思科身份服务引擎安装指南，版本 2.2

首次发布日期: 2016 年 11 月 04 日

上次修改日期: 2017 年 01 月 31 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

文本部件号:

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

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

- 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。

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	单个物理或虚拟思科 ISE 设备。
节点类型	思科ISE节点可以承担下列任何角色：管理、策略服务、监控
角色	确定节点提供的服务。思科ISE节点可以承担以下任一或全部角色：。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

Cisco ISE 节点可以根据它承担的角色提供各种服务。部署中的每个节点均可承担管理、策略服务、pxGrid 和监控角色。在分布式部署中，您可以在网络中使用以下节点组合：

- 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
- pxGrid 服务的一个或多个 pxGrid 节点

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

承担策略服务角色的思科 ISE 提供网络访问、终端安全评估、访客接入、客户端调配和分析服务。此角色评估策略并作出所有决策。您可以让多个节点承担此角色。通常，分布式部署中可能有多个策略服务节点。驻留在同一高速局域网 (LAN) 中或负载均衡器后面的所有策略服务节点可以组合在一起，形成一个节点组。如果节点组中的一个节点发生故障，其他节点会检测到故障，并重置任何 URL 重定向会话。

分布式设置中至少有一个节点应当承担策略服务角色。

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。如果主监控节点断开连接，辅助监控节点会自动成为主监控节点。

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。

pxGrid 节点

您可以使用思科 pxGrid 与其他网络系统（例如 ISE 生态系统合作伙伴系统）和其他思科平台共享思科 ISE 会话目录中的情景相关信息。pxGrid 框架也可用来在思科 ISE 与第三方供应商之间、在节点（例如共享标记）与策略对象之间交换策略和配置数据，还能进行其他信息的交换。思科 pxGrid 还允许第三方系统调通过自适应网络控制操作 (EPS) 来隔离用户/设备以应对网络或安全事件。可通过 TrustSec 主题将标签定义、值和说明等 TrustSec 信息从思科 ISE 传输到其他网络。可通过终端配置文件元主题，将具有完全限定名称 (FQN) 的终端配置文件从思科 ISE 传输到其他网络。思科 pxGrid 还支持标签和终端配置文件的批量下载。

您可以通过 pxGrid 发布和订用 SXP 绑定（IP-SGT 映射）。有关 SXP 绑定的详细信息，请参阅思科身份服务引擎管理员指南中的“源组标记协议”部分。

在高可用性配置中，思科 pxGrid 服务器通过 PAN 在节点之间复制信息。当 PAN 断开连接时，pxGrid 服务器会停止处理客户端注册和订用。您需要手动升级 PAN，以激活 pxGrid 服务器。

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。

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

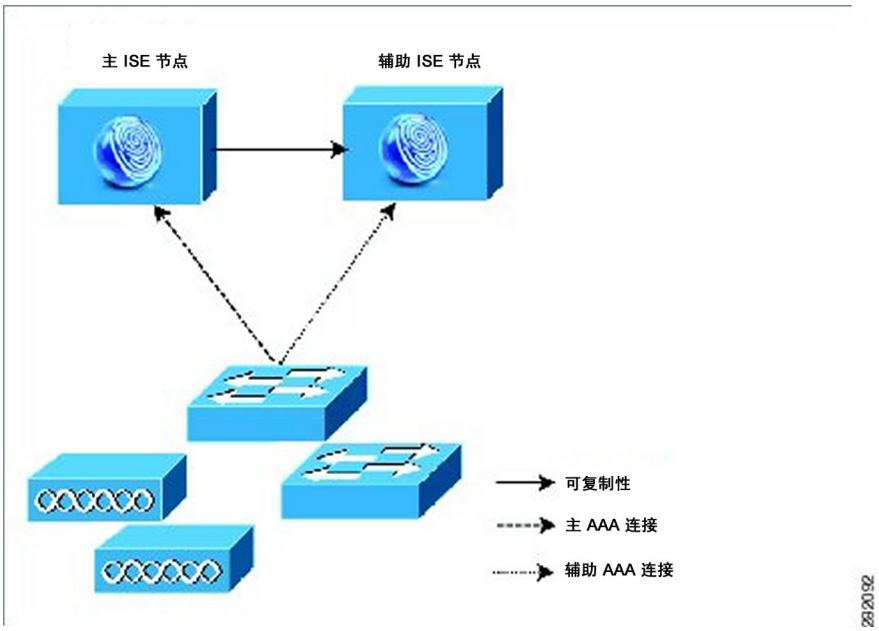
小型网络部署

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。

客户端与主思科 ISE 节点之间的集中式身份验证、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 *1*：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

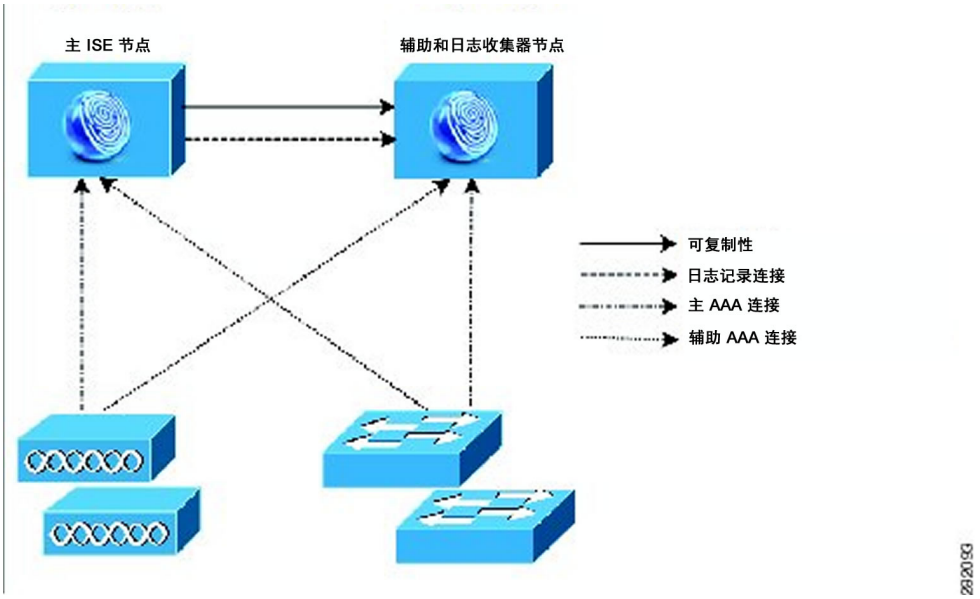
在分离式 Cisco ISE 部署中，您将按照小型 Cisco ISE 部署中所述继续维护主要节点和辅助节点。但是， AAA 负载会在两个 Cisco ISE 节点之间进行拆分，以优化 AAA 工作流程。如果 AAA 连接有任何问题，则每个 Cisco ISE 设备（主要或辅助）需要能够处理全部工作负载。主要节点和辅助节点在正常网络操作过程中均不处理任何 AAA 请求，因为此工作负载分布在两个节点之间。

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 *2*：分离式网络部署

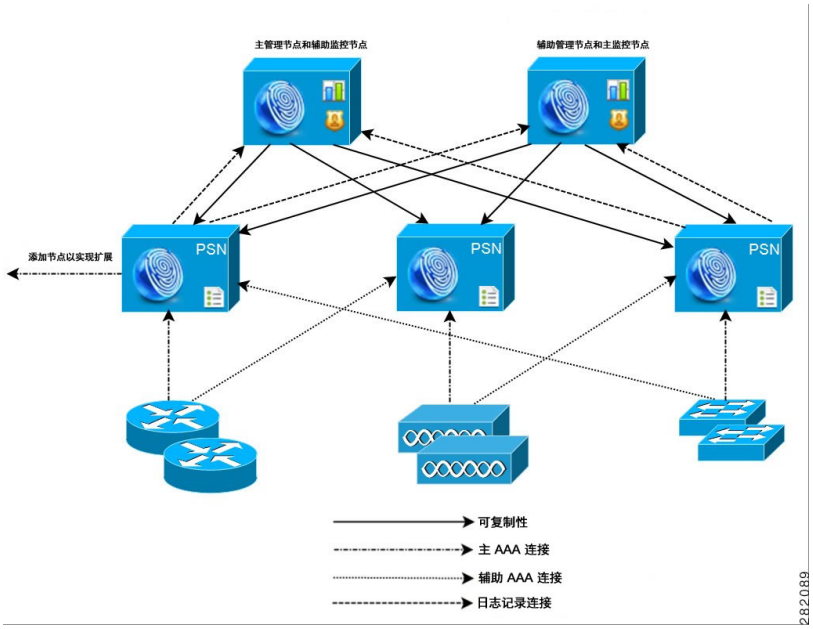


中型网络部署

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 3： 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。

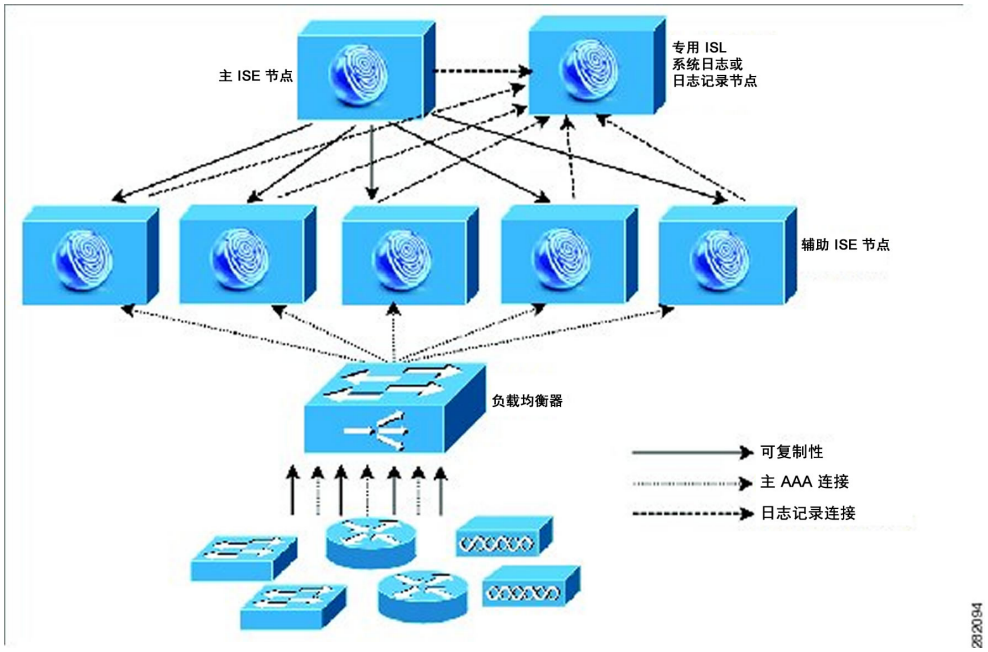
您也可以考虑使用设备将日志发送到 Cisco ISE 节点上的监控角色以及通用系统日志服务器。如果 Cisco ISE 节点上的监控角色关闭，则添加通用日志服务器可提供冗余备份。

