思科身份服务引擎硬件安装指南，版本 1.4

首次发布日期: 2015 年 02 月 15 日

上次修改日期: 2015 年 03 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 Internet 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)

© 2015 Cisco Systems, Inc. All rights reserved.

目 录

第 1 章

Cisco ISE 中的网络部署

Cisco ISE 网络架构

Cisco ISE 架构包括以下组件：

- 节点和角色类型

  Cisco ISE 节点 - Cisco ISE 节点可以承担以下任意或所有角色：管理、策略服务、监控或 pxGrid

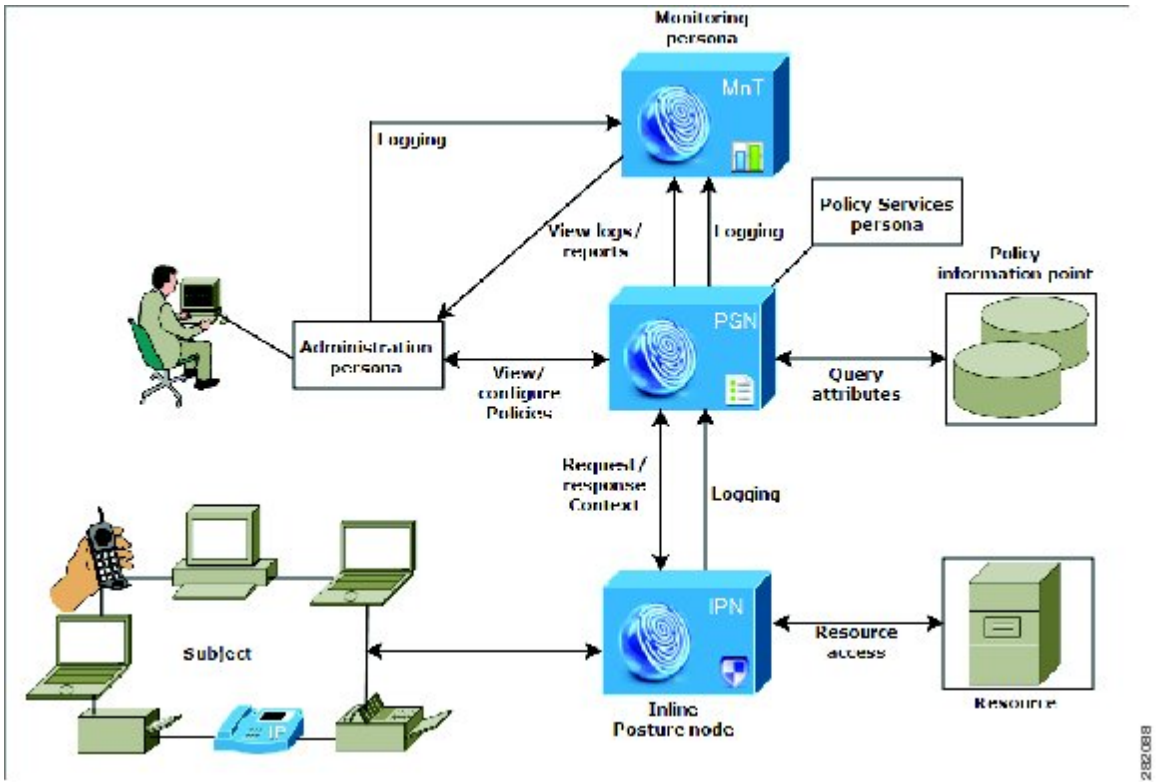
  Inline Posture 节点 - 负责处理访问策略实施的看管节点

- 网络资源
- 终端

策略信息点表示外部信息传达给策略服务角色所在的点。 例如，外部信息可以是轻量级目录访问协议 (LDAP) 属性。

下图显示 Cisco ISE 节点和角色（管理、策略服务和监控）、Inline Posture 节点和策略信息点。

图 *1*：*Cisco ISE* 架构



Cisco ISE 部署术语

本指南在讨论 Cisco ISE 部署方案时使用以下术语：

术语	定义
服务	角色提供的特定功能，例如网络访问、分析、状态、安全组访问、监控和故障排除。
节点	运行 Cisco ISE 软件的单个实例。 Cisco ISE 可用作设备以及用作能够在 VMware 上运行的软件。
节点类型	节点可以是以下两种类型之一：Cisco ISE 节点或 Inline Posture 节点。 节点类型和角色确定节点提供的功能的类型

术语	定义
角色	确定节点提供的服务。 Cisco ISE 节点可以承担以下任意或所有角色：管理、策略服务和监控。 通过管理用户界面可使用的菜单选项取决于节点承担的角色和人员。
角色	确定节点是独立节点、主要节点还是辅助节点，并且仅适用于管理和监控节点。

分布式部署中的节点类型和角色

在 Cisco ISE 分布式部署中，有两种类型的节点：

- Cisco ISE 节点（管理、策略服务、监控）
- Inline Posture 节点

Cisco ISE 节点可以根据它承担的角色提供各种服务。 部署中的每个节点，Inline Posture 节点除外，可以承担管理、策略服务和监控角色。 在分布式部署中，您可以在网络中具有以下节点组合：

- 实现高可用性的主要和次要管理节点
- 实现自动故障切换的监控节点对
- 实现会话故障切换的一个或多个策略服务节点
- 实现高可用性的 Inline Posture 节点对

管理节点

通过具有管理角色的 Cisco ISE 节点，您可以在 Cisco ISE 上进行所有管理操作。 它处理与诸如身份验证、授权和记帐等功能有关的所有系统相关配置。 在分布式部署中，您最多可以具有两个运行管理角色的节点。 管理角色可以承担独立、主要或辅助角色。

策略服务节点

具有策略服务角色的 Cisco ISE 节点可提供网络访问、状态、访客接入、客户端调配和概况分析服务。此角色会评估策略并根据策略评估结果提供对终端的网络访问权限。通常，在分布式部署中有多个服务策略节点。 驻留在负载均衡器背后的所有策略服务节点都共享一个通用组播地址，并可组合形成节点组。 如果节点组中的其中一个节点关闭，则其他节点会检测到故障并重置所有待处理会话。

分布式设置中至少有一个节点应承担策略服务角色。

监控节点

具有监控角色的 Cisco ISE 节点用作日志收集器，并且存储来自网络中所有管理节点和策略服务节点的日志消息。此角色提供可用于有效管理网络和资源的高级监控和故障排除工具。具有此角色的节点会将其收集的数据汇总和关联，并为您提供有意义的报告。通过 Cisco ISE，您最多可以拥有两个具有此角色的节点，并且这些节点可以承担主要角色或辅助角色，从而实现高可用性。 主要和辅助监控节点收集日志消息。 如果主要监控节点关闭，辅助监控节点会自动成为主要监控节点。

分布式设置中至少有一个节点应承担监控角色。 我们建议您不要在同一 Cisco ISE 节点上启用监控和服务策略角色。 我们建议监控节点仅专用于监控，以获取最佳性能。

Inline Posture 节点

Inline Posture 节点是位于网络接入设备（例如网络上的无线局域网控制器 (WLC) 和 VPN 集中器）背后的看管节点。 Inline Posture 节点在用户进行身份验证并被授予访问权限后实施访问策略，并会处理 WLC 或 VPN 无法适应的授权变更 (CoA) 请求。 通过 Cisco ISE，您可以拥有两个 Inline Posture 节点，并且这两个节点可以承担主要角色或辅助角色，从而实现高可用性。

Inline Posture 节点必须是专用的节点。 它必须只专用于 Inline Posture 服务，且无法与其他 Cisco ISE 服务并发运行。 同样，由于服务专业性质，Inline Posture 节点不能承担任何角色。 例如，它不能用作管理节点（提供管理服务）、策略服务节点（提供网络接入、状态、配置文件和访客服务）或监控节点（提供监控和故障排除服务）。

Cisco SNS 3495 平台不支持 Inline Posture 节点。 确保在以下任何一个受支持的平台上安装 Inline Posture 节点：

- Cisco ISE 3315
- Cisco ISE 3355
- Cisco ISE 3395
- Cisco SNS 3415

安装 Inline Posture 节点

开始之前

- 从 Cisco.com 下载 Inline Posture ISO 映像
- 为节点配置证书并向主要管理节点注册该节点

操作步骤

步骤 1 在其中一个受支持的平台上安装 Inline Posture ISO 映像。

步骤 2 登录到 CLI。

步骤 3 为节点配置证书。

步骤 4 登录到主要管理节点的用户界面。

步骤 5 注册 Inline Posture 节点。

Inline Posture 节点重复使用

如果您决定不再需要 Inline Posture 节点，则无法向其添加任何服务或角色，但是可以将其更改为 Cisco ISE 节点，然后向其分配任何角色。 如果要重复使用 Inline Posture 节点，您必须先撤销注册该节点，然后重新映像设备并在其上安装 Cisco ISE。

独立和分布式 ISE 部署

具有单个 Cisco ISE 节点的部署称为独立部署。 此节点运行管理、策略服务和监控角色。

具有多个 Cisco ISE 节点的部署称为分布式部署。 要支持故障切换和提高性能，您可以分布式方式设置具有多个 Cisco ISE 节点的部署。 在 Cisco ISE 分布式部署中，管理和监控活动会进行集中，而处理则分布在多个策略服务节点上。 根据您的性能需求，您可以扩展您的部署。 Cisco ISE 节点可以承担以下任何角色：管理、策略服务和监控。 Inline Posture 节点由于其专用性质而无法承担任何其他角色，并且其必须是专用节点。

分布式部署方案

- 小型网络部署
- 中型网络部署
- 大型网络部署

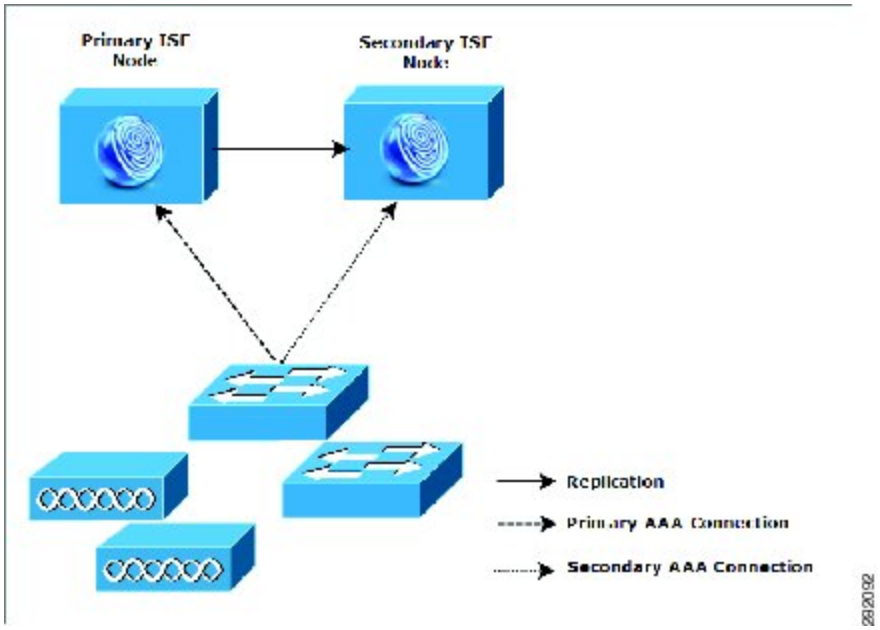
小型网络部署

最小的 Cisco ISE 部署包含两个 Cisco ISE 节点，其中一个 Cisco ISE 节点在小型网络中用作主要设备。

主要节点提供此网络模型所需的所有配置、身份验证和策略功能，并在备份角色中提供辅助 Cisco ISE 节点功能。 辅助节点支持主要节点，并会在主要节点与网络设备、网络资源或 RADIUS 之间的连接断开时维持网络正常工作。

客户端与主要 Cisco ISE 节点之间的集中身份验证、授权和记帐 (AAA) 操作使用 RADIUS 协议来执行。 Cisco ISE 会将驻留在主要 Cisco ISE 节点上的所有内容与辅助 Cisco ISE 节点同步或复制这些内容。因此，辅助节点与主要节点的状态保持一致。在小型网络部署中，通过此类型的配置模式，您可以使用此类型的部署或类似方法在所有 RADIUS 客户端上同时配置主要节点和辅助节点。

图 2： 小型网络配置



随着网络环境中设备、网络资源、用户和AAA客户端数量的增加，您应从基本的小模式更改部署配置并更多地使用分离式或分布式部署模式。

分离式部署

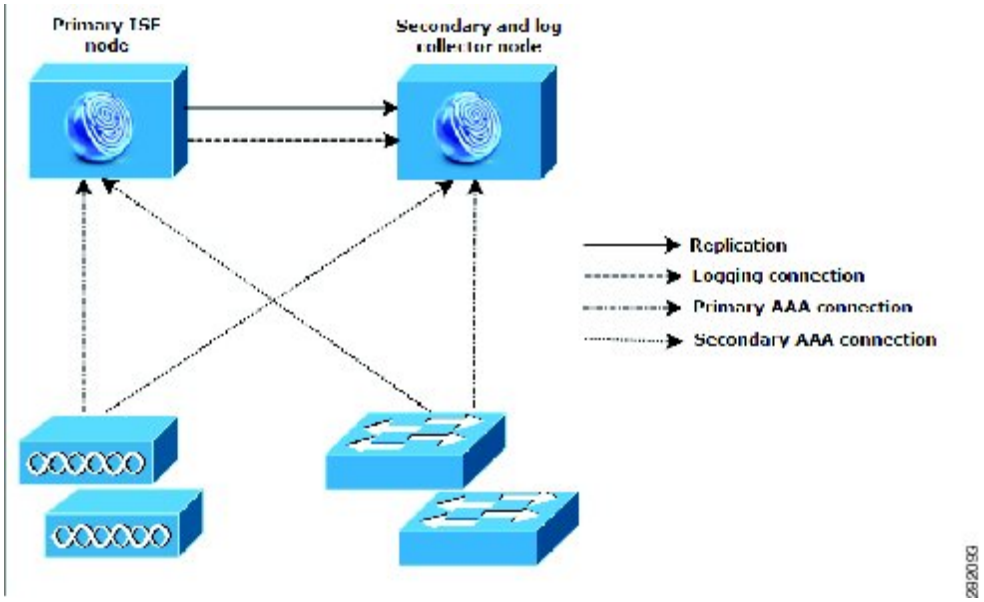
在分离式 Cisco ISE 部署中，您将按照小型 Cisco ISE 部署中所述继续维护主要节点和辅助节点。 但是， AAA 负载会在两个 Cisco ISE 节点之间进行拆分，以优化 AAA 工作流程。 如果 AAA 连接有任何问题，则每个 Cisco ISE 设备（主要或辅助）需要能够处理全部工作负载。 主要节点和辅助节点在正常网络操作过程中均不处理任何 AAA 请求，因为此工作负载分布在两个节点之间。

以此方式拆分负载的功能会直接减少系统中每个 Cisco ISE 节点上的压力。 此外，拆分负载可提供更好的加载，同时辅助节点的功能状态会在正常网络操作过程中得以维护。

在分离式Cisco ISE部署中，每个节点可以执行各自的特定操作（例如网络准入或设备管理），并且在发生故障的情况下仍然执行所有 AAA 功能。 如果您有两个 Cisco ISE 节点，分别用于处理身份验证请求和从AAA客户端收集记帐数据，则建议您将其中一个Cisco ISE节点设置为用作日志收集器。

此外，分离式 Cisco ISE 部署设计具有优势，因为它允许增长。

图 3：分离式网络部署

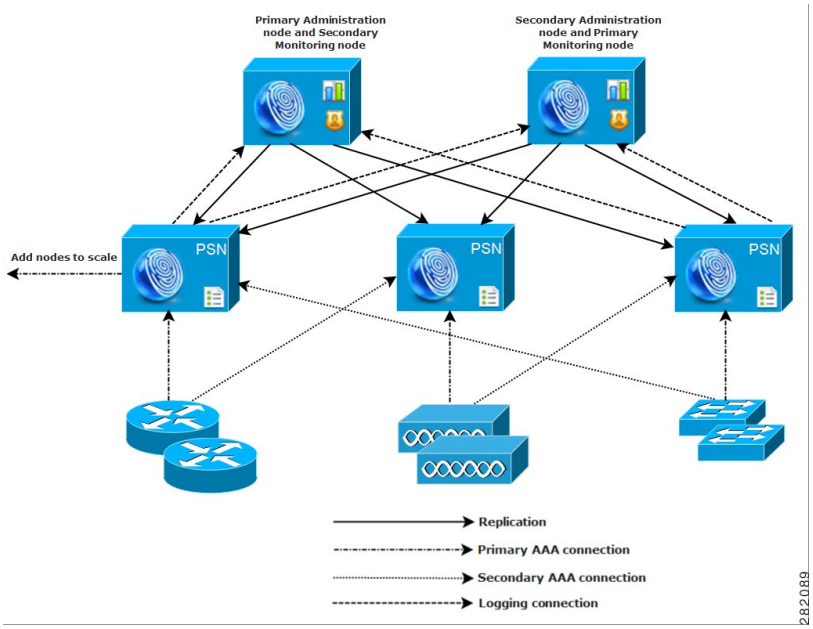


中型网络部署

随着小型网络的增长，您可以通过添加 Cisco ISE 节点创建中型网络来跟上步伐和管理网络增长。在中型网络部署中，您可以将新节点专用于所有 AAA 功能，并将原始节点用于配置和日志记录功能。

