思科身份服务引擎升级指南，版本 1.4

首次发布日期: 2015 年 02 月 12 日

上次修改日期: 2015 年 04 月 30 日

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

本手册中有关产品的规格和信息如有更改，恕不另行通知。本手册中的所有声明、信息和建议均准确可靠，但我们不为其提供任何明示或暗示的担保。用户必须承担使用产品的全部责任。

随附产品的软件许可和有限担保在随产品一起提供的信息包中提供，且构成本文的一部分。如果您无法找到软件许可或有限担保，请与思科代表联系以获取副本。

思科所采用的 TCP 报头压缩是加州大学伯克利分校 (UCB) 开发的一个程序的改版，是 UCB 的 UNIX 操作系统公共域版本的一部分。保留所有权利。版权所有 © 1981，加州大学董事会。

无论本手册中是否有任何其他保证，这些供应商的所有文档文件和软件均按“原样”提供，并可能包含缺陷。思科和上面所提及的提供商拒绝所有明示或暗示担保，包括（但不限于）适销性、特定用途适用性和无侵权担保，或者因买卖或使用以及商业惯例所引发的担保。

在任何情况下，对于任何间接、特殊、连带发生或偶发的损坏，包括（但不限于）因使用或无法使用本手册而导致的任何利润损失或数据损失或损坏，思科及其供应商概不负责，即使思科及其供应商已获知此类损坏的可能性也不例外。

本文档中使用的任何互联网协议 (IP) 地址和电话号码并非实际地址和电话号码。本文档中所含的任何示例、命令显示输出、网络拓扑图和其他图形仅供说明之用。说明性内容中用到的任何真实 IP 地址或电话号码纯属巧合，并非有意使用。

思科和思科徽标是思科和/或其附属公司在美国和其他国家/地区的商标或注册商标。要查看思科商标列表，请访问此网址：http://www.cisco.com/go/trademarks。文中提及的第三方商标为其相应所有者的财产。“合作伙伴”一词的使用并不意味着思科和任何其他公司之间存在合作伙伴关系。(1110R)

目 录

第 1 章

准备工作

开始升级前，仔细阅读下列信息，并尽可能记录这些配置（备份、导出、获取屏幕截图）：

支持的升级路径

您可以从以下任何版本直接升级到思科 ISE 版本 1.4：

- 思科 ISE 版本 1.2 补丁 14 或更高版本
- 思科 ISE 版本 1.2.1 补丁 5 或更高版本

- 思科 ISE 版本 1.3 或更高版本

如果您的版本早于思科 ISE 版本 1.2 补丁 14，则必须先升级到上述版本之一，然后才能升级到版本 1.4。

从 Cisco Secure ACS 迁移至思科 ISE

您只能从 Cisco Secure ACS 版本 5.5 和 5.6 直接迁移至思科 ISE 版本 1.4。有关从 Cisco Secure ACS 版本 5.5 和 5.6 迁移至思科 ISE 版本 1.4 的信息，请参阅 思科身份服务引擎迁移工具指南。

您无法从下列版本或设备迁移至版本 1.4：Cisco Secure ACS 4.x 或更早的版本，Cisco Secure ACS 5.1、5.2、5.3 或 5.4，或者思科网络准入控制 (NAC) 设备。要从 Cisco Secure ACS 版本 4.x、5.1、5.2、5.3 和 5.4 迁移，您必须先升级到 ACS 版本 5.5 或 5.6，然后再迁移至思科 ISE 版本 1.4。

可用的升级捆绑包

您可以选择下列升级捆绑包之一，升级到版本 1.4：

- 要从版本 1.2 或 1.2.1 升级到 1.4，请使用 **ise-upgradebundle-1.2.x-to-1.4.0.253.x86_64.tar.gz**。MD5 校验和为 6c12533aee5f5e6995fe0518d086fbbe。
- 要从版本 1.3 升级到 1.4，请使用 **ise-upgradebundle-1.4.0.253.x86_64.tar.gz**。MD5 校验和为 35a159416afd0900c9da7b3dc6c72043。

升级所需的时间

升级时间估算

取决于几个因素，升级所需的具体实际时间或会有所不同。如果您有多个 PSN 作为节点组的一部分，则在升级过程中，您的生产网络会继续正常运行，而不会停机。

升级思科 ISE 节点所需的最长时间为 2 小时。如果升级不完整，升级过程在 2 小时后超时。

影响升级时间的因素

- 网络中的端点数量
- 网络中的用户和访客用户的数量
- 数量登录监控或独立节点
- 分析服务（如果启用）

注释 升级虚拟机上 Cisco ISE 节点所需的时间可能比物理设备更长。

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。

对 UCS 和 IBM 设备的网络接口卡 (NIC) 进行排序

注释 如果您从 Cisco ISE 版本 1.2 或 1.2.1 直接升级到任何更高的版本，则本节内容适用。

网络接口卡 (NIC) 与 Cisco UCS SNS 3415 和 Cisco UCS SNS 3495 以及 IBM Cisco ISE 3315 设备连接的顺序可能会影响到升级。您应确保执行升级前的检查，然后再对 NIC 进行排序。

升级前检查 UCS 和 IBM 设备的 NIC

升级过程中，UCS 和 IBM 设备上的 NIC 的排序可能会带来潜在问题。

对于 UCS 设备，Intel NIC 应为 eth0 和 eth1，而 Broadcom NIC 应为 eth2 和 eth3。

对于 IBM 设备，Broadcom NIC 应为 eth0 和 eth1，而 Intel NIC 应为 eth2 和 eth3。

- 使用 **show inventory** 命令检查 UCS 设备的 NIC 排序。如果顺序不正确，**show inventory** 命令将显示以下输出。

```
Hard Disk Count(*):  1
Disk 0:  Device Name:  /dev/sda
Disk 0:  Capacity:600.10 GB
Disk 0:  Geometry:  255 heads 63 sectors/track  72961 cylinders
NIC count:  4
NIC 0: Device Name: eth0
NIC 0:  HW Address: 00:10:18:D4:FC:EC
NIC 0:  Driver Descr:  Broadcom NetXtreme II  BCM5706/5708/5709/5716 Driver
NIC 1:  Device Name: eth1
NIC 1:  HW Address: 00:10:18:D4:FC:EE
NIC 1:  Driver Descr:  Broadcom NetXtreme II  BCM5706/5708/5709/5716 Driver
NIC 2:  Device Name: eth2
NIC 2:  HW Address: 60:73:5C:69:59:26
NIC 2:  Driver Descr:   Intel(R) Gigabit Ethernet Network Driver
NIC 3:  Device Name: eth3
NIC 3:  HW Address: 60:73:5C:69:59:27
NIC 3:  Driver Descr:  Intel(R) Gigabit Ethernet Network Driver

(*) Hard Disk Count may be Logical
```

- 使用 **show inventory** 命令检查 IBM 设备的 NIC 排序。如果顺序不正确，**show inventory** 命令将显示以下输出。

```
Cisco Identity Service Engine
------------------------------------------------------------------------
Version              :  1.2.0.899
Build Date           :  Wed Jul 24 01:37:31  2013
Install Date         :  Thu Nov 20 04:12:01 2014

acsview-srv11/admin# sh inventory | include NIC
NIC count:  4
NIC 0: Device Name: eth0
NIC 0:  HW Address: 00:15:17:CA:D8:62
NIC 0:  Driver Descr:  Intel(R) PRO/1000 Network Driver
NIC 1:  Device Name: eth1
NIC 1:  HW Address: 00:15:17:CA:D8:63
NIC 1:  Driver Descr:  Intel(R) PRO/1000 Network Driver
NIC 2:  Device Name: eth2
NIC 2:  HW Address: 00:21:5E:95:7F:44
NIC 2:  Driver Descr:  Broadcom Tigon3 ethernet Driver
NIC 3:  Device Name: eth3
NIC 3:  HW Address: 00:21:5E:95:7F:45
NIC 3:  Driver Descr:  Broadcom Tigon3 ethernet Driver
acsview-srv11/admin#
```