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 4：大型网络部署

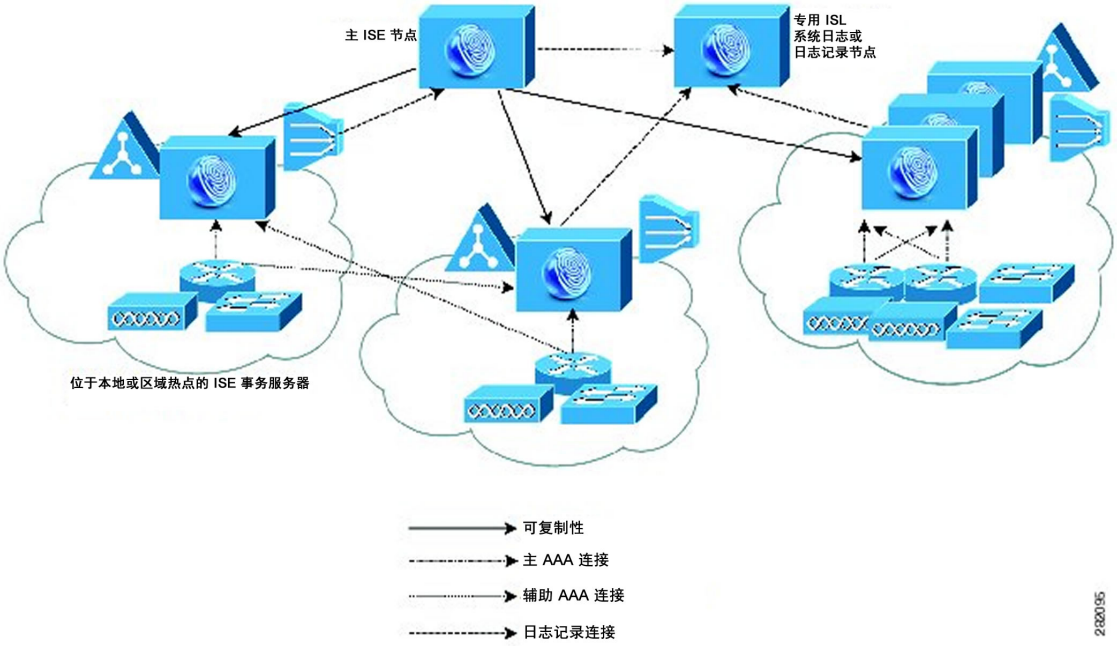


离散网络部署

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 5： 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 SNS 3515	0	最多 5,000 个终端
		Cisco SNS 3595	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 SNS 3595 设备	5	最多 5,000 个终端
		用于承担管理和监控角色的 Cisco SNS 3595 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 SNS 3595 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 SNS-3515	5,000
	大型	Cisco SNS-3595	20,000

外形规格	平台规模	设备	最大终端数
虚拟机	小型/中型/大型	可与物理设备相比较	3,000 至 20,000

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。

ISE 社区资源

有关使用 WLC 设置思科 ISE 的信息，请参阅使用 WLC 设置思科 ISE 视频。

第 2 章

系统要求

本章提供指向思科安全网络服务器数据表的链接，并列出虚拟设备要求。

硬件和虚拟设备要求

思科身份服务引擎 (ISE) 可以安装在思科 SNS 硬件或虚拟设备上。为了实现可与思科 ISE 硬件设备相媲美的性能和可扩展性，为虚拟机分配的系统资源应与为 Cisco SNS 3515 和 3595 设备分配的系统资源相当。本节列出安装思科 ISE 所需的硬件、软件和虚拟机要求。

Cisco SNS-3400 和 SNS-3500 系列设备

有关 SNS 硬件设备规范，请参阅思科安全网络服务器数据表中的“表 1：产品规范”。

有关合规性和安全信息，请参阅适用于 Cisco SNS-3415、Cisco SNS-3495、Cisco SNS-3515 和 Cisco SNS-3595 设备的合规性和安全信息。

有关 SNS 设备硬件安装，请参阅

- 有关 SNS-3400 系列设备，请参阅 Cisco SNS-3400 系列设备硬件安装指南。
- 有关 SNS-3500 系列设备，请参阅 Cisco SNS-3500 系列设备硬件安装指南。

VMware 虚拟机要求

Cisco ISE 支持以下 VMware 服务器和客户端：

- 适用于 ESXi 5.*x* 的 VMware 版本 8（默认）

注释 如果您要通过在 ESXi 5.*x* 服务器上安装思科 ISE 来支持 RHEL 7 作为访客操作系统，请将 VMware 硬件版本更新至 9 或更高版本。RHEL 7 支持与 VMware 硬件版本 9 及更高版本配合使用。

- 适用于 ESXi 6.*x* 的 VMware 版本 11（默认）

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 主机必须与千兆或更快的以太网链路互连。
- 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。

思科 ISE 提供以下 OVA 模板，可供您在虚拟机 (VM) 上安装和部署思科 ISE 使用：

注释 200 GB OVA 模板完全可以作为专用策略服务的思科 ISE 节点或 pxGrid 节点。

建议用 600 GB 和 1.2 TB OVA 模板来满足运行管理或监控角色的 ISE 节点的最低要求。有关磁盘空间要求的附加信息，请参阅磁盘空间要求，第 17 页。

如果您需要自定义磁盘大小、CPU 或内存分配，可以使用标准 .iso 映像手动部署思科 ISE。但是，务必要确保满足本文档中指定的最低要求和资源预留。OVA 模板可以通过自动应用每个平台所需的最少资源来简化 ISE 虚拟设备部署。

ISE 2.2 OVA 模板与用于 vCenter 6.5 的 VMware Web 客户端不兼容。此问题的解决方法是，用 VMware OVF 工具导入 OVA 模板。

- ISE-2.2.0.*xxx*-eval.ova
- ISE-2.2.0.*xxx*-virtual-200GB-SNS3415.ova
- ISE-2.2.0.*xxx*-virtual-200GB-SNS3495.ova
- ISE-2.2.0.*xxx*-virtual-200GB-SNS3515.ova
- ISE-2.2.0.*xxx*-virtual-200GB-SNS3595.ova
- ISE-2.2.0.*xxx*-virtual-600GB-SNS3415.ova
- ISE-2.2.0.*xxx*-virtual-600GB-SNS3515.ova
- ISE-2.2.0.*xxx*-virtual-1.2TB-SNS3495.ova
- ISE-2.2.0.*xxx*-virtual-1.2TB-SNS3595.ova

下表提供了基础 SNS 平台的 OVA 模板预留。

表 3：*OVA* 模板预留

OVA 模板	内存	CPU
虚拟评估 OVA	8 GB RAM 注释 要评估访客访问和基本访问策略流，需要至少 8 GB RAM。要评估高级功能（例如 pxGrid、内部 CA、SXP、设备管理和被动身份服务），我们建议您在部署评估 OVA 之后将 VM 的 RAM 配置为 16 GB。	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 SNS-3515 OVA	16 GB RAM	12000 MHz
虚拟 SNS-3595 OVA	64 GB RAM	16000 MHz

下表列出了 VMware 虚拟机要求。

要求类型	规范
CPU	• 评估： 时钟速度：2.0 GHz 或更快 核心数量：2 个 CPU 核心 • 生产： 时钟速度：2.0 GHz 或更快 内核数量：6 个（小型）到 8 个（大型）CPU 内核 Cisco ISE 支持超线程。我们建议您启用超线程（如果可用）。 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。

要求类型	规范
内存	• **评估：** 基本 - 8 GB（用于评估访客访问和基本访问策略流） 高级 - 16 GB（用于评估高级功能，例如 pxGrid、内部 CA、SXP、设备管理和被动身份服务） • **生产：** 小型 - 16 GB 大型 - 64 GB
硬盘	• **评估：**200 GB • **生产：** 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。 **注释** 为思科 ISE 创建虚拟机时，请使用单个虚拟磁盘来满足存储要求。如果使用多个**虚拟**磁盘来满足磁盘空间要求，安装程序可能无法识别所有磁盘空间。
存储和文件系统	思科 ISE 虚拟设备的存储系统要求的写入性能最低为每秒 50 MB，读取性能最低为每秒 300 MB。部署的存储系统应满足这些性能条件并受 VMware 服务器的支持。 思科 ISE 在安装之前、安装期间以及安装之后，会提供很多方法来验证您的存储系统是否满足以上最低要求。有关详细信息，请参阅虚拟机资源和性能检查，第 29 页。 我们推荐使用 VMFS 文件系统，因为它经过了最广泛的测试，不过如果其他文件系统、传输和媒体满足上述要求，也是可以部署的。
磁盘控制器	半虚拟化（默认用于 64 位 RHEL 7）或 LSI 逻辑并行 为了获得最佳性能和冗余，建议使用缓存 RAID 控制器。RAID 10（也称为 1+0）等控制器选项比 RAID 5 等选项提供的整体写入性能和冗余要高。此外，带后备电池的控制器缓存可以大幅提高写入操作性能。
网卡	需要 1 GB NIC 接口（建议使用两个或多个 NIC；支持六个 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，可能必须重新映射 ESXi 适配器，以使其与 ISE 适配器顺序同步。

