動收集身份資訊。 它無需裝置主動參與即可收集系統詳細資訊，如裝置主機名、作業系統版本及其他相關屬性。

2.與ISE策略整合:由PassiveID WMI服務收集的資訊已整合到ISE策略框架中。它有助於基於裝置屬性（如型別、作業系統和安全標準合規性）的動態應用策略。

驗證PassiveID WMI服務並對其進行故障排除

一個高度安全和精確的來源，也是最常見的來源，從中接收使用者資訊。作為探測器，AD與WMI技術配合使用以傳送經過身份驗證的使用者身份。此外，AD本身（而不是探測器）用作源系統（提供程式），其他探測器也將從中檢索使用者資料。

進行故障排除所需的有用調試和資訊。將這些屬性設定為PassiveID WMI問題的調試級別：

- 被動ID（被動式*）
- runtime-logging(prrt-server.log)
- Active Directory(ad)_agent.log) — 跟蹤級別
- collector(collector.log)(在PassiveID、MnT節點上和在活動pxGrid節點上（如果會話已發佈）
- pxGrid(pxgrid/)（如果會話已發佈，則在輔助MnT和活動pxGrid節點上）

排除PassiveID WMI故障所需的資訊：

1. 以前是否工作正常？最近所做的任何更改。 （如升級，在ISE上安裝補丁程式/在DC升級）

2. 測試連線是否工作正常（在整合之前，檢查測試連線）
3. 有關用於加入AD的使用者名稱以及用於WMI的使用者名稱的詳細資訊。（無論是管理員帳戶還是非管理員帳戶）
4. 檢查DC中是否記錄了事件(4768、4770)。（來自DC的事件檢視器日誌）
5. 捕獲日誌：設定被動ID和運行時記錄的調試級別，然後對該DC、AD執行配置wmi — 具有時間戳的跟蹤級別。

PassiveID Syslog服務

PassiveID Syslog服務是一項服務，它啟用PassiveID分析功能以收集和處理來自環境中網路裝置的syslog消息。這些系統日誌消息包含有關連線到網路的終端的重要資訊，ISE使用這些資訊來分析這些裝置以進行網路訪問控制和策略實施。

被動ID系統日誌服務的關鍵功能

1.被動身份驗證：Passive ID Syslog服務允許Cisco ISE通過從指示使用者和裝置活動的網路裝置（如交換機或路由器）收集系統日誌消息來被動驗證使用者和裝置。這適用於傳統主動驗證方法（例如802.1X）不合適或不可行的情況。

2.事件記錄:被動ID系統日誌服務依靠系統日誌協定從跟蹤使用者訪問和網路行為的網路裝置接收日誌。這些日誌中包含的資訊可能包括裝置登入嘗試、接入點和介面詳細資訊等內容，從而幫助ISE被動識別裝置或使用者。

PassiveID API服務

PassiveID API服務是一項服務，支援與需要有關連線到網路的裝置或使用者身份資訊的系統整合。它通常用於網路管理員希望執行基於身份的策略和操作而不要求每台裝置使用主動網路身份驗證協定（如802.1X）的環境。

被動ID API服務的主要功能

1.與外部系統的整合：被動ID API允許ISE從第三方系統或網路裝置（如交換機、路由器、防火牆或任何可以生成身份相關事件的系統）接收身份資訊。 這些外部系統可以傳送系統日誌消息、身份驗證日誌或其他相關資料等資訊，以幫助ISE被動識別使用者或裝置。

2.被動身份驗證:被動ID API服務用於通過收集身份資料來被動驗證使用者和裝置，而無需主動身份驗證(例如：無需802.1X、MAB或Web驗證)。 例如，它可以從網路裝置、Active Directory日誌或安全裝置捕獲資訊，並使用該資訊識別使用者或裝置。

3.對映身份資訊:被動ID API可用於將身份資料對映到特定安全策略。此資訊用於為使用者和裝置動態分配安全組標籤(SGT)或角色，從而影響網路訪問控制（如分段和防火牆策略）的實施。

PassiveID代理服務

PassiveID代理服務是一項服務，通過使用安裝在終端（如電腦、膝上型電腦、流動裝置等）上的PassiveID代理啟用裝置分析。 PassiveID代理允許ISE通過偵聽來自終端的流量來收集有關網路上的裝置的分析資訊，而無需主動掃描或直接與裝置互動。

被動ID代理服務的關鍵功能

1.被動使用者和裝置識別：被動ID代理服務負責被動收集身份相關資訊（通常是從網路裝置或終端），並將此資料傳送到ISE。此服務允許ISE根據使用者和裝置的活動或特徵進行身份驗證和識別，無需從裝置進行主動身份驗證(例如：未提供802.1X憑證)。

2.與其他思科元件的整合:被動ID代理與交換機、無線控制器和接入點等思科網路裝置緊密合作，從網路流量、系統日誌或其他管理系統中收集身份相關資訊。它還可以與Cisco TrustSec和思科身份服務整合，以將此資料對映到特定安全組標籤(SGT)或其他基於身份的策略。

3.情景網路訪問控制:被動ID代理將此資訊傳送給思科ISE，思科ISE然後根據使用者或裝置的身份和情景應用適當的訪問控制策略。這可能包括：

- 基於角色的訪問控制。
- 動態VLAN分配。
- 網路分段。
- 根據使用者角色或裝置安全狀態實施安全策略。

PassiveID端點服務

PassiveID Endpoint Service是一項服務，負責基於PassiveID技術識別和分析網路上的終端（裝置）。此服務可幫助ISE收集、處理和分類連線到網路的裝置相關資訊，而無需與終端本身進行主動互動。PassiveID端點服務在分析分析、網路訪問控制和安全策略實施中扮演著關鍵角色。

PassiveID端點服務的關鍵功能

1.被動使用者和裝置識別：PassiveID Endpoint Service允許Cisco ISE利用網路活動或系統日誌中的資訊被動地識別和驗證網路上的裝置。這包括根據使用者和裝置的網路行為或特徵(例如MAC地址、IP地址或從Active Directory(AD)等外部身份庫登入資訊)識別使用者和裝置。

2.從端點收集資料:終端服務從不同來源收集各種型別的終端特定資料：

- 使用者從外部身份庫（如Active Directory或其他目錄）登入資訊。
- 裝置特性，例如IP地址、MAC地址和裝置型別(例如：無論裝置是Windows PC、行動電話還是IoT裝置)。
- 終端網路活動，例如DHCP請求、ARP請求和其他網路層通訊。

PassiveID SPAN服務

PassiveID SPAN服務是一項服務，利用網路裝置上的SPAN（交換連線埠分析器）連線埠映象，擷取和分析網路流量以進行端點分析。此服務可幫助ISE通過分析網路上的終端（裝置）的網路通訊模式，被動收集有關網路上的終端（裝置）的資訊，而無需在裝置本身安裝主動探測或代理。