执行升级前检查后对 NIC 进行排序

执行升级前检查后，如果需要交换NIC，请确保您具有该设备的物理访问权限。此外，开始升级前，请确保您已备份所有最新的配置和操作文件。

请参阅适用于不同的部署类型的升级方法一章，了解更多信息。如本指南中所述，在升级过程中，设备会重新启动两次。此时，系统会显示以下消息。

```
% NOTICE: The appliance will reboot twice to upgrade software and ADE-OS. During this time
 progress of the upgrade is visible on console.
 It could take up to 30 minutes for this to complete. Rebooting to do Identity Service
Engine upgrade...
```

看到上述通知后，应交换以下接口的以太网电缆，而无需切断电源。

eth0 <> eth2

eth1 <> eth3

如果显示通知时无法交换以太网电缆，则请等待升级完成。重新启动两次后，系统将显示登录提示。您可以执行 **show application status** 命令验证升级是否完成。您可以在验证升级过程，第 16 页一节中查看完整的验证步骤。当确认升级已经完成后，您可以按如上所述交换以太网电缆，并使用 **reload** 命令重新启动设备。

对升级后的网络中断和应用启动故障进行故障排除

如果对 NIC 进行排序后遇到问题，例如网络中断或应用启动故障，请检查所下载捆绑包的版本。有可能您下载了捆绑包之前的版本，从而导致 NIC 的状态不一致。验证捆绑包是否具有以下 MD5 校验和：

- ise-upgradebundle-1.2.x-to-1.4.0.253.x86_64.tar.gz—MD5: 6c12533aee5f5e6995fe0518d086fbbe
- ise-upgradebundle-1.4.0.253.x86_64.tar.gz—MD5: 35a159416afd0900c9da7b3dc6c72043

如果由于使用较旧版本的捆绑包而导致升级后出现网络中断或应用启动故障，可以重新映像具有 Cisco ISE 1.2 软件的故障节点，在旧部署中注册该节点并还原操作备份（如果节点具有监控角色）。然后，您可以尝试使用最新版本的捆绑包再次执行升级。此恢复步骤适用于辅助管理节点，这是部署过程中要升级的第一个节点。

对于部署中的其他节点，您可以使用相同的步骤或直接重新映像具有 Cisco ISE 1.4 软件的节点，在新部署中注册该节点并还原备份操作（如有）。

确保按照“执行升级前检查后对网络接口卡 (NIC) 进行排序”一节中所述的步骤操作。

如果是独立的节点，您可以重新映像具有 Cisco ISE 1.4 软件的节点，并还原配置和操作备份。

如果上述所有步骤均不成功，并且您在 ISE 升级后遇到网络连接故障的问题，请联系思科 TAC。

VMware 虚拟机的设置

如果您要升级虚拟机 (VM) 上版本为 1.2 或 1.2.1 的 Cisco ISE 节点，升级后请务必关闭 VM，将访客操作系统更改为 Red Hat Enterprise Linux 6（64 位），完成更改后再次启动 VM。

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）。

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。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。

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 ise-upgradebundle-1.4.0.253.x86_64.tar.gz* **disk:/**

例如，**copy sftp://***aaa.bbb.ccc.ddd ise-upgradebundle-1.4.0.253.x86_64.tar.gz* **disk:/**

其中，*aaa.bbb.ccc.ddd* 是 SFTP 服务器的 IP 地址或主机名， *ise-upgradebundle-1.4.0.253.x86_64.tar.gz* 是升级捆绑包的名称。

将升级捆绑包复制到本地磁盘可以节约升级过程的时间。执行 **application upgrade prepare** 命令，可将升级捆绑包复制到本地磁盘并提取文件。

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*

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，这些存储库类型为只读或者协议不支持文件列表。

1. 依次选择 **管理 (Administration) > 系统 (System) > 备份和恢复 (Backup and Restore)**。
2. 点击**立即备份 (Backup Now)**。
3. 根据需要输入值以执行备份。
4. 点击 **OK**。
5. 验证备份是否成功完成。

   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。

   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。

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*

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。

在生产环境中使用前检查实验室设置中的自定义门户迁移

注释 仅在您从 Cisco ISE 版本 1.2 或 1.2.1 直接升级到更高的版本时，本节内容适用。

Cisco ISE 将带来全新的简化后的访客和员工注册体验，以及全新的门户自定义体验，并提供从多语言支持到WYSIWYG自定义等大量新功能。当您升级到新版本时，所有自定义门户都将迁移至全新的 ISE 体验。以下列出您必须了解的几个注意事项：

- 通过升级过程，将之前版本的 ISE 中使用 CSS 和 HTML 完成的基本外观和自定义迁移到全新的访客和个人设备流程。
- 使用基本 HTML 和本地管理工具完成的自定义应能正确地迁移。使用 JavaScript 修改访客流程的自定义可能无法正确地迁移。升级后，您可以从 ISE 管理员门户重新创建这些门户。
- 您无法编辑迁移到新版本的任何自定义门户。如果您要更改外观、流程或功能，就必须在升级后从 ISE 管理员门户创建新的门户。
- ISE 1.2 和 1.2.1 的客户能够进行各种门户自定义。其中一些自定义可能无法如预期迁移至新版本。我们建议您在生产环境中使用前，检查实验室设置中新迁移的门户。
- 升级后，当您执行下列操作时，ISE 无法创建访客帐户：

  1. 在 ISE 1.2 或 1.2.1 中将访客门户配置为允许自助服务
  2. 自定义门户期间对时区值进行硬编码
  3. 通过 ISE 升级过程将自定义门户迁移至新版本

  发生这种情况是因为自定义门户中硬编码的时区值可能与新版本中的访客位置名称不匹配。ISE 1.2 和 1.2.1 版本中的“时区”在新版本中重命名为“访客位置”。

  解决办法是，升级到新版本后，将您在 1.2 或 1.2.1 版本中进行硬编码的相同时区作为访客位置添加到新版本中。为此，请从ISE管理员门户中，选择 **Guest Access** > **Settings** > **Guest Locations and SSIDs**，在“位置名称”文本框中，选择相应的时区，然后点击 **Add** 并保存设置。

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。

否则，MDM 重定向的现有授权配置文件不会随 MDM 供应商详细信息一起更新。升级后，您必须手动更新激活供应商的上述配置文件，然后用户才能再次进入注册流程。

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(Administration > System > Deployment > <*node*> > Profiling Configuration)。您可以记录该配置或获取屏幕截图。

第 2 章

适用于不同的部署类型的升级方法

请参阅本章中的以下小节，了解有关如何在下列不同类型的部署上执行升级的信息：

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 执行 **application upgrade** 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 **application upgrade** 命令，从而节省升级时间。或者，您可以使用下述 **application upgrade prepare** 和 **application upgrade proceed** 命令。

运行 **application upgrade prepare** 命令下载升级捆绑包，并将其提取到本地。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。

开始之前

确保您已阅读“升级前的准备工作”一章中的说明。

过程

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 从思科 ISE 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。

示例：

```
ise/admin# application upgrade prepare ise-upgradebundle-1.4.0.253.x86_64.tar.gz upgrade
Getting bundle to local machine...
 md5: 35a159416afd0900c9da7b3dc6c72043
 sha256: e3358ca424d977af67f8bb2bb3574b3e559ce9578d2f36c44cd8ba9e6dddfefd
% Please confirm above crypto hash matches what is posted on Cisco download site.
% Continue? Y/N [Y] ?
```

步骤 3 输入 **Y** 继续。
从升级包中提取文件。系统将显示以下消息：

示例：

```
Getting bundle to local machine...
 md5: 35a159416afd0900c9da7b3dc6c72043
 sha256: e3358ca424d977af67f8bb2bb3574b3e559ce9578d2f36c44cd8ba9e6dddfefd
% Please confirm above crypto hash matches what is posted on Cisco download site.
% Continue? Y/N [Y] ?
```

