管理 ISE-PIC

管理 ISE-PIC 节点

添加或删除辅助节点，在节点之间同步数据，将辅助节点升级为主节点等。

思科 ISE-PIC 部署设置

在所有节点上安装思科 ISE-PIC 后，如《思科身份识别服务引擎硬件安装指南》所述，节点显示为独立状态。必须定义一个节点作为主管理节点 (PAN)，并将辅助节点注册到 PAN。

所有思科 ISE-PIC 系统和功能相关配置应当只在 PAN 上进行。在 PAN 上执行的配置更改将复制到部署中的辅助节点。从辅助节点可以执行的唯一操作是将辅助节点升级为 PAN。

在向 PAN 注册了辅助节点之后，在登录此辅助节点的管理员门户时，必须使用 PAN 的登录凭证。

将数据从主 ISE-PIC 节点复制到辅助节点

将思科 ISE 节点注册为辅助节点时，思科 ISE-PIC 会立即创建一个从主要节点到辅助节点的数据复制通道并开始执行复制进程。复制是从主节点向辅助节点共享思科 ISE-PIC 配置数据的过程。复制可确保作为您的部署组成部分的两个思科 ISE-PIC 节点中配置数据的一致性。

首次将 ISE-PIC 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-PIC节点保持同步。在思科ISE-PIC管理员门户的部署页面，可在“节点状态”(Node Status) 列查看复制的状态。将思科 ISE-PIC 节点注册为辅助节点或与 PAN 进行手动同步时，节点状态显示橙色图标，表示正在进行所请求的操作。操作完成后，节点状态变为绿色，表示辅助节点已与 PAN 同步。

在思科 ISE-PIC 中修改节点的影响

在思科 ISE-PIC 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）
- 升级节点（辅助节点升级为主节点）
- 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。

在部署中设置两个节点的指南

使用两个节点设置思科 ISE-PIC 之前，请仔细阅读以下声明。

- 为两个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。
- 安装思科 ISE-PIC 时配置思科 ISE-PIC 管理员密码。以前的思科 ISE-PIC 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 服务器中输入部署中包含的两个思科 ISE-PIC 节点的 IP 地址和完全限定域名 (FQDN)。否则，节点注册将失败。
- 从 DNS 服务器为高可用性部署中的两个思科 ISE-PIC 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-PIC 节点时可能会遇到部署相关问题。如果没有为两个节点配置反向 DNS 查找，则性能可能会降低。
- （可选）从 PAN 对辅助思科 ISE-PIC 节点取消注册以从中卸载思科 ISE-PIC。
- 确保即将注册为辅助节点的 PAN 和独立节点运行的是同一版本的思科 ISE-PIC。

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 ISE-PIC 节点（主节点和辅助节点）。

步骤 1 登录主思科 ISE-PIC 管理员门户。

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

列出部署中的所有思科 ISE 节点。

注册辅助思科 ISE-PIC 节点

注册辅助节点后，辅助节点的配置会被添加到主要节点的数据库中，而辅助节点上的应用服务器会重启。完成重新启动后，可以查看您在 PAN 的“部署”(Deployment) 页面中做出的所有配置更改。但是，您的更改会延迟 5 分钟生效并出现在部署 (Deployment) 页面中。

步骤 1 登录到 PAN。

步骤 2 选择**管理 (Administration)** > **部署 (Deployment)**。
如果部署中未注册辅助节点，则**添加辅助节点 (Add Secondary Node)** 部分将显示在页面底部。

步骤 3 在**添加辅助节点 (Add Secondary Node)** 部分中，输入辅助思科 ISE 节点的 DNS 可解析主机名。

如果在注册思科 ISE-PIC 节点时使用主机名，则准备注册的独立节点的完全限定域名 (FQDN) 必须从可 PAN 进行 DNS 解析，例如 *abc.xyz.com*。否则，节点注册将失败。您必须事先在 DNS 服务器中定义辅助节点的 IP 地址和 FQDN。

步骤 4 在“用户名”(Username) 和“密码” (Password) 字段中输入独立节点的基于 UI 的管理员凭证。

步骤 5 点击**保存 (Save)**。

思科 ISE-PIC 会与辅助节点通信，获取一些基本信息，例如主机名、默认网关等，并显示这些信息。

当辅助节点注册到部署时，节点将重新启动，这可能需要 5 分钟才能在“部署”(Deployment) 页面显示辅助节点信息。

成功注册辅助节点后，“部署”(Deployment) 页面会在**辅助节点 (Secondary Node)** 部分显示此节点的详细信息。

成功注册辅助节点后，您会在 PAN 上收到确认节点注册成功的警报。如果辅助节点与 PAN 注册失败，则不会生成警报。节点注册后，该节点上的应用服务器会重启。注册成功和数据库同步成功后，请输入主要管理节点的凭证登录到辅助节点的用户界面。

注释 除了部署中现有的主要节点外，当您成功注册新的节点时，不会显示新注册节点的对应警报。配置更改警报则会反应新注册节点的对应信息。您可以使用此信息确定新节点是否注册成功。

同步主要和辅助思科 ISE-PIC 节点

只能通过主 PAN 对思科ISE-PIC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)** > **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。

手动将辅助 PAN 升级为主 PAN

如果主 PAN 出现故障则必须手动将辅助 PAN 升级为新的主 PAN。

开始之前

确保已配置的第二个思科 ISE-PIC 节点，以将其升级为主 PAN。

步骤 1 登录辅助 PAN GUI。

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

步骤 3 点击**升级为主节点 (Promote to Primary)**。

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。

步骤 4 点击**保存 (Save)**。

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-PIC 节点。

取消注册节点时，终端数据将丢失。如果您希望节点在成为独立节点后保留终端数据，可以从主 PAN 获取备份，并在节点上恢复此数据备份。

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

要从部署中删除节点，您必须取消注册该节点。从 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。

在从部署中删除某个辅助节点之前，请对思科 ISE-PIC 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)** > **部署 (Deployment)**。

