思科身份服务引擎被动身份连接器安装和升级指南，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

目录

第 1 章 **思科 ISE-PIC 安装和升级概览** 1

思科 ISE-PIC 术语 1

思科 ISE-PIC 架构、部署和节点 2

前提条件和虚拟设备要求 3

第 2 章 **安装思科 ISE-PIC** 5

下载和运行 ISO 映像 5

运行设置程序 6

验证安装过程 9

第 3 章 **升级思科 ISE-PIC** 11

思科 ISE-PIC 升级概览 11

验证数据以防止升级失败 12

下载并运行升级就绪工具 14

创建存储库并复制 URT 捆绑包 14

运行升级就绪工具 14

必须开放用于通信的防火墙端口 15

从主管理节点备份思科 ISE-PIC 的配置和运行数据 15

从主管理节点备份系统日志 16

检查证书有效性 16

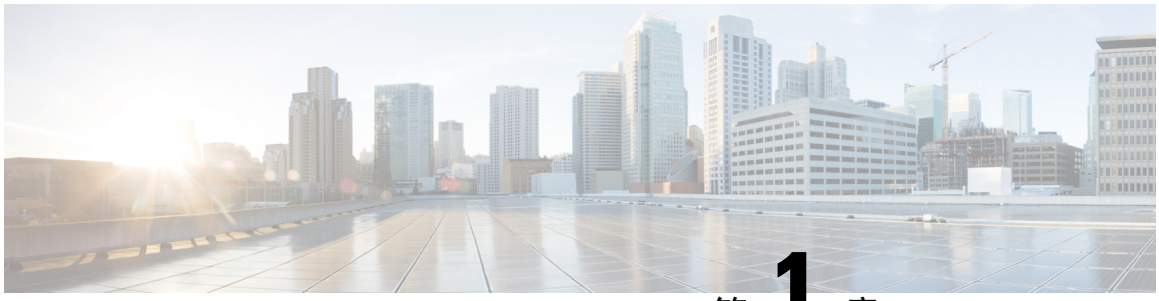
导出证书和私钥 16

禁用计划备份 16

配置 NTP 服务器和验证可用性 17

升级双节点部署 17

升级独立节点 18
验证升级过程 19
从升级失败中恢复 19
升级失败 19
二进制安装期间升级失败 21
回滚到之前版本的 ISO 映像 21
升级后的任务 22



第 1 章

思科 ISE-PIC 安装和升级概览

注释 此产品的文档集力求使用无偏见语言。在本文档集中，无偏见定义为不暗示基于年龄、残障、性别、种族身份、族群身份、性取向、社会经济地位和交叉性的歧视的语言。由于产品软件的用户界面中使用的硬编码语言，基于 RFP 文档使用的语言或引用的第三方产品使用的语言，文档中可能存在例外情况。

本指南介绍了如何：

- 首次安装和配置任何思科 ISE-PIC 版本。请参阅 安装思科 ISE-PIC ， 第 5 页。
- 从较旧版本升级到较新版本。请参阅 升级思科 ISE-PIC ， 第 11 页。

本章的其余部分概述了 ISE-PIC 术语和基础设施。有关配置和使用 ISE-PIC 的其他信息和详细信息，请参阅《身份服务引擎被动身份连接器 *(ISE-PIC)* 管理员指南》。

- 思科 ISE-PIC 术语， 第 1 页
- 思科 ISE-PIC 架构、部署和节点， 第 2 页
- 前提条件和虚拟设备要求 ， 第 3 页

思科 ISE-PIC 术语

本指南在讨论 Cisco ISE-PIC 时使用以下术语：

术语	定义
GUI	图形用户界面。GUI 是指 ISE-PIC 软件安装中的任何屏幕和选项卡。
网卡	网络接口卡。
节点	单个物理或虚拟思科 ISE-PIC 设备。

