思科 ISE 的部署

思科 ISE 部署术语

以下是讨论思科 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：节点是运行思科 ISE 软件的单个实例。思科 ISE 可用作设备，也可用作能在 VMware 上运行的软件。运行思科 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。思科ISE节点可以承担以下任意角色：。InlinePosture角色需要使用专用思科 ISE 节点。通过管理员门户可用的菜单选项取决于思科 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

思科 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Inline Posture 节点除外均可承担管理、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)
- 用于高可用性的一对 Inline Posture 节点

配置思科 ISE 节点

在安装思科 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。您必须登录思科 ISE 节点的 Admin 门户进行配置。您无法编辑独立思科 ISE 节点的角色或服务。但是，您可以编辑主要和辅助思科 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。

我们建议不要更改生产中在思科 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

您应该对如何在思科 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 依次选择**管理 (Administration)** > **系统 (System)** > **部署 (Deployment)**。

步骤 2 选中您要配置的思科 ISE 节点旁边的复选框，然后点击 **Edit**。

步骤 3 按照需要输入相应值，然后单击**保存 (Save)**。

配置主策略管理节点

要设置分布式部署，必须首先将思科 ISE 节点配置为主 PAN。

步骤 1 依次选择**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 **Edit**。

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

步骤 4 点击 **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

您可以将思科 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。在完成数据复制后，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。有关更多详细信息，请参阅创建策略服务节点组，第 34 页。

步骤 1 登录到主 PAN。

步骤 2 依次选择**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 GUI 的管理员凭证。

步骤 6 单击**下一步**。

主 PAN 会在节点注册后尝试建立 TLS 通信（首次）。

- 如果节点使用受信任的证书，则可以继续执行第 7 步。
- 如果节点使用了不受信任的自签证书，则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。点击**导入证书并继续 (Import Certificate and Proceed)** 选项以信任此证书并继续注册。思科 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，请选中相应PAN旁边的**信任 ISE 内部的身份验证 (Trust for Authentication within ISE)** 复选框，以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，表示在设置证书信任之前无法继续注册。

步骤 7 选中复选框，以便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）。在思科 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，并计划使用内部思科 ISE CA 服务，则必须备份主 PAN 的思科 ISE CA 证书和密钥，并在辅助 PAN 恢复这些证书和密钥。

支持多种部署方案

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

思科 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。思科 ISE 具有不同的可配置角色、服务和职责，允许创建和

应用网络中所需的思科 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思科 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思科 ISE 节点。每个角色在整体网络策略管理拓扑中发挥不同但很重要的作用。使用管理角色安装思科 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 平台还可以部署为“内联终端安全评估”(Inline Posture) 节点，以便在用户通过无线控制器或 VPN 集中器（它们不支持便于思科 ISE 策略管理所需的功能）访问网络时进行策略实施并执行授权更改 (CoA) 请求。

思科 ISE 分布式部署

具有不止一个思科 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思科 ISE 节点。在思科 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。部署中的每个思科 ISE 节点都可以担任其中任何一个角色 - 管理、策略服务和监控。Inline Posture 节点由于具有专用性质而不能承担任何其他角色。Inline Posture 节点必须为专用节点。

思科 ISE 部署设置

在所有节点上安装思科 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。

所有思科 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思科 ISE 节点

当您将思科 ISE 节点注册为辅助节点时，思科 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思科 ISE 配置数据的过程。复制可确保部署中的所有思科 ISE 节点的配置数据一致。中点击相应的单选按钮，以便启用或禁用在思科 ISE 部署中的所有节点之间复制动态发现的终端：

首次将思科 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思科 ISE 节点保持同步。在思科 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。当您将思科 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。节点状态变为绿色后，思科 ISE 应用服务器需要大约 5 分钟时间来重新启动和运行，才能完成辅助 ISE 节点配置。

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。

注释 无法取消注册主 PAN。

思科 ISE 部署中的节点状态

表 *1:* 思科 *ISE* 节点状态

Node Status	说明	准则
互联	节点已连接，复制工作正常。	-
复制已停止	节点已连接，但复制已停止。可在端口 443 和 12001 上访问该节点。 这是一种临时状态，在解决基本复制问题后会发生变化。	根本问题可能会自行解决。否则，请登录到思科 ISE GUI 并从**部署 (Deployment)** 窗口执行手动同步。
节点不可达	无法在端口 443 上访问节点，但复制工作正常。	当根本问题解决后，节点可能会自行恢复。否则，请登录到思科 ISE GUI 并从**部署 (Deployment)** 窗口执行手动同步。
已断开	节点不可访问，复制已停止。	如果节点关闭超过五分钟，则会设置此状态。 当根本问题解决后，节点可能会自行恢复。否则，请登录到思科 ISE GUI 并从**部署 (Deployment)** 窗口执行手动同步。
注册失败	节点注册失败。	执行手动同步。取消注册并重新注册受影响的思科 ISE 节点。

Node Status	说明	准则
进行中	正在进行节点注册或手动同步。 目前，正在进行状态的超时值为 300 分钟，在此之后状态将更改为： • 如果注册或手动同步成功，则连接成功。 • 如果节点注册失败，则注册失败。 • 如果手动同步失败，则不同步。	如果状态更改为“已连接”(Connected)，则无需执行任何操作。如果它变成“注册失败”(Registration Failed) 或“不同步”(Not in Sync)，请检查相应的行并执行必要的操作。
不同步。	节点不同步。	执行手动同步。取消注册并重新注册受影响的思科 ISE 节点。
Upgrading	节点正在升级。	-

