部署

思科 ISE 部署术语

以下是讨论Cisco ISE 部署方案时常用的术语：

- 服务：服务是角色提供的特定功能，例如网络访问、分析器、终端安全评估、安全组访问、监控和故障排除等。
- 节点：节点是运行Cisco ISE 软件的单个实例。Cisco ISE 可用作设备，也可用作能在 VMware 上运行的软件。运行Cisco ISE 软件的每个实例（设备或 VMware）叫节点。
- 角色：节点的角色决定节点提供的服务。Cisco ISE 节点可以承担以下任意角色：管理、策略服务、监控和 pxGrid。通过管理员门户可用的菜单选项取决于Cisco ISE 节点承担的职责和角色。
- 部署模式：决定您的部署是分布式、独立式还是作为基本双节点部署的独立式高可用性部署。

分布式思科 ISE 部署中的角色

Cisco ISE 节点可以承担管理、策略服务或监控角色。

Cisco ISE 节点可以根据它承担的角色提供各种服务。部署中的每个节点均可承担管理、策略服务和监控角色。在分布式部署中，您可以在网络中使用以下节点组合：

- 支持高可用性的主策略管理节点（主 PAN）和辅助策略管理节点（辅助 PAN）
- 支持高可用性的主监控节点（主 MnT 节点）和辅助监控节点（辅助 MnT 节点）
- 用于主 PAN 自动故障转移的一对运行状况检查节点或单个运行状况检查节点
- 用于会话故障转移的一个或多个策略服务节点 (PSN)

环境下载成功，结果中仅显示正在运行的Cisco ISE 节点。

配置思科 ISE 节点

在安装Cisco ISE 节点后，系统会在其上运行管理、策略服务和监控角色提供的默认服务。此节点将处于独立状态。您必须登录Cisco ISE 节点的 Admin 门户进行配置。您无法编辑独立Cisco ISE 节点的角色或服务。但是，您可以编辑主要和辅助Cisco ISE 节点的角色和服务。您必须先配置主要 ISE 节点，然后向主要 ISE 节点注册辅助 ISE 节点。

如果首次登录节点，您必须更改默认管理员密码并安装有效许可证。

建议不要更改生产中在Cisco ISE 上配置的主机名和域名。如有必要，则在初始部署期间为设备重置映像，执行更改，并配置详细信息。

开始之前

您应该对如何在Cisco ISE 中设置分布式部署有基本了解。请参阅设置分布式部署的规定。

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)** > **部署 (Deployment)**。

步骤 2 选中您要配置的Cisco ISE 节点旁边的复选框，然后点击**编辑 (Edit)**。

步骤 3 按照需要输入相应值，然后点击**保存 (Save)**。

配置主策略管理节点 (PAN)

要设置分布式部署，必须首先将Cisco ISE 节点配置为主 PAN。

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)** > **部署 (Deployment)**。

一开始 Register 按钮将会处于禁用状态。要启用此按钮，必须配置主 PAN。

步骤 2 选中当前节点旁边的复选框，然后点击**编辑 (Edit)**。

步骤 3 点击**设为主 (Make Primary)** 以配置主 PAN。

步骤 4 点击**保存 (Save)**，保存节点配置。

下一步做什么

1. 向您的部署添加辅助节点。
2. 如有必要，请启用分析器服务并配置探测功能。

注册辅助思科 ISE 节点

您可以将Cisco ISE 节点注册到主 PAN 以形成多节点部署。部署中除主 PAN 以外的节点称为辅助节点。在注册节点时，可以选择必须在节点上启用的角色和服务。注册的节点可从主 PAN 管理（例如，管理节点角色、服务、证书、许可证、应用补丁等）。

注册辅助节点后，主PAN 会将配置数据推送到辅助节点，而辅助节点上的应用服务器会重启。完成数据后，在主PAN 上完成的进一步配置更改将复制到辅助节点。在辅助节点上复制更改所需的时间取决于各种因素，如网络延迟、系统负载等。

开始之前

确保主 PAN 和正在注册的节点可相互进行 DNS 解析。如果正在注册的节点使用不受信任的自签证书，则系统会提示包含证书详细信息的证书警告。如果接受该证书，则会将其添加到主PAN 的受信任证书存储区，以启用与节点的 TLS 通信。

如果节点使用非自签证书（例如，由外部 CA 签名），则必须将该节点的相关证书链手动导入到主 PAN 的受信任证书库。当将辅助节点的证书导入受信任证书库时，请选中**受信任证书 (Trusted**

Certificates) 窗口中的**信任 ISE 中的身份验证 (Trust for Authentication within ISE)** 复选框，以便主 PAN 验证辅助节点的证书。

在注册启用了会话服务（如网络访问、访客、终端安全评估等）的节点时，可以将其添加到节点组。有关详细信息，请参阅创建策略服务节点组，第 48 页一节。

步骤 1 登录到主 PAN。

步骤 2 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **部署 (Deployment)**。

步骤 3 点击**注册 (Register)** 以开始注册辅助节点。

步骤 4 输入要注册的独立节点的可 DNS 解析完全限定域名 (FQDN)，采用的格式为 hostname.domain-name，例如，abc.xyz.com。主 PAN 的 FQDN 和正在注册的节点必须能够相互解析。

步骤 5 在**用户名 (Username)** 和 **密码 (Password)** 字段中，输入辅助节点的基于 UI 的管理员凭证。

步骤 6 点击**下一步 (Next)**。

主 PAN 会尝试与正在注册的节点（首次）建立 TLS 通信。

- 如果节点使用受信任的证书，则可以继续执行第 7 步。
- 如果节点使用不受信任的自签证书，则会显示证书警告消息。证书警告消息显示有关证书的详细信息（如颁发给、颁发者、序列号等），可对照节点上的实际证书进行验证。您可以选择**导入证书并继续 (Import Certificate and Proceed)** 选项以信任此证书并继续注册。Cisco ISE 会将该节点的默认自签证书导入到主 PAN 的受信任证书库。如果不想使用默认的自签证书，请点击**取消注册 (Cancel Registration)** 并将该节点的相关证书链手动导入到主 PAN 的受信任证书库。当将辅助节点的证书导入到受信任证书库时，请选中**信任 ISE 内部的身份认证 (Trust for Authentication within ISE)** 复选框，以便 PAN 验证辅助节点的证书。
- 如果节点使用 CA 签名的证书，则系统会显示一条错误消息，指出在设置证书信任之前无法继续注册。

步骤 7 选择要在节点上启用的角色和服务，然后点击**保存 (Save)**。

注册节点时，主 PAN 上会生成警报（确认已将节点添加到部署中）。在Cisco ISE GUI **控制板 (Dashboard)** 的**警报 (Alarms)** Dashlet 中查看此警报。注册节点同步并重新启动后，您可以使用主 PAN 上所用的相同凭证登录到辅助节点 GUI。

下一步做什么

- 对于时间敏感型任务（例如访客用户访问和授权、登录等），请确保节点上的系统时间已经同步。
- 如果您注册了辅助 PAN，并计划使用内部Cisco ISE CA 服务，则必须备份主 PAN 的Cisco ISE CA 证书和密钥，并在辅助 PAN 恢复这些证书和密钥。

  请参阅 思科 ISE CA 证书和密钥的备份与恢复

支持多种部署方案

可以在企业基础网络架构中部署Cisco ISE，支持 802.1X 有线、无线和虚拟专用网络 (VPN)。

Cisco ISE 架构同时支持独立和分布式（也称为高可用性 或冗余）部署，其中一台计算机承担主要角色，另一台“备份”计算机承担辅助角色。Cisco ISE 具有不同的可配置角色、服务和职责，允许创建和应用网络中所需的Cisco ISE 服务。这样得到的是一个用作功能齐全的集成式系统的全面Cisco ISE 部署。

可以使用一个或多个管理、监控和策略服务角色部署Cisco ISE 节点。每个角色在整体网络策略管理拓扑中发挥不同的重要作用。使用管理角色安装Cisco ISE，可以从集中式门户配置和管理网络以提高效率和易用性。

思科 ISE 分布式部署

具有不止一个Cisco ISE 节点的部署称作分布式部署。要支持故障切换和提高性能，您可以以分布式方式为您的部署设置多个Cisco ISE 节点。在Cisco ISE 分布式部署中，管理和监控活动会进行集中，而处理则分布在多个 PSN 上。根据您对性能的要求，您可以扩展您的部署。部署中的每个Cisco ISE 节点可以承担以下任意角色：管理、策略服务和监控。

思科 ISE 部署设置

在所有节点上安装Cisco ISE 后，如《思科身份服务引擎硬件安装指南》所述，节点显示为独立状态。然后必须定义一个节点作为主 PAN。定义主 PAN 时，必须在该节点上启用管理和监控角色。您可以在主 PAN 上选择启用策略服务角色。在主 PAN 上完成定义角色的任务后，可以向主 PAN 注册其他辅助节点，为辅助节点定义角色。

所有Cisco ISE 系统和功能相关配置应当只在主 PAN 上进行。在主 PAN 上执行的配置更改被复制到部署中的所有辅助节点上。

分布式部署中必须至少有一个 MnT。配置主 PAN 时，必须启用监控角色。在部署中注册 MnT 节点后，如果需要，可以编辑主 PAN 并禁用监控角色。

从主要 ISE 节点将数据复制至辅助 ISE 节点

当您将Cisco ISE 节点注册为辅助节点时，Cisco ISE 会立即创建一个从主节点到辅助节点的数据复制通道并开始执行复制进程。复制是从主要节点向辅助节点共享Cisco ISE 配置数据的过程。复制可确保部署中的所有Cisco ISE 节点的配置数据一致。

首次将Cisco ISE 节点注册为辅助节点时，通常会进行完全复制。完全复制之后进行增量复制，确保在辅助节点中反映所有新的更改，例如对 PAN 中配置数据的添加、修改或删除。复制过程可确保部署中的所有Cisco ISE 节点保持同步。在Cisco ISE 管理员门户的**部署 (Deployment)** 窗口中，可从**节点状态 (Node Status)** 列查看复制状态。当您将Cisco ISE 节点注册为辅助节点或执行与 PAN 的手动同步时，节点状态显示橙色图标，表示正在进行所请求的操作。同步完成后，节点状态会变为绿色，表示辅助节点已与 PAN 同步。

思科 ISE 节点取消注册

要从部署中删除节点，您必须对该节点取消注册。从主 PAN 取消注册辅助节点时，被取消注册的节点的状态更改为独立，主节点和辅助节点之间的连接将丢失。复制更新不再发送到被取消注册的独立节点。

取消注册 PSN 时，终端数据将丢失。如果您希望 PSN 在成为独立节点后保留终端数据，可以执行以下任一操作：

- 从主 PAN 获取备份，并在 PSN 成为独立节点时在其上恢复此数据备份。
- 将 PSN 的角色更改为“管理”(Administration)（辅助 PAN），从管理员门户的**部署 (Deployment)** 窗口同步数据，然后取消注册节点。此节点现在拥有所有数据。然后可以将辅助 PAN 添加至现有部署。

注释 无法取消注册主 PAN。

设置分布式部署的规定

在分布式环境中设置Cisco ISE 之前，请仔细阅读以下声明。

- 选择Cisco ISE 服务器节点类型。对于管理、策略服务和监控功能，必须选择Cisco ISE 节点。
- 为所有节点选择同一网络时间协议 (NTP) 服务器。要避免节点之间发生时区问题，您必须在每个节点的设置过程中提供同一 NTP 服务器名称。此设置可确保来自部署中的各种节点的报告和日志与时间戳始终同步。
- 安装Cisco ISE 时配置Cisco ISE 管理员密码。以前的Cisco ISE 管理员默认登录凭证 (admin/cisco) 不再有效。使用初始设置过程中创建的用户名和密码或当前密码（如果后来更改了密码）。
- 配置域名系统 (DNS) 服务器。在 DNS 服务器中输入分布式部署中包含的所有Cisco ISE 节点的 IP 地址和完全限定域名 (FQDN)。否则，节点注册将失败。
- 在 DNS 服务器中为分布式部署中的所有Cisco ISE 节点配置正向和反向 DNS 查找。否则，在注册并重新启动Cisco ISE 节点时可能会遇到部署相关问题。如果未为所有节点配置反向 DNS 查找，则性能可能会降低。
- （可选）从主 PAN 注销辅助Cisco ISE 节点以从中卸载Cisco ISE。
- 备份主 MnT，然后将数据恢复到新的辅助 MnT。由于会复制新的更改，因此这可确保主 MnT 的历史记录与新 MnT 同步。
- 确保即将注册为辅助节点的主 PAN 和独立节点运行的是同一版本的Cisco ISE。
- 在向部署中添加新节点时，请确保通配符证书的颁发者证书链是新节点的受信任证书的一部分。将新节点添加到部署中时，通配符证书随后会复制到新节点。