要求类型	规范
VMware 虚拟硬件版本/虚拟机监控程序	ESXi 5.*x* 和 6.*x* 上的 VMware 虚拟机硬件版本 8 或更高版本。 注释 如果您要通过在 ESXi 5.*x* 服务器上安装思科 ISE 来支持 RHEL 7 作为访客操作系统，请将 VMware 硬件版本更新至 9 或更高版本。RHEL 7 支持与 VMware 硬件版本 9 及更高版本配合使用。

Linux KVM 要求

下表列出了 Linux KVM 虚拟机要求。

要求类型	最低要求
CPU	• 评估： 时钟速度：2.0 GHz 或更快 核心数量：2 个 CPU 核心 • 生产： 时钟速度：2.0 GHz 或更快 核心数量：6（小型）至 8 个（大型）CPU 核心 6 个核心；2.0 Ghz 或更快。 Cisco ISE 支持超线程。我们建议您启用超线程（如果可用）。 注释 尽管超线程可能会提高整体性能，但它不会改变每个虚拟机设备所支持的扩展限制。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	• 评估： 基本 - 8 GB（用于评估访客访问和基本访问策略流） 高级 - 16 GB（用于评估高级功能，例如 pxGrid、内部 CA、SXP、设备管理和被动身份服务） • 生产： 小型 - 16 GB 大型 - 64 GB

要求类型	最低要求
硬盘	• 评估：200 GB • 生产： 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。 注释 为思科 ISE 创建虚拟机时，请使用单个虚拟磁盘来满足存储要求。如果使用多个**虚拟**磁盘来满足磁盘空间要求，安装程序可能无法识别所有磁盘空间。
KVM 磁盘设备	磁盘总线 - virtio，缓存模式 - 无，I/O 模式 - 本机 使用预分配的 RAW 存储格式。
网卡	需要 1 GB NIC 接口（建议使用两个或多个 NIC；支持六个 NIC）。思科 ISE 支持 VirtIO 驱动程序。我们建议使用 VirtIO 驱动程序以提高性能。
虚拟机监控程序	RHEL 7.0 上的 KVM

Microsoft Hyper-V 要求

下表列出了 Microsoft Hyper-V 虚拟机要求。

要求类型	最低要求
CPU	• 评估： 时钟速度：2.0 GHz 或更快 核心数量：2 个 CPU 核心 • 生产： 时钟速度：2.0 GHz 或更快 核心数量：6（小型）至 8 个（大型）CPU 核心

要求类型	最低要求
内存	• **评估**： 基本 - 8 GB（用于评估访客访问和基本访问策略流） 高级 - 16 GB（用于评估高级功能，例如 pxGrid、内部 CA、SXP、设备管理和被动身份服务） • **生产**： 小型 - 16 GB 大型 - 64 GB
硬盘	• **评估**：200 GB • **生产**：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。 **注释** 为思科 ISE 创建虚拟机时，请使用单个虚拟磁盘来满足存储要求。如果使用多个**虚拟**磁盘来满足磁盘空间要求，安装程序可能无法识别所有磁盘空间。
网卡	需要 1 GB NIC 接口（建议使用两个或多个 NIC；支持六个 NIC）。
虚拟机监控程序	Hyper-V (Microsoft)

磁盘空间要求

下表列出针对在生产部署中运行虚拟机建议的思科 ISE 磁盘空间分配。

表 *4*：建议的虚拟机磁盘空间

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

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 - 仅管理	200 GB	2 TB	250 至 300 GB
分布式 ISE - 仅监控	200 GB	2 TB	600 GB 至 2 TB
分布式 ISE - 仅策略服务	200 GB	2 TB	200 GB
分布式 ISE - 仅 pxGrid	200 GB	2 TB	200 GB
分布式 ISE - 管理和监控（以及可选的 pxGrid）	200 GB	2 TB	600 GB 至 2 TB
分布式 ISE - 管理、监控和策略服务（以及可选的 pxGrid）	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：

- 您可以为一台思科 ISE 虚拟机分配最多 2 TB 的磁盘空间。
- 思科 ISE 必须安装在虚拟机中的单个磁盘上。
- 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，最多可为虚拟机磁盘大小增加 2 TB 的日志存储。

如果增加了虚拟机的磁盘大小，则不得进行升级，而应在虚拟机上全新安装思科 ISE。

表 5：日志可在监控节点中存储的天数 根据分配的磁盘空间以及连接至网络的终端数列出了日志可以在 Monitoring 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 *5*：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

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

第 3 章

安装思科 ISE

本章列出系统要求，并提供简要安装步骤来帮助您快速安装思科 ISE。

安装思科 ISE

本部分列出简要安装步骤帮助您快速安装思科 ISE：

> ISE 社区资源
>
> 要快速设置思科无线控制器和思科 ISE，请参阅 ISE 无线访客设置指南和 ISE 无线访客设置视频。

开始之前

- 确保您已满足本指南中指定的硬件和虚拟设备要求。
- （可选；仅在虚拟机上安装思科 ISE 时需要满足此要求）确保您已正确创建虚拟机。有关详细信息，请参阅以下主题：

  配置 VMware 服务器，第 33 页

  在 KVM 上安装思科 ISE，第 43 页

  在 Hyper-V 上创建思科 ISE 虚拟机，第 46 页

- （可选；仅在 SNS 硬件设备上安装思科 ISE 时需要满足此要求）确保要设置思科集成管理接口 (CIMC) 配置实用程序以管理设备并配置 BIOS。有关详细信息，请参阅以下文档。

  有关 SNS 3400 系列设备，请参阅 Cisco SNS-3400 系列设备硬件安装指南。

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

步骤 1 如果要在以下设备上安装思科 ISE：

- 思科 SNS 设备 - 安装硬件设备。连接到 CIMC 进行服务器管理。
- 虚拟机 - 确保 VM 已正确配置。如果您要在 VMware VM 上安装思科 ISE，请使用 OVA 模板。

步骤 2 下载思科 ISE ISO 映像。要在 VMware VM 上安装思科 ISE，请下载 OVA 模板。有关部署 OVA 模板的详细信息，请参阅使用 OVA 模板在虚拟机上部署思科 ISE ，第 29 页。

注释 ISE 2.2 OVA 模板与用于 vCenter 6.5 的 VMware Web 客户端不兼容。此问题的解决方法是，使用 VMware OVF 工具导入 OVA 模板。

a) 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。

b) 点击 **Download Software for this Product**。
思科 ISE 映像上已经安装 90 天的评估许可证，因此在完成安装和初始配置后，可以对所有思科 ISE 服务进行测试。

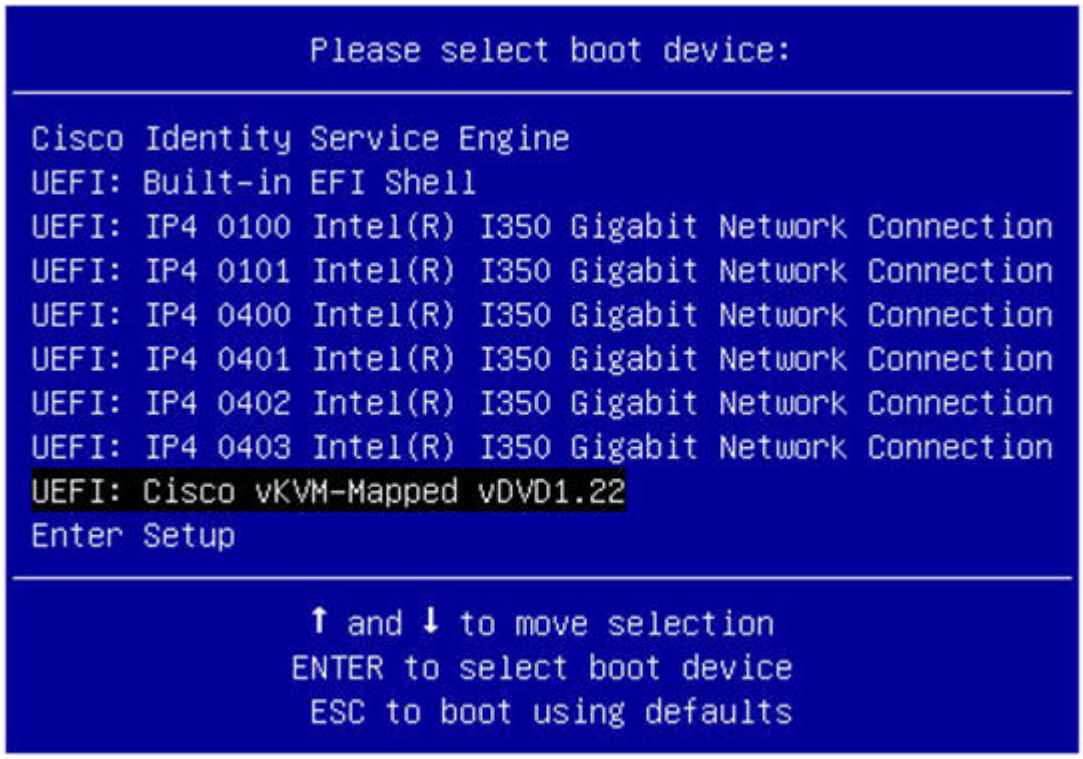
步骤 3 启动设备或虚拟机。

- 思科 SNS 设备：

1. 连接到 CIMC 并使用 CIMC 凭证登录。
2. 启动 KVM 控制台。
3. 选择 Virtual Media > Activate Virtual Devices。
4. 选择 Virtual Media > Map CD/DVD，并选择 ISE ISO 映像，然后点击 Map Device。
5. 选择 Macros > Static Macros > Ctrl-Alt-Del 以使用 ISE ISO 映像启动设备。

6 按 F6 以显示启动菜单。类似如下的屏幕随即会显示：

图 6：启动设备选择



- 虚拟机：

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

```
Welcome to the Cisco Identity Services Engine Installer
Cisco ISE Version: 2.2.0.xxx


Available boot options:

Cisco ISE Installation (Serial Console)
Cisco ISE Installation (Keyboard/Monitor)
System Utilities (Serial Console)
System Utilities (Keyboard/Monitor)
```