PassiveID SPAN服務的主要功能

1.從SPAN流量進行被動身分識別收集:PassiveID SPAN服務允許ISE根據通過交換機上的SPAN埠映象或複製的網路流量收集身份資料。SPAN連線埠通常用於透過映象來自其他連線埠或VLAN的網

路流量進行網路監控。通過捕獲此流量，ISE可以被動收集身份資訊，例如：

- 裝置的MAC地址。
- 與裝置關聯的IP地址。
- DHCP從捕獲的流量請求或其他身份相關資訊。
- 來自網路裝置（例如交換機或無線控制器）的身份驗證日誌。

2.捕獲使用者和裝置身份資訊:SPAN服務實質上會監聽通過網路的流量，並從網路資料包中識別關鍵身份資訊，而無需直接與裝置互動。這可能包括以下資料：

- 使用者通過EAP（可擴展身份驗證協定）等協定進行身份驗證時的身份。
- 基於MAC地址和IP地址的裝置標識。
- 基於觀察到的流量模式和事件的裝置角色和行為。

PassiveID Stack（PassiveID SPAN服務、PassiveID Syslog服務、PassiveID Endpoint服務、PassiveID Agent、PassiveID API服務）的驗證和故障排除

1. PassiveID stack是提供程式的清單，PassiveID堆疊中的所有服務預設處於禁用狀態。導航到ISE GUI > Administration > Deployment > Select the node, Enable Passive Identity Service，點選Save。要驗證PassiveID堆疊服務狀態，請登入到ISE節點的CLI並運行show application status ise命令。

2.如果被動ID代理有問題，請檢查是否可以從ISE節點解析代理的FQDN。要執行此操作，請登入到ISE CLI並運行nslookup < FQDN of Agent configured > 命令。

3.確保ISE索引引擎處於活動狀態，並且在ISE中配置的DNS或名稱伺服器正在解析反向和正向DNS查詢。

4.為確保與系統日誌提供商進行無縫通訊，請檢查UDP埠40514和TCP埠1468是否已在網路中開啟。

5.要在節點上配置SPAN提供程式，請確保已啟用ISE被動身份服務。使用ISE CLI中的show interface命令，驗證要在SPAN提供程式上配置的介面在ISE中可用。

要基於被動ID提供程式檢查日誌，您需要檢視passiveid-syslog.log、passiveid-agent.log、passiveid-api.log、passiveid-endpoint.log、passiveid-span.log。可以從ISE節點的支援捆綁包保護上述日誌。

DHCP伺服器(dhcpd)

DHCP伺服器(dhcpd)服務是一種向網路裝置提供動態主機配置協定(DHCP)功能的服務。它主要用於將IP地址分配給嘗試連線到網路的裝置（終端）。在ISE中，DHCP伺服器在將IP地址提供給端點方面發揮著關鍵作用，這些端點在連線到網路時請求這些地址。該服務還可以提供其他配置資訊，例如DNS伺服器、預設網關和其他網路設定。

ISE中DHCP伺服器(dhcpd)服務的關鍵功能

1.動態IP地址分配：ISE中的dhcpd服務充當DHCP伺服器，為連線到網路時請求IP地址的裝置提供

IP地址分配。在裝置動態加入網路的場景中，例如在BYOD（自帶裝置）環境中，或者當裝置配置為自動獲取其IP地址時，這一點非常重要。

2.基於配置檔案的DHCP:dhcpd服務可以根據裝置的配置檔案分配IP地址。如果ISE已分析裝置(例如：如果確定它是智慧手機、筆記型電腦、物聯網裝置)，則可以根據裝置型別或角色分配適當的IP地址或應用其他設定。

3.支援DHCP中繼：ISE可以充當DHCP中繼代理，如果ISE不處理實際IP地址分配，則將DHCP請求從裝置轉發到外部DHCP伺服器。在這種情況下，dhcpd服務可以將來自裝置的請求轉發到中央DHCP伺服器，而ISE繼續應用網路策略和訪問控制。

檢驗DHCP伺服器(dhcpd)並排除故障

1.聯絡Cisco TAC驗證DHCP伺服器軟體包是否安裝在ISE上。

2.登入到**ISE > rpm -qi dhcp的根**。

DNS伺服器（已命名）

DNS伺服器（命名）服務是允許ISE充當DNS（域名系統）伺服器或DNS解析程式的服務。它主要負責將域名解析為IP地址，反之亦然，從而促進網路中裝置之間的通訊。

ISE中DNS伺服器（命名）服務的關鍵功能

1.用於ISE通訊的DNS解析:ISE中的命名服務有助於將域名解析為IP地址。當ISE需要使用域名而不是IP地址連線到其他網路裝置或外部服務（例如Radius伺服器、Active Directory或外部NTP伺服器）時，這一點尤為重要。

- 例如，當ISE需要到達Radius伺服器或外部目錄服務（如Active Directory）時，它需要將該伺服器的域名解析為IP地址。
- ISE查詢系統上配置的DNS伺服器以解析這些域名，確保順利通訊。

2.外部服務的DNS解析:DNS服務使ISE能夠連線到需要域名的外部服務。例如，ISE需要解析外部服務的名稱，例如：

- 基於雲的服務。
- NTP（網路時間協定）伺服器。
- 證書頒發機構(CA)或LDAP伺服器。

3.多域和冗餘DNS伺服器:可以將ISE配置為使用多個DNS伺服器實現冗餘。當一個DNS伺服器不可用時，ISE可以回退到另一個DNS伺服器以確保持續運行和DNS解析。

驗證DNS伺服器（已命名）並排除故障

1.在ISE節點的CLI中，使用**ping <IP of DNS server / name server>** 命令驗證對部署中的名稱伺服器或DNS伺服器的可訪問性。

2.通過ISE CLI使用**nslookup <ISE節點的FQDN/IP地址>**命令驗證ISE FQDN的DNS解析。

ISE消息服務

ISE消息服務是促進ISE系統內各種服務和元件之間非同步通訊的元件。它在ISE的整體系統架構中扮演著關鍵角色，使平台的不同部分能夠傳送和接收消息、管理任務以及同步活動。

ISE消息服務的主要功能

1.進程間通訊(IPC):ISE消息服務在實現各種ISE服務之間的進程間通訊(IPC)方面發揮著關鍵作用。它確保不同的ISE模組和服務（如身份驗證、授權和策略實施）能夠以協調的方式交換資料和指令。

2.分散式環境支援:在較大或分散式ISE部署中（例如在多節點或高可用性配置中），消息服務有助於促進各種ISE節點之間的通訊。這可確保資料（如身份驗證請求、使用者會話和策略更新）在ISE系統中的不同節點之間正確同步。

3.策略和配置同步:消息服務參與在ISE節點之間同步配置和策略。當對主節點進行配置更改時，該服務確保這些更改傳播到系統中的輔助節點或備份節點。這對於保持一致性和確保跨不同位置或分散式ISE節點應用的網路訪問策略保持同步至關重要。