- 在将Cisco ISE 部署配置为支持Cisco TrustSec 时，或者在Cisco ISE 与Cisco DNA 中心集成时，请勿将 PSN 配置为仅 SXP。SXP 是Cisco TrustSec 和非Cisco TrustSec 设备之间的接口。SXP 不与支持Cisco TrustSec 的网络设备通信。

主要节点和辅助节点上可用的菜单选项

作为分布式部署组成部分的Cisco ISE 节点中可用的菜单选项取决于在节点上启用的角色。您必须通过主 PAN 执行所有管理和监控活动。对于其他任务，您必须使用辅助节点。因此，根据辅助节点上启用的角色，辅助节点的用户界面提供有限的菜单选项。

如果节点担任不止一个角色，例如某个主职责同时具备策略服务角色和监控角色，则针对 PSN 和主 MnT 列出的菜单选项在该节点上可用。

下表列出在担任不同角色的Cisco ISE 节点上可用的菜单选项。

表 *1:* 思科 *ISE* 节点和可用的菜单选项

Cisco ISE 节点	可用的菜单选项
所有节点	• 查看和配置系统时间以及 NTP 服务器设置 • 安装服务器证书并管理证书签名请求。您可以通过集中管理所有服务器证书的主 PAN 为该部署中的所有节点执行服务器证书操作 **注释** 私钥不存储于本地数据库中，也不从相关节点复制。私钥存储于本地文件系统中。
主策略管理节点（主 PAN）	所有菜单和子菜单
主监控节点（主 MnT 节点）	• 提供对监控数据的访问 **注释** 只能从主 PAN 查看**操作 (Operations)** 菜单。**操作 (Operations)** 菜单不显示在Cisco ISE 2.1 及更高版本的监控节点中。
PSN（策略服务节点）	加入、离开和测试 Active Directory 连接的选项可用。必须单独将每个 PSN 加入到 Active Directory 域中。必须先定义域信息并且将 PAN 联接到 Active Directory 域中。然后，逐一将其他 PSN 加入到 Active Directory 域中。

Cisco ISE 节点	可用的菜单选项
辅助策略管理节点（辅助 PAN）	将辅助 PAN 升级为主 PAN 的选项 注释 在向主 PAN 注册了辅助节点之后，在登录任意辅助节点的管理员门户时，您必须使用主 PAN 的登录凭证。

部署和节点设置

您可以通过**部署节点 (Deployment Nodes)** 窗口配置Cisco ISE（PAN、PSN 和 MnT）节点并设置部署。

部署节点列表 窗口

下表介绍了**部署节点列表** 窗口上的字段，您可以使用此窗口在部署中配置Cisco ISE 节点。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **部署 (Deployment)**.

字段名称	使用指南
主机名 (Hostname)	显示节点的主机名。
相关角色 (Personas)	（只有在节点类型为Cisco ISE 时才显示）列出 Cisco ISE 节点承担的角色。 例如，**管理 (Administration)**、**策略服务 (Policy Service)**、**监控 (Monitoring)** 或 **pxGrid**。
角色 (Rol)e	如果在此节点上启用了管理和监控角色，则指示管理和监控角色承担的职责（主要、辅助或独立职责）。职责可以是以下一项或多项： • **PRI(A)**：指主 PAN • **SEC(A)**：指辅助 PAN • **PRI(M)**：指主 MnT • **SEC(M)**：指辅助 MnT

字段名称	使用指南
服务 (Services)	（只有在启用策略服务角色时才显示）列出此Cisco ISE 节点上运行的服务。服务可包括以下任意一项： • 身份映射 • 会话 • 剖析 • 全部
节点状态	指示部署中每个Cisco ISE 节点的数据复制状态。 • 绿色（已连接）：表示部署中已注册的Cisco ISE 节点与主 PAN 处于同步状态。 • 红色（断开）：表示Cisco ISE 节点无法到达、已断开或未进行数据复制。 • 橙色（处理中）：表示向主PAN新注册了新Cisco ISE 节点、您已执行手动同步操作或Cisco ISE 节点与主 PAN 不同步。 有关详细信息，请点击**节点状态 (Node Status)** 列中每个Cisco ISE 节点的快速查看图标。

相关主题

思科 ISE 分布式部署，第 5 页
思科 ISE 部署术语，第 2 页
配置思科 ISE 节点，第 2 页
注册辅助思科 ISE 节点

常规节点设置

下表说明Cisco ISE 节点的**常规设置 (General Settings)** 窗口中的字段。在此窗口中，可以将角色分配给节点并配置要在其上运行的服务。 要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **部署 (Deployment)** > **部署节点 (Deployment Node)** > **编辑 (Edit)** > **常规设置 (General Settings)**。

表 *2:* 常规节点设置

字段名称	使用指南
主机名 (Hostname)	显示Cisco ISE 节点的主机名。

字段名称	使用指南
FQDN	显示Cisco ISE 节点的完全限定域名。例如 ise1.cisco.com。
IP 地址 (IP Address)	显示Cisco ISE 节点的 IP 地址。
节点类型 (Node Type)	显示节点类型。
相关角色 (Personas)	
管理 (Administration)	如果Cisco ISE 节点承担管理角色，请启用此切换按钮。只有在受许可提供管理服务的节点上才可以启用 Administration 角色。 **角色 (Role)** - 显示管理角色在部署中承担的职责。角色可以采用以下任一值：**独立 (Standalone)**、**主 (Primary)** 或**辅助 (Secondary)**。 **设为主要 (Make Primary)** - 选择此按钮可使该节点成为主Cisco ISE 节点。在部署中您只能有一个主要Cisco ISE 节点。当您将此节点设置为主要节点之后，此页面的其他选项将进入活动状态。在部署中您只能有两个 Administration 节点。如果节点具有**独立 (Standalone)** 角色，则旁边会显示**设为主要 (Make Primary)** 按钮。如果节点具有**辅助 (Secondary)** 角色，则旁边会显示**升级为主要 (Promote to Primary)** 按钮。如果节点具有**主要 (Primary)** 角色，并且没有其他节点注册到该节点，则旁边会显示**设为独立 (Make Standalone)** 按钮。您可以点击此按钮以使您的主要节点成为独立节点。

字段名称	使用指南
监控 (Monitoring)	如果要Cisco ISE 节点承担监控角色并充当日志收集器，请启用此切换按钮。分布式部署中必须至少有一个监控节点。配置主 PAN 时，必须启用监控角色。在部署中注册辅助监控节点之后，如有必要，可以编辑主 PAN 和禁用监控角色。 要在 VMware 平台上将Cisco ISE 节点配置为您的日志收集器，请使用以下规定确定您所需要的最低磁盘空间：您的网络中每天每个终端 180 KB，您的网络中每天每个Cisco ISE 节点 2.5 MB。 您可以根据您想要将多少个月的数据至于监控模式下，计算您所需的最大磁盘空间。如果您的部署中只有一个监控节点，则该节点会承担独立职责。如果在部署中有两个监控节点，Cisco ISE 会显示另一个监控节点的名称以供您配置主要/辅助角色。要配置这些职责，请选择以下选项之一： • **主 (Primary)**：使当前节点成为主监控节点。 • **辅助 (Secondary)**：使当前节点成为辅助监控节点。 • **无 (None)** - 如果要使监控节点不承担主要-辅助角色。 如果您将您的一个监控节点配置为主要或辅助节点，另一个监控节点相应地自动成为辅助或主要节点。主要监控节点和辅助监控节点都接收管理和策略服务日志。如果将一个监控节点的角色改为**无 (None)**，则另一个监控节点的角色也会成为**无 (None)**，从而会在您将某个节点指定为监控节点之后取消高可用性对。您会在**远程日志记录目标 (Remote Logging Targets)** 窗口中发现此节点被列为系统日志目标。要查看此处窗口，请点击**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)**。

字段名称	使用指南
策略服务 **(Policy Service)**	

字段名称	使用指南
	启用此切换按钮可启用以下任一或所有服务： • **启用会话服务 (Enable Session Services)**：选中此复选框可启用网络访问、终端安全评估、访客和客户端调配服务。从**在节点组中包含节点 (Include Node in Node Group)** 下拉列表中选择此策略服务节点所属的组。请注意，证书颁发机构 (CA) 和安全传输注册 (EST) 服务只能在已启用会话服务的策略服务节点上运行。 对于**在节点组中包含节点 (Include Node in Node Group)**，如果不希望此策略服务节点加入任何组，请选择**无 (None)**。 同一个节点组中的所有节点都应在网络接入设备上配置为 RADIUS 客户端，并获 CoA 授权，因为这些节点中的任何一个节点均可为通过节点组中的任何节点建立的会话发出 CoA 请求。如果您未使用负载均衡器，则节点组中的节点应与在NAD上配置的RADIUS服务器和客户端相同，或作为RADIUS服务器和客户端的子集。这些节点还将配置为 RADIUS 服务器。 虽然可以使用多个Cisco ISE 节点将单个NAD配置为RADIUS服务器和动态授权客户端，但并不要求所有节点都属于同一个节点组。 一个节点组中的所有成员应通过高速 LAN 连接（例如，千兆以太网）互相建立连接。虽然节点组成员不需要在第二层相邻，但是我们依然建议节点组成员在第 2 层相邻，以确保足够的宽带和可达性。有关详细信息，请参阅《》中的“创建策略服务节点组”部分请参阅创建策略服务节点组，第 48 页。 • **启用分析服务 (Enable Profiling Service)**：选中此复选框可启用分析服务。如果启用分析服务，必须点击**分析配置 (Profiling Configuration)** 选项卡并根据要求输入详细信息。当您启用或禁用策略服务节点上运行的任意服务或对此节点做任何更改时，您将重新启动运行这些服务的应用服务器进程。这些服务重新启动时预计会有延迟。您可以从 CLI 使用 *show application status ise* 命令，确定何时在节点上重新启动了应用服务器。

字段名称	使用指南
	• **启用威胁中心 NAC 服务 (Enable Threat Centric NAC Service)**：选中此复选框可启用威胁中心网络访问控制 (TC-NAC) 功能。通过此功能，您可依据威胁和漏洞适配器发送的威胁和漏洞属性创建授权策略。威胁严重级别和漏洞评估结果可用于动态控制终端或用户的访问级别。 • **启用 SXP 服务 (Enable SXP Service)**：选中此复选框可在节点上启用 SXP 服务。您还必须指定 SXP 服务使用的接口。 如果已配置 NIC 绑定或组合，则还会在使用**接口 (Use Interface)** 下拉列表中列出绑定接口以及物理接口。 • **启用设备管理员服务 (Enable Device Admin Service)**：选中此复选框可创建 TACACS 策略集和策略结果等，以便控制和审计网络设备的配置。 • **启用被动身份服务 (Enable Passive Identity Service)**：选中此复选框可启用身份映射功能。通过此功能，您可以监控通过域控制器 (DC)（而不是Cisco ISE）进行身份验证的用户。在Cisco ISE 不主动对用户进行网络访问身份验证的网络中，您可以使用身份映射功能从 Active Directory (AD) 域控制器收集用户身份验证信息。
pxGrid	选中此复选框可启用 pxGrid 角色。Cisco pxGrid 用于将来自Cisco ISE 会话目录区分上下文的信息共享给Cisco自适应安全设备 (ASA)。此 pxGrid 框架还可用于在节点之间交换策略和配置数据，例如在Cisco ISE 和第三方供应商之间共享标签和策略对象，以及交换威胁信息等非Cisco ISE 相关信息。

相关主题

分布式思科 ISE 部署中的角色，第 2 页
管理节点，第 23 页
策略服务节点，第 30 页
监控节点，第 33 页
思科 pxGrid 节点，第 40 页
同步主要和辅助思科 ISE 节点，第 47 页

创建策略服务节点组，第 48 页
部署思科 pxGrid 节点，第 41 页
更改节点角色和服务，第 47 页
配置用于自动故障切换的监控节点，第 39 页

分析节点的设置

下表介绍“分析配置”(Profiling Configuration) 窗口上的字段，您可以使用此窗口为分析器服务配置探测功能。 要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **部署 (Deployment)** > **ISE 节点 (ISE Node)** > **编辑 (Edit)** > **分析配置 (Profiling Configuration)**。