随着网络中日志流量的增加，您可以选择将一个或两个辅助 Cisco ISE 节点专用于网络中的日志收集。

图 4：中型网络部署



大型网络部署

集中日志记录

我们建议您对大型 Cisco ISE 网络使用集中日志记录。 要使用集中日志记录，您必须先设置担任监控角色（用于监控和日志记录）的专用日志记录服务器，以处理大型繁忙网络可能会生成的高系统日志流量。

由于会针对出站日志流量生成系统日志消息，因此任何符合RFC 3164的系统日志设备都可以用作出站日志记录流量的收集器。 通过专用日志记录服务器，您可以使用 Cisco ISE 中提供的报告和警报功能支持所有 Cisco ISE 节点。

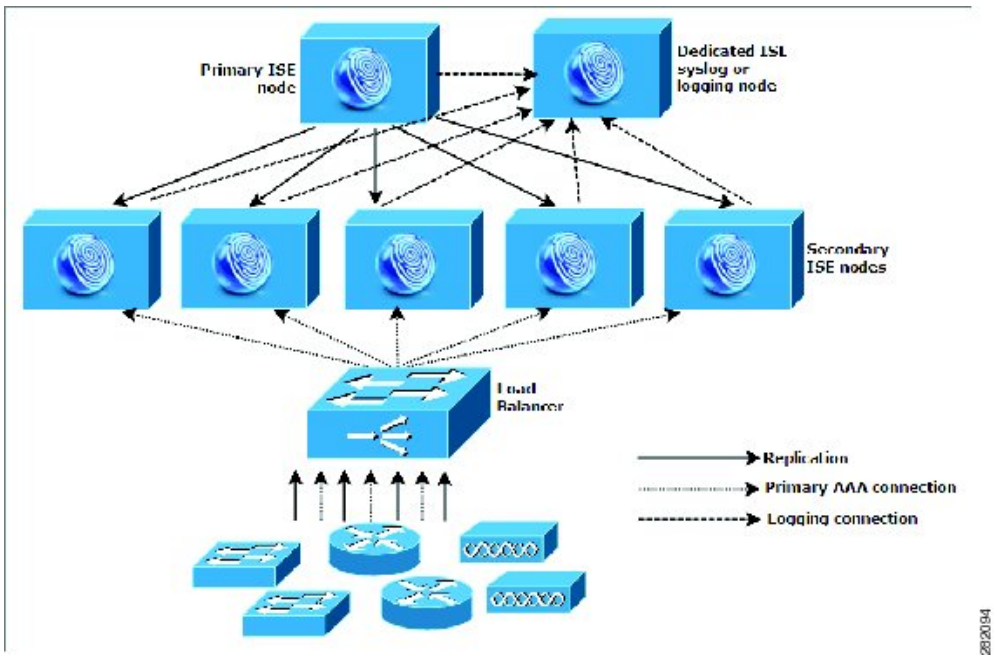
您也可以考虑使用设备将日志发送到 Cisco ISE 节点上的监控角色以及通用系统日志服务器。 如果 Cisco ISE 节点上的监控角色关闭，则添加通用日志服务器可提供冗余备份。

负载均衡器

在大型集中式网络中，您应该使用负载均衡器，以此简化 AAA 客户端的部署。 使用负载均衡器只需单个条目即可表示多个 AAA 服务器，并且负载均衡器会优化 AAA 请求至可用服务器的路由。

但是，只有一个负载均衡器可能会发生单点故障。 要避免此潜在问题，请部署两个负载均衡器，以确保采取冗余和故障切换措施。 此配置要求您在各 AAA 客户端中设置两个 AAA 服务器条目，并且此配置会在整个网络保持一致。

图 *5*：大型网络部署

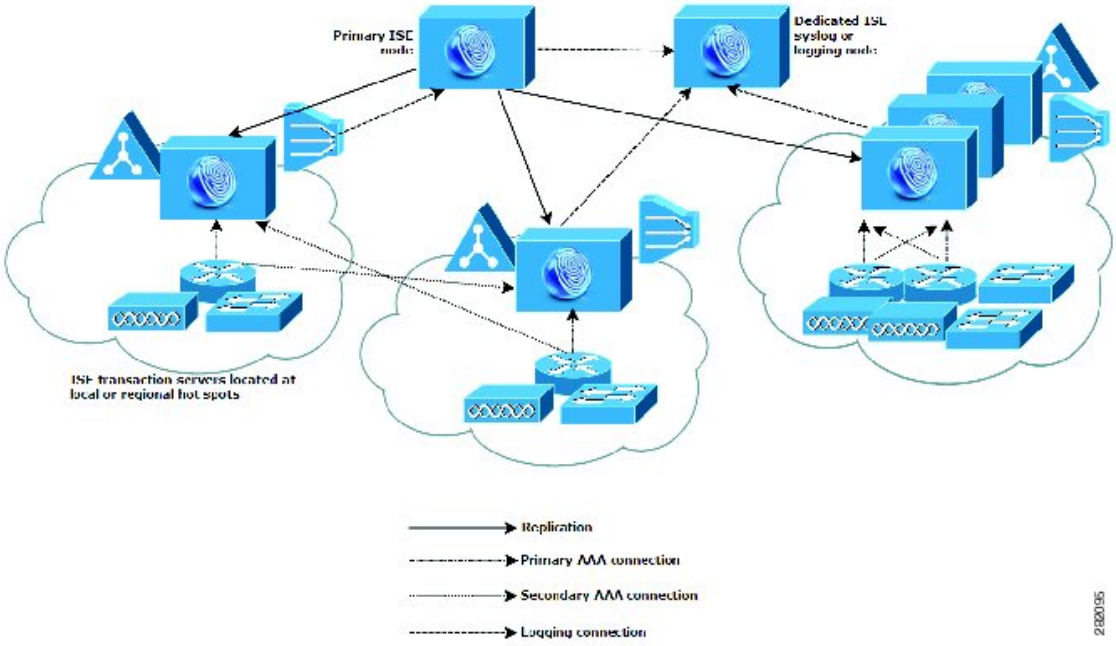


离散网络部署

离散 Cisco ISE 网络部署对于具有主园区且在其他位置有区域、国家或办事处场所的组织最有用。主园区是主网络驻留所在的位置，连接到其他 LAN，规模从小到大不等，并且支持不同地理区域和位置中的设备及用户。

大型远程站点可具有各自的 AAA 基础设施，以实现最佳 AAA 性能。 集中管理模式有助于维护一致、同步的 AAA 策略。 集中配置模式将主要 Cisco ISE 节点与辅助 Cisco ISE 节点结合使用。 我们仍建议您在 Cisco ISE 节点上使用单独的监控角色，但是，各远程位置应保留其特有的网络要求。

图 *6*: 离散部署



规划具有多个远程站点的网络的注意事项

- 验证使用的是中央数据库还是外部数据库，例如 Microsoft Active Directory 或轻量级目录访问协议 (LDAP)。 每个远程站点应具有同步的外部数据库实例，可供 Cisco ISE 访问以优化 AAA 性能。
- AAA 客户端的位置非常重要。 您应使 Cisco ISE 节点的位置尽可能接近 AAA 客户端，以减少网络延迟影响以及由 WAN 故障导致无法访问的可能性。
- Cisco ISE 对某些功能（例如备份）具有控制台访问权限。 请考虑在每个站点使用终端，从而允许进行直接、安全的控制台访问，以此绕过对每个节点进行网络访问。
- 如果小型远程站点距离接近并具有到其他站点的可靠 WAN 连接，请考虑使用 Cisco ISE 节点作为本地站点的备份以提供冗余。
- 应在所有 Cisco ISE 节点上正确配置域名系统 (DNS)，以确保对外部数据库的访问。

部署规模和扩展建议

下表根据连接到网络的终端数提供有关所需的部署类型、Cisco ISE 节点数和设备类型（小型、中型、大型）的指导。

表 *1*：*Cisco ISE* 部署规模和扩展建议

部署类型	节点/角色的数量	设备平台	专用策略服务节点的最大数量	活动终端的数量
小型	已启用管理、策略服务和监控角色的独立或冗余 (2) 节点	Cisco ISE 3300 系列（3315、3355、3395）	0	最多 2,000 个终端
		Cisco ISE 3415	0	最多 5,000 个终端
		Cisco ISE 3495	0	最多 10,000 个终端
中型	单一或冗余节点上的管理和监控角色。 最多 2 个管理和监控节点。	用于承担管理和监控角色的 Cisco ISE-3355 或 Cisco SNS 3415 设备	5	最多 5,000 个终端
		用于承担管理和监控角色的 Cisco ISE 3395 或 Cisco SNS 3495 设备	5	最多 10,000 个终端
大型	一个或多个专用管理节点。 最多 2 个管理节点。 一个或多个专用监控节点。 最多 2 个监控节点。 专用策略服务节点。 最多 40 个专用策略服务节点。	用于承担管理和监控角色的 Cisco ISE 3395 设备	40	最多 100,000 个终端
		用于承担管理和监控角色的 Cisco SNS 3495 设备	40	最多 250,000 个终端

下表根据专用策略服务节点所服务的活动终端数提供有关针对该节点所需的设备类型的指导。

表 *2*：策略服务节点大小建议

外形规格	平台规模	设备	最大终端数
物理	小型	Cisco ISE-3315	3,000
		Cisco SNS-3415	5,000
	中型	Cisco ISE-3355	6,000
	大型	Cisco ISE-3395	10,000
		Cisco SNS-3495	20,000
虚拟机	小型/中型/大型	可与物理设备相比较	3,000 至 20,000

下表提供单个 Inline Posture 节点可以支持的最大吞吐量和最大终端数。

表 *3*：*Inline Posture* 节点大小建议

属性	性能
每个物理设备的最大终端数	5,000 至 20,000（由策略服务节点进行门控）
每个物理设备的最大吞吐量	936 Mbps

Inline Posture 规划注意事项

网络或系统架构师在规划部署 Inline Posture 节点时必须解决以下基本问题：

- 配置计划是否将包括 Inline Posture 主/次对配置？ Cisco ISE 网络支持任何时候在网络上配置最多两个 Inline Posture 节点。
- 您将选择什么类型的 Inline Posture 操作模式？

注意 配置 Inline Posture 节点时，应将 Inline Posture 节点上不受信任的接口断开连接。如果受信任和不受信任的接口在初始配置过程中连接到同一 VLAN，并且 Inline Posture 节点在更改角色后启动，则组播数据包流量会泛洪溢出不受信任的接口。此组播事件可能会使连接到同一子网或 VLAN 的设备崩溃。 Inline Posture 节点此时处于维护模式。

注意 添加到部署后，请勿更改 Inline Posture 节点的 CLI 密码。 如果密码更改，通过管理节点访问 Inline Posture 节点时，系统会显示 Java 异常错误，并且 CLI 会锁定。 您需要通过使用安装 DVD 并重启 Inline Posture 节点来恢复密码。 或者，您可以将密码设置为原始密码。

如果要更改密码，请撤销注册部署中的 Inline Posture 节点，修改密码，然后使用新凭证将节点添加到部署中。

支持 Cisco ISE 功能所需的交换机和无线局域网控制器配置

要确保 Cisco ISE 能够与网络交换机互操作，并且来自 Cisco ISE 的功能可跨网段成功实施，您必须使用某些所需的网络时间协议 (NTP)、RADIUS/AAA、IEEE 802.1X、MAC 身份验证绕行 (MAB) 和其他设置来配置网络交换机。

第 2 章

Cisco SNS-3400 系列设备

Cisco SNS 对 Cisco ISE 的支持

Cisco ISE 软件在专用 Cisco SNS-3400 系列设备上或在 VMware 服务器上运行。 Cisco ISE 软件不支持在此专用平台上安装任何其他软件包或应用。

Cisco ISE 3300 系列、Cisco NAC 3300 系列和 Cisco Secure ACS 1121 设备也支持此 Cisco ISE 软件。您可以将现有的 Cisco ISE 3300 系列设备升级到最新版本。

Cisco SNS-3400 系列设备硬件规格

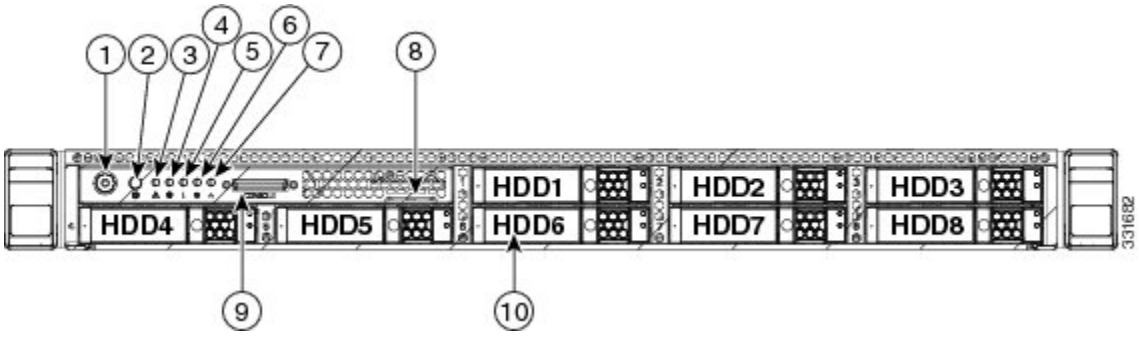
Cisco SNS-3400 系列设备硬件包括 Cisco SNS 3415 和 3495 设备。

表 *4*: *Cisco ISE SNS 3415/3495* 设备硬件摘要

Cisco ISE 设备	硬件规格
Cisco SNS- 3415-K9	• Cisco UCS C220 M3 • 单插槽 Intel E5-2609 2.4Ghz CPU，共 4 个内核，4 个线程 • 16 GB RAM • 1 个 600-GB 磁盘 • 嵌入式软件 RAID 0 • 4 GE 网络接口
Cisco SNS- 3495-K9	• Cisco UCS C220 M3 • 双插槽 Intel E5-2609 2.4Ghz CPU，共 8 个内核，8 个线程 • 32 GB RAM • 2 个 600-GB 磁盘 • RAID 0+1 • 4 GE 网络接口

Cisco SNS-3400 系列前面板

图 *7*: *Cisco SNS 3415/3495* 前面板

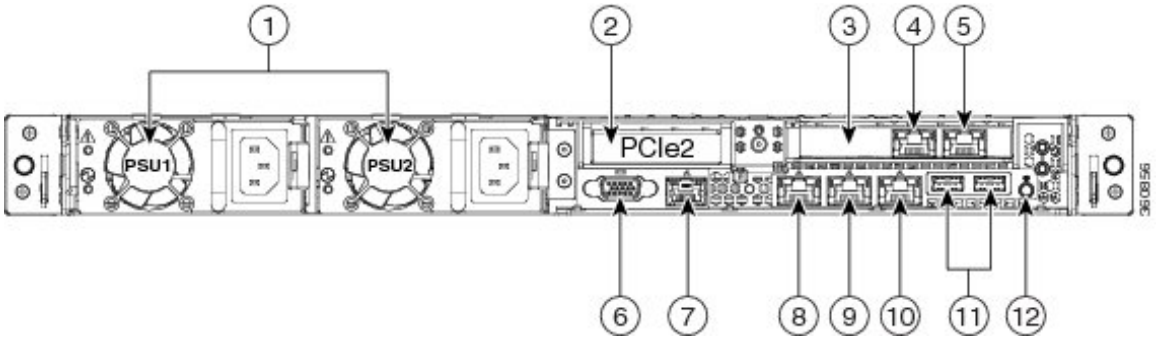


1	电源按钮/电源状态 LED	6	电源状态 LED
2	标识按钮 LED	7	网络链路活动 LED

3	系统状态 LED	8	资产标签（序列号）
4	风扇状态 LED	9	键盘、视频、鼠标 (KVM) 连接器（与 KVM 电缆结合用于提供两个USB、一个视频图形适配器 (VGA) 和一个串行连接器）
5	温度状态 LED	10	驱动器（最多八个2至5英寸热插拔驱动器）

Cisco SNS-3400 系列后面板

图 *8*：*SNS 3415/3495* 后面板



1	电源（最多两个）	7	串行端口（RJ-45 连接器）
2	插槽2：转接卡上的矮小型外围组件快速互连 (PCIe) 插槽（半高、半长、x16 连接器、x16 通道宽度）	8	1-GB 以太网专用管理端口，用于访问 CIMC（标有 M）
3	插槽 1 ：PCIe1 卡，其中包含 1-GB 以太网端口（GigE2 和 GigE3）	9	1-GB 以太网端口 1 (GigE0)，用于 Cisco ISE 管理通信
4	1-GB 以太网端口 3 (GigE2)	10	1-GB 以太网端口 2 (GigE1)
5	1-GB 以太网端口 4 (GigE3)	11	USB 端口
6	VGA 视频连接器	12	后标识按钮

序列号位置

服务器的序列号印在服务器顶部靠近前面的标签上。

第 3 章

安装和配置 Cisco SNS-3400 系列设备

安装 SNS-3400 系列设备的必备条件

在您尝试 Cisco SNS-3400 系列设备上配置 Cisco ISE 软件之前，请审查本章所列的配置必备条件，以及本指南中后面介绍的物理、环境和电源规格。 有关合规性和安全性的信息，请参阅《Cisco SNS-3415 和 Cisco SNS-3495 设备的 RCSI》。

Cisco SNS-3400 系列设备预安装有思科应用部署引擎操作系统 (ADE-OS) 和 Cisco ISE 软件。

确保您在继续之前确定部署中每个节点的以下所有配置设置：

- 主机名
- 千兆以太网 0 (eth0) 接口的 IP 地址
- 网络掩码
- 默认网关
- 域名系统 (DNS) 域
- 主要域名服务器
- 主要网络时间协议 (NTP) 服务器