术语	定义
PAN	ISE-PIC 部署中的主节点是主管理节点 (PAN)，您可以从此节点执行所有可用操作。在ISE-PIC中，最多可以安装两个节点。如果安装第二个节点，则此节点将称为辅助管理节点（辅助 PAN）。
解析器	接收系统日志消息，并将输入拆分为可管理、映射并发布到 ISE-PIC 的各部分的 ISE-PIC 后端组件。解析器将在系统日志消息到达时解析每行信息，查找关键信息。例如，如果解析器配置为查找“mac=”，则解析器会在查找此短语时解析每行信息。解析器设置为在找到已配置的关键短语后，将定义的信息传送到 ISE。
主节点	ISE-PIC 部署中的主节点是主管理节点 (PAN)，您可以从此节点执行所有可用操作。在ISE-PIC中，最多可以安装两个节点。如果安装第二个节点，则此节点将称为辅助管理节点（辅助 PAN）。
探测功能	探测器是从给定源收集数据的机制。探测器是一个说明任何机制的通用术语，但不具体描述如何收集数据或收集什么。例如，Active Directory (AD) 探测器有助于 ISE-PIC 从 AD 收集数据，而系统日志探测器则从读取系统日志消息的解析器收集数据。
提供程序	ISE-PIC 从中接收、映射和发布用户身份信息的客户端或源。
辅助节点	ISE-PIC 部署中的主节点是主管理节点 (PAN)，您可以从此节点执行所有可用操作。在ISE-PIC中，最多可以安装两个节点。如果安装第二个节点，则此节点将称为辅助管理节点（辅助 PAN）。
用户	订用 ISE-PIC 服务以接收用户身份信息的系统。

思科 ISE-PIC 架构、部署和节点

Cisco ISE-PIC 架构包括以下组件：

- 节点 - 在思科 ISE-PIC 部署中，最多可以配置两个节点，如下所述
- 网络资源
- 终端

具有单个 Cisco ISE-PIC 节点的部署称为独立部署。

具有两个思科 ISE-PIC 节点的部署称为高可用性部署，其中一个节点用作主要设备（主管理节点，即 PAN）。高可用性部署可提高服务可用性。

PAN 提供此网络模型所需的所有配置功能，并提供备份角色的辅助思科 ISE 节点（辅助 PAN）功能。辅助节点支持主节点，并在与主节点失去连接时恢复功能。

思科 ISE-PIC 会将位于主思科 ISE-PIC 节点上的所有内容与辅助思科 ISE-PIC 节点同步或进行复制，以确保您的辅助节点与主节点的状态一致（因此可用作备份）。