设置分布式部署的规定

在分布式环境中设置思科 ISE 之前，请仔细阅读以下声明：

- 选择思科 ISE 服务器节点类型或内联终端安全评估节点。对于管理、策略服务和监控功能，必须选择思科 ISE 节点。对于 Inline Posture 服务，必须选择 Inline Posture 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，您必须在设置每个节点时提供同一 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。
- 安装思科 ISE 时配置思科 ISE 管理员密码。以前的思科 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 DNS 服务器。在 DNS 服务器中输入分布式部署中包含的所有思科 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思科 ISE 节点配置正向和反向 DNS 查找。否则，在注册并重新启动思科 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 注销辅助思科 ISE 节点以从中卸载思科 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思科 ISE。

- 在将其他节点添加到部署之前，在思科 ISE 主 PAN 上启用**内部 CA 设置 (Internal CA Settings)**，以确保思科 ISE 证书服务按预期运行。要启用内部 CA 设置，选择**管理 (Administration)** > **系统 (System)** > **证书 (Certificates)** > **证书颁发机构 (Certificate Authority)** > **内部 CA 设置 (Internal CA Settings)**。
- 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，通配符证书会被复制到新节点。
- 在将思科 ISE 部署配置为支持思科 TrustSec 时，或者在思科 ISE 与 Cisco Catalyst Center 集成时，请勿将 PSN 配置为仅 SXP。SXP 是思科 TrustSec 和非思科 TrustSec 设备之间的接口。SXP 不与支持思科 TrustSec 的网络设备通信。
- 确保主节点和辅助节点的数据库密码相同。如果在节点安装过程中以不同方式设置这些密码，则您可以使用以下命令对其进行修改：
  - **application reset-passwd ise internal-database-admin**
  - **application reset-passwd ise internal-database-user**

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思科 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思科 ISE 节点上可用的菜单选项。

表 *2:* 思科 *ISE* 节点和可用的菜单选项

思科 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。 **注释** 必须直接在各个节点上进行服务器证书操作。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。

思科 ISE 节点	可用的菜单选项
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。
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)** 窗口配置思科 ISE（PAN、PSN 和 MnT）节点和内联终端安全评估节点并设置部署。

部署节点列表窗口

表 *3:* 部署节点列表

字段名称	使用指南
主机名	显示节点的主机名。
Node Type	显示节点类型。 它可以是下列类型之一： • 思科 ISE（PAN、PSN、Mnt）节点 • Inline Posture 节点
相关角色	（只有在节点类型为思科 ISE 时才显示）列出思科 ISE 节点承担的角色，例如管理 (Administration)、策略服务 (Policy Service)、监控 (Monitoring) 或 pxGrid。 例如，**管理 (Administration)**、**策略服务 (Policy Service)**、**监控 (Monitoring)** 或 **pxGrid**。
角色	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	（只有在启用策略服务角色时才显示）列出此思科 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
Node Status	指示部署中每个思科 ISE 节点的数据复制状态： • 绿色（已连接）：表示部署中已注册的思科 ISE 节点与主 PAN 处于同步状态。 • 红色（断开）：表示思科 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 新注册了新思科 ISE 节点、您已执行手动同步操作或思科 ISE 节点与主 PAN 不同步。 有关详细信息，请点击**节点状态 (Node Status)** 列中每个思科 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，第 3 页

常规节点设置

下表说明思科 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。此窗口的导航路径为：**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 *4:* 常规节点设置

字段名称	使用指南
主机名	显示思科 ISE 节点的主机名。
FQDN	显示思科 ISE 节点的完全限定域名，例如 ise1.cisco.com。
IP 地址	显示思科 ISE 节点的 IP 地址。
Node Type	显示节点类型。可以为以下任一项：身份服务引擎 (ISE)、Inline Posture 节点
相关角色	

字段名称	使用指南
管理	如果思科 ISE 节点承担管理角色，请选中此复选框。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。个人可以选择其中一种值 - **独立 (Standalone)**、**主要 (Primary)** 或**辅助 (Secondary)**。 **设为主要 (Make Primary)** - 选择它可使该节点成为主思科 ISE 节点。在部署中您只能有一个主要思科 ISE 节点。当您将此节点设置为主要节点之后，此窗口中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。点击**设为独立 (Make Standalone)** 按钮以使您的主要节点成为独立节点。
Monitoring	如果要思科 ISE 节点承担监控角色并充当日志收集器，请选中此复选框。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 平台上将思科 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思科 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，思科 ISE 还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：**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	选中此复选框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某个组，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。 虽然单个 NAD 可以配置多个思科 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。有关详细信息，请参阅创建策略服务节点组，第 34 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。
pxGrid	选中此复选框可启用 pxGrid 角色。思科 pxGrid 用于将来自思科 ISE 会话目录区分上下文的信息共享给其他策略网络系统，如思科自适应安全设备 (ASA)。此pxGrid框架还可用于在节点之间交换策略和配置数据，例如在思科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思科 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 19 页
策略服务节点，第 20 页
监控节点，第 21 页
思科 pxGrid 节点，第 25 页
同步主要和辅助思科 ISE 节点，第 33 页
创建策略服务节点组，第 34 页