- 系统时区
- 用户名（CLI 管理员用户的用户名）
- 密码（CLI 管理员用户的密码）

有关这些具有示例值的参数的说明，请参阅Cisco ISE 设置程序参数，第 23 页。

注释 Cisco SNS-3400 系列设备必须配置 RAID，之后您才能在其之上安装 Cisco ISE。 如果您已删除 Cisco SNS-3400 系列设备上的 RAID 配置，则必须重新对其进行配置。 有关详细信息，请参阅在 SNS-3415 设备上配置 RAID，第 67 页和 使用 CIMC 在 SNS-3495 设备上配置 RAID，第 67 页。

从 Cisco.com 下载 Cisco ISE ISO 映像

下载 ISO 映像以在 Cisco SNS-3400 系列设备上安装 Cisco ISE。

开始之前

对于 Inline Posture 节点，您必须下载 Inline Posture 节点 ISO 并继续安装过程。

步骤 1 转至 http://www.cisco.com/go/ise。您必须已经具有有效的 Cisco.com 登录凭证才能访问此链接。

步骤 2 点击 **Download Software for this Product**
Cisco ISE 软件映像随附已安装的 90 天评估许可证，因此，您可以在安装和初始配置完成时开始测试所有 Cisco ISE 服务。

在 SNS-3400 系列设备上安装 Cisco ISE 软件的方法

如果您的 SNS-3400 系列设备运行的是较早版本的 Cisco ISE，则您可以选择使用应用升级命令将其升级。 或者，您可以重新映像现有 SNS-3400 系列设备，以执行 Cisco ISE 全新安装并将其注册到现有部署。

下载 ISO 映像后，您可以通过以下任何一种方法将其安装在 SNS-3400 系列设备上：

- 使用 CIMC 远程管理实用程序安装 ISO 映像。 您必须配置 CIMC 才能执行此远程安装。
  1. 配置 CIMC。
  2. 远程安装 Cisco ISE 软件。
- 使用 USB 闪存驱动器安装 ISO 映像。
  1. 使用 iso-to-usb.sh 脚本创建可启动 USB 闪存驱动器。

2 将 USB 闪存设备连接到 SNS-3400 系列设备。

3 使用本地 KVM 或远程使用 CIMC KVM 安装 Cisco ISE 软件。

- 使用具有 USB 端口的外部 DVD 驱动器安装 ISO。

1 将 ISO 映像刻录到 DVD。

2 将外部 USB DVD 连接到 SNS-3400 系列设备。

3 通过本地 KVM 或远程使用 CIMC KVM 安装 Cisco ISE 软件。

注释 使用USB 闪存设备或具有USB 端口的外部DVD 来安装Cisco ISE 软件时，CIMC 配置是可选的。

配置思科集成管理控制器

您可以通过 CIMC 在 Cisco SNS-3400 系列设备上执行所有操作，包括监控服务器和系统事件日志。为此，您必须先配置 IP 地址和 IP 网关，以从基于 Web 的浏览器访问 CIMC。

步骤 1 插入电源线。

步骤 2 按 **Power** 按钮启动服务器。

步骤 3 在启动过程中，当出现提示时，请按 **F8** 打开 BIOS CIMC 配置实用程序。

步骤 4 设置 NIC 模式，以指定哪些端口会访问 CIMC 进行服务器管理。 Cisco ISE 最多可以使用四个千兆以太网端口。

- Dedicated - 1-GB 以太网管理端口用于访问 CIMC。 您必须选择 NIC 冗余 *None* 并选择 IP 设置。
- Shared LOM (default) - 两个 1-GB 以太网端口用于访问 CIMC。 这是出厂默认设置，同时还启用了主动-主动 NIC 冗余和 DHCP。
- Cisco Card - 已安装的 Cisco UCS P81E VIC 上的端口用于访问 CIMC。 您必须选择 NIC 冗余和 IP 设置。

  注释 当前只有 PCIe 插槽 1 中安装的 Cisco UCS P81E VIC (N2XX-ACPCI01) 支持思科网络接口卡模式。

步骤 5 指定 NIC 冗余设置：

- None - 以太网端口独立运行，如果有问题，不会进行故障切换。
- Active-standby - 如果主动以太网端口发生故障，则流量会切换到备用端口。
- Active-active - 同时使用所有以太网端口。

步骤 6 选择为动态网络设置启用 DHCP 还是输入静态网络设置。

注释　在您启用 DHCP 之前，此 DHCP 服务器必须预配置有该服务器的 MAC 地址范围。 MAC 地址印在服务器后面的标签上。 此服务器的范围包括分配给 CIMC 的六个 MAC 地址。 标签上印的 MAC 地址是六个连续 MAC 地址所组成的范围的开头。

步骤 7　（可选）指定 VLAN 设置并设置默认 CIMC 用户密码。

注释　对这些设置的更改会在大约 45 秒后生效。 在下一步中重新启动服务器之前，请按 F5 刷新并等待直至显示新设置。

步骤 8　按 **F10** 保存设置并重新启动服务器。

注释　如果您选择启用 DHCP，则在启动过程中，控制台屏幕上会显示动态分配的 IP 和 MAC 地址。

接下来的操作

使用 CIMC 在 Cisco SNS-3400 系列设备上配置 ISE

创建可启动 USB 驱动器

Cisco ISE ISO 映像包含“images”目录，其中具有自述文件，以及用于创建可启动 USB 驱动器以安装 Cisco ISE 的脚本。

开始之前

- 确保您已阅读“images”目录中的自述文件
- 您需要以下各项：

  具有 RHEL-6.4 和 CentOS 6.4 的 Linux 计算机。 如果您即将使用 PC 或 MAC，请确保已在其上安装 Linux 虚拟机 (VM)。

  8-GB USB 驱动器

  iso-to-usb.sh 脚本

步骤 1　将 USB 驱动器插入 USB 端口。

步骤 2　将 iso-to-usb.sh 脚本和 Cisco ISE ISO 映像复制到 Linux 计算机上的目录。

步骤 3　输入以下命令：
iso-to-usb.sh*source_iso usb_device*

例如，# **./iso-to-usb.sh***ise-1.4.0.253-x86_64.iso /dev/sdb*，其中 **iso-to-usb.sh** 是脚本的名称，*ise-1.4.0.253-x86_64.iso /dev/sdb* 是 ISO 映像的名称，*/dev/sdb* 是 USB 设备。

步骤 4 为要安装映像的设备输入值。

步骤 5 输入 **Y** 以继续。

步骤 6 系统将显示一条成功消息。

步骤 7 拔下 USB 驱动器。

接下来的操作

使用 CIMC 在 Cisco SNS-3400 系列设备上配置 ISE

Cisco ISE 设置程序参数

当 Cisco ISE 软件配置开始时，交互式 CLI 会提示您输入配置系统所需的参数。

注释 如果您是在 VMware 服务器上安装 Cisco ISE 软件，则在初始设置过程中，Cisco ISE 还会安装和配置版本 8.3.2 的 VMware 工具。

表 5: *Cisco ISE* 设置程序参数

提示	描述	示例
Hostname	不得超过 15 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。 注释 我们建议您使用小写字母，以确保 Cisco ISE 中的证书身份验证不受基于证书的验证中细微差异的影响。 不能使用“localhost”作为节点的主机名。	isebeta1
(eth0) Ethernet interface address	必须是千兆以太网 0 (eth0) 接口的有效 IPv4 地址。	10.12.13.14
Netmask	必须是有效的 IPv4 网络掩码。	255.255.255.0
Default gateway	必须是默认网关的有效 IPv4 地址。	10.12.13.1
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	必须是主要域名服务器的有效 IPv4 地址。	10.15.20.25

提示	描述	示例
Add/Edit another name server	必须是其他域名服务器的有效 IPv4 地址。	（可选）允许您配置多个域名服务器。为此，请输入 y 以继续。
Primary NTP server	必须是网络时间协议 (NTP) 服务器的有效 IPv4 地址或主机名。	**clock.nist.gov**
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。为此，请输入 y 以继续。
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）。 您可以从 Cisco ISE CLI 运行**show timezones** 命令以获取受支持时区的完整列表。 注释 我们建议您将所有 Cisco ISE 节点都设置为 UTC 时区。此时区设置可确保来自部署中的各种节点的报告、日志和状态代理日志文件在时间戳方面始终同步。	UTC （默认值）
Username	识别用于对 Cisco ISE 系统进行 CLI 访问的管理用户名。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	识别用于对 Cisco ISE 系统进行 CLI 访问的管理密码。由于没有默认值，您必须创建此密码。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

使用 CIMC 在 Cisco SNS-3400 系列设备上配置 ISE

为设备配置 CIMC 后，您可以使用其管理 Cisco SNS-3400 系列设备。您可以通过 CIMC 执行所有操作，包括 BIOS 配置。

注意 安装后在 Cisco ISE 设备上更改时区会导致该节点上的 Cisco ISE 应用不可用。

开始之前

- 确保您已在设备上配置 CIMC。
- 确保您已按照建议的程序正确安装、连接受支持的设备并接通电源。
- 确保您在客户端计算机上具有用于从中访问 CIMC 的 Cisco ISE ISO 映像，或者具有包含用于安装的映像的可启动 USB。
- Cisco ISE 设备使用 UTC 时区在内部跟踪时间。 如果您不知道具体的时区，则可以根据 Cisco ISE 设备所在的城市、区域或国家/地区输入一个时区。我们建议您在安装过程中当设置程序提示您配置首选时区（默认为 UTC）时配置该设置。
- 研究如何在 Inline Posture 节点上配置证书。

步骤 1 连接到 CIMC 以进行服务器管理。 使用网络接口卡 (NIC) 模式设置选择的端口将以太网电缆从 LAN 连接到服务器。 主动-主动和主动-被动 NIC 冗余设置要求您连接到两个端口。

步骤 2 使用浏览器和 CIMC 的 IP 地址登录到 CIMC 设置实用程序。 IP 地址取决于所进行的 CIMC 配置（静态地址或由动态主机配置协议 [DHCP] 服务器分配的地址）。

注释 服务器的默认用户名为 *admin*。 默认密码为 *password*。

步骤 3 点击 **Launch KVM Console**。

步骤 4 使用 CIMC 凭证进行登录。

步骤 5 点击 **Virtual Media** 选项卡。

步骤 6 点击 **Add Image** 以从运行客户端浏览器的系统中选择 Cisco ISE ISO 映像。

步骤 7 针对已创建的虚拟 CD/DVD 驱动器选中 **Mapped** 复选框。

步骤 8 点击 **KVM** 选项卡。

步骤 9 选择 **Macros** > **Ctrl-Alt-Del** 以使用 ISO 映像启动 SNS-3400 系列设备。

步骤 10 按 **F6** 以显示启动菜单。

步骤 11 选择已映射的 CD/DVD 并按 **Enter** 键。

步骤 12 按照启动提示，输入 **2** 并按 **Enter** 键。

```
**********************************************

请键入“setup”以配置设备

**********************************************
```

步骤 13 按照提示，键入**setup** 以启动设置程序。 系统将提示您输入网络参数和凭证。

以下显示的是设置程序示例和默认提示：

```
Press 'Ctrl-C' to abort setup
Enter hostname[]: ise-server-1
Enter IP address[]: 10.1.1.10
Enter IP netmask[]: 255.255.255.0
Enter IP default gateway[]: 172.10.10.10
Enter default DNS domain[]: cisco.com
Enter primary nameserver[]: 200.150.200.150
Add secondary nameserver? Y/N [N]: n
Enter NTP server[time.nist.gov]: 200.150.200.151
```

```
Add another NTP server? Y/N[N]: n
Enter system time zone[UTC]: UTC
Enable SSH service?: Y/N [N]: Y
Enter username [admin]: admin
Enter password:
Enter password again:
Copying first CLI user to be first ISE admin GUI user...
Bringing up the network interface...
Pinging the gateway...
Pinging the primary nameserver...

Do not use `Ctrl-C' from this point on...

Installing Applications...
Installing ISE...
Unbundling Application Package...
Initiating Application Install...

Application bundle (ISE) installed successfully

===Initial Setup for Application: ISE ===

Welcome to the ISE initial setup.  The purpose of this setup is to provision the internal ISE database.
  This setup is non-interactive, and will take roughly 15 minutes to complete.

Running database cloning script...
Running database network config assistant tool...
Extracting ISE database contents...
Starting ISE database processes...

...
```