ISE 社区资源

有关部署和扩展的信息，请参阅ISE 部署历程。

注释 从思科 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）。

前提条件和虚拟设备要求

ISE-PIC 仅支持虚拟机。虚拟机应基于思科 SNS 3500 或 3600 系列设备规格。

有关 SNS-3500 系列设备，请参阅 Cisco SNS-3500 系列设备硬件安装指南。

有关 SNS-3600 系列设备，请参阅思科 SNS-3600 系列设备硬件安装指南。

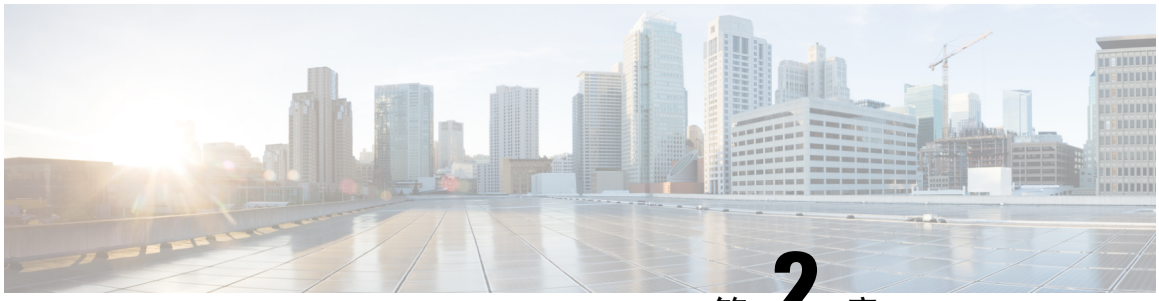
安装思科 ISE-PIC 的其他前提条件和系统要求如下表所述。

表 *1:* 虚拟设备要求和前提条件

类型	说明
虚拟设备	思科 ISE-PIC 节点的虚拟机要求、前提条件和相关程序与普通思科 ISE 节点相同。 思科 ISE-PIC 支持类似于思科 ISE 的小型、中型和大型部署模式。为了实现最佳性能，确保在使用ISO映像手动安装思科ISE-PIC时分配同等的资源预留。 思科 ISE-PIC 可安装在以下虚拟平台上： • VMware 虚拟机 • Linux KVM • Microsoft Hyper-V • Nutanix AHV 有关虚拟机要求的详细信息，请参阅《思科身份服务引擎安装指南》。 请务必遵循《思科身份服务引擎安装指南》中概述的配置前提条件和设置程序，以确保正确安装 ISE 或 ISE-PIC。
软件	没有特殊的操作系统或软件要求。ISE-PIC 的 ISO 映像包括所有必要的软件项目。

ISE 社区资源

有关部署和扩展的信息，请参阅ISE 部署历程。



第 2 章

安装思科 ISE-PIC

- 下载和运行 ISO 映像 ， 第 5 页
- 运行设置程序， 第 6 页
- 验证安装过程， 第 9 页

下载和运行 ISO 映像

开始之前

在任何支持的设备上安装思科 ISE-PIC 之前，请确保您：

1. 正确创建并访问虚拟机。
2. 符合如下所有固件和虚拟机要求：
   - 虚拟机 - 在安装 ISE-PIC 之前安装 OVA 模板，并确保虚拟机服务器配置正确。
   - Linux KVM - 确保满足所有虚拟化技术和硬件要求。

有关要求的详细信息，请参阅《思科 *ISE-PIC* 管理员指南》、《思科安全网络服务器产品手册》和《思科身份服务引擎安装指南》。

步骤 1 启动要安装 ISE-PIC 的虚拟机。

a) 将 CD/DVD 映射到 ISO 映像。系统随即会显示类似于以下的屏幕。以下消息和安装菜单随即会显示。

示例：

```
Please wait, preparing to boot.....................................................................
.....................................................................................................
```

将出现以下选项：

```
[1] Cisco ISE-PIC Installation (Keyboard/Monitor)
[2] Cisco ISE-PIC Installation (Serial Console)
[3] System Utilities (Keyboard/Monitor)
[4] System Utilities (Serial Console)
```

步骤 2 在启动提示符后，按 **2** 和 **Enter** 可使用串行控制台安装思科 ISE-PIC。

系统随即会显示以下消息：

```
********************************************
Please type 'setup' to configure the appliance
********************************************
```

步骤 3 在提示下，键入 **setup** 开始启动设置程序。有关设置程序参数的详细信息，请参阅运行设置程序，第 6 页。

步骤 4 在设置模式下输入网络配置参数后，设备会自动重新启动并返回到外壳提示符模式。

步骤 5 从外壳提示模式退出。设备即会正常运行。

步骤 6 继续执行验证安装过程，第 9 页。

运行设置程序

本部分介绍配置 ISE-PIC 服务器的设置过程。

设置过程会启动交互式命令行界面 (CLI)，提示您提供所需的参数。管理员可以使用控制台或哑终端配置初始网络设置，并使用设置程序为 ISE-PIC 服务器提供初始管理员凭证。此设置流程是一次性配置任务。

注释 如果要与 Active Directory (AD) 集成，最好使用专门为 ISE 创建的专用站点的 IP 和子网地址。在安装和配置之前，请咨询组织中负责 AD 的人员，并检索 ISE 节点的相关 IP 和子网地址。