部署思科 pxGrid 节点，第 27 页
更改节点角色和服务，第 33 页
配置用于自动故障切换的监控节点，第 24 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。此窗口的导航路径为： **管理 (Administration)** > **系统 (System)** > **部署 (Deployment)** > **ISE 节点 (ISE Node)** > **编辑 (Edit)** > **分析配置 (Profiling Configuration)**。

表 *5:* 分析节点的设置

字段名称	使用指南
NetFlow	选中此复选框可针对承担策略服务角色的每个思科 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)**：选择思科 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	选中此复选框可针对承担策略服务角色的每个思科 ISE 节点启用 DHCP，以便侦听来自 IP 帮助程序的 DHCP 数据包。为以下选项提供值： • **接口 (Interface)**：选择思科 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	选中此复选框可针对承担策略服务角色的每个思科 ISE 节点启用 DHCP，以便收集 DHCP 数据包。 • **接口 (Interface)**：选择思科 ISE 节点上的接口。
HTTP	选中此复选框可针对承担策略服务角色的每个思科 ISE 节点启用 HTTP，以便接收并解析 HTTP 数据包。 • **接口 (Interface)**：选择思科 ISE 节点上的接口。
RADIUS	选中此复选框可针对承担策略服务角色的每个思科 ISE 节点启用 RADIUS 服务器，以便收集 RADIUS 会话属性，以及来自已启用思科 IOS 传感器的设备的思科设备协议 (CDP) 和链路层发现协议 (LLDP) 属性。
Network Scan (NMAP)	选中此复选框可启用 NMAP 探测。

字段名称	使用指南
DNS	选中此复选框可针对承担策略服务角色的每个思科 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思科 ISE 节点上运行，您必须启用这些探测功能 - DHCP、DHCP SPAN、HTTP、RADIUS 或 SNMP。对于 DNS 查找，必须连同 DNS 探测功能一起启用这些探测功能之一。
SNMP Query	选中此复选框可针对承担策略服务角色的每个思科 ISE 节点启用 SNMP 查询，以便按照指定的间隔轮询网络设备。在**重试 (Retries)**、**超时 (Timeout)**、**事件超时 (Event Timeout)**（必填）和**说明 (Description)**（可选）字段中输入值。 注释　除配置 SNMP 查询探测功能之外，还必须在**管理 (Administration)** > **网络资源 (Network Resources)** > **网络设备 (Network Devices)** 中配置其他 SNMP 设置。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。
SNMP 陷阱	选中此复选框可针对承担策略服务角色的每个思科 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。提供或启用以下信息： • **链接陷阱查询 (Link Trap Query)**：选中此复选框可接收和解释通过 SNMP 陷阱接收的通知。 • **MAC 陷阱查询 (MAC Trap Query)**：选中此复选框可接收和解释通过 SNMP 陷阱接收的 MAC 通知。 • **接口 (Interface)**：选择思科 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	选中此复选框可扫描所定义的 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运行扫描。

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，并使思科 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。此页面的导航路径为**管理 (Administration)** > **系统 (System)** > **日志记录 (Logging)** > **远程日志记录目标 (Remote Logging Targets)**。单击**添加 (Add)**。

表 *6:* 远程日志记录目标设置

字段名称	使用指南
Name	为新的系统日志目标输入名称。
Target Type	从下拉列表中选择目标类型。默认值为 **UDP 系统日志 (UDP Syslog)**。
Description	输入新目标的简短说明。
IP 地址	输入将存储日志的目标计算机的 IP 地址或主机名。
端口	输入目标计算机的端口号。
Facility Code	从下拉列表中选择必须用于记录的系统日志设备代码。有效选项为 Local0 至 Local7。
Maximum Length	输入远程日志目标消息的最大长度。有效值为 200 至 1024 字节。
包括此目标的警报 (Include Alarms For This Target)	选中此复选框时，警报消息也会发送到远程服务器。
符合 RFC 3164 (Comply to RFC 3164)	选中此复选框时，即使使用了反斜线 (\)，发送到远程服务器的系统日志消息中的分隔符 (, ; { } \ \) 也不会转义。
Buffer Message When Server Down	当您从**目标类型 (Target Type)** 下拉列表中选择 **TCP 系统日志 (TCP Syslog)** 或**安全系统日志 (Secure Syslog)** 时，系统会显示此复选框。如果希望思科 ISE 在 TCP 系统日志目标或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。思科 ISE 会在与目标的连接恢复时重新尝试将消息发送到目标。连接恢复后，将按从最旧到最新的顺序发送消息。缓冲消息会始终在新消息之前发送。如果缓冲区已满，则会丢弃旧消息。
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。
Reconnect Timeout (Sec)	输入时间（以秒为单位），以便配置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。
Select CA Certificate	当您从**目标类型 (Target Type)** 下拉列表中选择 **安全系统日志 (Secure Syslog)** 时，系统会显示此下拉列表。从下拉列表中选择一个客户端证书。

字段名称	使用指南
Ignore Server Certificate Validation	当您从**目标类型 (Target Type)** 下拉列表中选择 **安全系统日志 (Secure Syslog)** 时，系统会显示此复选框。选中此复选框，以便让思科 ISE 忽略服务器证书身份验证并接受任何系统日志服务器。默认情况下，除非在禁用此复选框时系统处于 FIPS 模式，否则此选项设置为关闭。

