了解ISE服务、用途和故障排除

目录

简介

本文档介绍ISE服务、用途和故障排除。

先决条件

要求

思科建议您了解思科身份服务引擎。

使用的组件

本文档不限于思科身份服务引擎的任何特定软件和硬件版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

思科身份服务引擎(ISE)是一个全面的解决方案，旨在通过集中式策略管理、身份验证、授权和记帐(AAA)提供高级网络安全。 它使组织能够管理用户、设备和应用的网络访问，同时确保安全性、合规性和无缝的用户体验。

为实现这些目标，思科ISE利用一系列服务，每个服务负责使系统高效运行的特定任务。这些服务协同工作，可确保安全网络访问、强大的策略实施、详细的日志记录、与外部系统的无缝集成，以

及有效的设备分析。

ISE中的每项服务在维护解决方案的完整性和可用性方面发挥着至关重要的作用。有些服务处理核心功能，如数据库管理和身份验证，而有些服务则启用高级功能，如设备分析、证书管理和监控。

本文概述了思科ISE中的各种服务，说明其用途、重要性以及如果遇到问题的潜在故障排除步骤。无论您是管理员还是网络安全专业人员，了解这些服务都有助于确保您的ISE部署平稳安全运行。

了解ISE服务并进行故障排除

ISE使用屏幕截图中提到的服务来支持其功能。通过ISE节点的CLI使用show application status ise命令验证ISE中可用的状态或服务。以下是显示ISE上的状态或可用服务的示例输出。

```
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中提供的服务。

现在，详细了解每项服务。

数据库监听程序

数据库侦听程序服务是帮助管理ISE和数据库服务器之间通信的关键组件。它侦听和处理与数据库相关的请求，确保ISE系统可以读取和写入其基础数据库。

关于ISE中的数据库侦听程序服务的要点

1. 通信接口:它充当ISE和数据库服务器之间的通信网桥，允许系统检索和存储用户凭证、会话信息、网络策略等数据。

2. 外部数据库支持:可以将ISE配置为使用外部数据库（例如Oracle或Microsoft SQL Server）进行用户身份验证和策略存储。数据库侦听程序服务确保ISE可以安全高效地连接到此外部数据库并与之交互。

3. 数据处理:服务侦听来自ISE系统的数据库查询，然后将它们转换为外部数据库上的相应操作。它可以处理插入、更新或删除记录等请求，也可以从数据库中检索信息。

4. 数据库运行状况监控：除了提供通信通道外，它还有助于确保与外部数据库的连接稳定且正常运行。如果连接失败，ISE会根据配置回退到本地存储或进入降级模式。

数据库服务器

数据库服务器服务负责管理系统使用的数据的存储和检索。处理与底层数据库的交互，ISE使用该数据库存储配置、策略信息、用户数据、身份验证日志、设备配置文件和其他必要信息。

关于ISE中数据库服务器服务的要点

1.内部数据存储:数据库服务器服务主要管理ISE用于本地存储操作数据的内部嵌入式数据库。这包括身份验证和授权记录、用户配置文件、网络访问策略、设备和终端信息、会话信息等数据。

2.嵌入式数据库:在大多数思科ISE部署中，系统使用嵌入式PostgreSQL数据库进行本地存储。数据库服务器服务可确保此数据库顺利运行，并处理与其中存储的数据相关的所有查询、更新和管理任务。

3.数据库完整性:该服务确保所有事务都得到正确处理，并确保数据库的完整性。它处理诸如锁定记录、管理数据库连接和执行数据库查询等任务。

验证数据库监听程序和数据库服务器服务是否正在初始化或不运行，并对其进行故障排除

数据库监听程序和数据库服务器是必须一起运行才能使所有其他服务正常运行的基本服务。如果这些服务未在运行或在初始化期间停滞不前，这些故障排除步骤将有助于恢复。

1.使用application stop ise和application start ise命令重新启动ISE服务。

2.如果这是一个VM节点，从VM重新启动节点必须有助于恢复服务。

3.如果节点是物理节点，从CIMC重新启动/重新加载节点必须有助于恢复服务。

4.如果数据库损坏，请联系Cisco TAC进行进一步的故障排除。

当数据库中存在差异或数据库无法正确初始化时，数据库监听程序和数据库服务器通常关闭或无法启动。在这些情况下，使用application reset-config ise命令执行应用程序重置必须有助于数据库的恢复和全新启动。运行application reset-config ise命令将删除配置和证书，但会保留IP地址和域名详细信息。在将此命令应用于部署中的任何节点之前，建议与Cisco TAC联系以获取详细信息，并了解潜在影响。

应用服务器

应用服务器是负责运行和管理ISE平台核心功能和服务的关键组件。它托管允许ISE在网络访问控制、身份验证、授权、记账和策略管理中履行其角色的业务逻辑、用户界面和服务。

关于ISE中应用服务器服务的要点

1.用户界面(UI):应用服务器服务负责为ISE呈现基于Web的用户界面(UI)。这样，管理员可以配置和管理策略、查看日志和报告，以及与ISE的其他功能交互。

2.服务管理:它负责处理ISE提供的不同服务，包括策略管理、管理任务以及与分布式部署中的其他ISE节点的通信。

3.集中处理:应用服务器服务在ISE架构中扮演着核心角色，提供能够理解策略、身份验证请求以及来自网络设备、目录和外部服务的数据的逻辑。

应用程序服务器的验证正在初始化或未运行

应用服务器依赖于少量的Web应用，如证书、资源、部署、许可。当任何Web应用程序无法初始化时，应用程序服务器将停滞在初始化状态。根据节点上的配置数据，应用服务器从**Not running → Initializing → Running**状态大约需要15至35分钟。

1. 确保ISE的管理员证书在所有节点的部署中有效且处于活动状态。
2. 确保部署中的所有节点与主管理节点同步。
3. 如果节点是VM，请确保将建议的资源分配给该节点。

在ISE节点的CLI中使用**show application status ise**命令验证应用服务器的状态。大部分与应用服务器相关的日志位于

Catalina.Out和Localhost.log文件。

如果满足上述条件，并且应用服务器仍处于初始化状态，请从ISE的CLI/GUI保护支持捆绑包。使用application stop ise和application start ise命令恢复/重新启动服务。

Profiler数据库

Profiler数据库是一个专用数据库，用于存储有关网络设备、终端以及由Profiler服务发现的设备配置文件的信息。Profiler是ISE的重要组件，它根据网络特征和行为自动识别网络设备（如计算机、智能手机、打印机、IoT设备等）并对其进行分类。

关于ISE中的分析器数据库服务的要点

1.设备分析:分析器数据库服务的主要功能是支持分析过程。ISE使用此服务存储分析期间收集的信息，例如：

- 设备类型(例如：智能手机、笔记本电脑、打印机、物联网设备)
- 设备操作系统(例如：Windows®、macOS®、Cisco IOS®、Android®)
- 设备制造商
- 有助于设备分类的网络行为或模式

2.分析器信息:它存储分析器属性，例如设备硬件和软件配置文件，用于使设备与预定义策略相匹配。此信息还用于根据设备的配置文件将设备动态分配到正确的网络访问策略或VLAN。

3.分析过程:分析过程通常基于：

- 活动分析:ISE主动查询网络上的设备以获取信息。
- 被动分析:ISE从网络流量（例如DHCP请求、RADIUS属性、HTTP报头和其他网络协议）被动收集数据以确定设备类型。

验证**ISE分析服**务并对其进行故障排除

1.从ISE CLI运行show application status ise命令以验证分析器数据库服务正在运行。

2.从主管理节点的GUI中，导航到管理>部署>选择节点。单击Edit并验证会话服务和分析服务是否已启用。

3.现在，导航到管理>部署>选择节点。转到Profiler配置，并验证是否已启用保护终端数据所需的探测器。

4.导航到管理>系统>分析，并验证为CoA配置的分析器设置。

5.从情景可视性>端点 >选择端点并验证由不同的端点探测功能收集的属性。

用于故障排除分析问题的有用调试：

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

ISE索引引擎

索引引擎是一项服务，负责高效地搜索、索引和检索ISE数据库中存储的数据。它增强了ISE的性能和可扩展性，特别是在处理大量数据并提供对身份验证、授权、监控和报告任务所需信息的快速访问时。

关于ISE中的ISE索引引擎的要点

1.数据索引:ISE索引引擎为ISE中存储的各种类型的数据（例如身份验证日志、会话日志、策略命中

、分析数据和网络访问记录）创建索引。索引有助于以一种使搜索和查询更加高效的方式组织此数据。