步骤 4 从思科 ISE CLI中，输入 **application upgrade proceed** 命令。

示例：

```
ise45/admin# application upgrade proceed
Initiating Application Upgrade...
% Warning: Do not use Ctrl-C or close this terminal window until upgrade completes.
STEP 1: Stopping ISE application...
STEP 2: Verifying files in bundle...
-Internal hash verification passed for bundle
STEP 3: Validating data before upgrade...
STEP 4: Taking backup of the configuration data...
STEP 5: Registering this node to primary  of new deployment...
STEP 6: Downloading configuration data from primary  of new deployment...
STEP 7: Importing configuration data...
STEP 8: Running ISE configuration data upgrade for node specific data...
STEP 9: Running ISE M&T DB upgrade...
ISE Database Mnt schema upgrade completed.

Gathering Config schema(CEPM) stats .....
Gathering Operational schema(MNT) stats ..........
% NOTICE: Upgrading ADEOS. Appliance will be rebooted after upgrade completes successfully.

% This application Install or Upgrade requires reboot, rebooting now...
```

现在，安装过程完成了。

接下来的操作

验证升级过程，第 16 页

升级双节点部署

使用 **application upgrade prepare** 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，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 *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。
- 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。

过程

步骤 1 从 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 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，并将其指定为辅助节点。

步骤 3 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）。

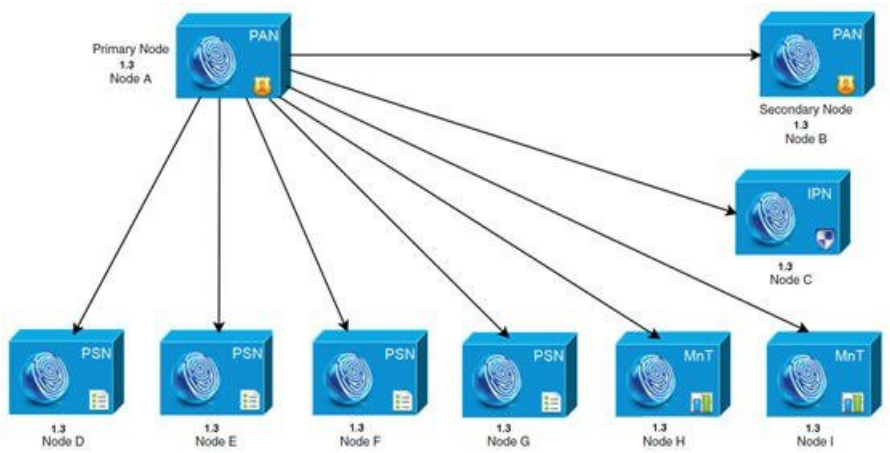
接下来的操作

验证升级过程，第 16 页

升级分布式部署

您必须先将辅助管理节点升级到新版本。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（节点 A）、一个辅助管理节点（节点 B）、一个内联状态节点 (IPN)（节点 C）、四个策略服务节点 (PSN)（节点 D、节点 E、节点 F 和节点 G），一个主监控节点（节点 H）和一个辅助监控节点（节点 I），您可以继续执行以下升级过程。

图 *2*：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** 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。

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，应采用以下升级顺序：

1. 辅助管理节点（主管理节点此时仍处于早期版本，因此如果升级失败，可用于回滚。）
2. 主监控节点
3. 策略服务节点

此时，请验证升级是否成功并进行网络测试以确保新配置可如预期一样运行。有关详细信息，请参阅验证升级过程，第 16 页。如果升级成功，请继续升级以下节点：

4 辅助监控节点

5 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。

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。
- 确保您阅读并遵循“升级前的准备工作”一章中提供的说明。
- 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。

过程

步骤 1 从 CLI 升级辅助管理节点（节点 B）。
升级过程自动从部署中取消注册节点 B 并对其进行升级。重新启动后，节点 B 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，因此升级过程会在节点 B 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。如果在旧部署中对节点 B 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（节点 H）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节点 A 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。请等待节点 A 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 接下来，升级策略服务节点（节点 D、E、F 和 G）。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。
如果您的 PSN 是节点组群集的一部分，您必须从 PAN 取消注册该 PSN，将其升级为独立节点，然后在新部署中向 PAN 注册该节点。

升级后，向新部署的主节点（节点 B）注册 PSN，并将主节点（节点 B）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 从主管理节点上取消注册 IPN 节点（节点 C）。

步骤 5 向新部署的主管理节点（节点 B）注册 IPN 节点（节点 C）。

步骤 6 如果旧部署中有第二个监控节点（节点 I），则必须执行以下操作：

a) 对节点 A 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。

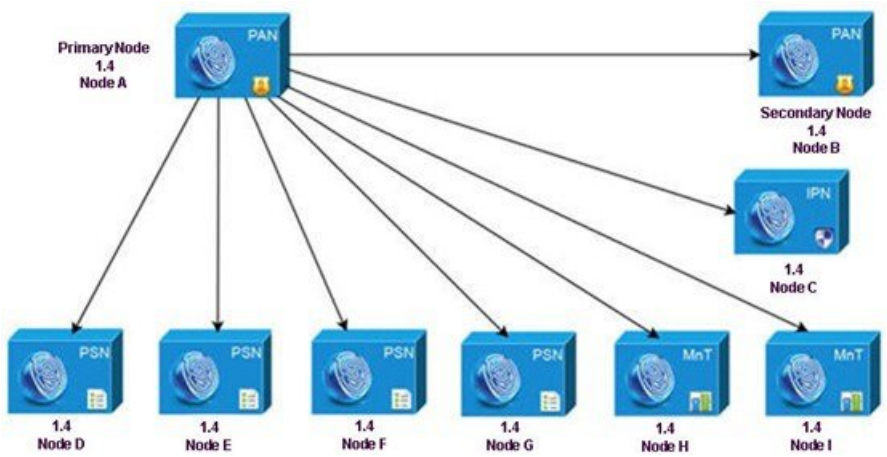
b) 将旧部署中的辅助监控节点（节点 I）升级到新部署。

除主管理节点（节点 A）外，您必须将所有其他节点升级到新部署。

步骤 7 最后，升级主管理节点（节点 A）。
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（节点 A）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）。