步骤 2 点击辅助节点详细信息旁的**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。

更改思科 ISE-PIC 节点的主机名或 IP 地址

可以更改独立思科 ISE-PIC 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-PIC 节点是两节点部署的一部分，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-PIC 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-PIC 应用配置以重新启动所有服务。

步骤 3 如果思科 ISE-PIC 节点为两节点部署的一部分，则将其注册到主 PAN。

注释 如果您在注册思科ISE-PIC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 服务器上部署一部分的思科ISE-PIC节点的 IP 地址和 FQDN。

将思科 ISE-PIC 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-PIC 节点。

更换思科 ISE-PIC 设备硬件

仅应在思科 ISE-PIC 设备硬件出现问题时更换硬件。对于任何软件问题，可以重新映像该设备并重新安装思科 ISE-PIC 软件。

步骤 1 在新的节点上重新映像或重新安装思科 ISE-PIC 软件。

步骤 2 借助 UDI 获取主要和辅助 PAN 的许可证，并安装到主 PAN 上。

步骤 3 恢复所更换的主 PAN 上的备份。

恢复脚本将尝试同步辅助PAN上的数据，但辅助PAN现已成为独立节点，同步将会失败。将数据设置为在主PAN上进行备份的时间。

步骤 4 通过主 PAN 将新节点注册为辅助服务器。

管理 ISE-PIC 安装

安装补丁、运行备份或实施系统恢复。

安装软件补丁

步骤 1 选择**管理 (Administration)** > **维护 (Maintenance)** > **补丁管理 (Patch Management)**，然后点击**安装 (Install)**。

步骤 2 点击**浏览 (Browse)**，然后选择已从 Cisco.com 下载的补丁。

步骤 3 点击**安装 (Install)** 安装补丁。

在 PAN 上安装补丁后，思科 ISE-PIC 会将您注销，您必须等待几分钟后才能再次登录。

注释　安装补丁期间，**Show Node Status** 是可在“补丁管理”(Patch Management) 页面上访问的唯一功能。

步骤 4 选择**管理 (Administration)** > **维护 (Maintenance)** > **补丁管理 (Patch Management)** 以返回至“补丁安装” (Patch Installation) 页面。

步骤 5 点击您安装的补丁旁边的单选按钮，然后点击**显示节点状态 (Show Node Status)** 以验证是否已完成安装。

思科 ISE-PIC 软件补丁

思科 ISE-PIC 软件补丁始终会累积。思科 ISE-PIC 允许您执行补丁安装和从 CLI 或 GUI 回滚。

可以在部署中从主 PAN 为思科 ISE-PIC 服务器安装补丁。要从主 PAN 安装补丁，您必须从 Cisco.com 将补丁下载至运行您的客户端浏览器的系统。

如果从 GUI 安装补丁，补丁将先自动安装到主 PAN 上。系统随后将按照 GUI 中列出的顺序，在部署中的其他节点上安装补丁。无法控制节点的更新顺序。还可以手动安装、回滚和查看补丁版本。在思科 ISE GUI 中，点击**菜单**图标 (☰)，然后选择**管理 (Administration) > 系统 (System) > 维护 (Maintenance) > 补丁管理 (Patch Management)**。

如果从 CLI 安装补丁，可以控制节点的更新顺序。但是，建议您先在主 PAN 上安装补丁。其余节点上的安装顺序不影响。您可以同时在多个节点上安装修补程序，以加快此过程。

如果要在升级整个部署之前在某些节点上验证补丁，可以使用 CLI 在选定节点上安装补丁。使用以下 CLI 命令安装补丁：

```
patch install <patch_bundle> <repository_that_stores_patch_file>
```

有关详细信息，请参阅《思科身份识别服务引擎 CLI 参考指南》中“执行模式下的思科 ISE CLI 命令”一章中的“安装补丁”部分。

您可以直接安装所需的补丁版本。例如，如果您当前使用的是思科 ISE 2.x，并且希望安装思科 ISE 2.x 补丁 5，则可以直接安装思科 ISE 2.x 补丁 5，而无需安装以前的补丁（在本例中为思科 ISE 2.x 补丁 1-4）。要在 CLI 中查看补丁版本，请使用以下 CLI 命令：

```
show version
```

软件补丁安装指南

在 ISE 节点上安装补丁时，节点会在安装完成后重新引导。可能必须等待几分钟才能再次登录。可以在维护时段安排补丁安装，以避免临时中断。

确保安装了适用于网络中部署的思科 ISE-PIC 版本的补丁。思科 ISE-PIC 会报告任何版本不匹配问题，以及补丁文件中的任何错误。

注释 思科 ISE 补丁也可以安装在 ISE-PIC 上。

安装的补丁版本不能低于当前安装在思科 ISE-PIC 上的补丁版本。同样，如果思科 ISE-PIC 当前安装的是高版本补丁，则无法回滚低版本补丁的更改。例如，如果思科 ISE-PIC 服务器安装的是补丁 3，则无法安装或回滚补丁 1 或 2。

从两节点部署中的主 PAN 安装补丁时，思科 ISE-PIC 会先后在主节点和辅助节点上安装补丁。如果在主 PAN 上成功安装，思科 ISE-PIC 之后会继续在辅助节点上安装补丁。如果在主 PAN 上安装失败，则不会继续在辅助节点上安装。