2.日志管理和报告:此服务通过提高报告和日志查询的性能在日志管理中起到关键作用。例如，当搜索特定的身份验证事件时，索引引擎可以更快地检索所需的记录，这对安全监控和合规性报告至关重要。

3.数据检索:索引引擎还负责确保ISE可以在需要时从其底层数据库中高效地检索索引数据。这允许ISE对来自用户界面、外部工具或API的查询提供快速响应。

验证ISE索引引擎未运行或未初始化

1. 使用**nslookup <FQDN / IP address of the ISE node >** 命令通过CLI验证正向和反向DNS查找是否工作或集群中的所有节点。
2. 验证ISE管理员证书对集群中的所有节点有效且处于活动状态。
3. 使用**show ntp**命令，通过CLI验证NTP是否工作以及是否与ISE节点同步。

环境可视性使用索引引擎，而环境可视性需要启动并运行索引引擎才能发挥作用。有助于索引引擎故障排除的有用日志包括**ADE.log**文件，可以在问题期间使用**show logging system ade/ADE.log tail**命令从支持捆绑包保护这些文件或通过CLI对其进行详细保护。

AD连接器

AD连接器(Active Directory Connector)是一项允许ISE与Microsoft Active Directory(AD)集成的服务，使ISE能够根据用户的AD凭证和组成员身份对用户进行身份验证、授权和管理。AD连接器充当ISE和Active Directory之间的桥梁，允许ISE利用AD进行网络访问控制(NAC)和策略实施。

ISE中AD连接器服务的关键功能

1.与Active Directory集成:AD连接器服务充当ISE和Active Directory之间的网桥。它允许ISE安全连接到AD，使ISE能够将AD用作集中身份库进行用户身份验证和策略实施。

2. 同步:AD连接器服务支持将用户和组数据从Active Directory同步到ISE。这可以确保ISE拥有有关用户和组的最新信息，这些信息对于准确策略实施至关重要。

3.安全通信:AD连接器服务在ISE和Active Directory之间建立安全通信通道，通常使用协议（如LDAP over SSL [LDAPS]）以确保身份验证和查询过程中的数据隐私和完整性。

4.多个Active Directory域支持:该服务可以支持与多个Active Directory域的连接。这在大型或多域环境中尤其有用，在这些环境中，ISE需要对来自不同AD林或域的用户进行身份验证。

5.用户和组查找:它使ISE能够查询AD的用户和组信息。这可能包括用户名、组成员身份和其他可用于实施网络访问策略的用户属性等详细信息。例如，可以根据用户AD组成员身份应用网络访问策略(例如：向不同组中的用户授予不同的访问级别)。

1.验证NTP是否与节点同步，并且AD和ISE之间的时间差必须小于5分钟。

2.验证DNS服务器是否可以解析与AD相关的FQDN和域。

3.定位至**操作**>报告>报告>诊断> **AD**连接器操作,验证与AD相关的事件或报告。

用于故障排除的有用日志是**ad_agent.log**，其中包含运行时组件的调试日志。

M&T会话数据库

M&T会话数据库（监控和故障排除会话数据库）在存储和管理网络访问事件的会话相关数据方面起着关键作用。M&T会话数据库保存有关活动会话的信息，包括用户身份验证、设备连接和网络访问事件，这对于监控、故障排除和分析网络活动至关重要。

ISE中M&T会话数据库服务的关键功能

1.会话数据存储:M&T Session Database服务负责存储和索引网络上有关用户和设备会话的数据。这包括会话开始和结束时间、身份验证结果、用户或设备身份和相关策略（例如角色分配或VLAN分配）。 数据还包括详细说明会话生命周期的RADIUS记帐信息，包括初始身份验证和跟踪会话事件的任何记帐消息。

2.实时数据和历史数据:该服务提供对实时会话数据（活动会话）和历史会话数据（过去会话）的访问。 这样，管理员不仅能够监控持续的用户访问，还可以查看过去的会话日志，以调查问题或验证访问事件。实时会话监控有助于确保网络中当前没有未经授权的设备。

3.加强监测:提供对用户和设备活动的见解，包括应用于其会话的策略，有助于检测潜在的安全问题或未经授权的访问。

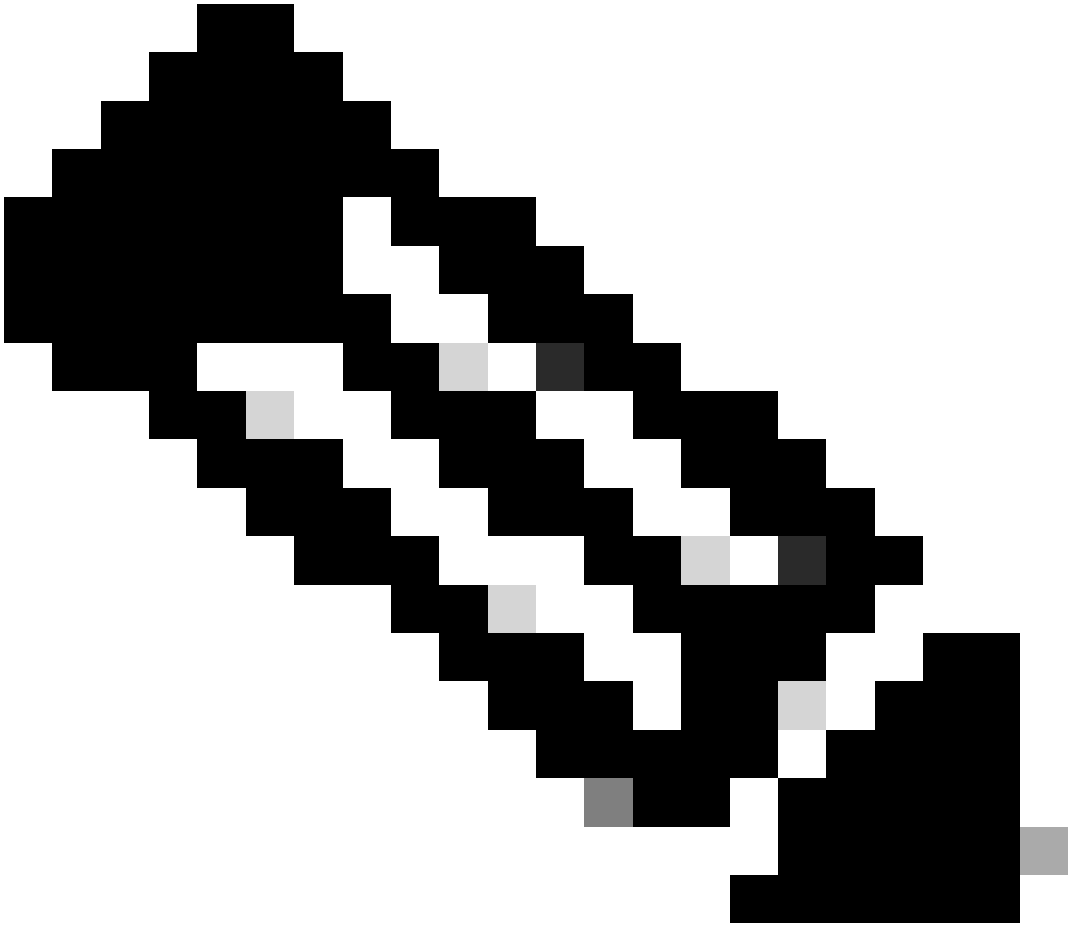
4.审计和报告:通过存储网络访问事件的历史记录和提供数据供监管报告来简化合规性审计和报告。

在ISE中验证**M&T**会话数据库并排除故障

1.验证节点是否分配了建议的资源。

2.从ISE CLI**保护show tech-support**，以进一步验证问题。

3.通过在中通过**ISE** CLI运行**application configure ise**命令并选择选项**1**，重置M&T会话数据库。



注意：只有在验证部署中的潜在影响之后，才能重置M&T数据库。联系思科TAC进行进一步验证。

已知缺陷

思科漏洞ID ·32364

M&T日志处理器

M&T日志处理器（监控和故障排除日志处理器）是一个负责收集、处理和管理由ISE内各种服务生成的日志数据的组件。它是监控和故障排除(M&T)框架的关键部分，可帮助管理员监控和排除ISE系统中的网络访问事件、身份验证尝试、策略实施和其他活动故障。M&T日志处理器专门处理日志条目的处理，确保ISE可以存储、分析和提供报告、审核和故障排除所需的信息。

ISE中M&T日志处理器服务的主要功能

1.日志收集和处理:M&T日志处理器服务收集和处理由各种ISE组件生成的日志，例如身份验证请求

、授权决策、记帐消息和策略实施活动。这些日志包含有关用户、设备和网络访问尝试的详细信息，例如时间戳、用户ID、设备类型、应用的策略、访问请求成功或失败以及失败原因。

2.报告和合规性:此服务处理的日志对于合规性报告至关重要。许多法规要求组织保留用户访问和安全事件日志。M&T日志处理器服务确保所有相关日志都得到处理并可用于合规性审核。它有助于根据日志数据（例如用户访问日志、身份验证成功/失败率或策略实施日志）生成详细报告。

在ISE中验证和排除**M&T日志**处理器服务故障

1.确保根据《思科安装指南》使用建议的资源部署ISE节点。

2.要验证问题，请通过ISE CLI运行**show logging system ade/ADE.log tail**命令，以了解相关异常/错误。

已知缺陷

思科漏洞ID ·15130

证书颁发机构服务

证书颁发机构(CA)服务是帮助管理数字证书以保护通信以及验证设备、用户和网络服务的关键组件。数字证书对于建立可信连接并确保客户端（计算机、智能手机、网络设备）和网络基础设施组件（交换机、无线接入点、VPN网关）之间的安全通信至关重要。 思科ISE中的CA服务与X.509证书配合使用，这些证书用于多种网络安全用途，包括802.1X身份验证、VPN访问、安全通信和SSL/TLS加密。

ISE中证书颁发机构服务的关键功能

1.证书管理:证书颁发机构服务负责处理ISE内数字证书的创建、颁发、管理和续订。这些证书用于网络中的各种身份验证协议和加密目的。它可以充当内部证书颁发机构，也可以与外部CA集成(例如：Microsoft AD CS、公共CA（例如VeriSign或DigiCert）以颁发证书。

二、发证:对于需要EAP-TLS或类似基于证书的身份验证方法的环境，ISE可为网络访问设备(NAD)、用户或终端颁发证书。ISE可以自动生成和部署用于验证设备和用户的证书，也可以从外部CA请求证书。

3.证书注册:CA服务支持终端（例如笔记本电脑、电话和其他网络设备）的证书注册，这些终端需要使用证书对网络进行身份验证。ISE使用SCEP（简单证书注册协议）或ACME（自动证书管理环境）等协议促进设备的证书注册。

4.证书续期:该服务可自动续订设备和用户的过期证书。它可确保证书始终有效且保持最新，防止因证书过期而导致服务中断。

5.与外部证书颁发机构集成：虽然ISE可以充当自己的CA，但更常见的是与外部CA集成(例如：Microsoft Active Directory证书服务)。 CA服务可以管理ISE和外部CA之间的交互，根据需要为用户、设备和网络资源请求证书。

EST服务

通过安全传输(EST)服务进行注册是一种协议，用于在基于证书的身份验证环境中向网络设备和用户安全地颁发数字证书。EST是一种证书注册协议，允许设备以安全且自动化的方式向证书颁发机构(CA)请求证书。EST服务对于设备身份验证尤其有用，例如在802.1X环境、VPN连接或BYOD（自带设备）场景中，设备需要使用证书对网络进行身份验证。

ISE中EST服务的主要功能

1.证书注册:EST服务负责为需要证书进行身份验证的设备（如交换机、接入点或终端）启用安全证书注册。注册通过安全传输（通常为HTTPS）完成，确保流程得到加密并保护免受未经授权的访问。

2.证书撤销和续期:注册证书后，EST服务还负责管理证书撤销或续订。例如，设备需要在当前证书过期时请求新证书，EST可以帮助自动完成此过程。

3.改进网络访问控制:通过使设备能够使用证书进行身份验证，EST服务增强了网络的安全状态，特别是在使用802.1X身份验证的环境中。

