故障排除

思科 ISE 中的监控和故障排除服务

监控和故障排除 (MnT) 服务是所有Cisco ISE 运行时服务的综合身份解决方案。**操作 (Operations)** 菜单包含以下组件，并且只能从主策略管理节点 (PAN) 查看。请注意，**操作 (Operations)** 菜单不会显示在主监控节点中。

- 监控：实时呈现代表网络上的访问活动状态的有意义数据。通过查看展示，您可以轻松地解释并影响操作条件。
- 故障排除：提供用来解决网络上的访问问题的上下文指导。然后，您可以解决用户的问题并及时提供解决方案。

- 报告：提供标准报告的目录，这些报告可用来分析趋势和监控系统性能以及网络活动。您可以用各种方式自定义这些报告，并可保存这些报告以供将来使用。您可以在所有报告中针对以下字段使用通配符和多个值搜索记录：**身份 (Identity)**、**终端 ID (Endpoint ID)** 和 **ISE 节点 (ISE Node)**（**运行状况摘要 (Health Summary)** 报告除外）。

ISE 社区资源

有关故障排除技术说明的完整列表，请参阅 ISE 故障排除技术说明。

运行状况检查

Cisco ISE 版本 3.0 引入了按需运行状况检查选项，用于诊断Cisco ISE 部署中的所有节点。执行任何操作之前，先在所有节点上进行运行状况检查有助于减少停机时间，并通过发现关键问题改善Cisco ISE 系统的整体功能。运行状况检查会提供组件的工作状态，如有任何Cisco ISE 组件损坏，将提供即时故障排除建议。

注释 在运行状况检查期间，如果任何节点在15分钟内没有发回响应，则该特定节点的运行状况检查会超时。

执行运行状况检查

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **运行状况检查 (Health Checks)**。

步骤 2 点击**启动运行状况检查 (Start health checks)**。

信息弹出窗口将显示以下消息：

已触发健康状况检查 (Health Checks triggered)。

步骤 3 点击**确定 (Ok)** 查看状态。

步骤 4 在**运行状况检查 (Health Checks)** 窗口中，您将能够查看每个组件的运行状况。以下颜色用于指示Cisco ISE 组件的运行状况：

颜色	运行状况	操作
红色	不佳	点击下拉选项查看框中提供的故障排除建议。解决问题，然后点击刷新图标。
橙色	良好 **注释** 组件的运行状况良好，可以执行操作。但是，存在的问题可能会在将来影响某些功能。	点击下拉选项查看框中提供的故障排除建议。

颜色	运行状况	操作
绿色	良好	无需任何操作。
蓝色	良好	点击信息图标查看关于功能的关键信息。

步骤 5 点击**下载报告 (Download report)**。

HealthChecksReport.json 文件将保存在本地系统中，其中包含Cisco ISE 部署的详细运行状况信息。

触发运行状况检查后，状态将在**运行状况检查 (Health Check)** 窗口中保留三小时。在**运行状况检查 (Health Check)** 窗口刷新/过期前，将无法运行健康状况检查。

网络权限框架事件流程

网络权限框架 (NPF) 身份验证和授权事件流程使用下表列出的过程：

流程阶段	说明
1	网络访问设备 (NAD) 执行正常授权或 Flex 授权。
2	使用 Web 授权分析无代理的未知身份。
3	RADIUS 服务器进行身份验证和授权。
4	在端口配置身份的授权。
5	丢弃未经授权的终端通信。

用于监控和故障排除功能的用户角色和权限

监控和故障排除功能与默认用户角色相关联。允许您执行的任务与分配给您的用户角色直接相关。

有关为每个用户角色设置的权限和限制的信息，请参阅思科 ISE 管理员组。

注释 不支持在没有思科 TAC 监管的情况下使用根 shell 访问思科 ISE，并且思科不对由此导致的任何服务中断负责。

监控数据库中存储的数据

Cisco ISE 监控服务会收集数据并将所收集的数据存储于专用监控数据库中。根据用于监控网络功能的数据速率和数据量，可能需要将某个节点专用于监控。如果Cisco ISE 网络以高速率从策略服务节点或网络设备收集日志数据，则我们建议将某个Cisco ISE 节点专用于监控。

要管理监控数据库中存储的信息，需要对数据库执行完整备份和增量备份。这包括清除不需要的数据，然后还原数据库。

思科 ISE 遥感勘测

遥测会监控网络中的系统和设备，向Cisco提供有关您如何使用产品的反馈。Cisco将这些信息用于改进产品。

遥测默认处于启用状态。要禁用此功能，请执行以下操作：

1. 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **设置 (Settings)** > **网络成功诊断 (Network Success Diagnostics)** > **遥测 (Telemetry)**
2. 取消选中**启用遥测 (Enable Telemetry)** 复选框以禁用遥测。

- **思科帐户 (Cisco Account)**：输入您的Cisco帐户，以便您可以通过遥测获取电子邮件。如果遥测发现任何可能影响您的严重问题，我们也可能使用此 ID 与您联系。
- **传输网关 (Transport Gateway)**：您可以在Cisco ISE 和Cisco外部遥测服务器之间使用代理，提供额外的安全性。要执行此操作，请选中此复选框并输入代理服务器的 FQDN。遥测不需要代理。

  Cisco提供传输网关软件。您可以从 Cisco.com 下载。此软件在 Linux 服务器上运行。有关如何在 RHEL 服务器上部署传输网关软件的信息，请参阅 Smart Call Home 部署指南。如果使用此 Cisco软件，则 URL 值为 **<FQDN of proxyserver>/ Transportgateway / services / DeviceRequestHandler**。您也可以使用此网关连接到智能许可服务器。从传输网关版本 3.5 开始，无法更改端口，但可以输入 IP 地址而不是 FQDN。

遥测收集的信息

遥测会将以下信息发送给Cisco。

节点：

对于每个策略管理节点 (PAN)

- 当前经过终端安全评估的终端数量
- 当前的 PxGrid 客户端数量
- 当前由 MDM 管理的终端数量
- 当前访客用户数
- 此遥测记录的开始和结束日期
- FIPS 状态

对于每个策略服务节点 (PSN)

- 分析器探测数
- 节点服务类型
- 已用的被动 ID

对于所有节点

- 总计和活动 NAD 数
- CPU 核心数量
- 虚拟机可用磁盘空间
- 虚拟机内存和 CPU 设置
- 系统名称
- 序列号
- VID 和 PID
- 正常运行时间
- 上次 CLI 登录

MnT 节点计数

pxGrid 节点计数

许可证

- 是否有许可证已到期？
- 可用的Cisco ISE Essentials 许可证数量、曾使用的最大数量
- 可用的Cisco ISE Advantage 许可证数量、曾使用的最大数量
- 可用的Cisco ISE Premier 许可证数量、曾使用的最大数量
- 小型、中型和大型虚拟机许可证的数量
- 是否正在使用评估许可证？
- 智能账户的名称
- TACACS 设备数量
- 到期日期、剩余天数、许可证期限
- 服务类型、主要和辅助 UDI

终端安全评估

- 非活动策略的数量
- 最后终端安全评估源更新

- 活动策略的数量
- 终端安全评估源更新

访客用户

- 当天经过身份验证的访客的最大数量
- 当天活动访客的最大数量
- 当天 BYOD 用户的最大数量
- 经过身份验证的访客的外部 ID 信息

网络访问设备 (NAD)

- 授权：激活的 ACL 数、VLAN 数、策略大小
- NDG 映射和 NAD 层次结构
- 身份验证：
  - RADIUS、RSA ID、LDAP、ODBC 和 Active Directory ID 存储区的数量
  - 本地（非管理员）用户数
  - NDG 映射和 NAD 映射
  - 策略行数

对于授权，包括活动 VLAN 数、策略计数、已激活的 ACL 数量：

- 状态，VID，PT
- 平均负载，内存使用量
- PAP、MnT、pxGrid 和 PIC 节点的数量
- 名称、配置文件名称、配置文件 ID

NAD 配置文件

对于每个 NAD 配置文件：

- 名称和 ID
- Cisco设备
- TACACS 支持
- RADIUS 支持
- TrustSec SXP 支持
- 默认配置文件

Profiler

- 最后源更新的日期
- 是否已启用自动更新？
- 已分析的终端数、终端类型、未知终端数、未知百分比和终端总数
- 自定义配置文件数量
- 序列号、范围、终端类型、自定义配置文件

移动设备管理 (MDM)

- MDM 节点列表
- 对于日期范围，包括当前 MDM 终端计数、当前访客用户计数、当前已经过终端安全评估的用户计数
- pxGrid 客户端计数
- 节点计数

SNMP 陷阱监控思科 ISE

思科 ISE 中的通用 SNMP 陷阱

SNMP 陷阱可帮助您监控Cisco ISE 的状态。如果要在不访问Cisco ISE 服务器的情况下监控Cisco ISE，可以在Cisco ISE 中将 MIB 浏览器配置为 SNMP 主机。然后您可以在 MIB 浏览器中监控Cisco ISE 的状态。

有关 **snmp-server host** 和 **snmp-server trap** 命令的信息，请参阅《思科身份服务引擎 CLI 参考指南》。

Cisco ISE 支持 SNMPv1、SNMPv2c 和 SNMPv3。

如果您在 CLI 中配置了 SNMP 主机，Cisco ISE 将发送以下通用系统陷阱：

- 冷启动：当设备重新引导时。
- Linkup：当以太网接口打开时。
- Linkdown：当以太网接口关闭时。
- 身份验证故障：当社区字符串不匹配时。

下表列出了Cisco ISE 中默认生成的通用 SNMP 陷阱。

OID	说明	陷阱示例
.1.3.6.1.4.1.8072.4.0.3 \n NET-SNMP-AGENT-MIB::nsNotifyRestart	表示代理已重新启动。	DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (478) 0:00:04.78 SNMPv2-MIB::snmpTrapOID.0 = OID: NET-SNMP-AGENT-MIB::nsNotifyRestart SNMPv2-MIB::snmpTrapEnterprise.0 = OID: NET-SNMP-MIB::netSnmpNotificationPrefix
.1.3.6.1.4.1.8072.4.0.2 \n NET-SNMP-AGENT-MIB::nsNotifyShutdown	表示代理正在关闭。	DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (479) 0:00:04.79 SNMPv2-MIB::snmpTrapOID.0 = OID: NET-SNMP-AGENT-MIB::nsNotifyShutdown SNMPv2-MIB::snmpTrapEnterprise.0 = OID: NET-SNMP-MIB::netSnmpNotificationPrefix
.1.3.6.1.6.3.1.1.5.4 \n IF-MIB::linkUp	表示 SNMP 实体（充当代理角色）检测到其中一条通信链路的 ifOperStatus 对象已从“关闭”(Down) 状态转换为其他状态（但不是“不存在”(notPresent) 状态）。其他状态由包含的 ifOperStatus 值表示。	DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (478) 0:00:04.78 SNMPv2-MIB::snmpTrapOID.0 = OID: IF-MIB::linkUp IF-MIB::ifIndex.12 = INTEGER: 12 IF-MIB::ifAdminStatus.12 = INTEGER: up(1) IF-MIB::ifOperStatus.12 = INTEGER: up(1) SNMPv2-MIB::snmpTrapEnterprise.0 = OID: NET-SNMP-MIB::netSnmpAgentOIDs.10

OID	说明	陷阱示例
.1.3.6.1.6.3.1.1.5.3 \n IF-MIB::linkDown	表示 SNMP 实体（充当代理角色）检测到其中一条通信链路的 ifOperStatus 对象即将从其他状态（但不是“不存在”(notPresent) 状态）进入“关闭”(Down) 状态。其他状态由包含的 ifOperStatus 值表示。	DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (479) 0:00:04.79 SNMPv2-MIB::snmpTrapOID.0 = OID: IF-MIB::linkDown IF-MIB::ifIndex.5 = INTEGER: 5 IF-MIB::ifAdminStatus.5 = INTEGER: up(1) IF-MIB::ifOperStatus.5 = INTEGER: down(2) SNMPv2-MIB::snmpTrapEnterprise.0 = OID: NET-SNMP-MIB::netSnmpAgentOIDs.10
.1.3.6.1.6.3.1.1.5.1 \n SNMPv2-MIB::coldStart	表示支持通知发起方应用的 SNMP 实体正在重新初始化自身，并且其配置可能已更改。	DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (8) 0:00:00.08 SNMPv2-MIB::snmpTrapOID.0 = OID: SNMPv2-MIB::coldStart SNMPv2-MIB::snmpTrapEnterprise.0 = OID: NET-SNMP-MIB::netSnmpAgentOIDs.10

思科 ISE 中的进程监控 SNMP 陷阱

如果从Cisco ISE CLI 配置 SNMP 主机，则Cisco ISE 允许将Cisco ISE 进程状态的 hrSWRunName 陷阱发送到 SNMP 管理器。Cisco ISE 使用时钟守护作业 (cron job) 来触发这些陷阱。Cron 作业会从 Monit 检索Cisco ISE 进程状态。当在 CLI 中配置 **SNMP-服务器主机** 命令后，cron 作业会每五分钟运行一次，并监控Cisco ISE。

注释 当 ISE 进程由管理员手动停止时，该进程的监控也会停止，并且系统不会向 SNMP 管理器发送陷阱。仅当进程意外关闭并且不自动恢复时，系统才会向 SNMP 管理器发送进程停止 SNMP 陷阱。