表 *3:* 分析节点的设置

字段名称	使用指南
NetFlow	启用此切换按钮可针对承担策略服务角色的每个 Cisco ISE 节点启用 NetFlow，以便接收从路由器发送的 NetFlow 数据包。为以下选项输入所需的值： • **接口 (Interface)**：选择Cisco ISE 节点上的接口。 • **端口 (Port)**：输入从路由器接收 NetFlow 导出数据的 NetFlow 侦听器端口号。默认端口为 9996。
DHCP	启用此切换按钮可针对承担策略服务角色的每个 Cisco ISE 节点启用 DHCP，以便侦听来自 IP 帮助程序的 DHCP 数据包。为以下选项输入所需的值： • **接口 (Interface)**：选择Cisco ISE 节点上的接口。 • **端口 (Port)**：输入 DHCP 服务器 UDP 端口号。默认端口为 67。
DHCP SPAN	启用此切换按钮可针对承担策略服务角色的每个 Cisco ISE 节点启用 DHCP，以便收集 DHCP 数据包。 • **接口 (Interface)**：选择Cisco ISE 节点上的接口。

字段名称	使用指南
HTTP	启用此切换按钮可针对承担策略服务角色的每个Cisco ISE 节点启用 HTTP，以便接收并解析 HTTP 数据包。 • **接口 (Interface)**：选择Cisco ISE 节点上的接口。
RADIUS	启用此切换按钮可针对承担策略服务角色的每个Cisco ISE 节点启用 RADIUS，以便收集 RADIUS 会话属性，以及来自已启用 IOS 传感器的设备的Cisco设备协议 (CDP) 和链路层发现协议 (LLDP) 属性。
网络扫描 (NMAP) (Network Scan [NMAP])	启用此切换按钮可启用 NMAP 探测。
DNS	启用此切换按钮可针对承担策略服务角色的每个Cisco ISE 节点启用 DNS，以便对 FQDN 执行 DNS 查找。以秒为单位输入**超时 (Timeout)** 期间。 **注释** 要使 DNS 探测功能在分布式部署中特定Cisco ISE 节点上运行，您必须启用以下任一探测功能：DHCP、DHCP SPAN、HTTP、RADIUS 或 SNMP。对于 DNS 查找，必须连同 DNS 探测功能一起启用上述另一个探测功能。
SNMP 查询 (SNMP Query)	启用此切换按钮可针对承担策略服务角色的每个Cisco ISE 节点启用 SNMP 查询，以便按照指定的间隔轮询网络设备。为以下字段输入值：**重试次数 (Retries)**、**超时 (Timeout)**、**事件超时 (Event Timeout)**和可选的**说明 (Description)**。 **注释** 除配置 SNMP 查询探测功能之外，还必须在以下位置配置其他 SNMP 设置：**管理 (Administration)** > **网络资源 (Network Resources)** > **网络设备 (Network Devices)**。当在网络设备上配置 SNMP 设置时，请确保在网络设备上全局启用 CDP 和 LLDP。

字段名称	使用指南
SNMP 陷阱 (SNMP Trap)	启用此切换按钮可针对承担策略服务角色的每个Cisco ISE 节点启用 SNMP 陷阱探测，以便从网络设备接收链路接通、链路断开和MAC通知陷阱。为以下选项输入所需的值： • **链路陷阱查询 (Link Trap Query)**：启用此切换按钮可接收和解释通过 SNMP 陷阱接收的链路接通和链路断开通知。 • **MAC 陷阱查询 (MAC Trap Query)**：启用此切换按钮可接收和解释通过 SNMP 陷阱接收的 MAC 通知。 • **接口 (Interface)**：选择Cisco ISE 节点上的接口。 • **端口 (Port)**：输入要使用的主机 UDP 端口。默认端口为 162。
Active Directory	启用此切换按钮可扫描所定义的 Active Directory 服务器，以获取有关 Windows 用户的信息。 • **重新扫描前的天数 (Days before rescan)**：选择您希望经过多少天后再次进行扫描。
pxGrid	启用此切换按钮可允许Cisco ISE 通过 pxGrid 收集（配置文件）终端属性。

相关主题

思科 ISE 分析服务

分析服务使用的网络探测功能

在思科 ISE 节点中配置分析服务

日志记录设置

下面的小节解释了如何配置调试日志的严重性、创建外部日志目标，并使Cisco ISE 能够将日志消息发送到这些外部日志目标。

远程日志记录目标设置

下表介绍“远程日志记录目标”(Remote Logging Targets) 窗口中的字段，您可以使用此窗口创建外部位置（系统日志服务器）来存储日志记录消息。要查看此处窗口，请点击**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)**。

表 *4:* 远程日志记录目标设置

字段名称	使用指南
名称 **(Name)**	输入新目标的名称。
目标类型 **(Target Type)**	选择目标类型。默认情况下设置为 UDP Syslog。
说明	输入新目标的简短说明。
IP 地址 **(IP Address)**	输入要存储日志的目标计算机的 IP 地址或主机名。 思科 ISE 支持 IPv4 和 IPv6 格式的日志记录。
端口 **(Port)**	输入目标计算机的端口号。
设备代码 **(Facility Code)**	选择要用于日志记录的系统日志设备代码。有效选项为 Local0 至 Local7。
最大长度 **(Maximum Length)**	输入远程日志目标消息的最大长度。有效选项为 200 至 1024 字节。
服务器关闭时缓冲消息 **(Buffer Message When Server is Down)**	如果希望Cisco ISE 在 TCP 系统日志目标和安全系统日志目标不可用时缓冲系统日志消息，请选中此复选框。Cisco ISE 会在连接恢复时重新尝试将消息发送到目标。连接恢复后，消息按从最旧到最新的顺序进行发送，并且缓冲消息始终在新消息之前发送。如果缓冲区已满，则会丢弃旧消息。
缓冲区大小 **(MB) (Buffer Size [MB])**	设置每个目标的缓冲区大小。默认情况下设置为 100 MB。更改缓冲区大小会清除缓冲区，并且特定目标的所有现有缓冲消息都会丢失。
重新连接超时（秒）**(Reconnect Timeout [Sec])**	输入时间（以秒为单位），提及在服务器关闭的情况下，TCP 和安全系统日志在被丢弃之前将会保留多长时间。
选择 **CA** 证书 **(Select CA Certificate)**	选择客户端证书。
忽略服务器证书验证 **(Ignore Server Certificate Validation)**	如果希望 ISE 忽略服务器证书身份验证并接受任何系统日志服务器，请选中此复选框。

相关主题

- 思科 ISE 日志记录机制
- 思科 ISE 系统日志
- 远程系统日志消息格式
- 思科 ISE 消息目录

集合过滤器
事件抑制绕行过滤器
配置远程系统日志收集位置
配置集合过滤器

日志记录类别设置

下表介绍了**日志记录类别 (Logging Categories)** 窗口中的字段，可以使用此窗口配置日志严重性级别，并为要存储的所选类别的日志选择日志记录目标。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择**管理 (Administration)** > **系统 (System)** > **日志记录 (Logging)** > **日志记录类别 (Logging Categories)**。

表 *5:* 日志记录类别设置

字段名称	使用指南
名称 (Name)	显示日志记录类别的名称。
日志严重性级别 (Log Severity Level)	允许您从以下选项中选择诊断日志记录类别的严重性级别： • **严重 (FATAL)**：紧急情况。此选项意味着无法使用Cisco ISE，并且必须立即采取操作。 • **错误 (ERROR)**：此选项表示严重或错误情况。 • **警告 (WARN)**：此选项表示正常但值得注意的情况。这是默认情况。 • **信息 (INFO)**：此选项表示信息性消息。 • **调试 (DEBUG)**：此选项表示诊断错误消息。
本地日志记录 (Local Logging)	选中此复选框可为本地节点上的类别启用日志记录事件。
目标 (Targets)	允许使用左侧和右侧图标在**可用 (Available)** 和**所选 (Selected)** 框之间转移目标来更改类别的目标。**可用 (Available)** 框包含本地（预定义）和外部（用户定义）的现有日志记录目标。初始为空的**所选 (Selected)** 框包含特定类别的选定目标。

相关主题

远程系统日志消息格式
思科 ISE 消息代码

配置远程系统日志收集位置
设置消息代码的严重性级别

管理员访问设置

您可以通过这些页面为管理员配置访问设置。

管理员密码策略设置

下表介绍了“管理员密码策略”(Administrator Password Policy) 窗口中的字段，可以使用此窗口定义管理员密码应满足的条件。。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择**管理 (Administration)** > **系统 (System)** > **管理员访问权限 (Admin Access)** > **身份验证 (Authentication)** > **密码策略 (Password Policy)**。

表 *6:* 管理员密码策略设置

字段名称	使用指南
最小长度 (Minimum Length)	指定密码的最小长度（以字符数为单位）。默认值为 6 个字符。

字段名称	使用指南
密码不得包含 **(Password must not contain)**	**管理员名称或其反向顺序的字符 (Admin name or its characters in reverse order)**：选中此复选框可限制使用管理员用户名或其反向顺序的字符。
	“cisco”或其反向顺序的字符 ("cisco" or its characters in reverse order)：选中此复选框可限制使用单词“cisco”或其反向顺序的字符。
	此单词或其反向顺序的字符 (This word or its characters in reverse order)：选中此复选框可限制使用您定义的任何单词或其反向顺序的字符。
	连续重复四次或以上的字符 (Repeated characters four or more times consecutively)：选中此复选框可限制使用连续重复四次或以上的字符。
	字典单词、其反向顺序的字符或其替换为其他字符的字母 (Dictionary words, their characters in reverse order or their letters replaced with other characters)：选中此复选框可限制使用字典单词、其反向顺序的字符或其替换为其他字符的字母。 不允许使用“$”替代“s”、“@”替代“a”、“0”替代“o”、“1”替代“l”、“!”替代“i”、“3”替代“e”。例如 Pa$$w0rd • **默认字典 (Default Dictionary)**：选择此选项可在Cisco ISE 中使用默认 Linux 字典。此默认字典包含约 480,000 个英文单词。 默认情况下，此选项已选中。 • **自定义字典 (Custom Dictionary)**：选择此选项可使用您自定义的字典。点击**浏览**选择自定义字典文件。此文本文件必须包含新行分隔单词，为 .dic 扩展，且大小低于 20 MB。
密码必须包含每个所选类型的至少一个字符 (Password must contain at least one character of each of the selected types)	指定管理员密码必须包含从以下选项中选择的类型的至少一个字符： • 小写字母字符 • 大写字母字符 • 数字字符 • 非字母数字字符

字段名称	使用指南
密码历史记录 **(Password History)**	指定必须与新密码不同的先前密码的数量，以防止重复使用同一密码。 此外，指定必须与先前密码不同的字符的数量。 输入在其之前不能重复使用密码的天数。
密码有效期 **(Password Lifetime)**	指定以下选项来强制用户在经过指定时间段后更改密码： • “如果此时间（按天计）过后未更改密码，则禁用管理员帐户。”(Time (in days) before the administrator account is disabled if the password is not changed.)（允许的范围是 0 至 2147483647 天。） • “禁用管理员帐户之前的提醒时间（按天计）。”(Reminder (in days) before the administrator account is disabled.)
显示网络设备敏感数据 **(Display Network Device Sensitive Data)**	
要求管理员密码 **(Require Admin Password)**	如果您希望管理员用户输入登录密码来查看网络设备敏感数据，例如共享密钥和密码，请选中此复选框。
密码缓存用于 **(Password cached for)**	在此段时间内，会对管理员用户输入的密码进行缓存。在此期间，如果管理员用户要查看网络设备敏感数据，系统不会再次提示输入密码。有效范围为 1 至 60 分钟。

相关主题

思科 ISE 管理员

创建新管理员

会话超时和会话信息设置

下表介绍**会话 (Session)** 窗口中的字段，您可以使用此窗口定义会话超时和终止活动管理会话。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择**管理 (Administration)** > **系统 (System)** > **管理员访问 (Admin Access)** > **设置 (Settings)** > **会话 (Session)**。

表 *7:* 会话超时和会话信息设置

字段名称	使用指南
会话超时 **(Session Timeout)**	

字段名称	使用指南
会话空闲超时 (Session Idle Timeout)	输入Cisco ISE 在没有活动的情况下注销管理员之前需要等待的时间（以分钟为单位）。默认值为 60 分钟。有效范围为 6 至 100 分钟。
会话信息 (Session Info)	
失效 (Invalidate)	选中要终止的会话 ID 旁边的复选框，然后点击 **失效 (Invalidate)**。

相关主题

管理员访问设置
配置管理员会话超时
终止活动管理会话

管理节点

通过具有管理角色的Cisco ISE 节点，您可以在Cisco ISE 上执行所有管理操作。此节点处理与诸如身份验证、授权和审核等功能有关的所有系统相关配置。在分布式环境中，最多可以具有两个运行管理角色的节点。管理角色可以承担以下任何一个角色：独立角色、主角色或辅助角色。