图 *3*：升级后的思科 *ISE* 部署



成功升级的 CLI 记录

以下是辅助管理节点成功升级的 CLI 记录示例。

```
ise74/admin# application upgrade proceed
Initiating Application Upgrade...
% Warning: Do not use Ctrl-C or close this terminal window until upgrade completes.
STEP 1: Stopping ISE application...
STEP 2: Verifying files in bundle...
-Internal hash verification passed for bundle
STEP 3: Validating data before upgrade...
STEP 4: De-registering node from current deployment.
STEP 5: Taking backup of the configuration data...
STEP 6: Running ISE configuration DB schema upgrade...
- Running db sanity check to fix index corruption, if any...
ISE Database schema upgrade completed.
STEP 7: Running ISE configuration data upgrade...
```

```
- Data upgrade step 1/77, NSFUpgradeService(1.3.0.100)... Done in 0 seconds.
- Data upgrade step 2/77, RegisterPostureTypes(1.3.0.170)... Done in 0 seconds.
- Data upgrade step 3/77, ProfilerUpgradeService(1.3.0.187)... Done in 4 seconds.
- Data upgrade step 4/77, GuestUpgradeService(1.3.0.194)... Done in 0 seconds.
- Data upgrade step 5/77, NetworkAccessUpgrade(1.3.0.200)... Done in 1 seconds.
- Data upgrade step 6/77, GuestUpgradeService(1.3.0.208)... Done in 1 seconds.
- Data upgrade step 7/77, GuestUpgradeService(1.3.0.220)... Done in 0 seconds.
- Data upgrade step 8/77, RBACUpgradeService(1.3.0.228)... Done in 9 seconds.
- Data upgrade step 9/77, NetworkAccessUpgrade(1.3.0.230)... Done in 2 seconds.
- Data upgrade step 10/77, GuestUpgradeService(1.3.0.250)... Done in 0 seconds.
- Data upgrade step 11/77, NetworkAccessUpgrade(1.3.0.250)... Done in 0 seconds.
- Data upgrade step 12/77, RBACUpgradeService(1.3.0.334)... Done in 5 seconds.
- Data upgrade step 13/77, RBACUpgradeService(1.3.0.335)... Done in 5 seconds.
- Data upgrade step 14/77, ProfilerUpgradeService(1.3.0.360)... .Done in 73 seconds.
- Data upgrade step 15/77, ProfilerUpgradeService(1.3.0.380)... Done in 2 seconds.
- Data upgrade step 16/77, NSFUpgradeService(1.3.0.401)... Done in 0 seconds.
- Data upgrade step 17/77, NSFUpgradeService(1.3.0.406)... Done in 0 seconds.
- Data upgrade step 18/77, NSFUpgradeService(1.3.0.410)... Done in 0 seconds.
- Data upgrade step 19/77, RBACUpgradeService(1.3.0.423)... Done in 0 seconds.
- Data upgrade step 20/77, NetworkAccessUpgrade(1.3.0.424)... Done in 0 seconds.
- Data upgrade step 21/77, RBACUpgradeService(1.3.0.433)... Done in 0 seconds.
- Data upgrade step 22/77, EgressUpgradeService(1.3.0.437)... Done in 0 seconds.
- Data upgrade step 23/77, NSFUpgradeService(1.3.0.438)... Done in 0 seconds.
- Data upgrade step 24/77, NSFUpgradeService(1.3.0.439)... Done in 0 seconds.
- Data upgrade step 25/77, CdaRegistration(1.3.0.446)... Done in 1 seconds.
- Data upgrade step 26/77, RBACUpgradeService(1.3.0.452)... Done in 8 seconds.
- Data upgrade step 27/77, NetworkAccessUpgrade(1.3.0.458)... Done in 0 seconds.
- Data upgrade step 28/77, NSFUpgradeService(1.3.0.461)... Done in 0 seconds.
- Data upgrade step 29/77, CertMgmtUpgradeService(1.3.0.462)... Done in 0 seconds.
- Data upgrade step 30/77, NetworkAccessUpgrade(1.3.0.476)... Done in 0 seconds.
- Data upgrade step 31/77, TokenUpgradeService(1.3.0.500)... Done in 0 seconds.
- Data upgrade step 32/77, NSFUpgradeService(1.3.0.508)... Done in 0 seconds.
- Data upgrade step 33/77, RBACUpgradeService(1.3.0.509)... Done in 8 seconds.
- Data upgrade step 34/77, NSFUpgradeService(1.3.0.526)... Done in 0 seconds.
- Data upgrade step 35/77, NSFUpgradeService(1.3.0.531)... Done in 0 seconds.
- Data upgrade step 36/77, MDMUpgradeService(1.3.0.536)... Done in 0 seconds.
- Data upgrade step 37/77, NSFUpgradeService(1.3.0.554)... Done in 0 seconds.
- Data upgrade step 38/77, NetworkAccessUpgrade(1.3.0.561)... Done in 0 seconds.
- Data upgrade step 39/77, CertMgmtUpgradeService(1.3.0.615)... Done in 1 seconds.
- Data upgrade step 40/77, CertMgmtUpgradeService(1.3.0.616)... Done in 2 seconds.
- Data upgrade step 41/77, CertMgmtUpgradeService(1.3.0.617)... Done in 0 seconds.
- Data upgrade step 42/77, OcspServiceUpgradeRegistration(1.3.0.617)... Done in 0 seconds.
- Data upgrade step 43/77, NSFUpgradeService(1.3.0.630)... Done in 0 seconds.
- Data upgrade step 44/77, NSFUpgradeService(1.3.0.631)... Done in 0 seconds.
- Data upgrade step 45/77, CertMgmtUpgradeService(1.3.0.634)... Done in 0 seconds.
- Data upgrade step 46/77, RBACUpgradeService(1.3.0.650)... Done in 3 seconds.
- Data upgrade step 47/77, CertMgmtUpgradeService(1.3.0.653)... Done in 0 seconds.
- Data upgrade step 48/77, NodeGroupUpgradeService(1.3.0.655)... Done in 0 seconds.
- Data upgrade step 49/77, RBACUpgradeService(1.3.0.670)... Done in 2 seconds.
- Data upgrade step 50/77, ProfilerUpgradeService(1.3.0.670)... .Done in 71 seconds.
- Data upgrade step 51/77, NSFUpgradeService(1.3.0.676)... Done in 0 seconds.
- Data upgrade step 52/77, AuthzUpgradeService(1.3.0.676)... Done in 0 seconds.
- Data upgrade step 53/77, GuestAccessUpgradeService(1.3.0.676)... .Done in 119 seconds.
- Data upgrade step 54/77, NSFUpgradeService(1.3.0.694)... Done in 0 seconds.
- Data upgrade step 55/77, ProvisioningRegistration(1.3.0.700)... Done in 0 seconds.
- Data upgrade step 56/77, RegisterPostureTypes(1.3.0.705)... Done in 0 seconds.
- Data upgrade step 57/77, CertMgmtUpgradeService(1.3.0.727)... Done in 0 seconds.
- Data upgrade step 58/77, CertMgmtUpgradeService(1.3.0.808)... Done in 0 seconds.
- Data upgrade step 59/77, NSFUpgradeService(1.3.0.810)... Done in 0 seconds.
- Data upgrade step 60/77, RBACUpgradeService(1.3.0.834)... Done in 9 seconds.
- Data upgrade step 61/77, ProfilerUpgradeService(1.3.0.844)... Done in 44 seconds.
- Data upgrade step 62/77, GuestAccessUpgradeService(1.3.0.855)... Done in 1 seconds.
- Data upgrade step 63/77, NSFUpgradeService(1.3.0.858)... Done in 0 seconds.
- Data upgrade step 64/77, NSFUpgradeService(1.3.0.861)... Done in 0 seconds.
- Data upgrade step 65/77, ProvisioningUpgradeService(1.3.0.876)... Done in 0 seconds.
- Data upgrade step 66/77, CertReqMgmtBootstrapService(1.4.0.0)... Done in 0 seconds.
- Data upgrade step 67/77, NSFUpgradeService(1.4.0.110)... Done in 0 seconds.
- Data upgrade step 68/77, NSFUpgradeService(1.4.0.119)... Done in 0 seconds.
- Data upgrade step 69/77, NSFUpgradeService(1.4.0.125)... Done in 0 seconds.
- Data upgrade step 70/77, NSFUpgradeService(1.4.0.157)... Done in 0 seconds.
- Data upgrade step 71/77, GuestAccessUpgradeService(1.4.0.157)... Done in 3 seconds.
- Data upgrade step 72/77, NSFUpgradeService(1.4.0.164)... Done in 0 seconds.
- Data upgrade step 73/77, MDMPartnerUpgradeService(1.4.0.166)... Done in 0 seconds.
```

```
- Data upgrade step 74/77, MDMPartnerUpgradeService(1.4.0.167)... Done in 0 seconds.
- Data upgrade step 75/77, ProfilerUpgradeService(1.4.0.175)... Done in 1 seconds.
- Data upgrade step 76/77, CertMgmtUpgradeService(1.4.0.217)... Done in 0 seconds.
- Data upgrade step 77/77, GuestAccessUpgradeService(1.4.0.253)... Done in 0 seconds.
STEP 8: Running ISE configuration data upgrade for node specific data...
 STEP 9: Making this node PRIMARY of the new deployment. When other nodes are upgraded it
will be added to this deployment.
STEP 10: Running ISE M&T DB upgrade...
ISE Database Mnt schema upgrade completed.
**Gathering Config schema(CEPM) stats ....
Gathering Operational schema(MNT) stats .......
Stopping ISE Database processes...
% NOTICE: The appliance will reboot twice to upgrade software and ADE-OS. During this time
 progress of the upgrade is visible on console. It could take up to 30 minutes for this to
 complete.
Rebooting to do Identity Service Engine upgrade...
```

