



思科身份服务引擎升级指南，版本 3.1

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2021 Cisco Systems, Inc. 保留所有权利。



目录

Short Description ?

第 1 章

升级思科 ISE 1

- 思科 ISE 升级概览 1
- 升级路径 2
- 虚拟机上支持的操作系统 3
- 许可更改 4
 - 虚拟设备许可证 5
 - 特定许可证预留 5
- 其他参考资料 5
- 通信、服务和其他信息 5
 - 思科漏洞搜索工具 6
 - 文档反馈 6

第 2 章

为升级做好准备 7

- 为升级做好准备 7
- 运行状况检查 8
- 加快升级速度与提高升级效率指南 8
- 验证数据以防止升级失败 10
 - 下载并运行升级就绪工具 11
 - 创建存储库并复制 URT 捆绑包 11
 - 运行升级就绪工具 12
 - 在存在同名预定义授权复合条件的情况下，更改授权简单条件的名称 12
 - 更改 VMware 虚拟机访客操作系统和设置 13

| | |
|--------------------------------|---|
| 删除发起人组名称中的非 ASCII 字符 | 13 |
| 必须开放用于通信的防火墙端口 | 13 |
| 从主管理节点备份思科 ISE 的配置和运行数据 | 13 |
| 从主管理节点备份系统日志 | 14 |
| CA 证书链 | 15 |
| 检查证书有效性 | 15 |
| 删除证书 | 15 |
| 导出证书和私钥 | 16 |
| | 16 |
| 升级前禁用 PAN 自动故障切换和禁用计划备份 | 16 |
| 配置 NTP 服务器和验证可用性 | 17 |
| 升级虚拟机 | 17 |
| 记录分析器的配置 | 17 |
| 获取 Active Directory 和内部管理员帐户凭证 | 18 |
| 升级前激活 MDM 供应商 | 18 |
| 创建存储库并复制升级捆绑包 | 18 |
| 检查可用磁盘大小 | 19 |
| 检查负载均衡器配置 | 19 |
| 日志保留和调整 MnT 硬盘大小 | 19 |
| <hr/> | |
| 第 3 章 | 执行升级 21 |
| | 节点的升级顺序 21 |
| | 选择升级方法 23 |
| | 使用备份和恢复方法升级思科 ISE 部署 26 |
| | 备份和恢复升级方法概述 26 |
| | 备份和恢复升级过程 27 |
| | 将辅助 PAN 和辅助 MnT 节点升级到思科 ISE 版本 2.6、2.7 或 3.0 28 |
| | 将辅助 PAN 和 MnT 节点升级到思科 ISE 版本 3.1 28 |
| | 将策略服务节点加入思科 ISE 版本 3.1 28 |
| | 将主 PAN 和 MnT 升级到思科 ISE 版本 3.1 29 |
| | 通过 GUI 升级思科 ISE 部署 29 |

| | | |
|-------|---------------------------|----|
| | 通过 GUI 升级思科 ISE 部署 | 29 |
| | 29 | |
| | 通过 GUI 全面升级思科 ISE 部署 | 30 |
| | 通过 GUI 拆分升级思科 ISE 部署 | 34 |
| | 从版本、2.6、2.7 或 3.0 到版本 3.1 | 37 |
| | 通过 CLI 升级思科 ISE 部署 | 40 |
| | 40 | |
| | 升级独立节点 | 40 |
| | 升级双节点部署 | 41 |
| | 升级分布式部署 | 42 |
| | 验证升级过程 | 44 |
| | 回滚到之前版本 | 45 |
| <hr/> | | |
| 第 4 章 | 安装最新补丁 | 47 |
| | 思科 ISE 软件补丁 | 47 |
| | 软件补丁安装指南 | 48 |
| | 安装软件补丁 | 48 |
| | 回滚软件补丁 | 49 |
| | 软件补丁回滚指南 | 49 |
| | 查看补丁安装和回滚更改 | 49 |
| <hr/> | | |
| 第 5 章 | 执行升级后的任务 | 51 |
| | 升级后的设置和配置 | 51 |
| | 转换为新的许可证类型 | 51 |
| | 验证虚拟机设置 | 51 |
| | 浏览器设置 | 51 |
| | 重新加入 Active Directory | 52 |
| | 反向 DNS 查找 | 53 |
| | 恢复证书 | 53 |
| | 重新生成根 CA 链 | 53 |
| | 以威胁防御为中心的 NAC | 54 |

- SMNP 原始策略服务节点设置 54
- 分析器源服务 55
- 客户端调配 55
 - 在线更新 55
 - 离线更新 55
- Cipher Suites 56
- 监控和故障排除 56
- 将策略刷新为 Trustsec NAD 56
- 更新请求者调配向导 56
- 分析器终端所有权同步/复制 57



第 1 章

升级思科 ISE

- [思科 ISE 升级概览，第 1 页](#)
- [升级路径，第 2 页](#)
- [虚拟机上支持的操作系统，第 3 页](#)
- [许可更改，第 4 页](#)
- [其他参考资料，第 5 页](#)
- [通信、服务和其他信息，第 5 页](#)

思科 ISE 升级概览

从 Cisco Identity Services Engine (思科 ISE) 版本 3.1 开始，所有 pxGrid 连接都必须基于 pxGrid 2.0。基于 pxGrid 1.0（基于 XMPP）的集成将从版本 3.1 开始在思科 ISE 上停止使用。

基于 WebSockets 的 pxGrid 版本 2.0 在思科 ISE 版本 2.4 中引入。我们建议将您的其他系统计划并升级到与 pxGrid 2.0 兼容的版本，以防止对集成造成可能的中断（如有）。

本文档介绍如何将思科 ISE 设备和虚拟机上的思科身份服务引擎 (思科 ISE) 软件升级到版本 3.1。（请参阅《思科身份服务引擎版本 3.1 版本说明》中的“[思科 ISE 版本 3.1 的新增功能](#)”部分。）

思科 ISE 部署升级过程包含多个步骤，必须按照本文档中指定的顺序执行。请使用本文档中提供的时间预计规划升级，以最大程度地减少业务中断时间。对于具有多个属于 PSN 组的策略服务节点 (PSN) 的部署，不会出现停机。如果没有终端通过正在升级的 PSN 进行身份验证，则请求将由节点组中的其他 PSN 处理。系统会重新对终端进行身份验证，验证成功后，会向其授予网络访问权限。



注意 如果您执行的是独立部署或仅一个 PSN 的部署，则在 PSN 升级时，所有身份验证都可能会造成停机。



注释 升级到思科 ISE 版本 3.2 及更高版本时，在升级流程中会自动重新生成根 CA。因此，不需要在升级后重新生成根 CA。

不同类型的部署

- 独立节点部署：单个的思科 ISE 节点担任管理、策略服务和监控角色。
- 多节点部署：几个 ISE 节点的分布式部署。

思科 ISE 本地云部署的差异

思科 ISE 升级工作流程在 AWS 上的思科 ISE 中不可用。仅支持全新安装。但是，您可以执行配置数据的备份和恢复。当您在思科 ISE AWS 实例中恢复数据时，数据会升级到思科 ISE 版本 3.1。

重新生成根 CA 链

如果发生以下事件，您必须重新生成根 CA 链：

- 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。

要重新生成根 CA 链，请执行以下操作：

1. 在思科 ISE GUI 中，单击菜单图标 (☰)，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)。
2. 单击生成证书签名请求 (Generate Certificate Signing Request (CSR))。
3. 从证书将用于 (Certificate(s) will be used for) 下拉列表中选择 ISE 根 CA。
4. 单击替换 ISE 根 CA 证书链 (Replace ISE root CA Certificate Chain)。

升级路径

单步升级

您可以直接从以下任何版本升级到 思科 ISE 版本 3.1：

- 思科 ISE 版本 2.6
- 思科 ISE 版本 2.7
- 思科 ISE 版本 3.0
- 思科 ISE 版本 3.1

两步升级

如果您的版本早于思科 ISE 版本 2.6，则必须先升级到上述版本之一，然后才能升级到版本 3.1。

虚拟机上支持的操作系统

思科 ISE 在基于 Red Hat Enterprise Linux (RHEL) 的思科应用部署引擎操作系统 (ADE-OS) 上运行。对于思科 ISE 3.1，ADE-OS 基于 RHEL 8.2。

下表显示了不同版本的思科 ISE 中使用的 RHEL 版本。

表 1: RHEL 版本

| 思科 ISE 版本 | RHEL 版本 |
|---------------|----------|
| 思科 ISE 1.3 | RHEL 6.4 |
| 思科 ISE 1.4 | RHEL 6.4 |
| 思科 ISE 2.0 | RHEL 7.0 |
| 思科 ISE 2.1 | RHEL 7.0 |
| 思科 ISE 2.2 | RHEL 7.0 |
| 思科 ISE 2.3 | RHEL 7.0 |
| 思科 ISE 2.4 | RHEL 7.3 |
| 思科 ISE 2.6 | RHEL 7.5 |
| Cisco ISE 2.7 | RHEL 7.6 |
| Cisco ISE 3.0 | RHEL 7.6 |
| Cisco ISE 3.1 | RHEL 8.2 |
| 思科 ISE 3.2 | RHEL 8.4 |



注释 RHEL 8.2 及更高版本支持以下 VMware ESXi 版本：

- VMware ESXi 6.5
- VMware ESXi 6.5 U1
- VMware ESXi 6.5 U2
- VMware ESXi 6.5 U3
- VMware ESXi 6.7
- VMware ESXi 6.7 U1
- VMware ESXi 6.7 U2
- VMware ESXi 6.7 U3
- VMware ESXi 7.0
- VMware ESXi 7.0 U1
- VMware ESXi 7.0 U2
- VMware ESXi 7.0 U3

除上述内容外，RHEL 8.2 还将支持较新的兼容 VMware ESXi 版本。

如果在升级后升级 VMware 虚拟机 (VM) 上的思科 ISE 节点，则必须将访客操作系统更改为支持的 RHEL 版本。要执行此操作，您必须关闭虚拟机，将访客操作系统更改为受支持的 RHEL 版本，并再打开虚拟机。



注释 如果您选择了访客操作系统 **RHEL 8** 和固件 **EFI**，请确保在 **VM Options** 选项卡中禁用 **Enable UEFI Secure Boot** 选项。默认情况下，为访客操作系统 RHEL 8 VM 启用此选项。确保禁用思科 ISE VM 的启用 **UEFI 安全启动** 选项。

使用 RHEL 操作系统升级思科 ISE 可能需要比正常升级过程更长的时间。此外，如果 Oracle 数据库版本发生更改，则升级可能需要更多时间，因为在操作系统升级期间安装了新的 Oracle 软件包。

许可更改

本节重点介绍思科 ISE 版本 3.1 中的许可更改。

有关思科 ISE 许可证的详细信息，请参阅以下资源：

- [思科 ISE 订购指南](#)
- [思科 ISE 迁移指南](#)

- [思科 ISE 许可常见问题](#)

有关在思科 ISE GUI 中激活许可证的信息，请参阅 [许可](#)。

虚拟设备许可证

思科 ISE 版本 3.1 及更高版本支持 ISE VM 许可证，该许可证取代了版本 3.1 之前的版本中支持的 VM 小型、VM 中型和 VM 大型许可证。新的 ISE VM 许可证涵盖内部部署和云部署中的思科 ISE VM 节点。

更多信息，请参阅《思科 ISE 管理员指南，版本 3.2》“许可证”一章中的“[思科 ISE 许可证](#)”。

特定许可证预留

特定许可证预留是一种智能许可方法，当您的组织的安全要求不允许思科 ISE 与思科智能软件管理器 (CSSM) 之间存在持久连接时，可帮助您管理智能许可。特定许可证预留允许您在思科 ISE 节点上保留特定许可证授权。

您可以通过定义需要预留的许可证的类型和数量来创建特定许可证预留，然后在思科 ISE 节点上激活预留。然后，您在其上注册并启用预留的思科 ISE 节点会跟踪许可证使用情况，同时强制执行许可证使用合规性。

有关更多信息，请参阅《思科 ISE 管理员指南版本 3.1》“许可”一章中的“[特定许可证保留](#)”。

其他参考资料

以下链接包含在使用思科 ISE 时可供使用的其他资源：

https://www.cisco.com/c/en/us/td/docs/security/ise/end-user-documentation/Cisco_ISE_End_User_Documentation.html

通信、服务和其他信息

- 要及时从思科收到相关信息，请注册[思科配置文件管理器](#)。
- 要使用重要技术实现您期望实现的业务影响，请访问[思科服务](#)。
- 要提交服务请求，请访问[思科支持](#)。
- 要了解并浏览安全且经过验证的企业级应用、产品、解决方案和服务，请访问[思科 DevNet](#)。
- 要获取一般网络、培训和认证主题相关的信息，请访问[思科出版社](#)。
- 要查找有关特定产品或产品系列的保修信息，请访问[思科保修服务查找工具](#)。

思科漏洞搜索工具

[思科漏洞搜索工具 \(BST\)](#) 是通往思科漏洞跟踪系统的网关，该系统包含一个关于思科产品和软件的缺陷和漏洞的综合列表。BST 提供关于您的产品和软件的详细漏洞信息。

文档反馈

要提供有关思科技术文档的反馈，请使用每个在线文档右窗格中提供的反馈表。



第 2 章

为升级做好准备

- 为升级做好准备，第 7 页
- 运行状况检查，第 8 页
- 加快升级速度与提高升级效率指南，第 8 页
- 验证数据以防止升级失败，第 10 页
- 在存在同名预定义授权复合条件的情况下，更改授权简单条件的名称，第 12 页
- 更改 VMware 虚拟机访客操作系统和设置，第 13 页
- 删除发起人组名称中的非 ASCII 字符，第 13 页
- 必须开放用于通信的防火墙端口，第 13 页
- 从主管理节点备份思科 ISE 的配置和运行数据，第 13 页
- 从主管理节点备份系统日志，第 14 页
- CA 证书链，第 15 页
- 检查证书有效性，第 15 页
- 删除证书，第 15 页
- 导出证书和私钥，第 16 页
- 升级前禁用 PAN 自动故障切换和禁用计划备份，第 16 页
- 配置 NTP 服务器和验证可用性，第 17 页
- 升级虚拟机，第 17 页
- 记录分析器的配置，第 17 页
- 获取 Active Directory 和内部管理员帐户凭证，第 18 页
- 升级前激活 MDM 供应商，第 18 页
- 创建存储库并复制升级捆绑包，第 18 页
- 检查可用磁盘大小，第 19 页
- 检查负载均衡器配置，第 19 页
- 日志保留和调整 MnT 硬盘大小，第 19 页

为升级做好准备

开始升级之前，请确保要执行以下任务：

运行状况检查

确保在升级过程之前对思科 ISE 部署运行运行状况检查，以便识别和解决可能导致升级停机的任何关键问题。有关详细信息，请参阅思科 ISE 管理员指南中“[故障排除](#)”一章中的[运行状况检查](#)部分。