以下是Cisco ISE 中进程监控 SNMP 陷阱的详尽列表。

OID	说明	陷阱示例
.1.3.6.1.2.1.25.4.2.1.2 \n HOST-RESOURCES-MIB::hrSWRunName	此运行软件的文本说明，包括制造商、版本和通常所知的名称。如果此软件是在本地安装的，则此字符串必须与相应的 hrSWInstalledName 中使用的字符串相同。所考虑的服务包括 app-server、rsyslog、redis-server、ad-connector、mnt-collector、mnt-processor、ca-server est-server 和 elasticsearch。	DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (63692139) 7 days, 8:55:21.39 SNMPv2-MIB::snmpTrapOID.0 = OID: HOSTRESOURCES- MIB::hrSWRunName HOSTRESOURCES- MIB::hrSWRunName = STRING: "redis-server:Running"

发生以下状况时，Cisco ISE 会向配置的 SNMP 服务器发送相应的陷阱：

- 进程开始（受监控状态）
- 进程停止（不受监控状态）
- 执行失败：当进程状态从“受监控”(Monitored) 变为“执行失败”(Execution Failed) 时，发送陷阱。
- 不存在：当进程状态从“受监控”(Monitored) 变为“不存在”(Does Not Exist) 时，发送陷阱。

在 SNMP 服务器中，会为每个对象生成唯一的对象 ID (OID)，并为 OID 分配一个值。您可以通过 OID 值在 SNMP 服务器查找对象。正在运行的陷阱的 OID 值为 *running*，不受监控的、不存在的和执行失败的陷阱的 OID 值为 *stopped*。

Cisco ISE 使用属于 HOST-RESOURCES MIB 的 hrSWRunName 的 OID 发送陷阱，并将 OID 值设置为 <进程名称> - <进程状态>，例如，runtime - running。

要终止Cisco ISE 发送 SNMP 陷阱至 SNMP 服务器，需在Cisco ISE CLI 中删除 SNMP 配置。此操作将终止来自 SNMP 管理器的 SNMP 陷阱和轮询。

思科 ISE 中的磁盘利用率 SNMP 陷阱

当Cisco ISE 分区达到利用率限制阈值时并且达到所配置的可用空间量时，将发送一个陷阱。

以下是可在Cisco ISE 中配置的磁盘利用率 SNMP 陷阱的详尽列表：

OID	说明	陷阱示例
.1.3.6.1.4.1.2021.9.1.9 \n UCD-SNMP-MIB::dskPercent	磁盘上已用空间的百分比。	DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (118198297) 13 days, 16:19:42.97 SNMPv2-MIB::snmpTrapOID.0 = OID: UCD-SNMP-MIB::dskPercent UCD-SNMP-MIB::dskPercent = INTEGER: 13
.1.3.6.1.4.1.2021.9.1.2 \n UCD-SNMP-MIB::dskPath	磁盘的挂载路径。 dskPath 可以为 ISE 管理命令 **show disks** 输出中的所有挂载点发送陷阱。	DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (118198304) 13 days, 16:19:43.04 SNMPv2-MIB::snmpTrapOID.0 = OID: UCD-SNMP-MIB::dskPath UCD-SNMP-MIB::dskPath = STRING: /opt

思科 ISE 警报

警报显示在 Alarms dashlet 中，通知您网络中的严重情况。警报还会提供关于系统活动的信息，如数据清除事件。可以配置要接收系统活动通知的方式，或完全禁用警报。还可以为某些警报配置阈值。

大多数警报没有关联的计划，会在事件发生后立即发送。在任何给定时间点，系统只会保留最新的 15,000 个警报。

如果事件再次发生，则系统会在约一个小时内抑制相同的警报。在事件再次发生期间，可能需要经过一个小时，警报才会再次出现（取决于触发器）。

下表列出所有Cisco ISE 警报、说明及其解决方法。

表 *1:* 思科 *ISE* 警报

警报名称	警报说明	警报解决方法
管理和操作审核管理		
部署升级失败	ISE 节点升级失败。	检查故障节点的 ADE.log，以查找升级失败的原因并制定纠正措施。
升级捆绑包下载失败	ISE 节点升级捆绑包下载失败。	检查故障节点的 ADE.log，以查找升级失败的原因并制定纠正措施。
SXP 连接失败	SXP 连接失败。	验证 SXP 服务正在运行。检查对等兼容性。

警报名称	警报说明	警报解决方法
应用于所有设备的Cisco配置文件	网络设备配置文件定义网络接入设备的功能，如MAB、Dot1X、CoA 和网络重定向。作为 ISE 2.0 升级的一部分，默认Cisco网络设备配置文件应用于所有网络设备。	编辑非Cisco网络设备的配置，以分配适当的配置文件。
由于CRL查找到已吊销的证书，安全 LDAP 连接重新连接	CRL 检查结果是用于 LDAP 连接的证书已吊销。	检查 CRL 配置并检验它是否有效。检查 LDAP 服务器证书及其颁发机构证书是否已吊销。如果已撤销，则颁发新证书并将其安装在 LDAP 服务器上。
由于 OCSP 查找到已吊销的证书，安全 LDAP 连接重新连接	OCSP 检查结果是用于 LDAP 连接的证书已吊销。	检查 OCSP 配置并检验它是否有效。检查 LDAP 服务器证书及其颁发机构证书是否已吊销。如果已撤销，则颁发新证书并将其安装在 LDAP 服务器上。
由于CRL查找到已吊销的证书，安全系统日志连接重新连接	CRL 检查结果是用于系统日志连接的证书已吊销。	检查 CRL 配置并检验它是否有效。检查系统日志服务器证书及其颁发机构证书是否已吊销。如果已撤销，则颁发新证书并将其安装在系统日志服务器上。
由于 OCSP 查找到已吊销的证书，安全系统日志连接重新连接	OCSP 检查结果是用于系统日志连接的证书已吊销。	检查 OCSP 配置并检验它是否有效。检查系统日志服务器证书及其颁发机构证书是否已吊销。如果已撤销，则颁发新证书并将其安装在系统日志服务器上。
管理员帐户已锁定/禁用	由于密码过期或登录尝试不正确，系统锁定或禁用管理员帐户。有关详细信息，请参阅管理员密码策略。	管理员密码可以由其他管理员使用 GUI 或 CLI 进行重置。
ERS 识别已弃用的 URL	ERS 识别已弃用的 URL	请求 URL 已弃用，建议避免使用此 URL
ERS 识别过时的 URL	ERS 识别过时的 URL	请求的 URL 已过时，建议使用更新的URL。未来的版本不会删除此 URL。

警报名称	警报说明	警报解决方法
ERS请求的内容类型信头已过时	ERS请求的内容类型信头已过时	在请求的内容类型信头内指定的请求资源版本已过时。这表明资源方案已被修改。可能已添加或删除一个或多个属性。为使用过时的方案解决这一问题，ERS引擎将使用默认值。
ERS XML 输入有 XSS 或注入攻击的嫌疑	ERS XML 输入有 XSS 或注入攻击的嫌疑。	请检查您的 XML 输入。
备份失败	ISE 备份操作失败。	检查Cisco ISE与存储库之间的网络连接性。确保： • 用于存储库的凭证是正确的。 • 存储库中有足够的磁盘空间。 • 存储库用户具有写入权限。
CA 服务器已关闭	CA 服务器已关闭。	检查以确保 CA 服务已启动并正在 CA 服务器上运行。
CA 服务器已启动	CA 服务器已启动。	通知管理员 CA 服务器已启动。
证书到期	此证书即将到期。证书到期时，Cisco ISE 可能无法与客户端建立安全通信。	更换证书。对于信任证书，请联系证书颁发机构 (CA)。对于 CA 签名的本地证书，请生成 CSR 并使 CA 创建新证书。对于自签名的本地证书，请使用Cisco ISE延长有效期。如果不再使用证书，可将其删除。
证书被吊销	管理员已撤销由内部 CA 颁发给终端的证书。	从头完成 BYOD 流程以提供新证书。
证书调配初始化错误	证书调配初始化失败	在主题中找到多个具有相同 CN (CommonName) 属性值的证书。无法构建证书链。检查系统中的所有证书，包括 SCEP 服务器中的证书。

警报名称	警报说明	警报解决方法
证书复制失败	到辅助节点的证书复制失败	证书在辅助节点上无效，或存在某些其他永久错误条件。检查辅助节点是否有预先存在的冲突证书。如果找到，请删除辅助节点上预先存在的证书，然后在主要节点上导出新证书，删除证书，然后将其导入以重新尝试复制。
证书复制暂时失败	到辅助节点的证书复制暂时失败	由于网络故障等临时条件，证书未复制到辅助节点。系统将重试复制，直至成功。
证书已过期	此证书已过期。Cisco ISE 可能无法与客户端建立安全通信。节点到节点通信可能也会受到影响。	更换证书。对于信任证书，请联系证书颁发机构 (CA)。对于 CA 签名的本地证书，请生成 CSR 并使 CA 创建新证书。对于自签名的本地证书，请使用Cisco ISE 延长有效期。如果不再使用证书，可将其删除。
证书请求转发失败	证书请求转发失败。	确保传入的认证请求与发件人的属性相匹配。
配置已更改	Cisco ISE 配置已更新。系统没有为任何用户和终端的配置更改触发此警报。	检查是否应存在配置更改。
CRL 检索失败	无法从服务器检索 CRL。如果指定的 CRL 不可用，就可能会出现这种情况。	确保下载 URL 正确且可用于服务。
DNS 解析失败	节点上的 DNS 解析失败。	检查是否可访问使用 **ip name-server** 命令配置的 DNS 服务器。 如果您收到的警报为 **DNS Resolution failed for CNAME <hostname of the node>**，则确保为每个Cisco ISE 节点创建 CNAME RR 以及 A 记录。
需要进行固件更新	需要在此主机上进行固件更新。	联系Cisco TAC 以获取固件更新。

警报名称	警报说明	警报解决方法
虚拟机资源不足	此主机上的虚拟机 (VM) 资源（如 CPU、RAM、磁盘空间或 IOPS）不足。	确保 VM 主机达到《Cisco ISE 硬件安装指南》中指定的最低要求。
NTP 服务故障	此节点上的 NTP 服务已关闭。	这可能是因为 NTP 服务器与 Cisco ISE 节点之间存在较大的时间差异（超过 1000s）。确保 NTP 服务器正常工作并使用 **ntp server <servername>** CLI 命令重新启动 NTP 服务并修复时间差。
NTP 同步失败	在此节点配置上的所有 NTP 服务器均无法访问。	从 CLI 执行 **show ntp** 命令，进行故障排除。确保可从Cisco ISE访问 NTP 服务器。如果已配置 NTP 身份验证，请确保密钥 ID 和值与服务器的相匹配。
未安排配置备份	未安排Cisco ISE 配置备份。	创建配置备份计划。
操作数据库清除失败	无法从操作数据库中清除较旧的数据。这会在 MnT 节点忙碌时发生。	检查数据清除审核报告并确保 used_space 小于 threshold_space。使用 CLI 登录 MnT 节点，手动执行清除操作。
分析器 SNMP 请求失败	SNMP 请求超时或 SNMP 社区或用户身份验证数据不正确。	确保 SNMP 正在 NAD 上运行并验证Cisco ISE 上的 SNMP 配置是否与 NAD 匹配。
复制失败	辅助节点无法使用复制的消息。	登录到Cisco ISE GUI 并从部署页面执行手动同步。取消注册并重新注册受影响的Cisco ISE 节点。
恢复失败	Cisco ISE 恢复操作失败。	确保Cisco ISE 与存储库之间存在网络连接。确保用于存储库的凭证正确。确保备份文件未损坏。从 CLI 执行 **reset-config** 命令并恢复已知的最后一次有效备份。
补丁失败	服务器上的补丁进程失败。	在服务器上重新安装补丁进程。
补丁成功	服务器上的补丁进程成功。	-

警报名称	警报说明	警报解决方法
外部 MDM 服务器 API 版本不匹配	外部 MDM 服务器 API 版本与 Cisco ISE 中配置的版本不匹配。	确保 MDM 服务器 API 版本与 Cisco ISE 中配置的版本相同。如有需要，更新Cisco ISE MDM 服务器配置。
外部 MDM 服务器连接失败	到外部 MDM 服务器的连接失败。	确保MDM服务器已启动且Cisco ISE-MDM API 服务正在 MDM 服务器上运行。
外部 MDM 服务器响应错误	外部 MDM 服务器响应错误。	确保Cisco ISE-MDM API 服务在 MDM 服务器上正常运行。
复制已停止	ISE 节点无法从 PAN 复制配置数据。	登录Cisco ISE GUI 以从部署页面执行手动同步，或取消注册并重新注册带必填字段的受影响 ISE 节点。
终端证书已过期	终端证书已由每天安排的作业标记为过期。	重新注册终端设备，获取新的终端证书。
终端证书已清除	过期的终端证书已由每天安排的作业清除。	无需执行任何操作。这是管理员发起的清理操作。
终端清除活动	清除终端上过去 24 小时的活动。此警报在午夜触发。	查看清除活动，方法是选择**操作 (Operations)** > **报告 (Reports)** > **终端和用户 (Endpoints and Users)** > **终端清除活动 (Endpoint Purge Activities)**。
复制减慢错误	系统检测到复制减慢或停滞。	验证节点是否可访问并且是部署的一部分。
复制减慢信息	系统检测到复制减慢或停滞。	验证节点是否可访问并且是部署的一部分。
复制减慢警告	系统检测到复制减慢或停滞。	验证节点是否可访问并且是部署的一部分。
PAN 自动故障转移 - 故障转移失败	到辅助管理节点的升级请求失败。	有关进一步操作，请参阅警报详细信息。
PAN 自动故障转移 - 故障转移已触发	已成功触发辅助管理节点到主要角色的故障转移。	等待辅助 PAN 完成升级，并调用旧的主 PAN。
PAN 自动故障转移 - 运行状况检查处于非活动状态	PAN 未收到指定监控节点的运行状况检查监控请求。	验证报告的监控节点是否关闭或不同步，如有需要，请触发手动同步。