以下是 PSN 节点成功升级的 CLI 记录示例。

```
ise/admin# application upgrade ise-upgradebundle-1.4.0.253.x86_64.tar.gz sftp
Save the current ADE-OS running configuration? (yes/no) [yes] ?
Please enter yes or no
Save the current ADE-OS running configuration? (yes/no) [yes] ?
Generating configuration...
Saved the ADE-OS running configuration to startup successfully
Getting bundle to local machine...
 md5: 35a159416afd0900c9da7b3dc6c72043
 sha256: 8b3b43057067b0995ecabf5673c69565c0d0dfa790dfe58d1e998aa9f8c7427a
% Please confirm above crypto hash matches what is posted on Cisco download site.
% Continue? Y/N [Y] ?
Unbundling Application Package...
Initiating Application Upgrade...
% Warning: Do not use Ctrl-C or close this terminal window until upgrade completes.
-Checking VM for minimum hardware requirements
STEP 1: Stopping ISE application...
STEP 2: Verifying files in bundle...
-Internal hash verification passed for bundle
STEP 3: Validating data before upgrade...
STEP 4: De-registering node from current deployment.
STEP 5: Taking backup of the configuration data...
STEP 6: Registering this node to primary  of new deployment...
STEP 7: Downloading configuration data from primary  of new deployment...
STEP 8: Importing configuration data...
STEP 9: Running ISE configuration data upgrade for node specific data...
STEP 10: Running ISE M&T DB upgrade...
ISE Database Mnt schema upgrade completed.
No gather stats needed as this is not PAP or MNT node

% NOTICE: Upgrading ADEOS. Appliance will be rebooted after upgrade completes successfully.

% This application Install or Upgrade requires reboot, rebooting now...
```

接下来的操作

验证升级过程，第 16 页

验证升级过程

要验证升级是否成功，请执行以下任一操作：

- 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**。
- 输入 **show version** 命令来验证 Build 版本。
- 输入 **show application status ise** 命令来验证所有服务正在运行。

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。有关详细信息，请参阅第 4 章“从失败的思科 ISE 升级中恢复”。

第 3 章

访客服务的变更

注释

本章内容仅适用于从版本 1.2 或 1.2.1 直接升级到 1.4。

访客服务的管理现在已经非常简化了。在访客接入菜单下的管理员门户中，集中进行配置。从 ISE 1.2 到更高的版本，Cisco ISE Web 门户发生了一些变化。本章列出了从版本 1.2 升级到更高版本时必须要了解的升级注意事项和依赖关系。

管理员门户的变更

下表列出了管理员门户发生的变化，并提供了 UI 导航路径和变更信息。请参考 *Cisco ISE* 管理员指南了解更多详情。

版本 1.2 中的对象名称	版本 1.2 中的 UI 导航路径	版本 1.4 中的对象名称	版本 1.4 中的 UI 导航路径	变更信息
语言模板	Administration > Web Portal Management > Settings > Portal > Language Template	语言	Guest Access > Configure > Guest Portals 或 Sponsor Portals > Edit > Portal Page Customization > Languages	在版本 1.3 及更高版本中，每种门户类型支持 15 种语言，可用于在门户中向用户显示文本。这些语言可用作单独的属性文件，并打包在单个压缩语言文件中。 版本 1.2 中创建的非默认语言会迁移至新版本。但对于这些配置文件，新版本中引入的任何新设置均被设为英文版的默认值。您必须确保这些值符合贵公司政策和标准，并在相应的语言中更新这些设置。
设备注册	Administration > Web Portal Management > Settings > Guest > Multi-Portal Configuration > Guest Portal > Edit > Operations > Guest users should be allowed to do device registration	访客设备注册设置	Guest Access > Configure > Guest Portals > Create /Edit /Duplicate > Portal Behavior and Flow Settings > Guest Device Registration Settings	在新的版本中，如果选中 **Automatically register guest devices** 复选框，设备会自动添加到端点身份组，而且访客 ID 会自动与其关联。

版本 1.2 中的对象名称	版本 1.2 中的 UI 导航路径	版本 1.4 中的对象名称	版本 1.4 中的 UI 导航路径	变更信息
时间配置文件和访客角色	Administration > Web Portal Management > Settings > Guest > Time Profiles Administration > Web Portal Management > Settings > Guest > Guest Roles Configuration Administration > Web Portal Management > Sponsor Groups > Sponsor Group > Guest Roles	访客类型	Guest Access > Configure > Guest Types	在新的版本中，如果选中 **Automatically register guest devices** 复选框，设备会自动添加到端点身份组，而且访客 ID 会自动与其关联。

版本 1.2 中的对象名称	版本 1.2 中的 UI 导航路径	版本 1.4 中的对象名称	版本 1.4 中的 UI 导航路径	变更信息
活动的访客角色	Administration > Web Portal Management > Settings > Guest > Guest Roles Configuration	允许访客绕过访客门户	Guest Access > Configure > Guest Type > Create / Edit	

版本 1.2 中的对象名称	版本 1.2 中的 UI 导航路径	版本 1.4 中的对象名称	版本 1.4 中的 UI 导航路径	变更信息
				在新版本中，默认情况下提供以下访客类型： • 按天 (Daily) - 默认设置允许的网络接入时间仅为 1 到 5 天。 • 按周 (Weekly) - 默认设置允许的网络接入时间为两周。 • 按合同方 (Contractor) - 默认设置允许的网络接入时间最长为一年。 新版本中的访客类型是通过版本 1.2 中的下列数据元素形成的：发起人组、访客角色和时间配置文件。新版本中会使用这三个数据元素的组合来创建访客类型。如果某个访客角色在版本 1.2 的授权政策中已经使用，则会在新版本中创建相应的访客类型。 如果上述任何数据元素未在版本 1.2 的任何策略中使用，则不在新版本中创建该元素的访客类型。 升级过程不迁移没有活动访客与之关联的时间配置文件。如果版本 1.2 中存在过期的访客帐户，则这些访客不会迁移至新版本（无论其状态是“suspended”还是“awaiting initial login”）。与这些访客关联的任何访客类型或发起人组均不会迁移。 如果您希望时间配置文件可在新版本中使用（访客类型），那么升级之前，您必须创建一个访客帐户，将其与所需的时间配置文件关联，然后激活该帐户。 注释 版本 1.2.x 中的 FromFirstLogin 时间配置文件在版本 1.4 中不可用。此时间配置文件用于允许接入时间从首次登录开始。在版本 1.2.x

版本 1.2 中的对象名称	版本 1.2 中的 UI 导航路径	版本 1.4 中的对象名称	版本 1.4 中的 UI 导航路径	变更信息
				中，当您使用 FromFirstLogin 时间配置文件创建访客帐户时，开始时间会设置为当前日期，到期日期会设置为开始时间加上时间配置文件中配置的持续时间。此配置会在访客首次登录时重置。升级过程不迁移已过期的访客帐户。您可以使用每日访客类型，提供一日的网络访问权限。
可选数据 1-5	Administration > Web Portal Management > Settings > Guest > Language Template	自定义字段	Guest Access > Configure > Guest Type > Create / Edit	在版本 1.2 中，发起人能够获取访客的其他信息，例如备用邮箱地址或出生日期（可选数据）。在新版本中，可选数据被称为自定义字段，显示在“访客类型”配置下。
时间限制	Administration > Web Portal Management > Settings > Guest > Time Profiles	最长接入时间	Guest Access > Configure > Guest Types > Create / Edit > Maximum Access Time	在版本 1.2 中，您可以配置时间限制（指定不再授予访客接入权限的时间），但在新版本中，您可以配置接入时间（指定可授予访客接入权限的时间）。
设备注册门户限制	Administration > Web Portal Management > Settings > Guest > Portal Policy	访客可注册的最多设备数量	Guest Access > Configure > Guest Type > Create / Edit > Login Options	—