步骤 4 在启动提示符后，按 **1** 和 **Enter** 可使用串行控制台安装思科 ISE。
如果要使用键盘和显示器，请使用箭头键选择 **Cisco ISE Installation (Keyboard/Monitor)** 选项。系统随即会显示以下消息：

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

步骤 5 在提示下，键入 **setup** 开始启动设置程序。有关设置程序参数的详细信息，请参阅运行设置程序，第 24 页。

步骤 6 在设置模式下输入网络配置参数后，设备会自动重新启动并返回到外壳提示符模式。

步骤 7 从外壳提示模式退出。设备即会正常运行。

步骤 8 继续执行验证安装过程，第 26 页。

运行设置程序

本部分介绍配置 ISE 服务器的设置过程。

设置过程会启动交互式命令行界面(CLI)，提示您提供所需的参数。管理员可以使用控制台或哑终端配置初始网络设置，并使用设置程序为 ISE 服务器提供初始管理员凭证。设置流程是一种一次性配置任务。

要运行设置程序，请执行以下操作：

步骤 1 打开设备
系统随即会显示以下设置提示：

```
Please type 'setup' to configure the appliance
localhost login:
```

步骤 2 在登录名提示下，输入 **setup** 并按 **Enter**。
控制台随即会显示一组参数。您必须按照下表中的说明输入参数

表 *6*：思科 *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

提示	描述	示例
Primary name server	必须是主要域名服务器的有效 IPv4 地址。	10.15.20.25
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。要执行此操作，请输入 **y** 继续。
Primary NTP server	必须是网络时间协议 (NTP) 服务器的有效 IPv4 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。要执行此操作，请输入 **y** 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）。 要获得受支持时区的完整列表，您可以从思科 ISE CLI 运行 **show timezones** 命令。 **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	识别对思科 ISE 系统进行 CLI 访问所用的管理用户名。如果选择不使用默认值 (admin)，则必须创建新用户名。用户名的长度必须为三至八个字符，并且由有效的字母数字字符（A－Z、a－z 或 0－9）组成。	admin（默认值）
Password	识别对思科 ISE 系统进行 CLI 访问所用的管理密码。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

运行设置程序后，系统会自动重新引导。

现在，您可以用设置过程中配置的用户名和密码登录到思科 ISE。

验证安装过程

要验证您是否已正确完成安装过程，请执行以下操作：

步骤 1 系统重新引导时，在登录名提示下输入您在设置期间配置的用户名，然后按 **Enter**。

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

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

控制台随即会显示：

```
Cisco Identity Services Engine
------------------------------------

Version: 2.2.0.323
Build Date: Mon Jan 11 19:31:27 2016
Install Date: Tue Jan 12 14:35:24 2016
```

注释 此次发布的不同版本的版本和日期可能会因版本不同而各不相同。

步骤 4 输入 **show application status ise** 命令检查 ISE 进程的状态，然后按 **Enter**。

控制台随即会显示：

```
ise/admin# show application status ise
ISE PROCESS NAME                       STATE            PROCESS ID
--------------------------------------------------------------------
Database Listener                      running          14586
Database Server                        running          84 PROCESSES
Application Server                     running          18537
Profiler Database                      running          15998
ISE Indexing Engine                    running          19731
AD Connector                           running          23164
M&T Session Database                   running          15898
M&T Log Collector                      running          18671
M&T Log Processor                      running          18585
Certificate Authority Service          running          22961
EST Service                            running          30193
SXP Engine Service                     disabled
Docker Daemon                          running          20399
TC-NAC Service                         disabled
Wifi Setup Helper Container            running          22582
 Wifi Setup Helper Vault               running          42
 Wifi Setup Helper MongoDB             running          15
 Wifi Setup Helper Web Server          running          219
 Wifi Setup Helper Auth Service        running          129
 Wifi Setup Helper Main Service        running          165
 Wifi Setup Helper WLC Service         running          203
pxGrid Infrastructure Service          disabled
pxGrid Publisher Subscriber Service    disabled
pxGrid Connection Manager              disabled
pxGrid Controller                      disabled
PassiveID WMI Service                  disabled
PassiveID Syslog Service               disabled
PassiveID API Service                  disabled
PassiveID Agent Service                disabled
PassiveID Endpoint Service             disabled
PassiveID SPAN Service                 disabled
DHCP Server (dhcpd)                    disabled
DNS Server (named)                     disabled
```

第 4 章

其他安装信息

本章涵盖与 SNS 硬件和虚拟设备相关的其他信息。

SNS 设备参考

创建一个可引导 USB 设备以安装思科 ISE

使用 Fedora LiveUSB Creator 工具从思科 ISE 安装 ISO 文件创建可引导 USB 设备。

开始之前

- 将适用于 Windows 或 Linux 的 Fedora LiveUSB Creator 从以下位置下载至本地系统：https://fedoraproject.org/wiki/How_to_create_and_use_Live_USB。

  注释 其他 USB 工具可能也适用，但思科还是建议使用 Fedora LiveUSB Creator，因为它已进行资格审查。

- 将思科 ISE 安装 ISO 文件下载至本地系统。

- 使用 8 GB（或更高）USB 设备。

步骤 1 将 USB 设备插入本地系统。

步骤 2 启动 **LiveUSB Creator**。

步骤 3 从 Use existing Live CD 区域中点击 **Browse**，并选择思科 ISE ISO 文件。

步骤 4 （如果本地系统只连接了一个 USB 设备，会自动选择该设备）从 **Target Device** 下拉列表中选择 USB 设备。

步骤 5 点击 **Create Live USB**。
进度条会指示可引导 USB 创建的进度。完成此过程后，USB 驱动器的内容即可在运行 USB 工具所用的本地系统进行访问。必须在手动更新两个文本文件后才能安装思科 ISE。

步骤 6 从 USB 驱动器中，在文本编辑器中打开以下文本文件：

- syslinux/*syslinux.cfg*
- EFI/BOOT/*grub.cfg*

步骤 7 替换两个文件中的术语“**cdrom:**”。

- 如果您有 Cisco SNS 3415 设备，请将两个文件中的术语“**cdrom:**”替换为“**hd:sda1**”。
- 如果您有 Cisco SNS 3495、3515 或 3595 设备，请将两个文件中的术语“**cdrom:**”替换为“**hd:sdb1**”。

具体而言，就是替换“**cdrom:**”字符串的所有实例。例如，将

ks=*cdrom:*/ks.cfg

替换为

ks=*hd:sdb1:*/ks.cfg

步骤 8 保存文件并退出。

步骤 9 从本地系统安全地删除 USB 设备。

步骤 10 要安装思科 ISE，请将可引导 USB 设备插入思科 ISE 设备，重启设备，从 USB 驱动器引导。

重新映像 Cisco SNS 3500 系列设备

Cisco SNS-3500 系列设备没有内置的 DVD 驱动器。因此，要使用思科 ISE 软件重新映像思科 ISE 硬件设备，可以执行以下操作之一：

注释 SNS 3515 和 SNS 3595 设备支持统一可扩展固件接口 (UEFI) 的安全引导功能。此功能可确保只有思科签名的 ISE 映像才能安装在 SNS 3515 和 SNS 3595 设备上，并且可以防止安装任何未获签名的操作系统，即使拥有对设备的物理访问权限也不行。举例来说，常规操作系统（Red Hat Enterprise Linux 或 Microsoft Windows）无法在此设备上引导。

SNS 3515 和 SNS 3595 设备仅支持思科 ISE 2.0.1 或更高版本。不能在 SNS 3515 或 SNS 3595 设备上安装 2.0.1 之前的版本。

- 使用思科集成管理控制器 (CIMC) 界面将安装 .iso 文件映射至虚拟 DVD 设备。有关详细信息，请参阅安装思科 ISE，第 21 页。
- 使用安装 .iso 文件创建安装 DVD，并将其插入 USB 外部 DVD 驱动器，然后从 DVD 驱动器引导设备。
- 使用安装 .iso 文件创建一个可引导 USB 设备，并从 USB 驱动器引导设备。有关详细信息，请参阅创建一个可引导 USB 设备以安装思科 ISE，第 27 页和安装思科 ISE，第 21 页。

VMware 虚拟机

虚拟机资源和性能检查

在虚拟机上安装思科ISE之前，安装程序会将虚拟机上可用的硬件资源与建议的硬件规范进行比较，以执行硬件完整性检查。

执行 VM 资源检查期间，安装程序会检查硬盘空间、分配给 VM 的 CPU 核心数量、CPU 时钟速度以及分配给 VM 的 RAM。如果 VM 资源不满足基本评估规范，安装即会中止。此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，安装程序会检查磁盘 I/O 的性能。如果磁盘 I/O 性能不满足建议的规范，则屏幕上会显示一条警告，不过还是会允许您继续进行安装。

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。

VM 性能检查也可以根据需要从思科 ISE CLI 中使用 **show tech-support** 命令完成。

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 OVA 模板在虚拟机上部署思科 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

注释 ISE 2.2 OVA 模板与用于 vCenter 6.5 的 VMware Web 客户端不兼容。此问题的解决方法是，使用 VMware OVF 工具导入 OVA 模板。

如果导入 OVA 之后虚拟硬盘的大小有变化，您必须从 ISO 重新映射思科 ISE，因为思科 ISE 不支持在安装后调整硬盘和文件系统大小。

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 VMware 虚拟机上安装思科 ISE

本部分介绍如何使用 ISO 文件在 VMware 虚拟机上安装思科 ISE。

配置 VMware ESXi 服务器的先决条件

尝试配置 VMWare ESXi 服务器之前，请查看本部分中列出的如下配置先决条件：

- 务必要以具有管理权限的用户的身份（根用户）登录 ESXi 服务器。
- Cisco ISE 是 64 位系统。安装 64 位系统之前，请确保在 ESXi 服务器上启用了虚拟化技术 (VT)。您还必须确保访客操作系统类型设置为 Red Hat Enterprise Linux 7（64 位）。
- 对于 Red Hat Enterprise Linux 7，默认 NIC 类型是 VMXNET3 适配器。您最多可以给您的思科 ISE 虚拟机添加六个 NIC，但要确保为所有 NIC 选择相同的适配器。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。确保在下表所列的 ESXi 服务器中将思科 ISE GigabitEthernet 0 接口映射至第 4 个接口 (NIC 4)。