警报名称	警报说明	警报解决方法
PAN 自动故障转移 - 无效的运行状况检查	收到无效的运行状况检查监控请求，无法进行自动故障转移。	验证运行状况检查监控节点是否不同步，如有需要，请触发手动同步。
PAN 自动故障转移 - 主管理节点已关闭	主管理节点已关闭或无法从监控节点访问。	调用 PAN 或等待进行故障转移。
PAN 自动故障转移 - 故障转移尝试被拒绝	辅助管理节点已拒绝运行状况检查监控节点提出的升级请求。	有关进一步操作，请参阅警报详细信息。
EST 服务已停止	EST 服务已停止。	确保 CA 和 EST 服务正常运行，且证书服务终端从属 CA 证书链完整。
EST 服务已启动	EST 服务已启动。	通知管理员 EST 服务已启动。
Smart Call Home 通信故障	Smart Call Home 消息未成功发送。	确保Cisco ISE 和Cisco系统之间存在网络连接。
遥测通信故障	遥测消息未成功发送。	确保Cisco ISE 和Cisco系统之间存在网络连接。
适配器不可访问。	Cisco ISE 无法连接到适配器。	有关故障的详细信息，请查看适配器日志。
适配器错误	适配器出错。	查看警报说明。
适配器连接失败	适配器无法连接到源服务器。	确保源服务器可访问。
适配器因错误已停止工作	适配器出错，且未处于预期状态。	确保适配器配置正确，且源服务器可访问。有关错误详细信息，请参阅适配器日志。
服务组件错误	服务组件遇到一个错误。	查看警报说明。
服务组件信息	服务组件已发送通知。	无。
ISE 服务		
TACACS 身份验证尝试次数过多	ISE 策略服务节点遇到的 TACACS 身份验证次数超过了预期次数。	• 检查网络设备的重新验证计时器。 • 检查 ISE 基础设施的网络连接。

警报名称	警报说明	警报解决方法
TACACS 身份验证失败次数过多	ISE 策略服务节点遇到的 TACACS 身份验证失败次数超过了预期次数。	• 检查身份验证步骤，找出根本原因。 • 检查 ISE/NAD 配置，确定身份与密钥是否不匹配。
可重新访问 MSE 位置服务器	可重新访问 MSE 位置服务器。	无。
无法访问 MSE 位置服务器。	无法访问 MSE 位置服务器或 MSE 位置服务器已关闭。	请检查 MSE 位置服务器是否正在运行且是否可从 ISE 节点访问该服务器。
AD 连接器必须重新启动	AD 连接器意外停止，必须重新启动。	如果此问题仍然存在，请联系 Cisco TAC 寻求帮助。
Active Directory 林不可用	Active Directory 林全局目录不可用，无法用于身份验证、授权，以及组和属性检索。	检查 DNS 配置、Kerberos 配置、错误条件和网络连接性。
身份验证域不可用	身份验证域不可用，无法用于身份验证、授权，以及组和属性检索。	检查 DNS 配置、Kerberos 配置、错误条件和网络连接性。
ISE 身份验证处于非活动状态	Cisco ISE 策略服务节点未收到网络设备的身份验证请求。	• 检查 ISE/NAD 配置。 • 检查 ISE/NAD 基础设施的网络连接。
ID 映射。身份验证处于非活动状态	身份映射服务在过去 15 分钟未收集任何用户身份验证事件。	如果应在此时间内进行用户身份验证（例如工作时间），请检查到 Active Directory 域控制器的连接。
CoA 失败	网络设备已拒绝Cisco ISE 策略服务节点发出的授权更改 (CoA) 请求。	确保网络设备已配置为接受Cisco ISE 的 CoA 请求。请检查是否在有效会话中发出 CoA。
配置的名称服务器已关闭	配置的名称服务器已关闭或不可用。	检查 DNS 配置和网络连接。

警报名称	警报说明	警报解决方法
请求方已停止响应	Cisco ISE 在 120 秒前向客户端发送了最后一条消息，但客户端未响应。	• 验证请求方是否正确配置为与Cisco ISE 进行完整的 EAP 会话。 • 验证 NAS 是否正确配置为与请求方之间互相传输EAP消息。 • 验证请求方或 NAS 是否不会对 EAP 会话执行短时间超时。
身份验证尝试次数过多	Cisco ISE 策略服务节点进行的身份验证次数超过了预期次数。	检查网络设备的重新验证计时器。检查Cisco ISE 基础设施的网络连接。 达到阈值后，系统会触发“身份验证尝试次数过多”警报和“失败尝试次数过多”警报。显示在**说明** 列旁边的数字是在过去 15 分钟针对Cisco ISE 进行的身份验证成功或失败的总数。
失败尝试次数过多	Cisco ISE 策略服务节点遇到的身份验证失败次数超过了预期次数。	检查身份验证步骤，找出根本原因。检查Cisco ISE/NAD 配置，确定身份与密钥是否不匹配。 达到阈值后，系统会触发“身份验证尝试次数过多”警报和“失败尝试次数过多”警报。显示在**说明 (Description)** 列旁边的数字是在过去 15 分钟针对Cisco ISE 进行的身份验证成功或失败的总数。
AD：计算机 TGT 刷新失败	ISE 服务器票证授予票证 (TGT) 刷新失败。TGT 用于 AD 连接和服务。	检查 ISE 计算机帐户是否存在且有效。另请检查是否存在时钟偏差、复制、Kerberos 配置和/或网络错误。
AD：ISE 帐户密码更新失败	ISE 服务器未能更新其 AD 计算机帐户密码。	检查 ISE 计算机帐户密码是否未更改，计算机帐户是否未禁用或限制。检查到 KDC 的连接。

警报名称	警报说明	警报解决方法
所加入的域不可用	所加入的域不可用，无法用于身份验证、授权，以及组和属性检索。	检查 DNS 配置、Kerberos 配置、错误条件和网络连接性。
身份库不可用	Cisco ISE 策略服务节点无法访问配置的身份库。	检查Cisco ISE 与身份存储库之间的网络连接。
已检测到网络设备配置错误	Cisco ISE 已检测到 NAS 的 RADIUS 记帐信息过多。 默认情况下，禁用此警报。要启用此警报，请参阅启用和配置警报。	NAS 已向 ISE 发送过多的重复 RADIUS 记账信息。为 NAS 配置准确的记账频率。
已检测到请求方配置错误	Cisco ISE 已检测到网络上的请求方配置错误。 默认情况下，禁用此警报。要启用此警报，请参阅启用和配置警报。	确保请求方的配置正确。
记账未启动	Cisco ISE 策略服务节点已授权会话，但未收到网络设备的记帐启动请求。	确保在网络设备上已配置 RADIUS 记账。检查网络设备配置的本地授权情况。
NAD 未知	Cisco ISE 策略服务节点收到未配置在Cisco ISE 中的网络设备的身份验证请求。	检查网络设备是否为真实请求，然后将其添加到配置中。确保密钥匹配。
SGACL 丢包	发生安全组访问 (SGACL) 丢包。如果支持 Trustsec 的设备因 SGACL 策略违规丢包，就会出现这种情况。	运行 RBACL 丢包摘要报告并查看导致 SGACL 丢包的源。向违规的源发出 CoA 以重新授权或断开会话连接。
RADIUS 请求已丢弃	NAD 的身份验证/记账请求已以静默方式丢弃。这可能是由于 NAD 未知、共享密钥不匹配或依照 RFC 数据包的内容无效。 默认情况下，禁用此警报。要启用此警报，请参阅启用和配置警报。	检查 NAD/AAA 客户端是否在 Cisco ISE 中存在有效配置。检查 NAD/AAA 客户端和Cisco ISE 上的共享密钥是否匹配。确保AAA 客户端和网络设备没有硬件问题或 RADIUS 兼容性问题。此外，请确保用于将设备连接到Cisco ISE 的网络没有硬件问题。
EAP 会话分配失败	由于达到 EAP 会话限制，RADIUS 请求已丢弃。此情况可能是由并行 EAP 身份验证请求过多导致。	在调用包含新 EAP 会话的其他 RADIUS 请求之前，请等待几秒钟。如果继续出现系统过载，请尝试重新启动 ISE 服务器。

警报名称	警报说明	警报解决方法
RADIUS 情景分配失败	由于系统过载，RADIUS 请求已丢弃。此情况可能是由并行身份验证请求过多导致。	在调用新 RADIUS 请求之前，请等待几秒钟。如果继续出现系统过载，请尝试重新启动 ISE 服务器。
AD：ISE 计算机帐户没有获取组所需的权限。	Cisco ISE 计算机帐户没有获取组所需的权限。	检查Cisco ISE 计算机帐户是否有权限获取 Active Directory 中的用户组。
系统运行状况		
高磁盘 I/O 利用率	Cisco ISE 系统遇到高磁盘 I/O 利用率。	检查系统是否有足够的资源。检查系统的实际工作量，例如，身份验证数量、分析器活动等。添加额外服务器以分配负载。
高磁盘空间利用率	Cisco ISE 系统遇到高磁盘空间利用率。	检查系统是否有足够的资源。检查系统的实际工作量，例如，身份验证数量、分析器活动等。添加额外服务器以分配负载。
高平均负载	Cisco ISE 系统遇到高平均负载。	检查系统是否有足够的资源。检查系统的实际工作量，例如，身份验证数量、分析器活动等。添加额外服务器以分配负载。 如果主 MNT 节点和辅助 MNT 节点的凌晨 2:00 时间戳出现对应的高平均负载警报，请注意，CPU 使用率可能由于在该小时运行 DBMS 统计信息而较高。当 DBMS 统计信息运行完成时，CPU 使用率将恢复正常。 高平均负载警报在每个星期日的凌晨 1:00 由每周维护任务触发。此维护任务将重新构建所有占用 1 GB 以上空间的索引。可以忽略此警报。
高内存利用率	Cisco ISE 系统遇到高内存利用率。	检查系统是否有足够的资源。检查系统的实际工作量，例如，身份验证数量、分析器活动等。添加额外服务器以分配负载。
高操作数据库使用率	Cisco ISE 监控节点遇到的系统日志数据量高于预期数据量。	检查并缩小操作数据的清除配置窗口。

警报名称	警报说明	警报解决方法
高身份验证延迟	Cisco ISE 系统遇到高身份验证延迟。	检查系统是否有足够的资源。检查系统的实际工作量，例如，身份验证数量、分析器活动等。添加额外服务器以分配负载。
运行状态不可用	监控节点未收到Cisco ISE 节点的运行状态。	确保Cisco ISE 节点正常运行，并能与监控节点通信。
进程已关闭	其中一个Cisco ISE 进程未运行。	重新启动Cisco ISE 应用。
已达到分析器队列大小限制	已达到 ISE 分析器队列大小限制。在达到队列大小限制后，收到的时间将被丢弃。	检查系统是否有足够的资源，并确保已启用终端属性过滤器。
已达到 OCSP 事务阈值	已达到OCSP 事务阈值。当内部 OCSP 服务达到较高流量时触发此警报。	检查系统是否有足够的资源。
许可		
许可证即将到期	Cisco ISE 节点上安装的许可证即将到期。	查看Cisco ISE 中的**许可 (Licencing)** 页面，可查看许可证使用情况。
许可证已过期	Cisco ISE 节点上安装的许可证已过期。	联系Cisco客户团队购买新许可证。
许可证违规	Cisco ISE 节点已检测到您超出或即将超出允许的许可证计数。	联系Cisco客户团队购买额外许可证。
智能许可授权已过期	智能许可的授权已过期。	请参阅**思科 ISE 许可管理 (Cisco ISE License Administration)** 窗口手动更新智能许可的注册，或检查与Cisco智能软件管理器的网络连接。如果问题仍然存在，请联系您的Cisco合作伙伴。
智能许可授权续订故障	从Cisco智能软件管理器更新授权失败。	请参阅**思科 ISE 许可证管理 (Cisco ISE License Administration)** 窗口，使用**许可证 (Licenses)** 表中的**刷新 (Refresh)** 按钮手动更新Cisco智能软件管理器的授权。如果问题仍然存在，请联系您的Cisco合作伙伴。

警报名称	警报说明	警报解决方法
智能许可授权续订成功	从Cisco智能软件管理器更新授权成功。	通知Cisco ISE 的Cisco智能软件管理器授权续订已成功。
智能许可通信故障	Cisco ISE 与Cisco智能软件管理器的通信失败。	检查与Cisco智能软件管理器的网络连接。如果问题依然存在，请登录Cisco智能软件管理器或联系您的Cisco合作伙伴。
智能许可通信已恢复	Cisco ISE 与Cisco智能软件管理器的通信已恢复。	通知与Cisco智能软件管理器的网络连接已恢复。
智能许可取消注册失败	从Cisco智能软件管理器取消注册Cisco ISE 失败。	请查看**思科 ISE 许可证管理 (Cisco ISE License Administration)** 窗口以了解详细信息。如果问题依然存在，请登录Cisco智能软件管理器或联系您的Cisco合作伙伴。
智能许可取消注册成功	从Cisco智能软件管理器取消注册Cisco ISE 成功。	通知从Cisco智能软件管理器取消注册Cisco ISE 成功。
智能许可已禁用	Cisco ISE 上的智能许可已禁用，正在使用传统许可。	请参阅**许可证管理 (License Administration)** 窗口以再次启用智能许可。请参阅《Cisco ISE 管理指南》或联系您的Cisco合作伙伴，以了解如何使用Cisco ISE 上的智能许可。
智能许可评估期已过期	智能许可的评估期已过期。	请参阅**思科 ISE 许可证管理 (Cisco ISE License Administration)** 窗口，以从Cisco智能软件管理器注册Cisco ISE。
智能许可 HA 角色已更改	在使用智能许可时已发生高可用性角色更改。	通知Cisco ISE 的高可用性角色已更改。
智能许可 Id 证书已过期	智能许可证书已过期。	请查看**思科 ISE 许可证管理 (Cisco ISE License Administration)** 窗口，以手动更新智能许可的注册。如果问题仍然存在，请联系您的Cisco合作伙伴。