管理节点的高可用性

在高可用性配置中，主策略管理节点 (PAN) 处于活动状态。辅助 PAN 处于备用状态，这意味着它会从主 PAN 接收所有配置更新，但在Cisco ISE 网络中不处于活动状态。

Cisco ISE 支持手动和自动故障转移。对于自动故障转移，当主 PAN 关闭时，辅助 PAN 会自动升级。自动故障转移需要非管理辅助节点（称为运行状况检查节点）。运行状况检查节点检查主 PAN 的运行状况。如果运行状况检测到主 PAN 已关闭或无法访问，则运行状况检查节点会让辅助 PAN 升级以接管主节点角色。

要部署自动故障转移功能，您必须至少有三个节点，其中两个节点承担管理角色，一个节点充当运行状况检查节点。运行状况检查节点为非管理节点，可以是 PSN、MnT、pxGrid 节点或其组合。如果主 PAN 和辅助 PAN 位于不同的数据中心，则每个 PAN 都必须有运行状况检查节点。

下表列出主 PAN 关闭且辅助 PAN 尚未接管时受影响的功能。

功能	主 **PAN** 关闭时是否可用？（是/否）
现有的内部用户 RADIUS 身份验证	是
现有或新的 AD 用户 RADIUS 身份验证	是
无配置文件更改的现有终端	是
有配置文件更改的现有终端	否

功能	主 **PAN** 关闭时是否可用？（是/否）
通过分析了解的新终端。	否
现有访客：本地 Web 身份验证 (LWA)	是
现有访客：集中式 Web 身份验证 (CWA)	是（除了为设备注册启用的流程之外，例如热点、自带设备和带自动设备注册功能的 CWA）
访客更改密码	否
访客：AUP	否
访客：最大登录失败次数实施	否
新访客（发起或自注册）	否
终端安全评估	是
具有内部 CA 的 BYOD	否
现有的注册设备	是
MDM 自行激活服务	否
pxGrid 服务	否
登录辅助节点的 GUI	是（登录过程延迟，因为对 PAN 发起了阻塞调用以更新上次登录详细信息。在上述调用超时后继续登录）

为支持使用内部证书颁发机构调配的证书，必须在升级后将原始主 PAN 的根证书及其密钥导入新的主要节点。自动故障转移之后，对于在辅助节点升级为主 PAN 后添加的 PSN 节点，证书调配不起作用。

高可用性运行状况检查节点

主 PAN 的运行状况检查节点称为主动运行状况检查节点。辅助 PAN 的运行状况检查节点称为被动运行状况检查节点。主动运行状况检查节点负责检查主 PAN 的状态，并管理管理节点的自动故障切换。我们建议使用两个非管理 ISE 节点作为运行状况检查节点，一个用于主 PAN，一个用于辅助 PAN。如果仅使用一个运行状况检查节点，并且该节点发生故障，则不会发生自动故障切换。

当两个 PAN 都位于同一数据中心时，可以使用单个非管理 ISE 节点作为主 PAN 和辅助 PAN 的运行状况检查节点。当一个运行状况检查节点同时检查主 PAN 和辅助 PAN 的运行状况时，它将承担主动和被动两种角色。

运行状况检查节点为非管理节点，意味着它可以是策略服务、监控或 pxGrid 节点，或它们的组合。我们建议将与管理节点处于同一数据中心的 PSN 节点指定为运行状况检查节点。但是，在两个管理节点不在相同位置（局域网或数据中心）的小型部署或集中部署中，没有管理角色的任意节点 (PSN/pxGrid/MnT) 都可用作运行状况检查节点。

如果选择不启用自动故障切换，并且在主PAN发生故障时依赖手动升级辅助节点，则无需任何检查节点。

辅助 PAN 的运行状况检查节点

辅助 PAN 的运行状况检查节点是一个被动监控器。在辅助 PAN 升级为主 PAN 之前，它不执行任何操作。当辅助PAN接管主要节点职责时，其关联的运行状况检查节点会承担主动职责，为管理节点管理自动故障切换。之前主 PAN 的运行状况检查节点现在成为辅助 PAN 的运行状况检查节点，并对此节点执行被动监控。

禁用和重新启动运行状况检查

当从运行状况检查角色删除某个节点或禁用自动故障切换配置时，系统会在该节点上停止运行状况检查服务。在指定的高可用性运行状况检查节点上启用自动故障切换配置时，节点又开始检查管理节点的运行状况。在节点上指定或删除高可用性运行状况检查角色不涉及在该节点上重新启用应用；系统只会启动或停止运行状况检查活动。

如果高可用性运行状况检查节点重新启动，该节点会忽略主PAN的之前停机并重新开始检查运行状态。

运行状况检查节点

活动的运行状况检查节点按照已配置的轮询间隔检查主PAN的运行状况。它会向主PAN发送请求，如果接收到的响应符合配置，则运行状况检查节点认为主PAN的运行状况良好。否则，运行状况检查节点认为主 PAN 的运行状况不佳。如果主 PAN 的运行状况持续不佳，超过了所配置的故障切换期，则运行状况检查节点会开始故障切换至辅助 PAN 。

在运行状况检查期间，如果发现之前报告为不佳的运行状况在故障切换期内转为良好，则运行状况检查节点会将主 PAN 的状态标记为良好，并重置运行状况检查周期。

主PAN运行状况检查的响应会对照其运行状况检查节点上的配置值进行验证。如果响应不匹配则会发出警报。但是，会向辅助 PAN 发送升级请求。

更改运行状况节点

您可以更改用于运行状况检查的Cisco ISE 节点，但需要考虑一些事项。

例如，假定运行状况节点 (H1) 无法同步而另一个节点 (H2) 被指定为主 PAN 的运行状况检查节点。在这种情况下，一旦主 PAN 关闭，H1 就无法获知还存在另一个节点 (H2) 在检查相同的主 PAN。稍后，如果 H2 也关闭或断开网络连接，则需要真正的故障切换。但是，辅助 PAN 会保留拒绝升级请求的权利。因此，一旦辅助 PAN 升级为主要角色，则来自 H2 的升级请求就会被拒绝，并出现错误。即使主 PAN 的运行状况检查节点无法同步，它仍会继续检查主 PAN 的运行状况。

自动故障转移至辅助 PAN

您可以将Cisco ISE 配置为在主 PAN 不可用时自动升级辅助 PAN。此配置是在**部署 (Deployment)** 窗口中的主策略管理节点（主 PAN）上完成的。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择**管理 (Administration)** > **系统 (System)** > **部署 (Deployment)**。故障转移时间段定义为**故障转移**

前轮询失败次数 (Number of Failure Polls Before Failover) 中配置的次数乘以**轮询间隔 (Polling Interval)** 中配置的秒数。使用默认配置时，该时间为 10 分钟。将辅助 PAN 升级为主 PAN 需要额外 10 分钟。因此，默认情况下，从主 PAN 故障到辅助 PAN 工作的总时间为 20 分钟。

当辅助 PAN 收到故障转移调用时，会在真正执行故障转移前进行以下验证：

- 主 PAN 在网络中不可用。
- 故障转移请求来自有效的运行状况检查节点。
- 故障转移请求面向此 PAN。

如果这些验证全部通过，则辅助 PAN 会自行升级为主角色。

以下是（但不限于）会尝试辅助 PAN 自动故障转移的部分场景示例。

- 在轮询期间，就**故障转移前轮询失败次数 (Number of failure polls before failover)** 值而言，主 PAN 的运行状况持续不佳。
- 主 PAN 上的Cisco ISE 服务被手动停止，并在故障转移期间保持停止状态。
- 主 PAN 通过软停止或重新启动选项关闭，并在配置的故障转移期间保持关闭状态。
- 主 PAN 突然关闭（断电），并在故障转移期间保持关闭状态。
- 主 PAN 的网络接口关闭（网络端口关闭或网络服务停止），或由于任何其他原因导致运行状况检查节点无法与之接通，并在配置的故障转移期间保持关闭状态。

运行状况检查节点重新启动

重新启动后，高可用性运行状况检查节点会忽略主 PAN 之前的停机并重新检查运行状况。

在自动故障转移到辅助 PAN 情况下自带设备

当主 PAN 故障时，对于已具有由主 PAN 根 CA 链颁发的证书的终端，身份验证不会中断。这是因为部署中的所有节点都具有用于信任和验证目的的整个证书链。

但是，在辅助 PAN 升级为主 PAN 之前，不会激活新的自带设备。自带设备激活需要处于活动状态的主 PAN。

当原主 PAN 恢复或升级辅助 PAN 后，新的自带设备终端将激活，不会出现任何问题。

如果发生故障的主 PAN 无法重新作为主 PAN 加入，请在新升级的主 PAN（原辅助 PAN）上重新生成根 CA 证书。

对于现有证书链，触发新的根 CA 证书会自动生成从属 CA 证书。即使生成新的从属证书，由上一个链生成的终端证书也继续有效。

避免自动故障转移时的示例场景

以下是描绘将会避免运行状况检查节点进行自动故障转移或将会拒绝向辅助节点提出的升级请求的情况的一些示例场景。

- 收到升级请求的节点不是辅助节点。
- 辅助 PAN 收到的升级请求没有正确的主 PAN 信息。
- 从错误的运行状况检查节点收到升级请求。
- 收到升级请求，但是主 PAN 已启动并处于良好运行状况。
- 收到升级请求的节点不同步。

受 PAN 自动故障转移功能影响的功能

下表列出如果部署中启用 PAN 自动故障转移配置而被阻止或需要其他配置更改的功能。

功能	影响详细信息
被阻止的操作	
升级	通过 CLI 的升级被阻止。 将Cisco ISE 从旧版本升级到 1.4 版本之后，可配置 PAN 自动故障转移功能。默认情况下，此功能处于禁用状态。 要部署自动故障转移功能，必须至少有三个节点，其中两个节点承担管理角色，一个节点充当运行状况检查节点。运行状况检查节点为非管理节点，可以是 PSN、MnT、pxGrid 节点或其组合。如果PAN位于不同的数据中心，则每个PAN都必须有运行状况检查节点。
备份恢复	通过 CLI 和用户界面的恢复将被阻止。 如果PAN自动故障转移配置已在恢复之前启用，则必须在成功恢复后重新配置。
更改节点角色	通过用户界面更改以下节点角色的操作将被阻止： • 主 PAN 和辅助 PAN 中的管理角色 • PAN 的角色 • 在启用PAN自动故障转移功能后注销运行状况检查节点

功能	影响详细信息
其他 CLI 操作	以下通过 CLI 的管理员操作将被阻止： • 补丁安装和回滚 • DNS 服务器更改 • eth1、eth2 和 eth3 接口的 IP 地址更改 • eth1、eth2 和 eth3 接口的主机别名更改 • 时区更改
其他管理门户操作	通过用户界面执行的以下管理员操作将被阻止： • 补丁安装和回滚 • 更改 HTTPS 证书 • 将管理员身份验证类型从基于密码的身份验证更改为基于证书的身份验证，或者相反
连接设备最多的用户无法连接。	某些会话数据存储在故障 PAN 上，无法由 PSN 更新。
需要禁用 PAN 自动故障转移的操作	
CLI 操作	如果 PAN 自动故障转移配置已启用，则通过 CLI 执行的以下管理操作将显示警告消息。如果服务或系统未在故障转移窗口期内重新启动，则这些操作可能会触发自动故障转移。因此，在执行以下操作时，建议禁用 PAN 自动故障转移配置： • 手动停止Cisco ISE 服务 • 使用管理员 CLI 对Cisco ISE 进行软重新加载（重新引导）

配置自动故障转移的主 PAN

开始之前

要部署自动故障转移功能，您必须至少有三个节点，其中两个节点承担管理角色，一个节点充当运行状况检查节点。运行状况检查节点为非管理节点，可以是 PSN、MnT、pxGrid 节点或其组合。如果 PAN 位于不同的数据中心，则每个 PAN 都必须有运行状况检查节点。

步骤 1 登录主要 PAN 的用户界面。

步骤 2 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **部署 (Deployment)** > **PAN 故障转移 (PAN Failover)**。

步骤 3 选中**启用 PAN 自动故障转移 (Enable PAN Auto Failover)** 复选框以启用主 PAN 的自动故障转移。

只能将辅助 PAN 升级为主 PAN。仅作为 PSN、MnT、pxGrid 节点或其组合的Cisco ISE 节点不能升级成为主 PAN。

步骤 4 从包含所有可用辅助节点的**主运行状况检查节点 (Primary Health Check Node)** 下拉列表中选择主 PAN 的运行状况检查节点。

建议将此节点保存在与主 PAN 相同的位置或数据中心。

步骤 5 从包含所有可用辅助节点的**辅助运行状况检查节点 (Secondary Health Check Node)** 下拉列表中选择辅助 PAN 的运行状况检查节点。