ADE-OS	Cisco ISE	E1000	VMXNET3
eth0	GE0	1	4
eth1	GE1	2	1
eth2	GE2	3	2
eth3	GE3	4	3
eth4	GE4	5	5
eth5	GE5	6	6

如果选择 E1000 适配器，默认情况下，ESXi 适配器和思科 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。请参阅 磁盘空间要求，第 17 页 部分以获取更多信息。
- 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。对于 VMFS5，1 MB 块大小支持最多 2 TB 虚拟磁盘大小。

虚拟化技术检查

如果已经安装了 ESXi 服务器，可以检查该服务器上是否已启用 VT，无需重新引导设备。要执行此操作，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 支持的值为 3，则在 ESXi 服务器上启用了 VT，您可以继续安装。

如果 HV 支持的值为 2，则 VT 受支持，但未在 ESXi 服务器上启用。您必须编辑 BIOS 设置并在 ESXi 服务器上启用 VT。

在 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。但在安装最新版本之前，您必须在 ESXi 服务器上启用虚拟化技术 (VT)。

步骤 1 重新启动 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。

为思科 ISE 分析器服务配置 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 服务器接口） **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**。
对用来进行 SPAN 或镜像流量的分析器数据收集的另一个 VMware ESXi 服务器接口重复相同的步骤。

使用串行控制台连接至 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**。

- 如果选择 Connect via Network 选项，则必须通过 ESXi 服务器打开防火墙端口。
- 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 ESXi 服务器的先决条件，第 30 页部分的详细信息。

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 主机或集群支持多个 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 7**。

步骤 8 从 Number of virtual sockets 和 Number of cores per virtual socket 下拉列表中选择一个值。核心总数应为 6（小型 VM 设备）或 8（大型 VM 设备）。
（可选；显示在某些版本的 ESXi 服务器上。如果仅显示 Number of virtual processors，请选择 **6** 或 **8**）。

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：

- 访客操作系统 - Red Hat Enterprise Linux 7
- CPU - 6
- 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**。

增加虚拟机启动引导延迟配置

在 VMware 虚拟机上，引导延迟默认设置为 0。您可以通过更改此引导延迟来帮助您选择引导选项（例如，当重置管理员密码时）。

步骤 1 从 VSphere 客户端，右键点击 VM 并选择 **Edit Settings**。

步骤 2 点击 **Options** 选项卡。

步骤 3 选择 **Advanced > Boot Options**。

步骤 4 从 **Power on Boot Delay** 区域中，选择延迟引导操作的时间（以毫秒为单位）。

步骤 5 选中 **Force BIOS Setup** 区域的复选框，以在 VM 下次引导时进入 BIOS 设置屏幕。

步骤 6 点击 **OK**，保存更改。

在 VMware 系统上安装思科 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 要使虚拟机进入 BIOS 设置模式，请右键点击 VM，然后点击 **Edit Settings**。

步骤 3 点击 **Options** 选项卡。

步骤 4 选择 **Boot Options** 并配置以下选项：

a) 在 Force BIOS Setup 区域，虚拟机启动时，选中复选框进入 BIOS 设置屏幕。

步骤 5 点击 **OK**。

步骤 6 确保在 BIOS 中设置协调世界时间 (UTC) 和正确的引导顺序：

a) 如果打开了虚拟机，则关闭系统。

b) 打开虚拟机。
系统进入 BIOS 设置模式。

c) 在 Main BIOS 菜单中，使用箭头键导航到 Date and Time 字段，并按 **Enter**。

d) 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。

e) 使用箭头键导航到 Boot 菜单，并按 **Enter**。

f) 使用箭头键选择 CD-ROM，并按 + 将 CD-ROM 驱动器的启动顺序向上移动。

g) 使用箭头键导航到 Exit 菜单，并选择 **Exit Saving Changes**。

h) 选择 **Yes** 保存更改并退出。

步骤 7 将思科 ISE 软件 DVD 插入 VMware ESXi 主机 CD/DVD 驱动器，并打开虚拟机。
当 DVD 启动时，控制台会显示以下内容：

```
Cisco ISE Installation (Serial Console)
Cisco ISE Installation (Keyboard/Monitor)
System Utilities (Serial Console)
System Utilities (Keyboard/Monitor)
```

步骤 8 使用箭头键选择 **Cisco ISE Installation (Serial Console)** 或 **Cisco ISE Installation (Keyboard/Monitor)**，并按 **Enter**。如果选择串行控制台选项，则应在您的虚拟机上设置串行控制台。有关如何创建控制台的信息，请参阅 VMware vSphere 文档。

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:
```

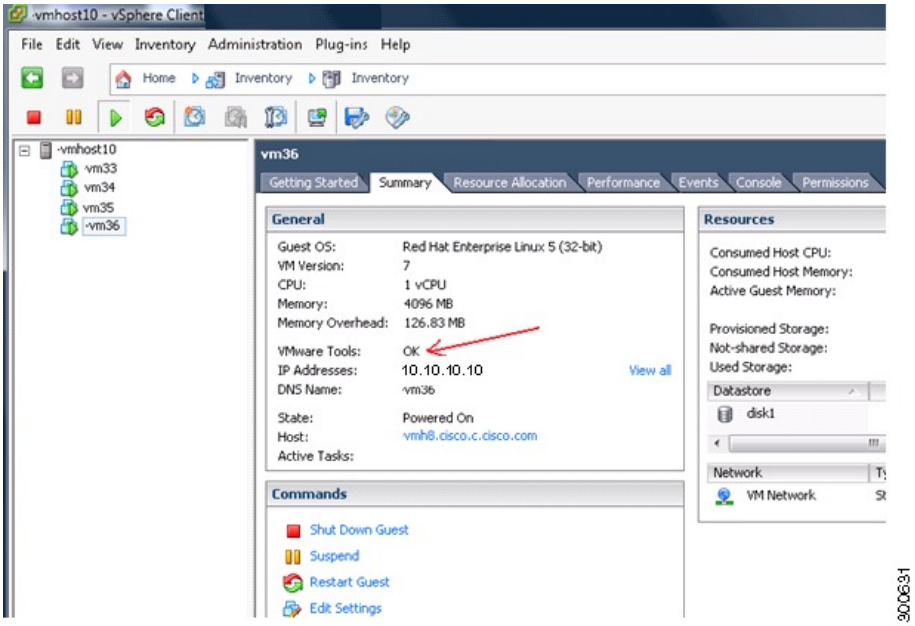
步骤 9 在系统提示符后，输入 **setup** 并按 **Enter**。
系统将显示安装向导并引导您完成初始配置。

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 7：在 *vSphere* 客户端中验证 *VMware* 工具



使用 CLI 验证 VMWare 工具安装

您也可以使用 **show inventory** 命令验证 VMware 工具是否已安装。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。

克隆思科 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。

注释 要进行克隆，需要使用 VMware vCenter。克隆必须在运行安装程序之前完成。

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 以获有管理权限的用户的身份（根用户）登录 ESXi 服务器。
执行此步骤需要 VMware vCenter。

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 的主机或集群，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 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

使用模板克隆思科 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：

开始之前

注释 要进行克隆，需要使用 VMware vCenter。克隆必须在运行安装程序之前完成。

步骤 1 创建虚拟机模板，第 38 页

步骤 2 部署虚拟机模板，第 39 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的身份（根用户）登录 ESXi 服务器。
执行此步骤需要 VMware vCenter。

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 选择您要在其上存储模板的 ESXi 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 选择您要在其上存储新思科 ISE 节点的 ESXi 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

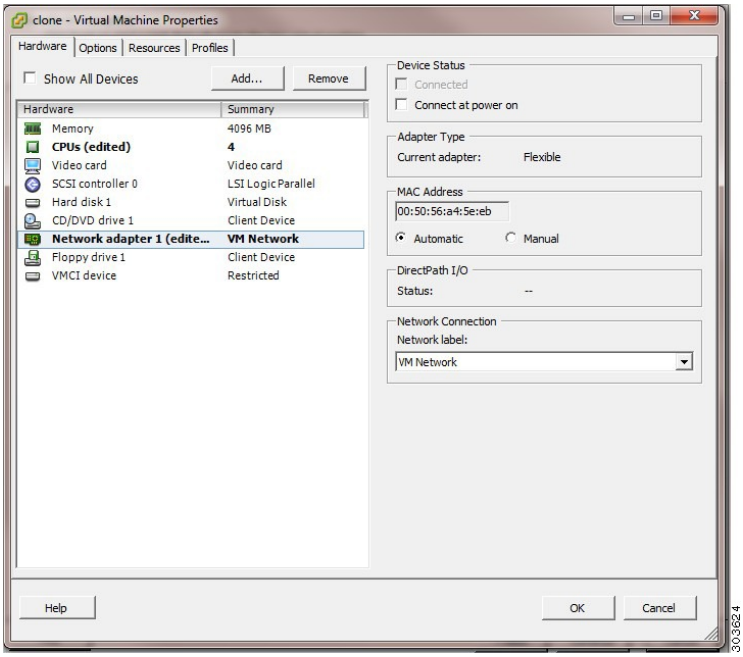
更改克隆虚拟机的 IP 地址和主机名

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 *8*：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 右键点击最近克隆的 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**。

将思科 ISE VM 从评估环境迁移至生产环境

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。

使用 Show Tech Support 命令按需检查虚拟机性能

您随时可以从 CLI 运行 **show tech-support** 命令来检查 VM 性能。此命令的输出类似如下：

```
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：

```
  Cisco ISE Installation (Serial Console)
  Cisco ISE Installation (Keyboard/Monitor)
  System Utilities (Serial Console)
  System Utilities (Keyboard/Monitor)
```

使用箭头键选择 **System Utilities (Serial Console)** 或 **System Utilities (Keyboard/Monitor)**，然后按 **Enter**。以下屏幕随即显示：

```
Available System Utilities:

  [1] Recover administrator password
  [2] Virtual Machine Resource Check
  [3] Perform System Erase
  [q] Quit and reload

Enter option [1 - 3] q to Quit
```

输入 **2** 检查 VM 资源。输出将类似于 如下：

```
*****
***** 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…
```