回滚软件补丁

您从属于部署一部分的 PAN 回滚补丁时，思科 ISE-PIC 会在主节点上回滚补丁，然后在部署中的辅助节点上回滚补丁。

步骤 1 在 ISE-PIC GUI 中，点击**菜单**图标 (☰)，然后选择**管理 (Administration)** > **维护 (Maintenance)** > **补丁管理 (Patch Management)**。

步骤 2 点击您要回滚更改的补丁版本的单选按钮，然后点击**回滚 (Rollback)**。

注释 回滚补丁期间，在“补丁管理”(Patch Management) 页面上仅可访问 **Show Node Status** 功能。

从 PAN 回滚补丁后，思科 ISE 会将您注销，您必须等待几分钟，然后才能再次登录。

步骤 3 您登录之后，请点击页面底部的**警报 (Alarms)** 链接以查看回滚操作的状态。

步骤 4 要查看补丁回滚的进程，请在“补丁管理”(Patch Management) 页面选择补丁，然后点击**显示节点状态 (Show Node Status)**。

步骤 5 在辅助节点上，点击补丁的单选按钮，然后点击**显示节点状态 (Show Node Status)**，确保从部署中的所有节点回滚补丁。

如果没有从任意辅助节点回滚补丁，请确保该节点正常运行并且重复此程序以从其余节点回滚更改。思科 ISE-PIC 仅从仍安装此版本补丁的节点回滚补丁。

软件补丁回滚指南

要从部署中的思科 ISE-PIC 节点回滚补丁，必须先从 PAN 回滚更改。如果此操作成功，则系统会从辅助节点回滚补丁。如果 PAN 上的回滚流程失败，则系统不会从辅助节点回滚补丁。

当思科 ISE-PIC 从辅助节点回滚补丁时，可以继续从 PAN GUI 执行其他任务。辅助节点将会在回滚后重新启动。

备份和恢复数据

注释 思科 ISE-PIC 的作用在许多情况下与思科 ISE 备份和恢复程序相同，因此，术语思科 ISE 有时可能会互换使用，以表示与思科 ISE-PIC 相关的操作和功能。

思科 ISE-PIC 允许您从主节点或独立节点备份数据。可以从 CLI 或用户界面完成备份。

思科 ISE-PIC 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。
- 运行数据 - 包含监控和故障排除数据。

备份和恢复存储库

思科 ISE-PIC 允许您创建和删除存储库。您可以创建以下类型的存储库：

- DISK
- FTP
- SFTP
- NFS
- CD-ROM
- HTTP
- HTTPS

您可以为使用 KVM 创建的虚拟 CD-ROM，创建类型为 CD-ROM 的存储库。

注释 存储库位于每台设备本地位置。

注释 我们建议您为小型部署（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。

在 GUI 中，密钥仅在主 PAN 上生成，因此在升级期间，需要在新的主管理节点的 GUI 中再次生成密钥，并将其导出到SFTP服务器。如果从部署中删除节点，需要在非管理节点的GUI中生成密钥，并将其导出到 SFTP 服务器。

可以在思科 ISE-PIC 中凭借 RSA 公共密钥身份验证配置 SFTP 存储库。您可以选择使用安全密钥的RSA公共密钥身份验证来加密数据库和日志，而不必使用管理员创建的密码。对于通过RSA公共密钥创建的 SFTP 存储库，在 GUI 中创建的存储库不会在 CLI 中复制，在 CLI 中创建的存储库也不会在 GUI 中复制。要在 CLI 和 GUI 中配置相同存储库，请在 CLI 和 GUI 中生成 RSA 公共密钥，并将密钥输出到 SFTP 服务器。

注释 即使未在 ISE 上启用 FIPS 模式，思科 ISE 也会在 FIPS 模式下启动出站 SSH 或 SFTP 连接。确保与 ISE 通信的远程 SSH 或 SFTP 服务器允许 FIPS 140 批准的加密算法。

思科 ISE 使用嵌入式 FIPS 140 验证加密模块。有关 FIPS 合规要求的详细信息，请参阅 FIPS 合规证明书。

开始之前

- 如果要使用 RSA 公共密钥身份验证创建 SFTP 存储库，请执行以下步骤：
  - 在 SFTP 存储库中启用 RSA 公共密钥身份验证。
  - 您必须以管理员 CLI 用户身份登录。从思科 ISE CLI 使用 **crypto host_key add** 命令输入SFTP服务器的主机密钥。主机密钥字符串应当与您在存储库配置页面的**路径 (Path)** 字段中输入的主机名匹配。
  - 生成密钥对，并从 GUI 将公共密钥导出到您的本地系统。在思科 ISE CLI 中，使用 **crypto key generate rsa passphrase** *test123* 命令生成密钥对，其中 passphrase 必须超过 13个字母，然后将密钥导出到任何存储库（本地磁盘或任何其他配置的存储库）。
  - 将导出的 RSA 公共密钥复制到启用 PKI 的 SFTP 服务器并将其添加到“authorized_keys”文件。

注释 当主 PAN 和主 MnT 是独立的节点时，您可以使用**存储库列表 (Repository List)** 窗口中的**生成密钥对 (Generate Key Pairs)** 选项来为主 PAN 和主 MnT 节点生成 RSA 密钥。您可以使用**存储库列表 (Repository List)** 窗口中的**导出公共密钥 (Export Public Key)** 选项来同时从主 PAN 和主 MnT 节点导出生成的 RSA 密钥。

步骤 1 选择**管理 (Administration)** > **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

下表介绍了**存储库列表 (Repository List)** 窗口上的字段，可以使用此页面创建存储备份文件的存储库。要查看此处窗口，请点击**菜单**图标 (☰)，然后选择 **管理 (Administration)** > **维护 (Maintenance)** > **存储库 (Repository)**。

