维护和监控

是一项在管理节点上运行的服务。此服务可监控和控制终端的网络访问。 由 ISE 管理员在管理 GUI 上调用，也可以通过 pxGrid 从第三方系统调用。 支持有线和无线部署，并且需要 Plus 许可证。

您可以使用 更改授权状态，无需修改系统的总体授权策略。 允许您在隔离终端时设置授权状态。结果会建立授权策略，这些授权策略定义为检查 EPSStatus 以限制或拒绝网络访问。您可以取消隔离终端，使其获得完整的网络访问权限。您也可以关闭网络连接系统 (NAS) 上的端口，断开终端与网络之间的连接。

一次可以隔离的用户数量没有限制。此外，隔离期长度没有时间限制。

您可以执行以下操作，以便通过 监控和控制网络访问：

- 隔离：允许您使用例外策略（授权策略）限制或拒绝终端接入网络。必须创建例外策略，以根据 EPSStatus 分配不同的授权配置文件（权限）。设置为隔离状态，本质上是将终端从其默认 VLAN 迁移到指定的隔离 VLAN。您必须提前定义隔离 VLAN，在同一 NAS 上作为终端获得支持。
- 取消隔离：允许您解除隔离状态，让终端获得完整的网络访问权限。这是通过使终端返回原 VLAN 实现的。
- 关闭：允许您禁用 NAS 上的端口，断开终端与网络之间的连接。当终端连接的 NAS 上的端口关闭后，应重新手动重置 NAS 上的端口。这可以让终端连接到网络（不适用于无线部署）。

隔离和取消隔离操作可以从活动终端的会话目录报告触发。

注释 如果取消隔离已隔离的会话，新取消隔离的会话的发起方法将取决于交换机配置指定的身份验证方法。

在思科 ISE 中启用

默认情况下禁用。您必须在管理员门户中手动启用 服务。

您必须拥有超级管理员和策略管理员角色权限才能在思科 ISE 中启用 。

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

步骤 2 点击 Service Status 下拉列表，然后选择 **Enabled**。

步骤 3 点击**保存 (Save)**。

配置网络访问设置

可以让您重置终端的网络访问状态，以便对端口进行隔离、取消隔离或关闭端口。这些定义了网络中终端的授权程度。

您可以使用终端 IP 地址或 MAC 地址隔离或取消隔离终端抑或关闭终端所连接的网络访问服务器 (NAS) 端口。您可以在同一终端上多次执行隔离和取消隔离操作，但不能同时执行这两种操作。如果在网络上发现恶意终端，可以使用 关闭 NAS 端口，从而禁止终端访问。

开始之前

- 启用 。
- 为 创建授权配置文件和例外类型授权策略。

步骤 1 选择**操作 (Operations)**。

步骤 2 在**策略列表 (Policy List)** 窗口中，输入终端的 IP 地址或 MAC 地址。

步骤 3 点击**操作 (Action)** 下拉列表，选择以下操作之一：

- **隔离 (Quarantine)** - 隔离终端，限制其在网络上的访问。
- **取消隔离 (Unquarantine)** - 取消隔离进程，允许完全访问网络。
- **关闭 (Shutdown)** - 关闭终端连接的 NAS 端口。

步骤 4 点击**提交 (Submit)**。

通过 创建网络访问的授权配置文件

您必须创建一个应该与 配合使用的授权配置文件。您可以在标准授权配置文件列表中查看该授权配置文件。终端可在网络中进行身份验证和授权，但是限用于接入网络。

步骤 1 选择**策略 (Policy)** > **策略元素 (Policy Elements)** > **授权 (Authorization)** > **授权配置文件 (Authorization Profiles)**。

步骤 2 点击**添加 (Add)**。

步骤 3 为授权配置文件输入唯一名称和说明，并将**访问类型 (Access Type)** 更新为 **ACCESS_ACCEPT**。

步骤 4 选中 **DACL Name** 复选框，然后从下拉列表中选择 **DENY_ALL_TRAFFIC**。

步骤 5 点击 **Submit**。

通过 为网络访问创建例外策略

对于 授权，应创建隔离例外策略，该策略先于所有标准授权策略进行处理。例外授权策略用于授权有限访问，满足特殊条件或权限或直接要求。标准授权策略应当保持稳定，适用于大型用户组、设备组以及共享一套常用权限的组。

开始之前

已创建标准授权配置文件以与 配合使用。

步骤 1 选择**策略 (Policy)** > **授权 (Authorization)**，然后展开**例外 (Exceptions)**。

步骤 2 选择**启用 (Enabled)** 或**禁用 (Disabled)** 或**监控唯一选项 (Monitor Only option)**。

步骤 3 点击**创建新规则 (Create a New Rule)**。

步骤 4 输入例外规则名称。

步骤 5 点击加号 [+]，选择身份组。

步骤 6 点击加号 [+]，选择**创建新条件（高级选项）(Create New Condition (Advanced Option))**。

步骤 7 点击第一个字段中的向下箭头，显示字典列表，依次选择**会话 (Session)** > **EPSStatus**。

步骤 8 从第二个字段中的下拉列表选择**等于 (Equals)**。

步骤 9 从第三个字段中的下拉列表选择**隔离 (Quarantine)**。

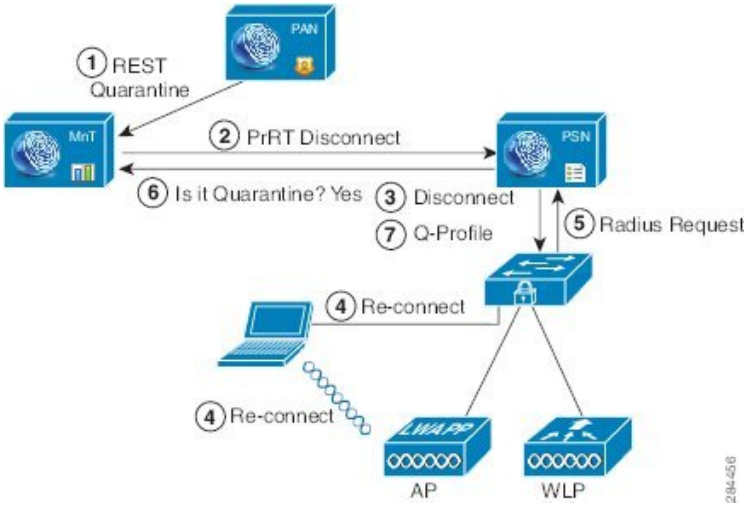
步骤 10 点击**保存 (Save)**。

隔离和取消隔离流程

可以使用 隔离所选终端，以限制其对网络的访问。您可以隔离终端并建立根据状态分配不同授权配置文件的例外授权策略。授权配置文件用作您在授权策略中定义的允许访问指定网络服务的权限的容器。当授权完成时，系统会为网络访问请求授予权限。如果之后对终端进行了验证，则可以对终端取消隔离以允许其对网络进行完全访问。

此图显示了隔离流程，它假定已配置授权规则并已建立 会话。

图 *1:* 隔离流程



1. 客户端设备通过无线设备 (WLC) 登录到网络，并且系统会从管理节点 (PAP) 向监控节点 (MnT) 发出隔离 REST API 调用。
2. 然后，监控节点会通过策略服务思科 ISE 节点 (PDP) 来调用 PrRT，从而引发授权证书 (CoA)。
3. 客户端设备的连接会断开。
4. 然后，客户端设备会重新进行身份验证并重新连接。
5. 对客户端设备的 RADIUS 请求会发回到监控节点。
6. 在进行检查时，系统将隔离客户端设备。
7. 系统将应用 Q-Profile 授权策略并验证客户端设备。
8. 系统会对客户端设备取消隔离，并向其提供对网络的完全访问权限。

NAS 端口关闭流程

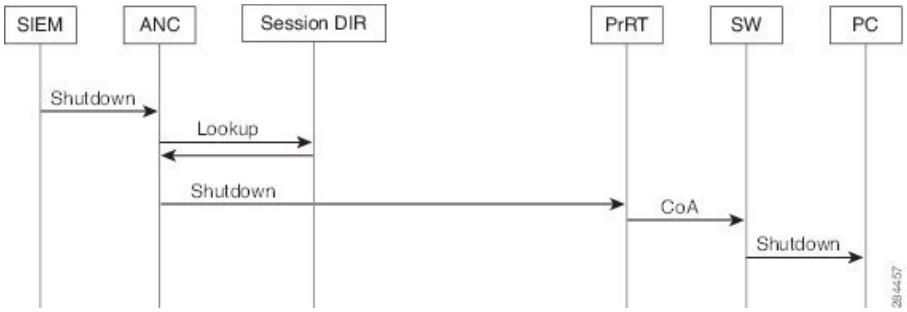
您可以使用终端 IP 地址或 MAC 地址关闭终端所连接的 NAS 端口。

通过此关闭功能您可以根据 MAC 地址的指定 IP 地址关闭 NAS 端口。您必须手动恢复该端口，才能将此终端重新接入网络，这仅对通过有线媒介连接的终端有效。

并非所有设备都支持此关闭功能。不过，大多数交换机应该都支持关闭命令。您可以使用 getResult() 命令验证关闭是否执行成功。

下图说明 关闭流程。对于客户端设备，关闭操作是在客户端设备用于访问网络的 NAS 上执行的。

图 *2:* 关闭流程



终端清除设置

可以根据身份组和其他条件，通过配置规则来定义终端清除策略。选择**管理 (Administration)** > **身份管理 (Identity Management)** > **设置 (Settings)** > **终端清除 (Endpoint Purge)**。您可以选择不清除特定终端以及根据选择的分析条件清除终端。

您可以安排终端清除作业计划。默认情况下，此终端清除计划处于启用状态。默认情况下，思科ISE会删除超出 30 天的终端和已注册设备。系统根据主 PAN 中配置的时区于每日凌晨 1 点（午夜）执行清除作业。

终端清除作业每 3 分钟删除 5000 多个终端。

以下是您可以用于清除终端的一些条件以及示例：

- InactivityDays - 距离终端上最后一次分析活动或更新的天数
  - 此条件用于清除随时间推移累积的陈旧设备，通常是临时访客或个人设备或废弃的设备。在您的部署中，这些终端容易形成干扰，因为它们在网络上不再活动或近期不再可能出现。如果它们偶然再进行连接，系统将在必要的情况下对其进行发现、分析、注册等。
  - 当存在来自终端的更新时，只要启用分析功能，InactivityDays 便会重置为 0。
- ElapsedDays - 创建对象之后经过的天数。
  - 此条件适用于获得特定时间段内未经身份验证或有条件的访问权限的终端，例如访客或承包商终端，或利用 webauth 进行网络访问的员工。在所允许的连接期限到期之后，他们必须重新进行完全身份验证和注册。
- PurgeDate - 要清除终端的日期。
  - 此选项用于在不考虑创建或开始时间的情况下，获得特定时间的访问权限的特殊事件或组。此选项允许同时清除所有终端。例如，贸易展览、会议或每周都有新成员的每周培训课程，在这种情况下，访问权限是根据特定周或月份授予的，而不是绝对的天、周、月。