Linux KVM

KVM 虚拟化检查

KVM 虚拟化需要主机处理器提供的虚拟化支持；包括 Intel 处理器的 Intel VT-x 和 AMD 处理器的 AMD-V。在主机上打开一个终端窗口，然后输入 **cat /proc/cpuinfo** 命令。您会看到 vmx 或 svm 标志。

- 对于 Intel VT-x：

```
# cat /proc/cpuinfo
flags: fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca cmov pat pse36 clflush
 dts acpi mmx fxsr sse sse2 ss ht tm pbe syscall nx
pdpe1gb rdtscp lm constant_tsc arch_perfmon pebs bts rep_good nopl xtopology nonstop_tsc
 aperfmperf eagerfpu pni pclmulqdq dtes64 monitor
ds_cpl vmx smx est tm2 ssse3 cx16 xtpr pdcm pcid dca sse4_1 sse4_2 x2apic popcnt
tsc_deadline_timer aes xsave avx lahf_lm arat epb xsaveopt
pln pts dtherm tpr_shadow vnmi flexpriority ept vpid
```

- 对于 AMD-V：

```
# cat /proc/cpuinfo
flags: fpu tsc msr pae mce cx8 apic mtrr mca cmov pat pse36 clflush mmx fxsr sse sse2
 ht syscall nx mmxext fxsr_opt rdtscp lm 3dnowext 3dnow
 pni cx16 lahf_lm cmp_legacy svm cr8_legacy
```

在 KVM 上安装思科 ISE

此过程介绍如何在 RHEL 上创建 KVM，并使用虚拟机管理器 (virt-manager) 在 KVM 上安装思科 ISE。

如果您选择通过 CLI 安装思科 ISE，请输入类似如下的命令：
#virt-install --name=*kvm-ise1* **--arch=x86_64 --cpu=host --vcpus=2 --ram=4096**
--os-type=linux --os-variant=rhel6 --hvm --virt-type=kvm
--cdrom=*/home/admin/Desktop/ise-2.2.0.470.SPA.x86_64.iso*
--disk=*/home/libvirt-images/kvm-ise1.img,size=100*
--network type=direct,model=virtio,source=*eth2***,source_mode=bridge**

其中 *ise-2.2.0.470.SPA.x86_64.iso* 是思科 ISE ISO 映像的名称。

开始之前

将思科 ISE ISO 映像文件下载至本地系统。

步骤 1 从 virt-manager 中点击 **New**。
Create a new virtual machine 窗口随即会显示。

步骤 2 点击 **Local install media (ISO media or CDROM)**，然后点击 **Forward**。

步骤 3 点击 **Use ISO image** 单选按钮，点击 **Browse**，然后从本地系统中选择 ISO 映像。

a) 取消选中 **Automatically detect operating system based on install media** 复选框，选择 Linux 作为 OS type，选择 Red Hat Enterprise Linux 7.0 作为 Version，然后点击 **Forward**。

步骤 4 选择 RAM 和 CPU 设置，然后点击 **Forward**。

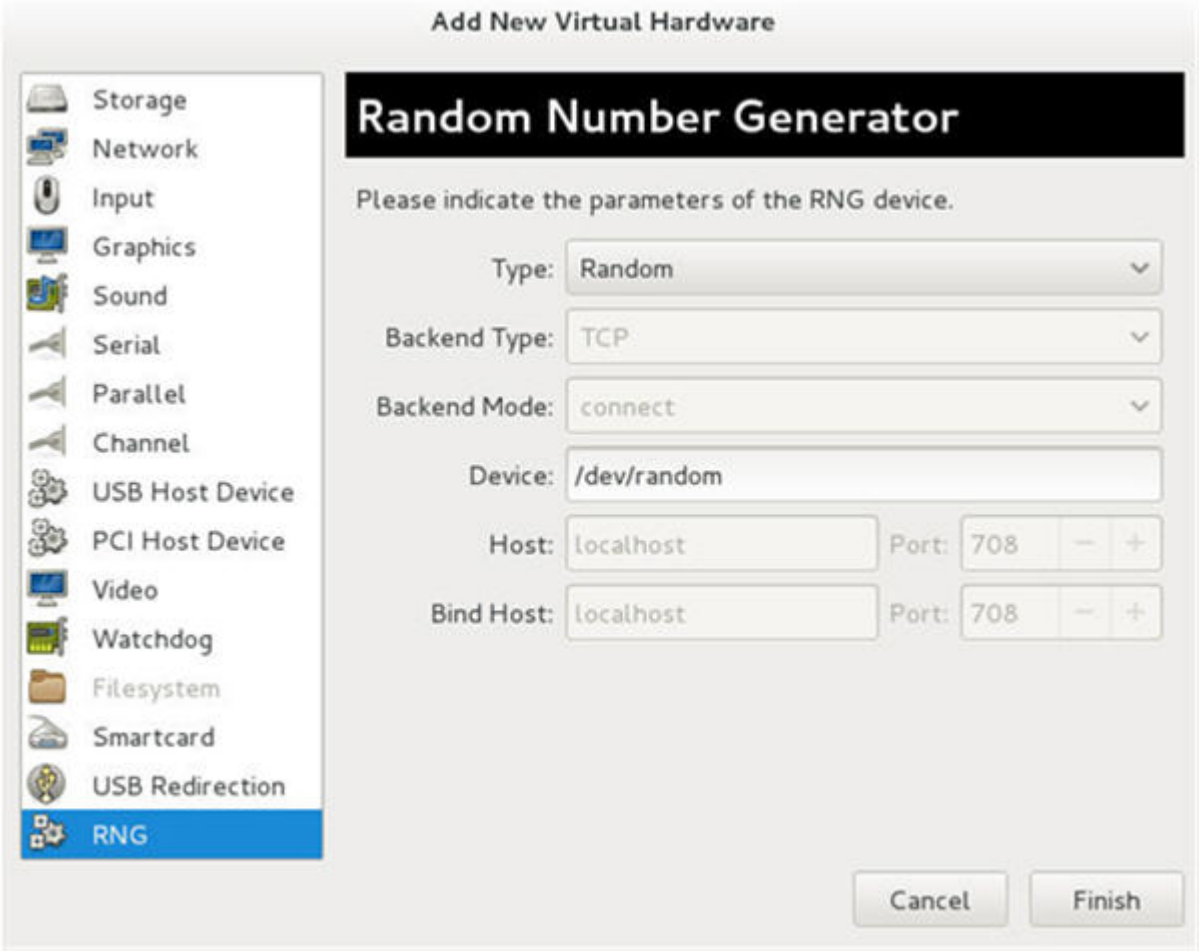
步骤 5 选中 **Enable storage for this virtual machine** 复选框，并选择存储设置。

a) 点击 **Select managed or other existing storage** 单选按钮。
b) 点击 **Browse**。
c) 从左侧的 Storage Pools 导航窗格中，点击 **disk FileSystem Directory**。
d) 点击 **New Volume**。
Create storage volume 窗口随即显示。
e) 为存储卷输入名称。
f) 从 **Format** 下拉列表中选择 **raw**。
g) 输入 Maximum Capacity。
h) 点击 **Finish**。
i) 选择您创建的卷，然后点击 **Choose Volume**。
j) 点击 **Forward**。
Ready to begin the installation 屏幕随即会显示。

步骤 6 选中 **Customize configuration before install** 复选框。

步骤 7 在 Advanced 选项下，选择 macvtap 作为接口源，在 Source mode 下拉列表中选择 Bridge，然后点击 **Finish**。

a) （可选）点击 **Add Hardware** 可添加其他 NIC。
选择 macvtap 作为 Network source，选择 virtio 作为 Device model。
b) 要支持 RHEL 7，KVM 虚拟管理器必须支持随机数发生器 (RNG) 硬件。请参阅下图了解 RNG 配置。



如果使用 CLI 创建新的 VM，请务必包含以下设置：

```
<rng model='virtio'
   <backend model='random'>/dev/random</backend>
   <address type='pci' domain='0x0000' bus='0x00' slot='0x08' function='0x0'/>
</rng>
```

c) 点击 **Finish**。

步骤 8 在 Virtual Machine 屏幕中，选择磁盘设备，并在 Advanced 和 Performance 选项下，选择以下选项，然后点击 **Apply**。

字段	值
Disk bus	VirtIO
Cache mode	none
IO mode	native

步骤 9 点击 **Begin Installation** 在 KVM 上安装思科 ISE。

思科 ISE 安装启动菜单随即会显示。

步骤 10 在系统提示符后，输入 **1** 选择显示器和键盘端口，或输入 **2** 选择控制器端口，并按 **Enter**。
安装程序将在 VM 上开始安装思科 ISE 软件。安装过程完成后，控制台随即会显示：

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

步骤 11 在系统提示符后，输入 **setup** 并按 **Enter**。
系统随即会显示安装向导并引导您完成初始配置。

Microsoft Hyper-V

在 Hyper-V 上创建思科 ISE 虚拟机

本部分介绍如何创建新虚拟机、将 ISO 映像从本地磁盘映射至虚拟 CD/DVD 驱动器、编辑 CPU 设置以及在 Hyper-V 上安装思科 ISE。

开始之前

将思科 ISE ISO 映像文件从 Cisco.com 下载至本地系统。

步骤 1 在受支持的 Windows 服务器上启动 Hyper-V Manager。

步骤 2 右键点击 VM 主机，然后点击 **New > Virtual Machine**。

步骤 3 点击 **Next** 以自定义 VM 配置。

步骤 4 为虚拟机输入名称（可选），并选择一条其他路径来存储 VM，然后点击 **Next**。

步骤 5 点击 **Generation 1** 单选按钮，然后点击 **Next**。

步骤 6 指定分配给此 VM 的内存量（例如 16000 MB），然后点击 **Next**。

步骤 7 选择网络适配器，然后点击 **Next**。

步骤 8 点击 **Create a virtual hard disk** 单选按钮，然后点击 **Next**。

步骤 9 点击 **Install an operating system from a bootable CD/DVD-ROM** 单选按钮。

a) 从 Media 区域中，点击 **Image file (.iso)** 单选按钮。

b) 点击 **Browse** 以从本地系统选择 ISE ISO 映像，然后点击 **Next**。

步骤 10 点击 **Finish**。
思科 ISE VM 已在 Hyper-V 上创建完成。

步骤 11 选择 VM 并编辑 VM 设置。

a) 选择 **Processor**。输入虚拟处理器的数量（例如 6），然后点击 **OK**。

步骤 12 选择 VM，然后点击 **Connect** 启动 VM 控制台。点击启动按钮以打开思科 ISE VM。

思科 ISE 安装菜单随即会显示。

步骤 13 输入 1 使用键盘和显示器安装思科 ISE。

第 5 章

安装后任务

本章提供安装后必须立即执行的任务列表。

登录到思科 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

思科 ISE 管理门户支持以下支持 HTTPS 的浏览器：

- Mozilla Firefox 版本 45.*x* ESR 和 48.0 及更高版本
- Google Chrome 版本 53.0 及更高版本
- Microsoft Internet Explorer 10.*x* 和 11.*x*