验证证书颁发机构和EST服务未运行/正在初始化

1. 导航到**管理>System >**证书>证书颁发机构>内部**CA**设置。确保CA、EST和OCSP Responder Status已排序并启用。
2. 有助于故障排除的有用调试有set 、 provisioning 、 ca-service和ca-service-cert。 请参阅**toise-psc.log** 、 **catalina.out** 、 **caservice.log**和error.log文件。
3. 验证ISE根CA和ISE消息证书在部署中有效。如果需要续订ISE根CA，请导航到**管理>**证书>证书签名请求>生成证书签名请求，选择usage as **ISE根CA**。单击renew **ISE Root CA**。

SXP引擎服务

SXP引擎服务负责使用安全组标记(SGT)和安全组交换协议(SXP)管理和促进ISE与网络设备之间的通信。 它在支持TrustSec策略方面发挥关键作用，TrustSec策略用于根据设备的安全组实施网络访问控制，而不只是实施IP地址或MAC地址。ISE中的SXP引擎主要用于交换安全组信息，这有助于根据用户或设备身份、应用程序和位置实施策略。它使设备能够共享安全组标记(SGT)，用于跨网络设备（例如路由器和交换机）实施安全策略。

ISE中SXP引擎服务的关键功能

1.与TrustSec集成:SXP通常部署在利用Cisco TrustSec的环境中，Cisco TrustSec解决方案可在有线和无线网络中实施一致的安全策略。SXP引擎便于设备之间的SGT通信，允许基于设备或用户的安全情景进行动态策略实施。

2.安全组标记(SGT):TrustSec策略实施的核心围绕SGT。这些标记用于对网络流量进行分类，SXP协议帮助共享这些标记到特定用户或设备的映射。这允许对网络访问和流量进行精细的、策略驱动的控制。

ISE中SXP引擎服务的验证和故障排除

1.默认情况下，ISE中禁用SXP引擎服务。要启用它，请转到**ISE GUI > Administration > Deployment，**选择节点。选中启用**SXP服**务框，然后选择接口。然后，使用**show application status ise**命令从ISE CLI验

证SXP引擎服务的状态。

2.如果存在网络通信问题，通过在CLI中使用show interface命令验证分配给SXP引擎的接口具有有效的IP地址，并确保网络中允许IP子网。

3.检查RADIUS实时日志以验证ISE上的SXP连接事件。

4.在ISE节点上启用SXP组件以调试和捕获与SXP相关的日志和异常。

TC-NAC服务

TC-NAC服务（TrustSec网络访问控制）是一个促进在网络设备上实施TrustSec策略的组件，确保访问控制基于安全组标记(SGT)而不是传统IP或MAC地址。

反过来，TrustSec是由思科开发的框架，它根据设备角色、用户或情景，而不是使用VLAN或IP地址等传统机制，在整个网络中实施安全策略。通过将设备分组到不同的安全组并使用SGT进行标记，可提供更精细和动态的网络访问控制。

ISE中TC-NAC服务的主要功能

1.与第三方NAC系统集成:TC-NAC服务使ISE能够与第三方网络访问控制解决方案进行通信和交互。对于已部署现有NAC基础设施但希望将其与思科ISE集成以改善功能、利用其他安全策略或利用思科的其他网络安全功能的组织，此功能非常有用。

2.提供无缝的策略实施:当与第三方NAC解决方案集成时，ISE可以接管策略实施和决策的某些方面。这样可以建立更统一的策略框架，确保思科和非思科NAC系统应用的策略在整个网络中保持一致。

3.支持传统NAC系统:TC-NAC服务帮助具有传统NAC系统的组织，允许它们继续使用这些系统，同时采用Cisco ISE为其增强的安全功能。ISE可以与旧的NAC解决方案集成并延长其生命周期，同时提供访问控制、安全和合规性实施。

4.促进第三方NAC供应商通信:此服务允许ISE促进与使用专有协议或标准的第三方NAC解决方案的通信。ISE可以通过行业标准协议（如RADIUS、TACACS+或SNMP）或自定义API与第三方NAC系统交互，具体取决于所使用的特定NAC解决方案。

在ISE中验证**TC-NAC服**务并对其进行故障排除

1.导航到**管理>部署> PSN**节点>启用以威胁为中心的**NAC**，以验证是否已启用以威胁为中心的NAC。

2.如果问题出在SourceFire FireAMP适配器上，请验证您的网络中是否允许端口**443**。

3.从**操作 > 以威**胁为中心的**NAC**实时日志验证终端会话详细信息。

由以威胁为中心的NAC触发的警报：

- 适配器无法访问(系统日志ID:91002):表示无法访问适配器。
- 适配器连接失败(系统日志ID:91018):表示适配器可访问，但适配器和源服务器之间的连接已关

闭。

- 适配器因错误而停止(系统日志ID:91006):如果适配器未处于所需状态，则会触发此警报。如果显示此警报，请检查适配器配置和服务器连接。有关详细信息，请参阅适配器日志。
- 适配器错误(系统日志ID:91009):表示Qualys适配器无法与Qualys站点建立连接或从Qualys站点下载信息。

用于排除TC-NAC问题的有用调试：

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

PassiveID WMI服务

PassiveID WMI服务是允许ISE执行设备分析的服务，使用Windows Management Instrumentation(WMI)作为被动机制来识别和分析网络中的终端。它在设备分析方面发挥着关键作用，尤其是在运行Windows OS的设备需要准确识别才能进行网络访问控制和策略实施的环境中。

ISE中PassiveID WMI服务的关键功能

1.设备身份收集:PassiveID WMI服务允许ISE使用Windows Management Instrumentation(WMI)从Windows设备被动收集身份信息。 它收集系统详细信息，例如设备的主机名、操作系统版本以及其他相关属性，而无需设备主动参与。

2.与ISE策略集成:由PassiveID WMI服务收集的信息已集成到ISE策略框架中。它有助于根据设备属性（如类型、操作系统和安全标准合规性）动态应用策略。

验证PassiveID WMI服务并对其进行故障排除

一个高度安全且精确的来源，也是最常见的用来接收用户信息的来源。作为探测器，AD可与WMI技术配合使用来提供经过身份验证的用户身份。此外，AD本身（而不是探测器）用作源系统（提供商），其他探测器也可以从中检索用户数据。

进行故障排除所需的有用调试和信息。将这些属性设置为PassiveID WMI问题的调试级别：

- PassiveID(passiveid*)
- runtime-logging(prrt-server.log)
- Active Directory(ad)_agent.log) — 跟踪级别
- collector(collector.log)(在PassiveID、MnT节点上和在主动pxGrid节点上（如果会话已发布）
- pxGrid(pxgrid/)（在辅助MnT和活动pxGrid节点上，如果会话已发布）

排除PassiveID WMI故障所需的信息：

1. 以前是否工作正常？最近完成的任何更改。 （与升级类似，在ISE上安装补丁/在DC上升级）

2. 测试连接是否工作正常（在集成之前，请检查测试连接）
3. 有关用于加入AD的用户名和用于WMI的用户名的详细信息。（无论管理员帐户还是非管理员帐户）
4. 检查是否记录了DC中的事件(4768、4770)。（来自DC的事件查看器日志）
5. 捕获日志：设置被动ID和运行时记录的调试级别，然后对该DC、AD执行config wmi — 具有时间戳的跟踪级别。

PassiveID系统日志服务

PassiveID Syslog服务是使PassiveID分析功能能够收集和处理环境中网络设备的syslog消息的一项服务。这些系统日志消息包含有关连接到网络的终端的重要信息，ISE使用这些信息分析这些设备以进行网络访问控制和策略实施。

被动ID系统日志服务的关键功能

1.被动身份验证：Passive ID Syslog服务允许Cisco ISE通过从指示用户和设备活动的网络设备（如交换机或路由器）收集系统日志消息来被动验证用户和设备。在传统主动身份验证方法（如802.1X）不适用或不可行的情况下，此功能非常有用。

2.事件记录:被动ID系统日志服务依靠系统日志协议从跟踪用户访问和网络行为的网络设备接收日志。这些日志中包含的信息可能包括设备登录尝试、接入点和接口详细信息等内容，从而帮助ISE被动识别设备或用户。

PassiveID API服务

PassiveID API服务是一项支持与需要有关连接到网络的设备或用户身份信息的系统集成的服务。它通常用于网络管理员希望执行基于身份的策略和操作而不要求每个设备使用主动网络身份验证协议（如802.1X）的环境。