版本 1.2 中的对象名称	版本 1.2 中的 UI 导航路径	版本 1.4 中的对象名称	版本 1.4 中的 UI 导航路径	变更信息
发起人组	Administration > Web Portal Management > Sponsor Groups	发起人组	Guest Access > Configure > Sponsor Groups	在新版本中，发起人组包括以下默认的发起人组： • ALL_ACCOUNTS • GROUP_ACCOUNTS • OWN_ACCOUNTS 如果您配置了 Active Directory 并在升级到新版本后加入 Active Directory 域，则会显示 AD 外部组。 升级过程不迁移所有发起人组。在访客角色的创建中未使用的发起人组不会被迁移。由于此变更，升级到新版本后部分发起人（内部数据库或 Active Directory 用户）可能无法登录。对于登录失败的发起人，您必须检查发起人组的映射。将发起人映射到相应的发起人组。
发起人组策略	Administration > Web Portal Management > Sponsor Group Policy	-	-	在新版本中已删除。新版本中的发起人组包含用户和 AD 组映射以及这些用户的权限。

版本 1.2 中的对象名称	版本 1.2 中的 UI 导航路径	版本 1.4 中的对象名称	版本 1.4 中的 UI 导航路径	变更信息
发起人组权限	Administration > Web Portal Management > Sponsor Groups > Sponsor Group > Authorization Levels	发起人权限	Guest Access > Configure > Sponsor Groups > Create / Edit > Sponsor Permissions	以下字段已变更： • 允许登录 - 在新版本中已删除 • 创建单个帐户 - 新版本中的 Known User 选项取代了版本 1.2 中的 Create Single Account 选项。与版本 1.2 类似，在新版本中，发起人可以创建多个随机帐户，并从CSV文件导入访客详细信息。 • Send Email - 在新版本中，默认情况下此选项显示在发起人门户中，所有发起人均可通过邮件发送访客凭证。 • Send SMS - 新版本中提供了 Send SMS notifications with guest credentials 选项。 • Account Start Time - 新版本中提供了 **Start date cannot be more than n days into the future** 选项。 • Maximum Duration of Account - 在新版本中，此选项显示在“访客类型”配置下方（**Guest Access** > **Configure** > **Guest Types** > **Create/Edit** > **Maximum Access Time** > **Maximum account duration**）。 • Allow Printing Guest Details - 在新版本中，默认情况下此选项显示在发起人门户中，所有发起人均可打印访客详细信息。
时区	Administration > Web Portal Management > Settings > Guest > Time Profiles	访客位置	Guest Access > Settings > Guest Locations and SSIDs	新版本会从版本 1.2 的访客帐户获取访客位置。在版本 1.2 中创建访客时，您会为该访客关联时区。在新版本中，此时区将用于创建访客位置，并且这些位置会与相应的访客组关联。

版本 1.2 中的对象名称	版本 1.2 中的 UI 导航路径	版本 1.4 中的对象名称	版本 1.4 中的 UI 导航路径	变更信息
访客帐户清除设置	Administration > Web Portal Management > Settings > General > Purge	安排清除过期的访客帐户	Guest Access > Settings > Guest Account Purge Policy	—
访客用户名策略	Administration > Web Portal Management > Settings > Guest > Username Policy	访客用户名策略	Guest Access > Settings > Guest Username Policy	在升级过程中，访客用户名策略可能会发生变更。您必须检查访客用户名策略，确保它符合您的标准。 您对版本 1.2 中的默认访客用户名策略所做的任何更改将作为自定义策略迁移至新版本。对于版本 1.2 和新版本，访客用户名支持的特殊字符有所不同，并且支持的特殊字符将作为自定义条目迁移。
访客密码策略	Administration > Web Portal Management > Settings > Guest Password Policy	访客密码策略	Guest Access > Settings > Guest Password Policy	在升级期间，访客密码策略可能已经有所变更。您必须检查访客密码策略，确保它符合您的标准。 您对版本 1.2 中的默认访客密码策略所做的任何更改将作为自定义策略迁移至新版本。对于版本 1.2 和新版本，访客密码支持的特殊字符有所不同，并且支持的特殊字符将作为自定义条目迁移。
SMTP 服务器设置	Administration > System > Settings > SMTP Server	访客邮件设置	Guest Access > Settings > Guest Email Settings Administration > System > Settings > SMTP Server	在版本 1.2 中，SMTP 服务器设置和访客邮件通知设置位于同一个 UI 页面。在新版本中，SMTP 服务器设置和访客邮件通知设置位于两个不同的位置（请参阅新版本的 UI 导航路径）。

版本 1.2 中的对象名称	版本 1.2 中的 UI 导航路径	版本 1.4 中的对象名称	版本 1.4 中的 UI 导航路径	变更信息
个人设备门户	Administration > Web Portal Management > Settings	配置设备门户	Administration > Device Portal Management	在新版本中，以下个人设备门户默认可用： • 黑名单门户 • BYOD 门户 • 客户端调配门户 • MDM 门户 • 我的设备门户 如果您更改了版本 1.2 中的默认访客门户界面和端口，新版本中将会创建与版本 1.2 访客门户对应的新 BYOD 和客户端配置门户。授权配置文件也会相应地更新。
门户主题	Administration > Web Portal Management > Settings > General > Portal Theme	门户主题	Administration > Device Portal Management > Portal > Edit > Portal Page Customization	在新版本中，您可以自定义门户主题，并在保存之前查看您的更改。
移动优化的访客门户	Administration > Web Portal Management > Settings > Guest > Mutli-Portal Configuration > Edit > Operations > Enable Mobile Portal	-	-	默认情况下，所有门户都针对移动环境进行了优化。系统会根据所用设备类型使用移动版本或桌面版本。

版本 1.2 中的对象名称	版本 1.2 中的 UI 导航路径	版本 1.4 中的对象名称	版本 1.4 中的 UI 导航路径	变更信息
SMS 文本消息通知	Administration > Web Portal Management > Settings > Sponsor > Language Template	SMS 网关设置	Administration > System > Settings > SMS Gateway	在新版本中，SMS 网关具有以下作用： • 发起人手动向访客发送 SMS 通知及其登录凭证和密码重置说明。 • 使访客能够在成功注册之后使用其登录凭证自动接收 SMS 通知。 • 访客自动接收提示访客帐户到期前需要采取的操作的 SMS 通知。

其他门户相关的变更

升级期间，所有 Cisco ISE 门户均迁移到新的版本。

- 默认门户 - 迁移到新版本后，您可以对默认门户（访客、发起人、我的设备等）进行编辑和更改。版本 1.4 中新引入的任何门户设置均被设为其默认值。升级过程中，保留默认门户的端口、允许界面以及门户主题的配置。
- 访客和个人设备的自定义门户 - 此版本的 Cisco ISE 将带来全新的简化后的访客和员工注册体验，以及全新的门户自定义体验，并提供从多语言支持到 WYSIWYG 自定义等大量新功能。当您升级到新版本时，所有自定义门户都将迁移到全新的体验。以下列出您必须了解的几个注意事项：

  通过升级过程，将之前版本的 ISE 中使用 CSS 和 HTML 完成的基本外观和自定义迁移到全新的访客和个人设备流程。

  使用基本 HTML 和本地管理工具完成的自定义应能正确地迁移。使用 JavaScript 修改访客流程的自定义可能无法正确地迁移。升级后，您可以从 ISE 管理员门户重新创建这些门户。