警报名称	警报说明	警报解决方法
智能许可 Id 证书续签失败	在Cisco智能软件管理器上续签智能许可的注册失败。	请参阅**思科 ISE 许可证管理 (Cisco ISE License Administration)** 窗口，以手动更新智能许可的注册。如果问题仍然存在，请联系您的Cisco合作伙伴。
智能许可 Id 证书续签成功	在Cisco智能软件管理器上续签智能许可的注册成功。	通知Cisco智能软件管理器的注册续签成功。
智能许可无效请求	对Cisco智能软件管理器的请求无效。	请查看**思科 ISE 许可证管理 (Cisco ISE License Administration)** 窗口以了解详细信息。如果问题依然存在，请登录Cisco智能软件管理器或联系您的Cisco合作伙伴。
智能许可不合规	Cisco ISE 许可证不合规。	请查看 **ISE 许可证管理 (Cisco ISE License Administration)** 窗口以了解详细信息。联系您的合作伙伴或Cisco客户团队购买新许可证。
智能许可注册失败	将Cisco ISE 注册到Cisco智能软件管理器失败。	请查看 **ISE 许可证管理 (Cisco ISE License Administration)** 窗口以了解详细信息。如果问题依然存在，请登录Cisco智能软件管理器或联系您的Cisco合作伙伴。
智能许可注册成功	将Cisco ISE 注册到Cisco智能软件管理器成功。	通知将Cisco ISE 注册到Cisco智能软件管理器成功。
系统错误		
日志收集错误	Cisco ISE 监控收集器进程无法留存从策略服务节点生成的审核日志。	这不会影响策略服务节点的实际功能。如需进一步解决问题，请联系Cisco TAC。
计划的报告导出失败	无法将导出的报告（CSV 文件）复制到配置的存储库。	验证配置的存储库。如果存储库已删除，请重新添加存储库。如果存储库不可用或不可访问，请将其重新配置为有效存储库。
TrustSec		

警报名称	警报说明	警报解决方法
已调配未知 SGT	已调配未知 SGT。	ISE 将未知 SGT 调配为授权流程的一部分。不应将未知 SGT 分配为已知流程的一部分。
部分 TrustSec 网络设备没有最新的 ISE IP-SGT 映射配置	部分 TrustSec 网络设备没有最新的 ISE IP-SGT 映射配置。	ISE 识别出部分网络设备带有不同的 IP-SGT 映射集。使用 **IP-SGT 映射部署 (IP-SGT Mapping Deploy)** 选项更新这些设备。
TrustSec SSH 连接失败	TrustSec SSH 连接失败。	ISE 无法建立与网络设备的 SSH 连接。在**网络设备 (Network Device)** 窗口检查网络设备 SSH 凭证是否与在网络设备上配置的凭证类似。检查网络设备是否已启用从 ISE（IP 地址）进行 SSH 连接。
TrustSec 识别出 ISE 被设置为与版本 1.0 以外的 TLS 版本配合使用	TrustSec 识别出 ISE 设置为与版本 1.0 以外的 TLS 版本配合使用。	TrustSec 仅支持 TLS 版本 1.0。
TrustSec PAC 验证失败	TrustSec PAC 验证失败。	ISE 无法验证网络设备发送的 PAC。在**网络设备 (Network Device)** 窗口以及设备 CLI 检查 Trustsec 设备凭证。确保设备使用由 ISE 服务器调配的有效 PAC。
TrustSec 环境数据下载失败	Trustsec 环境数据下载失败。	Cisco ISE 收到非法的环境数据请求。 请验证以下项目： • PAC 存在于该请求中且有效。 • 所有属性均存在于该请求中。
已忽略 TrustSec CoA 消息	已忽略 TrustSec CoA 消息。	Cisco ISE 已发送 TrustSec CoA 信息，但尚未收到响应。验证网络设备是否支持 CoA。查看网络设备配置。

警报名称	警报说明	警报解决方法
TrustSec 默认出口策略被更改	TrustSec 默认出口策略被更改。	TrustSec 默认出口策略单元格被更改。请确保它与您的安全策略一致。

注释 当您将用户或终端添加到思科 ISE 时，系统不会触发警报。

警报设置

下表说明了**警报设置 (Alarm Settings)** 窗口（ 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **设置 (Settings)** > **警报设置 (Alarm Settings)** > **警报配置 (Alarm Configuration)** > **添加 (Add)**）

字段名称	说明
警报类型	警报类型。
警报名称	警报的名称。
说明	警报说明。
建议的操作	触发警报时要执行的操作。
状态	启用或禁用警报规则。
严重性	选择警报的严重性级别。有效的选项包括： • “严重”(Critical)：指示严重错误情况。 • “警告”(Warning)：指示正常但重要的情况。这是默认情况。 • “信息”(Info)：指示信息性的消息。
发出系统日志消息	为Cisco ISE 生成的每个系统警报发送系统日志消息。
输入以逗号分隔的多个电子邮件 **(Enter multiple e-mails separated with comma)**	电子邮件地址或 ISE 管理员名称（或二者）的列表。
电子邮件中的备注（**0** 到 **4000** 个字符）	您希望与系统警报关联的自定义文本消息。

添加自定义报警

Cisco ISE 包含 12 个默认报警类型，例如高内存利用率和配置更改。Cisco定义的系统警报列在**警报设置 (Alarm Settings)** 窗口（在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **设置 (Settings)** > **警报设置 (Alarm Settings)**）。您只能编辑系统报警。

除现有系统警报外，还可以在现有警报类型下添加、编辑或删除自定义警报。

对于每种警报类型，最多可以创建五个警报。警报总数限制为 200。

在**警报设置 (Alarm Settings)** 窗口的**警报配置 (Alarm Configuration)** 选项卡中，**条件 (Conditions)** 列显示以下四个警报的详细信息：高身份验证延迟 (High Authentication Latency)、高磁盘 I/O 利用率 (High Disk I/O Utilization)、高磁盘空间利用率 (High Disk Space Utilization) 和高内存利用率 (High Memory Utilization)。其中，每个警报都有一个可配置的阈值。但是，即使已配置阈值，**条件 (Conditions)** 列也可能不显示详细信息。在这种情况下，请重新编辑警报的相关阈值字段，以查看**条件 (Conditions)** 列中的详细信息。

要添加报警，请按以下步骤操作：

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **设置 (Settings)** > **警报设置 (Alarm Settings)**

步骤 2 在**报警配置 (Alarm Configuration)** 选项卡中，点击**添加 (Add)**。

步骤 3 输入必要的详细信息。请参阅警报设置部分了解详细信息。

基于报警类型（高内存利用率 (High Memory Utilization)、RADIUS 身份验证尝试次数过多 (Excessive RADIUS Authentication Attempts)、TACACS 身份验证尝试次数过多 (Excessive TACACS Authentication Attempts) 等），**警报配置 (Alarm Configuration)** 窗口中会显示其他属性。例如，会为“配置更改”(Configuration Change) 警报显示**对象名称 (Object Name)** 和**对象类型 (Object Type)** 和**管理员名称 (Admin Name)** 字段。您可以为规定不同条件的相同报警添加多个实例。

步骤 4 点击**提交 (Submit)**。

思科 ISE 警报通知和阈值

您可以启用或禁用Cisco ISE 警报，并且配置警报通知行为以通知紧急状况。对于某些警报，您可以配置阈值，如“尝试失败次数过多”(Excessive Failed Attempts) 警报的最大失败尝试次数或“磁盘利用率高”(High Disk Utilization)警报的最大磁盘利用率。

您可以针对每个警报分别配置通知设置。可以输入每个警报（系统定义警报和用户定义警报）所需要通知的用户的电子邮件 ID。

注释 在警报规则级别指定的收件人邮件地址会覆盖全局收件人邮件地址设置。

启用和配置警报

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **设置 (Settings)** > **警报设置 (Alarm Settings)**。

步骤 2 从默认警报列表选择警报，点击**编辑 (Edit)**。

步骤 3 选择 **Enable** 或 **Disable**。

步骤 4 如果适用，则配置警报阈值。

步骤 5 点击**提交 (Submit)**。

用于监控的思科 ISE 警报

Cisco ISE 提供系统警报以通知您所发生的各种严重系统状况。由Cisco ISE 生成的警报在 Alarm dashlet 中显示。Alarm dashlet 中自动显示这些通知。

Alarm dashlet 显示最近警报的列表，您可以从列表中选择查看警报详细信息。您可以通过邮件和系统日志消息接收警报通知。

查看监控警报

步骤 1 转至Cisco ISE **Dashboard**。

步骤 2 在**警报 (Alarms)** Dashlet 中点击警报。系统会打开一个新窗口，其中显示警报详细信息和建议的措施。

步骤 3 点击 **Refresh** 以刷新警报。

步骤 4 将警报标记为已读以确认警报，减少警报计数（发出警报的次数）。可以通过选中时间戳旁边的复选框来选择要确认的警报。

从**确认 (Acknowledge)** 下拉列表中选择**确认所选 (Acknowledge Selected)**，将当前显示在窗口中的所有警报标记为已读。默认情况下，窗口中显示 100 行。可以通过从**行数/页数 (Rows/Page)** 下拉列表中选择所需的值来选择要显示的不同行数。

从**确认 (Acknowledge)** 下拉列表中选择**全部确认 (Acknowledge All)**，将列表中的所有警报标记为已读（无论这些警报当前是否显示在窗口中）。

注释　选中标题行中**时间戳 (Time Stamp)** 旁边的复选框后，将选择窗口中显示的所有警报。但是，如果之后取消选中一个或多个所选警报的复选框，则全选功能将失效。此时**时间戳 (Time Stamp)** 旁的复选框处于取消选中状态。

步骤 5 点击与您所选择的警报对应的 **Details** 链接。系统将打开一个新窗口，其中显示与所选警报对应的详细信息。

注释　与在角色更改之前生成的警报对应的**详细信息 (Details)** 链接不显示任何数据。

日志收集

监控服务收集日志和配置数据，存储数据，然后处理数据，以生成报告和警报。您可以查看从部署中的任何服务器收集的日志详情。

警报系统日志收集位置

如果将监控功能配置为将警报通知作为系统日志消息发送，您需要提供一个接收通知的系统日志目标。警报系统目标即发送警报系统日志消息的目标位置。

注释 Cisco ISE 监控要求日志记录源接口配置使用网络接入服务器 (NAS) IP 地址。您必须为Cisco ISE 监控配置交换机。

您还必须有一个配置为系统日志服务器的系统，才能接受系统日志消息。您可以创建、编辑和删除警报系统日志目标。

要将远程日志记录目标配置为警报目标，请执行此程序。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **日志记录 (Logging)** > **远程日志记录目标 (Remote Logging Targets)**。

步骤 2 点击**添加 (Add)**。

步骤 3 在**新建日志记录目标 (New Logging Target)** 窗口中，提交日志记录目标所需的详细信息，并选中**包括此目标的警报 (Include Alarms for this Target)** 复选框。

RADIUS 实时日志

下表介绍“实时日志”(Live logs) 窗口中的字段，其中显示最近的 RADIUS 身份验证。在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **操作 (Operations)** > **RADIUS** > **实时日志 (Live Logs)**。只能在主 PAN 中查看 RADIUS 实时日志。

表 *2: RADIUS* 实时日志

字段名称	说明描述
时间 (Time)	显示监控和故障排除收集代理接收日志的时间。此列为必选项，无法取消选择。
状态 (Status)	显示身份验证是否成功。此列为必选项，无法取消选择。绿色用于代表已通过的身份验证。红色用于代表失败的身份验证。

字段名称	说明描述
详细信息 **(Details)**	点击“详细信息”(Details) 列下的图标可在新浏览器窗口中打开**身份验证详细报告 (Authentication Detail Report)**。此报告提供有关身份验证和相关属性以及身份验证流程的信息。在**身份验证详细信息 (Authentication Details)** 框中，**响应时间 (Response Time)** 是Cisco ISE 处理身份验证流程所需的总时间。例如，如果身份验证包含三个往返消息，初始消息花费 300 毫秒，下一条消息花费 150 毫秒，最后一条消息花费 100 毫秒，则**响应时间 (Response Time)** 为 300 + 150 + 100 = 550 毫秒。 **注释** 您无法查看活动时间超过 48 小时的终端的详细信息。当点击活动时间超过 48 小时的终端的**详细信息 (Details)** 图标时，可能会看到一个包含以下消息的页面：此记录无可用数据。(No Data available for this record.) 数据可能已清除或此会话记录的身份验证发生在一周之前。(Either the data is purged or authentication for this session record happened a week ago.) 或者，如果这是“PassiveID”或“PassiveID 可视性”(PassiveID Visibility) 会话，则不会有 ISE 身份验证详细信息，只有会话。(Or if this is an 'PassiveID' or 'PassiveID Visibility' session, it will not have authentication details on ISE but only the session.)
重复次数 (Repeat Count)	显示过去 24 小时内身份验证请求的重复次数，它们在身份、网络设备和授权方面没有任何变化。