注释 建议您不要尝试离线安装思科 ISE，因为这可能导致系统不稳定。在离线运行思科 ISE 安装脚本时会显示以下错误：

无法与 NTP 服务器同步。时间不正确可能导致系统无法使用，直到其被重新安装。Retry? 是/否 [是]：

选择**是 (Yes)** 继续安装。选择**否 (No)** 重试与 NTP 服务器同步。

建议在运行安装脚本时与 NTP 服务器和 DNS 服务器建立网络连接。

要运行设置程序，请执行以下操作：

步骤 1 打开指定用于安装的设备。

系统随即会显示以下设置提示：

```
Please type ‘setup’ to configure the appliance
localhost login:
```

步骤 2 在登录提示下，输入 **setup** 并按 **Enter**。

控制台随即会显示一组参数。您必须按照下表中的说明输入参数。

注释　　如果要添加具有 IPv6 地址的域名服务器或 NTP 服务器，ISE 的 eth0 接口必须静态配置有 IPv6 地址。

表 *2*: 思科 *ISE-PIC* 设置程序参数

提示	说明	示例
Hostname	不得超过 19 个字符。有效字符包括字母数字（A－Z、a－z、0－9）和连字符 (-)。第一个字符必须是字母。	isebeta1
(eth0) Ethernet interface address	必须是千兆以太网 0 (eth0) 接口的有效 IPv4 或全局 IPv6 地址。	10.12.13.14/ 2001:420:54ff:4::458:121:119
Netmask	必须是有效的 IPv4 或 IPv6 网络掩码。	255.255.255.0/ 2001:420:54ff:4::458:121:119/122
Default gateway	必须是默认网关的有效 IPv4 或全局 IPv6 地址。	10.12.13.1/ 2001:420:54ff:4::458:1
DNS domain name	不能是 IP 地址。有效字符包括 ASCII 字符、任意数字、连字符 (-) 和句点 (.)。	example.com
Primary name server	必须是主域名服务器的有效 IPv4 或全局 IPv6 地址。	10.15.20.25 / 2001:420:54ff:4::458:118
Add/Edit another name server	必须是主域名服务器的有效 IPv4 或全局 IPv6 地址。	（可选）允许您配置多个域名服务器。要执行此操作，请输入**y**继续。
Primary NTP server	必须是网络时间协议 (NTP) 服务器的有效 IPv4 或全局 IPv6 地址或主机名。 注释　　确保主 NTP 服务器可访问。	**clock.nist.gov** / 10.15.20.25 / 2001:420:54ff:4::458:117
Add/Edit another NTP server	必须是有效的 NTP 域。	（可选）允许您配置多个 NTP 服务器。要执行此操作，请输入**y**继续。

提示	说明	示例
System Time Zone	必须是有效时区。例如，对于太平洋标准时间 (PST)，System Time Zone 为 PST8PDT（或协调世界时 (UTC) 减 8 小时）。 **注释** 确保系统时间和时区与 CIMC 或虚拟机监控程序主机操作系统时间和时区匹配。如果时区之间存在任何不匹配，系统性能可能会受到影响。 要获得受支持时区的完整列表，您可以从思科 ISE-PIC CLI 运行 **show timezones** 命令。	UTC （默认值）
Username	识别对思科 ISE-PIC 系统进行 CLI 访问所用的管理用户名。如果选择不使用默认值 (admin)，则必须创建新用户名。用户名的长度必须为三至八个字符，并且由有效的字母数字字符（A－Z、a－z 或 0－9）组成。	admin（默认值）
Password	识别对思科 ISE-PIC 系统进行 CLI 访问所用的管理密码。由于没有默认密码，您必须创建此密码才能继续。密码长度必须至少为六个字符，并且至少包含一个小写字母 (a－z)、一个大写字母 (A－Z) 和一个数字 (0－9)。	MyIseYPass2

注释 在 CLI 中进行安装时或完成安装后，当为管理员创建密码时，请勿在密码中使用 $ 字符（除非是将其作为密码的最后一个字符）。如果在密码开头或中间使用此字符，系统虽然会接受此密码，但您无法使用此密码登录 CLI。

如果您无意中创建了此类密码，请登录控制台并使用 CLI 命令或使用 ISE CD 或 ISO 文件来重置密码。有关如何使用 ISO 文件重置密码的说明，可在以下文档中找到： https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/200568-ISE-Password-Recovery-Mechanisms.html