被动ID API服务的关键功能

1.与外部系统的集成：被动ID API允许ISE从第三方系统或网络设备（例如交换机、路由器、防火墙或可以生成身份相关事件的任何系统）接收身份信息。 这些外部系统可以发送信息，例如系统日志消息、身份验证日志或其他相关数据，以帮助ISE被动识别用户或设备。

2.被动身份验证:被动ID API服务用于通过收集身份数据来被动验证用户和设备，无需主动身份验证(例如：无需802.1X、MAB或Web身份验证)。 例如，它可以捕获来自网络设备、Active Directory日志或安全设备的信息，并使用该信息识别用户或设备。

3.映射身份信息:被动ID API可用于将身份数据映射到特定安全策略。此信息用于将安全组标记(SGT)或角色动态分配到用户和设备，然后影响网络访问控制（如分段和防火墙策略）的实施。

PassiveID代理服务

PassiveID Agent Service是一项通过使用安装在终端（例如计算机、笔记本电脑、移动设备等）上的PassiveID Agent启用设备分析的服务。 PassiveID Agent允许ISE通过侦听来自终端的流量来收集有关网络上设备的分析信息，而无需主动扫描或直接与设备交互。

被动ID代理服务的主要功能

1.被动用户和设备识别：被动ID代理服务负责被动收集身份相关信息（通常是从网络设备或终端），并将此数据发送到ISE。此服务允许ISE根据用户和设备的活动或特征进行身份验证和识别，无需从设备进行主动身份验证(例如：不提供802.1X凭证)。

2.与其他思科组件的集成:被动ID代理与思科网络设备（如交换机、无线控制器和接入点）紧密合作，从网络流量、系统日志或其他管理系统中收集身份相关信息。它还可以与Cisco TrustSec和思科身份服务集成，以将此数据映射到特定安全组标记(SGT)或其他基于身份的策略。

3.情景网络访问控制:被动ID代理将此信息发送到思科ISE，思科ISE然后根据用户或设备的身份和情景应用适当的访问控制策略。这可能包括：

- 基于角色的访问控制。
- 动态VLAN分配。
- 网络分段。
- 根据用户角色或设备安全状态实施安全策略。

PassiveID端点服务

PassiveID Endpoint Service是一项服务，负责基于PassiveID技术识别和分析网络上的终端（设备）。此服务可帮助ISE收集、处理和分类有关连接到网络的设备的信息，而无需与终端本身进行主动交互。PassiveID Endpoint Service在分析分析、网络访问控制和安全策略实施方面起着关键作用。

PassiveID端点服务的关键功能

1.被动用户和设备识别：PassiveID Endpoint Service允许Cisco ISE利用网络活动或系统日志中的信息被动地识别和验证网络上的设备。这包括根据用户和设备的网络行为或特征(例如MAC地址、IP地址或来自外部身份库（例如Active Directory [AD]）的登录信息)识别用户和设备。

2.从终端收集数据:终端服务从不同来源收集各种类型的终端特定数据：

- 用户从Active Directory等外部身份库或其他目录登录信息。
- 设备特征，例如IP地址、MAC地址和设备类型(例如：无论设备是Windows PC、移动电话还是IoT设备)。
- 终端网络活动，例如DHCP请求、ARP请求和其他网络层通信。

PassiveID SPAN服务

PassiveID SPAN服务是一项利用网络设备上的SPAN（交换端口分析器）端口镜像来捕获和分析网络流量以进行终端分析的服务。此服务可帮助ISE通过分析网络上的终端（设备）的网络通信模式，从而被动收集有关终端的信息，而无需在设备上安装主动探测或代理。

PassiveID SPAN服务的关键功能

1.从SPAN流量进行被动身份收集:PassiveID SPAN服务允许ISE根据通过交换机上的SPAN端口镜

像或复制的网络流量收集身份数据。SPAN端口通常用于网络监控，通过镜像来自其他端口或VLAN的网络流量进行监控。通过捕获此流量，ISE可以被动收集身份信息，例如：

- 设备的MAC地址。
- 与设备关联的IP地址。
- DHCP请求或从捕获的流量获取其他身份相关信息。
- 来自网络设备（例如交换机或无线控制器）的身份验证日志。

2.捕获用户和设备身份信息:SPAN服务基本上监听通过网络传输的流量，并识别来自网络数据包的关键身份信息，而无需直接与设备交互。这可能包括以下数据：

- 用户通过协议(如EAP（可扩展身份验证协议）)进行身份验证时的身份。
- 基于MAC地址和IP地址的设备标识。
- 根据观察到的流量模式和事件确定设备角色和行为。

PassiveID Stack（PassiveID SPAN服务、PassiveID Syslog服务、PassiveID Endpoint服务、PassiveID Agent、PassiveID API服务）的验证和故障排除

1. PassiveID堆栈是一个提供程序列表，默认情况下PassiveID堆栈中的所有服务都处于禁用状态。导航到ISE GUI > Administration > Deployment > Select the node,Enable Passive Identity Service，然后单击Save。要验证PassiveID堆栈服务状态，请登录到ISE节点的CLI并运行show application status ise命令。

2.如果被动ID代理出现问题，请检查代理的FQDN是否可以从ISE节点解析。为此，请登录ISE CLI并运行nslookup < FQDN of Agent configured > 命令。

3.确保ISE索引引擎处于活动状态，并且在ISE中配置的DNS或名称服务器正在解析反向和转发DNS查找。

4.要确保与系统日志提供程序进行无缝通信，请检查UDP端口40514和TCP端口11468在您的网络中处于打开状态。

5.要在节点上配置SPAN提供程序，请确保已启用ISE被动身份服务。通过在ISE CLI中使用show interface命令，验证要在SPAN提供程序上配置的接口在ISE中可用。

要根据被动ID提供程序检查日志，您需要查看passiveid-syslog.log、passiveid-agent.log、passiveid-api.log、passiveid-endpoint.log、passiveid-span.log。可以从ISE节点的支持捆绑包保护上述日志。

DHCP服务器(dhcpd)

DHCP服务器(dhcpd)服务是为网络设备提供动态主机配置协议(DHCP)功能的服务。它主要用于将IP地址分配给尝试连接到网络的设备（终端）。在ISE中，DHCP服务器在向连接网络的终端提供IP地址时起着关键作用。该服务还可以提供其他配置信息，例如DNS服务器、默认网关和其他网络设置。

ISE中DHCP服务器(dhcpd)服务的关键功能

1.动态IP地址分配：ISE中的dhcpd服务用作DHCP服务器，为连接到网络的设备请求IP地址提供IP地址分配。在设备动态加入网络的场景中，例如在BYOD（自带设备）环境中，或者当设备配置为自动获取其IP地址时，这一点非常重要。

2.基于配置文件的DHCP:dhcpd服务可以根据设备的配置文件分配IP地址。如果ISE已分析设备(例如：如果确定它是智能手机、笔记本电脑或IoT设备)，则可以根据设备类型或角色分配适当的IP地址或应用其他设置。

3.支持DHCP中继：ISE可以充当DHCP中继代理，如果ISE不处理实际IP地址分配，则将DHCP请求从设备转发到外部DHCP服务器。在这种情况下，dhcpd服务可以将来自设备的请求转发到中央DHCP服务器，而ISE继续应用网络策略和访问控制。

检验**DHCP**服务器**(dhcpd)**并排除故障

1.联系思科TAC验证DHCP服务器软件包是否已安装在ISE上。

2.登录到**ISE > rpm -qi dhcp的根**。

DNS服务器（已命名）

DNS服务器（命名）服务是允许ISE充当DNS（域名系统）服务器或DNS解析程序的服务。它主要负责将域名解析为IP地址，反之亦然，从而促进网络中设备之间的通信。

ISE中DNS服务器（命名）服务的关键功能

1. ISE通信的DNS解析:ISE中的命名服务有助于将域名解析为IP地址。当ISE需要使用域名而不是IP地址连接到其他网络设备或外部服务（例如Radius服务器、Active Directory或外部NTP服务器）时，这一点尤为重要。

- 例如，当ISE需要到达Radius服务器或外部目录服务（如Active Directory）时，它需要将该服务器的域名解析为IP地址。
- ISE查询系统上配置的DNS服务器以解析这些域名，确保通信顺畅。

2.外部服务的DNS解析:DNS服务使ISE能够连接到需要域名的外部服务。例如，ISE需要解析外部服务的名称，例如：

- 基于云的服务。
- NTP（网络时间协议）服务器。
- 证书颁发机构(CA)或LDAP服务器。