字段名称	说明描述
身份 (Identity)	显示与身份验证关联的已登录用户名。 如果用户名不存在于任何 ID 存储区中，则显示为 INVALID。如果身份验证由于任何其他原因而失败，则显示为 USERNAME。 **注释** 这仅适用于用户。这不适用于 MAC 地址。 为了帮助进行调试，可以强制Cisco ISE 显示无效的用户名。为此，请选中位于以下路径下方的**披露无效用户名 (Disclose Invalid Usernames)** 复选框： **管理 (Administration)** > **系统 (System)** > **设置 (Settings)** > **安全设置 (Security Settings)**。您还可以将**披露无效用户名 (Disclose Invalid Usernames)** 选项配置为超时，这样就不必手动将其关闭。
终端 ID (Endpoint ID)	显示终端的唯一标识符，通常是 MAC 或 IP 地址。
终端配置文件 (Endpoint Profile)	显示所分析的终端的类型，例如分析为 iPhone、Android、MacBook、Xbox 等。
身份验证策略 (Authentication Policy)	显示为特定身份验证选择的策略的名称。
授权策略 (Authorization Policy)	显示为特定授权选择的策略的名称。
授权配置文件 (Authorization Profiles)	显示用于身份验证的授权配置文件。
IP 地址 (IP Address)	显示终端设备的 IP 地址。
网络设备 (Network Device)	显示网络访问设备的 IP 地址。
设备端口 (Device Port)	显示终端连接的端口号。
身份组 (Identity Group)	显示分配给生成了日志的用户或终端的身份组。
终端安全评估状态 (Posture Status)	显示安全评估验证的状态和身份验证的详细信息。
服务器 (Server)	指示生成日志的策略服务。
MDM 服务器名称 (MDM Server Name)	显示 MDM 服务器的名称。
事件 (Event)	显示事件状态。
故障原因 (Failure Reason)	如果身份验证失败，显示失败的详细原因。

字段名称	说明描述
身份验证方法 (Auth Method)	显示 RADIUS 协议（例如 Microsoft 质询握手身份验证协议版本 2 (MS-CHAPv2)、IEEE 802.1x 或 dot1X 等）使用的身份验证方法。
身份验证协议 (Authentication Protocol)	显示所使用的身份验证协议，例如受保护的可扩展身份验证协议 (PEAP) 和可扩展身份验证协议 (EAP) 等等。
安全组 (Security Group)	显示由身份验证日志标识的组。
会话 ID (Session ID)	显示会话 ID。

注释 在 **RADIUS 实时日志 (RADIUS Live Logs)** 和 **TACACS+ 实时日志 (TACACS+ Live Logs)** 窗口中，系统会为每个策略授权规则的第一个属性显示一个“已查询 PIP”(Queried PIP) 条目。如果授权规则中的所有属性都与已为之前的规则查询的字典相关，则不会显示其他“已查询 PIP”(Queried PIP) 条目。

您可以在 RADIUS **实时日志 (Live Logs)** 窗口中执行以下操作：

- 将数据导出为 CSV 或 PDF 格式。
- 根据要求显示或隐藏列。
- 使用快速或自定义过滤器过滤数据。您也可以保存过滤器供以后使用。
- 重新排列列并调整列宽。
- 对列值排序。

注释 所有用户自定义将存储为用户首选项。

TACACS 实时日志

下表列出“TACACS+ 实时日志”(TACACS Live Logs) 页面的字段，此页面显示 TACACS+ AAA 详细信息。在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **操作 (Operations)** > **TACACS** > **实时日志 (Live Logs)**。您只能在主 PAN 中查看 TACACS 实时日志。

表 *3: TACACS* 实时日志

字段名称	使用指南
生成时间 (Generated Time)	根据特定事件触发时间显示系统日志生成时间。

字段名称	使用指南
日志记录时间 **(Logged Time)**	显示监控节点处理和存储系统日志的时间。此列为必选项，无法取消选择。
状态 **(Status)**	显示身份验证是否成功。此列为必选项，无法取消选择。绿色用于代表已通过的身份验证。红色用于代表失败的身份验证。
详细信息 **(Details)**	在点击放大镜图标时显示报告，使您能够深入查看有关所选身份验证方案的更多详细信息。此列为必选项，无法取消选择。
会话密钥 **(Session Key)**	显示由 ISE 返回到网络设备的会话密钥（在 EAP 成功或 EAP 失败消息中查找）。
用户名 **(Username)**	显示设备管理员的用户名。此列为必选项，无法取消选择。
类型 **(Type)**	包括两种类型 - 身份验证和授权。显示身份验证已通过和/或失败的用户名。此列为必选项，无法取消选择。
身份验证策略 **(Authentication Policy)**	显示为特定身份验证选择的策略的名称。
授权策略 **(Authorization Policy)**	显示为特定授权选择的策略的名称。
ISE 节点 **(ISE Node)**	显示处理访问请求的 ISE 节点的名称。
网络设备名称 **(Network Device Name)**	显示网络设备的名称。
网络设备 **IP (Network Device IP)**	显示访问请求已处理的网络设备的 IP 地址。
网络设备组 **(Network Device Groups)**	显示网络设备所属相应网络设备组的名称。
设备类型 **(Device Type)**	显示用于处理来自不同网络设备的访问请求的设备类型。
位置 **(Location)**	显示用于处理来自网络设备的访问请求的基于位置的策略。
设备端口 **(Device Port)**	显示发出访问请求的设备端口号。
故障原因 **(Failure Reason)**	显示拒绝网络设备发出的访问请求的原因。
远程地址 **(Remote Address)**	显示唯一标识终端站的 IP 地址、MAC 地址，或任何其他字符串。

字段名称	使用指南
匹配的命令集 (Matched Command Set)	如果 MatchedCommandSet 属性值存在，则显示该值，或如果 MatchedCommandSet 属性值为空或属性本身不存在于系统日志，则显示一个空值。
外壳配置文件 (Shell Profile)	显示已授予设备管理员用于在网络设备执行命令的权限。

您可以在 TACACS 实时日志页面执行以下操作：

- 将数据导出为 CSV 或 PDF 格式。
- 根据要求显示或隐藏列。
- 使用快速或自定义过滤器过滤数据。您也可以保存过滤器供以后使用。
- 重新排列列并调整列宽。
- 对列值排序。

注释 所有用户自定义将存储为用户首选项。

相关主题

TACACS+ 设备管理
配置全局 TACACS+ 设置

实时身份验证

您可以在**实时身份验证 (Live Authentications)** 窗口实时监控最近发生的 RADIUS 身份验证。此窗口显示最近 24 小时内发生的前 10 项 RADIUS 身份验证。此节说明**实时身份验证 (Live Authentications)** 窗口的功能。

实时身份验证 (Live Authentications) 窗口显示与所发生的身份验证事件对应的实时身份验证条目。除了身份验证条目之外，此窗口还显示与这些事件对应的实时会话条目。您还可以向下钻取会话，查看与该会话对应的详细报告。

此**实时身份验证 (Live Authentications)** 窗口提供一个按所发生时间排序的最近 RADIUS 身份验证的表格说明。**实时身份验证 (Live Authentications)** 窗口底部显示的最近更新会显示服务器日期、时间和时区。

注释 如果 Access-Request 数据包中的密码属性为空，则会触发错误消息，访问请求将失败。

一个终端身份验证成功时，**实时身份验证 (Live Authentications)** 窗口会显示两个条目：一个条目对应身份验证记录，另一个条目对应会话记录（从会话实时视图下拉）。随后，当设备进行其他身份验证成功时，与会话记录对应的重复次数计数器会递增其次数。在**实时身份验证 (Live Authentications)** 窗口显示的重复次数计数器会显示所抑制的重复 RADIUS 身份验证成功消息的数量。

请参阅默认情况下显示的实时身份验证数据类别。“最近的 RADIUS 身份验证”(Recent RADIUS Authentications) 部分中说明了这些类别。

您可以选择查看所有列，也可以只显示所选择的数据列。在选择您想要显示的列之后，您可以保存您的选择。

监控实时身份验证

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **操作 (Operations)** > **RADIUS** > **实时日志 (Live logs)**

步骤 2 从**刷新 (Refresh)** 下拉列表中，选择更改数据刷新率的间隔。

步骤 3 点击**刷新 (Refresh)** 图标手动更新数据。

步骤 4 从**显示 (Show)** 下拉列表中，选择一个选项以更改显示的记录数量。

步骤 5 从**时间范围 (Within)** 下拉列表中，选择一个选项以指定时间间隔。

步骤 6 点击**添加或删除列 (Add or Remove Columns)** 并从下拉列表中选择选项以更改所显示的列。

步骤 7 点击下拉列表底部的**保存 (Save)** 以保存您的修改。

步骤 8 点击**显示实时会话 (Show Live Sessions)** 以查看实时 RADIUS 会话。

您可以使用实时会话的动态授权更改 (CoA) 功能，使您可以动态控制活动的 RADIUS 会话。您可以向网络接入设备 (NAD) 发送重新身份验证或断开连接请求。

在 实时身份验证 页面过滤数据

使用实时身份验证页面中的过滤器，可以过滤出您需要的信息，快速排除网络身份验证问题。您可以在身份验证（实时日志）页面筛选记录，只查看那些您感兴趣的记录。身份验证日志包含许多详细信息，过滤特定用户或位置的身份验证信息有助于您快速扫描数据。您可以使用实时身份验证页面的字段中可用的若干运算符，根据搜索条件筛选记录。

- “abc”：包含“abc”
- “!abc”：不包含“abc”
- “{}”：为空
- “!{}”：不为空
- “abc*”：以“abc”开头
- “*abc”：以“abc”结束
- “\!”、“*”、“\{”、“\\”：转义

通过 Escape 选项，您可以筛选包含特殊字符的文本（包括用作过滤器的特殊字符）。您必须将反斜线 (\) 放在特殊字符的前面。例如，如果您要查看身份为“Employee!”的用户的身份验证记录，请在**身份过滤器 (Identity Filter)** 文本框中输入“Employee\!”。在此例中，Cisco ISE 考虑将感叹号 (!) 作为文字字符，而不是作为特殊字符。

此外，使用**状态 (Status)** 字段您可以筛选出仅成功的身份验证记录、失败的身份验证、实时会话，等等。绿色复选标记会筛选过去发生的所有成功身份验证。红色十字标记会筛选所有失败身份验证。蓝色 i 图标会筛选所有实时会话。您还可以选择查看这些选项的组合。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **操作 (Operations)** > **RADIUS** > **实时日志 (Live logs)**

步骤 2 根据 Show Live Authentications 页面中的任意字段筛选数据。

您可以根据成功或失败身份验证，或实时会话筛选结果。

RADIUS实时会话 (Live Sessions)

下表说明了 RADIUS **实时会话 (Live Sessions)** 窗口中的字段，此窗口显示实时身份验证。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择您仅可在主 PAN 上查看 RADIUS 实时会话。

表 *4: RADIUS* 实时会话

字段名称	说明
启动时间 (Initiated)	显示启动会话时的时间戳。
已更新 (Updated)	显示会话上次由于更改而更新时的时间戳。
帐户会话时间 (Account Session Time)	显示用户会话的时间跨度（秒）。
会话状态 (Session Status)	显示终端设备的当前状态。
操作 (Action)	点击**操作 (Actions)** 图标可对活动 RADIUS 会话重新进行身份验证或断开活动 RADIUS 会话连接。
重复次数 (Repeat Count)	显示用户或终端重新进行身份验证的次数。
终端 ID	显示终端的唯一标识符，通常是 MAC 或 IP 地址。
身份 (Identity)	显示终端设备的用户名。
IP 地址 (IP Address)	显示终端设备的 IP 地址。
审核会话 ID (Audit Session ID）	显示唯一会话标识符。

字段名称	说明
帐户会话 ID (Account Session ID)	显示网络设备提供的唯一 ID。
终端配置文件	显示设备的终端配置文件。
终端安全评估状态 (Posture Status)	显示安全评估验证的状态和身份验证的详细信息。
安全组 (Security Group)	显示由身份验证日志标识的组。
服务器 (Server)	指示已从中生成日志的策略服务节点。
身份验证方法 (Auth Method)	显示RADIUS协议使用的身份验证方法，例如密码身份验证协议 (PAP)、质询握手身份验证协议 (CHAP)、IEE 802.1x 或 dot1x 等等。
身份验证协议 (Authentication Protocol)	显示所使用的身份验证协议，例如受保护的可扩展身份验证协议 (PEAP) 和可扩展身份验证协议 (EAP) 等等。
身份验证策略 (Authentication Policy)	显示为特定身份验证选择的策略的名称。
授权策略 (Authorization Policy)	显示为特定授权选择的策略的名称。
授权配置文件 (Authorization Profiles)	显示用于身份验证的授权配置文件。
NAS IP 地址 (NAS IP Address)	显示网络设备的 IP 地址。
设备端口 (Device Port)	显示网络设备的连接端口。
PRA 操作 (PRA Action)	显示客户端在网络上成功通过合规性验证后，在客户端上采取的定期重评估操作。
ANC 状态 (ANC Status)	设备的自适应网络控制状态，如“隔离”(Quarantine)、“取消隔离”(Unquarantine) 或“关闭”(Shutdown)。
WLC 漫游 (WLC Roam)	显示用于跟踪已在漫游期间从一个 WLC 传递到另一个 WLC 的终端的布尔值 (Y/N)。它的值为 cisco-av-pair=nas-update =Y 或 N。 **注释** Cisco ISE 依靠 WLC 中的 nas-update=true 属性识别会话是否处于漫游状态。当原始 WLC 在 nas-update=true 时发送记账停止属性时，不会在ISE中删除会话，以避免重新进行身份验证。如果漫游失败，ISE 将在会话处于非活动状态五天后清除该会话。