隔离的终端在策略更改后不会重新进行身份验证

问题

策略或其他身份更改后，身份验证失败，并且系统不会重新进行身份验证。身份验证失败或有问题的终端仍然无法连接网络。根据分配给用户角色的终端安全策略，未能通过安全评估的客户端计算机上经常会出现此问题。

可能的原因

客户端计算机上身份验证计时器的设置不正确，或者交换机上身份验证时间间隔的设置不正确。

解决方案

要解决此问题，有几种可能的办法：

1. 在思科 ISE 中查看指定 NAD 或交换机的**会话状态摘要 (Session Status Summary)** 报告，确保该界面已配置适当的身份验证间隔。
2. 在NAD/交换机上输入“show running configuration”命令，确保接口已配置适当的“authentication timer restart”设置。（例如，“authentication timer restart 15”和“authentication timer reauthenticate 15”。）
3. 输入“interface shutdown”和“no shutdown”退回 NAD/交换机上的端口，并在思科 ISE 的潜在配置更改后，强制重新进行身份验证。

注释 由于 CoA 需要 MAC 地址或会话 ID，因此我们建议您不要重启网络设备 SNMP 报告中显示的端口。

当无法找到 IP 地址或 MAC 地址时， 操作失败。

当终端的活动会话不包含关于IP地址的信息时，在该终端上执行的操作会失败。对于该终端的MAC地址和会话 ID，也存在这种情况。

注释 如果要通过 更改终端的授权状态时，则必须提供该终端的 IP 地址或 MAC 地址。如果在终端的活动会话中无法找到 IP 地址或 MAC 地址，则会看到以下错误消息：

```
No active session found for this MAC address, IP Address or Session ID
```

。

通过外部身份验证的管理员无法执行 操作

如果通过外部身份验证的管理员尝试从实时会话发出 CoA 隔离，思科 ISE 会返回以下错误消息：

```
CoA Action of Quarantine for xx:xx:xx:xx:xx:xx can not be initiated. (Cause:User
 not found internally. Possible use of unsupported externally authenticated user
```

如果通过外部身份验证的管理员在思科 ISE 使用终端的 IP 地址或 MAC 地址从**操作 (Operations)** > **终端保护服务 (Endpoint Protection Service)** > **自适应网络控制 (Adaptive Network Control)** 执行 操作，思科 ISE 会返回以下错误消息：

```
Server failure: User not found internally. Possible use of unsupported externally
 authenticated user
```

备份数据类型

思科 ISE 允许您从主 PAN 和从监控节点备份数据。可以从 CLI 或用户界面完成备份。

思科 ISE 允许您备份以下类型的数据：

- 配置数据 - 包含应用特定和思科 ADE 操作系统配置数据。备份可以使用 GUI 或 CLI 通过主 PAN 完成。
- 运行数据 - 包含监控和故障排除数据。备份可以通过主 PAN GUI 或使用监控节点的 CLI 来完成。

只要以前的版本在以后版本支持的直接升级路径中，就可以使用更低版本的思科 ISE 的备份文件执行恢复操作并且可以在更高版本上执行恢复操作。 上恢复此备份。

注释 在备份和恢复数据后重新创建部署时，需要主 PAN 和辅助 PAN 的 **情景可视性重置** 以确保两个节点上的数据同步。

备份和恢复存储库

思科 允许您通过管理员门户创建和删除存储库。您可以创建以下类型的存储库：

- DISK
- FTP
- SFTP
- NFS

- CD-ROM
- HTTP
- HTTPS

注释 存储库位于每台设备本地位置。

您应为小型部署（100 个终端以下）创建 10 GB 大小的存储库，为中型部署创建 100 GB 大小的存储库，为大型部署创建 200 GB 大小的存储库。

创建存储库

可以使用 CLI 和 GUI 创建存储库。由于以下原因，我们建议您使用 GUI：

- 通过 CLI 创建的存储库保存在本地且不会被复制到其他部署节点。这些存储库不会列于 GUI 的存储库页面。
- 在主 PAN 创建的存储库会被复制到其他部署节点。

开始之前

- 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。

步骤 1 选择 **管理 (Administration)** > **系统 (System)** > > **维护 (Maintenance)** > > **存储库 (Repository)**。

步骤 2 点击**添加 (Add)** 以添加新存储库。

步骤 3 根据需要输入值以设置新存储库。请参阅 存储库设置，第 10 页 以了解字段说明：

步骤 4 点击**提交 (Submit)** 以创建存储库。

步骤 5 通过点击左侧**操作 (Operations)** 导航窗格中的**存储库 (Repository)** 来验证是否成功创建存储库，或点击**存储库 (Repository)** 窗口顶部的**存储库列表 (Repository List)** 链接以转至存储库列表页面。

下一步做什么

- 确保已创建的存储库有效。可以从**存储库列表 (Repository listing)** 窗口执行此操作。选择对应存储库并点击**验证 (Validate)**。或者，您可以从思科 ISE 命令行界面执行以下命令：

  show repository *repository_name*

  其中 *repository_name* 是已创建的存储库的名称。

注释 如果在创建存储库时提供的路径不存在，则会收到以下错误消息：

```
%Invalid Directory
```

- 运行按需备份或安排备份。

存储库设置

表 *1:* 存储库设置

字段	使用指南
Repository	输入存储库的名称。允许使用字母数字字符，最大长度为 80 个字符。
协议 (Protocol)	从可用协议中选择一个您想要使用的协议。
服务器名称 (Server Name)	（对于 TFTP、HTTP、HTTPS、FTP、SFTP 和 NFS 为必填字段）输入您想要在其上创存储库的服务器的主机名或 IPv4 地址。 注释 如果要添加具有 IPv6 地址的存储库，请确保 ISE eth0 接口已配置有 IPv6 地址。
路径 (Path)	输入存储库的路径。此路径必须有效而且在您创建数据库时必须存在。 此值可以用双前斜杠 (//) 或单前斜杠 (/) 开头，表示服务器的根目录。但是，对于 FTP 协议，单前斜杠 (/) 表示 FTP 的本地设备主目录，而不是根目录。
用户名	（对于 FTP、SFTP 和 NFS 为必填字段）输入对指定服务器拥有写入权限的用户名。用户名可以包含字母数字和 _-。/@\$ 字符。
密码 (Password)	（对于 FTP、SFTP 和 NFS 为必填字段）输入用于访问指定服务器的密码。密码可以包含以下字符：0-9、a-z、A-Z、-、.、|、@、#、$、^、&、*、(、)、+、和 =。

相关主题

备份和恢复存储库，第 8 页
创建存储库，第 9 页

按需备份和计划备份

您可以配置主 PAN 和主监控节点的按需备份。当您希望立即备份数据时，系统会执行按需备份。

您可以安排一次性、每日、每周或每月运行系统级备份。由于备份操作持续时间较长，您可以将备份操作安排在空闲时间执行。您可以从管理门户安排备份。

注释 如果使用的是内部 CA，应使用 CLI 导出证书和密钥。在管理门户中使用的备份不会备份 CA 链。

有关详细信息，请参阅《思科身份识别服务引擎管理员指南》的“基本设置”一章中的“导出思科 ISE CA 证书和密钥”部分。

思科 ISE 上的配置和操作备份可能会在短时间内使系统过载。这种预期的临时系统过载行为将取决于系统的配置和监控数据库大小。

相关主题

维护设置

执行按需备份

可以执行按需备份以立即备份配置或监控（操作）数据。恢复操作可将思科 恢复到获取备份时的配置状态。

重要事项 当执行备份和恢复时，恢复功能会使用源系统中的证书列表覆盖目标系统上的受信任证书列表。需要注意的是，备份和恢复功能不包括与内部证书颁发机构 (CA) 证书关联的专用密钥，这一点至关重要。

如果正在从一个系统向另一个系统上执行备份和恢复，必须选择下面一个选项以避免错误：

- **选项 1：**

  通过 CLI 从源 节点导出 CA 证书并通过 CLI 将其导入到目标系统。

  优点：从源系统向终端颁发的所有证书将继续受信任。由目标系统颁发的所有新证书将由同一密钥签名。

  缺点：在恢复功能之前由目标系统颁发的所有证书将不受信任且需要重新颁发。

- **选项 2：**

  在恢复过程之后，为内部 CA 生成所有新证书。

  优点：推荐采用此选项，这是一种较为安全的方法，其中将使用原始源证书或原始目标证书。由原始源系统颁发的证书将继续受信任。

  缺点：在恢复功能之前由目标系统颁发的所有证书将不受信任且需要重新颁发。

开始之前

- 在执行按需备份之前，应对思科 中的备份数据类型有基本的了解。
- 确保已创建存储备份文件的存储库。
- 不要使用本地存储库进行备份。您无法在远程监控节点的本地存储库中备份监控数据。

- 确保在获取备份之前执行所有证书相关的更改。
- 要执行以下任务，您必须是超级管理员或系统管理员。

注释 对于备份和恢复操作，系统不支持以下存储库类型：CD-ROM、HTTP、HTTPS 或 TFTP。这是因为，这些存储库类型为只读或者协议不支持文件列表。要恢复备份，请选择存储库，然后点击**恢复 (Restore)**。

相关主题

思科 ISE 恢复操作，第 15 页
导出身份验证和授权策略配置，第 21 页

按需备份设置

下表介绍**按需备份 (On-Demand Backup)** 窗口上的字段，您可以随时使用此窗口获取备份。此窗口的导航路径为： **管理 (Administration)** > **系统 (System)** > **备份和恢复(Backup & Restore)**。

表 *2:* 按需备份设置

字段名称	使用指南
Backup Name	输入备份文件的名称。
Repository Name	应该保存您的备份文件的存储库。您无法在此处输入存储库。只能从下拉列表选择一个可用存储库。确保在运行备份之前创建了存储库。
Encryption Key	此密钥用于加密和解密备份文件。

相关主题

备份数据类型，第 8 页
按需备份和计划备份，第 10 页
备份历史记录，第 14 页
备份失败，第 15 页
思科 ISE 恢复操作，第 15 页
导出身份验证和授权策略配置，第 21 页
在分布式环境中同步主节点和辅助节点，第 21 页
执行按需备份，第 11 页

计划备份

可以执行按需备份以立即备份配置或监控（操作）数据。恢复操作可将思科 恢复到获取备份时的配置状态。

重要事项 当执行备份和恢复时，恢复功能会使用源系统中的证书列表覆盖目标系统上的受信任证书列表。需要注意的是，备份和恢复功能不包括与内部证书颁发机构(CA)证书关联的专用密钥，这一点至关重要。

如果您正在从一个系统向另一个系统上执行备份和恢复，您将必须选择下面一个选项以避免错误：

- **选项 1**：

  通过 CLI 从源 节点导出 CA 证书并通过 CLI 将其导入到目标系统。

  优点：从源系统向终端颁发的所有证书将继续受信任。由目标系统颁发的所有新证书将由同一密钥签名。

  缺点：在恢复功能之前由目标系统颁发的所有证书将不受信任且需要重新颁发。

- **选项 2**：

  在恢复过程之后，为内部 CA 生成所有新证书。

  优点：推荐采用此选项，这是一种较为安全的方法，其中将使用原始源证书或原始目标证书。由原始源系统发布的证书将继续受信任。

  缺点：在恢复功能之前由目标系统颁发的所有证书将不受信任且需要重新颁发。

开始之前

- 在安排备份之前，应对思科 中的备份数据类型有基本的了解。
- 确保已配置存储库。
- 不要使用本地存储库进行备份。您无法在远程监控节点的本地存储库中备份监控数据。
- 要执行以下任务，您必须是超级管理员或系统管理员。