表 *1:* 存储库设置

字段	使用指南
存储库 (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。
主机 (Host)	（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 IP 地址（IPv4 或 IPv6）。 **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。 请注意，某些特殊字符（如 !、?、~（不包括在上面的列表中）允许通过 GUI 配置 FTP 和 SFTP 密码。但是，这些特殊字符不允许通过 CLI 或开放式 API 进行配置。

相关主题

备份和恢复存储库

创建存储库，第 8 页

在 SFTP 存储库中启用 RSA 公共密钥身份验证

在 SFTP 服务器中，每个节点必须具有两个 RSA 公共密钥，一个用于 CLI，一个用于 GUI。要在 SFTP 存储库中启用 RSA 公共密钥身份验证，请执行以下步骤：

注释 在 SFTP 存储库中启用 RSA 公共密钥身份验证后，您将无法使用 SFTP 凭证登录。您可以使用基于 PKI 的身份验证或基于凭证的身份验证。如果要再次使用基于凭证的身份验证，则必须从 SFTP 服务器中删除公共密钥对。

步骤 1 用有权限编辑 */etc/ssh/sshd_config.file* 的帐户登录 SFTP 服务器。

注释 *sshd_config* 文件的位置可能根据操作系统安装而有所不用。

步骤 2 输入 **vi /etc/ssh/sshd_config** 命令。

系统列出 sshd_config 文件的内容。

步骤 3 从以下行中删除“#”符号以启用 RSA 公共密钥身份验证：

- RSAAuthentication 是
- PubkeyAuthentication 是

  注释 如果公共身份验证密钥为 no，则将其更改为 yes。

- AuthorizedKeysFile ~/.ssh/authorized_keys

按需备份和计划备份

您可以配置主 PAN 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。

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 ISE-PIC 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 ISE-PIC 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 ISE-PIC 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。

步骤 1 在 ISE-PIC GUI 中，点击**菜单**图标 (☰)，然后选择**管理 (Administration)** > **维护 (Maintenance)** > **备份和恢复 (Backup and Restore)**。

步骤 2 选择备份类型：“配置”(Configuration) 或“运行”(Operational)。

步骤 3 点击**立即备份 (Backup Now)**。

步骤 4 根据需要输入值以执行备份。

步骤 5 点击 **备份 (Backup)**。

步骤 6 验证备份是否成功完成。

思科 ISE-PIC 在备份文件名中附加时间戳并将文件存储在指定存储库中。除了时间戳外，思科 ISE-PIC 会为配置备份添加 CFG 标签，为运行备份添加 OPS 标签。确保备份文件位于指定的存储库中。

备份正在运行时，请勿升级节点。如果并发运行备份，这将关闭所有进程并可能导致数据不一致。在进行任何节点更改之前，请等待备份完成。

注释 备份正在运行时，可能会看到 CPU 使用率高并收到平均负载高的警报。备份完成时，CPU 使用率将恢复正常。

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 ISE-PIC 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 ISE-PIC 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 ISE-PIC 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。

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。

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 ISE-PIC 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：

- 检查是否存在任何 NTP 同步或服务失败问题。如果思科 ISE 上的 NTP 服务无效，思科 ISE 将发出 NTP 服务失败警报。当思科 ISE 无法与所有配置的 NTP 服务器同步时，思科 ISE 会发出 NTP 同步失败警报。如果 NTP 服务停止或有任何同步问题，思科 ISE 备份可能会失败。检查“警报”(Alarms) Dashlet 并修复 NTP 同步或服务问题，然后再重试备份操作。
- 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。

注释 思科 ISE-PIC 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 ISE-PIC 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

注释
- 从思科 ISE 版本 3.2 及更高版本开始，根 CA 会在恢复流程中自动重新生成。因此，不需要在 config-backup 后重新生成根 CA。

下面提供了恢复思科 ISE-PIC 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 ISE-PIC 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 ISE-PIC 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ISE-PIC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 ISE-PIC 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 ISE-PIC 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。（ 要查看此处窗口，请点击**菜单**图标 (☰)，然后选择 **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 ISE-PIC 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，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 ISE-PIC 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 ISE-PIC 中使用 restore 命令时，思科 ISE-PIC 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 ISE-PIC 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。

	说明
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。

步骤 1 选择**管理 (Administration)** > **维护 (Maintenance)** > **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，然后点击**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 ISE-PIC 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。

同步主节点和辅助节点

在 PAN 上恢复备份文件之后，主节点和辅助节点中的思科ISE-PIC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ISE-PIC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ISE-PIC，只能在同步完成后导航至其他思科ISE-PIC管理员门户页面和进行配置更改。

步骤 1 选择**管理 (Administration)** > **部署 (Deployment)**。

步骤 2 选中处于不同步复制状态的辅助节点旁边的复选框。

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ISE-PIC管理员门户。

恢复独立和两节点部署中断开的节点

此部分提供可用于恢复独立和两节点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 地址和主机名恢复两节点部署中断开连接的节点

场景

在两节点部署中，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 ISE-PIC 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 地址和主机名恢复两节点部署中断开的节点

场景

在两节点部署中，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 ISE-PIC 节点：N1（主策略管理节点，即主 PAN）和 N2（辅助节点）。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 ISE-PIC 节点在新位置被替换，新主机名为 N1A（主 PAN）和 N2A（辅助节点）。此处 N1A 和 N2A 都是独立节点。

假定条件

部署中的所有思科 ISE-PIC 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. 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 ISE-PIC 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。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。

在两节点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 ISE-PIC 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