加快升级速度与提高升级效率指南

以下准则可帮助您解决在升级过程中可能遇到的当前部署问题。因此，减少了整体升级停机时间，同时提高了效率。

- 在开始升级之前，先在现有版本中升级到最新的补丁。



注释 如果您从思科 ISE 版本 2.6 补丁 10 及更高版本 或 2.7 补丁 4 及更高版本升级，并配置了 SSM 本地部署服务器，则必须在开始升级过程之前断开 SSM 本地部署服务器。

- 我们建议您在模拟环境下测试升级，以便在升级生产网络之前发现并修复任何升级问题。
- 思科 ISE 部署中的所有节点都应处于同一补丁级别，以便交换数据。



注释 如果部署中的所有节点都不是同一思科 ISE 版本和补丁版本，您将收到一条警告消息：**Upgrade cannot begin**。此消息表明升级处于受阻状态中。请在开始升级之前确保部署中的所有节点版本（包括补丁版本，如果有）相同。

- 根据部署中的 PSN 数量和人员可用性，您可以安装需要升级到的思科 ISE 的最终版本，应用最新的补丁并使其保持就绪状态。
- 如果要恢复 MnT 日志，请对 MnT 节点执行上述任务，并将新部署作为 MnT 节点加入。但是，如果您不需要保留操作日志，可以通过重新映像 MnT 节点来跳过此步骤。
- 如果您有多节点部署，则可以并行完成思科 ISE 安装，而不影响生产部署。并行安装 ISE 服务器可节省时间，尤其是在使用先前版本的备份和恢复时。
- 可以将 PSN 添加到新部署，以便在注册过程中从 PAN 下载现有策略。使用 [ISE 延迟和带宽计算器](#) 了解思科 ISE 部署中的延迟和带宽要求。
- 最佳做法是存档旧日志，而不将其传输到新部署。这是因为，如果您稍后更改 MnT 角色，在 MnT 中恢复的操作日志不会同步到不同的节点。
- 如果您有两个完全分布式部署的数据中心 (DC)，请先升级备份 DC 并测试使用案例，然后再升级主 DC。

- 升级前先将升级软件下载并存储在本地存储库中，以加快升级速度。
- 如果您当前正在升级到思科 ISE 版本 3.0 或更高版本，则可以在启动升级过程之前使用运行状况检查或升级就绪工具 (URT) 运行系统诊断。
- 在开始升级过程之前，使用升级就绪性工具 (URT) 来检测和修复任何配置数据升级问题。大多数升级失败的原因是存在配置数据升级问题。在升级之前使用 URT 验证数据，以便尽可能发现、报告或修复问题。URT 可作为单独的可下载捆绑包下载，可在辅助策略管理节点或独立节点上运行。运行此工具不会造成停机时间。以下视频解释了如何使用 URT：
<https://www.cisco.com/c/en/us/td/docs/security/ise/videos/urt/v1-0/cisco-urt.html>



警告 请勿在主策略管理节点上运行 URT。URT 工具不会模拟 MnT 运营数据升级。

- 使用 GUI 升级思科 ISE 时，请注意每个节点的进程超时时间为 4 小时。如果该过程超过四个小时，则升级失败。如果使用升级就绪工具 (URT) 进行升级需要四个多小时，思科建议您使用 CLI 执行此过程。
- 在更改配置之前备份负载均衡器。您可以在升级过程中将 PSN 从负载均衡器中删除，然后在升级完成后进行重新添加。
- 在升级过程中禁用 PAN 自动故障切换（如果已配置）并禁用 PAN 之间的检测信号。
- 检查现有的策略和规则并删除过时、冗余和过期的策略和规则。
- 删除不必要的监控日志和终端数据。
- 您可以备份配置和运行日志并将其存储在未联网的临时服务器上。您可以在升级过程中使用远程日志记录目标。

您可以在升级后使用以下选项，以减少发送至 MnT 节点的日志数量并提高性能：

- 使用 MnT 收集筛选器（要查看此处窗口，请单击菜单图标 (☰)，然后选择 管理 > 系统 > 日志记录 > 收集过滤器）筛选进入的日志，避免 AAA 日志中出现重复的条目。
- 您可以创建远程日志记录目标（要查看此处窗口，请单击菜单图标 (☰)，然后选择 管理 > 系统 > 日志记录 > 远程日志记录目标）并将各个日志记录类别路由到特定的日志记录目标（要查看此处窗口，请单击菜单图标 (☰)，然后选择 系统 > 日志记录 > 日志记录类别）。
- 启用 忽略重复更新 选项。要查看此处窗口，请单击菜单图标 (☰)，然后选择 管理 > 系统 > 设置 > 协议 > RADIUS 窗口以避免重复更新。
- 下载并使用最新的升级捆绑包进行升级。在漏洞搜索工具中使用以下查询，找到未解决和已修复的升级相关缺陷：<http://cs.co/ise-upgrade-bugsearch>
- 使用较少的用户测试新部署的所有使用案例，以确保服务连续性。

验证数据以防止升级失败

在开始升级过程之前，您可以运行思科 ISE 提供的升级就绪工具 (URT) 检测和修复任何数据升级问题。

大多数升级失败的原因是存在数据升级问题。URT 旨在在升级之前验证数据，以便在任何可能的情况下识别，以及报告或修复问题。

URT 可作为单独的可下载捆绑包下载，它可在辅助管理节点上运行以获得高可用性并通过多个节点进行其他部署，也可在独立节点上运行以实现单节点部署。运行此工具时不会造成停机。



警告 在多节点部署中，请勿在主策略管理节点上运行 URT。

您可以通过思科 ISE 节点的命令行界面运行 URT。URT 执行以下操作：

1. 检查 URT 是否运行受支持的思科 ISE 版本。支持的版本包括版本 2.4、2.6 和 2.7。
2. 验证 URT 是在思科 ISE 独立节点上运行，还是在辅助策略管理节点（辅助 PAN）上运行
3. 检查 URT 捆绑包是不是在 45 天内生成的 - 执行这项检查是为了确保您使用的 URT 捆绑包是最新的
4. 检查是否满足所有必备条件。

URT 会检查以下必备条件：

- 版本兼容性
- 角色检查
- 磁盘空间



注释 使用 [磁盘要求大小 \(Disk Requirement Size\)](#) 来验证可用磁盘大小。如果需要增加磁盘大小，请重新安装 ISE 并恢复配置备份。

- NTP 服务器
- 内存
- 系统和受信任的证书验证

5. 克隆配置数据库
6. 将最新升级文件复制到升级捆绑包



注释 如果 URT 捆绑包中没有补丁，则输出将返回：不可用 (N/A)。这是安装热补丁时的预期行为。

7. 在克隆数据库上执行架构和数据升级

- （如果克隆数据库升级成功）提供完成升级所需的时间预估。
- （如果升级成功）删除克隆的数据库。
- （如果克隆数据库升级失败）收集所需的日志，提示加密码密码，生成日志捆绑包并将其存储在本地磁盘上。

下载并运行升级就绪工具

升级就绪性工具 (URT) 会在您实际运行升级之前验证配置数据，以确定可能会导致升级失败的任何问题。

开始之前

运行 URT 时，确保不要同时：

- 备份或恢复数据
- 执行任何角色更改

步骤 1 创建存储库并复制 URT 捆绑包，第 11 页

步骤 2 运行升级就绪工具，第 12 页

创建存储库并复制 URT 捆绑包

创建存储库并复制 URT 捆绑包。有关如何创建存储库的信息，请参阅《思科 ISE 管理员指南》中“维护和监控”一章中的“创建存储库”。

我们建议您使用 FTP，以实现更好的性能和可靠性。请勿使用低速 WAN 链路上的存储库。我们建议您使用离节点更近的本地存储库。

开始之前

确保您与存储库有良好的带宽连接。

步骤 1 从 Cisco.com ([ise-urtbundle-3.1.xxx-1.0.0.SPA.x86_64.tar.gz](#)) 下载 URT 捆绑包。

步骤 2 （可选）为了节省时间，请使用以下命令将 URT 捆绑包复制到思科 ISE 节点上的本地磁盘：

```
copy repository_url/path/ise-urtbundle-3.1.xxx-1.0.0.SPA.x86_64.tar.gz disk:/
```

例如，如果您想要使用 SFTP 复制升级捆绑包，可以执行以下操作：

```
(Add the host key if it does not exist) crypto host_key add host mySftpserver  
copy sftp://aaa.bbb.ccc.ddd/ ise-urtbundle-3.1.xxx-1.0.0.SPA.x86_64.tar.gz disk:/
```

aaa.bbb.ccc.ddd 是 SFTP 服务器的 IP 地址或主机名，而 ise-urtbundle-3.1.xxx-1.0.0.SPA.x86_64.tar.gz 是 URT 捆绑包的名称。

运行升级就绪工具

升级就绪工具可以识别可能会导致升级失败的数据问题，并在任何可能的情况下报告或修复问题。要运行 URT，请执行以下操作：

开始之前

将 URT 捆绑包复制到本地磁盘可以节省时间。

输入 **application install** 命令以安装 URT：

```
application install ise-urtbundle-3.1.0.x.SPA.x86_64.tar.gz reponame
```

如果在上述执行期间未成功安装应用，则 URT 会返回升级失败的原因。您需要修复问题并重新运行 URT。

在存在同名预定义授权复合条件的情况下，更改授权简单条件的名称

思科 ISE 具有多个预定义的授权复合条件。如果旧部署中的授权简单条件（用户定义）的名称与预定义授权复合条件的名称相同，升级过程会失败。在升级之前，请确保重命名具有以下任意预定义授权复合条件名称的授权简单条件：

- Compliance_Unknown_Devices
- Non_Compliant_Devices
- Compliant_Devices
- Non_Cisco_Profiled_Phones
- Switch_Local_Web_Authentication
- Catalyst_Switch_Local_Web_Authentication
- Wireless_Access
- BYOD_is_Registered
- EAP-MSCHAPv2
- EAP-TLS
- Guest_Flow

- MAC_in_SAN
- Network_Access_Authentication_Passed

更改 VMware 虚拟机访客操作系统和设置

如果要在虚拟机上升级思科 ISE 节点，请确保将访客操作系统更改为支持的 Red Hat Enterprise Linux (RHEL) 版本。要执行此操作，必须关闭虚拟机，更新访客操作系统，并在更改完之后再打开虚拟机。

RHEL 7 仅支持 E1000 和 VMXNET3 网络适配器。请务必在升级之前更改网络适配器类型。

删除发起人组名称中的非 ASCII 字符

在版本 2.2 之前的版本中，如果您使用非 ASCII 字符创建发起人组，则在升级之前，请务必重命名发起人组，仅使用 ASCII 字符。

思科 ISE 版本 2.2 及更高版本不支持发起人组名称中包含非 ASCII 字符。

必须开放用于通信的防火墙端口

如果您在主管理节点与任何其他节点之间部署了防火墙，则升级前必须开放以下端口：

- TCP 1521 - 用于主管理节点与监控节点之间的通信。
- TCP 443 - 用于主管理节点与所有其他辅助节点之间的通信。
- TCP 12001 - 用于全局群集复制。
- TCP 7800 和 7802 - (仅在节点组中包含策略服务节点时适用) 用于 PSN 组群集。

如需 Cisco ISE 所使用端口的完整列表，请参阅[思科身份服务引擎硬件安装指南](#)。

如需思科 ISE 所使用端口的完整列表，请参阅《[思科 ISE 端口参考](#)》。

从主管理节点备份思科 ISE 的配置和运行数据

从命令行界面 (CLI) 或 GUI 获取思科 ISE 配置和运行数据的备份。CLI 命令为：

```
backup backup-name repository repository-name {ise-config | ise-operational} encryption-key {hash | plain} encryption-keyname
```



注释 当思科 ISE 在 VMware 上运行时，不支持用 VMware 快照备份 ISE 数据。

VMware 快照在特定时间保存 VM 的状态。在多节点思科 ISE 部署中，所有节点中的数据都与当前数据库信息保持同步。恢复快照可能会导致数据库复制和同步问题。建议您使用思科 ISE 中包含的备份功能来存档和恢复数据。

使用 VMware 快照备份 ISE 数据将导致停止思科 ISE 服务。需要重启才能激活 ISE 节点。

您还可以从思科 ISE 管理门户获取思科 ISE 配置和运行数据的备份。确保您已创建存储备份文件的存储库。不要使用本地存储库进行备份。您无法在远程监控节点的本地存储库中备份监控数据。系统不支持以下存储库类型：CD-ROM、HTTP、HTTPS 或 TFTP。这是因为，这些存储库类型为全部只读或者其协议均不支持文件列表。

1. 选择管理 (Administration) > 维护 (Maintenance) > 备份和恢复 (Backup and Restore)。
2. 在思科 ISE GUI 中，单击菜单图标 (☰)，然后选择管理 (Administration) > 维护 (Maintenance) > 备份和恢复 (Backup and Restore)。
3. 单击立即备份 (Backup Now)。
4. 根据需要输入值以执行备份。
5. 单击确定 (OK)。
6. 验证备份是否成功完成。

在分布式部署中，不要在备份运行时更改节点角色或升级节点。如果并发运行备份，则更改节点角色会关闭所有进程，并可能导致数据不一致。在进行任何节点角色更改之前，请等待备份完成。

思科 ISE 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 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。



注释 利用思科 ISE，您可以从 ISE 节点 (A) 获取备份并将其恢复到另一个 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。

从主管理节点备份系统日志

从命令行界面 (CLI) 获取主管理节点系统日志的备份。CLI 命令为：

```
backup-logs backup-name repository repository-name encryption-key { hash | plain } encryption-key
name
```

CA 证书链

在升级到思科 ISE 3.1 之前，请确保内部 CA 证书链有效。

1. 在思科 ISE GUI 中，单击菜单图标 (☰)，然后选择 **管理 > 系统 > 证书 > 证书颁发机构证书**
2. 对于部署中的每个节点，请选择 **友好名称** 列中包含 **证书服务终端从属 CA** 的证书。单击 **查看** 并检查是否显示 **证书状态良好** 消息。
3. 如果任何证书链已损坏，您必须在升级思科 ISE 之前修复该问题。要查看此处窗口，请单击菜单图标 (☰)，然后选择 **管理 > 系统 > 证书 > 证书管理 > 证书签名要求 > ISE 根 CA**

检查证书有效性

如果思科 ISE 受信任证书或系统证书库中的任何证书已过期，升级过程会失败。在受信任的证书 (**Trusted Certificates**) 和系统证书 (**System Certificates**) 的到期日期 (**Expiration Date**) 字段中（要查看此处窗口，请单击菜单图标 (☰)，然后选择 **管理 (Administration) > 系统 (System) > 证书 (Certificates) > 证书管理 (Certificate Management)**）检查有消息，如有必要，则在升级前进行续订。