注释 对于备份和恢复操作，系统不支持以下存储库类型：CD-ROM、HTTP、HTTPS 或 TFTP。这是因为，这些存储库类型为只读或者协议不支持文件列表。

步骤 1 选择 **选择管理 (Administration)** > **系统 (System)** > **备份和恢复 (Backup and Restore)**。

步骤 2 点击**创建 (Create)**，安排配置或操作备份。

步骤 3 输入安排备份所需的值。

步骤 4 点击**保存 (Save)**，安排备份。

步骤 5 点击此页面顶部的**刷新 (Refresh)** 链接，查看计划的备份列表。

一次只能为配置或操作备份创建一个计划。可以启用或禁用计划的备份，但不能将其删除。

计划备份设置

下表介绍“定期备份”(Scheduled Backup) 窗口上的字段，您可以使用此窗口恢复完整备份或增量备份。此窗口的导航路径为： **管理 (Administration)** > **系统 (System)** > **备份和恢复(Backup and Restore)**。

表 *3:* 计划备份设置

字段名称	使用指南
Name	输入备份文件的名称。您可以输入您所选的描述性名称。思科 ISE 会将时间戳附加到备份文件名之后并将其存储在存储库中。即使您配置了一系列备份，也要有唯一的备份文件名。在“定期备份”(Scheduled Backup) 列表窗口上，备份文件名前面将附加“backup_occur”，表示文件是一次 **kron** 作业。
Description	输入对备份的说明。
Repository Name	选择保存您的备份文件的存储库。您无法在此处输入存储库。只能从下拉列表选择一个可用存储库。确保在运行备份之前创建了存储库。
Encryption Key	输入用于加密和解密备份文件的密钥。
Schedule Options	选择计划备份的频率并相应地填写其他选项。

相关主题

备份数据类型，第 8 页
按需备份和计划备份，第 10 页
备份历史记录，第 14 页
备份失败，第 15 页
思科 ISE 恢复操作，第 15 页
导出身份验证和授权策略配置，第 21 页
在分布式环境中同步主节点和辅助节点，第 21 页
使用 CLI 备份，第 14 页
计划备份，第 12 页

使用 CLI 备份

虽然可以从 CLI 和 GUI 安排备份，但是建议使用 GUI。不过，只能从 CLI 对辅助监控节点执行操作备份。

备份历史记录

备份历史记录提供关于定时备份和按需备份的基本信息。它会列出备份名称、备份文件大小、存储备份的库以及指明获得备份的时间的时间戳。此信息在操作审核报告以及历史记录表的 Backup and Restore 页面上列出。

对于故障备份，思科 将触发警报。备份历史记录页面提供故障原因。操作审核报告也引用故障原因。如果故障原因缺失或不清楚，您可以从思科 ISE CLI 运行 **backup-logs** 命令，查看 ADE.log 了解更多信息。

在备份操作运行的过程中，您可以使用 **show backup status** CLI 命令查看备份操作的进度。

备份历史记录与思科 ADE 操作系统配置数据一起存储。甚至在应用升级后历史记录依然存在，只有当您重置 PAN 映像时才能将历史记录删除。

备份失败

如果备份失败，请检查以下事宜：

-
- 确保没有同时运行任何其他备份。
- 检查已配置存储库的可用磁盘空间。
  - 如果监控数据占用的空间超过所分配的监控数据库大小的 75%，则监控（操作）备份会失败。例如，如果向监控节点分配的空间为 600 GB，而监控数据占用超过 450 GB 的存储空间，则监控备份会失败。
  - 如果数据库磁盘使用量超过 90%，系统会执行清除操作，使数据库的大小小于或等于所分配空间的 75%。
- 验证是否正在进行清除。进行清除时，备份和恢复操作不起作用。
- 验证存储库的配置是否正确。

思科 ISE 恢复操作

可以在主管理节点或独立管理节点上恢复配置数据。在主 PAN 上恢复数据后，必须手动将辅助节点与主 PAN 同步。

恢复运营数据的过程根据部署类型而异。

注释 思科 中新的备份/恢复用户界面利用备份文件名中的元数据。因此，在备份完成后，不应手动修改备份文件名。如果手动修改备份文件名，则思科 备份/恢复用户界面将无法识别备份文件。如果必须修改备份文件名，应使用思科 ISE CLI 恢复备份。

数据恢复指南

下面提供了恢复思科 备份数据时应遵守的指南。

- 利用思科 ISE，您可以从 ISE 节点 (A) 获取备份并将其存储到另一个 ISE 节点 (B) 上，这两个节点有相同的主机名（但 IP 地址不同）。但是，当您在节点 B 上恢复备份后，不会更改节点 B 的主机名，因为这样做可能会导致证书和门户组标记出现问题。
- 如果在一个时区内从主PAN获取备份，并尝试在另一时区中的另一个思科 节点上恢复该备份，恢复过程可能失败。如果备份文件中的时间戳晚于恢复备份所在的思科 节点上的系统时间，则会发生此故障。如果在获得备份之后一天恢复备份，那么备份文件中的时间戳则为过去时间，恢复过程将成功。
- 当主 PAN 上恢复的备份所使用的主机名不同于获得备份的主机名时，此主 PAN 将成为独立节点。部署已损坏，辅节点将无法运行。您必须使独立节点成为主节点，重置辅节点上的配置，并在主节点上重新注册这些辅节点。要重置思科节点上的配置，请从思科 ISE CLI 输入以下命令：
  - **application reset-config ise**
- 建议您在初始思科 安装和设置之后，不要更改系统时区。
- 如果更改了部署中的一个或多个节点上的证书配置，则必须获得另一个备份才能从独立思科 节点或主 PAN 恢复数据。否则，如果您尝试使用旧备份恢复数据，节点之间的通信可能失败。
- 在主 PAN 上恢复配置备份后，可以导入先前导出的思科 ISE CA 证书和密钥。

注释 如果没有导出思科 ISE CA 证书和密钥，则在主 PAN 上恢复配置备份后，在主 PAN 和策略服务节点 (PSN) 上生成根 CA 和从属 CA。

- 如果尝试恢复白金级数据库而没有使用正确的 FQDN（白金级数据库的 FQDN），则需要重新生成 CA 证书。（选择**管理 (Administration) > 证书 (Certificates) > 证书签名请求 (Certificate Signing Requests) > 更换 ISE 根 CA 证书链 (Replace ISE Root CA certificate chain)**）。不过，如果使用正确的 FQDN 恢复白金级数据库，请注意 CA 证书将自动重新注册。
- 需要一个数据存储库，供思科 保存备份文件。您必须创建一个存储库，然后才能运行按需备份或定期备份。
- 如果有一个独立管理节点发生故障，则必须运行配置备份进行恢复。如果主 PAN 发生故障，则可以使用分布式设置，将辅助管理节点升级为主管理节点。实现之后，可以在主 PAN 上恢复数据。

注释 思科 还提供 **backup-logs** CLI 命令，可用来收集日志和配置文件以用于故障排除。

从 CLI 恢复配置或监控（操作）备份

要通过思科 ISE CLI 恢复配置数据，请在执行模式下使用 **restore** 命令。使用以下命令从配置或操作备份恢复数据：

restore *filename* **repository** *repository-name* **encryption-key hash|plain** *encryption-key name* **include-adeos**

语法说明

restore	键入此命令，从配置或操作备份恢复数据。
filename	驻留在存储库的备份文件的名称。最多支持 120 个字母数字字符。 **注释** 必须在文件名后面添加 .tar.gpg 扩展名（例如，myfile.tar.gpg）。
repository	指定包含备份的存储库。
repository-name	您想要从其恢复备份的存储库的名称。
encryption-key	（可选）指定用户定义的加密密钥以恢复备份。
hash	恢复备份的散列加密密钥。指定跟随的加密（散列）加密密钥。最多支持 40 个字符。
plain	用于恢复备份的明文加密密钥。指定跟随的未加密密文加密密钥。最多支持 15 个字符。
encryption-key name	输入加密密钥。
include-adeos	（可选，仅适用于配置备份）如果您想要从配置备份恢复 ADE-OS 配置，请输入此命令运算符参数。当您恢复配置备份，如果不包含此参数，思科 ISE 仅恢复思科 ISE 应用配置数据。

默认值

无默认行为或值。

命令模式

EXEC

使用指南

在思科 中使用 restore 命令时，思科 服务器会自动重新启动。

恢复数据时，加密密钥为可选。要在您未提供加密密钥的情况下，支持恢复更早的备份，您可以使用 **restore** 命令，无需加密密钥。

示例

```
ise/admin# restore mybackup-100818-1502.tar.gpg repository myrepository encryption-key plain
```

```
 Lab12345
Restore may require a restart of application services. Continue? (yes/no) [yes] ? yes
Initiating restore.  Please wait...
ISE application restore is in progress.
This process could take several minutes. Please wait...
Stopping ISE Application Server...
Stopping ISE Monitoring & Troubleshooting Log Processor...
Stopping ISE Monitoring & Troubleshooting Log Collector...
Stopping ISE Monitoring & Troubleshooting Alert Process...
Stopping ISE Monitoring & Troubleshooting Session Database...
Stopping ISE Database processes...
Starting ISE Database processes...
Starting ISE Monitoring & Troubleshooting Session Database...
Starting ISE Application Server...
Starting ISE Monitoring & Troubleshooting Alert Process...
Starting ISE Monitoring & Troubleshooting Log Collector...
Starting ISE Monitoring & Troubleshooting Log Processor...
Note: ISE Processes are initializing. Use 'show application status ise'
      CLI to verify all processes are in running state.
ise/admin#
```

相关命令

	说明
backup	执行备份（思科 和思科 ADE OS），将备份放在存储库中。
backup-logs	备份系统日志。
repository	输入备份配置的存储库子模式。
show repository	显示位于特定存储库上的可用备份文件。
show backup history	显示系统的备份历史记录。
show backup status	显示备份操作的状态。
show restore status	显示恢复操作的状态。

如果任何辅助节点的应用恢复后同步状态和复制状态为 不同步 *(Out of Sync)*，则必须将此辅助节点的证书重新导入主 PAN，执行手动同步。

从 GUI 恢复配置备份

可以从管理门户恢复配置备份。

开始之前

在配置备份期间，如果您的部署是双节点部署，请确保满足以下条件：

- 如果用于恢复的源节点和目标节点与用于配置备份的相应节点相同，目标节点可以是独立节点或主节点。
- 如果用于恢复的源节点和目标节点与用于配置备份的相应节点不同，目标节点必须是独立节点。

注释 可以仅在主 PAN 上恢复配置数据库备份和重新生成根 CA。不过，无法恢复注册 PAN 上的配置数据库备份。

步骤 1 选择 **选择管理 (Administration)** > **系统 (System)** > **备份和恢复 (Backup and Restore)**。