3.多域和冗余DNS服务器:ISE可以配置为使用多个DNS服务器以实现冗余。如果一个DNS服务器不可用，ISE可以回退到另一个DNS服务器，以确保持续运行和DNS解析。

验证**DNS**服务器（已命名）并排除故障

1.在ISE节点的CLI中，使用**ping <IP of DNS server / name server>** 命令，验证可以访问部署的名称服务器或DNS服务器。

2.通过ISE CLI使用**nslookup <FQDN / IP address of ISE nodes>**命令验证ISE FQDN的DNS解析。

ISE消息服务

ISE消息传送服务是一个组件，可促进ISE系统内各种服务和组件之间的异步通信。它在ISE的整体系统架构中起着至关重要的作用，使平台的不同部分能够发送和接收消息、管理任务并同步活动。

ISE消息传送服务的主要功能

1.进程间通信(IPC):ISE消息服务在启用各种ISE服务之间的进程间通信(IPC)方面发挥着关键作用。它确保不同的ISE模块和服务（如身份验证、授权和策略实施）能够以协调的方式交换数据和指令。

2.分布式环境支持:在大型或分布式ISE部署中（例如多节点或高可用性配置），消息服务有助于促进各种ISE节点之间的通信。这可确保数据（例如身份验证请求、用户会话和策略更新）在ISE系统中的不同节点之间正确同步。

3.策略和配置同步:消息服务参与同步ISE节点之间的配置和策略。当对主节点进行配置更改时，该服务会确保这些更改传播到系统中的辅助节点或备份节点。这对于保持一致性和确保跨不同位置或分布式ISE节点应用的网络访问策略保持同步至关重要。

验证ISE消息服务未运行或正在初始化

1.验证防火墙中是否未阻止端口TCP 8671，因为该端口用于ISE设备之间的节点间通信。

2.验证队列链接错误，如果存在，请更新ISE消息传送和ISE根CA证书，因为通常由于内部证书损坏问题而发生队列链接错误。要解决队列链路错误，请通过参考以下文章更新ISE消息传送和ISE根CA证书：ISE — 队列链路错误

3.从GUI -> Administration -> Certificates -> Select ISE Messaging Certificate。点击View以验证证书的状态。

用于排除ISE消息服务故障的有用日志是ade.log，该日志可在支持捆绑包中提供，也可以在问题期间使用show logging system ade/ADE.log tail命令通过CLI进行详细分析。

4.如果ADE.log日志显示rabbitmq:连接拒绝错误，请联系思科TAC从ISE根删除Rabbitmq模块的锁定。

ISE API网关数据库服务

ISE API网关数据库服务是一个组件，负责管理和处理与ISE系统内的API请求和响应相关的数据。它充当连接ISE API网关与ISE数据库的中间设备，确保自定义应用也可以通过服务管理的API调用更新或修改ISE中的数据（例如，调整访问策略或添加/删除用户）。

ISE API网关数据库服务的关键功能

1.对ISE数据的API访问:ISE API网关数据库服务充当网桥，允许外部应用通过ISE RESTful API与ISE数据库交互。这些API可用于检索或修改存储在ISE数据库中的数据，例如：

- 用户身份验证日志。

- 网络访问策略。
- 设备分析信息。
- 系统配置和设置。

2.启用外部系统集成:此服务在将ISE与外部系统集成时起着关键作用，例如：

- 外部身份验证服务器(LDAP、Active Directory、RADIUS)。
- 网络管理系统(NMS)。
- 安全信息和事件管理(SIEM)解决方案。
- 需要与ISE数据交互的自定义应用或服务。

通过提供API访问，API网关数据库服务允许这些外部系统查询ISE数据、向ISE发送更新或触发ISE内的特定操作以响应外部事件。

3.支持RESTful API通信:ISE显示旨在通过HTTP/HTTPS工作的RESTful API。API网关数据库服务负责管理API请求和响应流，确保请求经过身份验证和处理，并从ISE数据库返回适当的数据作为响应。

ISE API网关服务

ISE API网关服务是提供对ISE服务、数据和功能的RESTful API访问的关键组件。它充当ISE和外部系统之间的桥梁，允许这些系统以编程方式与ISE网络访问控制、策略实施、身份验证和其他服务进行交互。API网关使第三方应用、网络管理系统和自定义应用能够与Cisco ISE交互，无需手动干预或直接访问ISE用户界面。

ISE API网关服务的关键功能

1.启用对ISE的API访问：ISE API网关服务使外部系统能够使用RESTful API安全地访问思科ISE数据和策略并与之交互。这样可以对ISE功能（如身份验证、策略实施、会话管理等）进行编程访问。

2.提供计划控制:API网关服务允许对ISE功能进行编程控制。管理员和开发人员可以使用API:

- 检索或修改网络策略。
- 查询或管理用户会话和身份验证日志。
- 创建和管理网络访问控制规则。
- 访问或更新设备配置文件。

此控制可用于自动化或自定义工作流程协调，例如根据实时数据动态调整网络访问策略或将ISE集成到更广泛的安全自动化平台中。

3.监测和报告:API网关服务允许外部系统从操作ISE日志、会话历史记录和策略实施详细信息收集数据。这对于以下方面非常重要：

- 合规性报告。
- 安全监控。
- 事件响应。

API调用可用于提取日志、审核信息和事件，允许安全团队从集中控制面板或报告工具监控ISE活动

。

验证ISE API网关服务和ISE API网关数据库服务并排除故障

1.验证ISE节点的管理员证书是否有效且有效。导航到管理>证书>选择节点>选择管理员证书。点击View以验证ISE节点的管理员证书的状态。

2.将ise-api-gateway、api-gateway、apiservice组件设置为调试，并且可以使用以下命令跟踪日志：

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

ISE pxGrid直接服务

ISE pxGrid直接服务是支持ISE中的pxGrid（平台交换网格）功能的重要组件。pxGrid是一种思科技术，可促进思科网络安全解决方案与第三方应用、服务和设备之间的安全、标准化且可扩展的数据共享和集成。ISE pxGrid直接服务使ISE和其他与pxGrid兼容的系统之间能够直接通信，而无需中间设备或服务。

ISE pxGrid直接服务的关键功能

1.与第三方系统的直接集成:ISE pxGrid直接服务允许ISE直接与第三方网络安全系统集成，例如防火墙、路由器、NAC解决方案、SIEM平台和其他安全设备。它允许这些系统交换有关网络访问事件、安全事件和情景网络数据的信息。

2.情景共享:pxGrid的主要功能之一是共享情景信息（如设备身份、用户角色、安全状态和网络访问信息）。借助pxGrid直接服务，ISE可以直接与其他设备或应用共享此情景，而无需依赖RADIUS或TACACS+等传统方法。

3.简化通信:通过使用pxGrid，ISE可以使用标准化协议与第三方解决方案进行通信和交换信息。这简化了集成过程，因为系统不需要为每个单独的第三方解决方案进行自定义集成。

4.增强安全性和合规性:pxGrid直接服务还可通过确保网络生态系统中的所有系统都能够访问相同的有关用户、设备和安全策略的实时情景数据，来改善安全状况和合规性。这可确保在整个环境中更协调地实施网络安全策略。

验证**ISEPxgrid Direct**服务并对其进行故障排除

1.联系思科TAC以验证/tmp文件夹中是否存在**edda*.lock***。如果是，思科TAC会删除锁定并从根目录重新启动Pxgrid Direct服务。

2.将**PxGrid Direct**组件设置为在ISE节点中调试以进行故障排除。可以使用以下命令通过ISE支持捆绑包或ISE CLI保护日志：

show logging application pxgriddirect-service.log

show logging application pxgriddirect-connector.log

提到的日志提供了由Cisco ISE获取和接收的终端数据以及Pxgrid连接器的连接状态的信息。

分段策略服务

分段策略服务是一个关键组件，负责根据用户身份、设备状态或其他情景信息实施网络分段策略。它有助于控制用户和设备对特定网段的访问，确保只有授权用户或合规设备才能访问网络的某些部分。 网络分段对于减少网络攻击面、防止威胁横向移动以及确保合规性至关重要。ISE中的分段策略服务用于在网络中动态灵活地实施这些网络分段规则。

分段策略服务的主要功能

1.定义网段:ISE中的分段策略服务允许管理员根据用户或设备的特性定义各种网段（子网或VLAN）。例如：

- 安全状况不同的设备可以分配到不同的网段(例如：一个VLAN中的受信任设备和另一个VLAN中的不受信任设备)。
- 可以将不同部门或角色的用户分配给不同的网段，以实施最小权限并限制对敏感资源的访问。