运行设置程序后，系统会自动重新引导。

现在，您可以用设置过程中配置的用户名和密码登录到思科 ISE-PIC。

验证安装过程

要验证您是否已正确完成安装过程，请执行以下操作：

步骤 1 一旦系统在安装后自动重新引导，在登录名提示下输入您在设置期间配置的用户名，然后按 **Enter**。

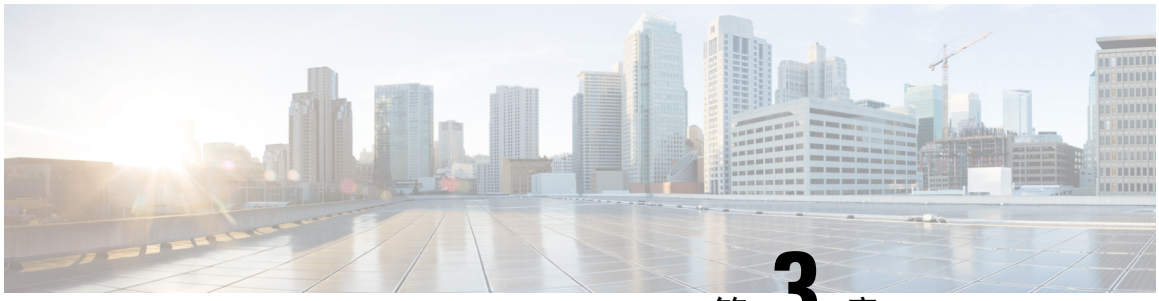
步骤 2 在密码提示下输入您在设置期间配置的密码，然后按 **Enter**。

步骤 3 输入 **show application** 命令验证应用是否已正确安装，然后按 **Enter**。

步骤 4 输入 **show application status ise** 命令检查 ISE-PIC 进程的状态，然后按 **Enter**。
系统随即会显示以下消息：

```
ise-server/admin# show application status ise

ISE PROCESS NAME                       STATE            PROCESS ID
------------------------------------------------------------------
Database Listener                      running          5072
Database Server                        running          90 PROCESSES
Application Server                     running          9117
AD Connector                           running          14187
Certificate Authority Service          running          9947
M&T Session Database                   running          6408
M&T Log Collector                      running          10166
M&T Log Processor                      running          10057
pxGrid Infrastructure Service          running          22303
pxGrid Publisher Subscriber Service    running          22575
pxGrid Connection Manager              running          22516
pxGrid Controller                      running          22625
PassiveID WMI Service                  running          10498
PassiveID Syslog Service               running          11483
PassiveID API Service                  running          12176
PassiveID Agent Service                running          13046
PassiveID Endpoint Service             running          13557
PassiveID SPAN Service                 running          13993
snsbu-c220-ORX/admin#
```



第 3 章

升级思科 ISE-PIC

- 思科 ISE-PIC 升级概览， 第 11 页
- 验证数据以防止升级失败， 第 12 页
- 必须开放用于通信的防火墙端口， 第 15 页
- 从主管理节点备份思科 ISE-PIC 的配置和运行数据， 第 15 页
- 从主管理节点备份系统日志， 第 16 页
- 检查证书有效性， 第 16 页
- 导出证书和私钥， 第 16 页
- 禁用计划备份， 第 16 页
- 配置 NTP 服务器和验证可用性， 第 17 页
- 升级双节点部署， 第 17 页
- 升级独立节点， 第 18 页
- 验证升级过程， 第 19 页
- 从升级失败中恢复， 第 19 页
- 回滚到之前版本的 ISO 映像， 第 21 页
- 升级后的任务， 第 22 页

思科 ISE-PIC 升级概览

本章介绍了如何将虚拟机上的思科 ISE-PIC 软件从 版本 2.6 或 2.7 升级到版本 3.1。

思科 ISE-PIC 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。每升级 15 GB 数据大约需要 240 分钟 + 60 分钟。