相关主题

- 思科 日志记录机制
- 思科 ISE 系统日志
- 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

配置日志记录类别

下表介绍了可用于配置日志记录类别的字段。设置日志严重性级别，然后为日志记录类别的日志选择日志记录目标。此窗口的导航路径为**管理 (Administration)** > **系统 (System)** > **日志记录 (Logging)** > **日志记录类别 (Logging Categories)**。

单击想要查看的日志记录类别旁边的单选按钮，单击**编辑 (Edit)**。下表对日志记录类别的编辑窗口中显示的字段进行了说明。

表 *7:* 日志记录类别设置

字段名称	使用指南
Name	显示日志记录类别的名称。
Log Severity Level	对于某些日志记录类别，默认情况下会设置此值，并且您无法对其进行编辑。对于某些日志记录类别，您可以从下拉列表中选择以下严重性级别之一： • **严重 (FATAL)**：紧急级别。此级别意味着您无法使用思科 ISE，并且必须立即采取必要的操作。 • **错误 (ERROR)**：此级别表示严重错误情况。 • **警告 (WARN)**：此级别表示正常但值得注意的情况。这是会为很多日志记录类别设置的默认级别。 • **信息 (Info)**：此级别表示供参考的消息。 • **调试 (DEBUG)**：此级别表示诊断错误消息。
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。

字段名称	使用指南
目标	该区域允许您使用左侧和右侧图标在**可用 (Available)** 和**所选 (Selected)** 区域之间转移目标，从而更改类别的目标。 **可用 (Available)** 区域包含本地（预定义）和外部（用户定义）的现有日志记录目标。 **选定 (Selected)** 区域最初为空，然后会显示为该类别选择的目标。

相关主题

- 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

您可以通过这些部分来为管理员配置访问设置。

管理员密码策略设置

下表介绍了**密码策略 (Password Policy)** 选项卡中的字段，可以使用此选项卡来定义管理员密码应满足的条件。此窗口的导航路径为：**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 *8:* 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。
密码不可包含管理员姓名或其反向顺序的字符	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。
密码不可包含“cisco”或其反向顺序的字符	选中此复选框可限制使用字词“cisco”或其反向顺序的字符。
密码不可包含 _____ 或其反向顺序的字符	选中此复选框可限制使用您定义的任何字词或其反向顺序的字符。
密码不可包含连续重复四次或以上的字符	选中此复选框可限制使用连续重复四次或以上的字符。

字段名称	使用指南
必用字符	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
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.)
“不正确的登录尝试之后锁定或暂停帐户”(Lock or Suspend Account with Incorrect Login Attempts)	指定思科 ISE 在将管理员锁定以及暂停或禁用帐户凭证之前记录错误管理员密码的次数。 系统会向其帐户已锁定的管理员发送邮件。您可以输入自定义邮件补救消息。

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。此窗口的导航路径为：**管理 (Administration)** > **系统 (System)** > **管理员访问 (Admin Access)** > **设置 (Settings)** > **会话 (Session)**。

表 *9:* 会话超时和会话信息设置

字段名称	使用指南
会话超时	

字段名称	使用指南
会话空闲超时 (Session Idle Timeout)	输入思科 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	
失效 (Invalidate)	选中要终止的会话 ID 旁边的复选框，然后单击**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思科 ISE 节点，您可以在思科 ISE 上进行所有管理操作。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角色 - 独立角色、主角色或辅助角色。

管理节点的高可用性

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 自动故障切换，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思科 ISE 节点，以将其升级为主 PAN。

步骤 1 登录辅助 PAN GUI。

步骤 2

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

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

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。

步骤 4 点击保存 (Save)。

策略服务节点

策略服务节点 (PSN) 是承担策略服务角色的思科 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 URL 重定向会话（如有）。

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。这些节点还应配置为 RADIUS 服务器。

注释 虽然单个 NAD 可以配置多个思科 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。有关更多详细信息，请参阅创建策略服务节点组，第 34 页。

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 故障转移，终端安全评估处于待处理状态。

分布式部署中的 PSN 不会彼此共享其计算机访问限制 (MAR) 缓存。如果启用了思科 ISE 的 MAR 功能，当对客户端计算机进行身份验证的PSN发生故障时，该部署内的另一个PSN会处理用户身份验证。但是，用户身份验证会失败，因为第二个 PSN 的 MAR 缓存中没有主机身份验证信息。

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。

监控节点

承担监控角色的思科 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。

思科 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。这可以按照手动修改 MnT 角色中所述的程序来完成。

分布式设置中至少有一个节点应承担监控角色。我们建议您不要对同一个思科 ISE 节点启用监控和策略服务角色，而应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 和主监控节点访问监控 (Monitoring) 菜单。

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 登录到主 PAN GUI。

步骤 2 依次选择**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 单击**编辑**。

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

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 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。

步骤 6 点击**保存 (Save)**。

MnT 节点中的自动故障切换

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。

自动故障切换过程

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，则主节点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，请备份辅助节点并恢复数据以更新主节点。

