故障排除

- 思科 ISE 中的监控和故障排除服务， 第 1 页
- 网络处理状态， 第 3 页
- 网络身份验证， 第 3 页
- Smart Call Home， 第 4 页
- 日志收集， 第 5 页
- RADIUS 实时日志， 第 6 页
- 实时身份验证， 第 8 页
- RADIUS 实时会话， 第 10 页
- 导出摘要， 第 12 页
- 身份验证摘要报告， 第 14 页
- 故障排除诊断工具， 第 14 页
- 用于验证传入流量的 TCP Dump 实用工具， 第 17 页
- 获取其他故障排除信息， 第 20 页

思科 ISE 中的监控和故障排除服务

监控和故障排除 (MnT) 服务是所有思科 ISE 运行时服务的综合身份解决方案，并使用以下组件：

- 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监控操作条件。
- 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。

网络权限框架

控制面板显示网络权限框架 (NPF) 上的活动并提供关于各个组件的详细信息。

NPF 由下表所述的三个层级组成：

表 *1: NPF* 层级

层	规范
1	使用 802.1x、MAC 身份验证绕行 (MAB)、思科 ISE 分析器服务，根据身份进行访问控制
2	利用 802.1x、MAB、分析器、对网络准入控制 (NAC) 管理器的访客调配、集中式 Web 身份验证，根据身份进行访问控制
3	利用 802.1x、MAB、分析器、对 NAC 管理器的访客调配、集中式 Web 身份验证，根据身份和安全评估进行访问控制

NPF 身份验证和授权生成事件流。然后，思科 ISE 监控和故障排除工具会收集不同来源的事件并进行汇总。您可以在控制面板上查看身份验证和授权结果，或选择运行任意数量的报告。

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

思科 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。如果思科 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，则我们建议将某个思科 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。

网络处理状态

您可以使用 System Summary dashlet 从思科 ISE 控制面板查看网络的处理状态。例如，当应用服务器或数据库等进程失败时，会生成警报，您可以使用 System Summary dashlet 查看结果。

系统状态图标的颜色指示系统的运行状况。

- 绿色 = 正常
- 黄色 = 警告
- 红色 = 严重问题
- 灰色 = 无信息

监控网络处理状态

步骤 1 转至思科 ISE **Dashboard**。

步骤 2 展开 **System Summary** dashlet。系统将显示详细的实时报告。

步骤 3 查看网络上正在运行的进程的以下信息：

- 进程的名称
- CPU 和内存使用情况
- 进程开始运行的时间

网络身份验证

您可以从 Authentications 面板中查看成功和失败的网络身份验证。此面板会提供有关用户或设备类型、位置和用户或设备所属身份组的数据。面板顶部的迷你图显示过去 24 小时和过去 60 分钟的分布。

监控网络身份验证

步骤 1 转至思科 ISE **Dashboard**。

步骤 2 展开**身份验证 (Authentications)** Dashlet。

系统将显示详细的实时报告。

步骤 3 查看网络上经过身份验证的用户或设备的信息。

步骤 4 展开数据类别，了解更多信息。

Smart Call Home

Smart Call Home (SCH) 监控您的网络中的思科 设备，并将关键事件通过电子邮件方式通知您。电子邮件包含实时告警，其中提供环境信息和补救建议。

如果您从思科 ISE 激活智能许可，则默认情况下将启用 SCH 功能。否则，要启用 SCH，您必须为 SCH 服务注册思科 ISE。有关如何启用 SCH 功能的信息，请参阅为 Smart Call Home 服务进行注册，第 5 页。

在激活智能许可或注册 SCH 服务后，您可以选择执行以下操作之一：

- 仅启用匿名报告。SCH 的匿名报告功能只提供少量的有关您的网络中的思科 ISE 设备运行状况的信息。
- 启用 SCH 提供的完整功能集。

Smart Call Home 配置文件

Smart Call Home 配置文件决定了您的设备所监控的事件类型。思科 包括以下默认配置文件：

- ciscotac-1 - 用于匿名报告
- isesch-1 - 用于 Smart Call Home 功能

您无法编辑用于 Anonymous Reporting 的默认配置文件 (ciscotac-1)。

Anonymous Reporting

思科 可以安全地收集有关部署、网络接入设备、分析器和正在使用的其他服务的非敏感信息。收集此数据有助于更好地了解思科 的使用情况，并改进该产品以及它提供的各种服务。

默认情况下，会启用匿名报告。如果要禁用匿名报告，可以通过 管理员门户（管理 (Administration) > 系统 (System) > 设置 (Settings) > Smart Call Home） 来禁用。

为 Smart Call Home 服务进行注册

注释 如果已从思科 ISE 激活智能许可，则无需注册 Smart Call Home (SCH) 服务。使用智能许可，默认情况下启用 SCH 功能。Smart Call Home 页面中的注册状态为活动。您可以选择仅启用匿名报告或启用 SCH 提供的完整功能集。

要在没有智能许可的情况下启用 SCH 服务，您必须先注册用于 SCH 服务的思科 ISE。您只可以从独立节点或主要管理节点执行此操作。

步骤 1 选择**管理 (Administration)** > **系统 (System)** > **设置 (Settings)** > **Smart Call Home**。