可能影响升级时间的因素包括：

- 网络中的终端和用户
- 主节点中的日志数

您必须使用思科 ISE 升级捆绑包来升级思科 ISE-PIC。您可以从 Cisco.com 下载升级捆绑包。以下升级捆绑包适用于：

- ise-upgradebundle-2.6.x-3.0.x-to-3.1.0.458.SPA.x86_64.tar.gz

要在最短的停机时间内升级您的部署，同时提供最大恢复能力和回滚能力并尽量减少错误，请按照以下顺序执行升级：

1. 在开始升级之前备份所有配置数据，以确保在必要时可手动轻松回滚。
2. 根据您的部署选择升级过程：
   - 独立式部署
     1. 升级节点。请参阅 升级独立节点，第 18 页。
     2. 在升级节点后运行升级验证和网络测试。有关详情，请参阅 验证升级过程，第 19 页。

     注释 有关此步骤各部分的详细信息，请参阅：
     - 升级双节点部署，第 17 页
     - 验证升级过程，第 19 页

   - **高可用性（两个节点）部署**
     1. 首先升级辅助节点，在确认辅助节点升级之前将PAN保留为之前的版本，以便在初始升级失败时使用 PAN 进行回滚。
     2. 在升级辅助节点后运行升级验证和网络测试。
     3. 升级 PAN。

        升级两个节点后，辅助管理节点现在就成为了主管理节点，并安装了升级后的版本；而原来的主管理节点现在成为了二级管理节点，并且也安装了升级后的版本。
     4. 在您升级主管理节点后，重新进行升级验证和网络测试。
     5. 如果完成了升级原来的主节点（第二次升级），在当前辅助节点的**编辑节点 (Edit Node)**窗口中单击**提升为主节点 (Promote to Primary)**，以便根据需要将它提升为主管理节点（就像在您的旧部署中）。

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-PIC 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，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，请勿在主管理节点上运行 URT。

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

1. 验证 URT 是在思科 ISE-PIC 独立节点上运行，还是在辅助管理节点上运行
2. 检查 URT 捆绑包是不是在 45 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
3. 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
   - 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
4. 克隆配置数据库
5. 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。
6. 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。

步骤 1 创建存储库并复制 URT 捆绑包，第 14 页

步骤 2 运行升级就绪工具，第 14 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 下载 URT 捆绑包。您必须使用面向思科 ISE-PIC 的思科 ISE URT 捆绑包。