配置 Cisco ISE 节点软件后，Cisco ISE 系统自动重新启动。 要重新登录到 CLI，您必须输入设置过程中配置的 CLI 管理员用户凭证。

步骤 14 登录到 Cisco ISE CLI 外壳，然后运行以下 CLI 命令以检查 Cisco ISE 应用进程的状态：

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


ISE PROCESS NAME                       STATE            PROCESS ID
--------------------------------------------------------------------
Database Listener                      running          3638
Database Server                        running          45 PROCESSES
Application Server                     running          5992
Profiler Database                      running          4481
AD Connector                           running          6401
M&T Session Database                   running          2319
M&T Log Collector                      running          6245
M&T Log Processor                      running          6286
Certificate Authority Service          running          6211
pxGrid Infrastructure Service          disabled
pxGrid Publisher Subscriber Service    disabled
pxGrid Connection Manager              disabled
pxGrid Controller                      disabled
Identity Mapping Service               disabled
```

步骤 15 在您确认 Cisco ISE 应用服务器正在运行后，可以使用受支持的 Web 浏览器之一登录到 Cisco ISE 用户界面。 要使用 Web 浏览器登录到 Cisco ISE 用户界面，请在 Address 字段中输入 **https://<your-ise-hostname or IP address>/admin/**，此处“your-ise-hostname or IP address”表示您在设置过程中为 Cisco SNS-3400 系列设备配置的主机名或 IP 地址。 输入基于 Web 的管理员登录凭证（用户名和密码）以访问 Cisco ISE 用户界面。 您最初可以使用设置过程中定义的 CLI 管理员用户的用户名和密码来访问 Cisco ISE Web 界面。 用于对 Cisco ISE 用户界面进行基于 Web 的访问的用户名和密码凭证不同于设置过程中创建的用于访问 Cisco ISE CLI 接口的 CLI 管理员用户凭证。 在您登录到 Cisco ISE 用户界面后，即可配置设备、用户库、策略和其他组件。

受支持的时区

本节提供三个表，其中提供有关欧洲、美国和加拿大、澳大利亚及亚洲的通用协调世界时 (UTC) 时区的详细信息。 Cisco ISE CLI**show timezones** 命令显示可供使用的所有时区的列表。

注释 我们建议您将所有 Cisco ISE 节点都设置为 UTC 时区。 此时区设置可确保来自部署中的各种节点的报告、日志和状态代理日志文件在时间戳方面始终同步。

时区的格式为 POSIX 或 System V。POSIX 时区格式语法类似于 America/Los_Angeles，System V 时区语法类似于 PST8PDT。

表 *6*：欧洲、美国和加拿大时区

缩写词或名称	时区名称
欧洲	
GMT、GMT0、GMT-0、GMT+0、UTC、格林威治、世界时、祖鲁	格林威治标准时间，即 UTC
GB	英国
GB-Eire、Eire	爱尔兰
WET	西欧时间，即 UTC
CET	中欧时间，即 UTC + 1 小时
EET	东欧时间，即 UTC + 2 小时
美国和加拿大	
EST、EST5EDT	东部标准时间，即 UTC - 5 小时
CST、CST6CDT	中部标准时间，即 UTC - 6 小时
MST、MST7MDT	山地标准时间，即 UTC - 7 小时
PST、PST8PDT	太平洋标准时间，即 UTC - 8 小时

缩写词或名称	时区名称
HST	夏威夷标准时间，即 UTC - 10 小时

表 7：澳大利亚时区

澳大利亚			
将国家/地区和城市一起输入，之间以正斜杠 (/) 分隔；例如澳大利亚/柯利。			
ACT（澳大利亚首度特区）	阿德莱德	布里斯班	布罗肯希尔
堪培拉	柯利	达尔文	霍巴特
豪勋爵	林德曼	LHI （豪勋爵岛）	墨尔本
北	NSW（新南威尔士）	珀斯	昆士兰州
南	悉尼	塔斯马尼亚岛	维多利亚
西	Yancowinna	—	—

表 8：亚洲时区

亚洲			
亚丁	阿拉木图	安曼	阿纳德尔
阿克套	阿克托别	阿什哈巴德	阿什喀巴德
巴格达	巴林	巴库	曼谷
贝鲁特	比什凯克	文莱	加尔各答
乔巴山	重庆	Columbo	大马士革
达喀尔	帝力	迪拜	杜尚别
加沙	哈尔滨	香港	科布多城
伊尔库茨克	伊斯坦布尔	雅加达	查亚普拉
耶路撒冷	喀布尔	堪察加	卡拉奇

亚洲			
喀什格尔	加德满都	吉隆坡	古晋
科威特	克拉斯诺雅茨克	—	—
注释 亚洲时区涵盖从东亚、东南亚南部、西亚到中亚的城市。 将地区和城市或国家/地区一起输入，之间以正斜杠 (/) 分隔；例如，亚洲/亚丁			

设置过程验证

要验证您是否已正确完成初始设置过程，请使用以下两种方法之一登录到 Cisco ISE 设备：

- Web 浏览器
- Cisco ISE CLI

登录到 Cisco ISE 用户界面后，您应执行以下任务：

- 注册许可证 - 有关详细信息，请参阅《*Cisco ISE* 管理员指南》中的注册许可证部分。
- 配置 Cisco ISE 系统 - 有关配置任务，请参阅《Cisco ISE 管理员指南》。

第 4 章

在 VMware 虚拟机上安装 ISE

虚拟机中不支持的 ISE 功能

只有 Cisco SNS-3415 和 Cisco ISE 3300 系列设备支持 Inline Posture 节点。 Cisco SNS-3495 系列或 VMware 服务器系统不支持该节点。 VMware 虚拟机支持使用所有其他指定角色。

受支持的 VMware 版本

Cisco ISE 支持以下 VMware 服务器和客户端：

- VMware ESXi 版本 5.*x*
- VMware vSphere 客户端 5.*x*

对 VMware vMotion 的支持

Cisco ISE 支持 VMware vMotion 功能，通过该功能，您可以在主机之间迁移实时虚拟机 (VM) 实例（运行任何角色）。 为使 VMware vMotion 功能正常工作，必须符合以下条件：

- 共享存储 - VM 的存储必须驻留在存储区域网络 (SAN) 上，并且该 SAN 必须可由能够托管正在移动的 VM 的所有 VMware 主机进行访问。
- VMFS 卷共享 - VMware 主机必须使用共享虚拟机文件系统 (VMFS) 卷。
- 千兆以太网互连 - SAN 和 VMware 主机必须通过千兆以太网链路进行互连。
- 处理器兼容性 - 必须使用一组兼容的处理器。 处理器必须来自同一供应商和处理器系列，以实现 vMotion 兼容性。

对开放式虚拟化格式的支持

Cisco ISE 支持开放式虚拟化格式 (OVF) 并提供可用于在虚拟机 (VM) 上安装和部署 Cisco ISE 的 OVA 模板。 以下 OVA 模板可用：

- ISE-1.4.*xxx*.*xxx*-eval.ova - 如果您评估的是 Cisco ISE，并且评估许可证最多支持 100 个终端，请使用此模板。
- ISE-1.4.*xxx*.*xxx*-virtual-SNS3415.ova - 如果 VMware 设备规格与 SNS-3415 设备兼容，请使用此模板。
- ISE-1.4.*xxx*.*xxx*-virtual-SNS3495.ova - 如果 VMware 设备规格与 SNS-3495 设备兼容，请使用此模板。

下表提供 OVA 模板保留。

OVA 模板	内存	CPU
虚拟评估 OVA	4 GB RAM	2300 MHz（无保留）
虚拟 SNS-3415 OVA	16 GB RAM	8000 MHz
虚拟 SNS-3495 OVA	32 GB RAM	16000 MHz

虚拟机要求

要实现可与 Cisco ISE 硬件设备相比的性能和可扩展性，应为 VMware 虚拟机分配与 Cisco SNS 3415 和 3495 设备相当的系统资源。

表 *9*：最低 *VMware* 系统要求

要求类型	最低要求
CPU	单四核；2.0 GHz 或更快。 Cisco ISE 支持超线程。 您可以在已启用或禁用超线程选项的 VMware 主机上安装 ISE。 **注释** 即使超线程可能会提高整体 VM 性能，但它不会更改每个 VM 设备支持的扩展限制。此外，您仍必须根据所需的物理核心数量而不是逻辑处理器的数量来分配 CPU 资源。
内存	16 至 32 GB RAM
硬盘	200 GB 至 2 TB 的磁盘存储（大小取决于部署和任务）。 我们建议您的 VM 主机服务器使用最低转速为 10,000 RPM 的硬盘。 Cisco ISE VM 要求最小写入带宽为 50 MB/秒，最小读取带宽为 300 MB/秒。 如果托管环境使用 10,000 RPM 磁盘，则可以轻松实现此写入带宽。 **注释** 请注意，当您为 Cisco ISE 创建虚拟机时，应使用符合存储要求的虚拟磁盘。如果为符合磁盘空间要求使用多个磁盘，则安装程序可能无法识别所有磁盘空间。
存储	• 文件系统 - VMFS 建议您使用 VMFS 进行存储。 其他存储协议未经测试，可能会导致一些文件系统错误。 • 内部存储 - SCSI/SAS • 外部存储 - iSCSI/SAN 不建议使用 NFS 存储。
磁盘控制器	Paravirtual （默认用于 64 位 RHEL）或 LSI 逻辑并行
网卡	需要 1 GB NIC 接口（建议使用两个或多个 NIC）。 Cisco ISE 支持 E1000 和 VMXNET3 适配器。 **注释** 我们建议您选择 E1000 以确保在默认情况下使用正确的适配器顺序。 如果选择 VMXNET3，则您可能必须重新映射 ESX 适配器以将其与 ISE 适配器顺序同步。
虚拟机监控程序	• VMware 版本 8，适用于 ESXi 5.*x* • VMware vSphere 客户端 5.*x*

VMware 设备大小建议

VMware 设备规格应可与生产环境中运行的物理设备相比较。

为设备分配资源时，请记住以下准则：

- 虚拟机资源应是专用资源。 VM 资源不应跨多个 VM 共享或超订用。
- 虚拟机上的策略服务节点可以部署为具有比管理或监控节点更少的磁盘空间。 建议将 100 至 200 GB 的磁盘空间用于策略服务节点。
- 虚拟机可配置有 1 至 4 个 NIC。 建议预留 2 个或更多 NIC。 其他接口可用于支持各种服务，例如分析或 RADIUS。

表 *10*：生产环境的 *VMware* 设备规格

平台	**SNS-3415**	**SNS-3495**
处理器	单插槽 Intel E5-2609 2.4 Ghz CPU 共 4 个内核	双插槽 Intel E5-2609 2.4 Ghz CPU 共 8 个内核
内存	16 GB	32 GB
总磁盘空间	600 GB	600 GB
以太网卡	4 个集成的千兆网卡	4 个集成的千兆网卡

磁盘空间要求

下表列出针对在生产部署中运行 VMware 服务器建议的 Cisco ISE 磁盘空间分配。

表 *11*：建议的 *VMware* 磁盘空间

ISE 角色	最小磁盘空间	最大磁盘空间	针对生产的建议磁盘空间
独立 ISE	200 GB	2 TB	600 GB 至 2 TB
分布式 ISE - 仅限管理	200 GB	2 TB	250 至 300 GB
分布式 ISE - 仅限监控	200 GB	2 TB	600 GB 至 2 TB
分布式 ISE - 仅限策略服务	200 GB	2 TB	200 GB

ISE 角色	最小磁盘空间	最大磁盘空间	针对生产的建议磁盘空间
分布式 ISE - 管理和监控	200 GB	2 TB	600 GB 至 2 TB
分布式 ISE - 管理、监控和策略服务	200 GB	2 TB	600 GB 至 2 TB

磁盘空间准则

在决定 Cisco ISE 的磁盘空间时，请记住以下准则：

- 您最多可以为 Cisco ISE 虚拟机 (VM) 分配 2 TB 的磁盘空间。
- Cisco ISE 必须安装在 VMware 中的单个磁盘上 。
- 磁盘分配根据日志记录保留要求而异。 在已启用监控角色的任何节点上，30% 的 VM 磁盘空间分配用于日志存储。 具有 25,000 个终端的部署每天会生成大约 1 GB 的日志。

  例如，如果您具有包含 600 GB VM 磁盘空间的监控节点，则 180 GB 分配用于日志存储。 如果每天 100,000 个终端连接到此网络，则每天会生成大约 4 GB 的日志。 在此情况下，您可以在监控节点中存储 38 天的日志，此后必须将旧数据转移到存储库并从监控数据库中将其清除。

为进行额外的日志存储，您可以增大 VM 磁盘空间。 每增加 100 GB 磁盘空间，即可额外获得 30 GB 用于日志存储。 根据您的要求，您可以将 VM 磁盘大小最多增大为 2 TB 或 614 GB 的最大日志存储大小。

如果增大虚拟机的磁盘大小，则不得对 Cisco ISE 进行升级，而是需要在虚拟机上执行 Cisco ISE 全新安装。

表 12：日志可在监控节点中存储的天数 根据分配给监控节点的磁盘空间和连接到网络的终端数提供日志可以在该节点上保留的天数。 数量根据日志抑制和异常客户端检测的启用情况而定。

表 *12*：日志可在监控节点中存储的天数

终端数	200 GB	400 GB	600 GB	1024 GB	2048 GB
10,000	126	252	378	645	1,289
20,000	63	126	189	323	645
30,000	42	84	126	215	430
40,000	32	63	95	162	323
50,000	26	51	76	129	258
100,000	13	26	38	65	129

终端数	200 GB	400 GB	600 GB	1024 GB	2048 GB
150,000	9	17	26	43	86
200000	7	13	19	33	65
250,000	6	11	16	26	52

虚拟机资源和性能检查

在虚拟机上安装 Cisco ISE 之前，安装程序会执行硬件完整性检查，将虚拟机上的可用硬件资源与建议的规格进行对比。

在 VMware 资源检查过程中，安装程序会检查硬盘空间、分配给 VM 的 CPU 内核数、CPU 时钟速度和分配给 VM 的 RAM。 如果 VM 资源不符合建议的规格，则安装会中止。 此 VMware 资源检查仅适用于基于 ISO 的安装。

当您运行设置程序时，系统会执行 VM 性能检查，其中安装程序将检查磁盘 I/O 性能。 如果磁盘 I/O 性能不符合建议的规格，则屏幕上会出现警告，但是您可以继续安装。 此性能验证检查适用于基于 ISO 的安装和 OVA 安装。

系统会定期（每小时）执行 VM 性能检查，并对一天的结果进行平均。 如果磁盘 I/O 性能不符合建议的规格，系统会生成警报。

此外，您也可以使用**show tech-support** 命令从 Cisco ISE CLI 按需执行 VM 性能检查。

VM 资源和性能检查可以在不依赖于 Cisco ISE 安装的情况下运行 。 您可以从 Cisco ISE 启动菜单执行此测试。

使用 Show Tech Support 命令按需检查虚拟机性能

您可以从 CLI 运行**show tech-support** 命令以随时检查 VM 性能。 此命令的输出将类似于以下内容。

```
ise-vm123/admin# show tech | begin "disk IO perf"
Measuring disk IO performance
****************************************
Average I/O bandwidth writing to disk device: 48 MB/second
Average I/O bandwidth reading from disk device: 193 MB/second
WARNING: VM I/O PERFORMANCE TESTS FAILED!
WARNING: The bandwidth writing to disk must be at least 50 MB/second,
WARNING: and bandwidth reading from disk must be at least 300 MB/second.
WARNING: This VM should not be used for production use until disk
WARNING: performance issue is addressed.
Disk I/O bandwidth filesystem test, writing 300 MB to /opt:
314572800 bytes (315 MB) copied, 7.81502 s, 40.3 MB/s
Disk I/O bandwidth filesystem read test, reading 300 MB from /opt:
314572800 bytes (315 MB) copied, 0.416897 s, 755 MB/s
```

从 Cisco ISE 启动菜单检查虚拟机资源

您可以在不依赖于 Cisco ISE 安装的情况下从启动菜单检查虚拟机资源。

CLI 记录显示如下：

```
Welcome to the Cisco Identity Services Engine Installer
     Cisco ISE Version: 1.4.0.205

Available boot options:

  [1] Cisco ISE Installation (Keyboard/Monitor)
  [2] Cisco ISE Installation (Serial Console)
  [3] System Utilities (Keyboard/Monitor)
  [4] System Utilities (Serial Console)
  <Enter> Boot existing OS from hard disk.

Enter boot option and press <Enter>.
```

从 CLI 启动菜单中，输入 **3** 或 **4** 以转至 System Utilities 菜单。

```
Cisco ISE System Utilities Menu

Available System Utilities:

  [1] Recover administrator password
  [2] Virtual Machine Resource Check
  [3] System Erase
  [4] Install Media Check
  [q] Exit and reload

Enter option and press <Enter>
```

输入 **2** 以检查 VM 资源。 其输出与下列显示类似：

```
*****
***** Virtual Machine host detected…
***** Hard disk(s) total size detected: 322 Gigabyte
***** Physical RAM size detected: 40443664 Kbytes
***** Number of network interfaces detected: 1
***** Number of CPU cores: 2
***** CPU Mhz: 2300.00
***** Verifying CPU requirement…
***** Verifying RAM requirement…
***** Writing disk partition table…
```

评估 Cisco ISE 版本

要获取 Cisco ISE 评估软件 (R-ISE-EVAL-K9=)，请与您的思科客户团队或授权的思科渠道合作伙伴联系。

要将 Cisco ISE 配置从评估系统迁移至完全许可的生产系统，您需要完成以下任务：

- 备份评估版本的配置。
- 确保您的生产VM具有所需的磁盘空间量。有关详细信息，请参阅“部署规模和扩展建议”。
- 安装生产部署许可证。
- 将配置恢复到生产系统。

注释 对于评估，VMware 服务器上的硬盘的最低分配要求为 200 GB。 将 VMware 服务器移至支持更多用户数的生产环境时，请务必将 Cisco ISE 安装重新配置为建议的最小磁盘大小或更高容量（最多达到允许的最大值，即 2 TB）。

开始之前

为进行评估，Cisco ISE 可以安装在任何符合 VM 要求的受支持 VMware 虚拟机 (VM) 上。 评估 Cisco ISE 时，您可以在 VM 中配置更少的磁盘空间，但是仍需要分配最小为 200 GB 的磁盘空间。

步骤 1 转至 http://www.cisco.com/go/ise。 您必须已经具有有效的 Cisco.com 登录凭证才能访问此链接。

步骤 2 点击 **Download Software for this Product**。
软件映像随附已安装的 90 天评估许可证，因此，您可以在安装和初始配置完成时开始评估所有 Cisco ISE 服务。

在虚拟机上安装 Cisco ISE

您可以通过以下任何一种方式在 VM 上安装 Cisco ISE。 我们建议您下载并部署 Cisco ISE OVA 模板。

- 使用 OVA 模板在虚拟机上部署 Cisco ISE ， 第 38 页
- 使用 ISO 文件在虚拟机上安装 Cisco ISE， 第 39 页
- 克隆 Cisco ISE 虚拟机， 第 45 页

使用 OVA 模板在虚拟机上部署 Cisco ISE

您可以使用 OVA 模板在虚拟机上安装和部署 Cisco ISE 软件。 从 Cisco.com 下载 OVA 模板。

开始之前

您可以使用 OVA 模板在虚拟机上安装和部署 Cisco ISE 软件

步骤 1 打开 **VMware vSphere** 客户端。

步骤 2 登录到 VMware 主机。

步骤 3 从 VMware vSphere 客户端中选择 **File** > **Deploy OVF Template**。

步骤 4 点击 **Browse** 选择 OVA 模板，然后点击 **Next**。

步骤 5 确认 OVF Template Details 页面中的详细信息，然后点击 **Next**。

步骤 6 在 Name and Location 页面中输入虚拟机的名称以对其进行唯一识别，然后点击 **Next**。

步骤 7 选择数据存储以托管 OVA。

步骤 8 点击 Disk Format 页面中的 **Thick Provision** 单选按钮，然后点击 **Next**。
Cisco ISE 同时支持详细和精简调配。 但是，我们建议您选择详细调配以获取更好的性能，尤其对于监控节点更加如此。 如果您选择精简调配，则诸如升级、备份和恢复，以及调试日志记录等需要更多磁盘空间的操作在初始磁盘扩展期间可能会受影响。

步骤 9 验证 Ready to Complete 页面中的信息。 选中 **Power on after deployment** 复选框。

步骤 10 点击 **Finish**。

使用 ISO 文件在虚拟机上安装 Cisco ISE

要使用 ISO 文件在 VM 上安装 Cisco ISE，请执行以下操作：

开始之前

- 确保您根据本章中指定的要求读取并分配 VM 资源。
- 确保您已阅读“配置 VMware ESX 或 ESXi 服务器的必备条件”部分。
- 从 Cisco.com 下载 Cisco ISE ISO 映像。

步骤 1 配置 VMware 服务器。 请参阅配置 VMware 服务器， 第 42 页。

步骤 2 配置 VMware 系统以从软件 DVD 启动。 请参阅将 VMware 系统配置为从 Cisco ISE 软件 DVD 启动， 第 43 页。

步骤 3 在 VM 上安装 Cisco ISE 软件。 请参阅从 DVD 安装 Cisco ISE 软件。

配置 VMware ESX 或 ESXi 服务器的必备条件

在您尝试配置 VMware ESX 或 ESXi 服务器之前，请审查本节所列的以下配置必备条件：

- 请记住，应使用具有管理权限的用户（root 用户）身份登录 ESXi 服务器。
- Cisco ISE 是 64 位系统。 在安装 64 位系统之前，请确保在 ESX/ESXi 服务器上启用虚拟化技术 (VT)。 此外，请确保虚拟机的访客操作系统设置为 64 位。 您还必须确保访客操作系统类型设置为 Red Hat Enterprise Linux 6（64 位）。
- 对于 Red Hat Enterprise Linux 6，默认 NIC 类型是 VMXNET3 适配器。 您最多可以为 Cisco ISE 虚拟机添加四个 NIC，但请确保为所有 NIC 选择同一适配器。 Cisco ISE 支持 E1000 适配器。

注释 如果您选择默认网络驱动程序 (VMXNET3) 作为网络适配器，请检查物理适配器映射。 确保将 Cisco ISE 千兆以太网 0 接口映射到 ESX 中的第 4 个接口 (NIC 4)。 如果您选择 E1000 适配器，则默认情况下 ESX 和 Cisco ISE 适配器会正确映射 。

- 确保在 VMware 虚拟机上分配建议的磁盘空间量。
- 如果您尚未创建 VMware 虚拟机文件系统 (VMFS)，则必须创建该文件系统以支持 Cisco ISE 虚拟设备。 系统会为 VMware 主机上配置的每个存储卷设置 VMFS。

  如果您使用 VMFS5，则 1 MB 块大小最多支持 2 TB 虚拟磁盘大小。

  如果您使用 VMFS3，则必须根据 VMware 主机上托管的最大虚拟磁盘大小选择 VMFS 块大小。 您配置 VMFS 块大小后，如果不重新格式化 VMFS 分区，则无法更改该大小。 对于 VMFS3，VMFS 块大小应取决于最大虚拟磁盘的大小：

表 *13*: *VMFS* 块大小

块大小	虚拟磁盘大小
1 MB	256 GB
2 MB	512 GB
4 MB	1 TB
8 MB	2 TB

虚拟化技术检查

如果您已经安装 ESX 或 ESXi 服务器，则可以检查是否在其之上启用了 VT，而无需重新启动计算机。 为此，请使用**esxcfg-info** 命令。 以下为输出示例：