2.动态分段:此服务支持动态网络分段，这意味着网段或VLAN可以根据实时情况更改。例如：

- 可以根据用户的角色或设备运行状况将其分配给特定VLAN。
- 被视为不合规或运行过时操作系统的设备可以移至隔离区或访客VLAN，直到其得到修复。

3.基于政策的执行:分段策略服务使用策略来决定设备或用户必须放入哪个分段。这些策略可以考虑各种因素，例如：

- 用户身份:基于用户角色或属性。
- 设备状态:设备的运行状况或合规性状态(例如：是否运行最新的防病毒软件？)。
- 地点：用户或设备在网络中的物理位置(例如：办公室、访客区域、远程访问)。
- 访问时间:发出访问请求时的一天中的时间或一周中的某一天。

4.安全策略实施:分段策略服务通过利用RADIUS和VLAN分配等行业标准，确保在网络设备（如交换机、路由器、防火墙）中一致地实施安全策略。这允许Cisco ISE与网络基础设施设备通信以实施所需的分段策略。

验证分段策略服务并对其进行故障排除

1.导航到工作中心> TrustSec >概述>控制面板，验证分段是否已正确配置。

2. Work Centers > TrustSec > Reports，选择TrustSec reports以验证分段策略服务状态和报告。

REST身份验证服务

REST身份验证服务是一项使用RESTful API提供身份验证功能的服务。它允许外部应用和系统通过使用标准REST协议通过HTTP(S)与ISE进行交互，从而对用户或设备进行身份验证。此服务允许将Cisco ISE身份验证功能与需要验证用户或设备但无法使用传统方法（如RADIUS或TACACS+）的第三方应用或系统无缝集成。

REST身份验证服务的关键功能

1. RESTful身份验证:REST身份验证服务通过REST API协议启用身份验证请求。这允许外部系统(例如：使用ISE作为身份验证服务器，但通过RESTful Web服务调用（而不是传统的身份验证协议，如RADIUS或TACACS+）对用户或设备进行身份验证。

2.与外部应用集成:此服务专为需要验证用户或设备但不使用传统身份验证方法（如RADIUS或TACACS+）的外部应用而设计。 相反，它们可以通过REST API与ISE交互，从而使ISE身份验证集成到基于Web的应用或云本机应用变得更加简单。

3.灵活且可扩展的身份验证:REST身份验证服务提供可扩展的身份验证方法，不仅限于网络设备或现场解决方案。云服务、移动应用和其他基于Web的平台可以通过查询ISE的凭证和策略对用户或设备进行身份验证。

4.易于应用:REST API提供标准化接口，与传统方法相比，更易于应用并与现代软件和应用集成。它提供JSON格式的响应，并使用GET、POST、PUT和DELETE等HTTP方法，使Web开发人员和集成ISE进行身份验证的系统更容易访问它。

Rest身份验证的验证和故障排除

1.要排除与Open API相关的问题，请将apiservice组件设置为debug。

2.要排除ERS API相关问题，请将ers组件设置为debug。

如果API服务GUI页面： https://{iseip}:{port}/api/swagger-ui/index.html或https://{iseip}:9060/ers/sdk可访问，表明API服务按预期运行。

有关API的详细信息，请参阅API文档。

SSE连接器

SSE连接器（安全软件定义边缘连接器）是一项将ISE与思科安全软件定义访问(SD-Access)解决方案集成的服务。SSE连接器允许ISE与思科DNA中心进行安全通信，从而在SD-Access环境中实现自动化网络策略、分段和边缘安全管理。

SSE连接器的主要功能

1.与第三方安全系统集成：SSE连接器促进思科ISE与第三方安全系统(如防火墙、入侵防御系统(IPS)、网络访问控制(NAC)解决方案，以及安全信息和事件管理(SIEM)系统的集成。它允许这些外部系统以安全方式从ISE发送或接收数据，可用于更动态的策略实施。

2.实时威胁情报:通过将ISE与其他安全系统连接，SSE连接器支持实时威胁情报的交换。此信息可能包括可疑活动、受感染的终端或其他安全系统检测到的恶意行为，从而允许ISE根据当前威胁级别或设备状态动态调整访问策略。

3.自动补救:由SSE连接器支持的集成可支持自动化补救工作流程。例如，如果系统被外部安全设备标记为已受危害，ISE可以自动实施阻止网络访问的策略，或将终端重定向到补救网段以进行进一步调查。

验证**SSE**连接器并排除故障

1.仅当在ISE中启用PassiveID服务时，才会启用SSE连接器。

2.debug中的sse-connector(connector.log)组件提供了有关SSE连接器相关消息的更多信息。

Hermes（pxGrid云代理）

Hermes（pxGrid云代理）是促进ISE与pxGrid（平台交换网格）生态系统在云环境中集成的组件。Hermes是基于云的代理，用于实现ISE与基于云的服务或平台之间的通信，支持pxGrid框架，用于跨不同网络和安全系统共享情景信息。

Hermes（pxGrid云代理）的主要特性和功能

1.云到现场集成：Hermes（pxGrid云代理）旨在促进基于云的服务与本地ISE基础设施之间的无缝集成。它将pxGrid的功能扩展到传统内部网络环境之外，实现跨基于云的应用和服务的安全数据交换和策略实施。

2.pxGrid生态系统支持:pxGrid是思科平台，可在各种网络安全解决方案间安全地共享情景和信息。Hermes充当pxGrid的云代理，实现ISE和各种基于云的服务之间的安全、实时通信。这种集成使内部环境和云环境之间的网络安全策略保持一致，从而更轻松地管理和实施安全性。

3.基于云的终端可视性:Hermes的一个核心优势是它提供对基于云的终端的可视性，类似于ISE如何提供内部终端的可视性。它可以收集有关云中设备和用户的数据，例如其合规状态、安全状态和身份信息。这允许ISE在云终端上实施网络访问策略，就像对内部设备一样。

4.将ISE无缝扩展到云环境:Hermes的一个主要优势是，它在ISE本地环境和日益增多的云本机应用之间提供了一个无缝的网桥。这样可以更轻松地将ISE安全策略、身份验证方法和访问控制扩展至云服务，而无需对现有基础设施进行彻底的改造。

对**Hermes**进行验证和故障排除（**Pxgrid**云代理）

1.默认情况下，Hermes服务处于禁用状态，将ISE与Cisco PxGrid云连接会启用Hermes服务。因此，如果在ISE中禁用了Hermes服务，请确认是否从**ISE GUI >管理>部署**启用了**Pxgrid云**选项，然后选择**ISE**节点。编辑，启用**Pxgrid云**。

2.用于解决与Pxgrid云相关的问题的有用调试是**hermes.log**和**pxcloud.log**。这些调试仅在启用了Pxgrid云的Pxgrid节点上可用。

McTrust（Meraki同步服务）

McTrust（Meraki同步服务）是一项支持Cisco ISE和Cisco Meraki系统之间集成的服务，特别是用于同步和管理网络设备和访问策略。McTrust服务充当连接器，用于在Meraki的云托管网络基础设施和ISE本地身份和策略管理系统之间同步用户和设备信息。

McTrust（Meraki同步服务）的主要特性和功能

1.与Meraki设备无缝集成：McTrust使ISE能够与Meraki的云托管设备同步和集成。其中包括Meraki产品组合中的设备，例如Meraki接入点、交换机和安全设备。它允许ISE直接与Meraki的基础设施通信，从而更轻松地对Meraki管理的设备应用网络访问控制策略。

2.自动设备同步:Meraki同步服务自动将ISE策略与Meraki网络设备同步。这意味着对ISE中的网络访问控制策略所做的任何更改都会自动反映在Meraki设备中，无需手动干预。这样管理员可以更轻松地管理跨Meraki和ISE平台的网络访问。

3. Meraki受管设备的策略实施:McTrust允许ISE根据身份验证和设备状态在Meraki设备上实施网络访问策略。它可以动态地将策略分配给Meraki网络元素，例如调整VLAN分配、应用访问控制列表(ACL)或限制对特定网络资源的访问，具体取决于请求访问的设备或用户的安全状态。

4. Meraki控制面板集成:McTrust将ISE直接与Meraki控制面板集成，提供统一的管理界面。通过此集成，管理员可以从Meraki云托管界面中查看和管理Meraki设备和ISE托管资源的网络策略和访问控制规则。

验证**McTrust（Meraki同步服**务）并对其进行故障排除

1.登录到ISE GUI -> Work Centers -> TrustSec -> Integrations -> Sync status。验证发现的任何问题/错误。

2.确保ISE节点的所有管理员证书都处于活动状态且有效。

用于Meraki同步服务故障排除的有用调试是meraki-connector.log。

ISE节点导出器

ISE节点导出器服务是一个用于监控和收集ISE系统性能度量的组件，特别是从ISE节点（无论是管理节点、监控节点还是策略服务节点）。