步骤 2 （可选）为了节省时间，将 URT 捆绑包复制到思科 ISE-PIC 节点上的本地磁盘。

```
copy repository_url/path/ise-urtbundle-3.0.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-3.0.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-3.0.*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-filename 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。

必须开放用于通信的防火墙端口

如果您在主管理节点和辅助节点之间部署了防火墙，则升级前必须开放以下端口：

- TCP 1521 - 用于主管理节点之间的通信。
- TCP 443 - 用于主管理节点与辅助节点之间的通信。
- 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。

如需思科 ISE-PIC 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-PIC 的配置和运行数据

从命令行界面 (CLI) 获取思科 ISE-PIC 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-PIC 在 VMware 上运行时，不支持用 VMware 快照备份 ISE-PIC 数据。

VMware 快照在特定时间保存 VM 的状态。在多节点思科 ISE-PIC 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-PIC 中包含的备份功能来存档和恢复数据。

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

您还可以从思科 ISE 管理门户获取思科 ISE-PIC 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。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。

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。

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

检查证书有效性

如果思科 ISE-PIC 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。

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）。
- 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）。

禁用计划备份

在思科 ISE-PIC 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：

- 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-PIC 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-PIC 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。

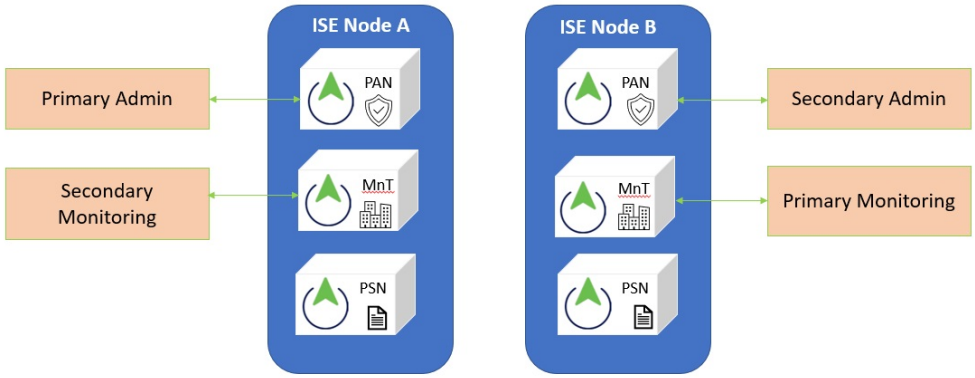
确保您的网络中的 NTP 服务器可以在升级过程中可建立连接、可响应且可同步。

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 服务器同步故障故障排除。

升级双节点部署

使用 **application upgrade prepare** 和 **proceed** 命令升级双节点部署。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。辅助节点的升级完成后，随后升级主节点。

图 *1:* 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。

步骤 1 通过 CLI 升级辅助节点。

升级过程自动从部署中删除原始辅助节点并对其进行升级。重新启动后，原始辅助节点将成为主节点。

步骤 2 升级原始主节点。

升级过程自动在部署中注册原始主节点，并将其指定为升级后环境中的辅助节点。

步骤 3 现在将辅助节点升级为新部署中的主节点。

升级完成后确保运行 **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 19 页

升级独立节点

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

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-PIC 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** 和 **application upgrade proceed** 命令。**application upgrade prepare** 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-PIC 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** 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-PIC 命令行界面 (CLI) 中，输入 **application upgrade prepare** 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-PIC CLI 中，输入 **application upgrade proceed** 命令。

下一步做什么

验证升级过程，第 19 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-PIC CLI 输入以下命令：**show logging system ade/ADE.log**
- 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。

从升级失败中恢复

本部分介绍在升级失败时应执行哪些操作进行恢复。

在极少数情况下，您可能必须重新映像、执行全新安装并还原数据。因此在开始升级之前，您需要对思科 ISE-PIC 配置数据进行备份。尽管在配置数据库发生故障的情况下我们会自动尝试回滚更改，但您还是需要对配置数据进行备份。

升级失败

本节介绍一些已知的升级错误，以及要从错误中恢复所要执行的操作。

注释 您可以通过 CLI 检查升级日志或从控制台检查升级状态。登录到 CLI，或通过思科 ISE-PIC 节点的控制台以查看升级过程。您可以使用 **show logging application** 命令，从思科 ISE-PIC CLI 查看以下日志（示例文件名在括号中给出）：

- 数据库数据升级日志 (*dbupgrade-data-global-20160308-154724.log*)
- 数据库方案日志 (*dbupgrade-schema-20160308-151626.log)*
- 操作系统升级后日志 (*upgrade-postosupgrade-20160308-170605.log*)

配置和数据升级错误

在升级期间，配置数据库架构和数据升级故障自动回滚。您的系统会返回到上次已知的良好状态。如果遇到这种情况，控制台上和日志中会显示以下消息：

```
% Warning: The node has been reverted back to its pre-upgrade state.
error: %post(CSCOcpm-os-1.4.0-205.i386) scriptlet failed, exit status 1
% Application upgrade failed. Please check logs for more details or contact Cisco Technical
 Assistance Center for support.
```

补救错误

如果您需要补救升级失败，让节点返回到原始状态，则控制台上会显示以下消息。查看日志以了解详细信息。

```
% Warning: Do the following steps to revert node to its pre-upgrade state."
error: %post(CSCOcpm-os-1.4.0-205.i386) scriptlet failed, exit status 1
% Application upgrade failed. Please check logs for more details or contact Cisco Technical
 Assistance Center for support.
```

验证错误

验证错误不是真正的升级失败。可能会出现验证错误。例如， 系统达不到指定要求，您可能会看到此错误。系统返回到上次已知的良好状态。如果遇到此错误，请确保您如本文档中所述执行升级。

```
STEP 1: Stopping ISE application...
% Warning: Cannot upgrade this node until the standby PAP node is upgraded and running. If
 standbyPAP is already upgraded
and reachable ensure that this node is in SYNC from current Primary UI.
Starting application after rollback...