仅两节点部署中的主节点出现故障。

解决步骤

1. 登录 N2 管理员门户。在思科 ISE GUI 中，点击**菜单**图标 (☰)，然后选择 ，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。

在两节点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。

解决步骤

1. 将辅助节点重新映像到默认独立状态。
2. 从主节点登录管理员门户并删除辅助节点。
3. 重新注册辅助节点。

   数据从主节点复制到辅助节点。无需恢复。

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。
- 清除同样依据数据库已使用的磁盘空间。当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%。系统总会在检查数据库磁盘空间限制之后，才继续执行清除。

运营数据清除

思科 ISE 监控操作数据库包含作为思科 ISE 报告生成的信息。最近发布的思科 ISE（Cisco ISE 版本 2.4 及更高版本）具有一些选项，可在运行 **application configure ise** 命令时清除监控运行数据并重置监控数据库。

清除选项用于清除数据，并会提示输入数据的保留天数。重置选项用于将数据库重置为出厂默认设置，这样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，可指定数据库。

注释 重置选项会导致思科 ISE 服务暂时不可用。

相关主题

清除较旧的运营数据，第 22 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。

步骤 1 选择管理 **(Administration)** > 维护 **(Maintenance)** > 操作数据清除 **(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。虽然 ISE-PIC 不提供 RADIUS 或 TACACS 功能，但与思科 ISE 共享某些基础设施，因此可能需要定期从数据库清除此类信息。
  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)** 字段中，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)**。

将 ISE-PIC 升级到完整 ISE 安装

思科 ISE-PIC 基于完整思科 ISE GUI 显示在简单的用户直观 GUI 中。因此，通过安装 ISE-PIC，您可以快速高效地轻松升级到 ISE。从 ISE-PIC 升级到 ISE 的基本版许可证时，ISE 继续提供在升级之前 ISE-PIC 中可供您使用的所有功能，如果您使用已升级的 ISE-PIC 节点作为主 PAN，则无需重新配置已配置的任何设置。

注释 如果您不使用现有已升级的 ISE-PIC 节点作为主 PAN，则升级时将清除该节点上的数据，并且您将能够从新添加的节点访问现有完整 ISE 部署中的数据。

有关升级到 ISE 的优势的详细信息，请参阅将ISE-PIC与思科 ISE 和思科 Context Directory Agent 进行比较。

通过注册许可证升级到 ISE

开始之前

启用 Essential 许可证可以将 ISE-PIC 节点升级为思科 ISE 节点。在启用基本许可证之前，您必须在 ISE-PIC 节点上购买并启用 ISE-PIC 和 ISE-PIC 升级许可证。在 CSSM 中注册许可证后，基本许可证会显示在许可证 (Licenses) 表中。应用服务会在升级期间重新启动。

有关许可模型的详细信息，请参阅 ISE-PIC 智能许可

步骤 1 如果已安装辅助节点，请在思科 ISE-PIC 主节点安装中，选择**管理 (Administration)** > **部署 (Deployment)**，并取消注册辅助节点。两个节点随后都将成为主节点，并且其中一个节点可以升级。

步骤 2 选择**管理 (Administration)** > **许可 (Licensing)**。

步骤 3 点击**导入许可证 (Import License)**。

步骤 4 点击**选择文件 (Choose File)**，浏览升级许可证文件，然后点击**确定 (OK)**。

步骤 5 **注释** 如果将此 ISE-PIC 节点添加到现有 ISE 部署，则完成此步骤后即已完成升级，现在可以从此部署中的主节点注册此节点来添加此节点。有关详细信息，请参阅https://www.cisco.com/c/en/us/support/security/identity-services-engine/products-installation-and-configuration-guides-list.html《思科身份识别服务引擎管理员指南》。

在**导入新许可证文件 (Import New License File)** 屏幕中，点击**导入 (Import)**。

步骤 6 要使此升级节点成为完整ISE部署中的主节点，请立即导入基本版许可证。再次点击**导入许可证(Import License)**。

步骤 7 点击**选择文件 (Choose File)**，浏览思科代表提供的许可证，然后点击**确定 (OK)**。

步骤 8 在**导入新许可证文件 (Import New License File)** 屏幕中，点击**导入 (Import)**。

步骤 9 点击**确定 (OK)**。
升级为 ISE 主节点的过程将开始，并显示以下消息：“此节点现在正在后台中升级到 *ISE*。请等待几分钟，然后登录 *ISE*。” *(This node is now being upgraded to ISE in the background. Please wait several minutes and then log in to ISE.)*

步骤 10 点击**确定 (OK)**。

几分钟后，将显示登录屏幕。重新登录并访问基本版许可证安装提供的所有菜单。

您现在已将主 ISE-PIC 节点升级为完整 ISE 安装中的主节点，以前的辅助节点现在是 ISE-PIC 独立安装中的主节点和唯一节点。现在可以使用相同方式单独升级最后一个 ISE-PIC 节点。

管理设置 ISE-PIC

基于角色的访问控制

思科 ISE-PIC 允许您定义基于角色的访问控制 (RBAC) 策略，以允许或拒绝向管理员授予某些系统操作权限。这些 RBAC 策略根据单个管理员或管理员所属管理员组的身份定义。

要进一步提高访问 Admin 门户的用户的安全和控制，您可以执行以下操作:

- 根据远程客户端的 IP 地址配置管理访问设置。
- 为管理帐户定义强密码策略。
- 为管理 GUI 会话配置会话超时。

思科 ISE-PIC 管理员

管理员可使用管理员门户执行下列操作：

- 管理部署节点监控和故障排除。
- 管理思科ISE-PIC服务管理员帐户以及系统配置和操作。
- 更改管理员和用户密码。

CLI 管理员可以启动和停止思科 ISE 应用、应用软件补丁和升级、重新加载或关闭思科 ISE 设备，以及查看所有系统和应用日志。由于授予 CLI 管理员的特殊权限，建议您保护 CLI 管理员凭证并创建基于 Web 的管理员来配置和管理思科 ISE 部署。

在设置过程中配置的用户名和密码仅用于对 CLI 进行管理访问。此角色被视为 CLI 管理员用户，也称为CLI管理员。默认情况下，CLI管理员用户的用户名为admin，密码是设置过程中定义的密码。没有默认密码。此 CLI 管理员用户是默认管理员用户，无法删除此用户帐户。不过，其他管理员可以编辑此用户帐户，包括启用、禁用相关帐户或者更改其密码。

您可以创建管理员，也可以将现有用户升级为管理员角色。通过禁用对应的管理权限，还可以将管理员降级为简单网络用户状态。

管理员是具有配置和操作思科 ISE-PIC 系统的本地权限的用户。

管理员会分配到一个或多个管理员组。方便起见，这些管理员组已在系统中预定义，如以下部分所述。

注释 从思科 ISE 版本 2.7 起，在思科 ISE 中创建用户账户时，请使用字母数字值。

相关主题

思科 ISE-PIC 管理员组 ，第 25 页

思科 ISE-PIC 管理员组

管理员组是思科ISE中基于角色的访问控制（RBAC）组。ISE-PIC属于同一组的所有管理员共用同一身份并且具有相同的权限。管理员作为特定管理组成员的身份可用作授权策略中的条件。管理员可以属于不止一个管理员组。

思科 ISE 支持多个外部身份库，以加强管理员的用户访问管理。

具有任何访问权限级别的管理员帐户可以在其有权访问的任何窗口上，修改或删除其拥有权限的对象。

下表列出了思科 ISE-PIC 中预定义的管理组以及这些组成员可以执行的任务。只有这些预定义的组才能定义系统中的管理员用户。

表 *2:* 思科 *ISE* 管理员组、访问级别、权限和限制

管理组角色	访问级别	权限	限制
超级管理员	所有思科 ISE-PIC 管理功能。默认管理员帐户属于此组。	对所有思科 ISE-PIC 资源拥有创建、读取、更新、删除和执行 (CRUDX) 权限。	
外部 RESTful 服务 (ERS) 管理员	对所有 ERS API 请求（GET、POST、DELETE、PUT）的完全访问权限	• 创建、读取、更新和删除 ERS API 请求	此角色仅适用于支持内部用户、身份组和终端的 ERS 授权

CLI 管理员与基于 Web 管理员的权限对比

CLI 管理员可以启动和停止思科 ISE-PIC 应用、应用软件补丁和升级、重新加载或关闭思科 ISE-PIC 设备，以及查看所有系统和应用日志。由于授予 CLI 管理员的特殊权限，我们建议您保护 CLI 管理员凭证并创建基于 Web 的管理员来配置和管理思科 ISE-PIC 部署。

创建新管理员

思科 ISE-PIC 管理员需要分配有特定角色的帐户才能执行特定管理任务。您可以创建多个管理员帐户，并根据管理员必须执行的管理任务向这些管理员分配一个或多个角色。

使用**管理员用户 (Admin Users)** 窗口查看、创建、修改、删除、复制或搜索思科 ISE-PIC 管理员的属性或更改其状态。

注释 如果管理员用户的域在 CLI 和 GUI 中相同，建议您先在 CLI 中配置 Active Directory 访问权限，然后再将其加入 GUI。另外，必须从 GUI 重新加入域，以避免此域发生身份验证失败。

步骤 1 选择**管理 (Administration)** > **管理员访问权限 (Admin Access)** > **管理员用户 (Admin Users)** > **添加 (Add)** > **创建管理员用户 (Create an Admin User)**。

步骤 2 在字段中输入值。**名称 (Name)** 字段支持的字符为 # $ ’ ( ) * + -。/ @ _。

管理员用户名必须唯一。如果输入了现有用户名，错误弹出窗口将显示以下消息：

```
User can't be created. A User with that name already exists.
```

步骤 3 点击**提交 (Submit)** 在思科 ISE-PIC 内部数据库中创建新管理员。

相关主题

只读管理员策略
自定义只读管理员的菜单访问权限

对思科 ISE-PIC 进行管理访问

思科 ISE-PIC 管理员可以根据其所属的管理组执行各种管理任务。这些管理任务至关重要。仅向有权在网络中管理思科 ISE-PIC 的用户授予管理访问权限。

注释 当将思科 ISE 服务器添加到网络时，一旦其 Web 界面出现，它就会被标记为处于运行状态。但是，由于一些高级服务（如安全评估服务）可能需要更长的时间才能完全可用，因此可能需要更多时间才能使所有服务完全运行。

管理访问方法

有多种方式可以连接到 思科 ISE 服务器。策略管理节点 (PAN) 运行管理员门户。需要管理员密码才能登录。其他 ISE 角色服务器可通过 SSH 或控制台（在其中运行 CLI）进行访问。本节介绍可用于每种连接类型的进程和密码选项：

- **管理员密码 (Admin password)**：默认情况下，在安装期间创建的思科 ISE 管理员用户将在 45 天后超时。您可以通过在**管理 (Administration)** > **系统 (System)** > **管理设置 (Admin Settings)** 中关闭**密码使用时间 (Password Lifetime)** 来防止此情况。点击**密码策略 (Password Policy)** 选项卡，并取消选中**密码有效期 (Password Lifetime)** 下的**管理密码到期 (Administrative passwords expire)** 复选框。