```
~ # esxcfg-info |grep "HV Support"
|----HV Support.......................................3
|----World Command Line..............................grep HV Support
```

如果 HV Support 的值为 3，则表明在 ESX 或 ESXi 服务器上启用了 VT，您可以继续安装。

如果 HV Support 的值为 2，则表明支持 VT，但未在 ESX 或 ESXi 服务器上将其启用。 您必须编辑 BIOS 设置并在 ESX 或 ESXi 服务器上启用 VT。

在 ESX 或 ESXi 服务器上启用虚拟化技术

您可以重复使用用于托管以前版本的 Cisco ISE 虚拟机的相同硬件。 但是，在安装最新版本之前，您必须在 ESX 或 ESXi 服务器上启用虚拟化技术 (VT)。

步骤 1 重新启动 SNS-3400 系列设备。

步骤 2 按 **F2** 以进入设置。

步骤 3 选择 **Advanced** > **Processor Configuration**。

步骤 4 选择 **Intel(R) VT** 并将其启用。

步骤 5 按 **F10** 以保存更改并退出。

为 Cisco ISE Profiler Service 配置 VMware 服务器接口

配置 VMware 服务器接口以支持将交换端口分析器 (SPAN) 或镜像流量收集到 Cisco ISE Profiler Service 的专用探测接口。

步骤 1 选择 **Configuration** > **Networking** > **Properties** > **VMNetwork**（VMware 服务器实例的名称）**VMswitch0**（其中一个 VMware ESXi 服务器实例） **Properties Security**。

步骤 2 在 **Security** 选项卡上的 Policy Exceptions 窗格中，选中 **Promiscuous Mode** 复选框。

步骤 3 在 Promiscuous Mode 下拉列表中，选择 **Accept**，然后点击 **OK**。
在用于对 SPAN 或镜像流量收集分析器数据的其他 VMware ESX 服务器接口上重复相同的步骤。

使用串行控制台连接到 VMware 服务器

步骤 1 关闭特定 VMware 服务器（例如 ISE-120）的电源。

步骤 2 右键点击 VMware 服务器，然后选择 **Edit**。

步骤 3 点击 Hardware 选项卡上的 **Add**。

步骤 4 选择 **Serial Port**，然后点击 **Next**。

步骤 5 在 Serial Port Output 区域中，点击 **Use physical serial port on the host** 或 **Connect via Network** 单选按钮，然后点击 **Next**。

- 如果您选择 Connect via Network 选项，则必须打开 ESX 服务器上的防火墙端口。
- 如果您在主机上选择 Use physical serial port，请选择端口。 您可以选择以下两个选项之一：

  /dev/ttyS0（在 DOS 或 Windows 操作系统中，这将显示为 COM1）。

  /dev/ttyS1（在 DOS 或 Windows 操作系统中，这将显示为 COM2）。

步骤 6 点击 **Next**。

步骤 7 在 Device Status 区域中，选中相应的复选框。 默认值为 Connected。

步骤 8 点击 **OK** 以连接到 VMware 服务器。

配置 VMware 服务器

开始之前

确保您已阅读“配置 VMware ESX 或 ESXi 服务器的必备条件”中的详细信息。

步骤 1 登录到 ESXi 服务器。

步骤 2 在 VMware vSphere 客户端的左窗格中，右键点击主机容器，然后选择 **New Virtual Machine**。

步骤 3 在 Configuration 对话框中，针对 VMware 配置选择 **Custom**，然后点击 **Next**。

步骤 4 输入 VMware 系统的名称，然后点击 **Next**。

提示 提示：请使用要用于 VMware 主机的主机名。

步骤 5 选择具有建议的可用空间量的 datastore，然后点击 **Next**。

步骤 6 （可选）如果 VM 主机或群集支持多个 VMware 虚拟机版本，请选择一个虚拟机版本（例如虚拟机版本 7），然后点击 **Next**。

步骤 7 从 Version 下拉列表中选择 **Linux** 和 **Red Hat Enterprise Linux 6 (64-bit)**。

步骤 8 从 Number of virtual sockets and the Number of cores per virtual socket 下拉列表中选择 **2**。 内核总数应为 4。（可选；显示在 ESX 服务器的某些版本中。 如果您仅看到 Number of virtual processors，请选择 **4**）。

步骤 9 选择内存量，然后点击 **Next**。

步骤 10 从 Adapter 下拉列表中选择 **E1000** NIC 驱动程序，然后点击 **Next**。
系统将显示 SCSI 控制器对话框。

步骤 11 选择 **Paravirtual** 作为 SCSI 控制器，然后点击 **Next**。

步骤 12 选择 **Create a new virtual disk**，然后点击 **Next**。

步骤 13 在 Disk Provisioning 对话框中，点击 **Thick Provision** 单选按钮，然后点击 **Next** 以继续。
Cisco ISE 同时支持详细和精简调配。 但是，我们建议您选择详细调配以获取更好的性能，尤其对于监控节点更加如此。 如果您选择精简调配，则诸如升级、备份和恢复，以及调试日志记录等需要更多磁盘空间的操作在初始磁盘扩展期间可能会受影响。

步骤 14 取消选中 **Support clustering features such as Fault Tolerance** 复选框。

步骤 15 选择高级选项，然后点击 **Next**。

步骤 16 验证配置详细信息，例如新创建的 VMware 系统的 Name、Guest OS、CPUs、Memory 和 Disk Size。 您必须看到以下值：

- Guest OS - Red Hat Enterprise Linux 6 (64-bit)
- CPUs - 4
- Memory - 16 GB 或 16384 MB
- Disk Size - 200 GB 至 2 TB（根据 VMware 磁盘大小建议而定）

为在虚拟机上成功安装 Cisco ISE，请确保遵守本文档中提供的建议。

步骤 17 点击 **Finish**。
系统现已安装 VMware 系统。

接下来的操作

要激活新创建的 VMware 系统，请右键点击 VMware 客户端用户界面的左窗格中的 VM，然后选择 **Power > Power On**。

将 VMware 系统配置为从 Cisco ISE 软件 DVD 启动

配置 VMware 系统后，您即可安装 Cisco ISE 软件。 要从 DVD 安装 Cisco ISE 软件，您需要将 VMware 系统配置为从该 DVD 启动。 这要求 VMware 系统配置有虚拟 DVD 驱动器。

开始之前

您必须下载 Cisco ISE ISO，在 DVD 上烧录 ISO 映像并使用它在虚拟机上安装 Cisco ISE。

步骤 1 在 VMware 客户端中，突出显示新创建的 VMware 系统并选择 **Edit Virtual Machine Settings**。

步骤 2 在 Virtual Machine Properties 对话框中，选择 **CD/DVD Drive 1**。

步骤 3 点击 **Host Device** 单选按钮，然后从下拉列表中选择 DVD 主机设备。

步骤 4 选择 **Connect at Power On** 选项，然后点击 **OK** 保存更改。
您现在可以使用 VMware ESX 服务器的 DVD 驱动器安装 Cisco ISE 软件。

接下来的操作

在您完成此任务后，请点击 VMware 客户端用户界面中的 **Console** 选项卡，右键点击左窗格中的 VM，选择 **Power**，然后选择 **Reset** 重新启动 VMware 系统。

在 VMware 系统上安装 Cisco ISE 软件

开始之前

- 安装后，如果您不安装永久许可证，则 Cisco ISE 会自动安装最多支持 100 个终端的 90 天评估许可证。
- 请从思科软件下载站点 (http://www.cisco.com/en/US/products/ps11640/index.html) 下载 Cisco ISE 软件并将其刻录在 DVD 上。 您将需要提供 Cisco.com 凭证。

步骤 1 登录到 VMware 客户端。

步骤 2 确保在 BIOS 中设置协调世界时 (UTC)：

a) 如果 VMware 系统已开启，请关闭系统。
b) 开启 VMware 系统。
c) 按 **F1** 以进入 BIOS 设置模式。
d) 使用箭头键导航至 Date and Time 字段并按 **Enter** 键。
e) 输入 UTC/格林威治标准时间 (GMT) 时区。
此时区设置可确保来自部署中的各种节点的报告、日志和状态代理日志文件在时间戳方面始终同步。
f) 按 **Esc** 以退出到 BIOS 主菜单。
g) 按 **Esc** 以从 BIOS 设置模式中退出。

步骤 3 将 Cisco ISE 软件 DVD 插入 VMware ESX 主机 CD/DVD 驱动器并开启虚拟机。

当 DVD 启动时，控制台会显示以下内容：

```
  Welcome to the Cisco Identity Services Engine Installer
      Cisco ISE Version: 1.4.0.205


Available boot options:
[1] Cisco ISE Installation (Keyboard/Monitor)
[2] Cisco ISE Installation (Serial Console)
[3] System Utilities (Keyboard/Monitor)
[4] System Utilities (Serial Console)
<Enter> Boot existing OS from hard disk.

Enter boot option and press <Enter>.

boot: 2
Loading vmlinuz......
Loading initrd.img.............................................ready.
Initializing cgroup subsys cpuset
Initializing cgroup subsys cpu
Linux version 2.6.32-431.el6.x86_64 (mockbuild@x86-023.build.eng.bos.redhat.com) (gcc version 4.4.7
 20120313 (Red Hat 4.4.7-4) (GCC) ) #1 SMP Sun Nov 10 22:19:54 EST 2013
```

您可以选择显示器和键盘端口或控制台端口来执行初始设置。

步骤 4 按照系统提示，输入 1 以选择显示器和键盘端口，或者输入 2 以选择控制台端口并按 **Enter** 键。

安装程序在 VMware 系统上启动 Cisco ISE 软件安装。 请预留 20 分钟时间来完成安装过程。 当安装过程完成时，虚拟机会自动重新启动。 当 VM 重新启动时，控制台会显示以下内容：

```
Type 'setup' to configure your appliance
localhost:
```

步骤 5 按照系统提示，键入**setup** 并按 **Enter** 键。

安装向导显示并引导您完成初始配置。

虚拟机上的 Cisco ISE ISO 安装失败

如果在虚拟机上全新安装 Cisco ISE 失败，并且您已选择默认网络驱动程序 (VMXNET3) 作为网络适配器，请检查物理适配器映射。 确保将 Cisco ISE 千兆以太网 0 接口映射到 ESX 中的第 4 个接口 (NIC 4)。 该解决方法是使用 E1000 驱动程序作为网络适配器。

克隆 Cisco ISE 虚拟机

您可以克隆 Cisco ISE VMware 虚拟机 (VM) 来创建与 Cisco ISE 节点完全相同的副本。 例如，在具有多个策略服务节点 (PSN) 的分布式部署中，VM 克隆有助于您快速有效地部署 PSN。 您不必单独安装和配置 PSN。

您也可以使用模板克隆 Cisco ISE VM。

开始之前

- 确保关闭您即将克隆的 Cisco ISE VM。 在 vSphere 客户端中，右键点击即将克隆的 Cisco ISE VM，然后选择 **Power** > **Shut Down Guest**。
- 确保在开启克隆计算机并将其连接到网络之前更改其 IP 地址和主机名。

步骤 1 以具有管理权限的用户（root 用户）身份登录到 ESXi 服务器。

步骤 2 右键点击要克隆的 Cisco ISE，然后点击 **Clone**。

步骤 3 在 Name and Location 对话框中输入正在创建的新计算机的名称，然后点击 **Next**。
这不是正在创建的新 Cisco ISE VM 的主机名，而是供参考的描述性名称。

步骤 4 选择要运行新 Cisco ISE VM 的主机或群集，然后点击 **Next**。

步骤 5 为正在创建的新 Cisco ISE VM 选择 datastore，然后点击 **Next**。
此 datastore 可以是 ESX 或 ESXi 服务器上的本地 datastore，也可以是远程存储。 确保 datastore 具有足够的磁盘空间。

步骤 6 点击 Disk Format 对话框中的 **Same format as source** 单选按钮，然后点击 **Next**。
此选项会复制正在从其克隆新计算机的 Cisco ISE VM 中使用的同一格式。

步骤 7 点击 Guest Customization 对话框中的 **Do not customize** 单选按钮，然后点击 **Next**。

步骤 8 点击 **Finish**。

接下来的操作

- 更改克隆虚拟机的 IP 地址和主机名
- 将克隆的思科虚拟机连接到网络

使用模板克隆 Cisco ISE 虚拟机

如果您使用的是 vCenter，则可以使用 VMware 模板克隆 Cisco ISE 虚拟机 (VM)。 您可以将 Cisco ISE 节点克隆到模板并使用该模板创建多个新的 Cisco ISE 节点。 使用模板克隆虚拟机是一个两个步骤的过程：

步骤 1 创建虚拟机模板， 第 47 页

步骤 2 部署虚拟机模板， 第 47 页

创建虚拟机模板

开始之前

- 确保关闭您即将克隆的 Cisco ISE VM。 在 vSphere 客户端中，右键点击即将克隆的 Cisco ISE VM，然后选择 **Power > Shut Down Guest**。
- 我们建议您从刚安装且未运行设置程序的 Cisco ISE VM 创建模板。 然后，您可以在已创建的每个单独的 Cisco ISE 节点上运行设置程序，并且单独配置 IP 地址和主机名。

步骤 1 以具有管理权限的用户（root 用户）身份登录到 ESXi 服务器。

步骤 2 右键点击要克隆的 Cisco ISE VM，然后选择 **Clone** > **Clone to Template**。

步骤 3 输入模板的名称，在 Name and Location 对话框中选择用于保存模板的位置，然后点击 **Next**。

步骤 4 选择要在其中存储模板 ESX 主机，然后点击 **Next**。

步骤 5 选择要用于存储模板的 datastore，然后点击 **Next**。
确保此 datastore 具有所需的磁盘空间量。

步骤 6 点击 Disk Format 对话框中的 **Same format as source** 单选按钮，然后点击 **Next**。
系统将显示 Ready to Complete 对话框。

步骤 7 点击 **Finish**。

部署虚拟机模板

创建虚拟机模板后，您可以将其部署在其他虚拟机 (VM) 上。

步骤 1 右键点击已创建的 Cisco ISE VM 模板，然后选择 **Deploy Virtual Machine from this template**。

步骤 2 输入新 Cisco ISE 节点的名称，在 Name and Location 对话框中选择该节点的位置，然后点击 **Next**。

步骤 3 选择要在其中存储新 Cisco ISE 节点的 ESX 主机，然后点击 **Next**。

步骤 4 选择要用于新 Cisco ISE 节点的 datastore，然后点击 **Next**。
确保此 datastore 具有所需的磁盘空间量。

步骤 5 点击 Disk Format 对话框中的 **Same format as source** 单选按钮，然后点击 **Next**。

步骤 6 点击 Guest Customization 对话框中的 **Do not customize** 单选按钮。
系统将显示 Ready to Complete 对话框。

步骤 7 选中 **Edit Virtual Hardware** 复选框，然后点击 **Continue**。
系统将显示 Virtual Machine Properties 页面。

步骤 8 选择 **Network adapter**，取消选中 **Connected** 和 **Connect at power on** 复选框，然后点击 **OK**。

步骤 9 点击 **Finish**。

您现在可以打开此 Cisco ISE 节点的电源，配置 IP 地址和主机名，然后将其连接到网络。

接下来的操作

- 更改克隆虚拟机的 IP 地址和主机名
- 将克隆的思科虚拟机连接到网络

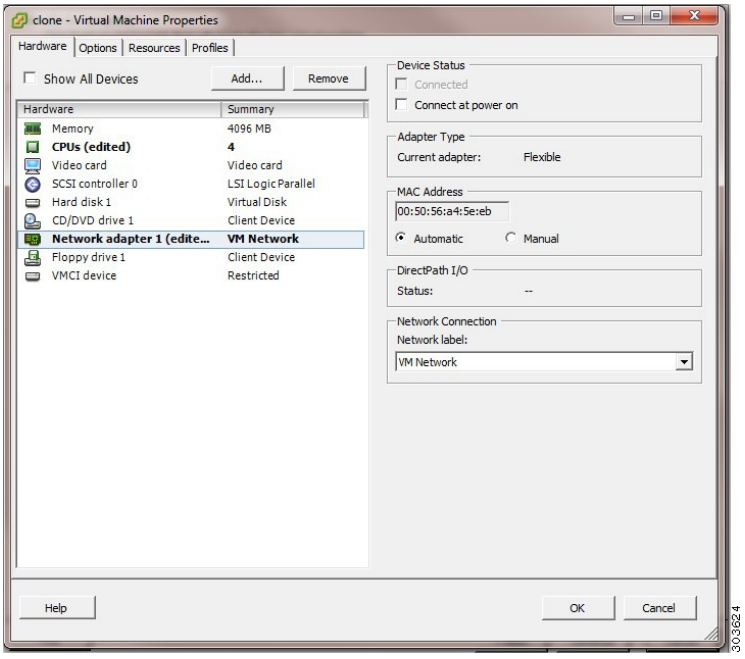
更改克隆虚拟机的 IP 地址和主机名

在您克隆 Cisco ISE 虚拟机 (VM) 后，必须打开其电源并更改 IP 地址和主机名。

开始之前

- 确保 Cisco ISE 节点处于独立状态。
- 确保在打开计算机电源时，最近克隆的 Cisco ISE VM 上的网络适配器未连接。 取消选中 **Connected** 和 **Connect at power on** 复选框。 否则，如果此节点启动，它将与对其进行克隆的源计算机具有相同的 IP 地址。

图 *9*：断开网络适配器连接



- 确保您具有打开计算机电源时就将为最近克隆的 VM 配置的 IP 地址和主机名。 此 IP 地址和主机名条目应包含在 DNS 服务器中。 不能使用“localhost”作为节点的主机名。
- 确保您具有基于新 IP 地址或主机名的 Cisco ISE 节点的证书。

操作步骤

步骤 1 右键单击最近克隆的 Cisco ISE VM，然后选择 **Power** > **Power On**。

步骤 2 选择最近克隆的 Cisco ISE VM，然后点击 **Console** 选项卡。

步骤 3 在 Cisco ISE CLI 上输入以下命令：