% Warning: The node has been reverted back to its pre-upgrade state.
error: %post(CSCOcpm-os-1.4.0-205.i386) scriptlet failed, exit status 1
% Application upgrade failed. Please check logs for more details or contact Cisco Technical
 Assistance Center for support.
```

应用二进制升级错误

如果 ADE-OS 或应用二进制升级失败，那么在系统重启之后，当您通过 CLI 运行 **show application status ise** 命令时，会显示以下消息。您应重新映像并还原配置和运行备份。

```
% WARNING: An Identity Services Engine upgrade had failed. Please consult logs. You have
to reimage and restore to previous version.
```

其他错误类型

对于任何其他类型的故障（包括取消升级、控制台会话断开、电源故障等），您必须根据节点上原本启用的角色，重新映像并还原备份。

重新映像

重新映像一词是指思科 ISE-PIC 的全新安装。在重新映像前，确保您已通过运行 **backup-logs** CLI 命令生成支持捆绑包，并将该捆绑包放于远程存储库中，以帮助查明故障原因。您必须重新映像至旧或新版本，如下所示：

- 辅助管理节点 - 重新映像至旧版本并还原配置和运行备份。

- 主管理节点 - 如果PAN的升级失败，系统通常会返回到上次已知的良好状态。如果系统不回滚到旧版本，您可以重新映像至新版本，在新部署中注册。

发生故障后升级

如果升级失败，再次尝试升级前执行以下操作：

- 分析日志。检查支持捆绑包是否存在错误。
- 将您生成的支持捆绑包提交至思科技术支持中心 (TAC)，识别并解决问题。

注释 您可以查看升级进度，方法是通过 SSH 登录并使用 **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…

二进制安装期间升级失败

问题 数据库升级后需要进行应用二进制升级。如果二进制升级失败，则控制台和 ADE.log 上会显示以下消息：

```
% Application install/upgrade failed with system removing the corrupted install
```

解决方法 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。

要执行回滚操作，请使用之前的 ISO 映像重新映像思科 ISE-PIC 设备，并从备份文件还原数据。每次重试升级时，您都需要有新的升级捆绑包。

- 分析日志。检查支持捆绑包是否存在错误。
- 将您生成的支持捆绑包提交至思科技术支持中心 (TAC)，识别并解决问题。

回滚到之前版本的 ISO 映像

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-PIC 设备。恢复数据后，您可以在旧部署中注册。因此，我们建议您在开始升级之前备份思科 ISE-PIC 配置数据。

有时，因为配置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。

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。

升级后的任务

请参阅《身份服务引擎被动身份连接器 *(ISE-PIC)* 管理员指南》，了解各项任务的其他详细信息。

清除浏览器高速缓存

升级后，请确保先清除浏览器高速缓存、关闭浏览器并打开新的浏览器会话，然后再接入思科ISE-PIC管理员门户。

重新配置 Active Directory 加入点

升级期间 Active Directory 加入点可能会丢失。登录到管理员门户，然后导航检查是否需要重新配置加入点。

配置 Active Directory 身份搜索属性

思科 ISE-PIC 使用属性 SAM、CN 或两者来识别用户，而 sAMAccountName 属性是默认属性。

如果环境需要，您可以配置思科 ISE-PIC 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-PIC 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**提供程序 (Providers)** > **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。
   - **Comment** - 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。

配置反向 DNS 查找

确保从 DNS 服务器为双节点部署中的所有思科 ISE-PIC 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。

恢复思科 CA 证书和密钥

从主管理节点获取思科ISE-PIC CA 证书和密钥的备份，并在辅助管理节点上恢复备份。这样，即便发生 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。

重新配置强制 ISE-PIC 系统设置

- 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/或过滤器。默认情况下，升级后所有警报均会启用。