驗證ISE消息服務未運行或正在初始化

1.驗證埠TCP 8671在防火牆中未被阻止，因為該埠用於ISE裝置之間的節點間通訊。

2.驗證隊列連結錯誤，如果存在隊列連結錯誤，請續訂ISE消息傳遞和ISE根CA證書，因為隊列連結錯誤通常會因內部證書損壞問題而發生。要解決隊列連結錯誤，請通過參考以下文章更新ISE消息和ISE根CA證書：ISE — 隊列連結錯誤

3.從GUI ->管理 — >證書 — >選擇ISE消息傳遞證書。單擊「檢視」以驗證證書的狀態。

用於ISE消息服務故障排除的有用日誌是ade.log，可在支援捆綁包中獲得，也可以在問題發生期間使用show logging system ade/ADE.log tail命令通過CLI進行跟蹤。

4.如果ADE.log log showup rabbitmq:連線拒絕錯誤，請聯絡Cisco TAC從ISE根刪除Rabbitmq模組的鎖。

ISE API網關資料庫服務

ISE API網關資料庫服務是一個元件，負責在ISE系統內管理和處理與API請求和響應相關的資料。它充當連線ISE API網關與ISE資料庫的中介，確保自定義應用程式也可以通過服務管理的API呼叫更新或修改ISE中的資料（例如，調整訪問策略或新增/刪除使用者）。

ISE API網關資料庫服務的主要功能

1.對ISE資料的API訪問:ISE API網關資料庫服務充當網橋，允許外部應用程式通過ISE RESTful API與ISE資料庫互動。這些API可用於檢索或修改儲存在ISE資料庫中的資料，例如：

- 使用者身份驗證日誌。
- 網路訪問策略。
- 裝置分析資訊。

- 系統配置和設定。

2.啟用外部系統整合:此服務在將ISE與外部系統整合時起著關鍵作用，例如：

- 外部身份驗證伺服器(LDAP、Active Directory、RADIUS)。
- 網路管理系統(NMS)。
- 安全資訊和事件管理(SIEM)解決方案。
- 需要與ISE資料互動的自定義應用程式或服務。

通過提供API訪問，API網關資料庫服務允許這些外部系統查詢ISE資料、向ISE傳送更新或觸發ISE內的特定操作以響應外部事件。

3.支援RESTful API通訊:ISE公開設計為通過HTTP/HTTPS工作的RESTful API。API網關資料庫服務負責管理API請求和響應流，確保請求經過身份驗證、處理，並且從ISE資料庫返回適當的資料作為響應。

ISE API閘道服務

ISE API網關服務是一個關鍵元件，它提供對ISE服務、資料和功能的RESTful API訪問。它充當ISE與外部系統之間的橋樑，允許這些系統與ISE網路訪問控制、策略實施、身份驗證和其他服務進行程式設計互動。API網關使第三方應用、網路管理系統和自定義應用能夠與Cisco ISE互動，而無需手動干預或直接訪問ISE使用者介面。

ISE API網關服務的關鍵功能

1.啟用對ISE的API訪問：ISE API網關服務使外部系統能夠使用RESTful API安全地訪問思科ISE資料和策略並與之互動。這提供了對ISE功能的程式設計訪問，如身份驗證、策略實施、會話管理等。

2.提供方案控制:API網關服務允許對ISE功能進行程式設計控制。管理員和開發人員可以使用API:

- 檢索或修改網路策略。
- 查詢或管理使用者會話和身份驗證日誌。
- 建立和管理網路訪問控制規則。
- 訪問或更新裝置配置檔案。

此控制可用於自動化或自定義工作流程協調，例如基於即時資料動態調整網路訪問策略，或將ISE整合到更廣泛的安全自動化平台中。

3.監測和報告:API網關服務允許外部系統從操作ISE日誌、會話歷史和策略實施詳細資訊中收集資料。這對以下方面很重要：

- 合規性報告。
- 安全監控。
- 事件響應。

API呼叫可用於獲取日誌、稽核資訊和事件，允許安全團隊從集中儀表板或報告工具監控ISE活動。

驗證ISE API網關服務和ISE API網關資料庫服務並對其進行故障排除

1.驗證ISE節點的管理員證書是否處於活動狀態且有效。導航到Administration > Certificates > Select the node > Select Admin Certificate。點選View以驗證ISE節點的管理員證書的狀態。

2.將ise-api-gateway、api-gateway、apiservice元件設定為debug，並且可以使用以下命令跟蹤日誌：

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

ISE pxGrid直接服務

ISE pxGrid直接服務是支援ISE中的pxGrid（平台交換網格）功能的重要元件。pxGrid是一種思科技術，它有助於在思科網路安全解決方案和第三方應用、服務和裝置之間實現安全、標準化和可擴展的資料共用和整合。ISE pxGrid直接服務支援ISE與其他pxGrid相容系統之間的直接通訊，而無需中間裝置或服務。

ISE pxGrid直接服務的關鍵功能

1.與第三方系統的直接整合:ISE pxGrid直接服務允許ISE直接與第三方網路安全系統整合，例如防火牆、路由器、NAC解決方案、SIEM平台和其他安全裝置。它允許這些系統交換有關網路訪問事件、安全事件和情景網路資料的資訊。

2.情景共用:pxGrid的主要功能之一是共用情景資訊（如裝置身份、使用者角色、安全狀態和網路訪問資訊）。 藉助pxGrid直接服務，ISE可以直接與其他裝置或應用共用此情景，而無需依賴RADIUS或TACACS+等傳統方法。

3.簡化通訊:通過使用pxGrid，ISE可以使用標準化協定與第三方解決方案通訊和交換資訊。這簡化了整合過程，因為系統不需要對每個第三方解決方案進行自定義整合。

4.增強安全性和合規性:pxGrid Direct服務還可通過確保網路生態系統中的所有系統都能夠訪問相同的有關使用者、裝置和安全策略的即時情景資料，來改善安全狀況和合規性。這可確保在整個環境中更協調地實施網路安全策略。

驗證ISEPxgrid Direct服務並對其進行故障排除

1.聯絡Cisco TAC以驗證/tmp資料夾中是否存在**edda*.lock***。如果是，Cisco TAC會移除鎖定並從根重新啟動Pxgrid Direct服務。

2.將**PxGrid Direct**元件設定為在ISE節點中調試以進行故障排除。可以使用以下命令通過ISE支援捆綁包或ISE CLI保護日誌：

show logging application pxgriddirect-service.log

show logging application pxgriddirect-connector.log

提到的日誌提供了思科ISE獲取和接收的終端資料以及Pxgrid聯結器的連線狀態的資訊。

分段策略服務

分段策略服務是一個關鍵元件，負責根據使用者身份、裝置狀態或其他情景資訊實施網路分段策略。它有助於控制使用者和裝置對特定網段的訪問，確保只有授權使用者或合規裝置才能訪問網路的某些部分。 網路分段對於減少網路的攻擊面、防止威脅的橫向移動以及確保遵守管理法規至關重要。ISE中的分段策略服務用於在網路中動態和靈活地執行這些網路分段規則。