建议将此节点保存在与辅助 PAN 相同的位置或数据中心。

步骤 6 在**轮询间隔 (Polling Interval)** 中提供轮询间隔时间，在此时间之后，系统将检查 PAN 状态。有效范围为 30 - 300 秒。

步骤 7 为**故障转移前的故障轮询次数 (Number of Failure Polls before Failover)** 提供计数。

如果 PAN 的状态不适用于指定故障轮询次数，将发生故障转移。有效计数范围为 2 - 60。

步骤 8 点击**保存 (Save)**。

下一步做什么

将辅助 PAN 升级到主 PAN 之后，请执行以下操作：

- 手动同步旧的主 PAN 以将其带回至部署中。
- 手动同步任何其他不同步的辅助节点，以将其带回至部署中。

手动将辅助 PAN 升级为主 PAN

如果主 PAN 出现故障而且您没有配置 PAN 自动故障转移，则必须手动将辅助 PAN 升级为新的主 PAN。

开始之前

确保已配置具有管理角色的第二个Cisco ISE 节点，以将其升级为主 PAN。

步骤 1 登录辅助 PAN 的用户界面。

步骤 2 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **部署 (Deployment)**。

步骤 3 在“编辑节点”(Edit Node) 页面，点击**升级为主节点 (Promote to Primary)**。

只能将辅助 PAN 升级为主 PAN。仅承担策略服务角色和/或监控角色的Cisco ISE 节点无法升级为主 PAN。

步骤 4 点击保存 **(Save)**。

下一步做什么

如果原来为主PAN的节点恢复运行，则会自动降级成为辅助PAN。必须对此节点（原来为主PAN）执行手动同步，才能将其恢复到部署中。

在辅助节点的**编辑节点 (Edit Node)** 页面，无法修改角色或服务，因为这些选项已禁用。您必须登录 Admin 门户才能进行更改。

将现有思科 ISE 部署的节点重新用作新思科 ISE 部署的主 PAN

如果要将现有Cisco ISE 部署的节点重新用作新Cisco ISE 部署的主 PAN，必须执行以下步骤：

步骤 1 首先按照适用于您的Cisco ISE 版本的《Cisco ISE 安装指南》所述，运行Cisco ISE 实用程序“执行系统擦除” https://www.cisco.com/c/en/us/support/security/identity-services-engine/products-installation-guides-list.html

步骤 2 按照《Cisco ISE 安装指南》所述，执行Cisco ISE 的全新安装。

步骤 3 参阅配置主策略管理节点 (PAN)，第 3 页，将独立节点配置为主策略管理节点。

将服务恢复到主 PAN

Cisco ISE 不支持自动回退至原主 PAN。在启动到辅助 PAN 的自动故障切换后，如果将原主 PAN 重新接入网络，则应将其配置为辅助 PAN。

支持管理节点的自动故障转移

Cisco ISE 支持管理角色的自动故障转移。要启用自动故障转移功能，分布式设置中至少有两个节点应承担管理角色，一个节点应承担非管理角色。当主 PAN 关闭时，辅助 PAN 会自动升级。为此，系统将非管理辅助节点指定为每个 PAN 的运行状况检查节点。运行状况检查节点按配置的间隔检查主 PAN 的运行状况。如果收到的主 PAN 运行状况检查响应由于设备关闭或无法访问而不理想，运行状况检查节点会启动辅助 PAN 的升级，从而在等待已配置的阈值对应的时间后接管主角色。在辅助 PAN 自动故障转移后，有些功能不可用。Cisco ISE 不支持回退到原始主 PAN。有关详细信息，请参阅管理节点的高可用性部分。

策略服务节点

策略服务节点 (PSN) 是承担策略服务角色的Cisco ISE 节点，提供网络访问、终端安全评估、访客访问、客户端调配和分析服务。

分布式设置中至少有一个节点应当承担策略服务角色。此角色评估策略并制定所有决策。通常，分布式部署中会有多个 PSN。

驻留在同一高速局域网 (LAN) 中或负载均衡器后面的所有 PSN 可以组合在一起，形成一个节点组。如果节点组中的一个节点发生故障，其他节点会检测到故障，并重置任何 URL 重定向会话。

策略服务节点的高可用性

要检测节点故障并在故障节点上重置所有 URL 重定向的会话，可将两个或多个 PSN 放置在同一节点组中。当属于节点组的节点出现故障时，同一个节点组中的另一个节点会为故障节点上的所有 URL 重定向会话发出授权更改 (CoA) 请求。

同一个节点组中的所有节点都应在网络接入设备 (NAD) 上配置为 RADIUS 客户端并拥有 CoA 授权，因为这些节点中的任何一个节点均可为通过该节点组中的任一节点建立的会话发出 CoA 请求。如果您未使用负载均衡器，节点组中的节点应与在 NAD 上配置的 RADIUS 服务器和客户端相同，或是 RADIUS 服务器和客户端的子集。这些节点还将配置为 RADIUS 服务器。

虽然单个 NAD 可以配置多个Cisco ISE 节点以作为 RADIUS 服务器和动态授权客户端，但节点不必全部位于同一个节点组。

一个节点组中的所有成员应通过高速 LAN 连接（例如，千兆以太网）互相建立连接。虽然节点组成员不需要在第二层相邻，但是我们依然建议节点组成员在第 2 层相邻，以确保足够的宽带和可达性。请参阅 创建策略服务节点组，第 48 页 章节了解更多详细信息。

用于在 PSN 之间均匀分配请求的负载均衡器

如果您在部署中具有多个 PSN，则可以使用负载均衡器均匀分配请求。负载均衡器会将请求分配给其后面的功能节点。请参阅《思科和 F5 部署指南：使用 BIG-IP 的 ISE 负载均衡》中的信息并了解有关在负载均衡器后面部署 PSN 的最佳实践。

策略服务节点中的会话故障切换

节点组中的 PSN 共享会话信息。节点交换心跳消息以检测节点故障。如果某个节点出现故障，其节点组中的一个对等体会了解故障 PSN 上的会话并发出 CoA 以断开这些会话。大多数客户端会自动重新连接并建立新会话。

某些客户端不会自动重新连接。例如，如果客户端通过 VPN 连接，则此客户端可能看不到 CoA。作为 IP 电话、多主机 802.1X 端口或虚拟机的客户端也可能看不到或无法响应 CoA。URL 重定向客户端 (webauth) 也无法自动连接。这些客户端必须手动重新连接。

时间问题也会阻止重新连接。例如，如果发生 PSN 故障切换，终端安全评估处于待处理状态。

有关 PSN 会话共享的详细信息，请参阅轻量数据分配，第 32 页。

策略服务节点组中的节点数量

节点组中可以具有的节点数量取决于部署要求。节点组确保检测到节点故障，并且对等节点针对已获授权但尚未进行安全评估的会话发出 CoA。节点组的规模不必非常大。

如果节点组的规模增大，那么节点之间交换的消息和心跳数量也会显著增加。因此，流量也会随之增加。节点组中的节点较少时，有助于减少流量，同时提供足够的冗余来检测 PSN 故障。

节点组集群可以包含的 PSN 数量没有硬性限制。

轻量数据分配

轻量数据分布用于存储用户会话信息并在部署中的 PSN 之间复制这些信息，从而无需依赖 PAN 或 MnT 节点来获取用户会话详细信息。

轻量数据分布包括以下两个目录：

- Radius 会话目录
- 终端所有者目录

此外，还可以在**高级设置 (Advanced Settings)**下配置以下选项：

- **批量大小 (Batch Size)**：可以批量发送会话更新。此值可指定从一个轻量数据分布实例发送到部署中其他 PSN 的每一批记录的数量。如果此字段设置为 1，则不分批发送会话更新。默认值为 10 个记录。
- **TTL**：此值指定在更新轻量数据分布之前，会话等待批处理完成的最长时间。默认值为 1000 毫秒。

如果 PSN 之间存在连接问题（例如，当 PSN 关闭时），系统会从 MnT 会话目录检索会话详细信息并存储以供将来使用。

大型部署最多可以保留 2,000,000 个会话记录。小型部署可以存储 1,000,000 个会话记录。当收到会话的记账停止请求时，系统会从所有轻量数据分布实例中删除对应的会话数据。当存储的记录数量超过最大限制时，系统会根据时间戳删除最早的会话。

注释

- 如果会话的 IPv6 前缀长度小于 128 位并且未指定接口 ID，则 IPv6 前缀会被拒绝，从而防止多个会话具有相同的密钥。
- 轻量数据分布使用Cisco ISE 消息服务进行节点间通信。Cisco ISE 消息服务使用不同的证书（由内部 CA 链签名）。当遇到Cisco ISE 消息服务问题时，需要重新生成Cisco ISE 消息服务证书。在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **证书 (Certificates)** > **证书管理 (Certificate Management)** > **证书签名请求 (Certificate Signing Request)**。在**证书将用于 (Certificate(s) will be used for)** 部分选择 **ISE 消息服务 (ISE Messaging service)**。点击**生成 ISE 消息服务证书 (generate ISE messaging service certificate)**。

Radius 会话目录

RADIUS 会话目录用于存储用户会话信息，并在部署中的 PSN 之间复制信息。**RADIUS 会话目录**仅存储授权更改 (CoA) 所需的会话属性。

自Cisco ISE 2.7 版起，默认启用此功能。您可以通过选中或取消选中**轻量数据分配 (Light Data Distribution)** 窗口中的 **RADIUS 会话目录 (RADIUS Session Directory)** 复选框启用或禁用此功能。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **设置 (Settings)** > **轻量数据分配 (Light Data Distribution)**。

终端所有者目录

在Cisco ISE 版本 2.6 之前，当在策略服务节点 (PSN) 上收到的终端探测不同于最初为该特定终端处理请求的终端探测时，终端所有者将更改为新的 PSN。这会导致终端所有权摆动。

从Cisco ISE 版本 2.7 开始，**终端所有者目录**用于存储连接到Cisco ISE 的每个 MAC 地址的 PSN FQDN，并在部署中的 PSN 之间复制此数据。这可以避免终端所有权摆动，因为所有 PSN 现在都知道所有终端所有者。现在，仅当在另一个 PSN 上成功进行该终端的 RADIUS 身份验证后，终端所有权才会更改。

此外，静态终端分配优先于同一终端的传入探测器接收的属性，从而避免属性覆盖问题。

自Cisco ISE 2.7 版起，默认启用此功能。如果需要，您可以将其禁用以回退到不使用终端所有者目录的旧机制。**终端所有者目录**还用于分析，禁用此选项将使用传统分析器所有者的目录。您可以通过选中或取消选中**轻量数据分配 (Light Data Distribution)** 窗口中的**启用终端所有者目录 (Enable Endpoint Owner Directory)** 复选框启用或禁用此功能。 要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **设置 (Settings)** > **轻量数据分配 (Light Data Distribution)**。

监控节点

承担监控角色的Cisco ISE 节点用作日志收集器，并将来自 PAN 和 PSN 的日志消息存储在网络中。此角色提供高级监控和故障排除工具，可用于有效地管理网络和资源。承担此角色的节点会整合并关联收集到的数据，以报告形式向您提供有意义的信息。

Cisco ISE 最多允许有两个节点承担此角色（由主或辅助节点承担此角色），以实现高可用性。主要和辅助 MnT 节点均收集日志消息。如果主 MnT 断开，则主 PAN 将指向辅助节点以收集监控数据。但辅助节点不会自动升级为主节点。可以通过手动修改 MnT 角色 来完成升级。

在分布式设置中，至少应有一个节点应承担监控角色。我们建议您不要对同一个Cisco ISE 节点启用监控和策略服务角色。我们建议您只将该节点用于监控，以实现最佳性能。

您可以从部署中的 PAN 访问监控 (Monitoring) 菜单。

注释 如果已启用 pxGrid，必须为 pxGrid 节点创建新证书。创建使用数字签名用法的证书模板，并生成新的 pxGrid 证书。

手动修改 MnT 角色

您可以从主要 PAN 手动修改 MnT 角色（从主要改为辅助，从辅助改为主要）。

步骤 1 登录主要 PAN 的用户界面。

步骤 2 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **部署 (Deployment)**。

步骤 3 从节点列表中，选中要更改角色的 MnT 节点旁边的复选框。

步骤 4 点击**编辑 (Edit)**。

步骤 5 在**监控 (Monitoring)** 部分中，将角色更改为**主要 (Primary)** 或**辅助 (Secondary)**。

步骤 6 点击**保存 (Save)**。

注释 如果要禁用该节点上启用的所有其他角色和服务，可以启用**专用 MnT (Dedicated MnT)** 选项。启用此选项后，系统将停止该节点上的配置数据复制过程。这有助于提高MnT节点的性能。当禁用此选项时，将触发手动同步。