```
configure terminal
hostname hostname
```

主机名是您将要配置的新主机名。 系统会重新启动 Cisco ISE 服务。

步骤 4 输入以下命令：

```
interface gigabit 0
ip address ip_address netmask
```

ip_address 是对应于您在步骤 3 中输入的主机名的地址，netmask 是 ip_address 的子网掩码。 系统将提示您重新启动 Cisco ISE 服务。 有关 ip address 和 hostname 命令，请参阅《思科身份服务引擎 *CLI* 参考指南》。

步骤 5 输入 **Y** 重新启动 Cisco ISE 服务。

将克隆的思科虚拟机连接到网络

在您打开电源并更改 IP 地址和主机名后，必须将 Cisco ISE 节点连接到网络。

步骤 1 右键点击最近克隆的 Cisco ISE 虚拟机 (VM)，然后点击 **Edit Settings**。

步骤 2 点击 Virtual Machine Properties 对话框中的 **Network adapter**。

步骤 3 在 Device Status 区域中，选中 **Connected** 和 **Connect at power on** 复选框。

步骤 4 点击 **OK**。

将 Cisco ISE VM 从评估迁移至生产

评估 Cisco ISE 版本后，您可以从评估系统迁移至完全许可的生产系统。

开始之前

- 将 VMware 服务器移至支持更多用户数的生产环境时，请务必将 Cisco ISE 安装重新配置为建议的最小磁盘大小或更高容量（最多达到允许的最大值，即 2 TB）。

- 请注意，您不能将数据从所创建的磁盘空间小于 200 GB 的 VM 迁移至生产 VM。 您只能将数据从所创建的具有 200 GB 或更多磁盘空间的 VM 迁移至生产环境。

步骤 1 备份评估版本的配置。

步骤 2 确保您的生产 VM 具有所需的磁盘空间量。

步骤 3 安装生产部署许可证。

步骤 4 将配置恢复到生产系统。

第 5 章

在 Cisco ISE 3300 系列、Cisco NAC 和 Cisco Secure ACS 设备上安装 Cisco ISE 软件

受支持的 Cisco ISE、Secure ACS 和 NAC 设备

如果已重新映像以下某些思科设备，则您可以在这些设备上从 DVD 安装 Cisco ISE 软件。 设备类型包括：

- Cisco ISE-3315
- Cisco ISE-3355
- Cisco ISE-3395
- Cisco Secure ACS-1121
- Cisco NAC-3315
- Cisco NAC-3355
- Cisco NAC-3395

在 Cisco Secure ACS 或 Cisco NAC 设备上安装软件是简化过程，因为将在其上安装 Cisco ISE 软件的基础硬件是同一物理设备类型。

要重复使用 Cisco Secure ACS 或 Cisco NAC 设备作为 Cisco ISE 设备，请重新映像设备，然后安装 ISE 软件。

有关 Cisco ISE 3300 系列硬件平台的特定详细信息，请参阅《思科身份服务引擎硬件安装指南，版本 *1.2*》。

从 DVD 安装 Cisco ISE 软件

开始之前

- 下载 Cisco ISE 版本或 Inline Posture 节点 ISO 映像，在 DVD 上刻录 ISO 映像并使用它在 Cisco ISE-3300 系列以及传统的 Cisco NAC 和 Cisco Secure ACS 设备上安装软件。
- 在运行设置程序之前，请检查 Cisco ISE 安装参数并准备好此信息。

步骤 1 将键盘和 VGA 显示器连接到设备。

步骤 2 确保将电源线连接到设备，在设备 CD/DVD 驱动器中插入 DVD 并开启设备。
控制台会显示启动选项。

步骤 3 按照启动提示，输入 **1** 并按 **Enter** 键。

步骤 4 按照提示，键入**setup** 以启动设置程序。

步骤 5 输入设置程序参数的值。
配置 Cisco ISE 或 IPN 软件后，系统自动重新启动。 要重新登录到 CLI，您必须输入设置过程中配置的 CLI 管理员用户凭证。

接下来的操作

- 如果您已安装 IPN ISO，则必须为 Inline Posture 节点配置证书。
- 如果已安装 Cisco ISE ISO 映像，则登录到 Cisco ISE CLI 外壳后，您可以运行**show application status ise** CLI 命令检查 Cisco ISE 应用进程的状态。

在重新映像的 Cisco ISE-3300 系列设备上安装 Cisco ISE 软件

开始之前

- 下载 Cisco ISE 或 Inline Posture 节点 ISO 映像，在 DVD 上刻录 ISO 映像并使用它在思科设备上安装软件。
- 查看配置 Cisco SNS-3400 设备的必备条件。
- 在运行设置程序之前，请检查 Cisco ISE 设置程序参数并准备好此信息。

- 查看 DVD 安装说明。

步骤 1 如果 Cisco ISE 设备开启，请将其关闭。

步骤 2 开启 Cisco ISE 设备。

步骤 3 按 **F1** 以进入 BIOS 设置模式。

步骤 4 使用箭头键导航至 Date and Time 字段并按 **Enter** 键。

步骤 5 将时间设置为 UTC/GMT 时区。

注释 我们建议您将所有 Cisco ISE 节点都设置为 UTC 时区。 此时区设置可确保来自部署中的各种节点的报告和日志在时间戳方面始终同步。

步骤 6 按 **Esc** 以退出到 BIOS 主菜单。

步骤 7 按 **Esc** 以从 BIOS 设置模式中退出。

步骤 8 从 DVD 安装软件。

接下来的操作

登录到 Cisco ISE 管理门户并安装许可证。

在重新映像的 Cisco Secure ACS 设备上安装 Cisco ISE 软件

开始之前

- 下载 Cisco ISE 或 Inline Posture 节点 ISO 映像，在 DVD 上刻录 ISO 映像并使用它在传统 Cisco Secure ACS 设备上安装 Cisco ISE 或 IPN 软件。
- 查看配置思科设备的必备条件。
- 在运行设置程序之前，请检查 Cisco ISE 设置程序参数并准备好此信息。
- 查看 DVD 安装说明。

步骤 1 如果 Cisco Secure ACS 设备开启，请将其关闭。

步骤 2 开启 Cisco Secure ACS 设备。

步骤 3 按 **F1** 以进入 BIOS 设置模式。

步骤 4 使用箭头键导航至 Date and Time 字段并按 **Enter** 键。

步骤 5 将设备的时间设置为 UTC/GMT 时区。

注释 我们建议您将所有 Cisco ISE 节点都设置为 UTC 时区。 此时区设置可确保来自部署中的各种节点的报告和日志在时间戳方面始终同步。

步骤 6 按 **Esc** 以退出到 BIOS 主菜单。

步骤 7 按 **Esc** 以从 BIOS 设置模式中退出。

步骤 8 从 DVD 安装软件。

接下来的操作

登录到 Cisco ISE 管理门户并安装许可证。

在重新映像的 Cisco NAC 设备上安装 Cisco ISE 软件

开始之前

- 下载 Cisco ISE 软件或 Inline Posture 节点 ISO 映像，在 DVD 上刻录 ISO 映像并使用它在传统 Cisco NAC 设备上安装软件。
- 查看配置思科设备的必备条件。
- 在运行设置程序之前，请检查 Cisco ISE 设置程序参数并准备好此信息。
- 查看 DVD 安装说明。

步骤 1 如果 Cisco NAC 设备开启，请将其关闭。

步骤 2 开启 Cisco NAC 设备。

步骤 3 按 **F1** 以进入 BIOS 设置模式。

步骤 4 使用箭头键导航至 Date and Time 字段并按 **Enter** 键。

步骤 5 将设备的时间设置为 UTC/GMT 时区。

注释 我们建议您将所有 Cisco ISE 节点都设置为 UTC 时区。 此时区设置可确保来自部署中的各种节点的报告和日志在时间戳方面始终同步。

步骤 6 按 **Esc** 以退出到 BIOS 主菜单。

步骤 7 按 **Esc** 以从 BIOS 设置模式中退出。

步骤 8 从 DVD 安装软件。

接下来的操作

如果 Cisco ISE DVD 安装过程返回一条消息，指示“The installer requires at least 600GB disk space for this appliance type”，则您可能需要重置设备上的 RAID 设置以方便安装。

登录到 Cisco ISE 管理门户并安装许可证。

在 Cisco NAC 设备上重置现有 RAID 配置

可能有必要在 NAC 设备上重置 RAID 设置，以方便 Cisco ISE 软件安装。

步骤 1 使用 Cisco ISE 软件 DVD 重新启动 Cisco NAC 设备。

步骤 2 当 CLI 中显示 RAID 控制器版本信息时，请按**Ctrl-C**。 RAID 控制器版本信息出现，其中显示诸如 `LSI Corporation MPT SAS BIOS` 的标签，并且 LSI Corp Config Utility 会变为活动状态。

步骤 3 按**Enter 键** 以指定默认控制器。（突出显示的控制器名称显示类似于 `SR-BR10i` 的内容。） 系统将显示包含 Cisco NAC 设备适配器信息的屏幕。

步骤 4 使用箭头键导航至“RAID properties”，然后按**Enter 键**。

步骤 5 使用箭头键导航至“Manage Array”，然后按**Enter 键**。

步骤 6 使用箭头键导航至“Delete Array”，然后按**Enter 键**。

步骤 7 输入 Y 以确认要删除现有 RAID 阵列。

步骤 8 按**Esc 键** 两次以退出 RAID 配置实用程序。
系统会通过 `Exit the Configuration Utility and Reboot?` 对您进行提示。

步骤 9 按**Enter 键**。 Cisco NAC 设备重新启动。 只要仍然插入 Cisco ISE 软件 DVD，设备就会自动启动到安装菜单。

步骤 10 按**1** 以开始安装 Cisco ISE。

第 6 章

管理管理员帐户

CLI 管理员和基于 Web 的管理员用户权限差异

使用 Cisco ISE 设置程序时设置的用户名和密码旨在用于对 Cisco ISE CLI 和 Cisco ISE Web 界面进行管理访问。 具有 Cisco ISE CLI 访问权限的管理员称为 CLI 管理员用户。 默认情况下，CLI 管理员用户的用户名为 admin，密码是设置过程中用户定义的密码。 没有默认密码。

您最初可以使用设置过程中定义的 CLI 管理员用户的用户名和密码来访问 Cisco ISE Web 界面。 基于 Web 的管理员没有默认用户名和密码。

CLI 管理员用户会被复制到 Cisco ISE 基于 Web 的管理员用户数据库。 只有第一个 CLI 管理员用户会复制作为基于 Web 的管理员用户。 您应将 CLI 管理员用户库与基于 Web 的管理员用户库保持同步，以便可以对两种管理员角色使用同一用户名和密码。

Cisco ISE CLI 管理员用户具有与 Cisco ISE 基于 Web 的管理员用户不同的权限和功能，并且可以执行其他管理任务。

表 *14*: *CLI* 管理员和基于 *Web* 的管理员用户执行的任务

管理员用户类型	任务
CLI 管理员和基于 Web 的管理员	• 备份 Cisco ISE 应用数据。 • 显示 Cisco ISE 设备上的所有系统、应用或诊断日志。 • 应用 Cisco ISE 软件补丁、维护版本和升级。 • 设置 NTP 服务器配置。

管理员用户类型	任务
仅限 CLI 管理员	• 启动和停止 Cisco ISE 应用软件。 • 重新加载或关闭 Cisco ISE 设备。 • 在锁定的情况下重置基于 Web 的管理员用户。 • 访问 ISE CLI。

CLI 管理员用户创建

通过 Cisco ISE，您可以创建除安装过程期间创建的 CLI 管理员用户帐户以外的其他 CLI 管理员用户帐户。 要保护 CLI 管理员用户凭证，请创建访问 Cisco ISE CLI 所需的最小数量的 CLI 管理员用户。

您可以通过在 CLI 中进入配置模式并使用 **username** 命令来添加 CLI 管理员用户。

基于 Web 的管理员用户创建

首次对 Cisco ISE 系统进行基于 Web 的访问时，管理员用户名和密码与设置过程中配置的基于 CLI 的访问相同。

您可以通过用户界面本身添加基于 Web 的管理员用户。

第 7 章

安装后任务

登录到 Cisco ISE 基于 Web 的界面

首次登录到 Cisco ISE 基于 Web 的界面时，您将使用预安装的评估许可证。

注释 我们建议您使用 Cisco ISE 用户界面定期重置管理员登录密码。

注意 出于安全原因，我们建议您在完成管理会话时注销。 如果您不注销， 则 Cisco ISE 基于 Web 的界面会在处于非活动状态 30 分钟后将您注销，并且不保存任何未提交的配置数据。

开始之前

Cisco ISE 管理员门户支持以下已启用 HTTPS 的浏览器：

- Mozilla Firefox 版本 31.*x* ESR、36.*x* 和 37.*x*
- Microsoft Internet Explorer 10.*x* 和 11.*x*

注释 Adobe Flash Player 11.1.0.0 或更高版本必须安装在运行客户端浏览器的系统上。 查看 Cisco ISE GUI 所需的最低屏幕分辨率为 1280 x 800 像素。

步骤 1 在 Cisco ISE 设备重新启动完成后，启动其中一种受支持的 Web 浏览器。

步骤 2 在 Address 字段中，通过使用以下格式输入 Cisco ISE 设备的 IP 地址（或主机名），然后按 **Enter** 键。

```
https://<IP address or host name>/admin/
```

步骤 3 输入设置过程中定义的用户名和密码。

步骤 4 点击 **Login**。

Cisco ISE 配置验证

共有两种验证方法，它们分别通过 Web 浏览器和 CLI 使用一组不同的用户名和密码凭证来验证 Cisco ISE 配置。

注释 CLI 管理员用户和基于 Web 的管理员用户的凭证在 Cisco ISE 中不同。

使用 Web 浏览器验证配置

步骤 1 在 Cisco ISE 设备重新启动完成后，启动其中一种受支持的 Web 浏览器。

步骤 2 在 **Address** 字段中，使用以下格式输入 Cisco ISE 设备的 IP 地址（或主机名），然后按 **Enter** 键。

步骤 3 在 Cisco ISE Login 页面中，输入已在设置过程中定义的用户名和密码，然后点击 **Login**。
例如，输入 https://10.10.10.10/admin/ 会显示 Cisco ISE Login 页面。

```
https://<IP address or host name>/admin/
```

注释 首次对 Cisco ISE 系统进行基于 Web 的访问时，管理员用户名和密码与设置过程中配置的基于 CLI 的访问相同。

步骤 4 使用 Cisco ISE 控制面板验证设备是否正常工作。

接下来的操作

通过使用 Cisco ISE 基于 Web 的用户界面菜单和选项，您可以配置 Cisco ISE 系统以满足您的要求。有关配置 Cisco ISE 的详细信息，请参阅《思科身份服务引擎管理员指南》。

使用 CLI 验证配置

开始之前

要获取最新的 Cisco ISE 补丁并保持 Cisco ISE 为最新版本，请访问以下网站：http://www.cisco.com/public/sw-center/index.shtml

步骤 1 在 Cisco ISE 设备重新启动完成后，启动受支持的产品（例如 PuTTY），以建立到 Cisco ISE 设备的安全外壳 (SSH) 连接。

步骤 2 在 Host Name（或 IP Address）字段中，输入主机名（或 Cisco ISE 设备的点分十进制格式的 IP 地址），然后点击 **Open**。

步骤 3 在出现登录提示时，输入设置过程中配置的 CLI 管理员用户名（默认值为 admin），然后按 **Enter** 键。

步骤 4 在出现密码提示时，输入设置过程中配置的 CLI 管理员密码（此密码是用户定义的，没有默认值），然后按 **Enter** 键。

步骤 5 出现系统提示时，输入**show application version ise** 并按 **Enter** 键。

注释 Version 字段列出当前安装的 Cisco ISE 软件版本。

控制台输出显示如下：