  如果不执行此操作，当密码到期时，可以在 CLI 中运行 **application reset-passwd** 命令以重置管理员密码。要重置管理密码，可以连接至控制台以访问 CLI，或重新引导 ISE 映像文件以访问引导选项菜单。

- **CLI 密码 (CLI password)**：必须在安装期间输入 CLI 密码。如果在登录 CLI 时因密码无效而遇到问题，可以重置 CLI 密码。连接至控制台，并运行 **password** CLI 命令以重置密码。有关详细信息，请参阅《思科身份识别服务引擎 CLI 参考指南》。

-

管理员访问设置

思科 ISE-PIC 允许为管理员帐户定义某些规则以增强安全性。您可以限制对管理接口的访问，强制管理员使用强密码和定期更改密码等。在思科 ISE-PIC 中的“管理员帐户设置”(Administrator Account Settings) 中定义的密码策略适用于所有管理员帐户。

思科 ISE-PIC 支持包含 UTF-8 字符的管理员密码。

配置最大数量的并发管理会话和登录横幅

您可以配置最大数量的并发管理 GUI 或 CLI (SSH) 会话和登录横幅，它们对访问您的管理 Web 或 CLI 界面的管理员有帮助和指导作用。您可以将登录横幅配置为在管理员登录之前和登录之后显示。默认情况下，这些登录横幅处于禁用状态。但是，您无法为单个管理员账户配置最大并发会话数。

步骤 1 选择**管理 (Administration)** > **管理员访问 (Admin Access)** > **访问设置 (Access Settings)** > **会话 (Session)**。

步骤 2 输入您要允许通过 GUI 和 CLI 界面的最大数量的并发管理会话。并发管理 GUI 会话的有效范围为 1 至 20。并发管理 CLI 会话的有效范围为 1 至 10。

步骤 3 如果希望思科 ISE-PIC 在管理员登录之前显示消息，请选中**登录前横幅 (Pre-login banner)** 复选框，然后在文本框中输入消息。

步骤 4 如果希望思科 ISE-PIC 在管理员登录之后显示消息，请选中**登录后横幅 (Post-login banner)** 复选框，然后在文本框中输入消息。

步骤 5 点击**保存**。

注释 登录前横幅的字符数限制为 1500，登录后横幅的字符数限制为 3000。支持除 **%** 和 **<** 以外的所有字符。通过 CLI 安装登录横幅时，所用文件名的最大长度为 256 个字符。

允许从“选择 IP 地址”(Select IP Addresses) 对思科 ISE-PIC 进行管理访问

思科 ISE-PIC 允许您配置 IP 地址列表，管理员可通过列表中的 IP 地址访问思科 ISE-PIC 管理界面。

步骤 1 选择**管理 (Administration)** > **管理员访问 (Admin Access)** > **访问设置 (Access Settings)** > **IP 访问 (IP Access)**。

步骤 2 点击**仅允许列出的 IP 地址进行连接 (Allow only listed IP addresses to connect)** 单选按钮。

注释 端口 161 上的连接 (SNMP) 用于管理访问。但是，在配置 IP 访问限制时，如果从一个节点执行 snmpwalk 而没有为其配置管理访问，则 snmpwalk 会失败。

步骤 3 在**配置访问限制的 IP 列表 (Configure IP List for Access Restriction)** 区域中，点击**添加 (Add)**。

步骤 4 在**添加 IP CIDR (Add IP CIDR)** 对话框中，在 **IP 地址 (IP Address)** 字段中输入无类域间路由 (CIDR) 格式的 IP 地址。

注释 该 IP 地址可以是 IPv4 或 IPv6 地址。您可以为一个 ISE 节点配置多个 IPv6 地址。

步骤 5 在 **CIDR 格式的子网掩码 (Netmask in CIDR format)** 字段中输入网络掩码。

步骤 6 点击**确定 (OK)**。重复步骤 4-7 在此列表中添加更多 IP 地址范围。

步骤 7 点击**保存 (Save)** 保存所做的更改。

步骤 8 点击**重置 (Reset)** 以刷新 **IP 访问 (IP Access)** 窗口。

为管理员帐户配置密码策略

思科 ISE-PIC 还允许您为管理员帐户创建密码策略，以增强安全性。您在此处定义的密码策略将应用于思科 ISE-PIC 中的所有管理员帐户。

注释

- 内部管理员用户的电子邮件通知将发送到 root@host。无法配置电子邮件地址，并且许多 SMTP 服务会拒绝此电子邮件。

  遵循开放缺陷 CSCui5583，此增强允许您更改电子邮件地址。

- 思科 ISE-PIC 支持包含 UTF-8 字符的管理员密码。

步骤 1 选择**管理 (Administration)** > **管理员访问权限 (Admin Access)** > **身份验证 (Authentication)**。

步骤 2 点击**密码策略 (Password Policy)** 选项卡并输入所需的值，以便配置思科 ISE GUI 和 CLI 密码要求。

步骤 3 点击**保存 (Save)** 保存管理员密码策略。

注释 如果在登录时使用外部身份库验证管理员的身份，请记住，即便为应用到该管理员配置文件的密码策略配置了此设置，外部身份库也仍会验证管理员的用户名和密码。

为管理员帐户配置帐户禁用策略

如果在配置的连续几天内，管理员帐户没有通过身份验证，思科 ISE-PIC 允许您禁用该管理员帐户。

步骤 1 选择**管理 (Administration)** > **管理员访问 (Admin Access)** > **身份验证 (Authentication)** > **帐户禁用策略 (Account Disable Policy)**。