经思科 ISE 消息服务传递的系统日志

Cisco ISE 版本 2.6 为默认内置 UDP 系统日志收集目标 LogCollector 和 LogCollector2 提供 MnT WAN 生存性。要启用此生存性，请使用选项**使用“ISE 消息服务”将 UDP 系统日志发送到 MnT (Use "ISE Messaging Service" for UDP Syslogs delivery to MnT)**（在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **系统 (System)** > **日志记录 (Logging)** > **日志设置 (Log Settings)**）。启用此选项时，UDP 系统日志受传输层安全 (TLS) 保护。

在Cisco ISE 版本 2.6 首次发货 (FCS) 中，**使用“ISE 消息服务”将 UDP 系统日志发送到 MnT (Use "ISE Messaging Service" for UDP Syslogs delivery to MnT)** 选项在默认情况下处于禁用状态。在Cisco ISE 版本 2.6 累积补丁 2 及更高版本中，此选项在默认情况下处于启用状态。

将Cisco ISE 消息服务用于 UDP 系统日志可在有限的持续时间内保留运行数据，即使无法访问 MnT 节点也是如此。MnT WAN 生存期约为 2 小时 30 分钟。

此服务使用 TCP 端口 8671。请相应地配置网络，并允许从部署中的所有其他Cisco ISE 节点连接到每个Cisco ISE 节点上的 TCP 端口 8671。以下功能也使用Cisco ISE 消息服务：轻型会话目录（请参阅《思科身份识别服务引擎管理员指南》中“在分布式环境中设置Cisco ISE”一章中的“轻型会话目录”部分以及分析器持久化队列。

注释 如果您的部署将 TCP 或安全系统日志用于思科 ISE 部署，则此功能与早期版本相同。

队列-链接警报

Cisco ISE 消息服务使用由内部 CA 链签名的不同证书。您可能会在Cisco ISE GUI 控制板的**警报 (Alarms)** Dashlet 中收到队列-链接警报。如果您正在执行任何部署操作（例如，将节点注册到部署、从主 PAN 手动同步节点、节点处于不同步状态或在节点中重新启动应用服务），则会触发此警报。确保符合以下条件以解决警报：

- 所有节点均已连接并同步。
- 所有节点和思科 ISE 消息服务均正常运行。
- 防火墙等外部实体不会阻止思科 ISE 消息服务端口。
- 每个节点上的思科 ISE 消息证书链未中断且证书状态良好。

如果满足上面列出的先决条件，则队列-链接警报将因以下操作而触发：

- 更改 PAN 或 PSN 的域名或主机名。
- 在新部署中恢复备份。
- 在升级后将旧的主 PAN 升级为新的主 PAN。

替换Cisco ISE 根 CA 链时，Cisco ISE 消息服务证书也将替换。此后将重新启动Cisco ISE 消息服务，停机时间约为 2 分钟。因此，系统日志将在此停机期间丢失。为避免在停机期间丢失系统日志，可在短时间内禁用Cisco ISE 消息服务。

启用或禁用Cisco ISE 消息服务以将 UDP 系统日志传送到 MnT：

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **系统 (System)** > **日志记录 (Logging)** > **日志设置 (Log Settings)**。

步骤 2 选中或取消选中**使用“ISE 消息服务”将 UDP 系统日志传送到 MnT (Use “ISE Messaging Service” for UDP Syslogs delivery to MnT)** 复选框以启用或禁用 ISE 消息服务。

步骤 3 点击**保存 (Save)**。

MnT 节点中的自动故障转移

MnT 节点不提供高可用性，但支持主用备用。PSN 会将操作审核数据同时复制到主 MnT 节点和辅助 MnT 节点。

自动故障转移过程

当主 MnT 节点断开时，辅助 MnT 节点会接管所有监控和故障排除信息。

要将辅助节点转换为主节点，请参阅手动修改MnT角色。如果主节点在辅助节点升级后恢复运行，则将承担辅助节点的角色。如果未升级辅助节点，则主 MnT 节点将在恢复运行后继续承担主要角色。

⚠

注意 当主节点在故障转移后恢复正常时，请获取辅助节点的备份并恢复数据以更新主节点。

MnT 节点主用备用对设置指南

您可以在Cisco ISE 网络上指定两个 MnT 节点，然后将其配置为主用备用对。我们建议备份主 MnT 节点，然后将数据恢复到新的辅助 MnT 节点。由于会复制新数据，因此这可确保主 MnT 节点的历史记录与新的辅助节点同步。以下规则适用于主用备用对：

- 所有更改都会记录到主 MnT 节点。辅节点为只读。
- 对主节点所做的更改会在辅助节点上自动复制。
- 主节点和辅助节点列为日志收集器，其他所有节点会向其发送日志。
- Cisco ISE 控制面板是监控和故障排除的主要入口点。控制板上显示来自 PAN 的监控信息。如果主节点关闭，可以从辅助节点获得信息。
- 备份和清除 MnT 数据不在标准Cisco ISE 节点备份过程中。必须同时在主辅 MnT 节点上为备份和数据清除配置存储库，并且在每个节点上使用相同的存储库。

MnT 节点故障转移方案

以下方案适用于 MnT 节点对应的主用备用或单节点配置：

- 在 MnT 节点的主用备用配置中，主 PAN 始终指向主 MnT 节点以收集监控数据。在主 MnT 节点故障后，PAN 会指向备用 MnT 节点。从主节点到辅助节点的故障转移发生在其关闭超过五分钟后。

  但是，在主节点发生故障后，辅助节点不会成为主节点。如果主节点启动，PAN 会再次开始从恢复的主节点收集监控数据。

- 如果主 MnT 节点关闭，并且您希望将备用 MnT 节点升级为主用状态，则可以通过手动修改 MnT 角色或注销现有主 MnT 节点来实现。注销现有 MnT 节点时，备用节点成为主 MnT 节点，并且 PAN 自动指向新升级的主节点。
- 在主用-备用对中，如果注销辅助 MnT 节点或辅助 MnT 节点关闭，则现有主 MnT 节点仍然为当前主节点。
- 如果Cisco ISE 部署中只有一个 MnT 节点，则该节点用作主 MnT 节点，并向 PAN 提供监控节点。但是，当注册新 MnT 节点并使其成为部署中的主节点时，现有主 MnT 节点会自动成为备用节点。PAN 会指向新注册的主 MnT 节点以收集监控数据。

监控数据库

鉴于监控功能使用的数据的比例和数量，需要在专用节点上将一个单独的数据库用于这些用途。

像 PSN 一样，MnT 节点有一个专用数据库，要求您执行维护任务，例如本节所涵盖的主题所涉及的任务：

监控数据库的备份和恢复

监控数据库处理大量数据。随着时间推移，MnT 节点的性能和效率取决于您对这些数据的管理水平。要提高效率，我们建议您定期备份数据并将其传输到远程存储库。通过计划自动备份，您可以将此任务自动化。

注释 如果正在进行清除操作，则不应执行备份。如果在清除操作过程中启动备份，则清除操作会停止或失败。

如果注册辅助 MnT 节点，我们建议先备份主 MnT 节点，然后将数据恢复到新的辅助 MnT 节点。由于会复制新的更改，因此这可确保主 MnT 节点的历史记录与新的辅助节点同步。

监控数据库清除

清除过程允许您通过以月为单位指定在清除期间保留数据的时间，管理监控数据库的大小。默认值为三个月。当达到清除流程的磁盘空间使用率阈值（占磁盘空间的百分比）时，会用到此值。对于该选项，每月包括 30 天。三个月的默认值等于 90 天。

监控数据库清除指南

请遵循以下监控数据库磁盘使用量的相关指南：

- 如果监控数据库磁盘使用量超过 80% 的阈值设置，则会生成严重警报，表示数据库大小已超过所分配的磁盘容量。如果磁盘使用量超过百分之九十，则会生成另一个警报。

  系统将运行清除过程，并创建状态历史报告，可以在**数据清除审核 (Data Purging Audit)** 窗口中查看该报告。 要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **操作 (Operations)** > **报告 (Reports)** > **报告 (Reports)** > **审核 (Audit)** > **数据清除审核 (Data Purging Audit)**。清除完成后会生成信息 (INFO) 警报。

- 清除同样依据数据库已使用的磁盘空间。当监控数据库已使用的磁盘空间达到或超过阈值时（默认为 80%），则会启动清除过程。此过程仅删除最近七天的监控数据，不论在管理员门户中进行了怎样的配置。系统将循环继续此过程直至磁盘空间使用量低于百分之八十。系统总会在检查监控数据库磁盘空间限制之后，才继续执行清除。

运营数据清除

Cisco ISE 监控操作数据库包含作为Cisco ISE 报告生成的信息。在Cisco ISE 最新版本中，可以选择在运行Cisco ISE 管理 CLI 命令 **application configure ise** 后清除监控操作数据并重置监控数据库。

清除选项用于清除数据，会通过提示符询问保留天数。重置选项用于将数据库重置为出厂默认设置，这将永久删除所有备份的数据。如果文件占用了文件系统的过多空间，您可以重置数据库。

注释 重置选项会导致思科 ISE 服务在系统完成重启前暂时不可用。

操作数据清除 (Operational Data Purging) 窗口包含**数据库利用率 (Database Utilization)** 和**立即清除数据 (Purge Data Now)** 区域。 要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **维护 (Maintenance)** > **操作数据清除 (Operational Data Purging)**。可以查看总可用数据库空间，以及存储在**数据库利用率 (Database Utilization)** 区域中的 RADIUS 和 TACACS 数据。您可以将鼠标悬停在状态栏上以显示可用磁盘空间，以及现有数据存储在数据库中的天数。可以指定在**数据保留期 (Data Retention Period)** 区域保留 RADIUS 和 TACACS 数据的时间段。系统在每天凌晨 4 点清除数据，此外，您还可以进行配置，以在清除数据前通过指定保留天数将其导出到存储库。可以选中**启用导出存储库 (Enable Export Repository)** 复选框以选择和创建存储库，并指定**加密密钥**。

在**立即清除数据 (Purge Data Now)** 区域中，可以清除所有 RADIUS 和 TACACS 数据，或指定天数以在超过该天数时将数据清除。

注释 可以在清除前将 RADIUS 身份验证和记账、TACACS 授权和记账、RADIUS 错误和错误配置的请求方表导出到存储库。

相关主题

清除较旧的运营数据，第 38 页

清除较旧的运营数据

运营数据在一段时间内收集到服务器上。可以立即或定期清除它。可以通过查看**数据清除审核 (Data Purging Audit)** 报告，验证数据清除是否成功。

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 **管理 (Administration)** > **系统 (System)** > **维护 (Maintenance)** > **运行数据清除 (Operational Data Purging)**。

步骤 2 执行以下操作之一：

- 在**数据保留期 (Data Retention Period)** 区域：
  1. 以日为单位指定 RADIUS 和 TACACS 数据的应保留期限。指定期限之前的所有数据都会导出到存储库。
  2. 在**存储库 (Repository)** 区域中，选中**启用导出存储库 (Enable Export Repository)** 复选框以选择保存数据的存储库。
  3. 在**加密密钥 (Encryption Key)** 文本框中，输入所需的密码。
  4. 点击**保存 (Save)**。

注释　如果配置的保留期限短于与诊断数据对应的现有保留阈值，则配置值将覆盖现有阈值。例如，如果将保留期配置为三天，而且该值小于诊断表中的现有阈值（例如，默认值为五天），则将根据在此窗口中配置的值（三天）清除数据。

- 在**立即清除数据 (Purge Data Now)** 区域：
  1. 选择清除所有数据或清除超过指定天数的数据。数据不会保存在任何存储库中。
  2. 点击**清除 (Purge)**。

配置用于自动故障切换的监控节点

如果部署中有两个MnT节点，则可以配置用于自动故障切换的主节点-辅助节点对，以避免Cisco ISE监控服务出现停机。主节点-辅助节点对可确保辅助 MnT 节点在主节点出现故障时自动提供监控。

开始之前

- 要配置用于自动故障切换的 MnT 节点，必须将这些节点注册为Cisco ISE 节点。
- 您必须在两个节点上配置监控角色和服务，适当地根据其主要和辅助角色进行命名。
- 在主要和辅助MnT节点上同时配置用于备份和数据清除的存储库。要让备份和清除功能正常运行，请对这两个节点使用相同的存储库。清除同时在冗余对的主要和辅助节点中发生。例如，如果主要 MnT 节点将两个存储库用于备份和清除，则必须为辅助节点指定相同的存储库。

  使用系统 CLI 中的 **repository** 命令为 MnT 节点配置数据存储库。

> ⚠ **注意**　要让计划的备份和清除在监控冗余对的节点上正常工作，请使用 CLI 在主节点和辅助节点上同时配置相同的存储库。存储库不会自动在两个节点之间同步。