```
ise-vm123/admin# show application version ise

Cisco Identity Services Engine
------------------------------------------
Version      : 1.4.0.205
Build Date   : Tue Mar  3 19:31:27 2015
Install Date : Tue Mar  3 21:06:31 2015
```

步骤 6 要检查 Cisco ISE 进程的状态，请输入**show application status ise** 并按 **Enter** 键。

控制台输出显示如下：

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

ISE PROCESS NAME                       STATE            PROCESS ID
--------------------------------------------------------------------
Database Listener                      running          3638
Database Server                        running          45 PROCESSES
Application Server                     running          5992
Profiler Database                      running          4483
AD Connector                           running          6401
M&T Session Database                   running          2313
M&T Log Collector                      running          6247
M&T Log Processor                      running          6274
Certificate Authority Service          running          6213
```

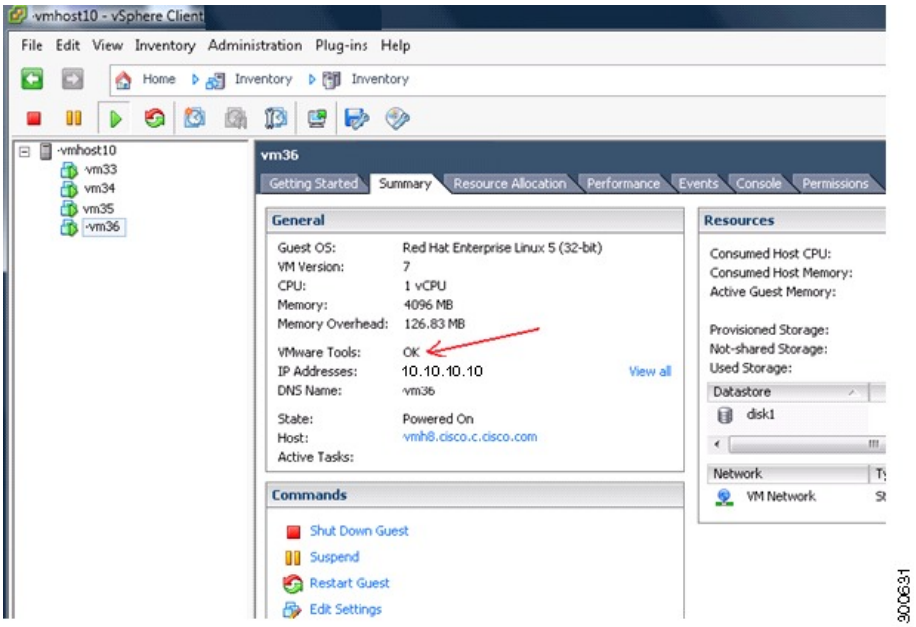
```
pxGrid Infrastructure Service          disabled
pxGrid Publisher Subscriber Service    disabled
pxGrid Connection Manager              disabled
pxGrid Controller                      disabled
Identity Mapping Service               disabled
```

VMware 工具安装验证

使用 vSphere 客户端中的 Summary 选项卡验证 VMWare 工具安装

转至 vShpere 客户端中指定的 VMware 主机的 Summary 选项卡。 VMware Tools 字段中的值应该适用。

图 *10*: 在 *vSphere* 客户端中验证 *VMware* 工具



使用 CLI 验证 VMWare 工具安装

您还可以验证 VMware 工具是否是使用**show inventory** 命令安装。 此命令列出 NIC 驱动程序信息。在安装了 VMware 工具的虚拟机上，VMware 虚拟以太网驱动程序将列于 Driver Descr 字段中。

```
vm36/admin# show inventory
NAME: "ISE-VM-K9 chassis", DESCR: "ISE-VM-K9 chassis"
PID: ISE-VM-K9, VID: V01 , SN: 8JDCBLIDLJA
```

```
Total RAM Memory: 4016564 kB
CPU Core Count: 1
CPU 0: Model Info: Intel(R) Xeon(R) CPU E5504 @ 2.00GHz
Hard Disk Count(*): 1
Disk 0: Device Name: /dev/sda
Disk 0: Capacity: 64.40 GB
Disk 0: Geometry: 255 heads 63 sectors/track 7832 cylinders
NIC Count: 1
NIC 0: Device Name: eth0
NIC 0: HW Address: 00:0C:29:BA:C7:82
NIC 0: Driver Descr: VMware Virtual Ethernet driver
(*) Hard Disk Count may be Logical.
vm36/admin#
```

对升级 VMware 工具的支持

Cisco ISE ISO 映像（常规、升级或补丁）包含受支持的 VMware 工具。 Cisco ISE 不支持通过 VMware 客户端用户界面升级 VMware 工具 。 如果要将任何 VMware 工具升级到更高版本，则需要通过更新版本的 Cisco ISE（常规、升级或补丁版本）提供支持。

管理员密码重置

使用 DVD 重置已丢失、已忘记或已泄漏的密码

开始之前

确保您了解在尝试使用 Cisco ISE 软件 DVD 启动 Cisco ISE 设备时可能导致问题的以下连接相关情况：

- 您的终端服务器与设置为 exec 的 Cisco ISE 设备的串行控制台连接相关联。 通过将其设置为 no exec，您可以使用 KVM 连接和串行控制台连接。
- 您具有到 Cisco ISE 设备的键盘和视频显示器 (KVM) 连接（它可以是远程 KVM 或 VMware vSphere 客户端控制台连接）。
- 您具有到 Cisco ISE 设备的串行控制台连接。

步骤 1 确保 Cisco ISE 设备已接通电源。

步骤 2 插入 Cisco ISE 软件 DVD。

例如，Cisco ISE 3415 控制台会显示以下消息：

```
Welcome to the Cisco Identity Services Engine Installer
     Cisco ISE Version: 1.4.0.205

Available boot options:

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

```
  [4] System Utilities (Serial Console)
  <Enter> Boot existing OS from hard disk.

Enter boot option and press <Enter>.
```

步骤 3 按照系统提示，如果您使用到设备的键盘和视频显示器连接，请输入3；如果使用本地串行控制台端口连接，请输入 4。
系统会显示 ISO 实用程序菜单，如下所示。

```
     Cisco ISE System Utilities Menu

Available System Utilities:

  [1] Recover administrator password
  [2] Virtual Machine Resource Check
  [3] System Erase
  [4] Install Media Check
  [q] Exit and reload

Enter option and press <Enter>
```

步骤 4 输入 1 以恢复管理员密码。
控制台会显示：

```
Admin username:
[1]:admin
[2]:admin2
[3]:admin3
[4]:admin4
Enter number of admin for password recovery:2
Password:
Verify password:
Save change and reboot? [Y/N]:
```

步骤 5 输入对应于要重置其密码的管理员用户的数字。

步骤 6 输入新密码并进行验证。

步骤 7 输入 Y 以保存更改。

由于管理员锁定重置密码

管理员输入不正确的密码达到足够次数便会禁用帐户。 最少和默认尝试次数为 5。

使用这些说明在 Cisco ISE CLI 中通过**application reset-passwd ise** 命令重置管理员用户界面密码。它不会影响管理员的 CLI 密码。 在您成功重置管理员密码后，凭证立即生效，并且您可以登录，而不必重新启动系统。 。

Cisco ISE 会在 **Monitor** > **Reports** > **Catalog** > **Server Instance** > **Server Instance** > **Server Administrator Logins** 报告中添加日志条目，并会将该管理员 ID 的凭证暂挂，直至重置与该管理员 ID 关联的密码。

步骤 1 访问直接控制台 CLI 并输入：
application reset-passwd iseadministrator_ID

步骤 2 指定并确认与用于此管理员 ID 的之前两个密码不同的新密码：

```
Enter new password:
Confirm new password:

Password reset successfully
```

更改 Cisco ISE 设备的 IP 地址

开始之前

- 在更改 IP 地址之前，请确保 Cisco ISE 节点处于独立状态。 如果该节点是分布式部署的一部分，请从部署中撤销注册该节点并使其成为独立节点。
- 更改 Cisco ISE 设备 IP 地址时，请勿使用**no ip address**命令。

步骤 1 登录到 Cisco ISE CLI。

步骤 2 输入以下命令：

a) **configure terminal**
b) **interface GigabitEthernet 0**
c) **ip address new_ip_address new_subnet_mask**
系统会提示您更改 IP 地址。 输入**Y**。 系统将显示类似于以下的屏幕。

```
ise-13-infra-2/admin(config-GigabitEthernet)# ip address a.b.c.d 255.255.255.0

% Changing the IP address might cause ISE services to restart
Continue with IP address change? Y/N [N]: y
Stopping ISE Monitoring & Troubleshooting Log Collector...
Stopping ISE Monitoring & Troubleshooting Log Processor...
Stopping ISE Identity Mapping Service...
Stopping ISE pxGrid processes...
Stopping ISE Application Server...
Stopping ISE Certificate Authority Service...
Stopping ISE Profiler Database...
Stopping ISE Monitoring & Troubleshooting Session Database...
Stopping ISE AD Connector...
```

```
Stopping ISE Database processes...
Starting ISE Monitoring & Troubleshooting Session Database...
Starting ISE Profiler Database...
Starting ISE pxGrid processes...
Starting ISE Application Server...
Starting ISE Certificate Authority Service...
Starting ISE Monitoring & Troubleshooting Log Processor...
Starting ISE Monitoring & Troubleshooting Log Collector...
Starting ISE Identity Mapping Service...
Starting ISE AD Connector...
Note: ISE Processes are initializing. Use 'show application status ise'
CLI to verify all processes are in running state.
```

Cisco ISE 提示您重新启动系统。

步骤 3 输入**Y** 重新启动系统。

查看安装和升级历史记录

Cisco ISE 提供一个命令行界面 (CLI) 命令来查看 Cisco ISE 版本和补丁的安装、升级和卸载详细信息。 **show version history** 命令提供以下详细信息：

- Date - 执行安装或卸载的日期和时间
- Application - Cisco ISE 应用
- Version - 已安装或删除的版本
- Action - 安装、卸载、补丁安装或补丁卸载
- Bundle Filename - 已安装或删除的捆绑包的名称
- Repository - 从其安装 Cisco ISE 应用捆绑包的存储库。 不适用于卸载。

步骤 1 登录到 Cisco ISE CLI。

步骤 2 输入以下命令：**show version history**。

系统将显示以下输出：

```
Positron/admin# Show version history
--------------------------------------------
Install Date: Tue Mar 03 20:25:58 UTC 2015
Application: ise
Version: 1.4.0.205
Install type: Application Install
Bundle filename: ise.tar.gz
Repository: SystemDefaultPkgRepos
```

在 SNS-3415 设备上配置 RAID

在 SNS-3415 设备上，您必须在安装 Cisco ISE 之前手动配置独立磁盘冗余阵列 (RAID)。

步骤 1 按 Ctrl + Alt + Del 可重新启动设备。

步骤 2 按 Ctrl+M 可进入 **LSI Software RAID Configuration** 菜单。

步骤 3 从 **Management** 菜单中，选择 **Configure**。

步骤 4 选择 **Clear Configuration** 并确认选择。

步骤 5 选择 **Easy Configuration**。
系统将显示具有 READY 标签的方框。

步骤 6 按空格键选择该卷。
标签更改为 ONLIN A00-xx。

步骤 7 按 F10 配置该卷，然后按空格键选择阵列。

步骤 8 按 F10 配置该阵列。
系统将显示一个方框，其中会指定卷数据，包括大小 (557.8 GB) 和 RAID 0。

步骤 9 使用箭头键导航至 **Accept**，然后按 **Enter** 键。

步骤 10 按 Esc 键并保存配置。

步骤 11 按两下 Esc 键以退出所有菜单。
系统将提示您重新启动设备。

步骤 12 重新启动设备。

步骤 13 在您安装 Cisco ISE 并重新启动设备后，按 F6 以进入 **Boot Order** 菜单。

步骤 14 选择 **Embedded SCU RAID** 以从硬盘启动。

使用 CIMC 在 SNS-3495 设备上配置 RAID

在安装 Cisco ISE 之前，您必须使用 CIMC 配置独立磁盘冗余阵列 (RAID)。

开始之前

您必须在配置 CIMC 后才能在 SNS-3495 设备上配置 RAID。 有关详情，请参阅 配置思科集成管理控制器，第 21 页

步骤 1 在 CIMC 用户界面中，选择 **Server** > **BIOS** > **Configure BIOS Parameter**。

步骤 2 点击 **Advanced** 选项卡。 在 **Onboard Storage** 区域中，将 **Onboard SCU Storage Support** 选项设置为 **Enabled**。

步骤 3 点击 **Save Changes**。 系统将显示以下消息：

```
Reboot Host Immediately option is not selected. BIOS settings will be applied only on next host reboot. Continue?
```

步骤 4 点击 **Yes**。

步骤 5 选择 **Server** > **Summary** > **Power Cycle Server**。

步骤 6 点击 **OK**。

步骤 7 选择 **Server** > **Summary** > **Launch KVM Console**。
系统将显示基于内核的虚拟机 (KVM) 的控制台屏幕。

步骤 8 选择 **Server** > **Summary** > **Power Cycle Server**。

步骤 9 在启动过程中，按 Ctrl+H 访问 WebBIOS。

步骤 10 在 KVM WebBIOS 中，点击 **Start**。

步骤 11 在 **BIOS Config Utility Physical Configuration** 窗格中，点击 **Configuration Wizard**。

步骤 12 点击 **Add Configuration**，然后点击 **Next**。

步骤 13 点击 **Automatic Configuration**。

步骤 14 在 **Redundancy** 下拉列表中，选择 **Redundancy When Possible** 选项，然后点击 **Next**。

步骤 15 点击 **Yes** 以保存配置。

步骤 16 点击 **Yes** 以初始化新的虚拟驱动器。

步骤 17 点击 **Set Boot Drive**，然后点击 **Go**。

步骤 18 点击 **Home**。

步骤 19 点击 **Exit**。

步骤 20 点击 **Yes**。

步骤 21 重新启动服务器。

步骤 22 选择 **Inventory** > **Storage** > **Virtual Drive Info**。 确保在 Virtual Drive info 选项卡中列出新添加的虚拟驱动器。

执行系统清除

您可以执行系统清除以安全地清除 Cisco ISE 设备或 VM 中的所有信息。 这个用于执行系统清除的选项可确保 Cisco ISE 符合 NIST 特别出版物 800-88 数据销毁标准。

开始之前

确保您了解在尝试使用 Cisco ISE 软件 DVD 启动 Cisco ISE 设备时可能导致问题的以下连接相关情况：

- 您的终端服务器与设置为 exec 的 Cisco ISE 设备的串行控制台连接相关联。 通过将其设置为 no exec，您可以使用 KVM 连接和串行控制台连接。
- 您具有到 Cisco ISE 设备的键盘和视频显示器 (KVM) 连接（它可以是远程 KVM 或 VMware vSphere 客户端控制台连接）。
- 您具有到 Cisco ISE 设备的串行控制台连接。

步骤 1 确保 Cisco ISE 设备已接通电源。

步骤 2 插入 Cisco ISE 软件 DVD。

例如，Cisco ISE 3415 控制台会显示以下消息：

```
Welcome to the Cisco Identity Services Engine Installer
     Cisco ISE Version: 1.4.0.205

Available boot options:

  [1] Cisco ISE Installation (Keyboard/Monitor)
  [2] Cisco ISE Installation (Serial Console)
  [3] System Utilities (Keyboard/Monitor)
  [4] System Utilities (Serial Console)
  <Enter> Boot existing OS from hard disk.