步骤 2 选择以下其中一个选项：

- 打开全部 SCH 功能
- 保留默认 SCH 遥测设置并只发送匿名数据
- 禁用一切

步骤 3 （仅当您选择**打开全部 SCH 功能 [Turn on full SCH Capability]** 选项时）在注册状态 (Registration Status) 区域输入您的邮箱地址。

步骤 4 点击**保存 (Save)**。

如果已选择打开全部 SCH 功能，您将收到一封包含激活链接的邮件。点击激活链接并按照提供的说明完成注册。

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 思科 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。您必须为思科 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 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。此页面的访问路径为：**操作 (Operations)** > **RADIUS** > **实时日志 (Live Logs)**。请注意，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
时间	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	显示身份验证成功还是失败。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	单击详细信息 **(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。 如果已为该会话处理审计事件，则点击详细信息 **(Details)** 列下的图标可打开审计详细信息 **(Accounting Detail)** 报告。如果会话处于已验证状态，当您点击详细信息 **(Details)** 列下的 图标时，会显示身份验证详细信息 **(Authentication Detail)** 报告。 身份验证详细信息 **(Authentication Detail)** 报告中的响应时间 **(Response Time)** 是思科 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 为 300 + 150 + 100 = 550 毫秒。 注释 您无法查看活动时间超过 7 天的终端的详细信息。当点击活动时间超过 7 天的终端的详细信息 **(Details)** 图标时，您会看到一个包含以下消息的窗口：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.)

字段名称	说明
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。
Identity	显示与身份验证关联的已登录用户名。
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	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	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	显示终端设备的 IP 地址。
Network Device	显示网络访问设备的 IP 地址。
Device Port	显示终端连接的端口号。
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	指明从其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	显示事件状态。
Failure Reason	如果身份验证失败，显示失败的详细原因。
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	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。
Security Group	显示由身份验证日志标识的组。
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。

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。

一个终端成功通过身份验证时，**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 选择**操作 (Operations)** > **身份验证 (Authentications)**。

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 单击窗口底部的**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”(Live Authentications) 页面过滤数据

使用**实时身份验证 (Live Authentications)** 窗口中的过滤器，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 (Live Logs)** 窗口筛选记录，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 (Live Authentications)** 窗口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，思科 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 选择**操作 (Operations)** > **身份验证 (Authentications)**。

步骤 2 根据**显示实时身份验证 (Show Live Authentications)** 窗口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

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。此页面的导航路径为：**操作 (Operations)** > **RADIUS** > **实时会话 (Live Sessions)**。您仅可在主 PAN 上查看 RADIUS 实时会话。

表 *3: 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。
CoA 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 (Endpoint 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。

字段名称	说明
审核会话 ID (Audit Session ID）	显示唯一会话标识符。
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 (Endpoint Profile)	显示设备的终端配置文件。
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。
身份验证方式 (Auth Method)	显示 RADIUS 协议使用的身份验证方式，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)**。

字段名称	说明
WLC 漫游 (WLC Roam)	显示用于跟踪是否已在漫游期间从一个无线局域网控制器 (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 思科 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。
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)	显示终端通过 RADIUS 或是身份映射进行身份验证。
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。

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 (Export Summary)** 窗口每 2 分钟自动刷新一次。单击**刷新**图标可手动刷新**导出摘要 (Export Summary)** 窗口。

超级管理员可以取消**正在进行 (In-Progess)** 或处于**排队 (Queued)** 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会排队。计划导出的报告没有此类限制。

下表列出**导出摘要 (Export Summary)** 窗口中的字段。此页面的导航路径为：**操作 (Operations)** > **报告 (Reports)** > **导出摘要 (Export Summary)** 。

表 *4:* 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。
Repository	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。
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)** 窗口中执行以下操作：

- 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。

注释　您只能生成最近 30 天的“身份验证摘要”报告。

网络接入问题故障排除

步骤 1　选择**操作 (Operations)** > **报告 (Reports)** > **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**身份验证失败原因 (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。

故障排除诊断工具

诊断工具可帮助您诊断思科 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，思科 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，思科 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 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 Active Directory 相关的身份验证，但在部署中未配置 Active Directory 服务器，则系统将显示未配置 *AD"(AD not configured)* 消息。

步骤 4 从表格中选择 RADIUS 身份验证记录，并单击**故障排除 (Troubleshoot)**。

要对 Active Directory 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 （可选）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，请单击**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：

1. 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)**。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)**。
2. 在显示的 **执行网络设备命令** 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 **显示** 命令。
3. 点击**运行 (Run)**。

执行思科 IOS show 命令以检查配置

步骤 1 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 在思科 ISE GUI 中，点击菜单图标 (☰)，然后选择 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 3 在相应字段中输入信息。

步骤 4 点击 **Run** 以在指定网络设备上执行此命令。

步骤 5 点击需要用户输入 **(User Input Required)**，必要时修改字段。

步骤 6 点击 **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。

解决网络设备配置问题

步骤 1 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 **Run**。

步骤 5 点击需要用户输入 **(User Input Required)**，必要时修改字段。

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

步骤 7 （可选）单击显示结果摘要 **(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 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**。