在Cisco ISE 控制板中，验证 MnT 节点是否准备就绪。**系统摘要 (System Summary)** Dashlet 会在 MnT 节点服务准备就绪时显示左侧带绿色复选标记的 MnT 节点。

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)** > **部署 (Deployment)**。

步骤 2　在**部署节点 (Deployment Nodes)** 窗口中，选中要指定主节点的 MnT 节点旁边的复选框，然后点击**编辑 (Edit)**。

步骤 3　点击**常规设置 (General Settings)** 选项卡，然后从**角色 (Role)** 下拉列表中选择**主要 (Primary)**。

选择 MnT 节点作为主节点时，另一个 MnT 节点将自动成为辅助节点。如果是独立部署，主要和辅助角色配置会处于禁用状态。

步骤 4 点击**保存 (Save)**。主节点和辅助节点都会重新启动。

思科 pxGrid 节点

可以使用Cisco pxGrid 与其他网络系统（例如Cisco ISE 生态系统合作伙伴系统）和其他Cisco平台共享Cisco ISE 会话目录中的情景相关信息。pxGrid 框架也可用来在Cisco ISE 与第三方供应商之间、在节点（例如共享标记）与策略对象之间交换策略和配置数据，还能进行其他信息的交换。Cisco pxGrid 还允许第三方系统调通过自适应网络控制操作 (EPS) 来隔离用户和/或设备以应对网络或安全事件。可通过Cisco TrustSec 主题将标签定义、值和说明等Cisco TrustSec 信息从Cisco ISE 传输到其他网络。可通过终端配置文件元主题，将具有完全限定名称 (FQN) 的终端配置文件从Cisco ISE 传输到其他网络。Cisco pxGrid 还支持标签和终端配置文件的批量下载。

可通过Cisco pxGrid 发布和订用 SXP 绑定（IP-SGT 映射）。有关 SXP 绑定的详细信息，请参阅安全组标记交换协议。

在高可用性配置中，Cisco pxGrid 服务器通过 PAN 在节点之间复制信息。当 PAN 关闭时，Cisco pxGrid 服务器会停止处理客户端注册和订用。需要手动升级 PAN，以激活Cisco pxGrid 服务器。可以查看“思科 pxGrid 服务”(Cisco pxGrid Services) 窗口（“管理”(Administration) > “pxGrid 服务”(pxGrid Services)）以验证思科 pxGrid 节点当前处于主用状态还是备用状态。

在活动 Cisco pxGrid 1.0 节点上，这些进程显示为**正在运行 (Running)**。在备用 Cisco pxGrid 1.0 节点上，它们显示为**已禁用 (Disabled)**。如果活动 pxGrid 1.0 节点关闭，备用 pxGrid 节点会检测到此情况，并启动四个 pxGrid 进程。在几分钟内，这些进程显示为**正在运行 (Running)**，备用节点成为活动节点。可以运行 CLI 命令 **show logging application pxgrid** 或 **show logging application pxgrid.state** 来验证Cisco pxGrid 服务在此节点上是否处于备用状态。

对于 XMPP（可扩展消息传送和在线状态协议）客户端，Cisco pxGrid 节点在主用-备用高可用性模式下工作，这意味着Cisco pxGrid 服务在主用节点上处于“正在运行”(Running) 状态，在备用节点上处于“已禁用”(Disabled) 状态。

注释 在Cisco pxGrid 1.0 中，节点在主用-备用高可用性模式下工作表示Cisco pxGrid 服务在主用节点上处于“正在运行”(Running) 状态，在备用节点上处于“已禁用”(Disabled) 状态。可以运行 CLI 命令 **show logging application pxgrid** 或 **show logging application pxgrid.state** 来验证Cisco pxGrid 在此节点上是否处于备用状态。pxGrid 2.0 不存在此问题，pxGrid 显示备用。

启动面向辅助Cisco pxGrid 节点的自动故障切换后，如果原始主Cisco pxGrid 节点重新接入网络，则除非当前主节点关闭，否则原始主Cisco pxGrid 节点将继续具有辅助角色，并且不会重新升级到主角色。

注释 有时，原始主思科 pxGrid 节点可能会自动重新升级回主角色。

在高可用性部署中，当主 pxGrid 节点关闭时，可能需要大约 3 到 5 分钟来切换到辅助 pxGrid 节点。建议客户端等待故障切换完成，然后再清除缓存数据，以防主Cisco pxGrid 节点发生故障。

以下日志可用于Cisco pxGrid 节点：

- pxgrid.log：状态变更通知。
- pxgrid-cm.log：有关客户端与服务器之间的发布者和/或用户以及数据交换活动的更新。
- pxgrid-controller.log：显示客户端功能、组和客户端授权的详细信息。
- pxgrid-jabberd.log：与系统状态和身份验证相关的所有日志。
- pxgrid-pubsub.log：与发布者和用户事件相关的信息。

注释 如果在节点上禁用思科 pxGrid 服务，则端口 5222 将关闭，但是端口 8910（由 Web 客户端使用）将正常工作，并将继续对请求作出响应。

注释 可以使用思科 ISE Advantage 许可证启用 Cisco pxGrid 和 Cisco pxGrid 角色。

注释 应定义Cisco pxGrid，以便使用被动 ID 工作中心。有关详细信息，请参阅被动 ID 工作中心。

部署思科 pxGrid 节点

在独立节点和分布式部署节点上都可以启用Cisco pxGrid 角色。

开始之前

- 您必须具有Cisco ISE Advantage 许可证才能启用Cisco pxGrid 角色。
- 有关许可要求，请参阅 ISE 许可/订购。
- 所有节点都将 CA 证书用于Cisco pxGrid 服务用途。如果在升级之前对Cisco pxGrid 服务使用默认证书，则升级时会将该证书替换为内部 CA 证书。
- 必须为 Websocket (pxGrid 2.0) 打开端口 8910，并为 XMPP (pxGrid V1.0) 打开端口 5222。如果在节点上禁用Cisco pxGrid 服务，则端口 5222 将关闭，但是端口 8910 仍正常工作，并继续响应请求。

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)** > **部署 (Deployment)**。

步骤 2 在**部署节点 (Deployment Nodes)** 窗口中，选中要为其启用Cisco pxGrid 服务的节点旁的复选框，然后点击**编辑 (Edit)**。

步骤 3 点击**常规设置 (General Settings)** 选项卡， 启用 **pxGrid** 切换按钮。

步骤 4 点击**保存 (Save)**。

当从以前的版本升级时，系统可能会禁用**保存 (Save)** 选项。当浏览器缓存引用以前版本的Cisco ISE 中的旧文件时，就会发生这种情况。清除浏览器缓存以启用**保存 (Save)** 选项。

配置思科 pxGrid 设置

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 **管理 (Administration)** > **pxGrid服务 (pxGrid Services)** > **设置 (Settings)**。

步骤 2 根据您的需求选择以下选项：

- **自动审批新的基于证书的帐户 (Automatically approve new certificate-based accounts)**：选中此复选框可自动批准来自新Cisco pxGrid 客户端的连接请求。
- **允许创建基于密码的帐户 (Allow password based account creation)**：选中此复选框可为Cisco pxGrid 客户端启用基于用户名或密码的身份验证。如果启用此选项，则无法自动批准Cisco pxGrid 客户端。

  Cisco pxGrid 客户端可以通过 REST API 发送用户名，从而向Cisco pxGrid 控制器注册自身。在客户端注册时，Cisco pxGrid 控制器会为Cisco pxGrid 客户端生成密码。管理员可以批准或拒绝连接请求。

步骤 3 点击**保存 (Save)**。

您可以使用Cisco pxGrid **设置 (Settings)** 窗口上的**测试 (Test)** 选项对Cisco pxGrid 节点执行运行状况检查。在 pxgrid 或 pxgrid-test.log 文件中可以查看详细信息。

生成思科 pxGrid 证书

开始之前

某些版本的Cisco ISE 具有使用 NetscapeCertType 的Cisco pxGrid 证书。建议您生成新证书。

- 要执行以下任务，您必须是超级管理员或系统管理员。
- 必须从主 PAN 生成Cisco pxGrid 证书。
- 如果Cisco pxGrid 证书使用了使用者替代名称 (SAN) 扩展名，请确保将使用者身份的 FQDN 包含为 DNS 名称条目。

- 创建使用数字签名用法的证书模板，并使用该模板生成新的Cisco pxGrid 证书。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **pxGrid 服务 (pxGrid Services)** > **客户端管理 (Client Management)** > **证书 (Certificates)**。

步骤 2 从**我想 (I want to)** 下拉列表中选择以下选项之一：

- **生成无证书签名请求的单个证书 (Generate a single certificate without a certificate signing request)**：如果选择此选项，则必须输入通用名称 (CN)。
- **生成单个证书（带证书签名请求）Generate a single certificate (with a certificate signing request)**：如果选择此选项，则必须输入证书签名请求详细信息。
- **生成批量证书 (Generate bulk certificates)**：可以上传包含所需详细信息的 CSV 文件。
- **下载根证书链 (Download Root Certificate Chain)**：下载根证书，并将其添加到受信任证书存储区。必须指定主机名和证书的下载格式。

步骤 3 **通用名称 (CN) (Common Name (CN))**：（如果选择**生成单个证书（无证书签名请求）(Generate a single certificate (without a certificate signing request))** 选项，则必须选择此选项。）输入 pxGrid 客户端的 FQDN。

步骤 4 **证书签名请求详细信息 (Certificate Signing Request Details)**：（如果选择**生成单个证书（无证书签名请求）(Generate a single certificate (without a certificate signing request))** 选项，则必须选择此选项。）输入完整的证书签名请求详细信息。

步骤 5 **说明**：（可选）可以输入此证书的说明。

步骤 6 **证书模板 (Certificate Template)**：点击 **pxGrig_Certificate_Template** 链接可下载证书模板，并根据您的要求进行编辑。

步骤 7 **使用者备用名称 (SAN) (Subject Alternative Name (SAN))**：可以添加多个 SAN。可提供以下选项：

- **IP 地址 (IP address)**：输入要与证书关联的Cisco pxGrid 客户端的 IP 地址。
- **FQDN**：输入 pxGrid 客户端的完全限定域名。

注释　如果选定**生成批量证书 (Generate Bulk Certificate)** 选项，则不会显示此字段。

步骤 8 从**证书下载格式 (Certificate Download Format)** 下拉列表中选择以下选项之一：

- **加强隐私电子邮件 (PEM) 格式的证书和 PKCS8 PEM 格式的密钥（包括证书链）(Certificate in Private Enhanced Electronic Mail (PEM) format, key in PKCS8 PEM format (including certificate chain))**：根证书、CA 中间证书和终端实体证书均采用 PEM 格式。PEM 格式的证书是采用 BASE64 编码的 ASCII 文件。每个证书的开头采用“-------证书开始 (BEGIN CERTIFICATE) -----”标签，结尾采用“-----证书结束 (END CERTIFICATE) ----”标签。终端实体的私钥使用 PKCS* PEM 存储。其开头采用“-----加密私钥开始 (BEGIN ENCRYPTED PRIVATE KEY) ----”标签，结尾采用“-----加密私钥结束 (END ENCRYPTED PRIVATE KEY) ----”标签。
- **PKCS12 格式（包括证书链；证书链和密钥的文件）(PKCS12 format (including certificate chain; one file for both the certificate chain and key))**：CA 根证书、CA 中间证书以及终端实体的证书和私钥存储在一个加密文件时，所采用的二进制格式。

步骤 9 **证书密码 (Certificate Password)**：输入证书的密码，并在下一字段中再次输入以确认密码。

步骤 10 点击**创建 (Create)**。

您创建的证书在Cisco ISE 的**已颁发证书 (Issued Certificates)** 窗口中可见。要查看此处窗口，请点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **证书 (Certificates)** > **证书颁发机构 (Certificate Authority)** > **已颁发证书 (Issued Certificates)**。证书也会下载到浏览器的“下载”目录中。

注释 从Cisco ISE 2.4 补丁 13 开始，pxGrid 服务的证书要求变得更加严格。如果您使用Cisco ISE 默认自签名证书作为 pxGrid 证书，则Cisco ISE 可能会在应用Cisco ISE 2.4 补丁 13 或更高版本后拒绝此证书。这是因为此证书的旧版本具有指定为 **SSL 服务器 (SSL Server)** 的 **Netscape 证书类型 (Netscape Cert Type)** 扩展，此扩展现在会失败（现在还需要客户端证书）。