此外，请在 **CA 证书 (CA Certificates)** 窗口中的证书到期日期 (**Expiration Date**) 字段中（要查看此处窗口，请单击菜单图标 (☰)，然后选择 **管理 (Administration) > 系统 (System) > 证书 (Certificates) > 证书颁发机构 (Certificate Authority) > 证书颁发机构证书 (Certificate Authority Certificates)**）检查有效性，如有必要，则在升级前进行续订。

删除证书

要删除过期的证书，请执行以下步骤：

步骤 1 在思科 ISE GUI 中，单击菜单图标 (☰)，然后选择 **管理 > 系统 > 证书 > 证书管理 > 系统证书**。

步骤 2 选择过期的证书。

步骤 3 单击删除 (**Delete**)。

步骤 4 在思科 ISE GUI 中，单击菜单图标 (☰)，然后选择 **管理 > 系统 > 证书 > 证书管理 > 受信任证书**。

步骤 5 选择过期的证书。

步骤 6 单击删除 (**Delete**)。

步骤 7 选择 **管理 (Administration) > 系统 (System) > 证书 (Certificates) > 证书颁发机构 (Certificate Authority) > 证书颁发机构证书 (Certificate Authority Certificates)**。

步骤 8 选择过期的证书。

步骤 9 单击删除。

导出证书和私钥

我们建议您：

- 从部署的所有节点将全部本地证书及其私钥导出到安全的位置。记录证书的配置（该证书用于何种服务）。

步骤 1 在思科 ISE GUI 中，单击菜单图标 (☰)，然后选择管理 > 系统 > 证书 > 证书管理 > 系统证书

步骤 2 选择的证书，并单击 **Export**。

步骤 3 选择导出证书和私钥单选按钮。

步骤 4 输入私钥密码和确认密码。

步骤 5 单击 **Export**。

-
- 从主管理节点的受信任证书库导出全部证书。记录证书的配置（该证书用于何种服务）。

步骤 1 在思科 ISE GUI 中，单击菜单图标 (☰)，然后选择管理 > 系统 > 证书 > 证书管理 > 系统证书

步骤 2 选择的证书，并单击 **Export**。

步骤 3 单击保存文件以导出证书。

步骤 4 在思科 ISE GUI 中，单击菜单图标 (☰)，然后选择管理 > 系统 > 证书 > 证书颁发机构 > 证书颁发机构证书

步骤 5 选择的证书，并单击 **Export**。

步骤 6 选择导出证书和私钥单选按钮。

步骤 7 输入私钥密码和确认密码。

步骤 8 单击 **Export**。

步骤 9 单击保存文件以导出证书。

升级前禁用 PAN 自动故障切换和禁用计划备份

在思科 ISE 中运行备份时，无法执行部署更改。因此，为了确保自动配置不会影响升级过程，您必须将其禁用。确保在升级思科 ISE 前禁用了以下配置：

- 主管理节点自动故障切换 - 如果您已配置主管理节点进行自动故障切换，请确保在升级思科 ISE 前禁用自动故障切换选项。
- 计划备份 - 当计划部署升级时，请在升级后重新计划备份。您可以选择禁用备份计划，并在升级后重新创建这些计划。

计划运行一次的备份在思科 ISE 应用每次重启时都会触发。因此，如果您将备份计划配置为仅运行一次，请务必在升级前将其禁用。

配置 NTP 服务器和验证可用性

升级过程中，思科 ISE 节点会重启、进行迁移并将数据从主管理节点复制到辅助管理节点。对于这些操作而言，网络中的 NTP 服务器配置正确且可以建立连接这一点非常重要。如果 NTP 服务器未设置正确或无法建立连接，升级过程会失败。

确保您的网络中的 NTP 服务器可以在升级过程中可建立连接、可响应且可同步。

思科 ISE 版本 2.7 及更高版本使用 `chrony` 而不是网络时间协议后台守护程序 (`ntpd`)。Ntpd 可与具有 10 秒以下根分散的服务器同步，而 `chrony` 可与具有 3 秒以下根分散的服务器同步。因此，我们建议您在升级到思科 ISE 2.7 或更高版本之前，使用根分散较低的 NTP 服务器，以避免 NTP 服务中断。有关详细信息，请参阅 [Microsoft Windows 上的 ISE 和 NTP 服务器同步故障排除](#)。

升级虚拟机

思科 ISE 软件必须与芯片和设备容量同步，以支持 UCS 硬件中可用的最新 CPU/内存容量。随着 ISE 版本的发展，对旧硬件的支持将被逐步淘汰，并引入更新的硬件。最好升级虚拟机 (VM) 容量以获得更好的性能。在规划 VM 升级时，我们强烈建议使用 OVA 文件安装 ISE 软件。每个 OVA 文件都是一个包，其中包含用于描述 VM 的文件，并在设备上保留思科 ISE 软件安装所需的硬件资源。

有关 VM 和硬件要求的详细信息，请参阅 [思科身份服务引擎安装指南](#) 中的“硬件和虚拟设备要求”

思科 ISE VM 需要 VM 基础设施中的专用资源。ISE 需要足够数量的 CPU 核心，类似于硬件设备，以实现性能和扩展。发现资源共享会影响 CPU 的性能、用户身份验证延迟、注册、延迟和丢弃日志、报告、控制面板响应等。这会直接影响企业中的最终用户和管理员用户体验。



注释 在升级期间，请务必使用预留的 CPU、内存和硬盘空间资源，而不是共享资源。

思科 ISE 版本 2.4 及更高版本要求虚拟机的最小磁盘大小为 300GB，因为本地磁盘分配已增加到 29GB。

记录分析器的配置

如果您使用分析器服务，请确保为管理员门户中的每个策略服务节点记录分析器的配置（要查看此处窗口，请单击菜单图标 (☰)，然后选择 **管理 > 系统 > 部署 > <节点>**）。选择节点，然后单击 **编辑节点**。在 **编辑节点** 页面中，转到 **分析配置** 选项卡。您可以记录该配置信息或获取屏幕截图。

获取 Active Directory 和内部管理员帐户凭证

如果您使用 Active Directory 作为外部身份源，请确保具有 Active Directory 凭证以及有效的内部管理员帐户凭证。升级后，可能会丢失 Active Directory 连接。如果发生这种情况，您需要具有用于登录管理员门户的 ISE 内部管理员帐户，以及用于在 Active Directory 中加入 Cisco ISE 的 Active Directory 凭证。

升级前激活 MDM 供应商

如果您使用 MDM 功能，则应在升级前确保 MDM 供应商为激活状态。

如果授权策略中使用了 MDM 服务器的名称并且相应的 MDM 服务器处于禁用状态，升级过程会失败。可以执行以下操作之一，解决此问题：

1. 在升级前启用 MDM 服务器。
2. 将使用 MDM 服务器名称属性的条件从授权策略中删除。

创建存储库并复制升级捆绑包

创建存储库，以获取备份并复制升级捆绑包。有关如何创建存储库的信息，请参阅《思科 ISE 管理员指南》中“维护和监控”一章中的“创建存储库”。

我们建议您使用 FTP，以实现更好的性能和可靠性。请勿使用低速 WAN 链路上的存储库。我们建议您使用离节点更近的本地存储库。

确保到存储库的互联网连接正常。



注释 当您从存储库下载升级捆绑包到节点时，如果需要超过 35 分钟才能完成，则下载时间超时。出现这个问题的原因是互联网带宽连接不佳。

将升级捆绑包复制到本地磁盘可以节约升级过程的时间。或者，您可以使用 **application upgrade prepare <upgrade bundle name> <repository name>** 命令将升级捆绑包复制到本地磁盘并解压缩。



注释

- 确保您与存储库有良好的带宽连接。当您从存储库下载升级捆绑包（文件大小约 9GB）到节点时，如果需要超过 35 分钟才能完成，则下载时间超时。
- 如果使用本地磁盘存储配置文件，则执行升级时将删除这些文件。因此，我们建议您创建思科 ISE 存储库并将文件复制到此存储库。

您可以从 [Cisco.com](https://www.cisco.com) 下载升级捆绑包。

要升级到版本 3.1，请使用以下升级捆绑包：`ise-upgradebundle-2.x-to-3.1.0.xxx.SPA.x86_64.tar.gz`

为进行升级，您可使用以下命令将升级捆绑包复制到思科 ISE 节点的本地磁盘：

```
copy repository_url/path/ise-upgradebundle-2.x-to-3.1.0.xxx.SPA.x86_64.tar.gz disk:/
```

例如，如果您想要使用 SFTP 复制升级捆绑包，可以执行以下操作：

1. （如果主机密钥不存在，请进行添加）`crypto host_key add host mySftpserver`
2. `copy sftp://aaa.bbb.ccc.ddd/ise-upgradebundle-2.x-to-3.1.0.xxx.SPA.x86_64.tar.gz disk:/`

`aaa.bbb.ccc.ddd` 是 SFTP 服务器的 IP 地址或主机名，而

`ise-upgradebundle-2.x-to-3.1.0.xxx.SPA.x86_64.tar.gz` 是升级捆绑包的名称。

检查可用磁盘大小


确保已为虚拟机分配所需的磁盘空间。有关详细信息，请参阅 [思科 ISE 安装指南](#)。如果需要增加磁盘大小，请重新安装 ISE 并恢复配置备份。

检查负载均衡器配置

如果您在主管节点 (PAN) 和策略服务节点 (PSN) 之间使用任何负载均衡器，请确保负载均衡器上配置的会话超时不会影响升级过程。如果会话超时设置为较低的值，它可能会影响负载均衡器后方的 PSN 上的升级过程。例如，如果在 PAN 到 PSN 的数据库转储期间出现会话超时，则 PSN 上的升级过程可能会失败。

日志保留和调整 MnT 硬盘大小

升级不需要更改 MnT 磁盘容量。但是，如果您一直在填满日志并需要更大的硬件容量，则可以根据日志保留需求来规划 MnT 的硬盘大小。必须了解的是，日志保留容量已从思科 ISE 版本 2.2 增加了许多倍。

您还可以为来自不同设备的不必要的日志启用收集过滤器（要查看此处窗口，请单击 [菜单](#) 图标 ），然后选择 [管理 > 系统 > 日志记录 > 收集过滤器](#)），这些日志可能会使思科 ISE MnT 不堪重负。

有关收集过滤器的详细信息，请参阅 [《思科身份服务引擎管理员指南》](#) “维护和监控”一章中的“配置收集过滤器”部分

请参阅 [思科 ISE 性能和可扩展性社区](#) 页面下的 ISE 存储要求。该表根据 RADIUS 的终端数量和 TACACS+ 的网络设备数量列出了日志保留时间。应单独为 TACACS+ 和/或 RADIUS 计算日志保留时间。



第 3 章

执行升级

- [节点的升级顺序](#)，第 21 页
- [选择升级方法](#)，第 23 页
- [使用备份和恢复方法升级思科 ISE 部署](#)，第 26 页
- [通过 GUI 升级思科 ISE 部署](#)，第 29 页
- [通过 CLI 升级思科 ISE 部署](#)，第 40 页

节点的升级顺序

您可以使用 GUI、备份和恢复或 CLI 升级思科 ISE。如果您使用 GUI 进行升级，则可以选择要升级的节点的顺序。但是，我们建议您按照以下提供的节点顺序升级部署。这将帮助您减少停机时间，同时提供最大的恢复能力和回滚能力。

1. 备份所有配置和监控数据。您还应导出内部 CA 密钥和证书链的副本，并备份所有 ISE 节点的 ISE 服务器证书。此任务应在启动升级之前完成，以确保您可以在必要时轻松手动回滚。

2. 辅助管理节点

此时，主管理节点仍然是之前的版本，如果升级失败，可用于回滚。

3. 主监控节点或辅助监控节点

如果您有分布式部署，请升级具有现有思科 ISE 部署的辅助管理节点的站点中可用的所有节点。

4. 策略服务节点

如果您使用 GUI 从思科 ISE 版本 2.6 升级到更高版本，则可以选择一组要同时升级的 PSN。这将减少总体升级停机时间。

升级一系列策略服务节点后，请验证升级是否成功（请参阅[验证升级过程](#)，第 44 页）并运行必要的网络测试，以确保新部署运行正常。如果升级成功，就可以升级接下来的一组策略服务节点。

5. 辅助监控节点或主监控节点

6. 主管理节点

在您升级主管理节点后，重新进行升级验证和网络测试。



注释 如果在注册主管理节点（旧部署中要升级的最后一个节点）的过程中升级失败，升级会回滚，并且此节点会成为独立节点。在 CLI 中，将此节点作为独立节点进行升级。将此节点作为辅助管理节点注册到新部署中。

升级后，辅助管理节点成为主管理节点，原始主管理节点成为辅助管理节点。如有必要，在 Edit Node 窗口中，点击 **Promote to Primary** 即可将辅助管理节点升级为主管理节点（与旧部署中一样）。

如果管理节点还承担监控角色，请按照下表中给出的顺序进行升级：

| 当前部署中的节点角色 | 升级顺序 |
|--------------------------------|---|
| 辅助管理/主监控节点、策略服务节点、主管理/辅助监控节点 | <ol style="list-style-type: none"> 1. 辅助管理/主监控节点 2. 策略服务节点 3. 主管理/辅助监控节点 |
| 辅助管理/辅助监控节点、策略服务节点、主管理/主监控节点 | <ol style="list-style-type: none"> 1. 辅助管理/辅助监控节点 2. 策略服务节点 3. 主管理/主监控节点 |
| 辅助管理节点、主监控节点、策略服务节点、主管理/辅助监控节点 | <ol style="list-style-type: none"> 1. 辅助管理节点 2. 主监控节点 3. 策略服务节点 4. 主管理/辅助监控节点 |
| 辅助管理节点、辅助监控节点、策略服务节点、主管理/主监控节点 | <ol style="list-style-type: none"> 1. 辅助管理节点 2. 辅助监控节点 3. 策略服务节点 4. 主管理/主监控节点 |
| 辅助管理/主监控节点、策略服务节点、辅助监控节点、主管理节点 | <ol style="list-style-type: none"> 1. 辅助管理/主监控节点 2. 策略服务节点 3. 辅助监控节点 4. 主管理节点 |

| 当前部署中的节点角色 | 升级顺序 |
|--------------------------------|---|
| 辅助管理/辅助监控节点、策略服务节点、主监控节点、主管理节点 | <ol style="list-style-type: none"> 1. 辅助管理/辅助监控节点 2. 策略服务节点 3. 主监控节点 4. 主管理节点 |

在以下情况下，您将收到错误消息：**No Secondary Administration Node in the Deployment**

- 部署中没有辅助管理节点。
- 辅助管理节点已关闭。
- 辅助管理节点已完成升级并移动到升级后的部署中。当您在完成辅助管理节点升级后使用 **Refresh Deployment Details** 选项时一般会出现此问题。

要解决此问题，请根据实际情况执行以下其中一个任务：

- 如果部署没有辅助管理节点，请配置辅助管理节点，然后重新尝试升级。
- 如果辅助管理节点已关闭，则启动节点，然后重新尝试升级。
- 如果辅助管理节点已升级并移动到升级后的部署中，请使用 CLI 手动升级部署中的其他节点。