步骤 2 从配置备份列表中选择备份名称，然后单击**恢复 (Restore)**。

步骤 3 输入在备份过程中使用的加密密钥。

步骤 4 点击 **Restore**。

下一步做什么

如果使用思科 ISE CA 服务，必须：

1. 重新生成整个思科 ISE CA 根链。
2. 从主 PAN 获取思科 ISE CA 证书和密钥的备份，然后在辅助 PAN 上恢复备份。这样确保了辅助 PAN 可以在主 PAN 故障时用作外部 PKI 的根 CA 或从属 CA，您可将辅助 PAN 升级为主 PAN。

恢复监控数据库

恢复监控数据库的流程因部署类型不同而异。以下各节介绍如何在独立和分布式部署中恢复监控数据库。

必须使用 CLI 从思科 ISE 的先前版本恢复按需监控数据库备份。不支持跨思科 ISE 版本恢复定期备份。

注释 如果尝试将数据恢复到调取数据所在节点以外的节点，必须将日志记录目标设置配置为指向新节点。这可以确保监控系统日志发送到正确节点。

在独立环境中恢复监控（运行）备份

GUI 只列出从当前版本提取的备份。要恢复从早期版本获取的备份，请从 CLI 使用恢复命令。

开始之前

- 清除旧的监控数据。
- 计划备份或执行按需备份。

步骤 1 选择**管理 (Administration)** > **系统 (System)** > **备份和恢复 (Backup and Restore)**。

步骤 2 从操作备份列表中选择备份的名称，然后点击 **Restore**。

步骤 3 输入在备份过程中使用的加密密钥。

步骤 4 点击**恢复 (Restore)**。

通过管理和监控角色恢复监控备份

您可以使用管理和监控角色在分布式环境中恢复监控备份。

开始之前

- 清除旧的监控数据。
- 计划备份或执行按需备份。

步骤 1 如果使用的是主 PAN 和辅助 PAN，请同步 PAN。

同步 PAN 时，必须选择一个 PAN 并将其升级为活动的主 PAN。

步骤 2 在注销监控节点之前，应将监控角色分配给部署中的其他节点。

每个部署必须至少有一个正常运行的监控节点。

步骤 3 注销监控节点以进行备份。

步骤 4 将监控备份恢复到最近注销的节点。

步骤 5 向当前管理节点注册新恢复的节点。

步骤 6 将新恢复和注册的节点升级为主用监控节点。

通过监控角色恢复监控备份

只能通过监控角色恢复分布式环境中的监控备份。

开始之前

- 清除旧的监控数据。
- 计划备份或执行按需备份。

步骤 1 准备取消注册要恢复的节点。这是通过将监控角色分配给部署中的另一个节点来完成的。

部署必须至少有一个正常运行的监控节点。

步骤 2 取消注册要恢复的节点。

注释 请等待，直到取消注册完成后，再继续执行恢复操作。该节点必须处于独立状态，然后您才能继续执行恢复操作。

步骤 3 将监控备份恢复到最近注销的节点。

步骤 4 向当前管理节点注册新恢复的节点。

步骤 5 将新恢复和注册的节点升级为主用监控节点。

恢复历史记录

可以从**操作审核报告 (Operations Audit Report)** 中获取所有恢复操作、日志事件和状态的相关信息。

注释 但**操作审核报告 (Operations Audit Report)** 窗口不提供与之前的恢复操作对应的起始时间的相关信息。

要获得故障排除信息，必须从思科 ISE CLI 运行 **backup-logs** 命令并查看 ADE.log 文件。

在恢复操作进行过程中，所有思科 服务都会停止。可以使用 CLI 命令 **show restore status** 查看恢复操作的进度。

导出身份验证和授权策略配置

您可以将身份验证和授权策略配置导出为 XML 文件，您可以离线阅读此文件以识别任何配置错误并用于故障排除。此 XML 文件包括身份验证和授权策略规则、简单和复合策略条件、自主访问控制列表 (dACL) 和授权配置文件。您可以选择以邮件方式发送 XML 文件或将其保存在本地系统中。

步骤 1 选择 **管理 (Administration)** > **系统 (System)** > **备份和恢复 (Backup & Restore)**。

步骤 2 点击**策略导出 (Policy Export)**。

步骤 3 根据需要输入值。

步骤 4 点击**导出 (Export)**。

使用文本编辑器，例如 WordPad，查看 XML 文件的内容。

在分布式环境中同步主节点和辅助节点

在分布式环境中，在PAN上恢复备份文件之后，主节点和辅助节点中的思科数据库有时不会自动同步。如果发生这种情况，可以手动强制从 PAN 完全复制到辅助节点。只能强制从 PAN 同步到辅助节点。在同步操作过程中，无法进行任何配置更改。通过思科，只能在同步完成后导航至其他思科管理员门户页面和进行配置更改。

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 **管理 (Administration)** > **系统 (System)** > **部署 (Deployment)**。

步骤 2 选中处于不同步复制状态的辅助 ISE 节点旁边的复选框。

步骤 3 点击**同步 (Syncup)**，等到节点与 PAN 同步。必须等到此流程完成，然后才能再次访问思科管理员门户。

恢复独立和分布式部署中断开的节点

此部分提供可用于恢复独立和分布式部署中断开的节点的故障排除信息。以下某些使用案例使用备份和恢复功能，而其他使用案例则使用复制功能恢复已丢失的数据。

使用现有 IP 地址和主机名恢复分布式部署中断开连接的节点

场景

在分布式部署中，一场自然灾害导致丢失了所有节点。在恢复之后，您想要使用现有 IP 地址和主机名。

例如，您有两个节点：N1（主策略管理节点，即主PAN）和N2（辅助策略管理节点，即辅助PAN）。可提供在时间 T1 执行的 N1 节点的备份。后来，由于自然灾害，N1 和 N2 节点都出现了故障。

假定条件

部署中的所有思科 节点都已被破坏。已使用相同的主机名和 IP 地址对新硬件进行映像。

解决步骤

1. 您必须更换 N1 和 N2 节点。N1 和 N2 节点现在具有独立配置。
2. 用 N1 和 N2 节点的 UDI 获取许可证并将其安装在 N1 节点上。
3. 然后，您必须在更换的 N1 节点上恢复备份。恢复脚本将尝试在 N2 上同步数据，但是，N2 现已成为独立节点，所以同步失败。N1 上的数据将重置至时间 T1。
4. 您必须登录 N1 Admin 门户以删除和重新注册 N2 节点。N1 和 N2 节点都将使数据重置至时间 T1。

使用新 IP 地址和主机名恢复分布式部署中断开的节点

场景

在分布式部署中，一场自然灾害导致丢失了所有节点。新硬件在新位置进行了重新镜像并且需要新的 IP 地址和主机名。

例如，您有两个 节点：N1（主策略管理节点，即主 PAN）和 N2（辅助策略服务节点）。系统可以提供在时间 T1 执行的 N1 节点备份。后来，由于自然灾害，N1 和 N2 节点都出现了故障。思科 节点在新位置被替换，新主机名为 N1A（主 PAN）和 N2A（辅助策略服务节点）。此处 N1A 和 N2A 都是独立节点。

假定条件

部署中的所有思科 节点都已被破坏。新硬件已使用不同的主机名和 IP 地址在另一位置进行镜像。

解决步骤

1. 获取 N1 备份并在 N1A 上恢复此备份。恢复脚本将识别主机名更改和域名更改，并且将根据当前主机名在部署配置中更新主机名和域名。
2. 您必须生成新的自签证书。
3. 必须在 N1A 上登录思科 管理员门户，选择**管理 (Administration)** > **系统 (System)** > **部署 (Deployment)**，然后执行以下操作：

   删除旧 N2 节点。

   将新 N2A 节点注册为辅助节点。系统会将 N1A 节点的数据复制到 N2A 节点。

使用现有 IP 地址和主机名恢复独立部署中的节点

场景

独立管理节点出现故障。

例如，您有一个独立管理节点 N1。已在时间 T1 执行 N1 数据库的备份。N1 节点由于物理故障宕机，必须重置映像此节点或需要使用新的硬件。必须以相同的 IP 地址和主机名恢复 N1 节点。

假定条件

此部署是独立部署，而且新硬件或重置映像的硬件具有相同的 IP 地址和主机名。

解决步骤

N1 节点在重置映像或您采用具有相同 IP 地址和主机名的新思科 节点后开始运行时，您必须从旧 N1 节点恢复备份。您无需执行任何角色变更。

使用新 IP 地址和主机名恢复独立部署中的节点

场景

独立管理节点出现故障。

例如，您有一个独立管理节点 N1。系统可以提供在时间 T1 执行的 N1 数据库备份。N1 节点由于物理故障而宕机，此节点更换为另一位置具有不同 IP 地址和主机名的新硬件。

假定条件

这是独立部署，并且所更换的硬件具有不同的 IP 地址和主机名。

解决步骤

1. 使用新硬件更换 N1 节点。此节点将处于独立状态，主机名为 N1B。
2. 您可以在 N1B 节点恢复备份。不需要更改角色。

配置回滚

问题

有时候，您可能会不小心更改配置，然后您发现所做的更改不正确。例如，您可能会错误地删除几个 NAD 或修改一些 RADIUS 属性，然后在数小时后才发现这个问题。在这种情况下，可以通过恢复您在进行更改之前所做的备份，恢复原来的配置。

可能的原因

有两个节点：N1（主策略管理节点，即主 PAN）和 N2（辅助策略管理节点，即辅助 PAN），并且可提供 N1 节点的备份。您在 N1 节点上做了一些错误的配置更改并且想要撤消更改。

解决方案

获取在执行错误的配置更改之前所执行的 N1 节点备份。在 N1 节点上恢复此备份。恢复脚本会将数据从 N1 同步至 N2。

在分布式部署出现故障的情况下恢复主节点

场景

在多节点部署中，PAN 出现故障。

例如，您有两个思科 节点：N1 (PAN) 和 N2（辅助管理节点）。由于硬件问题，N1 出现了故障。

假定条件

仅分布式部署中的主节点出现故障。

解决步骤

1. 登录 N2 管理员门户。选择**管理 (Administration)** > **系统 (System)** > **部署 (Deployment)**，并将 N2 配置为主节点。

   使用新硬件更换 N1 节点，重新镜像此节点并使之处于独立状态。

2. 从 N2 管理员门户，将新的 N1 节点注册为辅助节点。

   现在，N2 节点就成为您的主要节点，而 N1 节点则成为您的辅助节点。

如果您希望重新将 N1 节点设置为主要节点，请登录 N1 Admin 门户并将其设置为主要节点。N2 就自动成为辅助服务器。不会有数据丢失。

在分布式部署出现故障的情况下恢复辅助节点

场景

在多节点部署中，一个辅助节点出现故障。无需恢复。

例如，具有多个节点：N1（主 PAN）、N2（辅助 PAN）、N3（辅助策略服务节点）、N4（辅助策略服务节点）。其中一个辅助节点 N3 出现故障。

解决步骤

1. 将新的 N3A 节点重新映像到默认独立状态。
2. 登录到 N1 管理门户并删除 N3 节点。
3. 重新注册 N3A 节点。

   数据将从 N1 复制到 N3A。无需恢复。

思科 日志记录机制

思科 提供用于审核、故障管理和故障排除的日志记录机制。日志记录机制可以帮助您识别所部署的服务中的故障情况并有效地对相应问题进行故障排除。它还以一致的方式从监控和故障排除主要节点提供日志记录输出。