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思科 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。

⚠

注意 如果启动 TCP Dump，系统会自动删除之前的转储文件。要保存之前的转储文件，请执行“保存 TCP Dump 文件”一节描述的任务，再开始新的 TCP Dump 会话。

使用 TCP Dump 监控网络流量

开始之前

TCP 转储 (TCP Dump) 窗口页面中的**网络接口 (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 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 在思科 ISE GUI 中，点击**菜单**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 3 从**主机名称 (Host Name)** 下拉列表中选择 TCP Dump 实用工具的源。不支持 Inline Posture 节点。

步骤 4 从**网络接口 (Network Interface)** 下拉列表中选择要监控的接口。

步骤 5 点击**混合模式 (Promiscuous Mode)** 切换按钮以设置为“On”(开) 或“关”(Off)。默认值为 On。

混合模式为默认数据包嗅探模式，在此模式下，网络接口将所有流量都传输到系统的 CPU。建议将该选项保留为“开”(On)。

步骤 6 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 TCP 转储过滤器表达式：

- ip host 10.77.122.123
- ip host ISE123
- ip host 10.77.122.123 and not 10.77.122.119

步骤 7 点击**开始 (Start)**，开始监控网络。

步骤 8 收集足够数据后，点击**停止 (Stop)**，或者等进程在累计到最大数据包数量 500,000 后自动结束。

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 还可以通过思科 ISE CLI 访问 TCP 转储。有关详细信息，请参阅思科身份服务引擎 *CLI* 参考指南。

步骤 1 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 （可选）若要清除以前的转储文件而无需保存，请点击**删除 (Delete)**。

比较终端或用户的意外 SGACL

步骤 1 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 在思科 ISE GUI 中，点击**菜单**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 3 输入想要比较其 SGACL 策略的 TrustSec 设备的网络设备 IP 地址。

步骤 4 点击**运行 (Run)**。

步骤 5 单击**需要用户输入 (User Input Required)**，必要时修改字段。

步骤 6 点击 **Submit**。

步骤 7 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

出口策略诊断工具会使用下表中介绍的流程：

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	检查并确保已在思科 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 策略与从思科 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 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 单击**运行 (Run)**。

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 单击**需要用户输入 (User Input Required)**，然后在字段中输入必要信息。

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 **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 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 **Run**。

系统会提示您输入其他信息。

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

步骤 5 点击 **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。

通过对比设备 SGT 映射排除启用 TrustSec 的网络中的连接故障

步骤 1 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 **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

通过思科，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思科技术支持中心 (TAC) 准备诊断信息来对思科 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。可以使用思科 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 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 格式的思科 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思科 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。

  调试日志为特定的思科 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 调试日志 ，第 22 页。

- 本地日志：包含来自思科 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 - 包含思科应用部署引擎 (ADE) 相关信息。
- 策略配置：包含在思科 ISE 中配置的可读格式的策略。

使用 **backup-logs** 命令可以从思科 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 对于内嵌式状态节点，您不能从管理员门户下载支持捆绑包。必须从思科 ISE CLI 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 日志文件。 ，第 21 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 日志文件。

在对网络中的问题进行故障排除时，可以下载思科 日志文件，以查找更多信息。

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 点击要从其下载支持捆绑包的节点。

步骤 3 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 4 输入生成支持捆绑包的**起始日期 (From)** 和**结束日期 (To)**。

步骤 5 输入支持捆绑包的加密密钥，并重新输入加以确认。

步骤 6 点击 **创建支持捆绑包 (Create Support Bundle)**。

步骤 7 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 调试日志

调试日志为各种思科 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）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。请参阅思科 组件和相应的调试日志 ， 第 23 页。

步骤 2 下载调试日志。

思科 组件和相应的调试日志

表 *5:* 组件和相应的调试日志

组件	调试日志
Active Directory	ad_agent.log
Cache Tracker	tracking.log
Entity Definition Framework (EDF)	edf.log
JMS	ise-psc.log
License	ise-psc.log
Notification Tracker	tracking.log
Replication-Deployment	replication.log
Replication-JGroup	replication.log
Replication Tracker	tracking.log
RuleEngine-Attributes	ise-psc.log
RuleEngine-Policy-IDGroups	ise-psc.log
accessfilter	ise-psc.log
admin-infra	ise-psc.log
boot-strap wizard	ise-psc.log
cisco-mnt	ise-psc.log
client	ise-psc.log
cpm-clustering	ise-psc.log
cpm-mnt	ise-psc.log
epm-pdp	ise-psc.log
epm-pip	ise-psc.log
	ise-psc.log
anc	ise-psc.log
ers	ise-psc.log
guest	ise-psc.log
guestauth	ise-psc.log
guestportal	ise-psc.log
identitystore-AD	ise-psc.log
infrastructure	ise-psc.log
ipsec-api	api-service.log

组件	调试日志
ipsec-ui	ise-psc.log
mdm	ise-psc.log
mdm-pip	ise-psc.log
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

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“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 3 点击**调试日志 (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 4 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

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。