选择升级方法

此版本的思科 ISE 支持以下升级过程。您可以从以下升级流程中进行选择，具体取决于您的技术专业知识和升级时间。

- 使用备份和恢复程序升级思科 ISE（推荐）
- 通过 GUI 升级思科 ISE 部署
- 通过 CLI 升级思科 ISE 部署

表 2: 思科 ISE 升级方法比较

| 比较因素 | 备份和恢复（推荐） | 使用 GUI 升级 | 使用 CLI 升级 |
|------|------------------|------------------|------------------|
| 比较概要 | 快速，但需要更多管理 | 时间长，但所需的管理更少 | 需要更长的时间和更多的管理 |
| 难度 | 困难 | 容易 | 中等 |
| 最低版本 | 思科 ISE 2.6 及更高版本 | 思科 ISE 2.6 及更高版本 | 思科 ISE 2.6 及更高版本 |

| 比较因素 | 备份和恢复（推荐） | 使用 GUI 升级 | 使用 CLI 升级 |
|------|-------------------------------------|--------------------------|------------------------------|
| VM | 如果您有足够的容量，则可以预先安排新的虚拟机并立即将其加入新的 PAN | 每个 PSN 按顺序升级，这会线性增加总升级时间 | 每个 PSN 都会升级，但可以并行完成，以减少总升级时间 |
| 时间 | 最短升级停机时间，因为 PSN 使用新版本进行映像而不是升级 | 每个 PSN 按顺序升级，这会线性增加总升级时间 | 每个 PSN 都会升级，但可以并行完成，以减少总升级时间 |
| 人员 | 跨业务部门的多个利益相关者参与传输配置设置和操作日志。 | 自动升级过程，减少手动干预 | 思科 ISE 的技术专业知识。 |
| 回滚 | 需要重新映像节点。 | 轻松回滚选项。 | 轻松回滚选项。 |

升级方法的详细比较如下：

使用备份和恢复方法升级思科 ISE

思科 ISE 节点的重新映像可在初始部署和故障排除期间完成，但您也可以重新映像思科 ISE 节点以升级部署，同时在新版本发布后将策略恢复到新部署已部署。

如果资源有限，并且新部署无法启动并行 ISE 节点，则会从生产部署中删除辅助 PAN 和 MnT，然后再升级其他节点。节点移至新部署；配置和操作备份从相应节点上的先前部署恢复，从而创建并行部署。这允许将策略集、自定义配置文件、网络访问设备和终端恢复到新的部署中，而无需手动干预。

使用备份和恢复流程升级思科 ISE 的优势如下：

- 您可以从之前的 ISE 部署恢复配置设置和操作日志。因此，防止数据丢失。
- 您可以手动选择应重新用于新部署的节点。
- 您可以并行升级多个 PSN，从而减少升级停机时间。
- 您可以在维护窗口之外暂存节点，从而减少生产期间的升级时间。

使用“备份和恢复”功能升级思科 ISE 之前需要考虑的事项

所需资源： 备份和恢复升级过程需要额外的资源，这些资源可以在释放之前为 ISE 部署预留。在重复使用现有硬件的情况下，需要将额外的负载均衡到保持在线状态的节点上。因此，您需要在部署开始之前评估当前负载和延迟限制，以确保部署可以处理每个节点的用户数量增加。

所需人员： 您将需要多个业务部门（包括网络管理、安全管理、数据中心和虚拟化资源）的参与才能执行升级。此外，您需要将节点重新加入新部署，恢复证书，重新加入 Active Directory，并等待策略同步。这可能会导致多次重新加载，并且需要网络新部署的时间范围。

回滚机制： 由于节点的重新映像，所有信息和配置设置都将从之前的部署中清除。因此，备份和恢复升级的回滚机制与第二次重新映像节点的过程相同。

备份和恢复升级过程的最佳实践：

- 创建独立环境或专用负载均衡器来切换 RADIUS 请求的虚拟 IP 地址。
- 您可以在维护窗口之前启动部署过程，并将用户负载均衡器指向新部署。

通过 GUI 升级思科 ISE 部署

您还可以使用一些可自定义的选项从 GUI 中点击一下升级思科 ISE。在思科 ISE GUI 中，单击菜单图标 (☰)，然后选择 **ISE 管理 > 升级**。创建新存储库以下载 ISO 映像。

在升级过程中，辅助 PAN 会自动移至升级后的部署中，并首先升级主 MnT。因此，如果其中任何一个升级失败，则必须将节点回滚到之前的版本并重新加入之前的 ISE 部署。稍后 PSN 将逐个移至新部署并升级。如果升级失败，您还可以选择继续或停止升级。这将导致同一思科 ISE 部署的双版本，允许在继续升级之前进行故障排除。升级所有 PSN 后，辅助 MnT 和主 PAN 将升级并加入新的思科 ISE 部署。

鉴于此升级过程需要的技术专业知识有限，一名管理员开始升级并指派 NOC 或 SOC 工程师监控和报告升级状态或提交 TAC 支持案例。

从 GUI 升级思科 ISE 的优势如下：

- 升级是自动化的，干预最少。
- 您可以选择 PSN 的升级顺序，以确保连续性，尤其是在数据中心之间存在冗余时。
- 单个管理员无需任何额外人员、第三方虚拟机监控程序或网络接入设备即可执行升级。

从 GUI 升级思科 ISE 之前要考虑的事项

失败场景下的继续： 如果升级失败，您还可以选择继续或停止升级。这将导致同一思科 ISE 部署的双版本，允许在继续升级之前进行故障排除。虽然思科升级就绪工具应指示任何不兼容或错误配置，但如果选中“继续”字段，则如果在升级前未执行尽职调查，则可能会遇到其他错误。

回滚机制： 如果 PAN 或 MnT 节点上的升级失败，则节点会自动回滚。但是，如果 PSN 升级失败，则节点将保留在同一思科 ISE 版本上，并且可以在损害冗余的同时进行修复。在此期间，思科 ISE 仍在运行，因此在不重新映像的情况下，回滚功能会受到限制。

所需时间： 每个 PSN 升级大约需要 90-120 分钟，因此，如果您有大量 PSN，则需要时间来升级所有 PSN。

从 GUI 升级的最佳实践： 如果您有大量的 PSN，请将 PSN 分组并执行升级。

通过 CLI 升级思科 ISE 部署

从 CLI 升级思科 ISE 是一个复杂的过程，需要管理员将升级映像下载到本地节点，执行升级，并在整个升级过程中单独监控每个节点。虽然升级顺序在本质上与 GUI 升级类似，但从监控和操作的角度来看，这种方法需要大量操作。

由于所需的工作量，建议仅出于故障排除目的从 CLI 升级。

从 CLI 升级思科 ISE 的优势如下：

- 执行升级时，CLI 会向管理员显示其他日志记录消息。

- 可以选择具有更多控制权并并行升级的升级节点。未升级的节点可以在整个部署中重新平衡终端时处理额外的负载。
- 由于能够指示脚本撤消以前的更改，因此在 CLI 中回滚要容易得多。
- 由于映像驻留在本地节点上，因此可以消除 PAN 和 PSN 之间的复制错误（如果有）。

从 CLI 升级思科 ISE 之前需要考虑的事项

您需要技术专业知识和更长的时间才能使用 CLI 升级思科 ISE。

使用备份和恢复方法升级思科 ISE 部署

备份和恢复升级方法概述

我们建议使用备份和恢复升级过程，而不是其他升级过程，因为它有助于恢复当前的思科 ISE 部署节点设置，并在升级过程中出现任何损坏时防止数据丢失。此程序首先创建现有思科 ISE 部署的配置和操作备份，然后将其应用于新部署。

备份和恢复升级过程的最佳实践：

- 创建独立环境或专用负载均衡器来切换 RADIUS 请求的虚拟 IP 地址。
- 您可以在维护窗口之前启动部署过程，并将用户负载均衡器指向新部署。
- 如果使用 RSA SecurID 身份源，则在添加新的 PSN 时，必须在 RSA 身份验证管理器的主实例中生成包含所有 PSN 的新配置文件。



注释 为避免每次添加新的 PSN 时都生成新的 RSA 配置，在开始备份和恢复过程之前，必须知道要添加到部署中的所有节点的 IP 地址。然后，您必须使用所有 IP 地址生成 RSA 配置文件，并将其上传到 PAN UI。

操作步骤：

1. 在 RSA 身份验证管理器安全控制台主实例上生成身份验证管理器配置文件，其中包含所有节点的 IP 地址，包括不在部署中的节点。
2. 将新配置文件导入到 PAN UI。



注释 在上传新的 RSA 配置文件之前，必须清除 RSA 身份验证管理器上的节点密钥。这有助于创建新的节点密钥并在 ISE 和 RSA 身份验证管理器之间共享。

现在，您可以将新节点添加到部署，而无需生成新的配置文件，因为它会使用已导入的配置文件中的 IP 地址作为配置的一部分进行复制。

以下是“备份和恢复升级”方法中涉及的步骤的概述：

1. 取消注册节点

要从部署中删除节点，您需要取消注册该节点。有关取消注册或删除节点的详细信息，请参阅 [思科身份服务引擎管理员指南](#) 中的“从部署中删除节点”部分。

2. 重新映像节点

要重新映像思科 ISE 节点，必须先将其从部署中删除，然后继续安装思科 ISE。有关 思科 ISE 安装的更多信息，请参阅 [《Cisco 身份服务引擎安装指南》](#) 中的“安装 思科 ISE”一章。

我们建议您应用新安装的思科 ISE 版本的最新补丁。

3. 备份和恢复配置或操作数据库

有关备份和恢复操作的详细信息，请参阅 [思科身份服务引擎管理员指南](#) 中的“备份和恢复操作”部分。

4. 为节点分配主角色或辅助角色。

您可以根据需要为节点分配主要或辅助角色。

有关如何将角色分配给监控和故障排除 (MnT) 节点的详细信息，请参阅 [思科身份服务引擎管理员指南](#) 中的“手动修改 MnT 角色”部分。

5. 加入策略服务节点

要将策略服务节点 (PSN) 加入新部署，您需要将该节点注册为 PSN。有关注册或加入 PSN 的详细信息，请参阅 [思科身份服务引擎管理员指南](#) 中的“注册辅助思科 ISE 节点”部分。

6. 导入证书

您需要将系统证书导入到思科 ISE 中新部署的节点。有关如何将系统证书导入思科 ISE 节点的详细信息，请参阅 [思科身份服务引擎管理员指南](#) 中的“导入系统证书”部分。

备份和恢复升级过程

本节介绍使用推荐的备份和恢复升级方法的升级过程。

如果您正在使用 思科 ISE 版本 2.6 或更高版本，您可以直接升级到 思科 ISE 版本 3.1。

如果您使用的 思科 ISE 版本与 思科 ISE 3.1 版本不兼容，则需要首先升级到与 思科 ISE 3.1 版本兼容的中间版本。然后，您可以从中间版本升级到 思科 ISE 版本 3.1。请按照以下步骤升级到 思科 ISE 中间版本。

将辅助 PAN 和辅助 MnT 节点升级到思科 ISE 版本 2.6、2.7 或 3.0

开始之前

将备份从现有思科 ISE 恢复到中间思科 ISE 版本。如果您不想保留较早的报告数据，请跳过步骤 4 至 6。

-
- 步骤 1** 取消注册辅助 PAN 节点。
 - 步骤 2** 将已取消注册的辅助 PAN 节点作为独立节点重新映像到中间思科 ISE 版本。安装后，此节点会成为新部署中的主管理节点。
 - 步骤 3** 从备份数据恢复思科 ISE 配置。
 - 步骤 4** 取消注册辅助 PAN 节点。
 - 步骤 5** 将已取消注册的辅助 MnT 节点作为独立节点重新映像到中间思科 ISE 版本。
 - 步骤 6** 将主角色分配给此 MnT 节点，并从备份存储库恢复操作备份。这是一个可选步骤，仅当您需要报告较早的日志时才需要执行。
 - 步骤 7** 从原始思科 ISE 备份存储库导入 ise-https-admin CA 证书。
-

将辅助 PAN 和 MnT 节点升级到思科 ISE 版本 3.1

-
- 步骤 1** 备份思科 ISE 配置设置和操作日志。
 - 步骤 2** 取消注册辅助 PAN 节点。
 - 步骤 3** 将取消注册的辅助 PAN 节点重新映像到思科 ISE 版本 3.1。
 - 步骤 4** 从备份数据恢复 ISE 配置，并将此节点设置为新部署的主节点。
 - 步骤 5** 从此节点的备份导入 ise-https-admin CA 证书，除非您使用的是通配符证书。
 - 步骤 6** 取消注册辅助 PAN 节点。
 - 步骤 7** 将取消注册的辅助 MnT 节点重新映像到思科 ISE 版本 3.1。
 - 步骤 8** 恢复当前的 ISE 运行备份，并将节点作为主 MnT 加入新部署。这是一个可选步骤，仅当您需要报告较早的日志时才需要执行。
-

将策略服务节点加入思科 ISE 版本 3.1

如果您在多个站点部署了思科 ISE 节点，请先加入站点（具有辅助 PAN 和 MnT 节点）中可用的 PSN，然后加入其他站点中可用的 PSN（具有辅助 PAN 和 MnT 节点）现有思科 ISE 的主 PAN 和 MnT 节点）。

-
- 步骤 1** 取消注册 PSN。

步骤 2 将 PSN 重新映像到思科 ISE 版本 3.1 最新补丁，并将 PSN 加入新的思科 ISE 版本 3.1 部署。

下一步做什么

我们建议您此时测试部分升级的部署。您可以通过检查日志是否存在以及升级的节点功能来执行此操作。

将主 PAN 和 MnT 升级到思科 ISE 版本 3.1

步骤 1 重新映像主 MnT 节点并作为辅助 MnT 加入新部署。

如果要保留数据以进行报告，请将操作备份的副本恢复到辅助 MnT 节点。

步骤 2 重新映像主 PAN 节点并作为辅助 PAN 加入新部署。

通过 GUI 升级思科 ISE 部署

通过 GUI 升级思科 ISE 部署

通过 Cisco ISE，可以从管理门户执行基于 GUI 的集中式升级。升级过程是相当简单的，升级进度和节点状态显示在屏幕上。

选择 **Administration > System > Upgrade > Overview** 菜单选项列出了部署中的所有节点、这些节点上启用的角色、所安装 ISE 的版本以及节点的状态（指示节点是处于活动状态还是非活动状态）。只有在节点处于活动状态时，才能开始升级。

在思科 ISE GUI 中，单击 **菜单** 图标 (☰)，然后选择 **Administration > System > Upgrade > Overview** 菜单选项列出了部署中的所有节点、这些节点上启用的角色、所安装 ISE 的版本以及节点的状态（指示节点是处于活动状态还是非活动状态）。只有在节点处于活动状态时，才能开始升级。