字段名称	说明
接收的数据包 (Packets In)	显示接收的数据包数量。
发送的数据包 (Packets Out)	显示发送的数据包数量。
接收的字节 (Bytes In)	显示接收的字节数。
发送的字节 (Bytes Out)	显示发送的字节数。
会话源 (Session Source)	指示它是 RADIUS 会话还是被动 ID 会话。
用户域名 (User Domain Name)	显示用户的注册 DNS 名称。
主机域名 (Host Domain Name)	显示主机的注册 DNS 名称。
用户 NetBIOS 名称 (User NetBIOS Name)	显示用户的 NetBIOS 名称。
主机 NetBIOS 名称 (Host NetBIOS Name)	显示主机的 NetBIOS 名称。
许可证类型 (License Type)	显示使用的许可证类型。
许可证详细信息 (License Details)	显示许可证详细信息。
提供程序 (Provider)	终端活动获悉自不同的系统日志源。这些系统日志源称为提供程序。 • Windows Management Instrumentation (WMI) - WMI 是一种 Windows 服务，用于提供通用接口和对象模型来访问有关操作系统、设备、应用和服务的管理信息。 • 代理：代表客户端或另一个程序在客户端上运行的程序。 • 系统日志：客户端发送事件消息的日志记录服务器。 • REST：客户端通过终端服务器进行身份验证。对于此系统日志源，将会显示“TS代理ID”、“源端口开始时间”、“源端口结束时间”和“源第一个端口”值。 • SPAN：使用 SPAN 探测器发现的网络信息。 • DHCP：DHCP 事件。 • 终端 **注释** 从终端会话获悉来自不同提供程序的两个事件后，提供程序在实时会话页面中显示为逗号分隔值。

字段名称	说明
MAC 地址 (MAC Address)	显示客户端的 MAC 地址。
终端检查时间	显示终端探测器上次检查终端的时间。
终端检查结果	显示终端探测的结果。可能的值包括： • 无法接通 • 用户退出 • 活动用户
起始源端口 (Source Port Start)	（仅为 REST 提供程序显示值）显示端口范围中的第一个端口号。
结束源端口	（仅为 REST 提供程序显示值）显示端口范围中的最后一个端口号。
源第一个端口 (Source First Port)	（仅为 REST 提供程序显示值）显示由终端服务器代理分配的第一个端口。 终端服务器指允许多个终端在无需调制解调器或网络接口的情况下连接到其上的服务器或网络设备，可实现多个终端到 LAN 网络的连接。多个终端可能会有相同的 IP 地址，因此难以识别特定用户的 IP 地址。所以，为了识别特定用户，需在服务器上安装终端服务器代理，为每个用户分配一个端口范围。这有助于创建 IP 地址-端口用户映射。
TS 代理 ID (TS Agent ID)	（仅为 REST 提供程序显示值）显示安装在终端上的终端服务器代理的唯一标识。
AD 用户解析的身份 (AD User Resolved Identities)	（仅为 AD 用户显示值）显示匹配的潜在账户。
AD 用户解析的 DN (AD User Resolved DNs)	（仅为 AD 用户显示值）显示 AD 用户的可分辨名称，例如 CN=chris,CN=Users,DC=R1,DC=com

相关主题

更改 RADIUS 会话的授权

思科 ISE 活动 RADIUS 会话

导出摘要

您可以查看过去 7 天内所有用户导出的报告的详细信息以及状态。导出摘要包括手动报告和已计划的报告。导出摘要页面每 2 分钟自动刷新一次。点击刷新图标可手动刷新导出摘要页面。

超级管理员可以取消正在进行或处于排队状态的导出进程。其他用户只能取消他们发起的导出进程。

默认情况下，在给定的时间点只能运行 3 次报告手动导出，其余触发的报告手动导出将排队。计划导出的报告没有此类限制。

注释 当思科 ISE 服务器重新启动时，所有处于排队状态的报告都将重新安排，处于正在进行或正在取消状态的报告将标记为失败。

注释 如果主 MnT 节点关闭，则已计划的报告导出作业将在辅助 MnT 节点上运行。

下表列出“导出摘要”(Export Summary) 页面中的字段。 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **操作 (Operations)** > **报告 (Reports)** > **导出摘要 (Export Summary)**。

表 *5:* 导出摘要

字段名称	说明
报告已导出	显示报告的名称。
导出依据	显示发起导出进程的用户的角色。
已计划	显示报告导出是否为计划性导出。
触发于	显示在系统中触发导出进程的时间。
存储库	显示将存储导出数据的存储库的名称。
过滤器参数	显示导出报告时选择的过滤器参数。

字段名称	说明
状态	显示导出的报告的状态。它可以是下列类型之一： • 已排队 • 正在进行 • 已完成 • 正在取消 • 已取消 • 失败 • 已跳过 注释 失败状态指示失败的原因。已跳过状态指示当主 MnT 节点关闭时，跳过了计划的报告导出。

您可以在“导出摘要”(Export Summary) 页面中执行以下操作：

- 根据要求显示或隐藏列。
- 使用快速或自定义过滤器过滤数据。您也可以保存过滤器供以后使用。
- 重新排列列并调整列宽。

身份验证摘要报告

您可以根据与身份验证请求相关的属性，针对具体用户、设备或搜索条件对网络接入进行故障排除。您可以通过运行“身份验证摘要”(Authentication Summary) 报告实现此目标。

网络接入问题故障排除

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **操作 (Operations)** > **报告 (Reports)** > **报告 (Reports)** > **设备管理 (Device Administration)** > **身份验证摘要报告 (Authentication Summary Report)**。

步骤 2 过滤报告以了解故障原因。

步骤 3 查看报告中 Authentication by Failure Reasons 部分的数据以对您的网络访问问题进行故障排除。

注释 由于身份验证摘要报告会收集和显示与失败或成功的身份验证对应的最新数据，所以报告内容会延迟几分钟后显示。

部署和支持信息的思科支持诊断

概述

Cisco Support Diagnostics Connector 是一项新功能，可帮助Cisco技术支持中心 (TAC) 和Cisco支持工程师从主管理节点获取部署信息。TAC 可以通过连接器获取部署中任何特定节点的支持信息。这些数据有助于更快、更准确地进行故障排除。

您可以通过Cisco ISE 管理门户启用 Cisco Support Diagnostics Connector。利用安全服务交换 (SSE) 云门户，此功能允许在部署中的主策略管理节点与 Cisco Support Diagnostics 之间建立双向连接。

前提条件

- 您必须具有超级管理员或系统管理员角色才能启用或禁用 Cisco Support Diagnostics。

配置 Cisco Support Diagnostics Connector

启用 Cisco Support Diagnostics 功能：

- 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **设置 (Settings)** > **网络成功诊断 (Network Success Diagnostics)** > **Cisco Support Diagnostics** > **Cisco Support Diagnostics 设置 (Cisco Support Diagnostics Setting)**。
- 默认情况下会禁用此功能。否则，请选中**启用 Cisco Support Diagnostics (Enable Cisco Support Diagnostics)** 复选框以激活 Cisco Support Diagnostics。

验证 Cisco Support Diagnostics 双向连接

要验证Cisco ISE 是否已成功注册/注册 Cisco Support Diagnostics，以及是否已通过安全服务交换门户建立双向连接，请执行以下操作：

- 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **操作 (Operations)** > **报告 (Reports)** > **报告 (Reports)** > **审核 (Audit)** > **更改配置审核 (Change Configuration Audit)**。
- 查找以下事件报告：

  1. Cisco Support Diagnostics 已启用。
  2. ISE 服务器已注册到 Cisco Support Diagnostics。
  3. ISE SSE 服务已登记到 Cisco Support Diagnostics。
  4. Cisco Support Diagnostics 双向连接已启用。

- 您还可以转到“操作审核”(Operations Audit) 窗口 （在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **操作 (Operations)** > **报告 (Reports)** > **报告 (Reports)** > **审核 (Audit)** > **操作审核 (Operations Audit)**），了解作为 Cisco Support Diagnostics 组成部分启用、禁用、注册、取消注册、登记或取消登记的服务的详细信息。

故障排除信息。

如果 Cisco Support Diagnostics 双向连接显示为断开，请检查以下项目：

- **智能许可**：禁用智能许可会自动禁用 Cisco Support Diagnostics。重新启用智能许可以启用连接器。
- **与安全服务交换云的连接**：启用 Cisco Support Diagnostics 后，Cisco ISE 会持续检查与安全服务交换门户建立的持久连接。如果发现此连接断开，则会触发以下严重警报：“警报：Cisco Support Diagnostics 双向连接断开”(Alarms: The Cisco Support Diagnostics bi-directional connectivity is broken)。使用前面提供的配置步骤重新启用该功能。
-

相关信息

管理员可以使用 ERS API 执行以下特定任务：

- 触发特定节点上的支持信息。
- 获取已触发的支持捆绑包的状态。
- 下载支持捆绑包。
- 提取部署信息。

有关使用情况和其他信息，请参阅 ERS SDK 页面。

故障排除诊断工具

诊断工具可帮助您诊断Cisco ISE 网络上的问题并进行故障排除，同时提供关于如何解决问题的详细说明。您可以使用这些工具对身份验证进行故障排除并评估您网络上包括 Trustsec 设备在内的任何网络设备的配置。

RADIUS 身份验证故障排除工具

当身份验证结果不是预期结果时，可使用此工具搜索并选择 RADIUS 身份验证或与 RADIUS 身份验证相关的 Active Directory，以进行故障排除。如果希望通过身份验证但却未通过，或者希望用户或计算机具有特定级别的权限但用户或计算机没有这些权限，请使用此工具。

- 根据用户名、终端 ID、网络访问服务 (NAS) IP 地址和身份验证失败原因搜索 RADIUS 身份验证以排除故障时，Cisco ISE 只显示系统（当前）日期的身份验证。
- 根据 NAS 端口搜索 RADIUS 身份验证以排除故障时，Cisco ISE 显示自上个月初至当前日期的所有 NAS 端口值。

注释 根据 NAS IP 地址和终端 ID 字段搜索 RADIUS 身份验证时，先在操作数据库中执行搜索，然后在配置数据库中执行搜索。

对意外 RADIUS 身份验证结果进行故障排除

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **操作 (Operations)** > **故障排除 (Troubleshoot)** > **诊断工具 (Diagnostic Tools)** > **常规工具 (General Tools** > **RADIUS 身份验证故障排除 (RADIUS Authentication Troubleshooting)**。

步骤 2 根据需要在字段中指定搜索条件。

步骤 3 点击 **Search** 以显示与您的搜索条件匹配的 RADIUS 身份验证。

如果要搜索 AD 相关的身份验证，但在部署中未配置 Active Directory 服务器，则系统将显示消息：“未配置 AD”(AD not configured)。

步骤 4 从表格中选择 RADIUS 身份验证记录，并点击 **Troubleshoot**。

如果需要对 AD 相关的身份验证进行故障排除，请访问**管理 (Administration)** > **身份管理 (Identity Management)** > **外部身份源 (External Identity Sources)** > **Active Directory** > **AD 节点 (AD node)** 下的“诊断工具”(Diagnostics Tool)。

步骤 5 点击**需要用户输入 (User Input Required)**，根据需要修改字段，然后点击**提交 (Submit)**。

步骤 6 点击 **Done**。

步骤 7 故障排除完成后，点击 **Show Results Summary**。

步骤 8 若要查看诊断、为解决问题而采取的步骤以及故障排除摘要，请点击**完成 (Done)**。

执行网络设备命令诊断工具

执行网络设备命令诊断工具允许您在任何网络设备上运行 **show** 命令。

显示的结果与您应在控制台上看到的结果相同。通过此工具，您可以发现设备配置中的任何问题。

使用此工具可验证任何网络设备的配置，也可以使用此工具了解网络设备的配置方式。

要访问执行网络设备命令诊断工具，请选择以下导航路径之一：

- 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **操作 (Operations)** > **故障排除 (Troubleshoot)** > **诊断工具 (Diagnostic Tools)** > **执行网络设备命令 (Execute Network Device Command)**。
- 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **解析器 (Profiler)** > **故障排除 (Troubleshoot)** > **执行网络设备命令 (Execute Network Device Command)**。

在显示的**执行网络设备命令 (Execute Network Device Command)** 窗口中，在相应字段中输入网络设备的 IP 地址和您想要运行的 show 命令。点击**运行 (Run)**。

执行思科 IOS show 命令以检查配置

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **操作 (Operations)** > **故障排除 (Troubleshoot)** > **诊断工具 (Diagnostic Tools)** > **常规工具 (General Tools)** > **执行网络设备命令 (Execute Network Device Command)**。

步骤 2 在相应字段中输入信息。

步骤 3 点击**运行 (Run)** 以在指定网络设备上执行此命令。

步骤 4 点击**需要用户输入 (User Input Required)**，必要时修改字段。

步骤 5 点击 **提交 (Submit)** 以在网络设备上运行命令，然后查看输出。

评估配置验证程序工具

可以使用此诊断工具评估网络设备的配置并确定配置问题（如果有）。Expert Troubleshooter 会将设备的配置与标准配置进行比较。

无代理终端安全状态故障排除

“无代理终端安全评估”(Agentless Posture) 报告是当无代理终端安全评估未按预期工作时使用的主要故障排除工具。此报告显示无代理流的各个阶段，包括脚本上传完成、脚本上传失败、脚本执行完成等事件，以及任何已知的失败原因。