任何具有不合规证书的客户端都无法与Cisco ISE 集成。使用内部 CA 颁发的证书或生成具有正确使用扩展名的新证书：

- 证书中的**密钥使用 (Key Usage)** 扩展必须包含**数字签名 (Digital Signature)** 和**密钥加密 (Key Encipherment)** 字段。
- 证书中的**扩展密钥使用 (Extended Key Usage)** 扩展必须包含**客户端身份验证 (Client Authentication)** 和**服务器身份验证 (Server Authentication)** 字段。
- 不需要 **Netscape 证书类型 (Netscape Certificate Type)** 扩展。如果要包含此扩展，则必须在扩展中同时添加 **SSL 客户端 (SSL Client)** 和 **SSL 服务器 (SSL Server)**。
- 如果使用的是自签名证书，则**基本约束 CA (Basic Constraints CA)** 字段必须设置为 True，并且**密钥使用 (Key Usage)** 扩展必须包含**密钥证书签名 (Key Cert Sign)** 字段。

Cisco pxGrid 客户端的控制权限

您可以创建 Cisco pxGrid 授权规则来控制 Cisco pxGrid 客户端的权限。使用这些规则可控制提供给 Cisco pxGrid 客户端的服务。

您可以创建不同类型的组，并将提供给 Cisco pxGrid 客户端的服务映射到这些组。使用**客户端管理 (Client Management)** 窗口中的**组 (Groups)** 选项可添加新组。您可以在**客户端管理 (Client Management)** > **策略 (Policies)** 窗口中查看使用预定义组（如 EPS 和 ANC）的预定义授权规则。请注意，只能更新预定义规则的**自定义操作 (Custom Operations)** 字段。

要为 pxGrid 客户端创建授权规则，请执行以下操作：

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **pxGrid 服务 (pxGrid Services)** > **客户端管理 (Client Management)** > **策略 (Policy)**。

步骤 2 从**服务 (Service)** 下拉列表中，选择以下选项之一：

- **com.cisco.ise.pubsub**
- **com.cisco.ise.config.anc**
- **com.cisco.ise.config.profiler**
- **com.cisco.ise.config.trustsec**
- **com.cisco.ise.service**
- **com.cisco.ise.system**
- **com.cisco.ise.radius**
- **com.cisco.ise.sxp**
- **com.cisco.ise.trustsec**
- **com.cisco.ise.mdm**

步骤 3 从**操作 (Operation)** 下拉列表中，选择以下选项之一：

- **<ANY>**
- **publish**
- **publish /topic/com.cisco.ise.session**
- **publish /topic/com.cisco.ise.session.group**
- **publish /topic/com.cisco.ise.anc**
- **<CUSTOM>**

  注释　　如果选择此选项，可以指定自定义操作。

步骤 4 从**组 (Groups)** 下拉列表中，选择要映射到此服务的组。

预定义组（如 EPS 和 ANC）和手动添加的组列在此下拉列表中。

查看部署中的节点

在**部署节点 (Deployment Nodes)** 窗口，可以查看部署中的所有思科 ISE 节点（主节点和辅助节点）。

步骤 1 登录主Cisco ISE 管理员门户。

步骤 2 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **部署 (Deployment)**。

步骤 3 点击左侧导航窗格中的 **Deployment**。

列出部署中的所有Cisco ISE 节点。

从 MnT 节点下载终端统计数据

您可以从MnT节点下载联网终端的统计数据。关键性能指标(KPM)，其中包括负载、CPU使用率、身份验证流量数据，您使用这些指标监控并排除网络中的问题。在Cisco ISE 命令行界面 (CLI) 中使用 **application configure ise** 命令并选择选项 12 或 13 来分别下载每日 KPM 统计信息或过去八周的 KPM 统计信息。

此命令的输出提供以下终端数据：

- 网络中的终端总数
- 成功建立连接的终端数量
- 身份验证失败的终端数量
- 每日连接的新终端总数
- 每日连接的终端总数

输出还包括时间戳详情、通过部署中各策略服务节点 (PSN) 连接的终端总数、终端总数、活动的终端、负载以及身份验证流量详情。

请参阅思科身份服务引擎 *CLI* 参考指南查看有关此命令的更多信息。

数据库崩溃或文件损坏问题

如果 Oracle 数据库文件因断电或其他原因导致数据丢失而损坏，则Cisco ISE 可能会崩溃。根据具体的事件，按照以下步骤恢复丢失的数据。

- 如果部署中发生 PAN 损坏，则应将辅助 PAN 升级为主 PAN。
- 如果由于小型部署或任何其他原因导致无法升级辅助 PAN，请恢复最新的可用备份。
- 如果 PSN 损坏，请按照以下步骤取消注册、重置配置并重新注册节点。
- 如果是独立设备，请恢复最新的可用备份。

注释 定期从独立设备中获取备份，以避免丢失最新的配置更改。

设备的监控配置

MnT 节点会接收网络中设备的数据，并用于填充控制板显示内容。要启用 MnT 节点与网络设备之间的通信，必须正确配置交换机和 NAD。

同步主要和辅助思科 ISE 节点

只能通过主 PAN 对Cisco ISE 的配置进行更改。系统会将配置更改复制到所有辅助节点。如果出于某些原因未能正常执行复制，则可以手动同步辅助 PAN 与主 PAN。

步骤 1 登录到主 PAN。

步骤 2 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **部署 (Deployment)**。

步骤 3 选中要与主 PAN 同步的节点旁边的复选框，然后点击**同步 (Syncup)** 强制执行数据库完全复制。

更改节点角色和服务

您可以编辑Cisco ISE 节点配置来更改在节点上运行的角色和服务。

开始之前

- 当启用或禁用在PSN上运行的任何服务或对PSN进行任何更改时，将会重新启动运行这些服务的应用服务器进程。这些服务重新启动时，预计会有延迟。
- 由于服务重新启动时的这一延迟，可能会启动自动故障转移（如果在部署中已启用）。要避免此问题，请确保关闭自动故障转移配置。

步骤 1 登录到主 PAN。

步骤 2 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **部署 (Deployment)**。

步骤 3 选中要更改其角色或服务的节点旁边的复选框，然后点击**编辑 (Edit)**。

步骤 4 选择所需的角色和服务。

步骤 5 点击**保存 (Save)**。

步骤 6 验证在主 PAN 上是否收到警报，以确认角色或服务更改。如果未成功保存角色或服务更改，则不会生成警报。

在思科 ISE 中修改节点的影响

在Cisco ISE 中对节点进行以下任一更改后，节点将重新启动，这会导致延迟：

- 注册节点（独立节点至辅助节点）
- 注销节点（辅助节点至独立节点）
- 将主要节点更改为独立节点（如果未向其注册任何其他节点；主要节点至独立节点）
- 升级管理节点（辅助节点升级为主节点）
- 更改角色（当向某个节点分配策略服务或监控角色或从该节点删除角色时）
- 修改策略服务节点中的服务（启用或禁用会话和分析器服务）
- 恢复主要节点上的备份，然后系统会触发一项同步操作，将数据从主要节点复制到辅助节点

创建策略服务节点组

当两个或多个策略服务节点 (PSNs) 连接到同一高速局域网 (LAN) 时，建议您将他们放入同一个节点组中。通过保留较少的本地组重要属性以及减少复制到网络中远程节点的信息，此设计对终端分析数据复制进行了优化。节点组成员还检查对等组成员的可用性。如果该组检测到某成员发生故障，则尝试重置和恢复失败节点上所有 URL 重定向的会话。

注释 我们建议您将同一个本地网络中的所有 PSN 放入同一个节点组。要加入同一个节点组，PSN 不需要成为负载均衡集群的一部分。但是，负载均衡集群中的每个本地 PSN 通常应该属于同一个节点组。

注释 节点组用于对实施 URL 重定向（终端安全评估服务、访客服务和 MDM）的会话执行 PSN 故障转移。

在您将 PSN 作为成员添加进某个节点组之前，您必须首先创建该节点组。您可以从管理员门户的“部署”(Deployment) 页面创建、编辑和删除 PSN 组。

开始之前

节点组成员可以通过 TCP/7800 通信。

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)** > **部署 (Deployment)**。

步骤 2 点击左侧导航窗格顶部的**设置 (Settings)** 图标。

步骤 3 点击**创建节点组 (Create Node Group)**。

步骤 4 输入节点组的唯一名称。

步骤 5 （可选）输入节点组的说明。

步骤 6 （可选）选中**启用 MAR 缓存分布 (Enable MAR Cache Distribution)** 复选框并填写其他选项。在启用此选项之前，请确保在 **Active Directory** 窗口中启用 MAR。

步骤 7 点击**提交 (Submit)** 保存节点组。

保存节点组之后，节点组应显示在左侧的导航窗格中。如果节点组未显示在左侧窗格中，则可能已隐藏。点击导航窗格中的**展开 (Expand)** 按钮可查看隐藏的对象。

下一步做什么

将节点添加到节点组。从**策略服务 (Policy Service)** 区域的**在节点组中包含节点 (Include node in node group)** 下拉列表中选择节点组，对节点进行编辑。

从部署中删除节点

要从部署中删除节点，您必须注销该节点。已注销的节点会成为独立Cisco ISE 节点。

它保留其从主 PAN 接收的最新配置，并且承担独立节点的默认角色，包括“管理”(Administration)、“策略服务”(Policy Service) 和“监控”(Monitoring)。如果注销 MnT 节点，则此节点将不再是系统日志目标。

注销主 PSN 时，终端数据将丢失。如果您希望 PSN 在成为独立节点后保留终端数据，可以执行以下任一操作：

- 从主 PAN 获取备份，并在 PSN 成为独立节点时在其上恢复此数据备份。
- 将 PSN 的角色更改为“管理”(Administration)（辅助 PAN），从管理员门户的**部署 (Deployment)** 窗口同步数据，然后注销节点。此节点现在拥有所有数据。然后可以将辅助 PAN 添加至现有部署。

可以从主 PAN 的**部署 (Deployment)** 窗口查看这些更改。但是，预计更改会延迟 5 分钟生效并显示在**部署 (Deployment)** 窗口上。

开始之前

在从部署中删除任何辅助节点之前，请对Cisco ISE 配置执行备份，稍后可在需要时恢复该备份。

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)** > **部署 (Deployment)**。

步骤 2 选择要删除的辅助节点旁边的复选框，然后点击**注销 (Deregister)**。

步骤 3 点击**确定 (OK)**。

步骤 4 验证在主PAN上是否收到警报，以确认辅助节点成功注销。如果从主PAN注销辅助节点失败，则不会生成警报。

关闭思科 ISE 节点

从Cisco ISE 命令行界面 (CLI) 发出 `halt` 命令之前，建议您停止Cisco ISE 应用服务，并确保它不执行任何备份、恢复、安装、升级或删除操作。如果在Cisco ISE 执行上述任一操作时发出 halt 命令，您将会收到以下其中一条警告消息：

```
WARNING: A backup or restore is currently in progress! Continue with halt?
```

```
WARNING: An install/upgrade/remove is currently in progress! Continue with halt?
```

在使用 halt 命令时，如果系统没有运行任何进程，或如果您输入`是 (Yes)`来回应显示的警告消息，则必须回答以下问题：

```
Do you want to save the current configuration?
```

如果输入`是 (Yes)`保存现有Cisco ISE 配置，系统将显示以下消息：

```
Saved the running configuration to startup successfully.
```

注释 建议您在重新引导设备之前停止应用进程。

也可以重新引导Cisco ISE。有关详细信息，请参阅《思科身份识别服务引擎 CLI 参考指南》

更改独立思科 ISE 节点的主机名或 IP 地址

可以更改独立Cisco ISE 节点的主机名、IP 地址或域名。不能使用 `localhost` 作为节点的主机名。

开始之前

如果Cisco ISE 节点是分布式部署的一部分，必须将其从部署中删除并确保该节点为独立节点。

步骤 1 从Cisco ISE CLI 使用 **hostname**、**ip address** 或 **ip domain-name** 命令更改Cisco ISE 节点的主机名或 IP 地址。

步骤 2 从Cisco ISE CLI 使用 **application stop ise** 命令重置Cisco ISE 应用配置以重启所有服务。

步骤 3 如果Cisco ISE 节点为分布式部署的一部分，则将其注册到主 PAN。

注释 如果您在注册Cisco ISE 节点时使用主机名，注册的独立节点的完全限定域名 (FQDN) 必须可以从主 PAN 进行 DNS 解析，例如 FQDN 可以为 *abc.xyz.com*。否则，节点注册将失败。必须输入作为 DNS 服务器上分布式部署一部分的Cisco ISE 节点的 IP 地址和 FQDN。

将Cisco ISE注册为辅助节点后，主PAN会将IP地址、主机名或域名中的更改复制到您的分布式部署中另一个Cisco ISE 节点。