仅当您当前使用 2.0 或更高版本并且希望升级到版本 2.0.1 或更高版本时，才支持从管理员门户进行基于 GUI 的升级。

您可以在 **Administration > System > Upgrade > Upgrade Selection** 窗口中选择以下选项之一来升级思科 ISE 部署：

- **完全升级：**完全升级是一个多步骤过程，可同时对思科 ISE 部署中的所有节点进行完整升级。与拆分升级过程相比，此方法将在更短的时间内升级部署。在此升级过程中，应用服务将关闭，因为所有节点都是并行升级的。
- **拆分升级：**拆分升级是一个多步骤过程，它可以升级思科 ISE 部署，同时允许在升级过程中保持服务可用。通过此升级方法，您可以选择要在部署中升级的思科 ISE 节点。



注释 思科 ISE 2.6 补丁 10 及更高版本、思科 ISE 2.7 补丁 4 及更高版本以及思科 ISE 3.0 补丁 3 及更高版本支持完全升级方法。拆分升级方法可以在任何受支持的思科 ISE 版本和补丁上执行。

虽然这些 GUI 升级方法从思科 ISE 2.6 补丁 10 开始可用，但您至少需要运行思科 ISE 2.7 补丁 4 才能升级到思科 ISE 3.2。

通过 GUI 全面升级思科 ISE 部署

通过 Cisco ISE，可以从管理门户执行基于 GUI 的集中式升级。全面升级是一个多步骤过程，可实现思科 ISE 部署的完整升级。

要执行思科 ISE 部署的完整升级，请执行以下操作：

步骤 1 在思科 ISE GUI 中，单击菜单图标 (☰)，然后选择 **管理 (Administration) > 系统 (System) > 升级 (Upgrade)**。

步骤 2 在升级选择窗口中，单击 **全面升级**，然后单击 **开始升级**。

步骤 3 在欢迎窗口中单击 **下一步** 以启动升级工作流程。

步骤 4 完成 **核对表** 窗口中列出的所有任务，以避免在升级过程中出现任何阻止程序或停机时间。

图 1: 显示核对表的升级窗口

The screenshot shows the Cisco ISE GUI Upgrade Checklist window. The breadcrumb path is Administration > System > Upgrade. The checklist includes the following tasks:

- Backup ISE**
 - Configuration and operational data (Administration > System > Backup & Restore)
 - Backup system logs (Operations > Troubleshoot > Download Logs)
 - Export certificates and private keys (Administration > System > Certificates > System Certificates)
- Software**
 - Review the ISE Upgrade Guide and Release Notes for upgrade information (<http://cisco.com/go/ise>)
 - Confirm valid ISE upgrade paths. Ensure that a repository is available to store the ISE upgrade bundle (Administration > System > Maintenance > Repository)
 - Download the ISE upgrade bundle and place it in the repository (ISE software is available at <http://cisco.com/go/ise>)
- Credentials**
 - Make a note of the Active Directory join credentials, and the RSA SecurID node secret, if applicable.
- Operational Data Purge**
 - Purge operational data to improve upgrade performance (Administration > System > Maintenance > Operational Data Purge)
- License**
 - Convert your old licenses to the new license types through the Cisco Smart Software Manager (CSSM).
 - Enable the new licenses in the Administration > System > Licensing window. Check the checkboxes for all your purchased licenses, and click Enable.

At the bottom, there is a checked checkbox "I have reviewed the checklist" and a "Print Checklist" button.

步骤 5 (可选) 点击 **打印核对表** 下载核对表以供参考。

步骤 6 选中 **我已查看核对表** 复选框，然后在验证升级核对表中列出的项目后点击 **下一步**。

屏幕上将显示 **准备升级** 窗口。

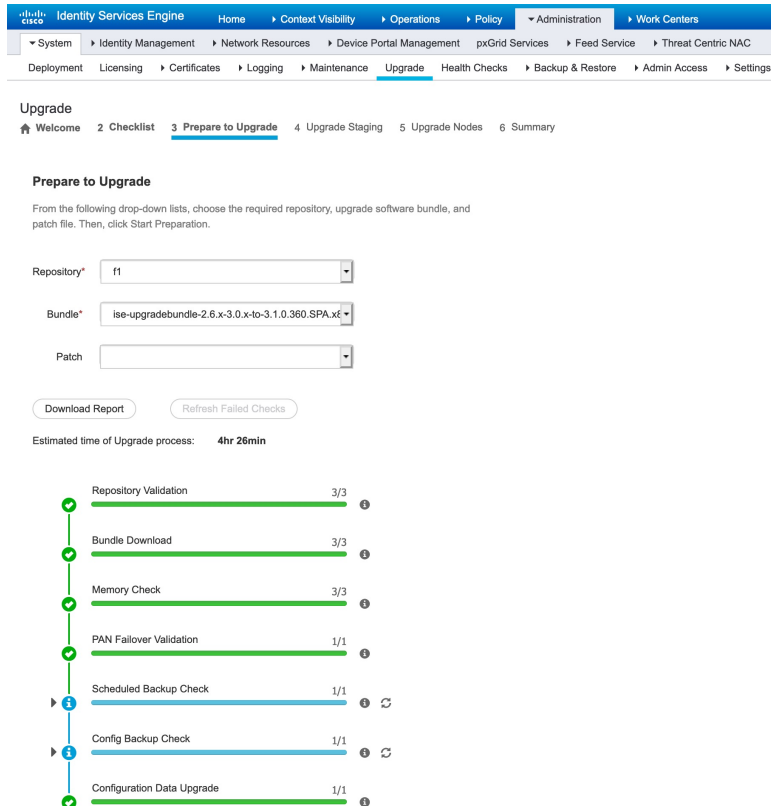
步骤 7 从 **存储库** 下拉列表中，选择存储升级捆绑包的存储库。

步骤 8 从 **捆绑包** 下拉列表中选择升级捆绑包。

步骤 9 所有 补丁版本都列在 **补丁** 下拉列表中。我们建议您为要升级到的思科 ISE 版本选择最新的补丁。

步骤 10 点击 **开始准备** 以验证所有思科 ISE 组件并为您的部署生成报告。

图 2: 在“准备升级”选项卡中显示节点的升级窗口



思科 ISE 在升级过程中会检查以下内容。

| 预先检查列表 | 说明 |
|--------|---|
| 存储库验证 | 检查是否为所有节点配置了存储库。 |
| 捆绑包下载 | 帮助下载和准备所有节点的升级捆绑包。 |
| 内存检查 | 检查 PAN 或独立节点上是否有 25% 的内存空间，以及所有其他节点上是否有 1 GB 的内存空间。 |

| 预先检查列表 | 说明 |
|---------------|--|
| PAN 故障切换验证 | 检查是否已启用 PAN 高可用性。 在开始升级之前，管理员会收到 PAN 高可用性将被禁用的通知。 |
| 计划的备份检查 | 检查计划备份是否已启用。 注释 对于升级过程，此检查不是强制性的。 |
| 配置备份检查 | 检查最近是否完成了配置备份。升级过程仅在备份完成后运行。 |
| 配置数据升级 | 在配置数据库克隆上运行配置数据升级，并创建升级后的数据转储。此检查在捆绑包下载后开始。 |
| 平台支持检查 | 检查部署中支持的平台。它会检查系统是否至少具有 12 个核心 CPU、300-GB 硬盘和 16-GB 内存。它还会检查 ESXi 版本是否为 6.5 或更高版本。 |
| 部署验证 | 检查部署状态节点是否处于同步状态或在进行中。 |
| DNS 解析 | 检查主机名和 IP 地址的正向和反向查找。 |
| 信任存储区证书验证 | 检查信任存储区证书是否有效或已过期。 |
| 系统证书验证 | 检查每个节点的系统证书验证。 |
| 磁盘空间检查 | 检查硬盘是否有足够的可用空间来继续执行升级过程。 |
| NTP 连通性和时间源检查 | 检查系统中配置的 NTP 以及时间源是否为 NTP 服务器。 |
| 平均负载检查 | 按指定时间间隔检查系统负载。频率可以是 1、5 或 15 分钟。 |
| 许可证验证 | 检查智能许可是否已配置且有效。如果智能许可未配置且无效，则会显示警告，要求您配置并验证许可证。 |
| 服务或流程故障 | 指示服务或应用的状态（是正在运行还是处于故障状态）。 |

如果任何组件处于非活动状态或发生故障，则会显示为红色。您还将获得故障排除建议。根据发生故障的组件的升级严重性，您可以继续执行升级过程，或者系统会要求您解决问题，以便继续执行升级过程。

刷新失败的检查 选项仅刷新以红色突出显示的失败。在执行升级之前，必须纠正这些故障。以橙色突出显示的警告不会停止升级过程。但是，它们可能会在升级后影响某些思科 ISE 功能。点击每个警告旁边显示的 **刷新** 图标，在解决问题后刷新这些检查。

点击 **展开以显示** 图标可查看有关每个节点及其状态的其他信息。

点击 **信息** 图标可查看有关每个组件的详细信息。

点击 **下载报告** 可获得生成的报告的副本。

您可以查看暂存和升级过程所需的估计时间。计算方法如下：

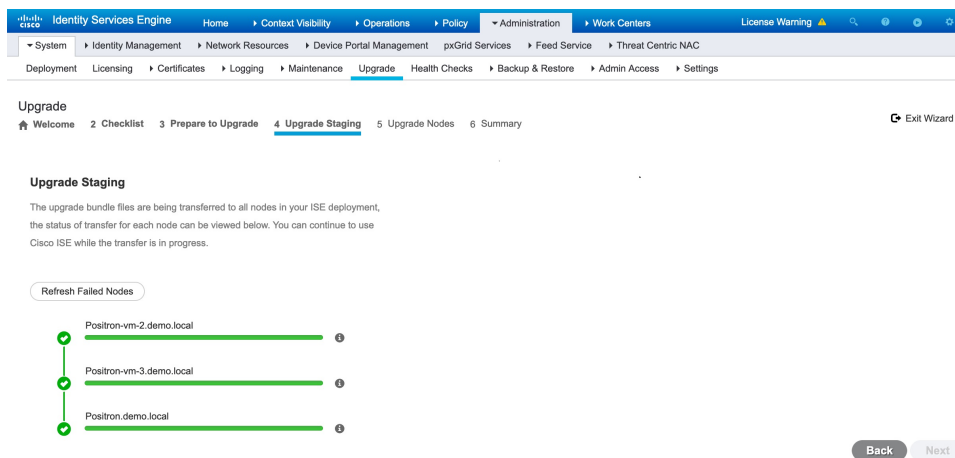
- 网速
- 节点配置：处理器、RAM 和硬盘的数量
- 数据库中的数据大小
- 节点启动应用服务器所用的时间

注释 除 **捆绑包下载** 和 **配置数据升级** 检查外，所有预先检查都将在启动系统验证四小时后自动到期。

步骤 11 完成所有节点的预先检查后，点击 **开始暂存** 以启动暂存过程。

在升级暂存期间，升级后的数据库文件将复制到部署中的所有节点，并在部署中的所有节点上备份配置文件。

图 3: 显示升级暂存的升级窗口



如果节点上的升级暂存成功，则显示为绿色。如果特定节点的升级暂存失败，则显示为红色。您还将获得故障排除建议。

点击 **刷新故障节点** 图标，为故障节点重新启动暂存升级。

步骤 12 点击 **下一步** 以进入 **升级节点** 窗口。

在 **升级节点** 窗口中，您可以查看总体升级进度以及部署中每个节点的状态。

步骤 13 点击 **开始** 以开始升级流程。

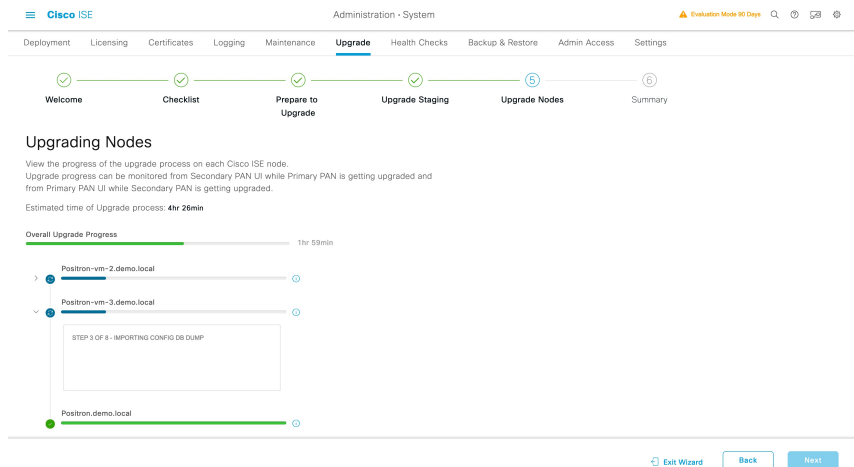
在升级过程完成之前，系统将显示消息 **系统将升级。注销。显示**。

步骤 14 点击**确定**以继续。

注释 您可以再次登录辅助 PAN 以监控升级进度。

在主 PAN 升级时，您可以从辅助 PAN 控制面板监控主 PAN 升级状态。主 PAN 升级后，您可以从主 PAN 控制面板监控所有思科 ISE 节点的升级状态。

图 4: 显示升级状态的升级节点窗口



注释 点击此窗口中的 **退出向导** 选项将阻止您稍后查看 **总结** 窗口。

步骤 15 点击升级节点窗口中的下一步，检查是否所有节点都已成功升级。

如果有任何故障节点，系统将显示一个对话框，其中包含有关故障节点的信息。

步骤 16 在对话框中点击**确定**，从部署中取消注册失败的节点。

升级过程完成后，您可以在**摘要**窗口中查看和下载部署的诊断升级报告。您可以验证并下载包含相关详细信息的升级摘要报告，例如**核对表**、**升级准备**、**升级报告**和**系统运行状况核对表**项目。

通过 GUI 拆分升级思科 ISE 部署

拆分升级是一个多步骤过程，可在允许用户使用其他服务的同时升级思科 ISE 部署。

要对思科 ISE 部署执行拆分升级，请执行以下程序。

步骤 1 在思科 ISE GUI 中，单击菜单图标 (☰)，然后选择 **管理 (Administration)** > **系统 (System)** > **升级 (Upgrade)**。

步骤 2 在升级选择窗口中，点击拆分升级，然后点击开始升级。

概述 选项卡列表列出了部署中的所有节点、这些节点上启用的角色、所安装思科 ISE 的版本以及节点的状态（指示节点是处于活动状态还是非活动状态）。只有在节点处于活动状态时，才能开始升级。