分段策略服務的主要功能

1.定義網段:ISE中的分段策略服務允許管理員根據使用者或裝置的特性定義各種網段（子網或VLAN）。舉例來說：

- 具有不同安全狀況的裝置可以分配給不同的網段(例如：一個VLAN中的受信任裝置和另一個VLAN中的不受信任裝置)。
- 可以將不同部門或角色的使用者分配給不同的網段，以實施最小許可權並限制對敏感資源的訪問。

2.動態分段:該服務支援動態網路分段，意味著網段或VLAN可以基於即時條件進行更改。舉例來說：

- 可以根據使用者的角色或裝置運行狀況狀態將其分配給特定VLAN。
- 被視為不合規或運行過期作業系統的裝置可以移至隔離區或訪客VLAN，直至修復。

3.基於政策的執行:分段策略服務使用策略來決定裝置或使用者必須置於哪個分段中。這些政策可以考慮各種因素，例如：

- 使用者身份:基於使用者角色或屬性。
- 裝置狀態:裝置的運行狀況或合規性狀態(例如：它是否運行最新的防病毒軟體？)。
- 位置:使用者或裝置在網路中的物理位置(例如：辦公室、訪客區域、遠端訪問)。
- 存取時間:提出訪問請求時一天的時間或一週中的某一天。

4.安全策略實施:分段策略服務通過利用RADIUS和VLAN分配等行業標準，確保跨網路裝置（如交換機、路由器、防火牆）一致地實施安全策略。這允許Cisco ISE與網路基礎設施裝置通訊以實施所需的分段策略。

驗證分段策略服務並對其進行故障排除

1.導航到工作中心> TrustSec >概述>控制面板，驗證分段是否正確配置。

2. Work Centers > TrustSec > Reports，選擇TrustSec reports以驗證分段策略服務狀態和報告。

REST身份驗證服務

REST身份驗證服務是一項使用RESTful API提供身份驗證功能的服務。它允許外部應用和系統通過使用標準REST協定通過HTTP(S)與ISE進行互動，從而驗證使用者或裝置。此服務允許將Cisco ISE身份驗證功能與需要驗證使用者或裝置但無法使用傳統方法（如RADIUS或TACACS+）的第三方應用或系統無縫整合。

REST身份驗證服務的關鍵功能

1. RESTful身份驗證:REST身份驗證服務通過REST API協定啟用身份驗證請求。這樣可允許外部系統(例如：應用、第三方網路裝置或服務)，驗證使用ISE作為身份驗證伺服器的使用者或裝置，但通過REST風格的Web服務呼叫，而不是傳統的身份驗證協定（如RADIUS或TACACS+）。

2.與外部應用程式的整合:此服務專為需要驗證使用者或裝置身份，但不使用傳統驗證方法（例如RADIUS或TACACS+）的外部應用而設計。 相反，它們可以通過REST API與ISE進行互動，從而簡化將ISE身份驗證整合到基於Web或雲原生應用程式中的過程。

3.靈活且可擴展的身份驗證:REST身份驗證服務提供可擴展的身份驗證方法，不僅限於網路裝置或本地解決方案。雲服務、移動應用和其他基於Web的平台可以使用它，這些平台需要通過查詢ISE的憑證和策略來驗證使用者或裝置。

4.易於應用:REST API提供標準化介面，與傳統方法相比，更易於應用並與現代軟體和應用整合。它提供JSON格式的響應，並使用HTTP方法（如GET、POST、PUT和DELETE），使Web開發人員和整合了ISE進行身份驗證的系統可以更輕鬆地訪問它。

Rest Auth的驗證和疑難排解

1.要排除與Open API相關的問題，請將apiservice元件設定為debug。

2.要排除與ERS API相關的問題，請將ers元件設定為調試。

如果API服務GUI頁面： https://{iseip}:{port}/api/swagger-ui/index.html或https://{iseip}:9060/ers/sdk可訪問，它認為API服務正在按預期工作。

有關API的詳細資訊，請參閱API文檔。

SSE聯結器

SSE聯結器（安全軟體定義邊緣聯結器）是一項將ISE與思科安全軟體定義存取(SD-Access)解決方案整合的服務。SSE聯結器允許ISE與Cisco DNA Center安全通訊，從而在SD-Access環境中實現自動網路策略、分段和邊緣安全管理。

SSE聯結器的主要功能

1.與第三方安全系統整合：SSE聯結器促進思科ISE與第三方安全系統(如防火牆、入侵防禦系統(IPS)、網路訪問控制(NAC)解決方案，以及安全資訊和事件管理(SIEM)系統的整合。它允許這些外部系統以安全方式從ISE傳送或接收資料，可用於更動態的策略實施。

2.即時威脅情報:通過將ISE與其他安全系統連線，SSE聯結器支援即時威脅情報的交換。此資訊可能包括可疑活動、受感染的終端或其他安全系統檢測到的惡意行為，從而允許ISE根據當前威脅級別或裝置狀態動態調整訪問策略。

3.自動補救:由SSE聯結器支援的整合可支援自動修復工作流程。例如，如果系統被外部安全裝置標籤為已受損，ISE可以自動實施阻止網路訪問的策略，或將終端重定向到補救網段以進行進一步調查。

驗證SSE聯結器並對其進行故障排除

1.僅當在ISE中啟用PassiveID服務時，才會啟用SSE聯結器。

2.debug中的sse-connector(connector.log)元件提供了有關SSE聯結器相關消息的更多資訊。

Hermes（pxGrid雲代理）

Hermes(pxGrid Cloud Agent)是一個元件，可促進ISE和pxGrid（平台交換網格）生態系統在雲環境中的整合。Hermes是一種基於雲的代理，用於實現ISE與基於雲的服務或平台之間的通訊，支援pxGrid框架以跨不同的網路和安全系統共用情景資訊。

Hermes(pxGrid Cloud Agent)的主要特性和功能

1.雲到現場整合：Hermes（pxGrid雲代理）旨在促進基於雲的服務與本地ISE基礎設施之間的無縫整合。它將pxGrid的強大功能擴展到傳統的內部網路環境之外，實現了跨基於雲的應用程式和服務的安全資料交換和策略實施。

2.pxGrid生態系統支援:pxGrid是一種思科平台，用於跨網路安全解決方案安全地共用情景和資訊。Hermes充當pxGrid的雲代理，實現ISE和各種基於雲的服務之間的安全、即時通訊。這種整合使網路安全策略在本地和雲環境中保持一致，從而更輕鬆地管理和實施安全性。

3.基於雲的終端可視性:Hermes的核心優勢之一是它提供了對基於雲的終端的可視性，類似於ISE如何提供內部終端的可視性。它可以收集有關雲中裝置和使用者的資料，例如其合規狀態、安全狀態和身份資訊。這允許ISE在雲終端上實施網路訪問策略，就像對本地裝置一樣。