如果使用 Internet Explorer 10.x，需启用 TLS 1.1 和 TLS 1.2，并禁用 SSL 3.0 和 TLS 1.0（Internet 选项 > 高级）。

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**。

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 7：*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。

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。

因管理员锁定而重置密码

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。

按照这些指令，使用思科 ISE CLI 中的 **application reset-passwd ise** 命令重置管理员用户接口密码。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 ise administrator_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
```

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 在系统提示时，输入 **show application version ise** 并按 **Enter**。

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      : 2.2.0.349
Build Date   : Wed Oct 12 22:00:39 2016
Install Date : Thu Oct 13 11:26:00 2016

ise-vm123/admin# show application version ise

Cisco Identity Services Engine
------------------------------------------
Version      : 2.2.0.349
Build Date   : Wed Oct 12 22:00:39 2016
Install Date : Thu Oct 13 11:26:00 2016
```

步骤 6 要查看思科 ISE 进程的状态，请输入 **show application status ise** 并按 **Enter**。

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          4930
Database Server                        running          66 PROCESSES
Application Server                     running          8231
Profiler Database                      running          6022
ISE Indexing Engine                    running          8634
AD Connector                           running          9485
```

```
M&T Session Database                  running          3059
M&T Log Collector                     running          9271
M&T Log Processor                     running          9129
Certificate Authority Service         running          8968
EST Service                           running          18887
SXP Engine Service                    disabled
TC-NAC Docker Service                 disabled
TC-NAC MongoDB Container              disabled
TC-NAC RabbitMQ Container             disabled
TC-NAC Core Engine Container          disabled
VA Database                           disabled
VA Service                            disabled
pxGrid Infrastructure Service         disabled
pxGrid Publisher Subscriber Service   disabled
pxGrid Connection Manager             disabled
pxGrid Controller                     disabled
PassiveID Service                     disabled
DHCP Server (dhcpd)                   disabled
DNS Server (named)                    disabled
```

安装后任务列表

安装思科 ISE 后，您必须执行以下必要任务：

表 *8*：必要的安装后任务

任务	管理指南中的链接
应用最新补丁（如果有）	安装软件补丁
安装许可证	有关详细信息，请参阅思科 ISE 订购指南。有关如何注册许可证的信息，请参阅管理指南。
安装证书	有关详细信息，请参阅《思科 ISE 管理指南》中的管理证书一章。
创建备份存储库	有关详细信息，请参阅《思科 ISE 管理指南》中的创建存储库一节。
配置备份计划	有关详细信息，请参阅《思科 ISE 管理指南》中的计划备份一节。
部署思科 ISE 角色	请参阅《思科 ISE 管理指南》中的在分布式环境中设置思科 ISE 一章。

第 6 章

维护任务

本章列出安装后可以执行的多项维护任务。这些任务是独立的，可以按任意顺序执行。

绑定以太网接口以实现高可用性

思科 ISE 支持将两个以太网接口绑定为一个虚拟接口，以为物理接口提供高可用性。此功能称为网络接口卡 (NIC) 绑定或 NIC 分组。两个接口绑定在一起时，两个 NIC 似乎是具有单个 MAC 地址的单台设备。

思科 ISE 中的 NIC 绑定功能不支持负载均衡或链路汇聚功能。思科 ISE 仅支持 NIC 绑定的高可用性功能。

接口绑定可以确保思科 ISE 服务在下列情况下不受影响：

- 物理接口故障
- 交换机端口断开连接（关闭或出现故障）
- 交换机线卡故障

两个接口绑定在一起时，其中一个接口将成为主接口，另一个接口成为备用接口。两个接口绑定在一起时，正常情况下，所有流量都会流经主接口。如果主接口因某种原因出现故障，则备用接口承接此任务，并处理所有流量。绑定将采用主接口的 IP 地址和 MAC 地址。

当您配置 NIC 绑定功能时，思科 ISE 会与固定的物理 NIC 配对，以形成绑定的 NIC。下表列出了哪些 NIC 可以绑定在一起形成绑定的接口。

思科 ISE 物理 NIC 名称	Linux 物理 NIC 名称	绑定的 NIC 中的角色	绑定的 NIC 名称
千兆以太网 0	Eth0	主服务器	绑定 0
千兆以太网 1	Eth1	备份	
千兆以太网 2	Eth2	主服务器	绑定 1
千兆以太网 3	Eth3	备份	
千兆以太网 4	Eth4	主服务器	绑定 2
千兆以太网 5	Eth5	备份	

支持的平台

NIC 绑定功能在所有受支持的平台和节点角色上都受支持。受支持的平台包括：

- SNS-3400 系列设备 - 绑定 0 和 1（思科 ISE 3400 系列设备最多支持 4 个 NIC）
- SNS-3500 系列工具 - 绑定 0、1 和 2
- VMware 虚拟机 - 绑定 0、1 和 2（如果六个 NIC 可用于虚拟机）
- Linux KVM 节点 - 绑定 0、1 和 2（如果六个 NIC 可用于虚拟机）

绑定以太网接口指南

- 由于思科 ISE 最多可支持六个以太网接口，它只能有三个绑定，即绑定 0、绑定 1 和绑定 2。
- 您不能更改属于某个绑定的接口，也不能更改绑定中接口的角色。请参阅上表，了解有关如何将 NIC 绑定在一起及其在绑定中的角色的信息。
- Eth0 接口既用作管理接口，也用作运行时接口。其他接口用作运行时接口。
- 在您创建一个绑定之前，必须为主接口（主 NIC）分配 IP 地址。创建绑定 0 之前，必须为 Eth0 接口分配 IPv4 地址。类似地，在创建绑定 1 和 2 之前，必须为 Eth2 和 Eth4 接口分别分配 IPv4 或 IPv6 地址。
- 在您创建一个绑定之前，如果为备用接口（Eth1、Eth3 和 Eth5）分配了 IP 地址，请将该 IP 地址从备用接口删除。不应该给备用接口分配 IP 地址。
- 您可以选择仅创建一个绑定（绑定 0），并让剩余接口保持不变。在这种情况下，绑定 0 作为管理接口和运行时接口，剩余接口作为运行时接口。
- 您可以更改绑定中主接口的 IP 地址。绑定的接口将被分配新的 IP 地址，因为该地址将用作主接口的 IP 地址。

- 当您删除两个接口之间的绑定时，为绑定的接口分配的 IP 地址将重新分配给主接口。
- 如果要在属于某个部署的思科 ISE 节点上配置 NIC 绑定功能，则必须从部署中取消注册该节点，配置 NIC 绑定，然后将该节点重新注册到部署中。
- 如果作为某绑定中的主接口（Eth0、Eth2 或 Eth4）的物理接口配置了静态路由，则这些静态路由将自动更新，以在绑定的接口而非该物理接口上运行。

配置 NIC 绑定

您可以从思科 ISE CLI 配置 NIC 绑定。以下程序介绍了如何在 Eth0 和 Eth1 接口之间配置绑定 0。

开始之前

如果为一个充当备用接口的物理接口（例如 Eth1、Eth3，Eth5 接口）配置了 IP 地址，则必须从备用接口删除该 IP 地址。不应为备用接口分配 IP 地址。

步骤 1 使用您的管理员帐户登录思科 ISE CLI。

步骤 2 输入 **configure terminal** 进入配置模式。

步骤 3 输入 **interface GigabitEthernet 0** 命令。

步骤 4 输入 **backup interface GigabitEthernet 1** 命令。
控制台会显示：

```
 % Warning: IP address of interface eth1 will be removed once NIC bonding is enabled. Are you sure
you want to proceed? Y/N [N]:
```

步骤 5 输入 **Y** 并按 **Enter**。
绑定 0 现已配置。思科 ISE 会自动重启。等待一段时间，以确保所有服务均已成功启动和运行。从 CLI 中输入 **show application status ise** 命令，检查是否所有服务都在运行。

```
ise/admin# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ise/admin(config)# interface gigabitEthernet 0
ise/admin(config-GigabitEthernet)# backup interface gigabitEthernet 1
Changing backup interface configuration may cause ISE services to restart.
Are you sure you want to proceed? Y/N [N]: Y
Stopping ISE Monitoring & Troubleshooting Log Collector...
Stopping ISE Monitoring & Troubleshooting Log Processor...
ISE PassiveID Service is disabled
ISE pxGrid processes are disabled
Stopping ISE Application Server...
Stopping ISE Certificate Authority Service...
Stopping ISE EST Service...
ISE Sxp Engine Service is disabled
Stopping ISE Profiler Database...
Stopping ISE Indexing Engine...
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 Application Server...
Starting ISE Indexing Engine...
Starting ISE Certificate Authority Service...
```

```
Starting ISE EST Service...
Starting ISE Monitoring & Troubleshooting Log Processor...
Starting ISE Monitoring & Troubleshooting Log Collector...
Starting ISE AD Connector...
Note: ISE Processes are initializing. Use 'show application status ise'
      CLI to verify all processes are in running state.
ise/admin(config-GigabitEthernet)#
```

验证 NIC 绑定配置

要验证 NIC 绑定功能是否已配置，请从思科 ISE CLI 运行 **show running-config** 命令。您会看到类似如下的输出：