步骤 3 点击**升级 (Upgrade)** 选项卡。

完成 **核对表** 窗口中列出的所有任务，以避免在升级过程中出现任何阻止程序或停机时间。

步骤 4 选中 **我已检查核对表** 复选框，然后点击 **继续**。

屏幕上会显示 **将捆绑包下载至节点** 窗口。

步骤 5 从存储库中下载升级捆绑包至节点：

- a) 选中要下载升级捆绑包的节点旁边的复选框。
- b) 点击 **Download**。

屏幕上会显示 **选择存储库和捆绑包** 窗口。

- c) 从下拉列表中选择存储库。

注释 您可以选择相同的存储库或不同节点上不同的存储库，但是，您必须在所有节点上选择相同的升级捆绑包。

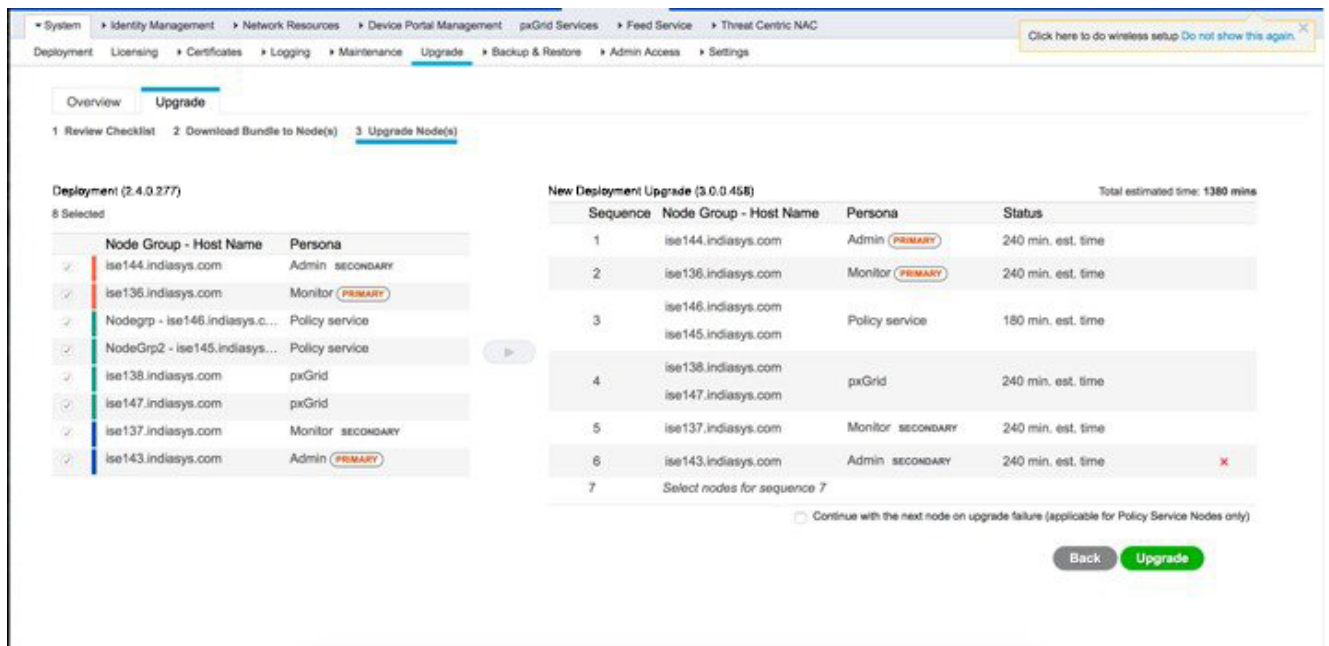
- d) 勾选您想要用于升级的捆绑包旁边的复选框。
- e) 点击 **Confirm**。

捆绑包下载到节点后，节点状态将更改为 **准备升级**。

步骤 6 点击继续 (**Continue**)。

系统将显示 **升级节点** 窗口。

图 5: 显示当前部署和新部署的升级窗口



步骤 7 选择节点并将其按要升级的顺序移动到 **新部署升级** 窗格。

当您节点移动到新部署中后，**升级节点** 窗口上将显示升级时间估值。您可以使用此信息进行升级规划并最大限度地减少业务中断时间。如果您有一对管理和监控节点和多个策略服务节点，请采用以下顺序的步骤。

- a) 默认情况下，辅助管理节点会首先在升级顺序中列出。升级后，此节点会成为新部署中的主管理节点。
- b) 在升级顺序列表中，主监控节点是下一个待升级至新部署的节点。

- c) 选择策略服务节点并将其移至新部署。您也可以修改策略服务节点升级的顺序。
- 您可以按顺序或并行升级策略服务节点。您可以选择一组策略服务节点进行并行升级。
- d) 选择辅助监控节点并将其移至新部署。
- e) 最后，选择主管理节点并将其移至新部署。

步骤 8 如果希望即使升级顺序中的任何策略服务节点升级失败仍继续升级，请选中 **失败后继续升级** 复选框。

此选项不适用于辅助管理节点和主监控节点。如果任意节点出现故障，升级过程会回滚。如果任何策略服务节点发生故障，则辅助监控节点和主管理节点不会升级，并且会保留在旧部署中。

步骤 9 点击升级 (Upgrade) 开始部署升级。

图 6: 显示升级进度的升级窗口

The screenshot shows the 'Upgrade' window in the Cisco ISE GUI. The 'Upgrade Node(s)' step is active, showing a list of nodes to be upgraded. The nodes are grouped by sequence, and their status is updated in real-time. A progress bar indicates the overall upgrade progress, and a 'Back' button is visible.

| Sequence | Node Group - Host Name | Persona | Status |
|----------|--|---------------------|-----------------|
| 1 | ise144.indiasys.com | Admin (PRIMARY) | Upgrading... |
| 2 | ise136.indiasys.com | Monitor (PRIMARY) | 5% Upgrading... |
| 3 | ise146.indiasys.com ise145.indiasys.com | Policy service | Upgrade queued |
| 4 | ise138.indiasys.com ise147.indiasys.com | pxGrid | Upgrade queued |
| 5 | ise137.indiasys.com | Monitor (SECONDARY) | Upgrade queued |
| 6 | ise143.indiasys.com | Admin (SECONDARY) | Upgrade queued |
| 7 | Select nodes for sequence 7 | | |

系统会显示每个节点的升级进度。在成功完成升级后，节点状态变为 **升级完成**。

注释 当您从管理员门户升级某节点，且该节点状态长时间未改变（并且保持在 80%），可以通过 CLI 检查升级日志或通过控制台检查升级状态。

您可以使用 **show logging application** 命令通过 CLI 查看以下升级日志：

- 数据库数据升级日志
- 数据库架构日志
- 操作系统升级后日志

如果您收到以下警告消息，请点击 **升级** 窗口中的 **详细信息** 链接：

The node has been reverted back to its pre-upgrade state.

解决升级失败详细信息 (**Upgrade Failure Details**) 窗口中列出的问题。修复所有问题后，点击 **升级 (Upgrade)** 重新开始升级。


注释 如果终端安全评估数据更新流程运行在新部署的主管理节点上，您无法向主管理节点注册节点。您可以在升级或向新部署中注册节点时等待终端安全评估流程结束（这大概需要 20 分钟），也可以从 **升级** 窗口（**管理 > 系统 > 设置 > 安全评估 > 升级**）页面禁用终端安全评估自动更新功能。

从版本、2.6、2.7 或 3.0 到版本 3.1

您可以从版本 2.0 开始使用管理员门户升级思科 ISE 部署中的所有节点。您还可以将思科 ISE 2.0 的有限可用性版本升级到通用版本。

开始之前

确保您已阅读[升级前的准备工作](#)一节中的说明。

步骤 1 在思科 ISE GUI 中，单击菜单图标 ()，然后选择 **管理 (Administration) > 系统 (System) > 升级 (Upgrade)**。

步骤 2 单击**继续**。

步骤 3 屏幕上会显示 **检查核对表** 窗口。仔细阅读提供的说明。

步骤 4 选中**我已检查核对表 (I have reviewed the checklist)** 复选框，然后单击**继续 (Continue)**。

屏幕上会显示 **将捆绑包下载至节点** 窗口。

步骤 5 从存储库中下载升级捆绑包至节点：

- a) 选中要下载升级捆绑包的节点旁边的复选框。
- b) 单击 **Download**。

屏幕上会显示 **选择存储库和捆绑包** 窗口。

- c) 选择存储库。

您可以选择相同的存储库或不同节点上不同的存储库，但是，您必须在所有节点上选择相同的升级捆绑包。

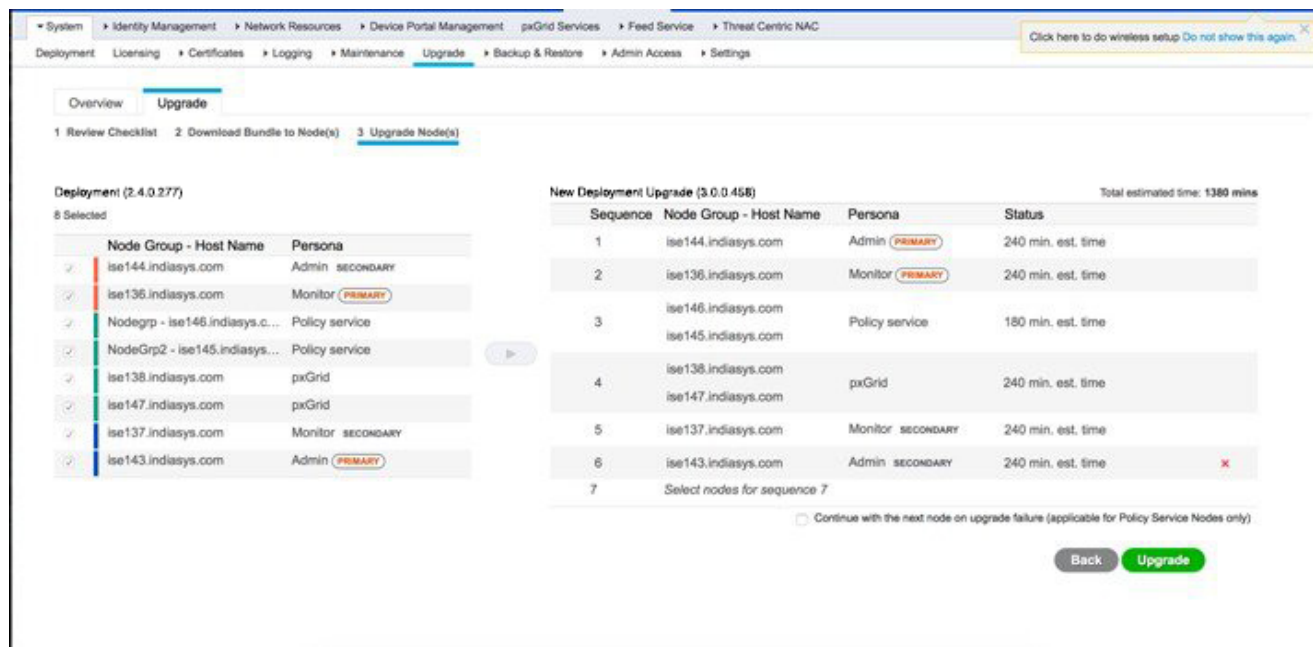
- d) 勾选您想要用于升级的捆绑包旁边的复选框。
- e) 单击 **Confirm**。

捆绑包下载到节点后，节点状态将更改为 **Ready for Upgrade**。

步骤 6 单击**继续**。

屏幕上将显示**升级节点 (Upgrade Nodes)** 窗口。

图 7: 显示各节点所选存储库的升级窗口

**步骤 7** 选择升级顺序。

当您节点移动到新部署中后，**Upgrade Nodes** 窗口上将显示升级时间估值。您可以使用此信息进行升级规划并最大限度地减少业务中断时间。如果您有一对管理和监控节点和多个策略服务节点，请采用以下升级顺序。

- 默认情况下，辅助管理节点会首先在升级顺序中列出。升级后，此节点会成为新部署中的主管理节点。
- 在升级顺序列表中，主监控节点是下一个待升级至新部署的节点。
- 选择策略服务节点并将其移至新部署。您可以修改策略服务节点升级的顺序。

您可以按顺序或并行升级策略服务节点。您可以选择一组策略服务节点进行并行升级。

- 选择辅助监控节点并将其移至新部署。
- 最后，选择主管理节点并将其移至新部署。

步骤 8 如果希望即使升级顺序中的任何策略服务节点升级失败仍继续升级，请选中失败后继续升级 (Continue with upgrade on failure) 复选框。

此选项不适用于辅助管理节点和主监控节点。如果任意一个节点出现故障，升级过程会回滚。如果任何策略服务节点发生故障，则辅助监控节点和主管理节点不会升级，并且会保留在旧部署中。

步骤 9 点击升级 (Upgrade) 开始部署升级。

图 8: 显示升级进度的升级窗口

Deployment (2.4.0.277)
8 Selected

| Node Group - Host Name | Persona |
|--------------------------------|-------------------|
| ise144.indiasys.com | Admin SECONDARY |
| ise136.indiasys.com | Monitor (PRIMARY) |
| Nodegrp - ise146.indiasys.c... | Policy service |
| NodeGrp2 - ise145.indiasys... | Policy service |
| ise138.indiasys.com | pxGrid |
| ise147.indiasys.com | pxGrid |
| ise137.indiasys.com | Monitor SECONDARY |
| ise143.indiasys.com | Admin (PRIMARY) |

New Deployment Upgrade (3.0.0.458) Total estimated time: 1140 mins

| Sequence | Node Group - Host Name | Persona | Status |
|----------|-----------------------------|-------------------|-------------------|
| 1 | ise144.indiasys.com | Admin (PRIMARY) | Upgrading... (5%) |
| 2 | ise136.indiasys.com | Monitor (PRIMARY) | Upgrade queued |
| 3 | ise146.indiasys.com | Policy service | Upgrade queued |
| | ise145.indiasys.com | | Upgrade queued |
| 4 | ise138.indiasys.com | pxGrid | Upgrade queued |
| | ise147.indiasys.com | | Upgrade queued |
| 5 | ise137.indiasys.com | Monitor SECONDARY | Upgrade queued |
| 6 | ise143.indiasys.com | Admin SECONDARY | Upgrade queued |
| 7 | Select nodes for sequence 7 | | |

Continue with the next node on upgrade failure (applicable for Policy Service Nodes only)

Back Upgrade

系统会显示每个节点的升级进度。在成功完成升级后，节点状态变为 **Upgrade Complete**。

注释 当您从管理员门户升级某节点，如果该节点状态长时间未改变（并且保持在 80%），可以通过 CLI 检查升级日志或通过控制台检查升级状态。登录到 CLI，或通过思科 ISE 节点的控制台以查看升级过程。您可以使用 **show logging application** 命令查看 *upgrade-uibackend-cliconsole.log* 和 *upgrade-postosupgrade-yyyyymmdd-xxxxxx.log*。

您可以使用 **show logging application** 命令通过 CLI 查看以下升级日志：

- 数据库数据升级日志
- 数据库架构日志
- 操作系统升级后日志

如果收到警告消息：**The node has been reverted back to its pre-upgrade state**，转到升级 (**Upgrade**) 窗口，单击详细信息 (**Details**) 链接。解决升级失败详细信息 (**Upgrade Failure Details**) 窗口中列出的问题。修复所有问题后，单击升级 (**Upgrade**) 重新开始升级。