MnT 节点主用备用对设置指南

您可以在思科ISE网络上指定两个MnT节点，然后将它们配置为主用备用对。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。
- 思科ISE控制面板是监控和故障排除的主要入口点。控制板上显示来自主监控节点的监控信息。如果主节点关闭，可以从辅助节点获得信息。
- 备份和清除 MnT 数据不在标准思科 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 节点升级为活动状态，则可以按照手动修改 MnT 角色中提供的程序或通过注销现有主 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。
- 如果思科 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，如本节所涵盖的主题所述：

备份和恢复监控数据库

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。在复制新的更改时，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 80%）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。

清除监控数据库指南

请遵循这些准则以优化 监控数据库磁盘的使用：

- 如果监控数据库磁盘使用率大于阈值设置的 80%，即总磁盘空间的 60%，则会生成严重警报，表示数据库大小即将超过分配的最大磁盘大小。如果磁盘使用率大于阈值设置的 90%，即总磁盘空间的 70%，则会生成另一个警报，表示数据库大小已超过分配的最大磁盘大小。

  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。此窗口的导航路径为**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（默认为总磁盘空间的 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 80%。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。

清除较旧的监控数据

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 依次选择 **Administration** > **System** > **Maintenance** > **Data Purging**。

步骤 2 以月为单位指定数据的保留期限。指定期限之前的所有数据都会清除。对于该选项，每月包括 30 天。三个月默认等于 90 天。

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 3 天，而且该值小于诊断表中的现有阈值（例如，默认值为 5 天），则根据在此页面中配置的值（3 天）清除数据。

步骤 3 点击 **Submit**。

步骤 4 查看数据清除审核报告，验证数据清除是否成功。

下一步做什么

思科 ISE 日志收集

执行按需备份

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，以避免思科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

- 在配置用于自动故障转移的 MnT 节点之前，必须将这些节点注册为思科 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。

注释 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。

在思科 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 依次选择**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，然后单击 **Edit**。

步骤 3 点击 **General Settings** 选项卡，然后从 **Role** 下拉列表中选择 **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 单击 **Save**。主节点和辅助节点都会重新启动。

思科 pxGrid 节点

可以使用思科 pxGrid 与其他网络系统（例如思科 ISE 生态系统合作伙伴系统）和其他思科平台共享思科 ISE 会话目录中的情景相关信息。pxGrid 框架也可用来在思科 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。思科 pxGrid 还允许第三方系统调通过自适应网络控制操作 来隔离用户和/或设备以应对网络或安全事件。可通过思科 TrustSec 主题将标签定义、值和说明等思科 TrustSec 信息从思科 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) 的终端配置文件从思科 ISE 传输到其他网络。思科 pxGrid 还支持标签和终端配置文件的批量下载。

在高可用性配置中，思科pxGrid服务器通过PAN在节点之间复制信息。当PAN关闭时，思科pxGrid服务器会停止处理客户端注册和订用。需要手动升级 PAN，以激活思科 pxGrid 服务器。

在具有 pxGrid 角色的活动思科节点上，这些进程会显示为**正在运行 (Running)**。在备用思科 pxGrid 节点上，它们会显示为**备用 (Standby)**。如果活动 pxGrid 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/pxgrid.state** 来验证思科 pxGrid 服务在此节点上是否处于备用状态。

启动面向辅助思科pxGrid节点的自动故障切换后，如果原始主思科pxGrid节点重新接入网络，则除非当前主节点关闭，否则原始主思科 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。我们建议客户端等待故障切换完成，然后再清除缓存数据，以防主思科 pxGrid 节点发生故障。

以下日志可用于思科 pxGrid 节点：

- pxgrid.log：通过状态变更通知。
- pxgrid-cm.log：显示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：显示与系统状态和身份验证相关的所有日志。
- pxgrid-pubsub.log：显示与发布者和用户事件相关的所有信息。

注释

注释 可以使用 Base 许可证启用思科 pxGrid，但必须使用 Plus 许可证才能启用思科 pxGrid 角色。

注释

思科 pxGrid 客户端和功能管理

使用 Cisco pxGrid 服务之前，连接到思科 ISE 的客户端必须注册并获得帐户审批。Cisco pxGrid 客户端使用 Cisco pxGrid SDK 中提供的 Cisco pxGrid 客户端库成为客户端。思科 ISE 同时支持自动和手动批准。客户端可以使用唯一名称和基于证书的相互身份验证登录Cisco pxGrid。类似于交换机上的 AAA 设置，客户端可以连接已配置的 Cisco pxGrid 服务器主机名或 IP 地址。

Cisco pxGrid 功能是指 Cisco pxGrid 上供客户端发布和订用的信息主题或信道。在思科 ISE 中，仅支持身份、自适应网络控制 (ANC) 和安全组访问 (SGA) 等功能。您可以启用或禁用功能。如果禁用这些功能，客户端就被取消订用。可通过发布、定向查询或批量下载查询，从发布方获取功能信息。