您可以将思科 ISE 配置为使用虚拟环回地址在本地系统中收集日志。要从外部收集日志，您可以配置外部系统日志服务器，这些服务器称为目标。日志分为多个预定义的类别。您可以根据各个类别的目标、严重性级别等编辑各个类别，以自定义日志记录输出。

作为最佳实践，请勿将网络设备配置为思科 ISE 监控和故障排除 (MnT) 节点，因为这会导致一些网络访问设备 (NAD) 系统日志丢失，并使 MnT 服务器过载，进而导致加载问题。

注释 如果将监控节点配置为网络设备的系统日志服务器，请确保该日志源按照如下格式发送正确的网络接入服务器 (NAS) IP 地址：

<message_number>sequence_number: NAS_IP_address: timestamp: syslog_type: <message_text>

否则，这可能会影响依赖 NAS IP 地址的功能。

配置系统日志清除设置

使用此流程可设置本地日志存储期，并可在一定时间后删除本地日志。

步骤 1 选择 **选择管理 (Administration)** > **系统 (System)** > **日志记录 (Logging)** > **本地日志设置 (Local Log Settings)**。

步骤 2 在 **Local Log Storage Period** 字段中，输入要将日志条目保留在配置源中的最大天数。

如果 localStore 文件夹达到 97 GB，则可能会早于配置的**本地日志存储期 (Local Log Storage Period)** 而删除日志。

步骤 3 点击**立即删除日志 (Delete Logs Now)** 可在存储期到期前的任何时间删除现有日志文件。

步骤 4 点击**保存 (Save)**。

思科 ISE 系统日志

在思科 ISE 中，日志记录目标的位置会收集系统日志。目标是指收集和存储日志的服务器的 IP 地址。您可以在本地生成和存储日志，也可以使用 FTP 工具将日志传输至外部服务器。思科 ISE 具有以下默认目标，在本地系统的环回地址中会动态配置这些目标：

- LogCollector - 日志收集器的系统日志默认目标。
- ProfilerRadiusProbe - 分析器 RADIUS 探测功能的默认系统日志目标。

默认情况下，在执行全新思科 ISE 安装或升级期间会禁用 AAA 诊断子类别和系统诊断子类别日志记录目标，以减少磁盘空间。您可以为这些子类别手动配置日志记录目标，但这些子类别的本地日志记录始终处于启用状态。

您可以使用在思科 ISE 安装结束时在本地配置的默认日志记录目标，也可以创建外部目录来存储日志。

相关主题

思科 ISE 消息代码，第 28 页

配置远程系统日志收集位置

您可以使用 Web 界面创建向其发送系统日志消息的远程系统日志服务器目标。日志消息根据系统日志协议标准被发送至远程系统日志服务器目标（请参阅 RFC-3164）。系统日志协议为非安全 UDP。

当发生某一事件时，系统会生成消息。事件可能是显示状态的事件，例如当存在某个程序时显示的消息，或报警。诸如内核、电子邮件和用户级别等多个设施会生成不同类型的事件消息。事件消息与严重性级别相关，它允许管理员过滤消息并将其进行优先级排序。数字代码被分配给该设备和严重性级别。系统日志服务器为事件消息收集器并从这些设施收集事件消息。管理员可以基于其严重性级别选择将消息转发至哪个事件消息收集器。

UDP 系统日志（日志收集器）是默认远程日志记录目标。当禁用此日志记录目标时，它不会再充当日志收集器，并且系统会将其从**日志记录类别 (Logging Categories)** 窗口中删除。当启用此日志记录目标时，它会成为**日志记录类别 (Logging Categories)** 窗口中的日志收集器。

注释 对默认远程日志记录目标 **SecureSyslogCollector** 的任何更改都会导致思科 ISE 监控和故障排除日志处理器服务重新启动。

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 输入必要的详细信息。

步骤 4 点击 **Save**。

步骤 5 转至 Remote Logging Targets 页面，然后验证新的目标是否创建。

然后，可以将日志记录目标映射到下面的每个日志记录类别。PSN 节点根据这些节点上启用的服务将相关日志发送到远程日志记录目标。

- AAA 审核
- AAA 诊断
- 记账
- 外部 MDM
- 被动 ID
- 终端安全评估和客户端调配审核
- 终端安全评估和客户端调配诊断
- Profiler

部署中的所有节点会将以下类别的日志发送到日志记录目标：

- 管理和操作审核

- 系统诊断
- 系统统计项

思科 ISE 消息代码

日志记录类别是用于说明功能、流程或用例的消息代码的捆绑包。在思科 ISE 中，每条日志根据日志消息内容与日志记录类别所捆绑的消息代码相关联。日志记录类别帮助说明其包含的消息的内容。

日志记录类别可升级日志记录配置。每个类别具有可以根据应用要求进行设置的名称、目标和严重性级别。

思科 ISE 为可以向其分配日志目标的 Posture、Profiler、Guest、AAA（身份验证、授权和记帐）等服务提供预定义日志记录类别。

对于日志记录类别**通过的身份验证 (Passed Authentications)**，默认情况下禁用允许本地日志记录的选项。启用此类别的本地日志记录将导致操作空间利用率高，并填写 prrt-server.log 与 iseLocalStore.log。

如果您选择为**通过的身份验证 (Passed Authentications)** 启用本地日志记录，请转至**管理 (Administration)** > **系统 (System)** > **日志记录 (Logging)** > **日志记录类别 (Logging Categories)**，从类别部分中单击**通过的身份验证 (Passed Authentications)**然后选中**本地日志记录 (Local Logging)** 复选框。

相关主题

设置消息代码的严重性级别 ，第 28 页

设置消息代码的严重性级别

您可以设置日志严重性级别，选择存储所选类别的日志的日志记录目标。

步骤 1 选择**管理 (Administration)** > **系统 (System)** > **日志记录 (Logging)** > **日志记录类别 (Logging Categories)**。

步骤 2 点击想要编辑的类别旁边的单选按钮，点击 **Edit**。

步骤 3 修改必填字段值。

步骤 4 点击 **Save**。

步骤 5 转至 Logging Categories 页面，验证对特定类别所做的配置更改。

思科 ISE 消息目录

您可以使用“消息目录”(Message Catalog) 页面查看所有可能的日志消息和说明。依次选择**管理 (Administration)** > **系统 (System)** > **日志记录 (Logging)** > **消息目录 (Message Catalog)**。。

系统将显示“日志消息目录”(Log Message Catalog) 页面，您可以在此查看所有显示在日志文件中可能的日志消息。 此页面中的数据仅供显示 。

请参阅思科 ISE 系统日志，了解思科 ISE 发送的系统日志消息的综合列表、它们的含义以及它们如何记录在本地和远程目标中。

调试日志

调试日志可捕获引导程序 (bootstrap)、应用配置、运行时间、部署、监控、报告和公共密钥基础设施 (PKI) 信息。调试日志包含过去 30 天内的严重和警告警报和过去 7 天内的信息警报。

您可以为单个组件配置调试日志严重级别。

您可以将调试日志存储在本地服务器中。

注释 从备份恢复系统或将其升级后，未保存调试日志配置。

相关主题

配置调试日志严重性级别，第 30 页

查看节点的日志记录组件

步骤 1 依次选择**管理 (Administration)** > **系统 (System)** > **日志记录 (Logging)** > **调试日志配置 (Debug Log Configuration)**。

步骤 2 选择要查看其日志记录组件的节点，然后点击**编辑 (Edit)**。

系统将显示“调试级别配置 (Debug Level Configuration)”页面。您可以查看以下详细信息：

- 基于所选节点上运行的服务的日志记录组件列表
- 每个组件的说明
- 为各个组件设置的当前日志级别

相关主题

配置调试日志严重性级别，第 30 页

配置调试日志严重性级别

可以配置调试日志的严重性级别。

步骤 1 选择**管理 (Administration)** > **系统 (System)** > **日志记录 (Logging)** > **调试日志配置 (Debug Log Configuration)**。

步骤 2 选择节点，然后单击**编辑 (Edit)**。

“调试日志配置”(Debug Log Configuration) 页面会根据在选定节点中运行的服务显示组件列表，以及为各个组件设置的当前日志级别。

步骤 3 选择要为其配置调试日志严重性级别的组件，然后单击**编辑 (Edit)**。从**日志级别 (Log Level)** 下拉列表中选择所需的日志严重性级别，然后单击**保存 (Save)**。

注释 更改runtime-AAA组件的日志严重性级别，会导致其子组件prrt-JNI的日志级别也发生更改。子组件日志级别的更改不会影响其父组件。

相关主题

配置调试日志严重性级别 ，第 30 页

思科 调试日志

终端调试日志收集器

要排除特定终端的问题，可以根据其 IP 地址或 MAC 地址为该特定终端下载调试日志。该特定终端专用部署中的各个节点的日志收集在一个文件中，从而帮助您快速、有效地排除问题。一次只能对一个终端运行此故障排除工具。日志文件列于 GUI 中。您可以为部署中的一个节点或所有节点的终端下载日志。

下载特定终端的调试日志

要解决与网络中的特定终端相关的问题，可以从管理员门户使用调试终端工具。或者，可以从 Authentications 页面运行此工具。从 Authentications 页面右键点击 Endpoint ID，然后点击 **Endpoint Debug**。此工具在一个文件中提供关于特定终端的所有服务的所有调试信息。

开始之前

需要准备收集其调试日志的终端的 IP 地址或 MAC 地址。

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)** > **终端调试 (Endpoint Debug)**。

步骤 2 点击 **MAC Address** 或 **IP** 单选按钮，输入终端的 MAC 或 IP 地址。

步骤 3 如果想要在指定的时间之后停止日志收集，请选中 **Automatic disable after *n* Minutes** 复选框。如果选中此复选框，必须输入 1 和 60 分钟之间的时间值。

显示以下消息：“Endpoint Debug degrades the deployment performance. Would you like to continue?”