注释 如果终端安全评估数据更新流程运行在新部署的主管理节点上，您无法向主管理节点注册节点。您可以在升级或向新部署中注册节点时等待终端安全评估流程结束（这大概需要 20 分钟），也可以从更新 (**Updates**) 窗口禁用终端安全评估自动更新功能。要查看此处窗口，请单击菜单图标 (≡)，然后选择管理 (**Administration**) > 系统 (**System**) > 设置 (**Settings**) > 终端安全评估 (**Posture**) > 更新 (**Updates**)。

通过 CLI 升级思科 ISE 部署

使用 CLI 的升级过程取决于部署类型。

升级独立节点

您可以直接使用 **application upgrade <upgrade bundle name> <repository name>** 命令，或者也可以按照指定顺序使用 **application upgrade prepare <upgrade bundle name> <repository name>** 和 **application upgrade proceed** 命令来升级独立节点。

在担任管理、策略服务和监控角色的独立节点上，您可以通过 CLI 运行 **application upgrade <upgrade bundle name> <repository name>** 命令。如果选择直接运行此命令，我们建议您先将远程存储库中的升级捆绑包复制到思科 ISE 节点的本地磁盘中，然后再运行命令以节省升级时间。

或者，您也可以使用 **application upgrade prepare <upgrade bundle name> <repository name>** 和 **application upgrade proceed** 命令。**application upgrade prepare <upgrade bundle name> <repository name>** 命令可下载升级捆绑包，并在本地进行解压缩。此命令会将远程存储库中的升级捆绑包复制到思科 ISE 节点的本地磁盘。在为升级准备好一个节点后，请运行 **application upgrade proceed** 命令来成功完成升级。

我们建议您运行下面描述的 **application upgrade prepare <upgrade bundle name> <repository name>** 和 **application upgrade proceed** 命令。

开始之前

确保您已阅读[升级前的准备工作](#)一节中的说明。

步骤 1 在本地磁盘上创建一个存储库。例如，您可以创建名为“upgrade”的存储库。

示例：

```
ise/admin# conf t
Enter configuration commands, one per line. End with CNTL/Z.
ise/admin(config)# repository upgrade
ise/admin(config-Repository)# url disk:
% Warning: Repositories configured from CLI cannot be used from the ISE web UI and are not replicated
to other ISE nodes.
If this repository is not created in the ISE web UI, it will be deleted when ISE services restart.
ise/admin(config-Repository)# exit
ise/admin(config)# exit
```

步骤 2 在思科 ISE 命令行界面 (CLI) 中，输入 **application upgrade prepare <upgrade bundle name> <repository name>** 命令。

此命令会将升级捆绑包复制到您在上一步中创建的本地存储库“upgrade”，并列出 MD5 和 SHA256 校验和。

步骤 3 注释 开始升级后，您可以查看升级进度，方法是通过 SSH 登录并运行 **show application status ise** 命令。显示以下消息：%通知：身份服务引擎升级正在进行中…

在 ISE CLI 中，输入 **application upgrade proceed** 命令。

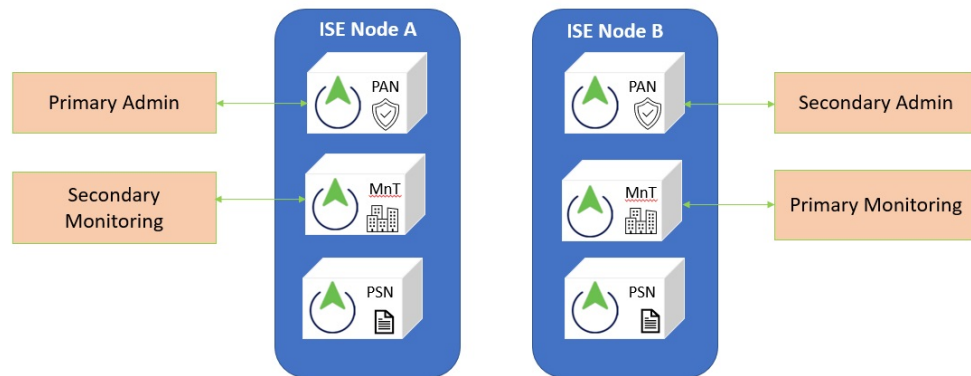
下一步做什么

[验证升级过程，第 44 页](#)

升级双节点部署

使用 **application upgrade prepare <upgrade bundle name> <repository name>** 和 **proceed** 命令升级双节点部署。您无需手动取消注册节点并再次注册。升级软件会自动取消注册节点，并将其迁移至新的部署。当您升级双节点部署时，最初应仅升级辅助管理节点（节点 B）。辅助节点的升级完成后，随后升级主节点（节点 A）。如果您如下图所示设置部署，则可以继续执行此升级过程。

图 9: 思科 ISE 双节点管理部署



开始之前

- 从主管理节点按需（手动）备份配置和运行数据。
- 确保在部署的双节点上启用管理和监控角色。

如果仅在主管理节点上启用了管理角色，则开始升级前必须在辅助节点上启用管理角色，这是因为升级过程要求先升级辅助管理节点。

或者，如果双节点部署中只有一个管理节点，则取消注册辅助节点。两个节点成为独立节点。将两个节点作为独立节点升级，并在升级后设置部署。

- 如果仅在其中一个节点上启用了监控角色，请确保您在另一个节点上也启用了监控角色，然后再继续。

步骤 1 通过 CLI 升级辅助节点（节点 B）。

升级过程自动从部署中删除节点 B 并对其进行升级。重新启动后，节点 B 将成为主节点。

步骤 2 升级节点 A。

升级过程自动在部署中注册节点 A，并将其指定为升级后环境中的辅助节点。

步骤 3 现在将节点 A 升级为新部署中的主节点。

升级完成后，如果节点包含旧的监控日志，请确保运行 **application configure ise** 命令并在这些节点上选择 5（刷新数据库统计数据）。

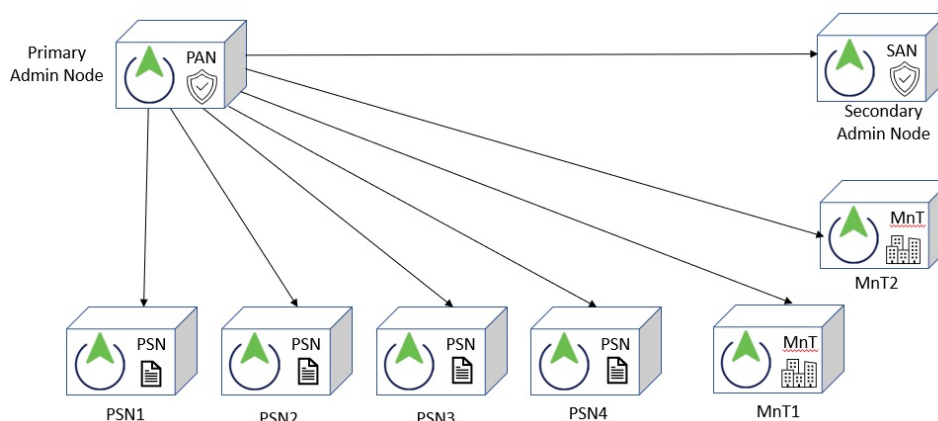
下一步做什么

[验证升级过程，第 44 页](#)

升级分布式部署

您必须先将辅助管理节点 (SAN) 升级到新版本。例如，如果您如下图所示设置部署，其中包含一个主管理节点 (PAN)、一个辅助管理节点、四个策略服务节点 (PSN)，一个主监控节点 (MnT1) 和一个辅助监控节点 (MnT2)，您可以继续执行以下升级过程。

图 10: 升级前的思科 ISE 部署



注释 升级前，您无需手动取消注册节点。使用 **application upgrade prepare <upgrade bundle name> <repository name>** 和 **proceed** 命令升级到新版本。升级过程会自动取消注册节点，并将其迁移至新的部署。如果您在升级前手动取消注册节点，请确保您拥有主管理节点的许可证文件，然后再开始升级。如果您手头没有该文件（例如，您的许可证被思科合作伙伴供应商安装），请联系思科技术支持中心获得帮助。

开始之前

- 如果部署中没有辅助管理节点，请配置一个策略服务节点用作辅助管理节点，然后再开始升级。
- 确保您已阅读并遵从[升级前的准备工作](#)一节中给出的说明。

- 当您升级完整的思科 ISE 部署时，必须执行域名系统 (DNS) 服务器解析（转发和反向查找）；否则，升级将会失败。

步骤 1 从 CLI 升级 SAN。

升级过程自动从部署中取消注册 SAN 并对其进行升级。重新启动后，SAN 成为新部署的主节点。由于每个配置至少需要一个监控节点，因此升级过程会在 SAN 上启用监控角色，即便在旧部署中并未启用该节点的监控角色。如果在旧部署中对 SAN 启用了策略服务角色，则升级到新版本后将保留此配置。

步骤 2 将其中一个监控节点（MnT1 和 MnT2）升级到新部署。

我们建议您先升级主监控节点，然后再升级辅助监控节点（如果在旧部署中主管理节点同时也被用作主监控节点，那么这种方法是不可行的）。您的主监控节点开始从新部署收集日志，并且您可以在主管理节点控制面板上查看详细信息。

如果旧部署中只有一个监控节点，那么升级前请确保对 PAN 启用监控角色，而该节点正是旧部署中的主管理节点。由于节点角色的变更，会导致思科 ISE 应用重新启动。请等待 PAN 出现，然后再继续执行操作。由于将监控节点升级到新部署所需的时间比其他节点要长，因此必须将运行数据迁移到新部署。

如果在旧部署中没有对节点 B（同时也是新部署中的主管理节点）启用监控角色，请禁用其监控角色。由于节点角色的变更，会导致思科 ISE 应用重新启动。请等待主管理节点出现，然后再继续执行操作。

步骤 3 升级策略服务节点 (PAN)。您可以同时升级多个 PSN，但如果您同时升级所有 PSN，网络将会中断。

升级后，向新部署的主节点 SAN 注册 PSN，并将主节点的数据复制到所有 PSN。PSN 保留其角色、节点组信息和分析探针配置。

步骤 4 如果旧部署中有第二个监控节点，则必须执行以下操作：

- a) 对 PAN 启用监控角色，而该节点正是旧部署中的主节点。

部署至少需要一个监控节点。升级旧部署中的第二个监控节点之前，对主节点启用此角色。由于节点角色的变更，会导致思科 ISE 应用重新启动。等待主 ISE 节点再次出现。

- b) 将旧部署中的辅助监控节点升级到新部署。

除主管理节点外，您必须将所有其他节点升级到新部署。

步骤 5 最后，升级主管理节点。

此节点已升级，并作为辅助管理节点添加到新部署中。您可以将辅助管理节点升级为新部署中的主节点。

升级完成后，如果升级的监控节点包含旧日志，请运行 `application configure ise` 命令并在监控节点上选择 5（刷新数据库统计数据）。

下一步做什么

[验证升级过程，第 44 页](#)

验证升级过程

我们建议您进行网络测试，以确保部署运行正常并且用户可以验证和访问您网络中的资源。

如果由于配置数据库问题而导致升级失败，则更改会自动回滚。

执行以下任意一个选项，以验证升级是否成功。

- 检查升级过程中使用的 `ade.log` 文件。要显示 `ade.log` 文件，请从思科 ISE CLI 输入以下命令：**show logging system ade/ADE.log?**

您可以使用 `grep STEP` 命令查看升级进度：

- `info:[application:install:upgrade:preinstall.sh] STEP 0: Running pre-checks`
- `info:[application:operation:preinstall.sh] STEP 1: Stopping ISE application...`
- `info:[application:operation:preinstall.sh] STEP 2: Verifying files in bundle...`
- `info:[application:operation:isedbupgrade-newmodel.sh] STEP 3: Validating data before upgrade...`
- `info:[application:operation:isedbupgrade-newmodel.sh] STEP 4: De-registering node from current deployment.`
- `info:[application:operation:isedbupgrade-newmodel.sh] STEP 5: Taking backup of the configuration data...`
- `info:[application:operation:isedbupgrade-newmodel.sh] STEP 6: Registering this node to primary of new deployment...`
- `info:[application:operation:isedbupgrade-newmodel.sh] STEP 7: Downloading configuration data from primary of new deployment...`
- `info:[application:operation:isedbupgrade-newmodel.sh] STEP 8: Importing configuration data...`
- `info:[application:operation:isedbupgrade-newmodel.sh] STEP 9: Running ISE configuration data upgrade for node specific data...`
- `info:[application:operation:isedbupgrade-newmodel.sh] STEP 10: Running ISE M&T database upgrade...`
- `info:[application:install:upgrade:post-osupgrade.sh] POST ADEOS UPGRADE STEP 1: Upgrading Identity Services Engine software...`
- `info:[application:operation:post-osupgrade.sh] POST ADEOS UPGRADE STEP 2: Importing upgraded data to 64 bit database...`
- 搜索此字符串以确保升级已成功完成：

```
Upgrade of Identity Services Engine completed
      successfully.
```
- 输入 **show version** 命令来验证版本。
- 输入 **show application status ise** 命令验证所有服务是否都在运行。

回滚到之前版本

在极少数情况下，您可能需要使用以前版本的 ISO 映像并从备份文件中恢复数据，来重新映像思科 ISE 设备。恢复数据后，您可以在旧部署中注册，并启用和旧部署中一样的角色。因此，我们建议您在开始升级之前备份思科 ISE 配置和监控数据。

有时，因为配置和监控数据库中的问题不会自动回滚，所以升级才会失败。在这种情况下，您将收到升级失败消息，获悉数据库无法回滚。如果遇到这种情况，您应手动重新映像系统、安装思科 ISE，并恢复配置数据和监控数据（如果已启用监控角色）。