相关主题

生成思科 pxGrid 证书

启用 pxGrid 服务

开始之前

- 至少在一个节点上启用 pxGrid 角色，以查看思科 pxGrid 客户端发送的请求。
- 启用身份映射。有关详细信息，请参阅配置身份映射，第 30 页。

步骤 1 选择**管理 (Administration)** > **pxGrid 服务 (pxGrid Services)**。

步骤 2 选中该客户端旁边的复选框，然后点击**通过 (Approve)**。

步骤 3 要查看功能，请点击右上角的**根据功能查看 (View by Capabilities)**。

步骤 4 点击**刷新 (Refresh)** 查看最新的状态。

步骤 5 选择要启用的功能，并点击**启用 (Enable)**。

步骤 6 单击**刷新 (Refresh)** 查看最新的状态。

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思科 pxGrid 角色。

开始之前

- 所有节点都将 CA 证书用于思科 pxGrid 服务用途。如果在升级之前对思科 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。
- 如果您使用的是分布式部署或从思科 ISE 1.2 升级，则需要为证书启用 pxGrid 用途选项。您可以在**系统证书 (System Certificates)** 窗口中启用 pxGrid 用途选项。此窗口的导航路径为**管理 (Administration)** > **证书 (Certificates)** > **系统证书 (System Certificates)**。选择用于部署的证书，然后点击**编辑 (Edit)** 选中 **pxGrid：使用 pxGrid 控制器证书 (pxGrid: use certificate for the pxGrid Controller)** 复选框。
- 必须为 Websocket (pxGrid 2.0) 打开端口 8910，并为 XMPP (pxGrid V1.0) 打开端口 5222。如果在节点上禁用思科 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 选择**管理 (Administration)** > **系统 (System)** > **部署 (Deployment)**。

步骤 2 在**部署节点 (Deployment Nodes)** 窗口中，选中要为其启用思科 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， 选中 **pxGrid** 复选框。

步骤 4 点击 **Save**。

注释　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思科 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。

思科 pxGrid 实时日志

“实时日志”(Live Logs) 窗口会显示所有 pxGrid 管理事件。事件信息包括客户端和功能名称，以及事件类型和时间戳。

此窗口的导航路径为**管理 (Administration)** > **pxGrid 服务 (pxGrid Services)** > **实时日志 (Live Log)**。您还可以清除日志并重新同步或刷新列表。

pxGrid 操作和服务使用案例

请注意，创建新的 pxGrid 策略时，某些 pxGrid 操作仅适用于特定服务。

您可以在思科 ISE GUI 中找到以下 pxGrid 操作。

操作 <ANY>

当您使用 <ANY> 与服务和特定用户组进行操作时，与该服务相关的任何操作都只能由所选用户组中的用户访问。

请考虑以下示例。

服务：com.cisco.ise.session；操作：<ANY>；组：SessionUsers。

在本示例中，只有属于“SessionUsers”组的 pxGrid 客户端才能执行与会话主题相关的任何操作（例如订阅/获取操作）。

操作发布

仅当选择 com.cisco.ise.pubsub 作为服务时，所有与发布相关的操作才适用。您可以使用发布操作创建 pxGrid 策略，指定只有特定用户组的 pxGrid 客户端可以发布所选主题或可以发布所有主题。

操作 <Custom>

您可以使用 <Custom> 操作：指定操作下拉列表中未提供的操作。目前，pxGrid 支持以下操作，但并非所有操作都列在“操作”(Operation) 下拉列表中：

1. “sets”（适用于除 pubsub 之外的所有服务和主题）- 您可以使用此选项限制对执行 set 操作的 REST API 调用的访问。
2. “gets”（适用于除 pubsub 之外的所有服务和主题）- 您可以使用它来限制对执行 get 操作的 REST API 调用的访问。
3. “publish”后跟特定主题名称（仅适用于发布订阅服务）- 您可以使用此选项将访问权限限制为可以发布特定主题的用户。

例如，服务：com.cisco.ise.pubsub，操作：publish/topic/com.cisco.ise.session。

但是，某些具有相同操作、服务和主题的规则难以理解，因此必须加以避免。例如，服务：com.cisco.ise.session、操作：publish /topic/com.cisco.ise.session。

4. “subscribe”后跟主题名称（仅适用于发布订阅服务）- 您可以使用此选项将访问权限限制为可以订用特定主题的用户。

   例如，服务：com.cisco.ise.pubsub，操作：publish /topic/com.cisco.ise.session

ISE pxGrid 身份映射

使用身份映射，您可以监控通过域控制器 (DC) 而不是通过思科 ISE 进行身份验证的用户。在思科 ISE 不主动对用户进行网络访问身份验证的网络中，可以使用身份映射从 Active Directory (AD) 域控制器收集用户身份验证信息。此身份映射选项使用 MS WMI 接口连接至 Windows 系统并且从 Windows 事件消息查询日志。用户登录网络并通过 Active Directory 的身份验证之后，域控制器将生成一份事件日志，此日志中包含用户名和为此用户分配的 IP 地址。

即使思科 ISE 主动执行身份验证，也仍可以启用身份映射。在这种情况下，同一会话可能会被验证两次。运行数据有一个指示来源的会话属性。您可以转至 Operations > Authentications，然后点击 **Show Live Sessions** 以检查会话来源。

身份映射组件从域控制器检索用户登录情况并将其导入至思科 ISE 会话目录。因此，通过 Active Directory (AD) 身份验证的用户会显示在思科 ISE 实时会话视图中，而且可以使用思科 pxGrid 接口由第三方应用从会话目录进行查询。已知信息为用户名、IP 地址、 AD DC 主机名以及 AD DC NetBios 名称。