  您无法编辑迁移到新版本的任何自定义门户。如果您要更改外观、流程或功能，就必须在升级后从 ISE 管理员门户创建新的门户。

  ISE 1.2 和 1.2.1 的客户能够进行各种门户自定义。其中一些自定义可能无法如预期迁移至新版本。我们建议您在生产环境中使用前，检查实验室设置中新迁移的门户。

  当您执行下列操作时，ISE 无法在新版本中创建访客帐户：

  1 在 ISE 1.2 或 1.2.1 中将访客门户配置为允许自助服务

2 自定义门户期间对时区值进行硬编码

3 通过 ISE 升级过程将自定义门户迁移至新版本

发生这种情况是因为自定义门户中硬编码的时区值可能与新版本中的访客位置名称不匹配。ISE 1.2 和 1.2.1 中的“时区”在新版本中重命名为“访客位置”。

解决办法是，升级后，将您在 1.2 或 1.2.1 版本中进行硬编码的相同时区作为访客位置添加到新版本中。为此，请从 ISE 管理员门户中，选择 **Guest Access** > **Settings** > **Guest Locations and SSIDs**，在“位置名称”文本框中，选择相应的时区，然后点击 **Add** 并保存设置。

- 访客门户 - 版本 1.2 或 1.2.1 中的所有访客门户均迁移至新版本，升级后您将看到以下门户。如果您没有对应的 1.2 或 1.2.1 版本访客门户，则创建默认访客门户。

  版本 1.2 或 1.2.1 中的 DRW 门户 - 新版本中的热点门户

  版本 1.2 或 1.2.1 中不提供自助服务的访客门户 - 新版本中有发起人的访客门户

  版本 1.2 或 1.2.1 中启用自助服务的访客门户 - 新版本中的自注册访客门户

- 发起人门户 - 在版本 1.2 和 1.2.1 中，您可以从 Manage Guest Accounts > My Settings 自定义下列发起人门户设置：语言模板、位置、电子邮件地址、访客角色、帐户持续时间、时区、通知语言和密码设置。升级后，只迁移发起人邮箱地址，其余的设置不迁移。如果在升级后对语言首选项进行了自定义，则当您登录发起人门户时，不保留您的语言首选项。
- BYOD 门户 - 从版本 1.2 或 1.2.1 迁移下列 BYOD 门户：

  版本 1.2 或 1.2.1 中的我的设备门户

  具有 BYOD 相关配置的访客门户

  升级到新版本后，创建下列默认 BYOD 门户（版本 1.2 或 1.2.1 中不提供这些门户）：

  默认黑名单门户

  默认 BYOD 门户

- 客户端配置门户 - 升级到新版本时，创建默认客户端配置 (CP) 门户。

有关新的 ISE 访客和个人设备功能及管理体验的更多信息，请参阅思科身份服务引擎管理员指南。

策略相关变更

此版本的 Cisco ISE 中对以下策略及策略元素进行了变更和增强：

- 发起人组策略 - 删除发起人组策略。新版本中的发起人组包含用户和 AD 组映射以及这些用户的权限。
- 授权配置文件 - 根据新格式设置重定向 URL 的格式。例如，热点门户的 URL 重定向为：https://ip:port/guestportal/gateway?sessionID=SessionIDValue&portal=PortalID&action=cwa&type=drw。

- 授权策略 - 新身份组（“访客类型”身份组）可在授权策略中使用。

第 4 章

升级后的任务

升级部署后，请执行本章中列出的任务。

升级后的任务

请参阅思科身份服务引擎管理员指南，了解各项任务的详细信息。

任务说明	其他信息/思科 ISE 管理员指南相关章节的链接
如果您要升级虚拟机 (VM) 上版本为 1.2 或 1.2.1 的思科 ISE 节点，请关闭 VM 并将访客操作系统更改为 Red Hat Enterprise Linux 6（64 位），完成更改后再次启动 VM。	-
升级后，请确保先清除浏览器缓存、关闭浏览器并打开新的浏览器会话，然后再访问思科 ISE 管理门户。支持的浏览器有： • Mozilla Firefox 版本 31.*x* ESR、36.*x* 和 37.*x* 在运行客户端浏览器的系统上，必须安装 Adobe Flash Player 11.1.0.0 或更高版本。 查看思科 ISE 管理门户且实现更好的用户体验所需的最低屏幕分辨率是 1280 x 800 像素。	-

升级后的任务

任务说明	其他信息/思科 ISE 管理员指南相关章节的链接
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，则使用 Active Directory 重新加入所有思科 ISE 节点。重新加入后，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 管理员帐户登录到思科 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帐户登录到思科 ISE 并使用该帐户加入到 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，这是因为升级期间与 Active Directory 的连接丢失。如果您遇到此问题，请从思科 ISE CLI 使用下列命令以安全模式启动 ISE 应用： **application start ise safe** 使用此命令，即可提供安全模式的思科 ISE 节点。执行以下任务： 1 使用内部管理员帐户登录到思科 ISE 用户界面。 如果您忘记密码或您的管理员帐户已锁定，请参阅《思科身份服务引擎硬件安装指南，版本 2.0》，以了解关于如何重置管理员密码的信息。 2 使用 Active Directory 加入思科 ISE	将 Active Directory 配置为外部身份源
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 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。	思科 ISE CA 证书和密钥的备份与恢复

任务说明	其他信息/思科 ISE 管理员指南相关章节的链接
在您升级分布式部署后，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（旧版本部署中的主管理节点）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 这可能会导致身份验证失败，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。 解决办法是，在您升级部署并将辅助管理节点升级为新部署中的主管理节点后，从管理门户生成新的 ISE 根 CA 证书链（依次选择 **Administration > Certificates > Certificate Signing Requests > Replace ISE Root CA certificate chain**）。	在 PAN 和 PSN 上生成根 CA 和从属 CA
如果您使用 RSA SecurID 服务器作为外部身份源，请重置 RSA 节点加密。	RSA 节点密钥重置
如果您已启用 Posture 服务，请在升级后从主管理节点执行状态更新。	将安全评估更新下载至思科 ISE
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。您必须重新配置此值。	请参阅网络设备定义设置下的 SNMP 设置。
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： 1 依次选择**管理 (Administration) > Feed 服务 (FeedService) > 配置文件 (Profiler)**。确保已启用 Profiler Feed 服务。 2 点击**立即更新 (Update Now)**。

任务说明	其他信息/思科 ISE 管理员指南相关章节的链接
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。	-
（仅在您从版本 1.2 或 1.2.1 直接升级时适用）对于登录失败的发起人，应检查发起人组的映射。将发起人映射到相应的发起人组。不是所有发起人组都能在升级过程中迁移，因此某些发起人可能无法登录到发起人门户。	-
（仅在您从版本 1.2 或 1.2.1 直接升级时适用）升级过程迁移默认门户（访客、发起人、我的设备等）和自定义门户。升级期间，保留这些门户使用的端口和允许的界面配置。您可以编辑默认门户，但自定义门户为只读属性。对于您不需要的默认门户，可以将其删除。	-
（仅在您从版本 1.2 或 1.2.1 直接升级时适用；仅适用于个人设备）如果您静态分配设备至某个特定设备组，则升级到新的部署后，确保更新 BYOD 门户配置（**管理 (Administration)** > **设备门户管理 (Device Portal Management)** > **自带设备 (BYOD)** > **编辑 (Edit)**），并在“终端身份组”字段中选择相应的设备组。否则，升级后，当设备连接到网络时会被分配到默认的 RegisteredDevices 组。授权策略规则不随此设备组的变更而更新，请求未能成功处理。	-
（仅在您从版本 1.2 或 1.2.1 直接升级时适用）检查端点清除策略的设置 (**Administration** > **Identity Management** > **Settings** > **Endpoint Purge**)。	-
（仅在您从版本 1.2 或 1.2.1 直接升级时适用）检查访客用户名、密码和清除策略 (**Guest Access** > **Settings**)。	-
（仅在您从版本 1.2 或 1.2.1 直接升级时适用）检查访客相关工作流程的授权策略，并更新策略条件中使用的访客组。	-