步骤 4 点击 **Continue** 收集日志。

步骤 5 当想要手动停止日志收集时，请点击 **Stop**。

相关主题

终端调试日志收集器，第 30 页

集合过滤器

您可以配置集合过滤器来禁止将系统日志消息发送到监控节点和外部服务器。可以根据不同属性类型在策略服务节点级别执行禁止。您可以使用特定属性类型和对应的值定义多个过滤器。

在将系统日志消息发送到监控节点或外部服务器之前，思科 ISE 会将这些值与要发送的系统日志消息中的字段进行比较。如果找到任何匹配项，则不会发送对应的消息。

注释 如果为任何**属性**和**过滤器类型**配置了收集过滤器（**管理 (Administration)** > **系统 (System)** > **日志记录 (Logging)** > **收集过滤器 (Collection Filter)**）；并且您还选中了**在 n 天不活动后禁用账户 (Disable account after n days of inactivity)** 复选框（**管理 (Administration)** 、 > **身份管理 (Identity Management)** 、 > **用户身份验证设置 (User Authentication Settings)**、 > **禁用账户策略 (Disable Account Policy)**），您的账户可能会因身份验证成功的系统日志消息未中继到监控节点而被禁用。

配置集合过滤器

您可以根据各种属性类型配置一系列集合过滤器。建议将过滤器数限制在20个以内。您可以添加、编辑或删除集合过滤器。

步骤 1 选择**管理 (Administration)** > **系统 (System)** > **日志记录 (Logging)** > **集合过滤器 (Collection Filters)**。

步骤 2 点击 **Add**。

步骤 3 从以下列表选择 **Filter Type**：

- User Name
- MAC Address
- Policy Set Name
- NAS IP Address
- Device IP Address

步骤 4 为您已选的过滤器类型选择对应的 **Value**。

步骤 5 从下拉列表中选择 **Result**。结果可能是 All、Passed 或 Failed。

步骤 6 点击**提交 (Submit)**。

相关主题

集合过滤器，第 31 页
事件抑制绕行过滤器，第 32 页

事件抑制绕行过滤器

思科 ISE 允许您设置过滤器，以禁止向监控节点和使用收集过滤器的其他外部服务器发送某些系统日志消息。有时，您需要访问这些禁止发送的日志消息。思科 ISE 现在为您提供根据特定属性（例如用户名）在可配置的时间内绕过事件抑制的选项。默认值为 50 分钟，但您可以将持续时间配置为 5 分钟至 480 分钟（8 小时）。配置事件抑制绕行后，该功能会立即生效。如果您设置的持续时间结束，则绕行抑制过滤器将过期。

您可以在思科 ISE 用户界面的 Collection Filters 页面中配置抑制绕行过滤器。使用此功能，您现在可以查看某个特定身份（用户）的所有日志并实时解决该身份遇到的问题。

您可以启用或禁用过滤器。如果您在绕行事件过滤器中配置的持续时间结束，则过滤器会自动禁用，直至您再次启用该过滤器。思科 ISE 在更改配置审核报告中捕获这些配置更改。此报告提供了事件抑制或绕行抑制配置人员的相关信息，以及抑制事件或绕行抑制的持续时间。

思科 ISE 报告

思科身份服务引擎 (ISE) 报告用于监控和故障排除功能分析趋势、和，监控系统性能和网络活动从中心位置。

思科 ISE 从您的网络收集日志和配置数据。然后，将数据聚合到报告，供您查看和分析。思科 ISE 提供一套标准的预定义报告，您可以直接使用，也可以自定义以满足自己的需求。

思科 ISE 报告经过预配置，划分为不同的类别，包含有关身份验证、会话流量、设备管理、配置和管理以及故障排除的信息。

相关主题

运行并查看报告，第 32 页
导出报告，第 33 页
添加收藏的报告，第 37 页
可用报告，第 39 页

运行并查看报告

本节描述如何使用报告视图运行、查看并导航报告。您可以指定报告中所显示数据的时间增量。

步骤 1 选择**操作 (Operations)** > **报告 (Reports)** > **ISE 报告 (ISE Reports)**。

步骤 2 单击 **" 可用报告**页上的类别的报告。

步骤 3 选择一个或多个过滤器以运行报告。每个报告都具有不同的可用过滤器，某些过滤器为必选而某些则为可选。

步骤 4 为过滤器输入适当的值。

步骤 5 运行该报告。

相关主题

导出报告，第 33 页
添加收藏的报告，第 37 页
可用报告，第 39 页

报告导航

您可以从报告输出中获得详细信息。例如，如果您为五个月的一个时间段生成了报告，其图表将按月列出报告的汇总数据。

您可以从表格中点击特定值以查看与此特定字段相关的其他报告。例如，身份验证摘要报告将显示用户或用户组的失败计数。当您点击失败计数时，系统就会打开该特定失败计数的身份验证摘要报告。

导出报告

可以将报告数据导出到 Excel 电子表格，作为逗号分隔值 (.csv) 文件。导出数据之后，会收到一封详细说明报告位置的邮件。

无法导出以下报告：

- 身份验证摘要
- 运行状况摘要
- RBACL 丢弃摘要

注释 RBACL 丢弃的数据包流仅适用于 Cisco Catalyst 6500 系列交换机。

- 访客赞助商摘要
- 终端配置文件修改
- 网络设备会话状态

注释 要在导出报告后正确查看非英文字符，必须通过启用UTF-8字符编码，将文件导入Microsoft Excel。如果选择在不启用 UTF-8 字符编码的情况下直接在 Microsoft Excel 中打开导出的 .csv 文件，则报告中的非英文字符可能会显示一些乱码。

注释 只能从主 PAN 将报告数据导出为 .csv 格式。

步骤 1 如“运行和查看报告”(Running and Viewing Reports) 一节所述运行报告。

步骤 2 点击报告摘要页面右上角的**导出 (Export)**。

步骤 3 指定要导出的数据列。

步骤 4 从下拉列表中选择存储库。

步骤 5 点击**导出 (Export)**。

步骤 6 选择以下选项之一：

- 存储库 (CSV)：将报告以 CSV 文件格式导出到存储库
- 本地 (CSV)：将报告以 CSV 文件格式导出到本地磁盘
- 本地 (PDF)：将报告以 PDF 文件格式导出到本地磁盘

注释
- 当选择本地CSV或PDF选项时，仅会导出前500条记录。您可以使用存储库CSV选项导出所有记录。
- 使用本地 pdf 选项导出多部分报告时，每个部分仅导出前 100 行。

我的报告

您可以将预配置的系统报告和个人过滤的报告添加到 **我的报告** 部分。保存到 **我的报告**部分的报告会保留对其应用的过滤器。

步骤 1 在 **报告** 窗口（**操作** > **报告**）中，从左侧显示的 **报告** 下拉菜单中点击需要的报告。

步骤 2 （可选）打开所选报告后，添加所需的过滤器以自定义报告。

步骤 3 点击窗口右上角的 **添加到我的报告** 按钮。

步骤 4 系统将打开 **保存到我的报告** 对话框。报告的名称和说明会自动填充。如果需要，您可以编辑这些字段。

步骤 5 （可选）所选报告与适用的过滤器一起保存，从而保留其自定义。

步骤 6 点击 **保存** 将报告另存为。系统将显示一个对话框，说明报告已成功保存。

步骤 7 所选报告现在将显示在 **我的报告** 下拉列表中，以便于访问。

您可以通过点击窗口右上角的 **从我的报告中删除** 按钮来删除添加到 **我的报告** 部分的报告。在显示的“警报”对话框中点击 **确定**，报告将从“我的报告”部分中删除。

安排思科 ISE 报告

您可以安排 思科 ISE 报告，以在特定时间或时间间隔运行和重新运行。您还可以将适当的过滤器应用于您选择的报告。您可以安排在思科ISE上以每小时、每天、每周、每月和每年的频率运行报告。它也可以是一次性报告计划作业。您可以选择报告的开始日期和结束日期，并选择要安排报告的星期几。您可以决定计划报告的运行时间。

对于生成的报告，还可以发送和接收电子邮件通知。这些电邮通知将告诉您计划的报告是否已成功运行，还将包含存储库的详细信息、计划报告的时间等。

以**每小时 (Hourly)** 频率安排报告时，可以让报告运行多天，但时间段不能跨越两天。

例如，在安排从 2019 年 5 月 4 日到 2019 年 5 月 8 日的每小时报告时，可以将时间间隔设置为每天上午 6:00 至晚上 11:00，但不能设置为某日下午 6:00 到次日上午 11:00。思科 ISE 会显示错误消息，说明在后一种情况下的时间范围无效。

无法安排以下报告：

- 身份验证摘要
- 运行状况摘要
- RBACL 丢弃摘要

注释 RBACL 丢弃的数据包流仅适用于 Cisco Catalyst 6500 系列交换机。

- 访客赞助商摘要
- 终端配置文件更改
- 网络设备会话状态

步骤 1 在 **报告** 窗口（**操作** > **报告**）中，从左侧显示的 **报告** 下拉菜单中选择要计划的报告。

步骤 2 （可选）打开所选报告时，应用要应用于该报告的过滤器。

步骤 3 点击窗口右上角的 **计划** 按钮。

步骤 4 **另存为计划** 对话框随即打开。

步骤 5 填写计划作业的详细信息，例如名称、说明、电邮、日期和时间。

步骤 6 从 **存储库** 下拉列表中，选择将保存计划报告的外部存储库。有关详细信息，请参阅 “表 1。 思科 ISE 管理员指南的“备份和恢复存储库”部分下的“外部存储库可支持性矩阵”。

步骤 7 从 **频率** 下拉列表中，根据需要选择计划的频率。例如，如果您只需要过去 12 小时的数据，请在安排报告时选择 **过去 12 小时** 数据字段。

步骤 8 根据需要选择 **开始日期** 和 **结束日期**，然后点击 **保存**。

步骤 9 在计划报告时，所有选定的过滤器都将自动应用于报告。

步骤 10 您可以在窗口底部的 **计划的报告** 部分中查看创建的计划和应用的过滤器。

您还可以根据需要编辑和删除计划报告。从计划报告下拉列表（**操作** > **报告** > **计划报告**）中选择您选择的**计划报告**。点击 **编辑计划** 以更改计划的报告，然后点击 **保存**。点击 **删除计划** 以删除计划的报告。

使用案例：计划的报告

要在当日上午 12 点获取前一天的数据，请按照以下程序安排报告：

步骤 1 在 **报告** 窗口（**操作** > **报告**）中，从左侧显示的 **报告** 下拉菜单中选择要计划的报告。

步骤 2 （可选）打开所选报告时，应用要应用于该报告的过滤器。

步骤 3 在此场景中，要获取前一天的数据，请选择 **记录时间** 字段并应用 **昨天** 过滤器。每当计划的报告运行时，这将返回前一天的数据。如果您只需要过去 12 小时的数据，请在计划报告时选择 **另存为计划** 对话框中的 **过去 12 小时数据**字段。

步骤 4 点击窗口右上角的 **计划** 按钮。

步骤 5 **另存为计划** 对话框随即打开。

步骤 6 填写计划作业的详细信息，例如名称、说明、电邮、日期和时间。

步骤 7 从 **存储库** 下拉列表中，选择将保存计划报告的外部存储库。有关详细信息，请参阅 “表 1。 思科 ISE 管理员指南的“备份和恢复存储库”部分下的“外部存储库可支持性矩阵”。

步骤 8 从 **频率** 下拉列表中，根据需要选择计划的频率。例如，如果您只需要过去 12 小时的数据，请在安排报告时选择 **过去 12 小时** 数据字段。