```
!
interface GigabitEthernet 0
  ipv6 address autoconfig
  ipv6 enable
  backup interface GigabitEthernet 1
  ip address 192.168.118.214 255.255.255.0
!
```

在上面的输出中，“备用接口千兆以太网 1”表示在千兆以太网 0 上配置了 NIC 绑定，其中千兆以太网 0 作为主接口，千兆以太网 1 作为备用接口。 此外，尽管主接口和备用接口实际上具有相同的 IP 地址，但 ADE-OS 配置不会在运行配置中的备用接口上显示 IP 地址。

您也可以运行 **show interfaces** 命令查看绑定的接口。

```
ise/admin# show interface
bond0: flags=5187<UP,BROADCAST,RUNNING,MASTER,MULTICAST>  mtu 1500
        inet 10.126.107.60  netmask 255.255.255.0  broadcast 10.126.107.255
        inet6 fe80::8a5a:92ff:fe88:4aea  prefixlen 64  scopeid 0x20<link>
        ether 88:5a:92:88:4a:ea  txqueuelen 0  (Ethernet)
        RX packets 1726027  bytes 307336369 (293.0 MiB)
        RX errors 0  dropped 844  overruns 0  frame 0
        TX packets 1295620  bytes 1073397536 (1023.6 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

GigabitEthernet 0
        flags=6211<UP,BROADCAST,RUNNING,SLAVE,MULTICAST>  mtu 1500
        ether 88:5a:92:88:4a:ea  txqueuelen 1000  (Ethernet)
        RX packets 1726027  bytes 307336369 (293.0 MiB)
        RX errors 0  dropped 844  overruns 0  frame 0
        TX packets 1295620  bytes 1073397536 (1023.6 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
        device memory 0xfab00000-fabfffff

GigabitEthernet 1
        flags=6147<UP,BROADCAST,SLAVE,MULTICAST>  mtu 1500
        ether 88:5a:92:88:4a:ea  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
        device memory 0xfaa00000-faafffff
```

删除 NIC 绑定

使用 **no** 形式的 **backup interface** 命令删除 NIC 绑定。

开始之前

步骤 1 使用您的管理员帐户登录思科 ISE CLI。

步骤 2 输入 **configure terminal** 进入配置模式。

步骤 3 输入 **interface GigabitEthernet 0** 命令。

步骤 4 输入 **no backup interface GigabitEthernet 1** 命令。

```
% Notice: Bonded Interface bond 0 has been removed.
```

步骤 5 输入 **Y**，然后按 Enter。

绑定 0 现已删除。思科 ISE 会自动重启。等待一段时间，以确保所有服务均已成功启动和运行。从 CLI 中输入 **show application status ise** 命令，检查是否所有服务都在运行。

```
ise/admin# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ise/admin(config)# interface gigabitEthernet 0
ise/admin(config-GigabitEthernet)# no backup interface gigabitEthernet 1

Changing backup interface configuration may cause ISE services to restart.
Are you sure you want to proceed? Y/N [N]: Y
Stopping ISE Monitoring & Troubleshooting Log Collector...
Stopping ISE Monitoring & Troubleshooting Log Processor...
ISE PassiveID Service is disabled
ISE pxGrid processes are disabled
Stopping ISE Application Server...
Stopping ISE Certificate Authority Service...
Stopping ISE EST Service...
ISE Sxp Engine Service is disabled
Stopping ISE Profiler Database...
Stopping ISE Indexing Engine...
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 Application Server...
Starting ISE Indexing Engine...
Starting ISE Certificate Authority Service...
Starting ISE EST Service...
Starting ISE Monitoring & Troubleshooting Log Processor...
Starting ISE Monitoring & Troubleshooting Log Collector...
Starting ISE AD Connector...
Note: ISE Processes are initializing. Use 'show application status ise'
      CLI to verify all processes are in running state.
ise/admin(config-GigabitEthernet)#
```

更改思科 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。
- 更改思科 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.
```

思科 ISE 会提示您重启系统。

步骤 3 输入 **Y** 重启系统。

查看安装和升级历史

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: Thu Oct 13 16:29:35 UTC 2016
Application: ise
Version: 2.2.0.349
Install type: Application Install
Bundle filename: ise.tar.gz
Repository: SystemDefaultPkgRepos
```

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 3515 控制台会显示以下消息：

```
Cisco ISE Installation (Serial Console)
Cisco ISE Installation (Keyboard/Monitor)
System Utilities (Serial Console)
System Utilities (Keyboard/Monitor)
```

步骤 3 使用箭头键选择 **System Utilities (Serial Console)**，并按 Enter。
系统随即会显示 ISO 实用程序菜单，如下所示：

```
Available System Utilities:

[1] Recover administrator password
[2] Virtual Machine Resource Check
[3] System Erase
[q] Quit and reload

Enter option [1 - 3] q to Quit:
```

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   **********
THIS UTILITY WILL PERFORM A SYSTEM ERASE ON THE DISK DEVICE(S). THIS PROCESS CAN TAKE UP TO 5 HOURS
 TO COMPLETE. THE RESULT WILL BE COMPLETE
DATA LOSS OF THE HARD DISK. THE SYSTEM WILL NO LONGER BOOT AND WILL REQUIRE A RE-IMAGE FROM INSTALL
 MEDIA TO RESTORE TO FACTORY DEFAULT STATE.

ARE YOU SURE YOU WANT TO CONTINUE? [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。

第 7 章

思科 ISE 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。
- 思科 ISE 服务器接口不支持 VLAN 标记。请务必在连接到思科 ISE 节点所用的交换机端口上禁用 VLAN 中继，并将这些端口配置为接入层端口。
- 所有 NIC 都可以配置有 IP 地址。

Cisco ISE 管理节点端口

Cisco ISE 服务	千兆以太网 0 或绑定 0 上的端口	其他以太网接口（千兆以太网 1 至 5 或绑定 1 和绑定 2）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 • 要从管理 GUI 显示发起者门户：TCP/9002 • ElasticSearch（情景可视性；将数据从主管理节点复制到辅助管理节点）：TCP/9300 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。 对 Cisco ISE 的 HTTPS 和 SSH 访问只限于千兆以太网 0。 TCP/9300 必须在主管理节点和辅助管理节点上对传入流量开放。	-
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 或绑定 0 上的端口	其他以太网接口（千兆以太网 1 至 5 或绑定 1 和绑定 2）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 KPASS：TCP/464 • WMI：TCP/135 • ODBC： 注释 ODBC 端口可在第三方数据库服务器上配置。 Microsoft SQL：TCP/1433 Sybase：TCP/2638 PortgreSQL：TCP/5432 Oracle：TCP/1512 • 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	
智能许可	通过 TCP/443 连接至思科云	

Cisco ISE 监控节点端口

Cisco ISE 服务	千兆以太网 0 或绑定 0 上的端口	其他以太网接口（千兆以太网 1 至 5 或绑定 1 和绑定 2）上的端口
管理	• HTTP：TCP/80 和 HTTPS：TCP/443 • SSH 服务器：TCP/22	-
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
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	

Cisco ISE 服务	千兆以太网 0 或绑定 0 上的端口	其他以太网接口（千兆以太网 1 至 5 或绑定 1 和绑定 2）上的端口
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 • WMI：TCP/135 • ODBC： 注释 ODBC 端口可在第三方数据库服务器上配置。 Microsoft SQL：TCP/1433 Sybase：TCP/2638 PortgreSQL：TCP/5432 Oracle：TCP/1512 • 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。	
pxGrid 批量下载	SSL：TCP/8910	

Cisco ISE 策略服务节点端口

Cisco ISE 服务	千兆以太网 0 或绑定 0 上的端口	其他以太网接口上或绑定 1 和绑定 2 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 服务	千兆以太网 0 或绑定 0 上的端口	其他以太网接口上或绑定 1 和绑定 2 上的端口
复制和同步	• HTTPS (SOAP)：TCP/443 • 数据同步/复制 (JGroups)：TCP/12001（全局）	—
集群（节点组）	节点组/JGroups：TCP/7800	-
CA PKI	TCP/9090	-
IPSec/ISAKMP	UDP/500	-
设备管理	TACACS+：TCP/49 注释 此端口可在版本 2.1 及更高版本中配置。	
SXP	• PSN（SXP 节点）到 NAD：TCP/64999 • PSN 到 SXP（节点间通信）：TCP/443	
TC-NAC	TCP/443	
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 或绑定 0 上的端口	其他以太网接口上或绑定 1 和绑定 2 上的端口
会话	• RADIUS 身份验证：UDP/1645 和 1812 • RADIUS 记帐：UDP/1646 和 1813 • RADIUS DTLS 身份验证/记帐：UDP/2083 • 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 • WMI：TCP/135 • ODBC： 注释 ODBC 端口可在第三方数据库服务器上配置。 Microsoft SQL：TCP/1433 Sybase：TCP/2638 PortgreSQL：TCP/5432 Oracle：TCP/1512 • 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。	
被动 ID（入站）	• TS 代理：tcp/9094 • AD 代理：tcp/9095 • 系统日志：UDP/40514 和 TCP/11468	

Cisco ISE 服务	千兆以太网 0 或绑定 0 上的端口	其他以太网接口上或绑定 1 和绑定 2 上的端口
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 - 证书调配 - 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。） • 证书调配门户：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	
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”。 思科 ISE 在 TCP 端口 8905 上提供安全评估和客户端调配管理证书。 思科 ISE 在 TCP 端口 8443（或者您为使用门户而配置的端口）上提供门户证书。 • 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)	

Cisco ISE 服务	千兆以太网 0 或绑定 0 上的端口	其他以太网接口上或绑定 1 和绑定 2 上的端口
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 或绑定 0 上的端口	其他以太网接口上或绑定 1 和绑定 2 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。	

Cisco ISE pxGrid 服务端口

Cisco ISE 服务	千兆以太网 0 或绑定 0 上的端口	其他以太网接口（千兆以太网 1 至 5 或绑定 1 和绑定 2）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

尽管思科 ISE 服务和端口参考分别列出了在思科 ISE 管理节点、策略服务节点监控节点中所用的基本端口，但对于在线证书状态协议服务 (OCSP) 和证书撤销列表 (CRL)，端口取决于 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。