任务说明	其他信息/思科 ISE 管理员指南相关章节的链接
（仅在您从版本 1.2 或 1.2.1 直接升级时适用）更新无线 LAN 控制器访客本地 Web 身份验证的配置。您必须将 Web 重定向外部服务器 URL 替换为 https://<ip>:<port>/portal/PortalSetup.action?portal=<portalId>。从门户设置和自定义页面上点击 **Portal test URL** 以获取此 URL (**Guest Access** > **Configure** > **Portal** > **Create/Edit** > **Portal Settings and Customization**)。	-
重新配置邮件设置、收藏夹报告和数据清除设置。	请参阅《思科 ISE 管理员指南》中的”监控和故障排除“章节。
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。	
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。	

任务说明	其他信息/思科 ISE 管理员指南相关章节的链接
如果您要升级虚拟机 (VM) 上版本为 1.2 或 1.2.1 的思科 ISE 节点，请关闭 VM 并将访客操作系统更改为 Red Hat Enterprise Linux 6（64 位），完成更改后再次启动 VM。	-
升级后，请确保先清除浏览器缓存、关闭浏览器并打开新的浏览器会话，然后再访问思科 ISE 管理门户。支持的浏览器有： • Mozilla Firefox 版本 31.*x* ESR、36.*x* 和 37.*x* 在运行客户端浏览器的系统上，必须安装 Adobe Flash Player 11.1.0.0 或更高版本。 查看思科 ISE 管理门户且实现更好的用户体验所需的最低屏幕分辨率是 1280 x 800 像素。	-

升级后的任务

任务说明	其他信息/思科 ISE 管理员指南相关章节的链接
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，则使用 Active Directory 重新加入所有思科 ISE 节点。重新加入后，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 管理员帐户登录到思科 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帐户登录到思科 ISE 并使用该帐户加入到 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，这是因为升级期间与 Active Directory 的连接丢失。如果您遇到此问题，请从思科 ISE CLI 使用下列命令以安全模式启动 ISE 应用： **application start ise safe** 使用此命令，即可提供安全模式的思科 ISE 节点。执行以下任务： 1 使用内部管理员帐户登录到思科 ISE 用户界面。 如果您忘记密码或您的管理员帐户已锁定，请参阅《思科身份服务引擎硬件安装指南，版本 2.0》，以了解关于如何重置管理员密码的信息。 2 使用 Active Directory 加入思科 ISE	将 Active Directory 配置为外部身份源
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 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。	思科 ISE CA 证书和密钥的备份与恢复

任务说明	其他信息/思科 ISE 管理员指南相关章节的链接
在您升级分布式部署后，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（旧版本部署中的主管理节点）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 这可能会导致身份验证失败，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。 解决办法是，在您升级部署并将辅助管理节点升级为新部署中的主管理节点后，从管理门户生成新的 ISE 根 CA 证书链（依次选择 **Administration > Certificates > Certificate Signing Requests > Replace ISE Root CA certificate chain**）。	在 PAN 和 PSN 上生成根 CA 和从属 CA
如果您使用 RSA SecurID 服务器作为外部身份源，请重置 RSA 节点加密。	RSA 节点密钥重置
如果您已启用 Posture 服务，请在升级后从主管理节点执行状态更新。	将安全评估更新下载至思科 ISE
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。您必须重新配置此值。	请参阅网络设备定义设置下的 SNMP 设置。
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： 1 依次选择**管理 (Administration) > Feed 服务 (FeedService) > 配置文件 (Profiler)**。确保已启用 Profiler Feed 服务。 2 点击**立即更新 (Update Now)**。

任务说明	其他信息/思科 ISE 管理员指南相关章节的链接
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。	-
（仅在您从版本 1.2 或 1.2.1 直接升级时适用）对于登录失败的发起人，应检查发起人组的映射。将发起人映射到相应的发起人组。不是所有发起人组都能在升级过程中迁移，因此某些发起人可能无法登录到发起人门户。	-
（仅在您从版本 1.2 或 1.2.1 直接升级时适用）升级过程迁移默认门户（访客、发起人、我的设备等）和自定义门户。升级期间，保留这些门户使用的端口和允许的界面配置。您可以编辑默认门户，但自定义门户为只读属性。对于您不需要的默认门户，可以将其删除。	-
（仅在您从版本 1.2 或 1.2.1 直接升级时适用；仅适用于个人设备）如果您静态分配设备至某个特定设备组，则升级到新的部署后，确保更新 BYOD 门户配置（**管理 (Administration)** > **设备门户管理 (Device Portal Management)** > **自带设备 (BYOD)** > **编辑 (Edit)**），并在“终端身份组”字段中选择相应的设备组。否则，升级后，当设备连接到网络时会被分配到默认的 RegisteredDevices 组。授权策略规则不随此设备组的变更而更新，请求未能成功处理。	-
（仅在您从版本 1.2 或 1.2.1 直接升级时适用）检查端点清除策略的设置 (**Administration** > **Identity Management** > **Settings** > **Endpoint Purge**)。	-
（仅在您从版本 1.2 或 1.2.1 直接升级时适用）检查访客用户名、密码和清除策略 (**Guest Access** > **Settings**)。	-
（仅在您从版本 1.2 或 1.2.1 直接升级时适用）检查访客相关工作流程的授权策略，并更新策略条件中使用的访客组。	-

任务说明	其他信息/思科 ISE 管理员指南相关章节的链接
（仅在您从版本 1.2 或 1.2.1 直接升级时适用）更新无线 LAN 控制器访客本地 Web 身份验证的配置。您必须将 Web 重定向外部服务器 URL 替换为 https://<ip>:<port>/portal/PortalSetup.action?portal=<portalId>。从门户设置和自定义页面上点击 **Portal test URL** 以获取此 URL (**Guest Access** > **Configure** > **Portal** > **Create/Edit** > **Portal Settings and Customization**)。	-
重新配置邮件设置、收藏夹报告和数据清除设置。	请参阅《思科 ISE 管理员指南》中的”监控和故障排除“章节。
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。	
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。	

升级后的任务

第 5 章

从升级失败中恢复

本章介绍了从失败的升级中恢复时需要做些什么。

升级软件执行一些验证。如果升级失败，请按照屏幕上提供的说明恢复并成功升级到版本 1.4。

通常情况下，升级失败是由于没有遵循节点升级的顺序造成的，例如先升级辅助管理节点。如果遇到此错误，您可以按照本指南中指定的升级顺序，再次升级部署。

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，您务必要对思科ISE配置和监控数据进行备份。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和监控数据进行备份。

注释

因为监控数据库中的问题不会自动回滚，所以升级才会失败。您必须以手动方式重新映像系统，安装思科 ISE 版本 1.4，并还原配置和监控数据。

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 您可以从 CLI 检查升级日志或从控制台检查升级状态。通过登录 CLI 或查看思科 ISE 节点的控制台来查看升级过程。您可以使用 **show logging application** 命令，从思科 ISE 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

如果有任何验证错误，而不是真正的升级失败，则会显示以下消息。例如，如果在升级辅助 PAN 之前尝试升级 PSN，或者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，重新映像并还原配置和运营备份。

重新映像

“重新映像”一词是指全新安装思科 ISE。对于监控数据库升级（架构 + 数据）错误，您必须重新映像并还原配置和运营备份。在重新映像前，确保您已通过运行 **backup-logs** 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。您必须根据节点角色重新映像至旧或新版本：

- 辅助管理节点 - 重新映像至旧版本并还原配置和运营备份。
- 监控节点 - 如果从现有部署中取消注册节点，则重新映像至新版本，在新部署中注册并启用监控角色。
- 所有其他节点 - 如果其他节点的升级失败，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，并启用和旧部署中一样的角色。

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。

升级进度

注释 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…

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 Cisco ISE 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。