思科 ISE 仅扮演被动角色并且不执行身份验证。当身份映射处于活动状态时，思科 ISE 从 AD 收集登录信息并将数据纳入会话目录中。

主要特性

- 身份映射从思科 ISE 管理控制台进行配置。此配置包括以下设置：
  - 定义身份映射从中收集用户身份验证信息的所有 DC。这包括使用 *.csv 文件导入和导出 DC 列表。
  - DC 连接属性，例如身份验证安全协议（NTLMv1 或 NTLMv2）以及用户会话老化时间
  - 连接测试，用于验证 DC 是否设置正确以启动与身份映射的有效连接
- 身份映射报告。此报告提供关于身份映射组件的信息以进行故障排除。
- 身份映射调试日志
- 思科 ISE 会话目录保留所收集的用户信息，从而使客户可以从实时会话查看这些信息并且可以从 pxGrid 接口进行查询
- 使用 CLI 命令**show application status** 可以提供使用身份映射的节点的运行状态

- 支持高可用性

配置身份映射

ID 映射需要 ISE 中的配置，且 Active Directory 域服务器必须具有正确的补丁和配置。有关为 ISE 配置 Active Directory 域控制器的信息，请参阅 用于支持身份映射 的 Active Directory 要求

配置身份映射

ISE 必须能与 AD 域控制器 (DC) 建立连接。

开始之前

启用 pxGrid 服务以配置身份映射。选择**管理 (Administration)** > **系统 (System)** > **部署 (Deployment)** 以启用 pxGrid 服务。

要为身份映射添加一个新域控制器 (DC)，您需要该 DC 的登录凭证。

确保为 ISE 身份映射正确配置域控制器。

步骤 1 选择 **管理 (Administration)** > **pxGrid 身份映射 (pxGrid Identity Mapping)** > **AD 域控制器 (AD Domain Controller)**。

步骤 2 点击 **General Settings**。

步骤 3 系统将显示 Directory General Settings 弹出窗口。设置所需的值，然后点击 **Save**。

- **历史间隔 (History interval)** 是身份映射读取已发生的用户登录信息的时间。在启动或重新启动身份映射以跟进生成的事件时（事件生成于身份映射不可用期间），需要使用此项。
- **用户会话老化时间 (User session aging time)** 是用户可登录的时间量。身份映射会识别 DC 中的新用户登录事件，但是 DC 不会报告用户的注销时间。通过老化时间，思科 ISE 可以确定用户登录的时间间隔。
- 您可以选择 **NTLMv1** 或 **NTLMv2** 作为 ISE 与 DC 之间的通信协议。

步骤 4 点击**添加 (Add)**。

步骤 5 在 **General Settings** 部分，输入 DC 的 **Display Name**、**Domain FQDN** 和 **Host FQDN**。

步骤 6 在 **Credentials** 部分，输入 DC 的 Username 和 Password。

步骤 7 （可选） 通过点击**验证 DC 连接设置 (Verify DC Connection Settings)** 来测试到指定域的连接。

此测试可确保到 DC 的连接是正常的。但是它不会检查思科 ISE 是否可以在登录后获取用户信息。

步骤 8 点击**提交 (Submit)**。系统会显示更新的表（新定义的 DC 已经包含在 DC 列表中）。状态列指示 DC 的不同状态。

您也可以导入或导出 DC 列表。

注释 当导入时，您需要在模板中提供密码。因为文件包含密码，导入模板应被视为敏感信息。Export 选项不会导出密码。

过滤器身份映射

您可以根据用户名称或 IP 地址过滤某些用户。您可以按照需要添加很多过滤器。“OR”逻辑运算符适用于过滤器之间。如果在单个过滤器中同时指定两个字段，则在这两个字段之间使用“AND”逻辑运算符。监控实时会话显示映射过滤器未过滤掉的身份映射组件。

步骤 1 依次选择**管理 (Administration)** > **pxGrid 身份映射 (pxGrid Identity Mapping)** > **映射过滤器 (Mapping Filters)**。

步骤 2 点击**添加 (Add)**，输入您想要过滤的用户的用户名和 Ip 地址，然后点击**提交 (Submit)**。

步骤 3 要查看当前登录到监控会话目录中的未过滤用户，请选择**操作 (Operations)** > **身份验证 (Authentications)**。

Inline Posture 节点

Inline Posture 节点是守门节点，放在网络访问设备后面，例如网络上的无线 LAN 控制器 (WLC) 和 VPN 集线器。Inline Posture 节点在用户通过身份验证并被授予访问权限后实施访问策略，并且处理 WLC 或 VPN 无法满足的授权更改 (CoA) 请求。思科 ISE 允许您有两个 Inline Posture 节点，承担主要或辅助角色，提供高可用性。

Inline Posture 节点必须为专用节点。它必须仅用于内联状态服务，不能与其他思科 ISE 服务同时运行。同样，由于其服务的专业化性质，Inline Posture 节点无法承担任何角色。例如，它不能用作管理节点提供管理服务，不能用作策略服务节点提供网络访问、安全评估、配置文件和访客服务，也不能用作监控节点为思科 ISE 网络提供监控和故障排除服务。

思科 ISE 3495 平台不支持 Inline Posture 角色。确保在以下任何受支持的平台上安装 Inline Posture 角色：思科 ISE 3315、思科 ISE 3355、思科 ISE 3395 或思科 ISE 3415。

您不能访问 Inline Posture 节点的基于 Web 的用户界面，只能从 PAN 配置这些节点。

Inline Posture 节点的安装

您必须从 Cisco.com 下载 Inline Posture ISO (IPN ISO) 映像，然后将其安装到任何支持的平台上。然后，您必须通过命令行界面 (CLI) 配置证书。接下来，您可以从管理员门户注册此节点。