Enter boot option and press <Enter>.
```

步骤 3 按照系统提示，如果您使用到设备的键盘和视频显示器连接，请输入3；如果使用本地串行控制台端口连接，请输入 4。

系统会显示 ISO 实用程序菜单，如下所示。

```
     Cisco ISE System Utilities Menu

Available System Utilities:

  [1] Recover administrator password
  [2] Virtual Machine Resource Check
  [3] System Erase
  [4] Install Media Check
  [q] Exit and reload

Enter option and press <Enter>
```

步骤 4 输入 3 以执行系统清除。

控制台会显示：

```
                  **********   W A R N I N G   **********
YOU ARE ABOUT TO PERFORM A SYSTEM ERASE. THIS ACTION WILL DELETE ALL
CONTENT OF THE HARD DISK BY WRITING A SEQUENCE OF RANDOM BYTES, FOLLOWED
BY ZEROS DIRECTLY TO THE HARD DISK DEVICE.
```

```
ARE YOU SURE YOU WANT TO PROCEED? [Y/N] Y
```

步骤 5 输入 Y。

控制台会显示另一个警告对您进行提示：

```
THIS IS YOUR LAST CHANGE TO ABORT. PROCEED WITH SYSTEM ERASE? [Y/N] Y
```

步骤 6 输入 Y 以执行系统清除。

控制台会显示：

```
Deleting system disk, please wait…
Writing random data to all sectors of disk device (/dev/sda)…
Writing zeros to all sectors of disk device (/dev/sda)…
Completed!  System is now erased.
Press <Enter> to reboot.
```

执行系统清除后，如果您要重复使用设备，则必须使用 Cisco ISE DVD 启动系统并从启动菜单中选择安装选项。

附 录 A

Cisco SNS-3400 系列服务器规格

物理规格

表 *15*: *Cisco SNS-3400* 系列服务器物理规格

描述	规格
高度	1.7 英寸（4.3 厘米）
宽度	16.9 英寸（42.9 厘米）
深度	28.5 英寸（72.4 厘米）
重量（满载机箱）	35.6 磅（16.1 千克）

环境规格

表 *16*: *Cisco SNS-3400* 系列服务器环境规格

描述	规格
工作温度	41 至 104°F（5 至 40°C）；海拔高度每上升 305 米，最高温度降低 1°C。

描述	规格
非工作温度	-40 至 149°F（-40 至 65°C）
湿度（相对），非冷凝	10% 至 90%
工作高度	-0 至 10,000 英尺
非工作高度	-0 至 40,000 英尺
声功率级 根据 ISO7779 标准测量 A 计权声功率级（贝尔） 在 73°F (23°C) 下工作	5.4
声压级 根据 ISO7779 标准测量 A 计权声压级 (dBA) 在 73°F (23°C) 下工作	37

电源规格

450 瓦特电源

注释 通过使用 Cisco UCS Power Calculator，您可以获取有关确切服务器配置的更多具体电源信息。

注释 请勿混淆服务器中的电源类型。 两个电源均必须为 450W。

表 *17*: *Cisco SNS-3400* 系列服务器 *450* 瓦特电源规格

描述	规格
交流输入电压范围	范围下限：100VAC 至 120VAC 范围上限：200VAC 至 240VAC
交流输入频率	范围：47 至 63Hz（单相，标称 50 至 60Hz）
交流线路输入电流（稳定状态）	100VAC 时的峰值电流为 6.0A 208VAC 时的峰值电流为 3.0A
每个电源的最大输出功率	450W

描述	规格
电源输出电压	主电源：12VDC 备用电源：12VDC

650 瓦特电源

注释 通过使用 Cisco UCS Power Calculator，您可以获取有关确切服务器配置的更多具体电源信息。

注释 请勿混淆服务器中的电源类型。 两个电源必须是 650W。

表 *18*：*Cisco SNS-3400* 系列服务器 *650* 瓦特电源规格

描述	规格
交流输入电压范围	90 至 264VAC（自行设置范围，标称 180 至 264VAC）
交流输入频率	范围：47 至 63Hz（单相，标称 50 至 60Hz）
交流线路输入电流（稳定状态）	100VAC 时的峰值电流为 7.6A 208VAC 时的峰值电流为 3.65A
每个电源的最大输出功率	650W
电源输出电压	主电源：12VDC 备用电源：12VDC

附 录 B

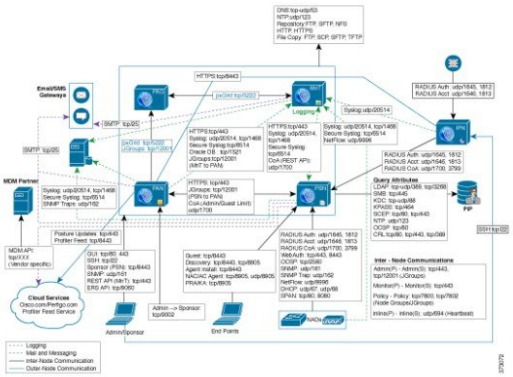
Cisco SNS-3400 系列设备端口参考

Cisco ISE 基础设施

本附录列出 Cisco ISE 用于与外部应用和设备进行网络内通信的 TCP 和用户数据报协议 UDP 端口。此附录中列出的 Cisco ISE 端口在对应的防火墙上必须处于打开状态。

在 Cisco ISE 网络上配置服务时，请记住以下信息：

- Cisco ISE 管理只限于千兆以太网 0。
- RADIUS 在所有网络接口卡 (NIC) 上进行侦听。
- 所有 NIC 都可以配置有 IP 地址。


DNS tcp-udp/53
NTP udp/123
Repository FTP, SFTP, NFS
HTTP, HTTPS
File Copy FTP, SCP, SFTP, TFTP
HTTPS tcp/8443
pxGrid tcp/5222
Logging
Syslog udp/20514
RADIUS Auth udp/1645, 1812
RADIUS Acct udp/1646, 1813
Email/SMS Gateways
SMTP tcp/25
MDM Partner
Syslog: udp/20514, tcp/1468
Secure Syslog: tcp/6514
SNMP Traps: udp/162
Posture Updates tcp/443
Profiler Feed: tcp/8443
MDM API: tcp/XXX (Vendor specific)
GUI: tcp/80, 443
SSH tcp/22
Sponsor (TCN): tcp/8443
SNMP: udp/161
REST API (ldeTr): tcp/443
ERS API: tcp/9060
Cloud Services
Cisco.com/Feedgo.com
Profiler Feed Service
Admin/Sponsor
Admin --> Sponsor: tcp/8002
End Points
HTTPS:tcp/443
Syslog: udp/20514, tcp/1468
Secure Syslog: tcp/6514
Oracle DB : tcp/1521
JGroups:tcp/12001
(MnT to PAN)
CoA (REST API): udp/1700
(JGroups: tcp/12001
(PSN to PAN)
CoA (Admin/Guest Limit): udp/1700
Quest: tcp/8443
Discovery: tcp/8443, tcp/8905
Agent Install: tcp/8443
NACIAC Agent: tcp/8905, udp/8905
PSN/PA: tcp/8905
RADIUS Auth: udp/1645, 1812
RADIUS Acct: udp/1646, 1813
RADIUS CoA: udp/1700, 3799
Web Auth: tcp/443, 8443
OCSP: tcp/2560
SNMP: udp/161
SNMP Trap: udp/162
NetFlow: udp/9996
DHCP: udp/67, udp/68
DHCP: udp/67, udp/68
(IPAM: tcp/80, 8080
NAC/MDM
Query Attributes
LDAP: tcp-udp/389, tcp/3268
SMB: tcp/445
KDC: tcp-udp/88
KPASS: tcp/464
SCEP: tcp/80, tcp/443
NTP: udp/123
OCSP: tcp/80
CRL:tcp/80, tcp/443, tcp/389
PIP
SSH tcp/22
Inter - Node Communications
Admin(P) - Admin(S): tcp/443, tcp/12001 (JGroups)
Monitor(P) - Monitor(S): tcp/443
Policy - Policy: tcp/7800, tcp/7802 (Node Groups)/(Groups)
mInter(P) - mInter(S): udp/694 (Heartbeat)
Logging
Mail and Messaging
Inter-Node Communication
Outer-Node Communication

Cisco ISE 管理节点端口

Cisco ISE 服务	千兆以太网 0 上的端口	千兆以太网 1 上的端口	千兆以太网 2 上的端口	千兆以太网 3 上的端口
管理	• HTTP：TCP/80 和 HTTPS：TCP/443（TCP/80 重定向到 TCP/443；不可配置） • SSH 服务器：TCP/22 • 外部 RESTful 服务 (ERS) REST API：TCP/9060 • TCP：9002（用于从管理 GUI 显示发起人门户） 注释 由于 Inline Posture 节点不支持管理角色，因此它们将无权访问端口 80 和 443。 注释 端口 80 和 443 支持管理员 Web 应用，并且默认情况下处于启用状态。	从 Cisco ISE 到外部身份验证库的出站流量（管理员用户界面身份验证）： • LDAP：TCP/389、3268、UDP/389 • SMB：TCP/445 • KDC：TCP/88 和 UDP/88 • KPASS：TCP/464 注释 对 Cisco ISE 的 HTTPS 和 SSH 访问只限于千兆以太网 0。		
复制和同步	• HTTPS (SOAP)：TCP/443 • 数据同步/复制 (JGroups)：TCP/12001（全局）	—	—	—
监控	SNMP 查询：UDP/161 注释 此端口因路由表而异。			

Cisco ISE 服务	千兆以太网 0 上的端口	千兆以太网 1 上的端口	千兆以太网 2 上的端口	千兆以太网 3 上的端口
日志记录（出站）	• 系统日志：UDP/20514 和 TCP/1468 • 安全系统日志：TCP/6514 注释 默认端口可配置用于外部日志记录。 • SNMP 陷阱：UDP/162			
外部身份源和资源（出站）	• 管理员用户界面和终端身份验证： LDAP：TCP/389、3268、UDP/389 SMB：TCP/445 KDC：TCP/88 和 UDP/88 KPASS：TCP/464 • NTP：UDP/123 • DNS：UDP/53 和 TCP/53 注释 对于只能通过除千兆以太网 0 以外的接口访问的外部身份源和服务，请相应地配置静态路由。			
访客	访客帐户到期电子邮件通知：SMTP：TCP/25			

Cisco ISE 监控节点端口

Cisco ISE 服务	千兆以太网 0 上的端口	千兆以太网 1 上的端口	千兆以太网 2 上的端口	千兆以太网 3 上的端口
管理	• HTTP：TCP/80 和 HTTPS：TCP/443 • SSH 服务器：TCP/22	—	—	—

Cisco ISE 服务	千兆以太网 0 上的端口	千兆以太网 1 上的端口	千兆以太网 2 上的端口	千兆以太网 3 上的端口
复制和同步	• HTTPS (SOAP)：TCP/443 • Oracle 数据库侦听程序：TCP/1521 • 数据同步/复制 (JGroups)：TCP/12001（全局）	Oracle 数据库侦听程序：TCP/1521	Oracle 数据库侦听程序：TCP/1521	Oracle 数据库侦听程序：TCP/1521
监控	简单网络管理协议 [SNMP]：UDP/161 注释 此端口因路由表而异。			
日志记录	• 系统日志：UDP/20514 和 TCP/1468 • 安全系统日志：TCP/6514 注释 默认端口可配置用于外部日志记录。 • SMTP：TCP/25 • SNMP 陷阱：UDP/162			
外部身份源和资源（出站）	• 管理员用户界面和终端身份验证： LDAP：TCP/389、3268、UDP/389 SMB：TCP/445 KDC：TCP/88 和 UDP/88 KPASS：TCP/464 • NTP：UDP/123 • DNS：UDP/53 和 TCP/53 注释 对于只能通过除千兆以太网 0 以外的接口访问的外部身份源和服务，请相应地配置静态路由。			

Cisco ISE 策略服务节点端口

Cisco ISE 服务	千兆以太网 0 上的端口	千兆以太网 1 上的端口	千兆以太网 2 上的端口	千兆以太网 3 上的端口
管理	• HTTP：TCP/80 和 HTTPS：TCP/443 • SSH 服务器：TCP/22 • OCSP：TCP/2560	Cisco ISE 管理只限于千兆以太网 0。	Cisco ISE 管理只限于千兆以太网 0。	Cisco ISE 管理只限于千兆以太网 0。
复制和同步	• HTTPS (SOAP)：TCP/443 • 数据同步/复制 (JGroups)：TCP/12001（全局）	—	—	—
群集（节点组）	• 节点组/JGroups：TCP/7800 • 节点故障检测：TCP/7802	—	—	—
监控	简单网络管理协议 [SNMP]：UDP/161 注释 此端口因路由表而异。			
日志记录（出站）	• 系统日志：UDP/20514 和 TCP/1468 • 安全系统日志：TCP/6514 注释 默认端口可配置用于外部日志记录。 • SNMP 陷阱：UDP/162			

Cisco ISE 服务	千兆以太网 0 上的端口	千兆以太网 1 上的端口	千兆以太网 2 上的端口	千兆以太网 3 上的端口
会话	• RADIUS 身份验证：UDP/1645 和 1812 • RADIUS 记帐：UDP/1646 和 1813 • RADIUS 授权变更 (CoA) 发送：UDP/1700 • RADIUS 授权变更 (CoA) 侦听/中继：UDP/1700 和 3799 注释 UDP 端口 3799 不可配置。			
外部身份源和资源（出站）	• 管理员用户界面和终端身份验证： LDAP：TCP/389 和 3268 SMB：TCP/445 KDC：TCP/88 KPASS：TCP/464 • NTP：UDP/123 • DNS：UDP/53 和 TCP/53 注释 对于只能通过除千兆以太网 0 以外的接口访问的外部身份源和服务，请相应地配置静态路由。			
Web 门户服务： - 访客/Web 身份验证 - 访客发起人门户 - 我的设备门户 - 客户端调配 - 黑名单门户	HTTPS（必须为 Cisco ISE 中的服务启用接口）： • 黑名单门户：TCP/8000-8999（默认端口为 TCP/8444。） • 访客门户和客户端调配：TCP/8000-8999（默认端口为 TCP/8443。） • 我的设备门户：TCP/8000-8999（默认端口为 TCP/8443。） • 发起人门户：TCP/8000-8999（默认端口为 TCP/8443。） • SMTP 通知：TCP/25			

Cisco ISE 服务	千兆以太网 0 上的端口	千兆以太网 1 上的端口	千兆以太网 2 上的端口	千兆以太网 3 上的端口
状态 - 发现 - 调配 - 评估/心跳	• 发现（客户端）：TCP/80 (HTTP) 和 TCP/8905 (HTTPS) 注释 默认情况下，TCP/80 重定向到 TCP/8443。 请参阅“Web 门户服务：访客门户和客户端调配”。 • 发现（策略服务节点端）：TCP/8443 和 8905 (HTTPS) • 调配 - URL 重定向：请参阅“Web 门户服务：访客门户和客户端调配” • 调配 - Active-X 和 Java Applet 安装，包括 IP 刷新、Web 代理安装以及启动 NAC 代理安装：请参阅“Web 门户服务：访客门户和客户端调配”。 • 调配 - NAC 代理安装：TCP/8443 • 调配 - NAC 代理更新通知：UDP/8905 (SWISS) • 调配 - NAC 代理和其他软件包/模块更新：TCP/8905 (HTTPS) • 评估 - 状态协商和代理报告：TCP/8905 (HTTPS) • 评估 - PRA/保持连接：UDP/8905 (SWISS)			
自带设备 (BYOD)/网络服务协议 (NSP) - 重定向 - 调配 - SCEP	• 调配 - URL 重定向：请参阅“Web 门户服务：访客门户和客户端调配” • 调配 - Active-X 和 Java Applet 安装（包括启动向导安装）：请参阅“Web 门户服务：访客门户和客户端调配” • 调配 - 从 Cisco ISE（Windows 和 Mac 操作系统）执行向导安装：TCP/8443 • 调配 - 从 Google Play (Android) 执行向导安装：TCP/443 • 调配 - 请求方调配过程：TCP/8905 • SCEP 代理至 CA：TCP/80 或 TCP/443（基于 SCEP RA URL 配置）			
移动设备管理 (MDM) API 集成	• URL 重定向：请参阅“Web 门户服务：访客门户和客户端调配” • API：供应商专用 • 代理安装和设备注册：供应商专用			

Cisco ISE 服务	千兆以太网 0 上的端口	千兆以太网 1 上的端口	千兆以太网 2 上的端口	千兆以太网 3 上的端口
分析	• NetFlow：UDP/9996 注释 此端口是可配置的。 • DHCP：UDP/67 注释 此端口是可配置的。 • DHCP SPAN 探测：UDP/68 • HTTP：TCP/80 和 8080 • DNS：UDP/53（查找） 注释 此端口因路由表而异。 • SNMP 查询：UDP/161 注释 此端口因路由表而异。 • SNMP 陷阱：UDP/162 注释 此端口是可配置的。			

Inline Posture 节点端口

注释 由于 Inline Posture 节点不支持管理角色，因此它们将无权访问端口 TCP 80 和 443。 Inline Posture 节点的高可用性不适用于任何其他 Cisco ISE 节点类型。

Cisco ISE 服务	千兆以太网 0 上的端口	千兆以太网 1 上的端口	千兆以太网 2 上的端口	千兆以太网 3 上的端口
管理	• HTTPS：TCP/8443 注释 TCP：8443 由管理节点使用。 • SSH 服务器：TCP/22	—	—	—
Inline Posture	• 用于身份验证的 RADIUS 代理：UDP/1645 和 1812 • 用于记帐的 RADIUS 代理：UDP/1646 和 1813 • RADIUS CoA：UDP/1700 和 3799 注释 UDP 端口 3799 不可配置。 • 重定向：TCP/9090	• 用于身份验证的 RADIUS 代理：UDP/1645 和 1812 • 用于记帐的 RADIUS 代理：UDP/1646 和 1813 • RADIUS CoA：不适用 • 重定向：TCP/9090	—	—
日志记录（出站）	系统日志：UDP/20154 注释 此端口是可配置的。	系统日志：UDP/20154 注释 此端口是可配置的。	—	—

Cisco ISE 服务	千兆以太网 0 上的端口	千兆以太网 1 上的端口	千兆以太网 2 上的端口	千兆以太网 3 上的端口
高可用性	—	—	心跳：UDP/694（心跳）	心跳：UDP/694

Cisco ISE pxGrid 服务端口

Cisco ISE 服务	千兆以太网 0 上的端口	千兆以太网 1 上的端口	千兆以太网 2 上的端口	千兆以太网 3 上的端口
管理	• SSL：TCP/5222（节点间通信） • SSL：TCP/7400（节点组通信）	—	—	—
复制和同步	数据同步和复制 (JGroups)：TCP/12001（全局）	—	—	—

OCSP 和 CRL 服务端口

对于在线证书状态协议服务 (OCSP) 和证书撤销列表 (CRL)，尽管对 Cisco ISE 服务和端口的引用会列出 Cisco ISE 管理节点、策略服务节点、监控节点和 Inline Posture 节点中分别使用的基本端口，但是端口仍然依赖于 CA 服务器或托管 OCSP/CRL 的服务。

对于 OCSP，可以使用的默认端口是 TCP 80/TCP 443。 Cisco ISE 管理员门户希望对 OCSP 服务使用基于 http 的 URL，因此默认值为 TCP 80。 您还可以使用非默认端口。

对于 CRL，默认协议包括 HTTP、HTTPS 和 LDAP，默认端口分别为 80、443 和 389。 实际端口取决于 CRL 服务器。

索 引

字母