ISE节点导出器的主要特性和功能

1.指标导出:ISE节点导出器提供多种与性能相关的度量，例如CPU使用情况、内存使用情况、磁盘利用率、网络统计信息、系统负载和其他操作系统级别的度量。这些度量随后用于监控ISE节点的运行状况和性能，并且可以在监控控制面板（如Grafana）中查看。

2.系统运行状况监控:通过将性能数据导出到Prometheus，ISE节点导出器允许持续监控ISE节点的运行状况和运行状态。管理员可以根据预定义的阈值创建警报，以通知他们性能降低或系统问题。

3. Prometheus集成:ISE节点导出器通常与Prometheus结合使用，Prometheus是一个开源监控和警报工具包，旨在实现可靠性和可扩展性。节点导出器显示系统级指标，Prometheus可以擦除这些指标来收集和存储时序数据。

ISE Prometheus服务

ISE Prometheus服务是一项将Prometheus与ISE集成以启用监控和从ISE系统收集性能指标的服务。Prometheus是一个开源监控和警报工具包，用于收集、存储和分析时序数据，ISE Prometheus服务允许ISE将其内部指标展示给Prometheus用于监控。

ISE Prometheus服务的主要特性和功能

1.用于监控的指标收集:ISE Prometheus服务旨在导出与ISE系统相关的各种运营和性能指标。这些指标通常包括（但不限于）CPU利用率和系统负载、内存使用、磁盘使用和I/O性能、网络统计数据、身份验证请求统计数据、策略实施统计数据、系统运行状况和正常运行时间数据

2. Prometheus集成:Prometheus服务允许ISE以与Prometheus兼容的格式显示数据，Prometheus会定期销毁此数据。然后，Prometheus将数据存储在时序数据库中，从而能够跟踪ISE系统的趋势和历史性能。

3. Grafana的可视化和报告:ISE中的Prometheus Service可与Grafana（一种流行的开源可视化工具）无缝集成。将度量导出到Prometheus后，管理员可以使用Grafana仪表板实时显示数据。这样可以轻松识别ISE部署中的性能瓶颈、系统趋势和潜在问题。

ISE Grafana服务

ISE Grafana服务是一项使用Grafana（用于监控和数据可视化的开源平台）提供系统性能指标可视化的服务。它与Prometheus集成以显示从ISE收集的实时和历史数据，使管理员可以创建交互式控制面板，提供对ISE系统的运行状况、性能和使用的见解。

ISE Grafana服务的主要特性和功能

1.可自定义的控制面板:Grafana可高度自定义，允许管理员根据特定监控需求创建和修改控制面板。可以创建自定义查询以从Prometheus提取特定数据点，并且这些查询可以各种格式可视化，如图形、表格、热图等。

2.对分布式ISE部署的集中监控:对于分布式ISE部署，多个ISE节点部署在不同位置，Grafana提供从每个节点收集的所有系统指标的集中视图。这使管理员能够从单个位置监控整个ISE部署的性能。

3.历史数据及趋势分析:利用存储在Prometheus中的数据，Grafana可对系统指标进行历史分析，使管理员能够跟踪随时间变化的趋势。例如，他们可以监控过去一个月内CPU使用率的变化情况或身份验证成功率的波动情况。这些历史数据对于容量规划、趋势分析和确定长期问题很有价值。

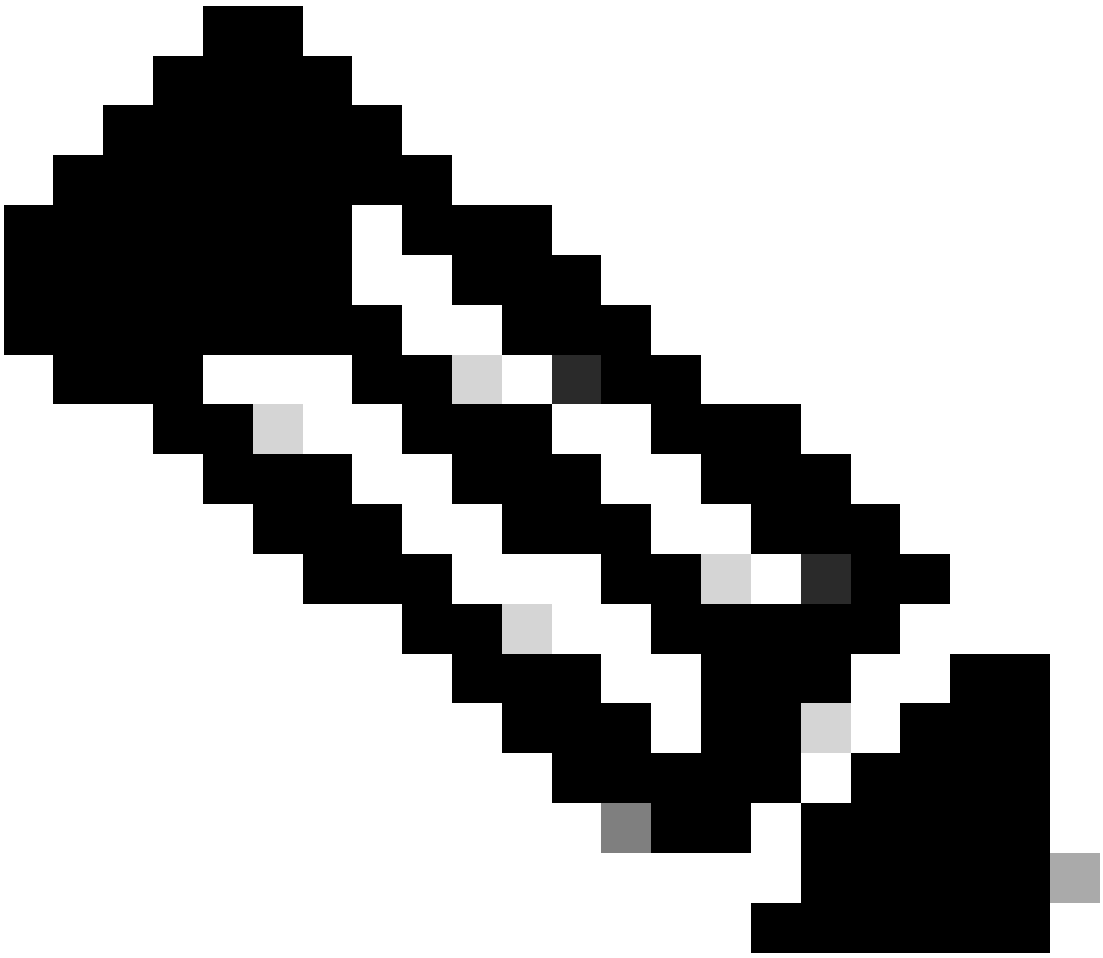
验证**ISE Grafana**服务、**ISE Prometheus**服务、**ISE**节点导出器并排除故障

1. ISE Grafana服务、ISE Prometheus服务和ISE节点导出器服务协同工作，称为Grafana堆栈服务。无需启用特定调试来对这些服务进行故障排除。但是，这些命令有助于排除故障。

show logging application ise-prometheus/prometheus.log

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

show logging application ise-grafana/grafana.log



注意：当监控启用时，ISE节点导出器、ISE　Prometheus服务和ISE　Grafana服务必须运行，并且这些服务的中断会在数据收集期间导致问题。

ISE MNT日志分析弹性搜索

ISE MNT LogAnalytics Elasticsearch是将Elasticsearch与ISE监控和故障排除(MNT)功能集成的组件。它用于与ISE日志和事件相关的日志聚合、搜索和分析。Elasticsearch是一个广泛使用的分布式搜索和分析引擎，与ISE集成后，可增强系统存储、分析和可视化由ISE组件生成的日志数据的能力。

ISE MNT LogAnalytics Elasticsearch的主要特性和功能

1.日志存储和索引：ISE中的Elasticsearch服务负责存储和索引ISE生成的日志数据。Elasticsearch是一个分布式搜索和分析引擎，它允许ISE日志以可快速搜索、查询和检索特定事件、错误或系统活动的方式存储。

2.与日志分析集成：ISE MNT LogAnalytics Elasticsearch与Log Analytics配合使用，可提供全面的日志记录解决方案。它使ISE能够收集与身份验证、策略实施、系统操作和其他活动相关的日志数

据。这些数据存储在Elasticsearch中，便于执行详细分析并深入了解ISE行为。

3.集中日志记录:通过与Elasticsearch集成，ISE提供集中日志记录解决方案，这对于需要分布式日志收集的环境至关重要。这样，管理员可以在单个统一界面中查看和分析来自多个ISE节点的日志，从而更轻松地对ISE性能进行故障排除和监控。

4.日志分析和故障排除:ISE MNT LogAnalytics Elasticsearch服务使日志数据易于访问，从而帮助管理员分析系统行为和排除问题。例如，如果身份验证故障突然增加或系统意外中断，Elasticsearch允许快速查询日志数据以确定根本原因。

验证**ISE M&T LogAnalytics Elasticsearch**并排除故障

1.在ISE中禁用和重新启用日志分析服务必须有所帮助。导航到操作>系统360 >设置>日志分析（通过使用切换选项禁用和启用）。

2.从ISE根重新启动M&T LogAnalytics可解决此问题。联系思科TAC执行此操作。

已知缺陷

思科漏洞ID ·66198

ISE Logstash服务

ISE Logstash Service是一个组件，它将Logstash（一个开源数据处理管道）与ISE集成在一起，用于日志收集、转换和转发。Logstash充当日志收集器和日志转发器，允许处理ISE日志并将其发送到其他系统进行分析、存储和监控。 Logstash是一个功能强大的开源工具，它收集、分析和转发来自不同来源的日志或其他数据，并将其集中到存储、分析和可视化中心。在ISE环境中，ISE Logstash服务用于以结构化格式处理日志并将其转发到集中式日志记录系统，在该系统中可以进一步分析、监控和可视化日志。

ISE Logstash服务的主要特性和功能

1.日志收集和转发：ISE Logstash Service的主要功能是从各种ISE组件（如身份验证日志、系统日志、策略实施日志等）收集日志数据，并将其转发到中央位置（通常是Elasticsearch或其他日志管理系统）进行存储和分析。

2.日志分析:Logstash可以将收集的日志解析为结构化格式。它处理原始日志数据并从其中提取有意义的信息，将日志条目转换为更易于查询和分析的格式。这可能涉及在将数据转发到Elasticsearch或其他系统之前对其进行过滤、解析和丰富。

验证**ISE Logstash**服务并对其进行故障排除

1.没有要启用的特定调试。但是，**show logging application ise-logstash/logstash.log**提供了有关服务状态的见解。

2.在ISE中禁用和重新启用日志分析服务必须有所帮助。导航到**操作>系**统360 >设置>日志分析（使用切换选项禁用和启用）。

与Logstash服务相关的已知缺陷

思科漏洞ID ·74832

思科漏洞ID ·58596

ISE Kibana服务

ISE　Kibana服务是一个组件，它将Kibana（一种开源数据可视化工具）与ISE日志记录和监控基础设施集成在一起。Kibana与Elasticsearch（存储和索引日志数据）配合工作，为可视化、搜索和分析ISE日志和性能指标提供强大的平台。

ISE Kibana服务的主要特性和功能

1.数据可视化:ISE Kibana服务允许管理员创建从ISE收集的日志数据的直观表示。这可能包括：

- 有关身份验证、策略实施、用户活动和系统健康状况的趋势的图表、图表和表格。