您可以从两个位置访问无代理终端安全评估故障排除：

- 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **操作 (Operations)** > **实时日志 (Live Logs)**：在要进行故障排除的客户端的“终端安全评估状态”(Posture Status) 列上，点击三个竖点。
- 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **操作 (Operations)** > **故障排除 (Troubleshoot)** > **诊断 (Diagnostic)** > **常规工具 (General Tools)** > **无代理终端安全评估故障排除 (Agentless Posture Troubleshooting)**。

无代理终端安全评估故障排除工具会收集指定客户端的无代理终端安全评估活动。**无代理终端安全评估流 (Agentless Posture Flow)** 会启动终端安全评估并显示当前活动客户端与Cisco ISE 之间的所有交互。**仅下载客户端日志 (Only Download Client Logs)** 会创建一些日志，其中包含最长过去 24 小时的客户端终端安全评估流。客户端可以随时删除日志。收集完成后，可以导出日志的 ZIP 文件。

报告

在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **操作 (Operations)** > **报告 (Reports)** > **报告 (Reports)** > **终端和用户 (Endpoints and Users)** > **无代理终端安全评估 (Agentless Posture)**，查看运行无代理终端安全评估的所有终端。

解决网络设备配置问题

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **操作 (Operations)** > **故障排除 (Troubleshoot)** > **诊断工具 (Diagnostic Tools)** > **常规工具 (General Tools)** > **评估配置验证器 (Evaluate Configuration Validator)**。

步骤 2 在**网络设备 IP (Network Device IP)** 字段中输入您想要评估其配置的网络设备的 IP 地址。

步骤 3 选中相应复选框，然后点击要与建议模板进行比较的配置选项旁边的单选按钮。

步骤 4 点击**运行 (Run)**。

步骤 5 在显示的**进度详细信息... (Progress Details...)** 区域中，点击**点击此处输入凭证 (Click Here to Enter Credentials)**。在显示的**凭证窗口 (Credentials Window)** 对话框中，输入与网络设备建立连接所需的连接参数和凭证，然后点击**提交 (Submit)**。

要取消工作流程，请在**进度详细信息... (Progress Details...)** 窗口中点击**点击此处取消正在运行的工作流程 (Click Here to Cancel the Running Workflow)**。

步骤 6 选中想要分析的接口旁边的复选框，然后点击**提交 (Submit)**。

步骤 7 点击**显示结果摘要 (Show Results Summary)** 以查看配置评估的详细信息。

排除终端安全评估故障

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **操作 (Operations)** > **故障排除 (Troubleshoot)** > **诊断工具 (Diagnostic Tools)** > **常规工具 (General Tools** > **终端安全评估故障排除 (Posture Troubleshooting)**。

步骤 2 在相应字段中输入信息。

步骤 3 点击 **Search**。

步骤 4 要查找说明和确定事件的解决方法，请在列表中选择事件，点击 **Troubleshoot**。

会话跟踪测试案例

此工具用于以一种可预测的方式测试策略流，以检查和验证策略的配置方式，而无需让实际流量源自实际设备。

您可以配置测试案例中使用的属性和值的列表。这些详细信息用于执行与策略系统的交互，以模拟对策略的运行时调用。

可通过使用词典配置属性。适用于简单 RADIUS 身份验证的所有词典都列在**属性 (Attributes)** 字段中。

注释 您可以配置仅适用于简单 RADIUS 身份验证的测试案例。

配置会话跟踪测试用例

开始之前

要执行以下任务，您必须是超级管理员或系统管理员。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **操作 (Operations) > 故障排除 (Troubleshoot) > 诊断工具 (Diagnostic Tools) > 常规工具 (General Tools) > 会话跟踪测试用例 (Session Trace Test Cases)**。

步骤 2 点击**添加 (Add)**。

步骤 3 在**测试详细信息 (Test Details)** 选项卡中，输入测试用例的名称和描述。

步骤 4 选择一个预定义的测试用例或配置必填属性及其值。可提供以下预定义的测试案例：

- 基本身份验证访问
- 已分析的Cisco电话
- 兼容设备访问
- Wi-Fi 访客（重定向）
- Wi-Fi 访客（访问）

当您选择预定义的测试案例时，Cisco ISE 会自动填充测试案例的相关属性。您可以使用这些属性的默认值，或从显示的选项中选择所需的值。您还可以向测试用例添加其他自定义属性。

添加到测试用例的属性和值会列在“文本”(Text) 字段（“自定义属性”(Custom Attributes) 字段下方）中。当您在文本 (Text) 字段中编辑内容时，Cisco ISE 会检查更新内容的有效性和语法。

您可以在测试详细信息 (Test Details) 页面底部查看所有属性的摘要。

步骤 5 点击**提交 (Submit)**。

Cisco ISE 验证属性及其值，并在保存测试详细信息之前指示任何错误。

步骤 6 在**测试可视化工具 (Test Visualizer)** 选项中，选择要运行此测试用例的节点。

注释 仅具有策略服务角色的节点显示在 **ISE 节点**下拉列表中。

点击**用户组/属性 (User Groups/Attributes)**，从外部身份库检索用户的组和属性。

步骤 7 点击**执行 (Execute)**

Cisco ISE 执行测试案例，并以表格格式显示测试案例的逐步结果。它显示策略阶段、匹配规则和结果对象。点击绿色图标可查看每个步骤的详细信息。

步骤 8 点击**先前测试执行 (Previous Test Executions)** 选项卡查看先前测试执行的结果。您还可以选择和比较任意两个测试案例。Cisco ISE 以表格格式显示每个测试案例的属性的比较视图。

您可以从“RADIUS 实时日志”(RADIUS Live Logs) 页面启动会话跟踪测试用例工具。您可以在“实时日志”(Live Logs) 页面上选择一个条目，然后点击“操作”(Actions) 图标（在“详细信息”(Details) 列中），启动会话跟踪测试用例工具。Cisco ISE 会从相应的日志条目中提取相关属性及其值。如果需要，可以修改这些属性和值，并执行测试用例。

用于高级故障排除的技术支持隧道

Cisco ISE 使用 Cisco IronPort Tunnel 基础设施为Cisco技术支持工程师创建了一个安全隧道，可以通过该系统连接到 ISE 服务器并进行故障排除。Cisco ISE 使用 SSH 通过该隧道创建安全连接。

作为管理员，您可以控制对隧道的访问；您可以选择允许支持工程师访问隧道的时间和期限。没有您的参与，Cisco客户支持无法建立隧道。您将收到有关服务登录的通知。您可以随时禁用隧道连接。默认情况下，技术支持隧道保持开放72小时。我们建议您或技术支持工程师在完成所有故障排除工作后关闭隧道。如有需要，您可以选择将隧道开放时间延长 72 小时。

使用 **tech support-tunnel enable** 命令发起隧道连接。

通过 **tech support-tunnel status** 命令可使系统显示连接状态。该命令提供关于是否已建立连接、身份验证是否失败，或是否无法访问服务器的信息。如果隧道服务器可访问，但ISE无法进行身份验证，ISE 会每隔 5 分钟再次尝试进行身份验证，如此持续 30 分钟，之后隧道会被禁用。

您可以使用 **tech support-tunnel disable** 命令禁用隧道连接。即使当前有技术支持工程师登录时，该命令也会断开现有的隧道。

如果您已从 ISE 服务器建立隧道连接，则生成的 SSH 密钥可在 ISE 服务器上使用。当您在较晚的时间点尝试启用支持隧道时，系统会提示您重新使用之前生成的 SSH 密钥。您可以选择使用相同的密钥或生成新密钥。您还可以使用 **tech support-tunnel resetkey** 命令手动重置密钥。如果您在隧道连接处于启用状态时执行该命令，系统会提示您需先禁用该连接。如果您选择保持现有的连接而不禁用该连接，则系统会在禁用现有连接后重置密钥。如果您选择禁用连接，则系统会断开隧道连接，并立即重置密钥。

在建立隧道连接后，您可以使用 **tech support-tunnel extend** 命令延长连接的持续时间。

有关 **tech support-tunnel** 命令的使用指南，请参阅《Cisco身份服务引擎 CLI 参考指南》。

建立一个技术支持隧道

您可以通过Cisco ISE 命令行界面 (CLI) 建立一个安全隧道。

步骤 1 在Cisco ISE CLI 上输入以下命令：

技术支持隧道启用

系统会提示您输入该隧道的密码和昵称。

步骤 2 输入密码。

步骤 3 （可选）输入隧道昵称。

系统生成一个 SSH 密钥并显示密码、设备序列号和 SSH 密钥。您必须向Cisco客户支持传输这些信息以供支持工程师连接到您的系统。

步骤 4 复制密码、设备序列号和 SSH 密钥并将其发送给Cisco客户支持。

支持工程师现在可以安全地连接到您的 ISE 服务器。您将收到有关服务登录的定期通知。

用于验证传入流量的 TCP Dump 实用工具

TCP 转储实用工具嗅探数据包，可以使用此实用工具验证预计数据包是否已到达节点。例如，当报告中没有显示传入身份验证或日志时，您可能会怀疑没有传入流量或传入流量无法到达Cisco ISE。在这种情况下，您可以运行此工具进行验证。

可以配置 TCP 转储选项，然后从网络流量收集数据以帮助您对网络问题进行故障排除。

使用 TCP Dump 监控网络流量

“TCP 转储”(TCP Dump) 页面列出了您创建的 TCP 转储进程文件。可以创建不同文件以用于不同目的，根据需要运行这些文件，然后在不需要这些文件时将其删除。

通过指定大小、文件数量以及进程运行时间来控制收集的数据。如果进程在时间限制之前完成，并且文件小于最大大小，并且您启用了多个文件，则进程会继续并创建另一个转储文件。

可以对更多接口运行 TCP 转储，包括绑定接口。

不再提供人可读格式选项，转储文件始终为原始格式。

支持与存储库的 IPv6 连接。

开始之前

TCP Dump 页面中的 Network Interface 下拉列表仅显示已配置 IPv4 或 IPv6 地址的网络接口卡 (NIC)。在 VMware 中，默认情况下将连接所有 NIC，因此，所有 NIC 均具有 IPv6 地址，并显示在“网络接口”(Network Interface) 下拉列表中。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **操作 (Operations)** > **故障排除 (Troubleshoot)** > **诊断工具 (Diagnostic Tools)** > **常规工具 (General Tools)** > **TCP 转储 (TCP Dump)**。

步骤 2 选择 **Host Name** 作为 TCP Dump 实用程序源。

步骤 3 从下拉列表中选择要监控的**网络接口 (Network Interface)**。

步骤 4 在“过滤器”(Filter) 字段中，输入要对其进行过滤的布尔表达式。

系统支持以下标准 tcpdump 过滤器表达式：

- ip host 10.77.122.123
- ip host ISE123

- ip host 10.77.122.123 and not 10.77.122.119

步骤 5 输入此 TCP 转储进程的**文件名 (File Name)**。

步骤 6 选择用于存储 TCP 转储日志文件的**存储库 (Repository)**。

步骤 7 **文件大小 (File Size)** - 选择最大文件大小。

如果转储超出此文件大小，则一个新文件将打开以继续转储。转储可通过新文件继续的次数受**限制为 (Limit to)** 设置的限制。

步骤 8 **限制为 (Limit to)** - 限制转储可扩展到的文件数。

步骤 9 **时间限制 (Time Limit)** - 配置转储在运行多长时间后结束。

步骤 10 通过点击单选按钮，将 Promiscuous Mode 设置为 On 或 Off。默认值为 On。

混合模式为默认包嗅探模式，在此模式下，网络接口将所有流量都传输到系统的 CPU。我们建议将该选项设置为 On。

注释 思科 ISE 不支持大于1500 MTU 的帧（巨帧）。

保存 TCP Dump 文件

开始之前

您应按照“使用 TCP Dump 文件监控网络流量”一节中所描述的内容成功完成任务。

注释 还可以通过Cisco ISE CLI 访问 TCP 转储。有关详细信息，请参阅《思科身份识别服务引擎 *CLI* 参考指南》。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **操作 (Operations)** > **故障排除 (Troubleshoot)** > **诊断工具 (Diagnostic Tools)** > **常规工具 (General Tools)** > **TCP 转储 (TCP Dump)**。

步骤 2 从**格式 (Format)** 下拉列表中选择选项。默认设置为**人可读 (Human Readable)**。

步骤 3 点击**下载 (Download)**，导航至所需位置，并点击**保存 (Save)**。

步骤 4 若要清除以前的转储文件而无需事先保存，请点击**删除 (Delete)**。

比较终端或用户的意外 SGACL

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **操作 (Operations)** > **故障排除 (Troubleshoot)** > **诊断工具 (Diagnostic Tools)** > **Trustsec 工具 (Trustsec Tools)** > **出口 (SGACL) 策略 (Egress (SGACL) Policy)**。

步骤 2 输入想要比较其 SGACL 策略的 Trustsec 设备的网络设备 IP 地址。

步骤 3 点击**运行 (Run)**。

步骤 4 点击 **User Input Required**，按需修改字段。

步骤 5 点击**提交 (Submit)**。

步骤 6 点击 **Show Results Summary**，查看诊断和建议的解决步骤。

出口策略诊断流程

出口策略诊断工具 使用下表中介绍的流程进行比较：

流程阶段	说明
1	使用您所提供的 IP 地址连接设备，然后获取每个源和目标 SGT 对的访问控制列表 (ACL)。
2	检查并确保已在Cisco ISE 中配置出口策略并为每个源和目标 SGT 对获取 ACL。
3	将从网络设备获取的 SGACL 策略与从Cisco ISE 获取的 SGACL 策略进行比较。
4	如果存在不匹配情况，则显示源和目标 SGT 对。此外，作为额外的信息，系统会显示匹配的条目。