4.將ISE無縫擴展至雲環境:Hermes的主要優勢之一是它可以在ISE本地環境和越來越多的雲本地應用之間提供一個無縫的網橋。這樣，無需對現有基礎設施進行全面徹底的改造，即可將ISE安全策略、身份驗證方法和訪問控制擴展至雲服務。

驗證Hermes（Pxgrid雲代理）並對其進行故障排除

1.預設情況下，Hermes服務處於禁用狀態，將ISE與Cisco PxGrid雲連線會啟用Hermes服務。因此，如果在ISE中禁用Hermes服務，驗證是否從**ISE GUI >管理>部署啟用Pxgrid雲選項，請選擇ISE節點**。編輯，啟用**Pxgrid Cloud**。

2.用於解決與Pxgrid雲相關的問題的有用調試是**hermes.log**和**pxcloud.log**。這些調試僅在啟用了Pxgrid雲的Pxgrid節點上可用。

McTrust（Meraki同步服務）

McTrust（Meraki同步服務）是一項支援思科ISE和思科Meraki系統之間整合的服務，專門用於同步和管理網路裝置和訪問策略。McTrust服務充當聯結器，用於在Meraki雲託管網路基礎設施和ISE本地身份和策略管理系統之間同步使用者和裝置資訊。

McTrust（Meraki同步服務）的主要特性和功能

1.與Meraki裝置的無縫整合：McTrust使ISE能夠與Meraki的雲託管裝置同步和整合。這包括屬於Meraki產品組合的Meraki接入點、交換機和安全裝置等裝置。它允許ISE直接與Meraki的基礎設施通訊，從而更輕鬆地將網路訪問控制策略應用到Meraki管理的裝置。

2.自動裝置同步:Meraki同步服務自動將ISE策略與Meraki網路裝置同步。這意味著對ISE中的網路訪問控制策略所做的任何更改都會自動反映在Meraki裝置中，無需手動干預。這使管理員可以更輕鬆地管理跨Meraki和ISE平台的網路訪問。

3. Meraki受管裝置的策略實施:McTrust允許ISE根據身份驗證和裝置狀態在Meraki裝置上實施網路訪問策略。它可以動態地將策略分配給Meraki網路元素，如調整VLAN分配、應用訪問控制清單(ACL)或限制對特定網路資源的訪問，具體取決於請求訪問的裝置或使用者的安全狀態。

4. Meraki控制面板整合:McTrust將ISE直接與Meraki控制面板整合，從而提供統一的管理介面。通過此整合，管理員可以在Meraki雲託管介面中檢視和管理Meraki裝置和ISE託管資源的網路策略和訪問控制規則。

驗證McTrust（Meraki同步服務）並對其進行故障排除

1.登入到ISE GUI ->工作中心 — > TrustSec ->整合 — >同步狀態。驗證發現的任何問題/錯誤。

2.確保ISE節點的所有管理員證書處於活動狀態且有效。

meraki-connector.log是對Meraki同步服務進行故障排查的有用調試。

ISE節點匯出器

ISE節點匯出器服務是一個用於監控和收集ISE系統效能度量的元件，特別是從ISE節點（無論是管理節點、監控節點還是策略服務節點）。

ISE節點匯出器的主要特性和功能

1.指標匯出:ISE節點匯出器提供多種與效能相關的度量，例如CPU使用情況、記憶體使用情況、磁碟利用率、網路統計資訊、系統負載和其他作業系統級別的度量。這些度量隨後用於監控ISE節點的運行狀況和效能，並且可以在監控控制面板（如Grafana）中進行視覺化。

2.系統運行狀況監控:通過將效能資料匯出到Prometheus，ISE節點匯出器允許持續監控ISE節點的運行狀況和運行狀態。管理員可以根據預定義的閾值建立警報，以通知他們效能下降或系統問題。

3. Prometheus整合:ISE節點匯出器通常與Prometheus結合使用，Prometheus是一個開源監控和警報工具包，旨在實現可靠性和可擴充性。節點匯出器顯示系統級度量，Prometheus可以擦除這些度量以收集和儲存時序資料。

ISE Prometheus服務

ISE Prometheus服務是將Prometheus與ISE整合以實現監控和從ISE系統收集效能指標的服務。Prometheus是一個開源的監控和警報工具包，用於收集、儲存和分析時間序列資料，ISE Prometheus服務允許ISE向Prometheus公開其內部度量以用於監控。

ISE Prometheus服務的主要特性和功能

1.用於監控的指標收集:ISE Prometheus服務旨在匯出與ISE系統相關的各種操作和效能指標。這些度量通常包括（但不限於）CPU利用率和系統負載、記憶體使用、磁碟使用和I/O效能、網路統計資訊、身份驗證請求統計資訊、策略實施統計資訊、系統運行狀況和正常運行時間資料

2. Prometheus整合:Prometheus Service允許ISE以與Prometheus相容的格式公開資料，Prometheus會定期銷毀此資料。然後，Prometheus將資料儲存在時間系列資料庫中，從而能夠跟蹤ISE系統的趨勢和歷史效能。

3. Grafana的視覺化和報告:ISE中的Prometheus Service與Grafana（一個流行的開源視覺化工具）無縫整合。將度量匯出到Prometheus後，管理員可以使用Grafana儀表板即時顯示資料。這樣可以輕鬆識別ISE部署中的效能瓶頸、系統趨勢和潛在問題。

ISE Grafana服務

ISE Grafana服務是一項使用Grafana（一個用於監控和資料視覺化的開源平台）提供系統效能指標視覺化的服務。它與Prometheus整合以顯示從ISE收集的即時和歷史資料，使管理員能夠建立互動式儀表板，提供對ISE系統的運行狀況、效能和使用的見解。

ISE Grafana服務的主要特性和功能

1.可自定義的控制面板：Grafana高度可自定義，允許管理員根據特定監控需求建立和修改儀表板。可以建立自定義查詢以從Prometheus提取特定資料點，並且這些查詢可以用各種格式進行視覺化，如圖形、表格、熱圖等。

2.對分散式ISE部署的集中監控:對於分散式ISE部署，其中多個ISE節點部署在不同位置，Grafana提供從每個節點收集的所有系統指標的集中檢視。這允許管理員從一個位置監控整個ISE部署的效能。

3.歷史資料和趨勢分析:Grafana利用儲存在Prometheus中的資料，對系統指標進行歷史分析，使管理員能夠跟蹤隨時間變化的趨勢。例如，他們可以監控過去一個月內CPU使用率的變化情況或身份驗證成功率的波動情況。此歷史資料對於容量規劃、趨勢分析和確定長期問題很有價值。