步骤 2 选定**在 n 天不活跃之后禁用帐户 (Disable account after *n* days of inactivity)** 复选框，并在相应的字段中输入天数。

如果管理员帐户在一段指定时间内处于不活跃状态，通过该选项，您可以禁用管理员帐户。

当管理员账户被禁用并在以后启用时，它的活动时间不会超过 24 小时。如果您希望管理员账户在禁用后仍保持活动状态，请取消选中 **Disable account after *n* days of inactivity** 复选框。

步骤 3 点击**保存 (Save)** 为管理员配置全局帐户禁用策略。

配置管理员会话超时

在思科 ISE-PIC 中，可以确定管理 GUI 会话处于非活动状态但仍保持连接的时间长度。可以指定思科 ISE-PIC 在注销管理员之前经过的时间（以分钟为单位）。会话超时后，管理员必须重新登录才能访问思科 ISE-PIC 管理员门户。

步骤 1 选择管理 **(Administration)** > 管理员访问权限 **(Admin Access)** > 会话设置 **(Session Settings)** > 会话超时 **(Session Timeout)**。

步骤 2 输入思科 ISE-PIC 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。

步骤 3 点击保存 **(Save)**。

终止活动管理会话

思科 ISE-PIC 显示所有活动管理会话，您可以从中选择任意会话并在必要时随时终止所选会话。并行管理 GUI 会话的最大数量为 20 个。如果达到 GUI 会话的最大数量，属于超级管理员组的管理员可以登录并阻止某些会话。

步骤 1 选择管理 **(Administration)** > 管理员访问权限 **(Admin Access)** > 会话设置 **(Session Settings)** > 会话信息 **(Session Info)**。

步骤 2 选中要终止的会话 ID 旁边的复选框，然后点击失效 **(Invalidate)**。

管理门户使用的端口

管理门户使用 HTTP 80 端口和 HTTPS 443 端口，并且您无法更改这些设置。您不能将任何最终用户门户配置为使用这些端口，以便降低管理门户的风险。

配置 SMTP 服务器以支持通知

配置简单邮件传输协议 (SMTP) 服务器，以执行以下操作：发送警报的电子邮件通知。

发送电子邮件的 ISE 节点

以下列表显示了分布式 ISE 环境中哪些节点会发送电子邮件。

电子邮件用途	发送电子邮件的节点
访客过期	主 PAN
警报	活动 MnT
来自访客和发起人门户的发起人和访客通知	PSN
密码过期	主 PAN

步骤 1 选择 设置 (Settings) > SMTP 服务器 (SMTP Server)。

步骤 2 在 SMTP 服务器 (SMTP Server) 字段中输入出站 SMTP 服务器的主机名。必须可从思科 ISE-PIC 服务器访问该 SMTP 主机服务器。该字段长度不得超过 60 个字符。

步骤 3 点击保存 (Save)。

警报通知的收件人可以是已启用在电子邮件中包括系统警报 (Include system alarms in emails) 选项的任何内部管理员用户。发送警报通知的发件人的邮件地址硬编码为 ise@<hostname>。

从 GUI 启用外部 RESTful 服务 API - ERS 设置

开始之前

您必须启用 Cisco ISE REST API 对于思科 ISE 开发的应用REST API可以访问思科 ISE。Cisco REST API使用HTTPS端口9060，默认情况下会关闭。Cisco ISE REST API 在思科 ISE 管理员服务器上未启用，客户端应用程序从所有访客 REST API 请求的服务器将收到超时错误。

所有类型外部宁静的服务请求的主要ESS节点有效。辅助节点可以访问（GET请求）。

步骤 1 选择设置 (Settings) > ERS 设置 (ERS Settings)。

步骤 2 选择启用 ERS 进行读/写 (Enable ERS for Read/Write) 并点击保存 (Save)。

下一步做什么

有关 API 调用和 ISE-PIC 的详细信息，请参阅《 ISE API参考指南》 。

配置安全设置

要配置安全设置：

步骤 1 选择设置 (Settings) > 安全设置 (Security Settings)。

步骤 2 在安全设置 (Security Settings) 窗口中，选择所需的选项：

1. **Allow TLS 1.0 (允许 TLS 1.0)**：在以下工作流程中允许 TLS 1.0 用于与以下传统对等体通信：
   - 思科 ISE 配置为 EAP 服务器
   - 思科 ISE 从 HTTPS 或安全 LDAP 服务器下载 CRL
   - 思科 ISE 配置为安全 TCP 系统日志客户端
   - 思科 ISE 配置为安全 LDAP 客户端

- 思科 ISE 配置为 ERS 服务器

还允许使用 TLS 1.0 与以下 ISE 组件通信：

- 所有门户
- 证书颁发机构
- MDM 客户端
- pxGrid
- PassiveID 代理

注释　建议客户端和服务器协商使用更高版本的 TLS 以增强安全性。

2. **Allow TLS 1.1 (允许 TLS 1.1)**：在以下工作流程中允许 TLS 1.1 用于与以下传统对等体通信：
   - 思科 ISE 配置为 EAP 服务器
   - 思科 ISE 从 HTTPS 或安全 LDAP 服务器下载 CRL
   - 思科 ISE 配置为安全 TCP 系统日志客户端
   - 思科 ISE 配置为安全 LDAP 客户端
   - 思科 ISE 配置为 ERS 服务器

   还允许使用 TLS 1.1 与以下 ISE 组件通信：
   - 管理 UI
   - 所有门户
   - 证书颁发机构
   - 外部 RESTful 服务 (ERS)
   - MDM 客户端
   - pxGrid

   注释　建议客户端和服务器协商使用更高版本的 TLS 以增强安全性。

步骤 3　点击**保存 (Save)**。

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。