- 饼图、折线图和条形图，用于跟踪特定指标，例如登录失败次数、会话持续时间或一段时间的错误。

验证**ISE Kibana**服务并进行故障排除

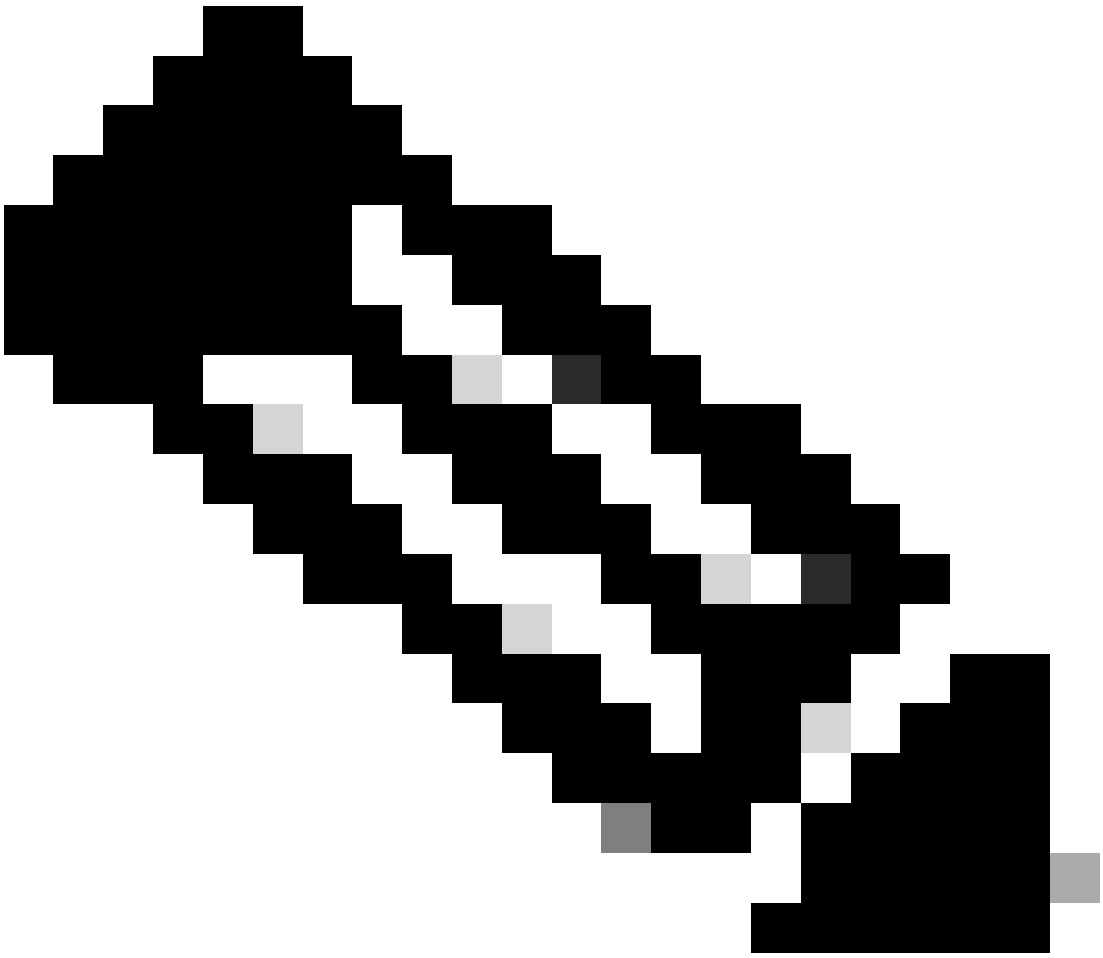
1.如果ISE　kibana服务未运行、禁用并重新启用ISE中的日志分析，请导航到操作>系统360　>设置，日志分析（通过使用切换选项禁用和启用）。

2.在许多情况下，/etc/hosts文件夹中可能存在导致问题的重复条目。联系TAC以删除重复条目。

与Kibana问题相关的已知缺陷

思科漏洞ID ·78050

思科漏洞ID ·59848



注意：启用日志分析后，ISE MNT LogAnalytics Elasticsearch、ISE Logstash Service和ISE Kibana Service必须正在运行，并且其中任何服务的中断都会在数据收集期间产生问题。

ISE本地IPSec服务

ISE本地IPSec服务是指内置的IPSec（互联网协议安全）支持，可提供ISE节点之间或ISE与其他网络设备之间的安全通信。IPSec是一套协议，用于通过验证和加密通信会话中的每个IP数据包来保护网络通信。本地IPSec服务是更广泛的安全和网络访问管理框架的一部分。它提供处理和管理IPsec VPN连接的功能，确保ISE系统和远程终端之间传输的数据是安全的。这可能涉及与客户端设备、网络访问设备（如路由器或防火墙）甚至其他ISE节点的交互，在这些节点中，IPsec加密和隧道对于保护敏感信息是必需的。

ISE本地IPSec服务的主要特性和功能

1.通过IPsec实现安全通信：ISE本地IPSec服务的主要功能是使用IPsec建立和维护安全通信通道。这涉及使用加密和身份验证机制来确保ISE和其他设备之间传输的数据受到保护，防止被拦截、篡改和未经授权的访问。

2. IPsec VPN连接:ISE本地IPSec服务有助于促进使用IPsec协议为数据传输提供安全、加密隧道的VPN连接。这对于需要通过不受信任的网络（例如互联网）安全访问ISE环境的远程员工、分支机构或其他位置尤其有用。

3.远程访问VPN支持:本地IPSec服务可以参与远程访问VPN配置，其中位于非现场的用户或设备（例如远程员工或分支机构）通过IPsec隧道安全地连接到ISE系统。此服务确保所有远程访问流量在到达ISE环境之前经过加密和身份验证。

4.IPsec VPN客户端兼容性:ISE本地IPSec服务确保与IPsec VPN客户端的兼容性。它支持常见的客户端配置，使设备能够安全地连接到网络，而不会将敏感数据暴露于风险中。

本机IPSec服务验证和故障排除

1.没有为本地IPSec服务启用特定调试。通过ISE CLI使用show logging application strongswan/charon.log tail命令验证日志。

2.如果发现隧道存在任何问题，请通过GUI > Administration > System > Settings > Protocols > IPSec > Native IPSec验证隧道建立的状态。

MFC分析器

MFC分析器是用于分析网络设备和端点的专用组件。分析是网络访问控制的关键部分，因为它允许ISE识别网络上的设备，对它们进行分类，并根据设备的类型和行为应用适当的网络策略。

ISE中MFC Profiler服务的主要特性和功能

1.流量分析：ISE中的MFC分析器服务负责收集和分析流量数据。它监控终端在网络上的行为，包括所使用的应用类型、所访问的服务以及设备显示的流量模式。此数据可帮助为每个终端构建配置文件。

2.终端分析:MFC分析器服务允许ISE根据终端的行为识别和分类终端。例如，它根据流量模式检测终端是打印机、计算机还是移动设备。这有助于针对不同类型的设备实施更具体的策略，从而提高安全性和运营效率。

验证**MFC分析器服**务并对其进行故障排除

1.导航到ISE GUI -> Administration -> Profiling -> MFC分析和AI规则，验证服务是否已启用。

2.如果服务已启用，但在ISE CLI中通过show application status ise命令显示为已禁用/未运行。请通过参阅Step1在ISE中禁用并重新启用MFC分析服务。

用于故障排除的有用调试：调试中的MFC分析器组件。可以通过支持捆绑包验证日志，也可以通过ISE CLI使用show logging application ise-pi-profiler.log tail命令跟踪日志。

MFC分析器的已知缺陷显示未运行而不是禁用状态：

思科漏洞ID ·72853

要点

1.要恢复服务，请通过ISE CLI使用application stop ise和application start ise命令重新启动服务。

2.出现问题时，请确保从ISE GUI/ISE CLI捕获支持捆绑包，以进一步验证问题。通过GUI和CLI创建ISE支持捆绑包的参考链接：收集身份服务引擎上的支持捆绑包

3.如果问题与资源、平均负载、磁盘利用率等相关，则必须收集线程转储和堆转储以供分析。

4.在执行节点重新加载之前，请联系Cisco TAC并提供安全日志以供进一步分析。

ISE中的标准问题

除ISE服务问题外，这些都是ISE节点中发现的一些问题，以及所需的基本故障排除步骤。

验证高负载平均值、资源利用率问题（CPU/内存/磁盘）、资源不足

1.通过ISE CLI使用show inventory命令验证思科建议的资源已分配给节点。

2.从ISE节点的CLI运行tech top命令以验证ISE的资源利用率。

3.通过ISE CLI使用show disk命令验证磁盘利用率。

4.清除非活动终端，清除节点的本地磁盘并执行升级清除。

如果问题仍然存在，请联系思科TAC并提供来自出现问题的节点的安全支持捆绑包、堆转储和线程转储。

要保护堆转储，请登录到ISE节点的CLI，运行**application configure ise**命令。选择选项22。

要保护线程转储，请登录到ISE节点的CLI，运行**application configure ise**命令，选择选项23。线程转储包含在支持捆绑包中，或者可以通过**ISE CLI使用show logging application appserver/catalina.out** 命令跟踪线程转储。

检验监控问题并排除故障

ISE的监控和故障排除(MnT)功能是提供监控、报告和警报功能的ISE架构的主要模块之一。

ISE显示许多位置的监控信息，包括：

- Cisco ISE主页
- 情景可视性视图
- RADIUS实时日志和实时会话
- 全局搜索
- 以威胁为中心的NAC实时日志
- TACACS实时日志

监控和故障排除类别中观察到的一般问题：

1. Radius/ TACACS实时日志不可用
2. 未提供实时会话
3. 运行状况摘要不可用
4. 在MnT节点上发现性能（高CPU/内存）问题

要在MnT节点上启用调试，以缩小问题范围：

1. Cisco-mnt
2. 收集器
3. Cpm-mnt
4. 运行时记录

除了调试中提到的组件之外，此信息还有助于排除故障：

1. 实时会话是否也受到影响，还是仅实时日志？
2. Radius或TACACS日志是否受到影响，或两者都受影响？
3. 您是否看到MnT节点上的CPU使用率较高或交换空间使用率较高？
4. 您在MnT节点上看到多少缓冲区文件。可在以下位置找到缓冲区文件：/opt/CSCOcpm/mnt/data/collector。
5. 是否启用了内存和CPU预留（如果未启用）。
6. 最近是否执行过MnT/config/session DB重置？
7. 您是否看到系统日志从PSN发送到MnT节点？

如果将Syslog服务用于MnT，则故障排除需要以下信息：

1. 您是否使用安全系统日志目标？如果不使用，请将其禁用，因为已知会导致线程死锁，从而导致收集器停止运行？
2. 是否使用安全系统日志目标，请确保在Administration -> Logging -> Remote logging Targets -> Secure Syslog collector 1和2下正确设置证书映射
3. 验证日志记录类别是否正确（建议删除未使用/不需要的日志记录类别 — 这样可减少MnT节点上的负载）设置以及日志记录目标是否正确配置。
4. 检查支持捆绑包中的awrrep*.html文件，了解并获取有关哪个组件发送更频繁的系统日志的提示。例如，如果通过插入或更新查询看到TACACS表，我们可以检查收集器日志以关联了解哪些系统日志发送更频繁

如果问题与MnT节点的性能有关，我们需要以下信息：

1.MnT节点的ISE CLI的tech top输出。

2.如果CPU使用率较高，您是否还会看到内存使用率较高或交换空间使用率较高？

3.支持捆绑包，确保堆转储和线程转储安全。

参考

- 思科身份服务引擎管理员指南，版本3.3
- 在ISE上排除故障并启用调试

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。