使用 SXP-IP 映射排除支持 TrustSec 的网络中的连接问题

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **操作 (Operations)** > **故障排除 (Troubleshoot)** > **诊断工具 (Diagnostic Tools)** > **Trustsec 工具 (Trustsec Tools)** > **SXP-IP 映射 (SXP-IP Mappings)**。

步骤 2 输入网络设备的 IP 地址。

步骤 3 点击**选择**。

步骤 4 点击**运行 (Run)**，然后点击 **User Input Required** 并修改必要字段。

专业的故障排除人员从网络设备检索 Trustsec SXP 连接，并提示您再次选择 SXP 对等设备。

步骤 5 点击 **User Input Required**，然后输入必要信息。

步骤 6 选中您要用于对比 SXP 映射的 SXP 对等设备的复选框，然后输入通用连接参数。

步骤 7 点击**提交 (Submit)**。

步骤 8 点击 **Show Results Summary** 查看诊断和解决步骤。

通过 IP-SGT 映射解决支持 TrustSec 的网络中的连接问题

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **操作 (Operations)** > **故障排除 (Troubleshoot)** > **诊断工具 (Diagnostic Tools)** > **Trustsec Tools (Trustsec 工具)** > **IP 用户 SGT (IP User SGT)**。

步骤 2 根据需要在字段中输入信息。

步骤 3 点击**运行 (Run)**。

系统会提示您输入其他信息。

步骤 4 点击**需要用户输入 (User Input Required)**，必要时修改字段。

步骤 5 点击**提交 (Submit)**。

步骤 6 点击 **Show Results Summary** 查看诊断和解决步骤。

设备 SGT 工具

对于启用 Trustsec 解决方案的设备，每个网络设备都会通过 RADIUS 身份验证分配到一个 SGT 值。设备 SGT 诊断工具连接至网络设备（使用您提供的 IP 地址）并获取网络设备 SGT 值，然后检查 RADIUS 身份验证记录以确定最近分配的最新 SGT 值。最后，它会用表格格式显示设备-SGT 对，并确定 SGT 值为相同还是不同。

通过在启用 Trustsec 的网络中比较设备 SGT 映射对连通性问题进行故障排除

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **操作 (Operations)** > **故障排除 (Troubleshoot)** > **诊断工具 (Diagnostic Tools)** > **Trustsec 工具 (Trustsec Tools)** > **设备 SGT (Device SGT)**。

步骤 2 根据需要在字段中输入信息。

Telnet 的默认端口号为 23，SSH 的默认端口号为 22。

步骤 3 点击**运行 (Run)**。

步骤 4 点击 **Show Results Summary** 查看设备 SGT 的比较结果。

获取其他故障排除信息

通过Cisco ISE，可以从管理员门户下载支持和故障排除信息。可以使用支持捆绑包为Cisco技术支持中心 (TAC) 准备诊断信息来对Cisco ISE 的问题进行故障排除。

注释 支持捆绑包和调试日志为 TAC 提供高级故障排除信息，并且难以解释。可以使用Cisco ISE 提供的各种报告和故障排除工具对在网络中面临的问题进行诊断和故障排除。

思科 ISE 支持捆绑包

您可以配置日志，使其成为支持捆绑包的一部分。例如，您可以配置来自特定服务的日志，使其成为调试日志的一部分。此外，您还可以根据日期过滤日志。

您可以下载的日志分类如下：

- 完整配置数据库：包含可读 XML 格式的Cisco ISE 配置数据库。当您尝试解决问题时，可以将此数据库配置导入另一个Cisco ISE 节点，以便重新创建场景。
- 调试日志： 捕获引导程序、应用配置、运行时、部署、公共密钥基础设施 (PKI) 信息以及监控和报告。

  调试日志为特定的Cisco ISE 组件提供故障排除信息。要启用调试日志，请参阅第 11 章，“日志记录”。如果不启用调试日志，所有信息消息 (INFO) 将包含在支持捆绑包中。有关详细信息，请参阅思科 ISE 调试日志，第 55 页。
- 本地日志：包含来自Cisco ISE 上运行的各种进程的系统日志消息。
- 核心文件 - 包含有助于识别突发事件的原因的重要信息。这些日志在应用发生崩溃并且包含大量转储时创建。
- 监控和报告日志：包含关于警报和报告的信息。
- 系统日志 - 包含Cisco应用部署引擎 (ADE) 相关信息。
- 策略配置：包含在Cisco ISE 中配置的可读格式的策略。

使用 **backup-logs** 命令，您可以从Cisco ISE CLI 下载这些日志。有关详细信息，请参阅思科身份服务引擎 *CLI* 参考指南。

注释 对于 Inline Posture 节点，您不能从 Admin 门户下载支持捆绑包。必须从Cisco ISE CLI 中使用 **backup-logs** 命令。

如果选择从 Admin 门户下载这些日志，您可以执行以下操作：

- 根据日志类型（例如调试日志或系统日志），仅下载日志子集。

- 对于所选日志类型，仅下载最新的 *n* 个文件。此选项允许您控制支持捆绑包的大小以及下载所需的时间。

监控日志提供关于监控、报告和故障排除功能的信息。有关下载日志的详细信息，请参阅 下载思科 ISE 日志文件，第 54 页。

支持捆绑包

您可以将支持捆绑包以简单 tar.gpg 文件的形式下载至您的本地计算机。支持捆绑包将按照 ise-support-bundle_ise-support-bundle-mm-dd-yyyy--hh-mm.tar..gpg 的格式用日期和时间戳命名。浏览器会提示您将支持捆绑包保存至适当的位置。您可以提取支持捆绑包的内容并查看 README.TXT 文件，此文件介绍该支持捆绑包的内容，以及在支持捆绑包包含 ISE 数据库内容的情况下如何导入 ISE 数据库内容。

下载思科 ISE 日志文件

在对网络中的问题进行故障排除时，可以下载Cisco ISE 日志文件，以查找更多信息。

您也可以下载包含 ADE-OS 和其他日志文件的系统日志来排除安装和升级方面的问题。

在下载支持捆绑包时，现在可以选择一个公共加密密钥，而无需手动输入加密密钥。如果选择此选项，会使用Cisco PKI 对支持捆绑包进行加密和解密。Cisco TAC 负责维护公钥和私钥。Cisco ISE 使用公钥来加密支持捆绑包。Cisco TAC 可使用私钥解密支持捆绑包。如果您想要提供支持捆绑包到 Cisco TAC 以进行故障排除，请使用此选项。如果您要在现场排除故障，请使用共享密钥加密。

开始之前

- 您必须具有超级管理员或系统管理员权限才能执行以下任务。
- 应已配置调试日志和调试日志级别。

步骤 1 选择 **操作 (Operations)** > **故障排除 (Troubleshoot)** > **下载日志 (Download Logs)** > **设备节点列表 (Appliance Node List)**。

步骤 2 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **操作 (Operations)** > **故障排除 (Troubleshoot)** > **下载日志 (Download Logs)** > **设备节点列表 (Appliance Node List)**。

步骤 3 点击要从其下载支持捆绑包的节点。

步骤 4 在**支持捆绑包 (Support Bundle)** 选项卡中，选择要填充在您的支持捆绑包中的参数。

如果您将所有日志包含在内，则您的支持捆绑包会非常大，下载会需要较长时间。要优化下载流程，请选择只下载最新的 *n* 个文件。

步骤 5 输入生成支持捆绑包的起始日期和结束日期。

步骤 6 选择以下其中一个选项：

- “公共密钥加密”(Public Key Encryption)：如果您想要向Cisco TAC 提供支持捆绑包以进行故障排除，请选择此选项。

- “共享密钥加密”(Shared Key Encryption)：如果您希望在现场排除故障，请选择此选项。如果选择此选项，您必须输入支持捆绑包的加密密钥。

步骤 7 输入支持捆绑包的加密密钥，并重新输入加以确认。

步骤 8 点击 **Create Support Bundle**。

步骤 9 点击**下载 (Download)** 以下载新创建的支持捆绑包。

支持捆绑包是下载到正在运行您的应用浏览器的客户端系统的一个 tar.gpg 文件。

下一步做什么

下载特定组件的调试日志。

思科 ISE 调试日志

调试日志为各种Cisco ISE 组件提供故障排除信息。调试日志包含过去 30 天生成的紧急和警告警报以及在过去 7 天生成的信息警报。报告问题时，可能会要求您启用并发送这些调试日志，以便诊断和解决问题。

注释 启用具有高负载的调试日志（例如监控调试日志）可能会生成有关高负载的警报。

获取调试日志

步骤 1 配置您希望获取调试日志的组件。

步骤 2 下载调试日志。

思科 ISE 组件和相应的调试日志

表 *6:* 组件和相应的调试日志

组件	调试日志
Active Directory	ad_agent.log
缓存跟踪器	tracking.log
实体定义框架 (EDF)	edf.log
JMS	ise-psc.log
许可证	ise-psc.log
通知跟踪器	tracking.log

组件	调试日志
复制部署	replication.log
Replication-JGroup	replication.log
复制跟踪器	tracking.log
RuleEngine-Attributes	ise-psc.log
RuleEngine-Policy-IDGroups	ise-psc.log
accessfilter	ise-psc.log
admin-infra	ise-psc.log
开机启动向导	ise-psc.log
cisco-mnt	ise-psc.log
客户端	ise-psc.log
cpm-clustering	ise-psc.log
cpm-mnt	ise-psc.log
epm-pdp	ise-psc.log
epm-pip	ise-psc.log
anc	ise-psc.log
anc	ise-psc.log
ers	ise-psc.log
guest	ise-psc.log
访客访问权限管理	guest.log
访客访问权限	guest.log
MyDevices	guest.log
门户	guest.log
Portal-Session-Manager	guest.log
Portal-web-action	guest.log
guestauth	ise-psc.log
guestportal	ise-psc.log
identitystore-AD	ise-psc.log
infrastructure	ise-psc.log
mdm	ise-psc.log
mdm-pip	ise-psc.log

组件	调试日志
mnt-report	reports.log
mydevices	ise-psc.log
nsf	ise-psc.log
nsf-session	ise-psc.log
org-apache	ise-psc.log
org-apache-cxf	ise-psc.log
org-apache-digester	ise-psc.log
posture	ise-psc.log
profiler	profiler.log
provisioning	ise-psc.log
prrt-JNI	prrt-management.log
runtime-AAA	prrt-management.log
runtime-config	prrt-management.log
runtime-logging	prrt-management.log
sponsorportal	ise-psc.log
swiss	ise-psc.log

配置调试向导（按功能）

调试向导包含调试模板，可用于对Cisco ISE 节点问题进行故障排除。可以配置调试配置文件和调试日志。

在**调试配置文件配置 (Debug Profile Configuration)** 窗口中，可以为模板中的各个组件配置调试日志严重性级别。

在**调试日志配置 (Debug Log Configuration)** 窗口中，可以配置调试日志的严重性级别。调试日志可捕获引导程序 (bootstrap)、应用配置、运行时间、部署、监控、报告和公钥基础设施 (PKI) 信息。

注释

- 每节点日志级别优先于调试向导配置文件。
- 当启用多个配置文件来编辑同一组件时，较高的日志级别优先，其中跟踪日志具有最高优先级。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **操作 (Operations)** > **故障排除 (Troubleshoot)** > **调试向导 (Debug Wizard)** > **调试配置文件配置 (Debug Profile Configuration)** 配置调试配置文件。

步骤 2 要创建新配置文件，请点击**添加 (Add)**。

步骤 3 输入新配置文件的**名称**和**描述**。

选中要包含在配置文件中的组件旁边的复选框，并为每个组件设置相应的**日志级别**。

步骤 4 要保存此配置文件，请点击**保存 (Save)**。

步骤 5 要立即启用 ISE 节点，请点击**启用 (Enable)**。否则，请点击**稍后执行 (Do it Later)**。

步骤 6 如果点击**启用 (Enable)**，请选中要为其启用配置文件的 ISE 节点旁边的复选框。

步骤 7 点击**保存 (Save)**。

步骤 8 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **操作 (Operations)** > **故障排除 (Troubleshoot)** > **调试向导 (Debug Wizard)** > **调试日志配置 (Debug Log Configuration)** 配置调试日志。

步骤 9 点击单选按钮以选择节点。

步骤 10 点击单选按钮以选择组件，然后点击**编辑 (Edit)** 以更改**组件名称**、**日志级别**、**说明**和组件的**日志文件名称**。

步骤 11 点击**保存 (Save)**。

下载调试日志

开始之前

要执行以下任务，您必须是超级管理员或系统管理员。

步骤 1 选择 **操作 (Operations)** > **故障排除 (Troubleshoot)** > **下载日志 (Download Logs)** > **设备节点列表 (Appliance Node List)**。

步骤 2 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **操作 (Operations)** > **故障排除 (Troubleshoot)** > **下载日志 (Download Logs)** > **设备节点列表 (Appliance Node List)**。

步骤 3 在“设备节点”(Appliance node) 列表中，点击您希望下载调试日志的节点。

步骤 4 点击 **Debug Logs** 选项卡。

系统会显示调试日志类型和调试日志的列表。此列表显示的内容取决于您的调试日志配置。

步骤 5 点击您希望下载的日志文件并将其保存到正在运行客户端浏览器的系统中。

您可以根据需要重复此过程下载其他日志文件。可以从**调试日志 (Debug Logs)** 页面下载以下额外的调试日志：

- isebootstrap.log：提供引导日志消息
- monit.log：提供监视程序消息
- pki.log：提供第三方加密库日志
- iseLocalStore.log：提供本地存储文件相关日志
- ad_agent.log：提供 Microsoft Active Directory 第三方库日志
- catalina.log：提供第三方日志