步骤 9 根据需要选择 **开始日期** 和 **结束日期**，然后点击 **保存**。

步骤 10 在计划报告时，所有选定的过滤器都将自动应用于报告。

步骤 11 您可以在窗口底部的 **计划的报告** 部分中查看创建的计划和应用的过滤器。

注释

- 大多数计划报告都以 .csv 格式导出。但是，Radius 身份验证、Radius 审计、TACACS 身份验证、TACACS 审计和操作审核的计划报告导出到包含 .csv 文件的 .zip 文件夹中。
- 如果外部管理员（例如 Active Directory 管理员）在未填写电子邮件 ID 字段的情况下创建计划报告，则不会发送任何电子邮件通知。
- 只有在删除由特定用户创建的计划报告后，才能删除内部或外部思科 ISE 用户，以确保在删除用户后没有活动计划正在运行。
- 只能从 PAN 保存或安排（使用过滤器）思科 ISE 报告。
- 计划的报告作业在主 MnT 和辅助 MnT 节点上运行。如果主 MnT 关闭，则辅助 MnT 将执行计划的报告作业。在这种情况下，辅助 MnT 首先对主 MnT 执行 ping 操作。仅当 ping 失败时，辅助 MnT 才会运行计划的导出作业。
- 从思科 ISE 3.1 补丁 1 开始，导出的报告中的日期格式已从 YYYY-MM-DD 更改为 DD-MM-YY。时间格式已从 hh:mm:ss.sss 更改为 hh:mm:ss.sss AM/PM（24 小时制改为 12 小时制）。

添加收藏的报告

您可以将预配置的系统报告，以及已自定义的报告添加到您的收藏夹列表。

您可以将常用的报告添加到收藏夹列表，让它们更易于查找，就像在浏览器中收藏喜爱的网站一样。您可以查看和编辑收藏报告的参数，然后保存自定义报告以重复使用。

注释 系统会为每个管理员帐户分配一个或多个管理角色。根据分配给您的帐户的角色，您可能无法执行本部分所述的任务。

步骤 1 按“运行和查看报告”部分所述运行报告。

步骤 2 点击报告摘要页面右上角的 **Favorite**。

报告将显示在收藏夹列表中。

注释 您只能从 PAN 将预配置的系统报告添加到收藏夹列表。

思科 ISE 活动 RADIUS 会话

思科 ISE 为实时会话提供动态的授权更改 (CoA) 功能，通过此功能，可以动态地控制活动 RADIUS 会话。可以将重新验证或断开请求发送到网络接入设备 (NAD) 以执行以下任务：

- 排除与身份验证相关的问题 - 可以使用 Session reauthentication 选项继续尝试重新验证。但是，不能使用此选项来限制访问。要限制访问，请使用 shutdown 选项。
- 阻止有问题主机 - 可以将 Session termination 与 port shutdown 选项一起使用，以阻止在网络上发送大量流量的被感染主机。但是，RADIUS 协议当前不支持重新启用已关闭端口的方法。
- 强制终端重新获取 IP 地址 - 可以将 Session termination 与 port bounce 选项一起使用，以便没有请求方或客户端的终端在 VLAN 更改之后生成 DHCP 请求。
- 将更新的授权策略推送到终端 - 可以使用 Session reauthentication 选项执行更新的策略配置，例如，根据管理员的决定更改现有会话的授权策略。例如，如果启用终端安全评估验证，当终端初次获得访问权限时，通常会被隔离。已知终端的身份和终端安全评估之后，可将 Session reauthentication 命令发送到终端，以便该终端根据其终端安全评估获取实际授权策略。

为了让设备读懂 CoA 命令，应适当地配置选项，这一点非常重要。

为了使 CoA 正常工作，必须为每台需要动态授权更改的设备配置共享密钥。思科 ISE 使用共享密钥配置向设备请求访问权限并向其发出 CoA 命令。

注释 在此思科 ISE 版本中，可以显示的经过身份验证的最大活动终端会话数限制为 100000。

相关主题

更改 RADIUS 会话的授权，第 38 页

更改 RADIUS 会话的授权

您网络中的某些网络接入设备可能不会在重新加载后发送 Accounting Stop 或 Accounting Off 数据包。因此，您可能会在 Session Directory 报告中找到两个会话，其中一个已过期。

要动态地更改活动 RADIUS 会话的授权或断开活动 RADIUS 会话的连接，请务必选择最近的会话。

步骤 1 依次选择**操作 (Operations)** > **身份验证 (Authentications)** 。

步骤 2 将视图切换到 **Show Live Session**。

步骤 3 点击要发出 CoA 的 RADIUS 会话的 CoA 链接，然后选择以下其中一个选项：

注释 在已经使用 Inline Posture 节点和无线 LAN 控制器 (WLC) 的情况下，只有两个选项可用：Session reauthentication 和 Session termination。

- **SAnet Session Query** - 使用此选项查询有关支持 SAnet 的设备的信息。
- **Session reauthentication** - 重新对会话进行身份验证。如果您为在支持 COA 的 ASA 设备上建立的会话选择此选项，则此操作将会调用 Session Policy Push CoA。
- **Session reauthentication with last** - 为此会话使用最后一个成功身份验证方法。
- **Session reauthentication with rerun** - 从头开始运行配置的身份验证方法。

注释 思科 IOS 软件中当前不支持 **Session reauthentication with last** 和 **Session reauthentication with rerun** 选项。

- **Session termination** - 仅终止会话。交换机会在不同的会话中重新对客户端进行身份验证。
- **Session termination with port bounce** - 终止会话并重新启动报告。
- **Session termination with port shutdown** - 终止会话并关闭报告。

步骤 4 点击 **Run** 使用选定的 reauthenticate 或 terminate 选项发出 CoA。

如果您的 CoA 失败，可能是由于以下其中一个原因引起：

- 设备不支持 CoA。
- 身份或授权策略已发生更改。
- 共享密钥不匹配。

可用报告

下表按照报告类别分组列出系统预配置的报告。此外还提供对报告功能和日志记录类别的说明。

表 *4:* 可用报告

报告名称	说明	日志记录类别
身份验证服务状态		
AAA 诊断	AAA 诊断报告提供思科 ISE 和用户之间所有网络会话的详细信息。如果用户无法访问网络，您可查看此报告以确定其动态并明确问题是仅限于特定用户还是普遍存在。	依次选择**管理 (Administration)** > **系统 (System)** > **日志记录 (Logging)** > **日志记录类别 (Logging Categories)**，然后选择以下日志记录类别：“策略诊断”(Policy Diagnostics)、“身份库诊断”(Identity Stores Diagnostics)、“身份验证流程诊断”(Authentication Flow Diagnostics） 和“RADIUS 诊断”(RADIUS Diagnostics)。
RADIUS 身份验证	您可以通过 RADIUS 身份验证报告查看身份验证失败和成功的历史记录。如果用户无法访问网络，您可以在此报告中查看详细信息以确定可能的原因。	依次选择**管理 (Administration)** > **系统 (System)** > **日志记录 (Logging)** > **日志记录类别 (Logging Categories)**，然后选择以下日志记录类别：“已通过的身份验证”(Passed Authentications) 和“失败的尝试”(Failed Attempts)。

报告名称	说明	日志记录类别
RADIUS 错误	您可以通过 RADIUS 错误报告检查已丢失的 RADIUS 请求（从未知网络访问设备丢弃的身份验证/记帐请求）、EAP 连接超时和未知 NAD。 **注释** 有时，如果正在进行用户身份验证，ISE 会以静默方式丢弃终端的计费停止 (Accounting Stop) 请求。但是，一旦用户身份验证完成，ISE 将开始确认所有计费请求。	选择**管理 (Administration)** > **系统 (System)** > **日志记录 (Logging)** > **日志记录类别 (Logging Categories)**，然后选择“失败尝试”(Failed Attempts)。
RADIUS 计费	RADIUS 计费报告指出用户访问网络持续的时间。如果用户失去了网络连接，您可以使用此报告确定是不是思科 ISE 导致的网络连接问题。	选择**管理 (Administration)** > **系统 (System)** > **日志记录 (Logging)** > **日志记录类别 (Logging Categories)**，然后选择“RADIUS 计费”(RADIUS Accounting)。
身份验证摘要	身份验证摘要报告以 RADIUS 身份验证为基础。您可以通过此报告确定最常见的身份验证以及任何身份验证失败的原因。例如，如果一个思科 ISE 服务器处理的身份验证明显多于其他服务器，您可能需要重新将用户分配给其他思科 ISE 服务器，以实现更好的负载均衡。 **注释** 由于身份验证摘要报告或控制面板要收集和显示与失败或成功的身份验证对应的最新数据，所以报告的内容会延迟几分钟才显示。	-

报告名称	说明	日志记录类别
OCSP 监控	OCSP监控报告指明在线证书状态协议 (OCSP) 服务的状态。它可以确定思科 ISE 能否成功连接证书服务器并提供证书状态审核，还提供对思科 ISE 执行的所有 OCSP 证书验证操作的汇总。此外，它可从 OCSP 服务器检索关于正常和已吊销主要证书与辅助证书的信息。思科ISE缓存响应并利用响应生成后续OCSP监控报告。如果缓存已清除，它将从 OCSP 服务器检索信息。	选择**管理 (Administration)** > **系统 (System)** > **日志记录 (Logging)** > **日志记录类别 (Logging Categories)**，然后选择“系统诊断”(System Diagnostics)。
AD 连接器操作	AD Connector Operations 报告提供关于 AD 连接器执行的操作的日志，例如思科 ISE 服务器密码更新、Kerberos 票证管理、DNS 查询、DC 发现、LDAP 和 RPC 连接管理等。 如果遇到某些 AD 故障，您可以在此报告中查看详细信息以确定可能的原因。	选择**管理 (Administration)** > **系统 (System)** > **日志记录 (Logging)** > **日志记录类别 (Logging Categories)**，然后选择“AD 连接器”(AD Connector)。
身份映射	您可以通过身份映射报告监控与域控制器的WMI连接的状态并收集与之相关的统计信息（例如接收的通知数量、每秒钟用户登录/注销的次数等）。	选择**管理 (Administration)** > **系统 (System)** > **日志记录 (Logging)** > **日志记录类别 (Logging Categories)**，然后选择“身份映射”(Identity Mapping)。
部署状态		
Administrator Logins	管理员登录报告提供关于所有基于 GUI 的管理员登录事件以及成功的 CLI 登录事件的信息。	选择**管理 (Administration)** > **系统 (System)** > **日志记录 (Logging)** > **日志记录类别 (Logging Categories)**，然后选择“管理和操作审核”(Administrative and Operational Audit)。