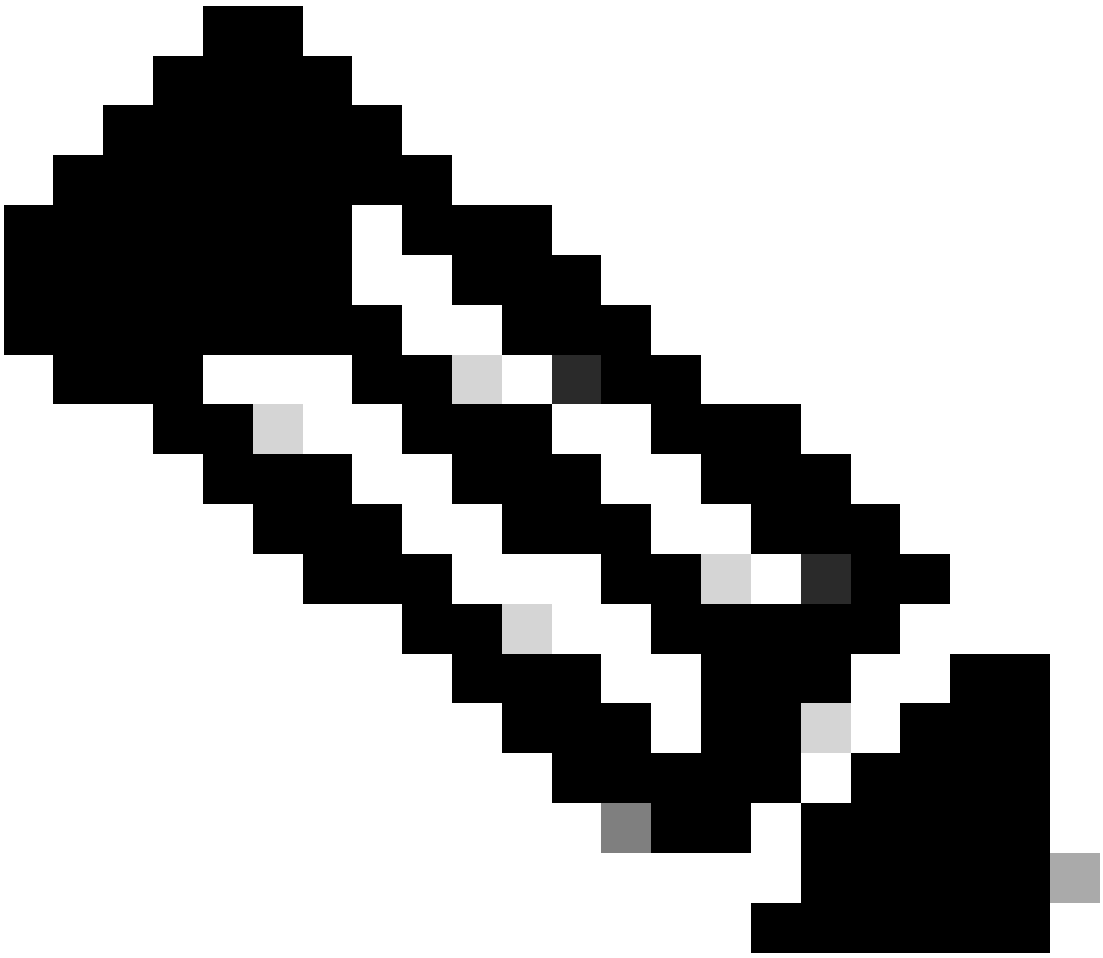
驗證ISE Grafana服務、ISE Prometheus服務、ISE節點匯出器並排除故障

1. ISE Grafana服務、ISE Prometheus服務和ISE節點匯出器服務協同工作，稱為Grafana堆疊服務。沒有特定的調試程式可用於對這些服務進行故障排除。但是這些指令有助於進行疑難排解。

show logging application ise-prometheus/prometheus.log

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

show logging application ise-grafana/grafana.log



附註：啟用監控後，ISE節點匯出器、ISE Prometheus服務和ISE Grafana服務必須正在運行，並且這些服務中的任何一個的中斷都會在資料收集期間導致問題。

ISE MNT日誌分析彈性搜尋

ISE MNT LogAnalytics Elasticsearch是將Elasticsearch與ISE監控和故障排除(MNT)功能整合的元件。它用於與ISE日誌和事件相關的日誌聚合、搜尋和分析。Elasticsearch是一個廣泛使用的分散式搜尋和分析引擎，與ISE整合後，可增強系統儲存、分析和視覺化由ISE元件生成的日誌資料的能力。

ISE MNT LogAnalytics Elasticsearch的主要特性和功能

1.日誌儲存和索引：ISE中的Elasticsearch服務負責儲存和索引ISE生成的日誌資料。Elasticsearch是一個分散式搜尋和分析引擎，它允許ISE日誌以快速搜尋、查詢和檢索特定事件、錯誤或系統活動的方式儲存。

2.與日誌分析整合：ISE MNT LogAnalytics Elasticsearch與Log Analytics配合使用，可提供全面的日誌記錄解決方案。它使ISE能夠收集與身份驗證、策略實施、系統操作和其他活動相關的日誌資

料。這些資料儲存在Elasticsearch中，便於執行詳細分析並深入瞭解ISE行為。

3.集中日誌記錄:通過與Elasticsearch整合，ISE提供了集中日誌記錄解決方案，這對於需要分散式日誌收集的環境至關重要。這使管理員可以在單個統一介面中檢視和分析來自多個ISE節點的日誌，從而更輕鬆地對ISE效能進行故障排除和監控。

4.日誌分析和故障排除:ISE MNT LogAnalytics Elasticsearch服務通過使日誌資料易於訪問，幫助管理員分析系統行為和排除問題。例如，如果身份驗證故障突然增加或系統意外中斷，Elasticsearch允許快速查詢日誌資料，以確定根本原因。

驗證ISE M&T LogAnalytics Elasticsearch並排除故障

1.在ISE中禁用和重新啟用日誌分析服務必須有所幫助。導航到操作>系統360 >設定>日誌分析（使用切換選項禁用和啟用）。

2.從ISE根重新啟動M&T LogAnalytics可解決此問題。聯絡Cisco TAC以執行此操作。

已知瑕疵

思科錯誤ID ·66198

ISE Logstash服務

ISE Logstash Service是一個整合了Logstash（一個開源資料處理管道）和ISE的元件，用於日誌收集、轉換和轉發。Logstash充當日誌收集器和日誌轉發器，允許處理ISE日誌並將其傳送到其他系統進行分析、儲存和監控。 Logstash是一個功能強大的開源工具，它收集、分析和轉發來自不同來源的日誌或其他資料，並將其傳送到一個中央位置進行儲存、分析和視覺化。在ISE環境中，ISE Logstash Service用於以結構化格式處理日誌並將其轉發到集中日誌系統，在此系統可以進一步分析、監控和視覺化。

ISE Logstash服務的主要特性和功能

1.日誌收集和轉發：ISE Logstash Service的主要功能是從各種ISE元件（如身份驗證日誌、系統日誌、策略實施日誌等）收集日誌資料，並將其轉發到中央位置（通常為Elasticsearch或其他日誌管理系統）進行儲存和分析。