在尝试执行任何回滚或恢复操作之前，使用 **backup-logs** 命令生成支持捆绑包，并将该支持捆绑包放于远程存储库中。



第 4 章

安装最新补丁

- [思科 ISE 软件补丁](#)，第 47 页
- [回滚软件补丁](#)，第 49 页
- [查看补丁安装和回滚更改](#)，第 49 页

思科 ISE 软件补丁

思科 ISE 软件补丁始终会累积。思科 ISE 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 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，单击菜单图标 (☰)，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
```

相关主题

- [软件补丁安装指南](#)，第 48 页
- [软件补丁回滚指南](#)，第 49 页
- [安装软件补丁](#)，第 48 页

回滚软件补丁，第 49 页

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 版本的补丁。思科 ISE 会报告任何版本不匹配问题，以及补丁文件中的任何错误。

安装的补丁版本不能低于当前安装在思科 ISE 上的补丁版本。同样，如果思科 ISE 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 服务器安装的是补丁 3，则无法安装或回滚补丁 1 或 2。

从分布式部署中的主 PAN 安装补丁时，思科 ISE 会先后在部署中的主节点和所有辅助节点上安装补丁。如果在主 PAN 上成功安装，思科 ISE 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。但是，如果出于任何原因导致任一辅助节点上的安装失败，则系统仍会继续在部署中的下一个辅助节点上安装补丁。

从两节点部署中的主 PAN 安装补丁时，思科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。

安装软件补丁

开始之前

- 您必须分配到了超级管理员或系统管理员的角色。
- 在思科 ISE GUI 中，单击菜单图标 (☰)，然后选择 **管理 (Administration) > 系统 (System) > 部署 (Deployment) > PAN 故障切换 (PAN Failover)**，并确保取消选中启用 PAN 自动故障切换 (**Enable PAN Auto Failover**) 复选框。在此任务期间必须禁用 PAN 自动故障切换配置。

步骤 1 在思科 ISE GUI 中，单击菜单图标 (☰)，然后选择 **管理 (Administration) > 系统 (System) > 维护 (Maintenance) > 补丁管理 (Patch Management) > 安装 (Install)**。

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

步骤 3 单击安装 (**Install**) 安装补丁。

在 PAN 上安装补丁后，思科 ISE 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 在思科 ISE GUI 中，单击菜单图标 (☰)，然后选择 **管理 (Administration) > 系统 (System) > 维护 (Maintenance) > 补丁管理 (Patch Management)** 以返回至“补丁安装” (Patch Installation) 页面。

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

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 会在主节点上回滚补丁，然后在部署中的所有辅助节点上回滚补丁。

开始之前

- 您必须分配到了超级管理员角色或系统管理员角色。

步骤 1 在思科 ISE GUI 中，单击菜单图标 (☰)，然后选择管理 (Administration) > 系统 (System) > 维护 (Maintenance) > 补丁管理 (Patch Management)。

步骤 2 单击您要回滚更改的补丁版本的单选按钮，然后单击回滚 (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，请单击页面底部的**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，然后单击**显示节点状态 (Show Node Status)**。

步骤 5 在辅助节点上，单击补丁的单选按钮，然后单击**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 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 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。但是，如果任一辅助节点上的补丁回滚失败，系统仍会从部署中的下一个辅助节点回滚补丁。

当思科 ISE 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。

查看补丁安装和回滚更改

要查看与已安装的补丁有关的报告，请执行以下步骤。

开始之前

您必须分配到了超级管理员角色或系统管理员角色。你可以安装或回滚补丁 在思科 ISE GUI 中，单击 **菜单** 图标 (☰)，然后选择 **管理 > 系统 > 维护 > 补丁管理** 窗口。您也可以通过选择一个特定补丁并单击 **显示节点状态** 按钮来查看部署中每个节点上的特定补丁的状态（已安装/正在安装/未安装）。

步骤 1 在思科 ISE GUI 中，单击 **菜单** 图标 (☰)，然后选择 **操作 > 报告 > 审核 > 操作审核**。默认情况下，会显示过去七天的记录。

步骤 2 单击 **过滤器** 下拉菜单，并选择 **快速过滤器** 或 **高级过滤器** 并使用所需的關鍵字，例如，`patch install initiated`，来生成包含已安装补丁的报告。。



第 5 章

执行升级后的任务

- [升级后的设置和配置](#)，第 51 页

升级后的设置和配置

升级思科 ISE 后执行以下任务。

转换为新的许可证类型

- 通过思科智能软件管理器 (CSSM) 将旧许可证转换为新许可证类型。
- 在思科 ISE 管理员门户中启用新许可证。

有关新思科 ISE 许可证类型的详细信息，请参阅《[思科 ISE 管理指南，版本 3.1](#)》。

验证虚拟机设置

如果要在虚拟机上升级思科 ISE 节点，请确保将访客操作系统更改为 Red Hat Enterprise Linux (RHEL) 7 (64-bit) 或 Red Hat Enterprise Linux (RHEL) 6 (64-bit)。要执行此操作，您必须关闭虚拟机，将访客操作系统更改为受支持的 RHEL 版本，并在更改完之后再打开虚拟机。

RHEL 7 仅支持 E1000 和 VMXNET3 网络适配器。请务必在升级之前更改网络适配器类型。

浏览器设置

升级后，请先清除浏览器缓存、关闭浏览器并打开新的浏览器会话，然后再接入思科 ISE 管理员门户。此外，请确认您使用的是版本说明中列出的受支持浏览器：<https://www.cisco.com/c/en/us/support/security/identity-services-engine/products-release-notes-list.html>

重新加入 Active Directory

如果您使用 Active Directory 作为外部身份源，并且与 Active Directory 的连接已丢失，则必须再次将所有思科 ISE 节点与 Active Directory 连接。全部加入后，请执行外部身份源调用流程以确保连接。

- 升级后，如果您使用 Active Directory 管理员账户登录到思科 ISE 用户界面，由于升级期间与 Active Directory 的连接丢失，因此登录会失败。您必须使用内部管理员账户登录到思科 ISE 并使用该账户加入到 Active Directory。
- 如果在升级前您为思科 ISE 的管理访问启用了基于证书的身份验证，并使用 Active Directory 作为您的身份源，则升级后您将无法启动 ISE 登录页面。这是因为升级过程中丢失了对 Active Directory 的加入。要恢复到 Active Directory 的联接，请连接到思科 ISE CLI，并使用下列命令以安全模式启动 ISE 应用：

application start ise safe

思科 ISE 在安全模式下启动后，请执行以下任务：

- 使用内部管理员账户登录到思科 ISE 用户界面。
如果您忘记密码或您的管理员账户已锁定，请参阅《管理员指南》中的[管理员访问 思科 ISE](#)，以了解关于如何重置管理员密码的信息。
- 使用 Active Directory 加入思科 ISE

有关加入 Active Directory 的详细信息，请参阅：

[将 Active Directory 配置为外部身份源](#)

与 Active Directory 配合使用的证书属性

思科 ISE 使用 SAM、CN 或这两者来识别用户。思科 ISE 版本 2.2 补丁 5 及更高版本，版本 2.3 补丁 2 及更高版本，将 sAMAccountName 属性用作默认属性。在早期版本中，默认搜索 SAM 和 CN 属性。此行为已在版本 2.2 补丁 5 及更高版本，以及版本 2.3 补丁 2 及更高版本中发生更改，是 [CSCvf21978](#) 漏洞修复的组成部分。在这些版本中，仅 sAMAccountName 属性用作默认属性。

如果环境需要，您可以配置思科 ISE 以使用 SAM、CN 或者这两者。使用 SAM 和 CN 时，sAMAccountName 属性的值不唯一，思科 ISE 还将比较 CN 属性值。

要配置 Active Directory 身份搜索的属性，请执行以下操作：

1. 选择管理 > 身份管理 > 外部身份源 > **Active Directory**。在 **Active Directory** 窗口中，单击高级工具 (**Advanced Tools**)，然后选择高级调整 (**Advanced Tuning**)。输入下列详细信息：
 - **ISE 节点 (ISE Node)** - 选择连接 Active Directory 的 ISE 节点。
 - **Name** - 输入您正更改的注册表项。要更改 Active Directory 搜索属性，请输入：
REGISTRY.Services\lsass\Parameters\Providers\ActiveDirectory\IdentityLookupField
 - **Value** - 输入 ISE 用于识别用户的属性：
 - **SAM** - 在查询中仅使用 SAM（此选项为默认选项）。
 - **CN** - 在查询中仅使用 CN。

- *SAMCN* - 在查询中使用 CN 和 SAM。
- **备注** - 说明您正在更改的内容，例如：将默认行为更改为 SAM 和 CN
- 2. 单击**更新值 (Update Value)** 以更新注册表。
系统将显示一个弹出窗口。阅读消息并接受更改。ISE 中的 AD 连接器服务重新启动。

反向 DNS 查找

确保在 DNS 服务器中，为分布式部署的所有思科 ISE 节点配置反向 DNS 查询。否则，升级后可能会遇到部署相关问题。

恢复证书

恢复 PAN 上的证书

当您在升级分布式部署时，同时符合下列两个条件时，主管理节点的根 CA 证书不会添加到信任证书存储库：

- 辅助管理节点升级为新部署中的主管理节点。
- 在辅助管理节点上禁用会话服务。

如果证书不在存储区中，您可能会看到身份验证失败并出现以下错误：

- 执行 BYOD 流程期间出现未知的 CA
- 执行 BYOD 流程期间发生 OCSP 未知错误

对于失败的身份验证，当您从实时日志页面点击“更多详细信息”链接时，会看到这些消息。

要恢复主管理节点的根 CA 证书，请生成新的思科 ISE 根 CA 证书链。在思科 ISE GUI 中，单击菜单图标 (≡)，然后选择**管理 > 证书 > 证书签名请求 > 更换 ISE 根 CA 证书链**。

将证书和密钥恢复到辅助管理节点

如果您使用的是辅助管理节点，从主管理节点获取思科 ISE CA 证书和密钥的备份，并在辅助管理节点上还原备份。这样，即便发生主 PAN 故障，辅助管理节点也能充当外部 PKI 的根 CA 或从属 CA，您可以将辅助管理节点升级为主管理节点。

有关备份和恢复证书和密钥的详细信息，请参阅：

[思科 ISE CA 证书和密钥的备份与恢复](#)

重新生成根 CA 链

在特定升级场景中，您必须在升级过程完成后重新生成根 CA 链。按照以下步骤重新生成根 CA 链：

1. 在思科 ISE 主菜单中，选择 **Administration > System > Certificates > Certificate Management > Certificate Signing Request**。
2. 单击生成证书签名请求 (**Generate Certificate Signing Request (CSR)**)。
3. 从证书将用于 (**Certificate(s) will be used for**) 下拉列表中选择 **ISE 根 CA**。
4. 单击替换 ISE 根 CA 证书链 (**Replace ISE root CA Certificate Chain**)。

表 3: 根 CA 链重新生成场景

| 升级场景 | 模式 | 重新生成 Root CA 链 |
|-------------------------------|-------|-------------------------------|
| 完整升级过程 | 部署 | 不需要重新生成根 CA，因为在升级过程中部署不会发生变化。 |
| 拆分升级过程 | 部署 | 重新生成根 CA 链 |
| 配置数据库恢复过程 | 独立 | 重新生成根 CA 链 |
| 节点升级：在拆分升级过程后将辅助 PAN 升级为主 PAN | 部署 | 重新生成根 CA 链 |
| 更改任何思科 ISE 节点的域名或主机名 | 独立和部署 | 重新生成根 CA 链 |

升级过程后，您可能会遇到以下事件：

1. 实时日志中没有数据。
2. 队列链路错误。
3. 运行状况不可用。
4. 某些节点的系统摘要中没有可用的日期。

您必须重置 [MnT 数据库](#)，并更换 ISE Root CA 证书链，以解决队列链接错误并恢复信息。

以威胁防御为中心的 NAC

如果已启用“Threat-Centric NAC (TC-NAC)”服务，则升级后，TC-NAC 适配器可能不会正常运行。您必须从 ISE GUI 的“Threat-Centric NAC”页面重新启动适配器。选择适配器并点击重新启动 (Restart) 以重新启动适配器。

SNMP 原始策略服务节点设置

在 SNMP 设置下，如果您手动配置了生成策略服务节点的值，则升级期间此配置将会丢失。您必须重新配置 SNMP 设置。

有关详情，请参阅：

请参阅 [网络设备定义设置](#) 下的 SNMP 设置。

分析器源服务

升级后更新分析器馈送服务，确保安装的是最新的 OUI。

从思科 ISE 管理门户：

步骤 1 在思科 ISE GUI 中，单击菜单图标 (☰)，然后选择 **管理 > FeedService > 分析器**。确保已启用 Profiler Feed 服务。

步骤 2 点击立即更新 (**Update Now**)。

客户端调配

检查客户端配置中使用的原生 Supplicant 客户端配置文件，并确保无线 SSID 是正确的。对于 iOS 设备，如果您尝试连接到的网络已隐藏，请从 **iOS 设置 (iOS Settings)** 区域中，选中 **目标网络隐藏时启用 (Enable if target network is hidden)** 复选框。

更新 ISE 上的客户端配置资源：

在线更新

步骤 1 在思科 ISE GUI 中，单击菜单图标 (☰)，然后选择 **策略 > 策略元素 > 结果 > 客户端调配 > 资源** 以配置客户端调配资源。

步骤 2 点击 **Add**。

步骤 3 选择 **Agent Resources From Cisco Site**。

步骤 4 在 **Download Remote Resources** 窗口中，选择 “Cisco Temporal Agent” 资源。

步骤 5 点击 **保存** 并验证下载的资源显示在 “资源” 页面中。

离线更新

步骤 1 依次选择 **策略 > 策略元素 > 结果 > 客户端调配 > 资源** 以配置客户端调配资源。

步骤 2 在思科 ISE GUI 中，单击菜单图标 (☰)，然后选择 **策略 > 策略元素 > 结果 > 客户端调配 > 资源** 以配置客户端调配资源。

步骤 3 点击 **Add**。

步骤 4 选择 **Agent Resources from Local Disk**。

步骤 5 从 **类别** 下拉列表中，选择 **思科提供的软件包**。

Cipher Suites

如果您基于思科 ISE 对使用已弃用密码的传统设备（例如旧 IP 电话）进行身份验证，身份验证会失败，因为这些设备使用传统密码。要在升级后使思科 ISE 能够对此类传统设备进行身份验证，请确保按照如下方法更新“允许的协议” (Allowed Protocols) 配置：

步骤 1 在思科 ISE GUI 中，单击菜单图标 (☰)，然后选择 **Policy > Policy Elements > Results > Authentication > Allowed Protocols**。

步骤 2 编辑“允许的协议” (Allowed Protocols) 服务并选中允许 EAP 使用弱密码 (Allow weak ciphers for EAP) 复选框。

步骤 3 点击 **Submit**。

相关主题

[思科身份服务引擎版本说明](#)

[Cisco 身份服务引擎网络组件兼容性](#)

监控和故障排除

- 重新配置邮件设置、收藏夹报告和数据清除设置。
- 为您需要的特定警报检查阈值和过滤器。默认情况下，升级后所有警报均会启用。
- 根据需要自定义报告。如果您已在旧配置中自定义报告，升级过程会覆盖您所做的更改。

恢复 MnT 备份

使用更新前创建的 MnT 数据的操作数据备份，恢复备份。

有关详情，请参阅：

[《思科 ISE 管理员指南》中的备份和恢复操作。](#)

将策略刷新为 Trustsec NAD

按以下顺序运行以下命令，在系统中启用思科 TrustSec 的第 3 层接口上下策略：

- `no cts role-based enforcement`
- `cts role-based enforcement`

更新请求者调配向导

升级到新版本或应用补丁时，请求方调配向导 (SPW) 不会更新。您必须手动更新 SPW，然后创建新的本地 supplicant 配置文件和引用新 SPW 的新客户端调配策略。ISE 下载页面上提供了新的 SPW。

分析器终端所有权同步/复制

当您升级到 思科 ISE 2.7 及更高版本时，作为 JEDIS 框架的一部分，需要在部署中的所有节点之间打开端口 6379，以进行往返通信。

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。