报告名称	说明	日志记录类别
内部管理员摘要	您可以通过内部管理员摘要报告验证管理员用户的注册情况。您还可以从此报告访问管理员登录和更改配置审核报告，从而可以查看每个管理员的此类详细信息。	-
Change Configuration Audit	更改配置审核报告提供关于指定时间内配置更改的详细信息。如果需要对某个功能进行故障排除，此报告可以帮助您确定是不是最近的配置更改导致了问题。	选择**管理 (Administration)** > **系统 (System)** > **日志记录 (Logging)** > **日志记录类别 (Logging Categories)**，然后选择“管理和操作审核”(Administrative and Operational Audit)。
Secure Communications Audit	安全通信审核报告提供关于思科 ISE 管理员 CLI 中的安全性相关事件的审核详细信息，该管理员 CLI 包括：身份验证失败、可能的入侵尝试、SSH 登录、失效密码、SSH 注销和无效用户帐户等。	-
操作审核	操作审核报告提供关于任何操作变更的详细信息，例如运行备份、注册思科 ISE 节点或重新启动应用。	选择**管理 (Administration)** > **系统 (System)** > **日志记录 (Logging)** > **日志记录类别 (Logging Categories)**，然后选择“管理和操作审核”(Administrative and Operational Audit)。
系统诊断	系统诊断报告提供关于思科 ISE 节点的状态的详细信息。如果思科 ISE 节点无法注册，您可查看此报告以对问题进行故障排除。 此报告要求首先启用几个诊断日志记录类别。收集这些日志可能会对思科 ISE 性能产生负面影响。因此，默认情况下未启用这些类别。如果您启用这些类别，应使其启用持续时间刚好满足收集数据的要求即可。否则，30 分钟后系统会自动禁用这些类别。	依次选择**管理 (Administration)** > **系统 (System)** > **日志记录 (Logging)** > **日志记录类别 (Logging Categories)**，然后选择以下日志记录类别：“内部操作诊断”(Internal Operations Diagnostics)、“分布式管理”(Distributed Management)、“管理员身份验证和授权”(Administrator Authentication and Authorization)。

报告名称	说明	日志记录类别
Health Summary	运行状况摘要报告提供与控制面板类似的详细信息。但是，控制面板仅显示前 24 小时的数据，而您可以使用此报告查看更久之前的历史数据。 您可以评估这些数据，以查看数据中的一致模式。例如，您可能预计当大多数员工都开始工作时，CPU 使用率较高。如果您发现这些趋势存在不一致性，您可以确定潜在的问题。	选择**管理 (Administration)** > **系统 (System)** > **日志记录 (Logging)** > **日志记录类别 (Logging Categories)**，然后选择以下日志记录类别：“系统统计信息”(System Statistics)、“系统诊断”(System Diagnostics)，以及“管理和操作审核”(Administrative and Operational Audit)。
网络设备会话状态	您可以通过网络设备会话状态摘要报告显示交换机配置，而无需直接登录交换机。 思科 ISE 使用 SNMP 查询功能获取这些详细信息，而且要求用 SNMP v1/v2c 配置您的网络设备。 如果用户遇到网络问题，此报告可帮助您识别问题是否与交换机配置相关，而与思科 ISE 无关。	-

报告名称	说明	日志记录类别
数据清除审核	数据清除审核报告记录何时清除了日志记录数据。 此报告会反映两个数据清除来源。 每天凌晨 4 点，思科 ISE 会检查是否有任何日志记录文件符合您在“管理”(Administration) > “维护”(Maintenance) > “数据清除”(Data Purging) 页面设置的条件。如有，思科 ISE 会删除这些文件并将其记录于此报告中。此外，思科ISE继续为日志文件保留最多 80% 的已用存储空间。思科 ISE 每小时都会检查此百分比并删除最早的数据，直到再次达到此 80% 的阈值。这些信息也会记录于此报告中。	-
pxGrid Administrator Audit	pxGrid 管理员审核报告提供关于 pxGrid 管理操作的详细信息，例如在主 PAN 上注册客户端、注销客户端、批准客户端、创建主题、删除主题、添加发布者-订用者，以及删除发布者-订用者。 每条记录都会注明在节点上执行相应操作的管理员名称。 您可以根据管理员和消息条件过滤 pxGrid 管理员审核报告。	-

报告名称	说明	日志记录类别
配置有误的请求方	配置有误的请求方报告提供配置错误的请求方的列表以及对具体请求方执行的失败尝试的统计信息。如果您已采取纠正措施并修复配置错误的请求方，此报告会显示修复确认信息。 **注释** 应启用RADIUS抑制才能运行此报告。	-
配置有误的 NAS	配置有误的NAS报告提供关于记帐频率不正确（通常指频繁地发送记帐信息）的NAD的信息。如果您已采取纠正措施并修复配置错误的NAD，此报告会显示修复确认信息。 **注释** 应启用RADIUS抑制才能运行此报告。	-
终端和用户		
客户端调配	客户端调配报告显示应用于特定终端的客户端调配代理。您可以使用此报告验证应用于每个终端的策略以确定是否正确调配了终端。	选择**管理 (Administration)** > **系统 (System)** > **日志记录 (Logging)** > **日志记录类别 (Logging Categories)**，然后选择“终端安全评估和客户端调配审核与终端安全评估和客户调配诊断”(Client Provisioning Audit and Posture and Client Provisioning Diagnostics)。
Current Active Sessions	您可以通过当前活动会话报告导出包含关于指定时间内哪些用户正在访问网络的详细信息的报告。 如果用户无法访问网络，您可以查看会话是否经过了身份验证或是否中断，或会话是否存在其他问题。	选择**管理 (Administration)** > **系统 (System)** > **日志记录 (Logging)** > **日志记录类别 (Logging Categories)**，然后选择以下日志记录类别：“记帐”(Accounting) 和“Radius 记帐”(Radius Accounting)。
	报告以 RADIUS 记账为基础。它可以显示每个终端所有网络会话的历史报告数据。	选择**管理 (Administration)** > **系统 (System)** > **日志记录 (Logging)** > **日志记录类别 (Logging Categories)**，然后选择“已通过身份验证”(Passed Authentications) 和 RADIUS 计费 (RADIUS Accounting)。

报告名称	说明	日志记录类别
外部移动设备管理	外部移动设备管理报告提供关于思科 ISE 与外部移动设备管理 (MDM) 服务器之间的集成的详细信息。 您可以使用此报告查看哪些终端经过了 MDM 服务器调配，而无需直接登录 MDM 服务器。此报告还显示注册和 MDM 合规状态等信息。	选择**管理 (Administration)** > **系统 (System)** > **日志记录 (Logging)** > **日志记录类别 (Logging Categories)**，然后选择 MDM。
终端安全详细评估	终端安全详细评估报告提供关于特定终端的安全评估合规性的详细信息。如果某个终端之前能访问网络，然后突然无法访问网络，您可以根据此报告确定是否出现了安全评估违规问题。	选择**管理 (Administration)** > **系统 (System)** > **日志记录 (Logging)** > **日志记录类别 (Logging Categories)**，然后选择“终端安全评估和客户端调配审核与终端安全评估和客户调配诊断”(Client Provisioning Audit and Posture and Client Provisioning Diagnostics)。
已分析的终端摘要	已分析的终端摘要报告提供关于正在访问网络的终端的分析详细信息。 **注释** 对于不注册会话时间的终端（例如思科 IP 电话），“终端会话时间”(Endpoint session time) 字段中会显示“不适用”(Not Applicable)。	选择**管理 (Administration)** > **系统 (System)** > **日志记录 (Logging)** > **日志记录 (Logging)**，然后选择“分析器”(Profiler)。
终端配置文件更改	终端配置文件更改报告用于以下两种用途： • 比较特定终端的配置文件更改以验证是否应用的是最新的配置文件。 • 显示分析器源服务（使用思科 ISE Plus 许可证可获得此服务）发起的配置文件更改。	-

报告名称	说明	日志记录类别
按终端查看顶级授权	终端顶级授权（MAC 地址）报告显示思科 ISE 已授权每个终端 MAC 地址访问网络的次数。	已通过身份验证、失败尝试
按用户查看顶级授权	按用户查看顶级授权报告显示思科 ISE 已授权每个用户访问网络的次数。	已通过身份验证、失败尝试
User Change Password Audit	用户更改密码审核报告显示关于员工密码更改的验证信息。	管理和操作审核
请求方调配	请求方调配报告提供关于调配至员工个人设备的请求方的详细信息。	终端安全评估和客户端调配审核
注册终端	注册终端报告显示员工注册的所有个人设备。	-
终端清除活动	用户可以通过终端清除活动报告查看终端清除活动的历史记录。此报告要求启用“分析器”(Profiler) 日志记录类别。该类别在默认情况下已启用。	选择**管理 (Administration)** > **系统 (System)** > **日志记录 (Logging)** > **日志记录 (Logging)**，然后选择“分析器”(Profiler)。
访客接入报告		
AUP Acceptance Status	AUP Acceptance Status 报告提供从所有 Guest 门户接受的 AUP 的详细信息。	选择**管理 (Administration)** > **系统 (System)** > **日志记录 (Logging)** > **日志记录类别 (Logging Categories)**，然后选择“访客”(Guest)。
Sponsor Login and Audit	Sponsor Login and Audit 报告提供关于访客用户的登录、添加、删除、启用、暂停和更新操作以及发起人在发起人门户上的登录活动的详细信息。 如果批量添加访客用户，则“访客用户”(Guest Users) 列下会显示这些用户。此列默认处于隐藏状态。在导出时，这些批量用户也会显示于导出的文件上。	选择**管理 (Administration)** > **系统 (System)** > **日志记录 (Logging)** > **日志记录类别 (Logging Categories)**，然后选择“访客”(Guest)。

报告名称	说明	日志记录类别
我的设备登录和审核	我的设备登录和审核报告提供关于用户通过设备在“我的设备门户”(My Devices Portal) 中执行的登录活动和操作的详细信息。	选择**管理 (Administration)** > **系统 (System)** > **日志记录 (Logging)** > **日志记录类别 (Logging Categories)**，然后选择“我的设备”(My Devices)。
主访客报告	主访客报告综合各个访客接入报告的数据，并且允许您从不同报告来源导出数据。主访客报告还提供关于访客用户正在访问的网站的详细信息。您可以使用此报告进行安全审核，以证明访客用户何时访问了网络以及他们在网络上执行了什么活动。 您还必须在用于访客流量的网络访问设备 (NAD) 上启用 HTTP 检查。这些信息由 NAD 发送回思科 ISE。 要检查客户端何时达到最大并行会话限制数，从管理员门户选择**管理 (Administration) > 系统 (System) > 日志记录 (Logging) > 日志记录类别 (Logging Categories)** 并执行以下操作： **1.** 将“身份验证流量诊断”(Authentication Flow Diagnostics) 日志类别的日志级别从警告提高到信息。 **2.** 从 AAA 诊断“日志记录类别”下，将 LogCollector 目标从可用的更改为已选的。	选择 **管理 (Administration)** > **系统 (System)** > **日志记录 (Logging)** > **日志记录类别 (Logging Categories)**，然后选择已通过的身份验证 (Passed Authentications)。
访客计费	访客计费报告是 RADIUS 计费报告的一部分。此报告中显示分配至激活访客或访客身份组的所有用户。	-

报告名称	说明	日志记录类别
TrustSec		
RBACL 丢包摘要	RBACL 丢包摘要报告专用于 TrustSec 功能，只有在具备思科 ISE 高级许可证的情况下才可用。 此报告还要求您将网络设备配置为向思科 ISE 发送关于丢包事件的 NetFlow 事件。 如果用户违反特定策略或访问权限，系统会丢弃数据包并在此报告中指明。	—
按用户前 N 个 RBACL 丢包	按用户前 N 个 RBACL 丢包报告专用于 TrustSec 功能，只有在具备思科 ISE 高级许可证的情况下才可用。 此报告还要求您将网络设备配置为向思科 ISE 发送关于丢包事件的 NetFlow 事件。 此报告显示特定用户违反策略的情况（依据数据包丢弃情况）。	—

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。