注释 不提供 版本的 Inline Posture ISO 映像。使用 1.2 IPN ISO 映像安装并设置 Inline Posture 节点。

安装和设置 Inline Posture 应用后，您必须先配置证书，然后才能注册 Inline Posture 节点。有关详细信息，请参阅《思科身份服务引擎硬件安装指南》。

注册 Inline Posture 节点

我们建议您在注册时确定节点的类型（思科 ISE 或 Inline Posture）。如果希望稍后更改节点类型，您必须将该节点从部署中注销，重启独立节点上的思科 ISE 并重新注册该节点。

开始之前

- 确保主节点的证书信任列表 (CTL) 具有适当的证书颁发机关 (CA) 证书，以验证要注册的辅助节点的 HTTPS 证书。
- 向主要节点注册辅助节点之后，如果您更改辅助节点上的 HTTPS 证书，您必须将相应的 CA 证书导入主要节点的 CTL。

步骤 1 登录到 PAN。

步骤 2 依次选择**管理 (Administration)** > **系统 (System)** > **部署 (Deployment)**。

步骤 3 点击左侧导航窗格中的 **Deployment**。

步骤 4 选择**注册 (Register)** > **注册 Inline Posture 节点 (Register an Inline Posture Node)** 以注册 Inline Posture 节点。

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 登录主思科 ISE 管理员门户。

步骤 2 选择**管理 (Administration)** > **系统 (System)** > **部署 (Deployment)**。

步骤 3 点击左侧导航窗格中的**部署 (Deployment)**。

列出部署中的所有思科 ISE 节点。

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，则思科 ISE 可能会崩溃。根据具体的事件，按照以下说明恢复丢失的数据。

- 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《Cisco 身份识别服务引擎 CLI 参考指南》中所述。
- 如果 PSN 损坏，请按照《Cisco 身份识别服务引擎 CLI 参考指南》中的说明，执行以下步骤取消注册、重置配置和注册。
- 如果是独立设备，请按照《Cisco 身份识别服务引擎 CLI 参考指南》中的说明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 对思科 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 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，然后单击**同步 (Syncup)** 强制执行数据库完全复制。

更改节点角色和服务

注释 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。

您可以编辑思科 ISE 节点配置来更改在节点上运行的角色和服务。

步骤 1 登录到主 PAN。

步骤 2 依次选择**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 **Edit**。

步骤 4 选择您要修改的角色和服务。

步骤 5 点击**保存**。

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

在思科 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）
- 取消注册节点（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

注释 当您将辅助管理节点提升为主 PAN 位置时，主节点将承担辅助角色。这会导致主节点和辅助节点重新启动，从而导致延迟。

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。

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。

注释 建议将所有 PSN 放在同一个本地网络中，并作为同一个节点组的一部分。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。

节点组成员可以通过 TCP/7800 通信。

在将 PSN 作为成员添加进某个节点组之前，您必须创建该节点组。您可以从管理员门户的**部署 (Deployment)** 窗口创建、编辑和删除 PSN 组。

步骤 1 依次选择**管理 (Administration)** > **系统 (System)** > **部署 (Deployment)**。

步骤 2 单击左侧导航窗格顶部的**设置 (Settings)** 图标。

步骤 3 点击**创建组 (Create Group)**。

步骤 4 输入节点组的唯一名称。

注释 建议不要配置名称为**无 (None)** 的节点组，否则可能会在节点注册时引起问题。

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。在选中此复选框之前，请确保在 **Active Directory** 窗口中启用 MAR。

步骤 7 点击 **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。

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

从部署中删除节点

要从部署中删除节点，您必须取消注册该节点。已取消注册的节点会成为独立思科 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) 或“监控”(Monitoring)。如果取消注册 MnT 节点，则此节点将不再是系统日志目标。

可以在主 PAN 的**部署 (Deployment)** 窗口中查看这些更改。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

在从部署中删除某个辅助节点之前，请对思科 ISE 配置执行备份，稍后可在需要时恢复该备份。

步骤 1 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**取消注册 (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取消注册。如果从主 PAN 取消注册辅助节点失败，则意味着不会生成警报。

关闭思科 ISE 节点

从思科 ISE CLI 发出 **halt** 命令之前，我们建议您停止思科 ISE 应用服务，并确保它不执行备份、恢复、安装、升级或删除操作。如果在思科 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 Yes 保存现有思科 ISE 配置，系统将显示以下消息：

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

注释 我们建议您在重新引导设备之前停止应用进程。

也可以重新引导思科 ISE。有关详细信息，请参阅思科身份服务引擎 CLI 参考指南。

更改独立思科 ISE 节点的主机名或 IP 地址

可以更改独立思科 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

如果思科 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 从思科 ISE CLI 使用 **hostname**、**ip address**、 或 **ip domain-name** 命令更改思科 ISE 节点的主机名或 IP 地址。

步骤 2 从思科 ISE CLI 使用 **application stop ise** 命令重置思科 ISE 应用配置以重新启动所有服务。

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

注释 如果您在注册思科 ISE 节点时使用主机名，则将要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思科 ISE 节点的 IP 地址和 FQDN。

将思科 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思科 ISE 节点。

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。