2.日誌分析:Logstash可以將收集到的日誌解析為結構化格式。它處理原始日誌資料並從其中提取有意義的資訊，將日誌條目轉換為易於查詢和分析的格式。這可能涉及在將資料轉發到Elasticsearch或其他系統之前對其進行過濾、解析和豐富。

驗證ISE Logstash服務並對其進行故障排除

1.沒有要啟用的特定調試。但是，**show logging application ise-logstash/logstash.log** 會提供關於服務狀態的見解。

2.在ISE中禁用和重新啟用日誌分析服務必須有所幫助。導航到**操作>系統360 >設定>日誌分析**（使用切換選項禁用和啟用）。

與Logstash服務相關的已知缺陷

思科錯誤ID ·74832

思科錯誤ID ·58596

ISE Kibana服務

ISE　Kibana服務是一個將Kibana（一種開源資料視覺化工具）與ISE日誌記錄和監控基礎設施整合的元件。Kibana與Elasticsearch（儲存和索引日誌資料）配合工作，為視覺化、搜尋和分析ISE日誌和效能度量提供了一個強大的平台。

ISE Kibana服務的主要特性和功能

1.資料視覺化:ISE Kibana服務允許管理員建立從ISE收集的日誌資料的視覺化表示。這可能包括：

- 有關身份驗證、策略實施、使用者活動和系統運行狀況趨勢的圖表、圖表和表。
- 餅圖、折線圖和條形圖，用於跟蹤特定指標，如登入失敗次數、會話持續時間或一段時間的錯誤。

驗證ISE Kibana服務並進行故障排除

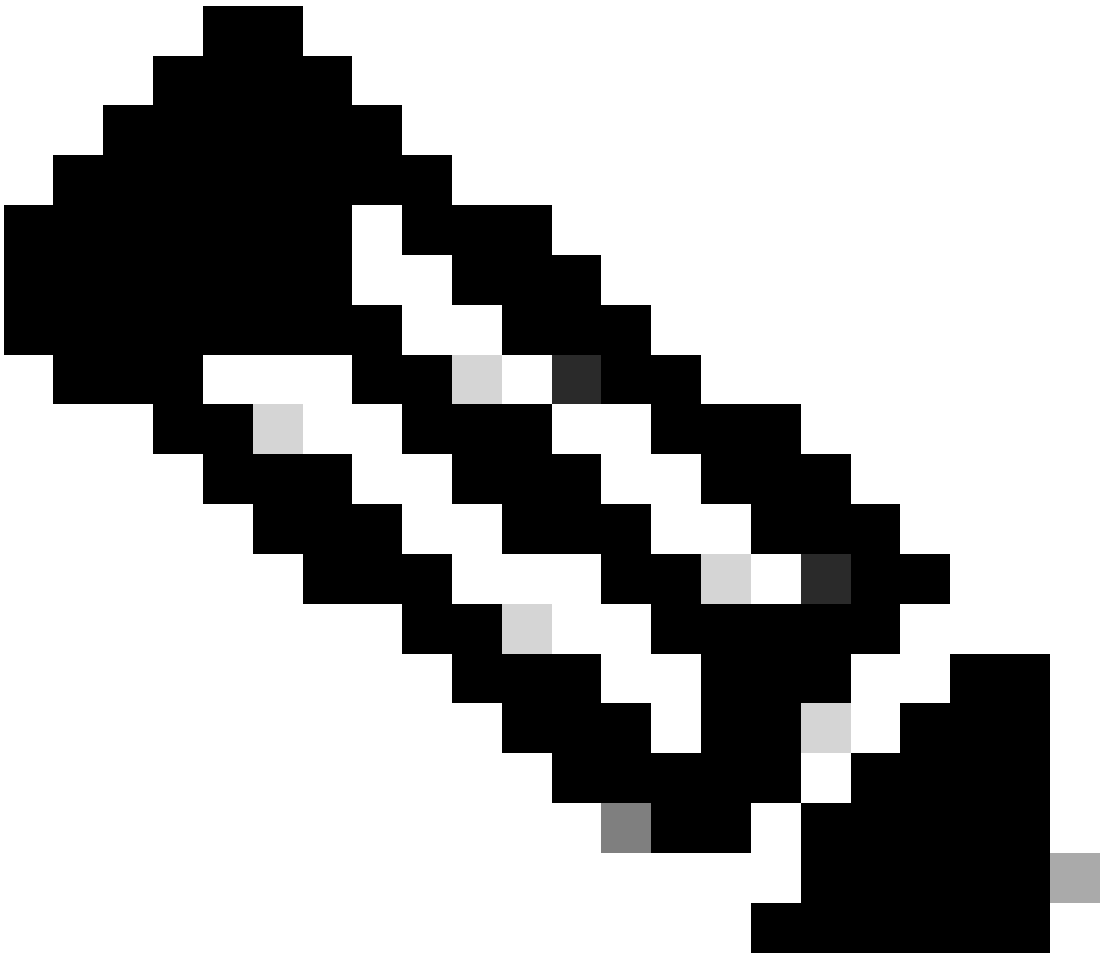
1.如果ISE kibana服務未運行，在ISE中禁用並重新啟用日誌分析，導航到操作>系統360 >設定，日誌分析（通過使用切換選項禁用和啟用）。

2.在許多情況下，/etc/hosts資料夾中可能有一個重復條目，必須導致問題。聯絡TAC以刪除重複條目。

與Kibana問題相關的已知缺陷

思科錯誤ID ·78050

思科錯誤ID ·59848



附註：啟用日誌分析後，ISE MNT LogAnalytics Elasticsearch、ISE Logstash Service和ISE Kibana Service必須正在運行，並且任何這些服務的中斷都會在資料收集期間產生問題。

ISE本地IPSec服務

ISE本地IPSec服務是指內建的IPSec（Internet協定安全）支援，可提供ISE節點之間或ISE與其他網路裝置之間的安全通訊。IPSec是一套協定，用於通過驗證和加密通訊會話中的每個IP資料包來保護網路通訊。本地IPSec服務是更廣泛的安全和網路訪問管理框架的一部分。它提供處理和管理IPsec VPN連線的功能，確保ISE系統和遠端終端之間傳輸的資料是安全的。這可能涉及到與客戶端裝置、網路訪問裝置（如路由器或防火牆）甚至其他ISE節點的互動，在這些節點中，IPsec加密和隧道對於保護敏感資訊是必需的。

ISE本地IPSec服務的主要特性和功能

1.通過IPsec的安全通訊：ISE本地IPSec服務的主要功能是使用IPsec建立和維護安全通訊通道。這涉及使用加密和身份驗證機制來確保ISE和其他裝置之間傳輸的資料受到保護，不會遭到攔截、篡改和未經授權的訪問。

2. IPsec VPN連線:ISE本地IPSec服務有助於促進使用IPsec協定為資料傳輸提供安全、加密隧道的VPN連線。這對於需要通過不受信任的網路（例如網際網路）安全訪問ISE環境的遠端員工、分支機構或其他位置尤其有用。

3.遠端訪問VPN支援:本地IPSec服務可參與遠端訪問VPN配置，其中位於非現場的使用者或裝置（如遠端員工或分支機構）通過IPsec隧道安全連線到ISE系統。此服務確保在到達ISE環境之前對所有遠端訪問流量進行加密和身份驗證。

4.IPsec VPN客戶端相容性:ISE本地IPSec服務確保與IPsec VPN客戶端的相容性。它支援常見的客戶端配置，使裝置能夠安全地連線到網路，而不會將敏感資料暴露於風險中。

對本機IPSec服務進行驗證和故障排除

1.本機IPSec服務沒有要啟用的特定調試。使用show logging application strongswan/charon.log tail命令通過ISE CLI驗證日誌。

2.如果發現隧道存在任何問題，請通過GUI > Administration > System > Settings > Protocols > IPSec > Native IPSec驗證隧道建立的狀態。

MFC探查器

MFC探查器是用於分析網路裝置和端點的專用元件。分析是網路訪問控制的關鍵部分，因為它允許ISE識別網路上的裝置，對它們進行分類，並根據裝置型別和行為應用適當的網路策略。

ISE中MFC Profiler服務的主要特性和功能

1.流量分析：ISE中的MFC分析器服務負責收集和分析流量資料。它監控終端在網路上的行為，包括所使用的應用型別、所訪問的服務以及裝置顯示的流量模式。此資料可幫助為每個端點構建配置檔案。

2.終端分析:MFC探查器服務允許ISE根據終端的行為識別終端並對其進行分類。例如，它根據流量模式檢測終端是否為印表機、電腦或流動裝置。這有助於針對不同型別的裝置實施更具體的策略，從而提高安全性和運營效率。

驗證MFC分析器服務並對其進行故障排除

1.導航到ISE GUI -> Administration -> Profiling -> MFC分析和AI規則，驗證服務是否已啟用。

2.如果服務已啟用，但通過show application status ise 命令在ISE CLI中顯示為已禁用/未運行。請參考Step1在ISE中禁用和重新啟用MFC分析服務。

用於故障排除的有用調試：調試中的MFC探查器元件。通過ISE CLI使用show logging application ise-pi-profiler.log tail 命令從支援捆綁包中驗證日誌或跟蹤日誌。

MFC探查器顯示未運行而不是禁用狀態的已知缺陷：

思科錯誤ID ·72853

要點

1.要恢復服務，請使用application stop ise和application start ise命令通過ISE CLI重新啟動服務。

2.出現問題時，確保從ISE GUI/ISE CLI捕獲支援捆綁包，以進一步驗證問題。通過GUI和CLI建立ISE支援捆綁的參考連結：在身份服務引擎上收集支援捆綁包

3.如果問題涉及資源、負載平均值、磁碟利用率等，則必須收集執行緒轉儲和堆轉儲進行分析。

4.執行節點重新載入之前，請與Cisco TAC聯絡並提供安全日誌以供進一步分析。

ISE中的標準問題

除ISE服務問題外，這些是ISE節點中需要的一些關注事項以及基本的故障排除步驟。

驗證高平均負載、資源利用率問題（CPU/記憶體/磁碟）、資源不足

1.使用show inventory命令，通過ISE CLI驗證是否已將思科建議的資源分配給節點。

2.從ISE節點的CLI運行tech top命令以驗證ISE的資源利用率。

3.通過ISE CLI使用show disk 命令驗證磁碟利用率。

4.清除非活動端點，清除節點的本地磁碟並執行升級清除。

如果問題仍然存在，請與Cisco TAC聯絡，並從遇到問題的節點提供安全支援捆綁包、堆轉儲和執行緒轉儲。

要保護堆轉儲，請登入到ISE節點的CLI，運行**application configure ise**命令。選擇**選項22**。

要保護執行緒轉儲，請登入到ISE節點的CLI，運行**application configure ise** 命令，選擇**選項23**。**執行緒轉儲包含在支援捆綁包中，或可以通過ISE CLI使用show logging application appserver/catalina.out** 命令跟蹤。

驗證和排除監控問題

ISE的監控和故障排除(MnT)功能是ISE架構的主要模組之一，它提供監控、報告和警報功能。

ISE顯示許多位置的監控資訊，包括：

- Cisco ISE首頁
- 上下文可見性檢視
- RADIUS即時日誌和即時會話
- 全域性搜尋
- 以威脅為中心的NAC即時日誌
- TACACS即時日誌

監控和故障排除類別中觀察到的一般問題：

1. Radius/ TACACS即時日誌不可用
2. 未提供即時會話
3. 運行狀況摘要不可用
4. 在MnT節點上出現的效能（高CPU/記憶體）問題)

要在MnT節點上啟用調試，以縮小問題範圍：

1. Cisco-mnt
2. 收集器
3. Cpm-mnt
4. 運行時記錄

除了偵錯中提到的元件之外，以下資訊也有助於進行疑難排解：

1. 活動會話是否也受到影響，還是僅影響活動日誌？
2. Radius或TACACS日誌是否受影響，或兩者都受影響？
3. 您是否看到MnT節點上的CPU使用率高或交換空間使用率高？
4. 您在MnT節點上看到多少緩衝區檔案。可在以下位置找到緩衝區檔案：/opt/CSCOcpm/mnt/data/collector。
5. 是否啟用記憶體和CPU保留（如果未啟用）。
6. 最近是否執行了MnT/config/session DB重置？
7. 您是否看到系統從PSN傳送到MnT節點？

如果您使用的是MnT的系統日誌服務，則為了進行故障排除，需要以下資訊：

1. 您是否使用安全系統日誌目標？如果不使用，請禁用它，因為已知它會造成執行緒死鎖，導致收集器停止運行？
2. 您是否使用安全系統日誌目標，請確保在管理 — >日誌記錄 — >遠端日誌記錄目標 — >安全系統日誌收集器1和2下正確設定證書對映
3. 驗證日誌記錄類別是否正確（建議刪除未使用/不需要的日誌記錄類別 — 這樣可以減少MnT節點上的負載）設定，並且日誌記錄目標設定正確。
4. 檢查支援捆綁包中的awrrep*.html檔案，瞭解並獲取有關哪個元件傳送更頻繁的系統日誌的提示。例如，如果通過插入或更新查詢看到TACACS表，我們可以檢查收集器日誌以相互關聯以瞭解哪些系統日誌傳送得更頻繁

如果問題與MnT節點上的效能有關，我們需要以下資訊：

1.MnT節點的ISE CLI的tech top輸出。

2.如果CPU使用率高，您是否也看到記憶體高或交換空間利用率高？

3.支援捆綁包，堆轉儲和執行緒轉儲受到保護。

參考

- 思科身份服務引擎管理員指南3.3版
- 在ISE上排除故障並啟用調試

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。